UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
DEPARTAMENTO DE ELETRÔNICA E SISTEMAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

RAVI BARRETO DORIA FIGUEIREDO

MAPAS TANGENTE-CHEBYSHEV SOBRE CORPOS FINITOS:
contribuições teóricas e cenários de aplicação

Recife
2023

RAVI BARRETO DORIA FIGUEIREDO

MAPAS TANGENTE-CHEBYSHEV SOBRE CORPOS FINITOS:
contribuições teóricas e cenários de aplicação

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração: Comunicações.

Orientador: Prof. Dr. Juliano Bandeira Lima

Recife
2023

Catalogação na fonte
Bibliotecária Margareth Malta, CRB-4 / 1198

F475m Figueiredo, Ravi Barreto Doria.
Mapas tangente-Chebyshev sobre corpos finitos: contribuições teóricas e cenários de aplicação / Ravi Barreto Doria Figueiredo. – 2023.
61 f.: il., figs., tabs., abrev. e siglas.

Orientador: Prof. Dr. Juliano Bandeira Lima.
Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2023.
Inclui Referências e Apêndice.

1. Engenharia Elétrica. 2. Corpos finitos. 3. Mapas sobre corpos finitos. 4. Polinômios sobre corpos finitos. 5. Polinômios de Chebyshev. 6. Trigonometria sobre corpos finitos. 7. Permutações. 8. Involuções. Criptografia. I. Lima, Juliano Bandeira (Orientador). II. Título.

UFPE

621.3 CDD (22. ed.) BCTG/2024-69

RAVI BARRETO DORIA FIGUEIREDO

MAPAS TANGENTE-CHEBYSHEV SOBRE CORPOS FINITOS:
contribuições teóricas e cenários de aplicação

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração: Comunicações.

Aprovada em: 09/08/2023.

Participação por videoconferência
Prof. Dr. Juliano Bandeira Lima (Orientador)
Universidade Federal de Pernambuco

Participação por videoconferência
Prof. Dr. Ricardo Menezes Campello de Souza (Examinador Interno)
Universidade Federal de Pernambuco

Participação por videoconferência
Prof. Dr. José Rodrigues de Oliveira Neto (Examinador Interno)
Universidade Federal de Pernambuco

Participação por videoconferência
Prof. Dr. José Sampaio de Lemos Neto (Examinador Externo)
Universidade Federal de Pernambuco

Participação por videoconferência
Prof. Dr. Francisco Madeiro Bernardino Jr. (Examinador Externo)
Escola Politécnica de Pernambuco
Universidade de Pernambuco

AGRADECIMENTOS

Primeiramente gostaria de agradecer a minha esposa Lucianna, por ser essa companheira incrível que essa vida me deu e por me aceitar da maneira que sou. Aos meus pais, Renan e Marizi, por abrir minha mente e pelo apoio que me deram em toda minha vida. Agradeço também aos meu queridos irmãos, Isa, Daniel, Paula, e os irmãos que a vida me deu, Tatianna e Julio. Agradeço aos momentos que estivemos juntos. E claro a minha querida sogra Germana. Agradeço a todos pelo grande apoio que me deram

Aos meus companheiros da pós-graduação, os colegas que fiz durante essa Jornada, agradeço a Carlos, Bruno Vinicious, Diego Canterle, José, Veruska, José Neto, Felipe e todos aqueles que estudamos e nos apoiamos nessa jornada. Um agradecimento especial para meu orientador Juliano, por acreditar em mim, as vezes mais do que eu mesmo, e por ser essa pessoal gentil que ele apresenta e representa. Agradeço aos meus professores Ricardo Campello, por ser, na minha percepção, é um modelo a ser seguido, Daniel Chaves, Cecílio Pimentel e Valdemar Costa pelas ótimas aulas e por todo o conhecimento que me passaram.

RESUMO

O estudo de mapas definidos sobre corpos finitos tem despertado grande interesse da comunidade científica interessada tanto em aspectos teóricos, quanto em cenários de aplicação. Existem, em particular, diversas famílias de mapas polinomiais e racionais, cuja utilidade em criptografia e em códigos corretores de erros, por exemplo, tem sido demonstrada. Nesse contexto, o presente trabalho possui como ponto de partida os recém-introduzidos mapas racionais do tipo tangente-Chebyshev, cuja definição, que se assemelha à dos bem conhecidos polinômios de Chebyshev do primeiro tipo, emprega funções trigonométricas em corpos finitos. Como contribuições originais desta tese, são apresentadas novas propriedades desses mapas, as quais incluem seus pontos fixos, sua relação com outros mapas e sua representação por meio de grafos. Além disso, é proposta a definição de um novo tipo de mapa tangente-Chebyshev, o qual possui, de certa forma, analogia com os polinômios de Chebyshev do terceiro tipo. Também são estudadas propriedades desses últimos mapas, o que inclui seu cálculo por meio de equações de recorrência, sua relação com os mapas tangente-Chebyshev (do primeiro tipo) e a especificação de seus zeros e polos. Por fim, é investigada a possibilidade de seu uso em esquemas de criptografia de chave pública.

Palavras-chave: corpos finitos; mapas sobre corpos finitos; polinômios sobre corpos finitos; polinômios de chebyshev; trigonometria sobre corpos finitos; permutações; involuções; criptografia.

ABSTRACT

The study of maps defined over finite fields has attracted the attention of researchers interested both in theoretical aspects and in application scenarios. In particular, there are several families of polynomial and rational maps, whose usefulness in cryptography and in error-correcting codes, for example, has been demonstrated. In this context, the present work has as its starting point the recently introduced tangent-Chebyshev rational maps, whose definition, which is similar to that of the well-known Chebyshev polynomials of the first kind, employs finite field trigonometric functions. As original contributions of this thesis, new properties of the referred maps are presented, which include their fixed points, their relationship with other maps and their representation by means of graphs. Furthermore, the definition of a new type of tangent-Chebyshev map is proposed; in a certain sense, it is analogous to the Chebyshev polynomial of the third kind. Properties of such maps are also studied, which includes their computation by means of recurrence equations, their relationship with tangent-Chebyshev maps (of the first kind) and the specification of their zeros and poles. Finally, the applicability of the investigated maps in the possibility of their use in public key cryptography schemes is illustrated.

Keywords: finite fields. maps over finite fields. polynomials over finite fields. chebyshev polynomials. finite field trigonometry. permutations. involutions. cryptography.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{F}$	Um corpo arbitrário.
$\mathbb{F}_p$	Corpo finito de ordem p.
$\mathbb{I}_p$	Conjunto dos inteiros Gaussianos sobre $\mathbb{F}_p$.
$\mathfrak{R}\{\zeta\}$	Parte real de ζ
$\mathfrak{I}\{\zeta\}$	Parte imaginária de ζ.
$\mathrm{G}_{1,p}$	Conjunto unimodular de $\mathbb{I}_p$.
$\mathbb{T}_p$	Conjunto de todos os possíveis valores da função tangente.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{N}$	Conjunto dos números naturais.
C_n	Mapa t-Chebyshev do primeiro tipo sobre $\mathbb{F}_p$.
R_n	Função de Rèdei.
π_N	Operação de permutação de comprimento N.
T	Transformação de Möbius.
A_T	Matriz de transformação de Möbius.
D_n	Mapa t-CHebyshev do segundo tipo sofre $\mathbb{F}_p$.
Π	Permutação de uma sequência finita.
α	Elemento primitivo em $\mathbb{F}_p$.

SUMÁRIO

1 INTRODUÇÃO

Mapas definidos sobre estruturas algébricas finitas têm sido estudados desde o século XIX por pesquisadores de diversas áreas do conhecimento (LIDL; MULLEN; TURNWALD, 1993). Têm-se investigado, em particular, mapas do tipo polinomial, cujas propriedades permitem diversas aplicações em Engenharia. Nesse contexto, encontram-se os chamados polinômios de permutação, que agem como permutações dos elementos de um anel finito. Por conseguinte, um polinômio de permutação num corpo finito é um polinômio que induz bijeções sobre $\mathbb{F}_q$. Mais precisamente, seja q a potência de um primo p e $\mathbb{F}_q$ o corpo finito com q elementos; o polinômio $f(x) \in \mathbb{F}_p[x]$ é dito ser um polinômio de permutação sobre $\mathbb{F}_q$ se $f : c \to f(c)$ de $\mathbb{F}_q$ para $\mathbb{F}_q$ é uma permutação em $\mathbb{F}_q$.

Dentre os estudos relativos a polinômios sobre estruturas algébricas finitas, podem ser destacados os trabalhos de Hermite (HERMITE, 1863), em que foram considerados corpos finitos primos $\mathbb{F}_p$, e de Dickson et al. (DICKSON, 1896), em que foram considerados também corpos finitos de extensão. Dickson classificou todos os polinômios de grau até cinco e todos os polinômios de grau seis para corpos finitos de característica ímpar (DICKSON, 1896). Posteriormente, Li et al. (LI; CHANDLER; XIANG, 2010) classificaram todos os polinômios de graus seis e sete sobre corpos finitos de característica 2. Em trabalhos mais recentes, novos resultados ligados a polinômios de permutação continuam sendo estabelecidos (GUPTA; SHARMA, 2016; FAN, 2019; LIU ; SUN; ZHANG, 2018). Esses resultados têm encontrado aplicabilidade em áreas importantes como criptografia (DING; ZHOU, 2014; SCHWENK; HUBER, 1998; MURATOVIC-RIBIC; PASALIC, 2014) e teoria da codificação (LAIGLE-CHAPUY, 2007).

As questões relacionadas ao estudo de polinômios de permutação costumam ser separadas em duas categorias: classificação e enumeração. A classificação dos polinômios envolve questões como testes e critérios para um polinômio ser uma permutação e diz respeito, também, às relações entre os coeficientes, graus dos seus termos e buscas por novas famílias de polinômios. A enumeração envolve a distribuição e a quantidade de polinômios de um certo grau e a não-existência de polinômios de permutação com determinadas características. Alguns dos progressos mais recentes sobre polinômios de permutação podem ser encontrados em (HOU, 2015; LI et al., 2019; YANBIN; QIANG; WENHONG, 2020).

Uma família de polinômios bastante conhecida e que, sob determinadas condições, ao ser avaliada sobre um corpo finito, pode prover polinômios de permutação, é a dos polinômios de Chebyshev (MASON; HANDSCOMB, 2003). Originalmente, esses polinômios foram definidos sobre o corpo dos reais, empregando funções trigonométricas usuais como o seno e o cosseno; sobre corpos finitos, a sua caracterização é mais recente e possui estreita relação com a dos polinômios de Dickson avaliados sobre as mesmas estruturas algébricas (HERMITE, 1863). Definições trigonométricas para polinômios de Chebyshev sobre corpos finitos foram propostas por Lima *et al*. em (LIMA; PANARIO; CAMPELLO DE SOUZA, 2014; LIMA; PANARIO; CAMPELLO DE SOUZA, 2010b; LIMA; PANARIO; CAMPELLO DE SOUZA, 2010a),

os quais investigaram novas propriedades desses polinômios e suas possíveis aplicações em criptografia.

Lima e Campello de Souza introduziram um novo mapa sobre corpos finitos (LIMA; CAMPELLO DE SOUZA, 2019) , o mapa racional tangente-Chebyshev ou, de forma abreviada, tangente-Chebyshev. A explicação para a nomenclatura que o mapa recebeu reside no fato de que a sua definição corresponde, basicamente, à de um polinômio de Chebyshev do primeiro tipo (sobre corpos finitos), porém, substituindo as funções cosseno e cosseno inversa sobre corpos finitos, respectivamente, pelas funções tangente e tangente inversa sobre corpos finitos, introduzidas também no referido trabalho; algumas propriedades dos mapas tangente-Chebyshev foram estabelecidas, incluindo aquela referente à possibilidade de esse mapa corresponder a uma permutação dos elementos do corpo finito sobre o qual ele é definido.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

A partir da pesquisa bibliográfica realizada na fase inicial deste trabalho, foi possível identificar lacunas teóricas e possibilidades de avanço sobre o tema “mapas sobre corpos finitos”. Em particular, considerando os recém-definidos mapas tangente-Chebyshev, percebe-se que uma série de propriedades podem ser estabelecida e novas definições podem ser propostas.

1.2 OBJETIVOS

O objetivo geral deste trabalho é a caracterização dos mapas tangente-Chebyshev e o estudo de aplicações desses mapas em cenários práticos de Engenharia. Os objetivos específicos são os seguintes:

1. Estudar os pontos fixos dos mapas tangente-Chebyshev;
2. Relacionar os mapas tangente-Chebyshev com outros mapas já conhecidos na literatura, como o mapa de Rèdei e o mapa de Möbius;
3. Representar os mapas tangente-Chebyshev por meio de grafos funcionais e investigar as propriedades desses grafos;
4. Definir novos tipos de mapas tangente-Chebyshev e investigar suas propriedades;
5. Investigar o uso dos mapas tangente-Chebyshev em aplicações de criptografia.

1.3 ESTRUTURA DA TESE E CONTRIBUIÇÕES ORIGINAIS

Este Tese de tese está organizada da seguinte forma:

- No Capítulo 1, é feita uma introdução sobre mapas de permutação sobre corpos finitos, abordando os principais tópicos de pesquisa nesta área. É apresentado a motivação e justificativa e objetivos.

- No Capítulo 2, é feita uma revisão bibliográfica sobre trigonometria em corpos finitos e a respeito dos recém-definidos mapas racionais tangente-Chebyshev;
- No Capítulo 3, que é o primeiro que contém contribuições decorrentes do trabalho realizado, são estabelecidas novas propriedades dos mapas tangente-Chebyshev e providos exemplos ilustrativos de grafos funcionais relacionados a esses mapas;
- No Capítulo 4, é apresentado um novo tipo de mapa tangente-Chebyshev: o mapa tangente-Chebyshev do terceiro tipo. Também são estudadas as suas principais propriedades;
- No Capítulo 5, é realizada uma investigação preliminar a respeito do uso de mapas tangente-Chebyshev em a sua aplicabilidade em cifragem de chave pública;
- No Capítulo 6, são apresentadas as considerações finais da tese e delineadas pespectivas de trabalhos futuros;
- No Apêndice A, é apresentada uma contribuição secundária desta tese: o enunciado de um lema empregado na demonstração da invertibilidade das transformadas do cosseno dos tipos III e IV sobre corpos finitos de característica 2.

2 TRIGONOMETRIA E MAPAS TANGENTE-CHEBYSHEV SOBRE CORPOS FINITOS

Neste capítulo são revisados os principais conceitos da trigonometria sobre corpos finitos e apresentadas definições e propriedades dos mapas tangente-Chebyshev sobre essas estruturas algébricas (LIMA; CAMPELLO DE SOUZA, 2019).

2.1 TRIGONOMETRIA SOBRE CORPOS FINITOS

A ideia de descrever funções trigonométrica em corpos finitos foi originalmente proposta em (CAMPELLO DE SOUZA et al., 1998a), quando da definição da transformada numérica de Hartley. Em trabalhos posteriores, a teoria foi expandida, fornecendo uma base para a criação de outras ferramentas matemáticas sobre as referidas estruturas algébricas e para o seu uso em aplicações em áreas como processamento de sinais, comunicações e criptografia (LIMA; CAMPELLO DE SOUZA, 2013; DA SILVA NETO; LIMA, 2016; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017; FIGUEIREDO; LIMA, 2019). Nesta seção, são apresentados os fundamentos da trigonometria sobre corpos finitos, com ênfase nos resultados necessários para o estudo dos mapas tangente-Chebyshev. No decorrer do texto, assume-se que o corpo finito $\mathbb{F}_q$ é usado, sendo $q = p^m$, em que m inteiro positivo e p um primo ímpar. Considera-se também que $m \geq 2$ os cálculos são computados utilizando um polinômio irredutível f de grau m em $\mathbb{F}_q$.

Definição 2.1. *(LIMA; PANARIO; CAMPELLO DE SOUZA, 2014) O conjunto dos números inteiros Gaussianos sobre $\mathbb{F}_q$ é o conjunto $\mathbb{I}_q$, com elementos na forma $a + bi$, em que $a, b \in \mathbb{F}_q$ e i^2 é um não-resíduo quadrático sobre $\mathbb{F}_q$.*

Um elemento $\zeta = a + bi \in \mathbb{I}_q$ pode ser interpretado como um número "complexo", sendo $\Re\{\zeta\} = a$ e $\Im\{\zeta\} = b$ a parte "real" e a "imaginária", respectivamente, e $\zeta^* = a - bi$ o seu conjugado. Além disso, nota-se que $\mathbb{I}_q$ é isomorfo a $\mathbb{F}_{q^2}$.

Definição 2.2. *O conjunto unimodular de $\mathbb{I}_q$ é o conjunto $\mathrm{G}_{1,q}$, de elementos $a + bi \in \mathbb{I}_q$, de modo que $\zeta \cdot \zeta^* = (a + bi) \cdot (a - bi) = a^2 - b^2 i^2 \equiv 1 \pmod{f}$ (LIMA; PANARIO; CAMPELLO DE SOUZA, 2014).*

Se o elemento $\zeta = a + bi$ é unimodular, então $\zeta^{-1} = \zeta^* = a - bi$.

Proposição 2.1. *$\langle \mathrm{G}_{1,q}, \cdot \rangle$ é um grupo cíclico de ordem $q + 1$ (LIMA; PANARIO; CAMPELLO DE SOUZA, 2014).*

Definição 2.3. *(LIMA; CAMPELLO DE SOUZA, 2019) Seja $\zeta \in \mathbb{I}_q$ um elemento de ordem multiplicativa denotada por $\mathrm{ord}(\zeta)$. O cosseno e o seno sobre corpos finitos relacionados ao ângulo de ζ^x, são dados, respectivamente, por*

$$\cos_\zeta(x) = \frac{\zeta^x + \zeta^{-x}}{2} \quad e \quad sen_\zeta(x) = \frac{\zeta^x - \zeta^{-x}}{2i},$$

para $x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$ (LIMA; PANARIO; CAMPELLO DE SOUZA, 2014).

Os cossenos e senos descritos na Definição 2.3 são periódicos com período $\mathrm{ord}(\zeta)$, simétricos de acordo com $\cos_\zeta(-x) = \cos_\zeta(x)$ e $\mathrm{sen}_\zeta(-x) = -\mathrm{sen}_\zeta(x)$, e conservam outras propriedades similares às das respectivas funções definidas sobre o campo dos reais (CAMPELLO DE SOUZA et al., 1998a; LIMA; PANARIO; CAMPELLO DE SOUZA, 2014). Como exemplo, considere a propriedade do círculo unitário, a qual é dada por

$$\cos^2_\zeta(x) - i^2\,\mathrm{sen}^2_\zeta(x) = 1, \tag{1}$$

a fórmula de Euler, que corresponde a

$$\zeta^x = \cos_\zeta(x) + i\,\mathrm{sen}_\zeta(x), \tag{2}$$

e o seno e o cosseno da soma de dois arcos, que são dados respectivamente por

$$\mathrm{sen}_\zeta(x+y) = \mathrm{sen}_\zeta(x)\cos_\zeta(y) + \mathrm{sen}_\zeta(y)\cos_\zeta(x), \tag{3}$$

e

$$\cos_\zeta(x+y) = \cos_\zeta(x)\cos_\zeta(y) + i^2\,\mathrm{sen}_\zeta(x)\,\mathrm{sen}_\zeta(y). \tag{4}$$

Vale ressaltar que se $q \equiv 3 \pmod 4$ e o elemento imaginário $i = \sqrt{-1}$, as expressões (1) e (4) se tornam similares às identidades trigonométricas clássicas.

Proposição 2.2. *(LIMA; CAMPELLO DE SOUZA, 2019) Seja $\zeta \in \mathbb{I}_q$ um elemento unimodular; o seno e o cosseno em corpo finito relacionados ao ângulo de ζ^x são calculados, respectivamente, por $\cos_\zeta(x) = \Re\{\zeta^x\}$ e $sen_\zeta(x) = \Im\{\zeta^x\}$, para $x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$ (LIMA; PANARIO; CAMPELLO DE SOUZA, 2014).*

Lema 2.1. *(LIMA; CAMPELLO DE SOUZA, 2019) Se $\zeta = a + bi \in \mathbb{I}_q$ tem ordem multiplicativa $\mathrm{ord}(\zeta) = 2(q+1)$, então $\zeta^{-1} = -\zeta^*$.*

Demonstração. Devido a Proposição 2.1, é sabido que $\zeta^2 = (a^2 + i^2b^2) + (2ab)i$ e, portanto, $\zeta^{-2} = (\zeta^2)^* = (a^2 + i^2b^2) - (2ab)i = (-a + bi)^2$. □

Proposição 2.3. *(LIMA; CAMPELLO DE SOUZA, 2019) Seja $\zeta \in \mathbb{I}_q$ um elemento de ordem multiplicativa $\mathrm{ord}(\zeta) = 2(q+1)$ e $\zeta_1 = \zeta^2$; o cosseno e o seno em corpo finito do ângulo relacionado a ζ^x são puramente "reais", isto é, pertencem a $\mathbb{F}_q$, se x for um número par, ou puramente "imaginários", isto é, tem a forma $b'i$, $b' \in \mathbb{F}_q$, se x for um número ímpar.*

Demonstração. Se x for número par, esse pode ser escrito como $x = 2y$ e, portanto, como $\zeta_1 = \zeta^2$. O cosseno e o seno em corpo finito do ângulo de ζ^x correspondem, respectivamente, ao cosseno e ao seno do ângulo de ζ_1^y, os quais, devido à Proposição 2.2, pertencem a $\mathbb{F}_q$ ($\mathrm{ord}(\zeta_1) = q+1$, isto é, ζ_1 é um gerador de G_1). Caso x seja ímpar, esse pode ser escrito como $x = 2y + 1$ e, portanto,

$$\mathrm{sen}_\zeta(x) = \mathrm{sen}_\zeta(2y+1) = \frac{\zeta^{2y+1} - \zeta^{-2y-1}}{2i} = \frac{\zeta_1^y\zeta - \zeta_1^{-y}\zeta^{-1}}{2i}.$$

Assumindo que $\zeta_1^y = a+bi$, $a, b \in \mathbb{F}_q$, que também é unimodular, tem-se que $\zeta_1^{-y} = a-bi$. Além disso, assumindo que $\zeta = c + di$, $c, d \in \mathbb{F}_q$, tem-se, a partir do Lema 2.1, que $\zeta^{-1} = -c + di$. Usando esses fatos na última equação, obtém-se

$$\text{sen}_\zeta(x) = \text{sen}_\zeta(2y+1) = \frac{(a+bi)(c+di) - (a-bi)(-c+di)}{2i} = \frac{ac + bdi^2}{i},$$

que é puramente "imaginário" . Um desenvolvimento similar é obtido para o cosseno em corpo finito. □

2.2 FUNÇÃO TANGENTE SOBRE CORPOS FINITOS

Nesta seção, são revisadas a definição e as propriedades da função tangente sobre corpos finitos (LIMA; CAMPELLO DE SOUZA, 2019). A partir deste ponto, assume-se que $\text{ord}(\zeta)$ é par.

Definição 2.4. *(LIMA; CAMPELLO DE SOUZA, 2019) Seja $\zeta \in \mathbb{I}_q$ um elemento com ordem multiplicativa $\text{ord}(\zeta)$. A tangente em corpo finito do ângulo relacionado a ζ^x é definida como*

$$\tan_\zeta(x) = \frac{sen_\zeta(x)}{\cos_\zeta(x)} = \frac{1}{i}\frac{\zeta^x - \zeta^{-x}}{\zeta^x + \zeta^{-x}}, \tag{5}$$

para $x = 0, 1, \ldots, \frac{\text{ord}(\zeta)}{2} - 1$.

Diferentemente do cosseno e do seno em corpo finito, a função tangente é periódica com período $\left(\frac{\text{ord}(\zeta)}{2}\right)$. Isso pode ser verificado considerando um número inteiro k e escrevendo

$$\tan_\zeta\left(x + k\frac{\text{ord}(\zeta)}{2}\right) = \frac{1}{i}\frac{\zeta^x\zeta^{k\frac{\text{ord}(\zeta)}{2}} - \zeta^{-x}\zeta^{-k\frac{\text{ord}(\zeta)}{2}}}{\zeta^x\zeta^{k\frac{\text{ord}(\zeta)}{2}} + \zeta^{-x}\zeta^{-k\frac{\text{ord}(\zeta)}{2}}}.$$

Como $\zeta^{k\frac{\text{ord}(\zeta)}{2}} = \zeta^{-k\frac{\text{ord}(\zeta)}{2}} = (-1)^k$, tem-se que $\tan_\zeta\left(x + k\frac{\text{ord}(\zeta)}{2}\right) = \tan_\zeta(x)$. É possível verificar que a função tangente tem simetria ímpar, isto é, $\tan_\zeta(-x) = -\tan_\zeta(x)$. O conjunto de todos os possíveis valores da função tangente calculados em relação a ζ é denotado por $\mathbb{T}_\zeta$.

Lema 2.2. *(LIMA; CAMPELLO DE SOUZA, 2019) Seja $\zeta \in \mathbb{I}_q$ um elemento com ordem multiplicativa $\text{ord}(\zeta)$. Para $0 \leq x, y \leq \frac{\text{ord}(\zeta)}{2} - 1$, tem-se*

$$\tan_\zeta(x) = \tan_\zeta(y) \quad \textit{se e somente se} \quad x = y.$$

Demonstração. Se $x = y$, tem-se claramente que $\tan_\zeta(x) = \tan_\zeta(y)$. Por outro lado, se $\tan_\zeta(x) = \tan_\zeta(y)$, tem-se que

$$\frac{\zeta^x - \zeta^{-x}}{\zeta^x + \zeta^{-x}} = \frac{\zeta^y - \zeta^{-y}}{\zeta^y + \zeta^{-y}} \Rightarrow \zeta^{x-y} = \zeta^{y-x}.$$

A última igualdade é satisfeita se e somente se $\zeta^{x-y} = \pm 1$, do qual a única solução, no intervalo $0 \leq x, y \leq \frac{\text{ord}(\zeta)}{2} - 1$, é $x - y = 0$, e portanto $x = y$. □

Proposição 2.4. *(LIMA; CAMPELLO DE SOUZA, 2019) Se $\zeta \in \mathbb{I}_q$ é um elemento com ordem multiplicativa $\mathrm{ord}(\zeta) = 2(q+1)$, tem-se que $\mathbb{T}_\zeta = \mathbb{F}_q \cup \{\infty\}$.*

Demonstração. Em função da periodicidade da função tangente em corpo finito e do Lema 2.2, a referida função produz $q+1$ resultados diferentes, dentre os quais uma quantidade q pertence a $\mathbb{F}_q$, visto que as funções cosseno e seno, para um dado x, são puramente "reais" ou puramente "imaginárias" (Proposição 2.3). Assim, todos os resultados em questão pertencem a $\mathbb{F}_q$, exceto quando $x = \frac{\mathrm{ord}(\zeta)}{4}$, que resulta em $\cos_\zeta\left(\frac{\mathrm{ord}(\zeta)}{4}\right) = 0$ e, consequentemente, em $\tan_\zeta\left(\frac{\mathrm{ord}(\zeta)}{4}\right) \to \infty$. □

Exemplo 2.1. *Como exemplo ilustrativo, a Tabela 1 fornece todos os valores para as funções cosseno, seno e tangente relativas ao elemento $\zeta = 2+3i \in \mathbb{I}_7$, com ordem $\mathrm{ord}(\zeta) = 2(q+1) = 16$, considerando $i^2 = 6$ e $x = 0, 1, \ldots, 7$. Na tabela, a coluna relacionada à função tangente é formada por todos os elementos de $\mathbb{F}_7$ juntamente com a entrada Inf, que denota "infinito" (Proposição 2.4).*

Tabela 1 – Valores para as funções seno, cosseno e tangente relacionadas ao elemento $\zeta = 2+3i \in \mathbb{I}_7$, em que $\mathrm{ord}(\zeta) = 2(q+1) = 16$, $i^2 = 6$ e $x = 0, 1, \ldots, 7$.

x	$\mathrm{sen}_\zeta(x)$	$\cos_\zeta(x)$	$\tan_\zeta(x)$
0	0	1	0
1	5i	3i	4
2	5	2	6
3	4i	2i	2
4	6	0	∞
5	4i	5i	5
6	5	5	1
7	5i	4i	3

Fonte: O Autor (2023)

Exemplo 2.2. *Neste outro exemplo, considera-se o corpo de extensão $\mathbb{F}_9$ e as operações foram realizadas usando o polinômio irredutível $f(X) = X^2 + 2X + 2$. Na Tabela 2, são mostrados os valores encontrados para as funções seno, cosseno e tangente relativas ao elemento $\zeta = \alpha + \alpha^3 i = \alpha + (2\alpha+1)i \in \mathbb{I}_9$, que tem ordem multiplicativa $\mathrm{ord}(\zeta) = 2(q+1) = 20$, considerando $i^2 = \alpha$ e $x = 0, 1, \ldots, 9$. Nesta tabela, a coluna relacionada à função tangente contém todos os elementos de $\mathbb{F}_9$ bem como o Inf (Proposição 2.4).*

2.2.1 Função tangente inversa sobre corpos finitos

Partindo de (5), é possível derivar uma expressão fechada para a função inversa da tangente sobre corpos finitos, a qual é denotada por $\arctan_\zeta(x)$, quando calculada com relação ao elemento $\zeta \in \mathbb{I}_q$. Substituindo $\tan_\zeta(x)$ e x por x e $y = \arctan_\zeta(x)$, respectivamente, em (5),

Tabela 2 – Resultados das funções seno, cosseno, e tangente computados com $\zeta = \alpha + \alpha^3 i = \alpha + (2\alpha + 1)i \in \mathbb{I}_9$, tal que $\mathrm{ord}(\zeta) = 2(q+1) = 20$, $i^2 = \alpha$, e $x = 0, 1, \ldots, 9$.

x	$\mathrm{sen}_\zeta(x)$	$\cos_\zeta(x)$	$\tan_\zeta(x)$
0	0	1	0
1	$i = \alpha^0 i$	$(2\alpha+1)i = \alpha^3 i$	$2\alpha = \alpha^5$
2	$1 = \alpha^0$	$2\alpha = \alpha^5$	$2\alpha + 1 = \alpha^3$
3	$(\alpha+1)i = \alpha^2 i$	$(\alpha+1)i = \alpha^2 i$	$1 = \alpha^0$
4	$\alpha = \alpha^1$	$2\alpha + 1 = \alpha^3$	$2\alpha + 2 = \alpha^6$
5	$2\alpha i = \alpha^5 i$	0	Inf
6	$\alpha = \alpha^1$	$\alpha + 2 = \alpha^7$	$\alpha + 1 = \alpha^2$
7	$(\alpha+1)i = \alpha^2 i$	$(2\alpha+2)i = \alpha^6 i$	$2 = \alpha^4$
8	$1 = \alpha^0$	$\alpha = \alpha^1$	$\alpha + 2 = \alpha^7$
9	$i = \alpha^0 i$	$(\alpha+2)i = \alpha^7 i$	$\alpha = \alpha^1$

Fonte: O Autor (2023)

obtém-se

$$\frac{1}{i}\frac{\zeta^y - \zeta^{-y}}{\zeta^y + \zeta^{-y}} = x \Rightarrow \frac{1}{i}\frac{\zeta^{2y} - 1}{\zeta^{2y} + 1} = x \Rightarrow \zeta^{2y} = \frac{1 + ix}{1 - ix}$$

e, consequentemente,

$$y = \arctan_\zeta(x) = \frac{1}{2}\log_\zeta\left(\frac{1+ix}{1-ix}\right). \tag{6}$$

2.3 MAPA RACIONAL TANGENTE-CHEBYSHEV SOBRE CORPOS FINITOS

Nesta seção, a função tangente em corpo finito descrita na Seção 2.2 é usada para definir um mapa cuja expressão é análoga à dos polinômios de Chebyshev do primeiro tipo. O mapa em questão é denominado tangente-Chebyshev (LIMA; CAMPELLO DE SOUZA, 2019).

Definição 2.5. *(LIMA; CAMPELLO DE SOUZA, 2019) O n-ésimo mapa tangente-Chebyshev sobre $\mathbb{F}_q$, com $n \in \mathbb{N}$, é definido como*

$$C_n(x) = \tan_\zeta\left(n \arctan_\zeta(x)\right), \tag{7}$$

em que $\zeta \in \mathbb{I}_q$ e $x \in \mathbb{T}_\zeta$.

Claramente, tem-se $C_0(x) = 0$ e $C_1(x) = x$, para todo $x \in \mathbb{F}_q$. Para outros valores de n, $C_n(x)$ pode ser obtido por meio de uma relação de recorrência, que é derivada a partir de (7) e usando $\theta = \arctan_\zeta(x)$. Mais especificamente, tem-se

$$C_{n+1}(\theta) = \frac{\mathrm{sen}_\zeta((n+1)\theta)}{\cos_\zeta((n+1)\theta)} = \frac{\mathrm{sen}_\zeta(n\theta + \theta)}{\cos_\zeta(n\theta + \theta)}.$$

Usando (3) e (4), reescreve-se a última equação como

$$C_{n+1}(\theta) = \frac{\mathrm{sen}_\zeta(n\theta)\cos_\zeta(\theta) + \cos_\zeta(n\theta)\,\mathrm{sen}_\zeta(\theta)}{\cos_\zeta(n\theta)\cos_\zeta(\theta) + i^2\,\mathrm{sen}_\zeta(n\theta)\,\mathrm{sen}_\zeta(\theta)}.$$

Dividindo o numerador e o denominador por $\cos_\zeta(\theta)\cos_\zeta(n\theta)$, observando que $\tan_\zeta(\theta) = x$ e, novamente, usando (7), obtém-se

$$C_{n+1}(x) = \frac{C_n(x) + x}{1 + i^2 x C_n(x)}. \tag{8}$$

Esta relação demonstra que os mapas tangente-Chebyshev são mapas racionais sobre $\mathbb{F}_q$; tem-se, por exemplo

$$C_2(x) = \frac{2x}{1 + i^2x^2}, \quad C_3(x) = \frac{3x + i^2x^3}{1 + i^2 3x^2},$$
$$C_4(x) = \frac{4x + i^2 4x^3}{1 + i^2 6x^2 + i^4x^4}, \quad C_5(x) = \frac{5x + i^2 10x^3 + i^4x^5}{1 + i^2 10x^2 + i^4 5x^4}.$$

Embora a Definição 2.5 mencione que $x \in \mathbb{T}_\zeta$, esta restrição pode ser negligenciada, se o interesse for simplesmente avaliar $C_n(x)$ sobre um corpo finito $\mathbb{F}_q$, para valores particulares de n e x; de certa forma, isso é equivalente a fixar ζ como um elemento de ordem $\mathrm{ord}(\zeta) = 2(q+1)$, que, devido à Proposição 2.4, garante que $\arctan_\zeta(x)$ pode ser avaliado para todo $x \in \mathbb{F}_q$. Tal condição é assumida a partir deste ponto no presente documento.

Uma forma alternativa de expressar $C_n(x)$ pode ser derivada aplicando as fórmulas do cosseno e do seno de ângulos múltiplos em corpo finito. Usando (2), as propriedades da simetria do $\cos_\zeta(\cdot)$ e do $\mathrm{sen}_\zeta(\cdot)$, e a identidade binomial, obtém-se

$$\zeta^{n\theta} = (\cos_\zeta\theta + i\,\mathrm{sen}_\zeta\theta)^n = \sum_{k=0}^{n}\binom{n}{k}(\cos_\zeta\theta)^{n-k}(i\,\mathrm{sen}_\zeta\theta)^k$$

e

$$\zeta^{-n\theta} = (\cos_\zeta\theta - i\,\mathrm{sen}_\zeta\theta)^n = \sum_{k=0}^{n}\binom{n}{k}(\cos_\zeta\theta)^{n-k}(-i\,\mathrm{sen}_\zeta\theta)^k.$$

Combinando estas duas equações, é possível obter as seguintes expressões para $\cos_\zeta(n\theta)$ e $\mathrm{sen}_\zeta(n\theta)$:

$$\begin{aligned}\cos_\zeta(nx) &= \sum_{k\text{ par}} i^k\binom{n}{k}(\cos_\zeta(x))^{n-k}(\,\mathrm{sen}_\zeta(x))^k \\ &= \sum_{k=0}^{\lfloor n/2\rfloor} i^{2k}\binom{n}{2k}(\cos_\zeta(x))^{n-2k}(\,\mathrm{sen}_\zeta(x))^{2k};\end{aligned} \tag{9}$$

$$\begin{aligned}\mathrm{sen}_\zeta(nx) &= \sum_{k\text{ ímpar}} i^{k-1}\binom{n}{k}(\cos_\zeta(x))^{n-k}(\,\mathrm{sen}_\zeta(x))^k \\ &= \sum_{k=0}^{\lfloor (n-1)/2\rfloor} i^{2k}\binom{n}{2k+1}(\cos_\zeta(x))^{n-2k-1}(\,\mathrm{sen}_\zeta(x))^{2k+1}.\end{aligned} \tag{10}$$

Como (7) pode ser reescrita como $C_n(\theta) = \mathrm{sen}_\zeta(n\theta)/\cos_\zeta(n\theta)$, $\theta = \arctan_\zeta(x)$, empregando as duas expressões acima obtidas, tem-se

$$C_n(x) = \frac{\sum_{k=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2k+1}i^{2k}x^{2k+1}}{\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{2k}i^{2k}x^{2k}}. \tag{11}$$

2.3.1 Polos e Zeros

A seguir, são determinados os polos e zeros do mapa C_n.

Proposição 2.5. *(LIMA; CAMPELLO DE SOUZA, 2019) Os zeros $r_k \in \mathbb{F}_q$ do mapa tangente-Chebyshev sobre $\mathbb{F}_q$ são dados por*

$$r_k = \tan_\zeta \left[\frac{k(q+1)}{n} \right], \tag{12}$$

em que k é qualquer número inteiro tal que $k(q+1)/n$ também é um número inteiro.

Demonstração. Para r_k ser um zero de C_n, é preciso que $\operatorname{sen}_\zeta(n \arctan_\zeta(s_k)) = 0$ ou, de modo equivalente, $n \arctan_\zeta(r_k) \equiv 0 \pmod{(q+1)}$. Noutras palavras, isso significa que $n \arctan_\zeta(r_k) = k(q+1)$, $k \in \mathbb{Z}$, de onde segue o resultado. □

Proposição 2.6. *(LIMA; CAMPELLO DE SOUZA, 2019) Os polos $s_k \in \mathbb{F}_q$ do mapa tangente-Chebyshev sobre $\mathbb{F}_q$ são dados por*

$$s_k = \tan_\zeta \left[\frac{(2k+1)(q+1)}{2n} \right], \tag{13}$$

em que k é qualquer número inteiro tal que $(2k+1)(q+1)/2n$ também é um número inteiro.

Demonstração. Para s_k ser um polo de C_n, é preciso que $\cos_\zeta(n \arctan_\zeta(s_k)) = 0$, ou de modo equivalente, $n \arctan_\zeta(s_k) \equiv \left(\frac{q+1}{2}\right) \pmod{(q+1)}$. Noutras palavras, isso significa que $n \arctan_\zeta(s_k) = (2k+1)(q+1)/2$, $k \in \mathbb{Z}$, de onde segue o resultado. □

Um fato interessante a destacar é que, se $\operatorname{mdc}(n, q+1) = 1$, o único zero de C_n sobre $\mathbb{F}_q$ é $r_0 = 0$; isso deve-se à periodicidade da função tangente em corpo finito e pelo fato de o argumento ser avaliado módulo $q+1$. Por outro lado, se n for da forma $n = q+1$ ($n = 4$ e $q = 3$, por exemplo) os q zeros de C_n são, precisamente, os q elementos de $\mathbb{F}_q$. De forma similar, é possível mostrar que, se $\operatorname{mdc}(q+1)/2, n) = 1$, não há polos sobre $\mathbb{F}_q$; se $(q+1)/2 = n$, o número de polos sobre $\mathbb{F}_q$ é $2\lfloor (q+1)/4 \rfloor$.

2.3.2 Propriedade de Semigrupo

Assim como acontece com os polinômios de Chebyshev sobre corpos finitos (YOSHIOKA, 2018a), os mapas racionais tangente-Chebyshev satisfazem à propriedade de semigrupo. Isso é demonstrado na proposição a seguir.

Proposição 2.7. *(LIMA; CAMPELLO DE SOUZA, 2019) Dados $m, n \in \mathbb{N}$, tem-se que*

$$C_m(C_n(x)) = C_n(C_m(x)) = C_{mn}(x). \tag{14}$$

Demonstração. Utilizando (7), pode-se escrever

$$\begin{aligned} C_m(C_n(x)) &= \tan(m \arctan(C_n(x))) \\ &= \tan(m \arctan(\tan(n \arctan(x)))) \\ &= \tan(mn \arctan(x)) = C_{mn}(x) = C_n(C_m(x)). \end{aligned}$$

□

A propriedade de semigrupo dos polinômios de Chebyshev é o fundamento do uso desses polinômios em criptografia de chave pública, conforme se demonstra originalmente em (KOCAREV; TASEV, 2003) (ainda considerando os polinômios T_n sobre o campo dos reais). De uma maneira geral, a propriedade de semigrupo permite que, dado $T_n(x)$, uma das partes do sistema de comunicação secretamente escolha m e calcule $T_{mn}(x) = T_m(T_n(x))$ sem precisar conhecer os parâmetros n e x. É demonstrado que, em sua forma original, isto é, utilizando polinômios de Chebyshev sobre o campo dos reais, este algoritmo é facilmente quebrado (BERGAMO et al., 2005; CHEONG; KOSHIBA, 2007); por outro lado, se polinômios de Chebyshev sobre uma estrutura algébrica finita forem usados e se os parâmetros do algoritmo forem escolhidos respeitando certas restrições (YOSHIOKA, 2016; YOSHIOKA, 2018b), um ataque similar ao proposto em (BERGAMO et al., 2005) requer calcular a função cosseno inversa na estrutura correspondente. Como isso é equivalente a calcular um logaritmo discreto (LIMA; PANARIO; CAMPELLO DE SOUZA, 2010), para números primos grandes, o algoritmo tornar-se-ia seguro. Dado que a função tangente sobre corpos finitos inversa também pode ser representada como um logaritmo (discreto), sua avaliação também se torna inviável para números primos grandes; noutros termos, dados $C_n(x)$ e x, seria difícil obter n.

2.3.3 Propriedades de Permutação

Nesta seção, são revisados resultados sobre as condições em que um mapa tangente-Chebyshev corresponde a uma permutação, isto é, uma bijeção em $\mathbb{F}_q$. Mapas de permutação são muito usados em aplicações como criptografia de chave secreta, teoria da codificação, análise combinatorial etc. Quando o assunto diz respeito a polinômios de permutação, existem muitos resultados já estabelecidos em relação aos polinômios de Chebyshev, especificamente (veja, por exemplo em (MULLEN; PANARIO, 2013) e as referências sobre este assunto). Para caracterizar os mapas tangente-Chebyshev neste contexto, são estabelecidos, inicialmente, resultados sobre a periodicidade desses mapas. Para isso, define-se

$$\eta(x) = \zeta^{\arctan_\zeta(x)}, \tag{15}$$

de maneira que $\mathrm{ord}(\eta(x)) = N_x$ e estabelece-se a proposição.

Proposição 2.8. *(LIMA; CAMPELLO DE SOUZA, 2019) Dado o elemento $x \in \mathbb{F}_q$, tem-se que*

1. *$C_{n'}(x) = C_n(x)$, se e somente se $n' \equiv n \pmod{N_x}$, para N_x ímpar, ou $n' \equiv n \pmod{N_x/2}$, para N_x par;*

2. $C_{n'}(x) = -C_n(x)$, *se e somente se* $n' \equiv -n \pmod{N_x}$, *para* N_x *ímpar, ou* $n' \equiv -n \pmod{N_x/2}$, *para* N_x *par.*

Demonstração. Se $n' \equiv n \pmod{N_x}$, para N_x ímpar, então $n' = n + kN_x$, $k \in \mathbb{Z}$. Além do mais, para $[\eta(x)]^{N_x} = 1$, e usando (5) e (7), tem-se que

$$\begin{aligned} C_{n'}(x) &= \frac{1}{i}\frac{\zeta^{(n+kN_x)\arctan_\zeta(x)} - \zeta^{-(n+kN_x)\arctan_\zeta(x)}}{\zeta^{(n+kN_x)\arctan_\zeta(x)} + \zeta^{-(n+kN_x)\arctan_\zeta(x)}} \\ &= \frac{1}{i}\frac{[\eta(x)]^n - [\eta(x)]^{-n}}{[\eta(x)]^n + [\eta(x)]^{-n}} \\ &= \frac{1}{i}\frac{\zeta^{n\arctan_\zeta(x)} - \zeta^{-n\arctan_\zeta(x)}}{\zeta^{n\arctan_\zeta(x)} + \zeta^{-n\arctan_\zeta(x)}} = C_n(x). \end{aligned}$$

Se $n' \equiv n \pmod{N_x/2}$, para N_x par, então $n' = n + kN_x/2$, $k \in \mathbb{Z}$. Observando que $[\eta(x)]^{\frac{N_x}{2}} = -1$ e, novamente, usando $[\eta(x)]^{N_x} = 1$, (5) e (7), tem-se que $C_{n'}(x) = C_n(x)$. A prova da Proposição 2.8, parte 1, é concluída demonstrando a veracidade, no sentido inverso, do que se acabou de provar; isso é feito considerando a periodicidade da função tangente em corpo finito e o Lema 2.2. A prova da parte 2 da proposição pode ser desenvolvida de forma similar. □

A seguir, é caracterizada a periodicidade de um elemento $x \in \mathbb{F}_q$ em relação ao mapa C_n.

Definição 2.6. *(LIMA; CAMPELLO DE SOUZA, 2019) Um elemento* $x \in \mathbb{F}_q$ *é periódico em relação ao mapa* C_n*, se existe um número inteiro mínimo* $\mathrm{per}_{C_n,\mathbb{F}_q}(x) = \pi \geq 1$*, tal que* $C_{n^\pi}(x) = C_1(x) = x$.

Proposição 2.9. *(LIMA; CAMPELLO DE SOUZA, 2019) Um elemento* $x \in \mathbb{F}_q$ *é periódico em relação ao mapa* C_n*, se e somente se* $\mathrm{mdc}(n, N_x/2) = 1$*, para* N_x *par, ou* $\mathrm{mdc}(n, N_x) = 1$*, para* N_x *ímpar.*

Demonstração. Para N_x par, a parte 1 da Proposição 2.8 afirma que $C_{n'}(x) = C_n(x)$, se e somente se $n' \equiv n \pmod{N_x/2}$. De acordo com a Definição 2.6, x é periódico se e somente se existe um número π, de modo que $C_{n^\pi}(x) = C_1(x)$; se substituir, na última congruência, n' e n por n^π e 1, respectivamente, a condição de periodicidade em questão é equivalente a

$$n^\pi \equiv 1 \pmod{N_x/2},$$

que é satisfeita se $\mathrm{mdc}(n, N_x/2) = 1$. Uma demonstração análoga pode ser desenvolvida para N_x ímpar (LIMA; CAMPELLO DE SOUZA, 2019).

□

A seguir, é dada uma condição necessária e suficiente para que o mapa tangente-Chebyshev seja uma permutação sobre $\mathbb{F}_q$.

Proposição 2.10. *(LIMA; CAMPELLO DE SOUZA, 2019) O mapa tangente-Chebyshev permuta os elementos de $\mathbb{F}_q$, se e somente se $(n, q+1) = 1$.*

Demonstração. O mapa C_n é uma permutação, se e somente se todo elemento $x \in \mathbb{F}_q$ é periódico. A partir de (15), é possível perceber que os possíveis valores de N_x são os divisores de $\mathrm{ord}(\zeta) = 2(q+1)$, e que este último é, naturalmente, o maior valor para N_x. Como $2(q+1)$ é par, usando a Proposição 2.9, a condição de periodicidade pode ser generalizada como $(n, 2(q+1)/2) = (n, q+1) = 1$. □

Exemplo 2.3. *Usando a Proposição 2.10, sabe-se que C_3 é uma involução sobre $\mathbb{F}_7$. Usando uma notação cíclica, é possível expressar tal permutação como*

$$(0)(1\ \ 6)(2\ \ 4)(3\ \ 5).$$

C_3 também é uma permutação sobre $\mathbb{F}_9$, sendo expressa por

$$(0)(1\ \ \alpha\ \ \alpha^4\ \ \alpha^5)(\alpha^2\ \ \alpha^7\ \ \alpha^6\ \ \alpha^3).$$

Um caso particular da permutação é a involução, isto é, uma permutação cuja inversa (segundo a composição de permutações) é a própria permutação. Involuções são usadas frequentemente em projetos de cifras de blocos, por exemplo, porque as etapas de permutação de símbolos (na cifragem) e de reversão dessa permutação (na decifragem) teriam, na verdade, a mesma arquitetura, o que é interessante do ponto de vista de implementação (CHARPIN; MESNAGER; SARKAR, 2016). Na seguinte proposição, é dada uma condição necessária e suficiente para que C_n seja uma involução.

Proposição 2.11. *(LIMA; CAMPELLO DE SOUZA, 2019) O mapa tangente-Chebyshev é uma involução sobre $\mathbb{F}_q$, se e somente se $n^2 \equiv 1 \pmod{(q+1)}$.*

Demonstração. O mapa C_n é uma involução, se todo o elemento $x \in \mathbb{F}_q$ tiver período 1 ou 2, isto é, $n^2 \equiv 1 \pmod{N_x/2}$, para N_x par, e $n^2 \equiv 1 \pmod{N_x}$, para N_x ímpar. Usando argumento semelhante ao da prova da Proposição 2.10, essas condições podem ser generalizadas em $n^2 \equiv 1 \pmod{(q+1)}$. □

Como mostrado no Exemplo 2.3, o mapa C_3 sobre $\mathbb{F}_7$ é uma involução. Outra involução é dada no exemplo a seguir.

Exemplo 2.4. *Usando a Proposição 2.11, sabe-se que C_5 é uma involução sobre $\mathbb{F}_{23}$. A sua expressão em ciclos é dada por*

$$(0)(1)(2\ 3)(4\ 17)(5\ 14)(6\ 19)(7\ 16)(8\ 12)(9\ 18)(10\ 13)$$
$$(11\ 15)(20\ 21)(22).$$

3 NOVAS PROPRIEDADES E REPRESENTAÇÃO POR GRAFOS FUNCIONAIS DOS MAPAS TANGENTE-CHEBYSHEV SOBRE CORPOS FINITOS

Neste capítulo são apresentadas as primeiras contribuições originais desta tese. Elas consistem nas novas propriedades dos mapas tangente-Chebyshev. Mais especificamente, são estudados os pontos fixos desses mapas e sua relação com as funções de Rédei e com a transformação de Möbius. Além disso, são providas representações dos mapas tangente-Chebyshev por meio de grafos funcionais.

3.1 PONTOS FIXOS

Pontos fixos podem ser descritos como um valor que não altera sob uma determinada transformação, mais especificamente quando a transformação é uma função, é um elemento que é mapeado em si pela função. O teorema enunciado a seguir, que é bastante conhecido (BURTON, 2010) , é usado na demonstração do resultado referente aos pontos fixos dos mapas tangente-Chebyshev, que é dado no Teorema 3.2.

Teorema 3.1. *Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$.*

1. *A congruência linear $ax \equiv b \pmod{n}$ possui solução se e somente se $d|b$, em que $d = \mathrm{mdc}(a, n)$.*
2. *Se $d|b$, então ela possui d soluções mutuamente incongruentes módulo n. Se $x_0 \in \mathbb{Z}$ é uma solução particular, então tais d soluções incongruentes são obtidas por*

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2\frac{n}{d}, \quad \ldots, \quad x_0 + (d-1)\frac{n}{d} \tag{16}$$

Teorema 3.2. *Seja $d = mdc(n-1, q+1)$. O mapa tangente-Chebyshev $C_n(x)$ sobre $\mathbb{F}_q$ possui apenas d pontos fixos x_k, os quais são dados por*

$$x_k = \tan_\zeta\left(k\frac{q+1}{d}\right), \tag{17}$$

em que $k = 0, 1, \ldots, d-1$ e, se d for par, $k \neq d/2$.

Demonstração. Seja $\zeta \in \mathbb{I}_p$ um elemento com ordem multiplicativa $\zeta = 2(q+1)$. Um ponto fixo x_k de $C_n(x)$ satisfaz

$$C_n(x_k) \equiv x_k \pmod{q+1} \Rightarrow \tan_\zeta(n \arctan_\zeta(x_k)) \equiv x_k \pmod{q+1}$$
$$n \arctan_\zeta(x_k) \equiv \arctan_\zeta(x_k) \pmod{q+1} \Rightarrow (n-1)\arctan_\zeta(x_k) \equiv 0 \pmod{q+1}.$$

Seja $y_k = \arctan_\zeta(x_k)$ e $d = \mathrm{mdc}(n-1, q+1)$. Do Teorema 3.1, como $d|0$ e $y_0 = \arctan_\zeta(0) = 0$ é uma solução particular da última congruência, todas as outras soluções da mesma congruência são dadas por

$$y_k = \arctan_\zeta(x_k) = k\frac{q+1}{d}, \quad k = 0, 1, \ldots, d-1,$$

o que fornece os d valores

$$x_k = \tan_\zeta\left(k\frac{q+1}{d}\right), \quad k = 0, 1, \ldots, d-1.$$

Como $\tan_\zeta\left(\frac{p+1}{2}\right) = \infty$, se d for par, exclui-se $k = d/2$ da faixa de valores de k na última expressão, restando, assim, $d-1$ valores de x_k. A distinção entre todos os valores x_k é garantida pelo Lema 2 em (LIMA; CAMPELLO DE SOUZA, 2019), os quais correspondem aos pontos fixos de $C_n(x)$. □

3.2 RELAÇÃO COM AS FUNÇÕES DE RÉDEI

As funções de Rèdei têm sido investigadas em diversos artigos recentes (QURESHI; PANARIO, 2015; BELLINI; MURRU, 2016; SHIHUI et al., 2019; NADIR, 2020) . Essas correspondem a funções racionais definidas como apresentado a seguir.

Definição 3.1 (Funções de Rèdei). *Seja $\mathbb{F}_q$ um corpo finito com característica ímpar e $a \in \mathbb{F}_q^*$ uma constante. A n-ésima, $n \in \mathbb{N}$, função de Rèdei é dada por*

$$R_n(x, a) = \sqrt{a}\frac{(x+\sqrt{a})^n + (x-\sqrt{a})^n}{(x+\sqrt{a})^n - (x-\sqrt{a})^n}. \tag{18}$$

Proposição 3.1. *Os mapas tangente-Chebyshev relacionam-se com as funções de Rédei conforme*

$$C_n(x) = R_n(x, a)|_{a=i^{-1}}.$$

Demonstração. A partir de sua definição e fazendo $\theta = \arctan_\zeta(x)$, o mapa tangente-Chebyshev $C_n(x)$ pode ser expresso como

$$C_n(x) = \tan_\zeta(n \arctan_\zeta(x)) = \frac{\mathrm{sen}_\zeta(\theta)}{\cos_\zeta(\theta)} = \frac{1}{i}\frac{\zeta^{n\theta} - \zeta^{-n\theta}}{\zeta^{n\theta} + \zeta^{-n\theta}}. \tag{19}$$

Empregando a forma logarítmica da função tangente inversa sobre corpos finitos, dada em (6), mostra-se que

$$\zeta^{n\theta} = \left(\frac{1+ix}{1-ix}\right)^{\frac{n}{2}}.$$

Assim, fazendo $B = \frac{i^{-1}+x}{i^{-1}-x}$, (19) pode ser reescrita como

$$C_n(x) = \frac{1}{i}\frac{B^{\frac{n}{2}} - B^{-\frac{n}{2}}}{B^{\frac{n}{2}} + B^{-\frac{n}{2}}} = \frac{1}{i}\frac{B^n - 1}{B^n + 1}. \tag{20}$$

Observando que

$$B^n \pm 1 = \frac{(i^{-1}+x)^n \pm (i^{-1}-x)^n}{(i^{-1}-x)^n},$$

(20) pode ser reescrita como

$$C_n(x) = \frac{1}{i}\frac{(i^{-1}+x)^n - (-1)^n(i^{-1}-x)^n}{(i^{-1}+x)^n + (-1)^n(i^{-1}-x)^n},$$

de onde se obtém, após algumas manipulações algébricas, se n for par

$$C_n(x) = \frac{1}{i}\frac{(x+i^{-1})^n - (x-i^{-1})^n}{(x+i^{-1})^n + (x-i^{-1})^n} \tag{21}$$

e se n for ímpar,

$$C_n(x) = \frac{1}{i}\frac{(x+i^{-1})^n + (x-i^{-1})^n}{(x+i^{-1})^n - (x-i^{-1})^n}. \tag{22}$$

O resultado segue ao se comparar a última expressão com (18). □

3.3 RELAÇÃO COM A TRANSFORMAÇÃO DE MÖBIUS

A seguir, define-se a transformação de Möbius, a qual tem sido investigada e empregada em cenários práticos em diversos trabalhos recentemente publicados (SUNGHAN; BYUNG-CHUL; HWANYUP, 2015; IOANNIS; GEORGIOS; FEDERICO, 2019; JELÍNEK et al., 2020; BARBIER; CHEBALLAH; BARS, 2020; SAKZAD et al., 2010).

Definição 3.2. *A transformação de Möbius é definida por*

$$T(x) = \begin{cases} \frac{ax+b}{cx+d}, & x \neq \frac{-d}{c}, \\ \frac{a}{c}, & x = \frac{-d}{c}. \end{cases}, \tag{23}$$

em que a, b, c *e* $d \in \mathbb{F}_q$.

A seguir, desenvolve-se a relação entre os mapas tangente-Chebyshev e a transformação de Möbius.

Proposição 3.2. *Os mapas tangente-Chebyshev relacionam-se com a transformação de Möbius conforme*

$$T(x) = C_n(y)\big|_{y=\frac{x^{1/n}-1}{x^{1/n}+1}}. \tag{24}$$

Demonstração. Usando a Definição 3.2, observa-se que $T(x)$ pode ser reescrita como

$$T(x) = \frac{x^{1/2}(ax^{1/2} + bx^{-1/2})}{x^{1/2}(cx^{1/2} + dx^{-1/2})}.$$

Substituindo os parâmetros $a = c = d = 1$ e $b = -1$, obtém-se

$$T(x) = \frac{x^{1/2}(x^{1/2} - x^{-1/2})}{x^{1/2}(x^{1/2} + x^{-1/2})} = \frac{x^{1/2} - x^{-1/2}}{x^{1/2} + x^{-1/2}}. \tag{25}$$

Por outro lado, utilizando a escrita logarítmica da função tangente sobre corpos finitos inversa, isto é, $\arctan_\zeta(y) = \frac{1}{2}\log_\zeta\left(\frac{1+iy}{1-iy}\right)$, bem como a expressão da própria função tangente, pode-se expressar o mapa tangente-Chebyshev $C_n(y)$ como

$$C_n(y) = \frac{1}{i}\frac{\zeta^{\frac{n}{2}\log_\zeta\left(\frac{1+iy}{1-iy}\right)} - \zeta^{\frac{-n}{2}\log_\zeta\left(\frac{1+iy}{1-iy}\right)}}{\zeta^{\frac{n}{2}\log_\zeta\left(\frac{1+iy}{1-iy}\right)} + \zeta^{\frac{-n}{2}\log_\zeta\left(\frac{1+iy}{1-iy}\right)}}. \tag{26}$$

Comparando (25) e (26), é possível perceber que $T(x) = C_n(y)$ se

$$x = \zeta^{\log_\zeta\left(\frac{1+iy}{1-iy}\right)^n} = \left(\frac{1+iy}{1-iy}\right)^n$$

ou, equivalentemente,

$$y = \frac{x^{1/n} - 1}{x^{1/n} + 1}. \tag{27}$$

□

3.4 GRAFOS FUNCIONAIS DOS MAPAS TANGENTE-CHEBYSHEV

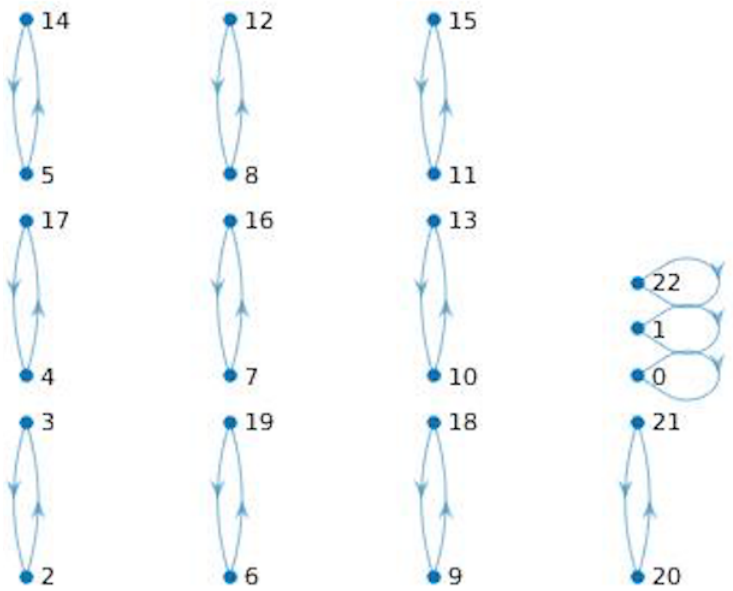
O grafo funcional de um mapa f sobre o corpo finito $\mathbb{F}_q$ é um grafo direcionado $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, em que $\mathcal{V} = \mathbb{F}_q$ é o conjunto de vértices e $\mathcal{E} = \{(x, f(x)), x \in \mathbb{F}_q\}$ é o conjunto de arestas (PANARIO; REIS, 2019) . Se o mapa for racional, como é o caso dos mapas tangente-Chebyshev, o conjunto de vértices pode incluir também um vértice rotulado com ∞. O estudo de grafos funcionais sobre corpos finitos, os quais podem ser construídos a partir de iterações desses mapas, têm despertado o interesse de vários pesquisadores em anos recentes (CAPAVERDE; MASUDA; RODRIGUES, 2020; CHENGQING et al., 2022; BORS; PANARIO; WANG, 2023). Isso se deve à importância que a caracterização desses grafos possui em aplicações relacionadas à criptografia (POLLARD, 1978), à geração de bits aleatórios (LENORE; MANUEL; MICHAEL, 1986), à fatoração de inteiros (POLLARD, 1975), entre outras (EDOUARD, 1878; LEHMER, 1930; TESKE; HUGH, 2000).

No contexto descrito, a caracterização de um grafo funcional envolve a contagem do seu número de ciclos, a determinação do comprimento de cada ciclo, o cálculo do pré-período de um elemento de $\mathbb{F}_q$ (número mínimo de arestas entre o vértice correspondente ao elemento, que não pertencer a um ciclo, e um vértice que pertença a um ciclo) etc. Características como as mencionadas têm relação direta, por exemplo, com a possibilidade de um mapa corresponder a uma permutação ou involução, ou mesmo possuir muitos pontos fixos.

Na Figura 1, é apresentado o grafo funcional do mapa C_5 sobre $\mathbb{F}_{23}$, que corresponde a uma involução. Observe que só há ciclos de comprimento 1 (indicando os pontos fixos) ou 2.

Na Figura 2, é apresentado o grafo funcional do mapa C_5 sobre $\mathbb{F}_{83}$, o qual corresponde a uma permutação, mas não a uma involução. Na Figura 3, é apresentado o grafo funcional do mapa C_5 sobre $\mathbb{F}_{157}$, o qual também corresponde a uma permutação, mas não a uma involução; neste caso, os rótulos dos vértices são omitidos. Nas figuras 1 e 2, pode-se contabilizar o número de ciclos e o de pontos fixos.

Figura 1 – Grafo funcional do mapa C_5 sobre $\mathbb{F}_{23}$, contendo 10 e 3 ciclos de comprimento 2 e 1 respectivamente. O mapa em questão é denominado como uma involução.



Fonte: O Autor (2023).

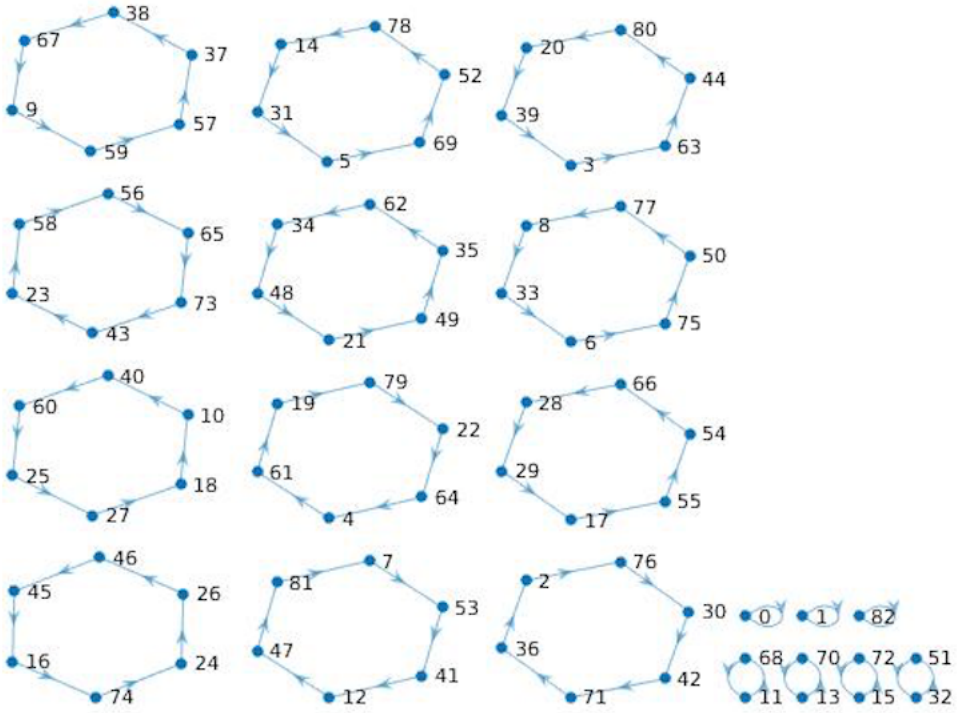
Nas Figuras 4 e 5, são apresentados os grafos funcionais dos mapas C_{12} sobre $\mathbb{F}_{31}$ e $\mathbb{F}_{83}$, respectivamente. Em ambos os casos, verifica-se que os mapas não correspondem a permutações. A partir do grafo do primeiro mapa, podem ser distintos três grupos de elementos: o 0, que é periódico (isto é, pertence a um ciclo), o grupo $\{1, 7, 9, 22, 24, 30\}$, cujos elementos possuem pré-período igual a 1 e um grupo com os 24 elementos restantes, os quais possuem pré-período igual a 2. Uma caracterização semelhante pode ser feita a partir do grafo do segundo mapa.

O resultado a seguir decorre diretamente da Proposição 2.9 e fornece o período de um elemento periódico $x \in \mathbb{F}_q$ com respeito a C_n.

Proposição 3.3. *Um elemento $x \in \mathbb{F}_q$ periódico com respeito a C_n possui período π dado pela ordem multiplicativa de n módulo $N_x/2$, se N_x for par, ou módulo N_x, se N_x for ímpar.*

Observe que a periodicidade (ou não) de um elemento $x \in \mathbb{F}_q$ com respeito a C_n depende, basicamente, do parâmetro N_x. Assim, é apresentada a proposição a seguir, por meio da qual todos os possíveis valores de N_x e o número de elementos cujos valores correspondentes de N_x coincidem são obtidos.

Figura 2 – Grafo funcional do mapa C_5 sobre $\mathbb{F}_{83}$, contendo 12, 4 e 3 ciclos de comprimento 6, 4 e 3 respectivamente. O mapa em questão é denominado como uma Permutação.



Fonte: O Autor (2023).

Proposição 3.4. *Assuma que* $\zeta \in \mathbb{I}_q$ *é tal que* $\mathrm{ord}(\zeta) = 2(q+1)$.

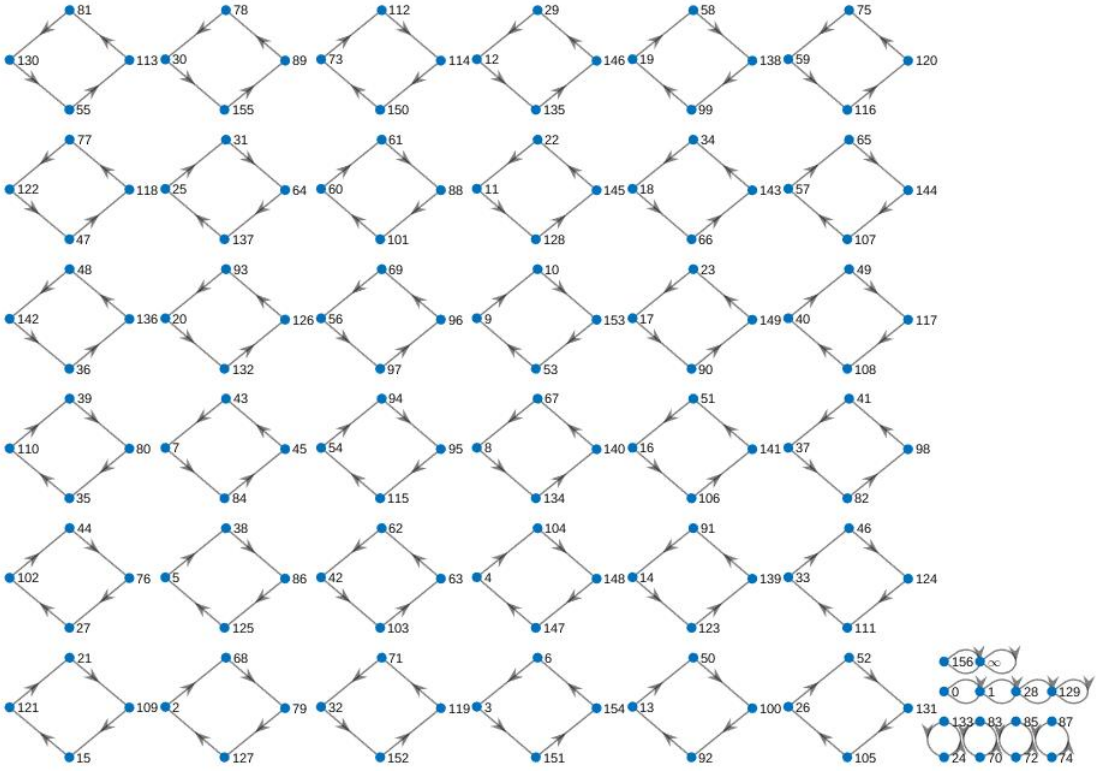
1. *Todos os possíveis valores de* N_x, $x \in \mathbb{T}_\zeta$, *são dados por* $N_x(y) = \frac{2(q+1)}{\mathrm{mdc}(2(q+1),y)}$, $y = 1, \ldots, q+1$; *isto é, os possíveis valores de* N_x *são dados por todos os divisores de* $2(q+1)$, *exceto* 1.

2. *Há* $\frac{\varphi(N_x)}{2}$ *elementos distintos* x, $x \neq 0$ *e* $x \neq \infty$, *cujos valores correspondentes de* N_x *coincidem* ($\varphi(\cdot)$ *denota a função totiente de Euler);* $N_x = 2$ *e* $N_x = 4$ *se e somente se* $x = 0$ *e* $x = \infty$, *respectivamente.*

Demonstração. O item 1 decorre diretamente da Proposição 2.4 e da definição de N_x na Proposição 2.9. Observe que a possibilidade $y = 0$, que não aparece na faixa de valores ao longo da qual y varia, é equivalente a $y = q + 1$, que é obtida para o ponto fixo $x = 0$, o único valor que fornece $N_x = 2$. Além disso, $y = \frac{q+1}{2}$ é obtido para o ponto fixo $x = \infty$, o único valor que fornece $N_x = 4$.

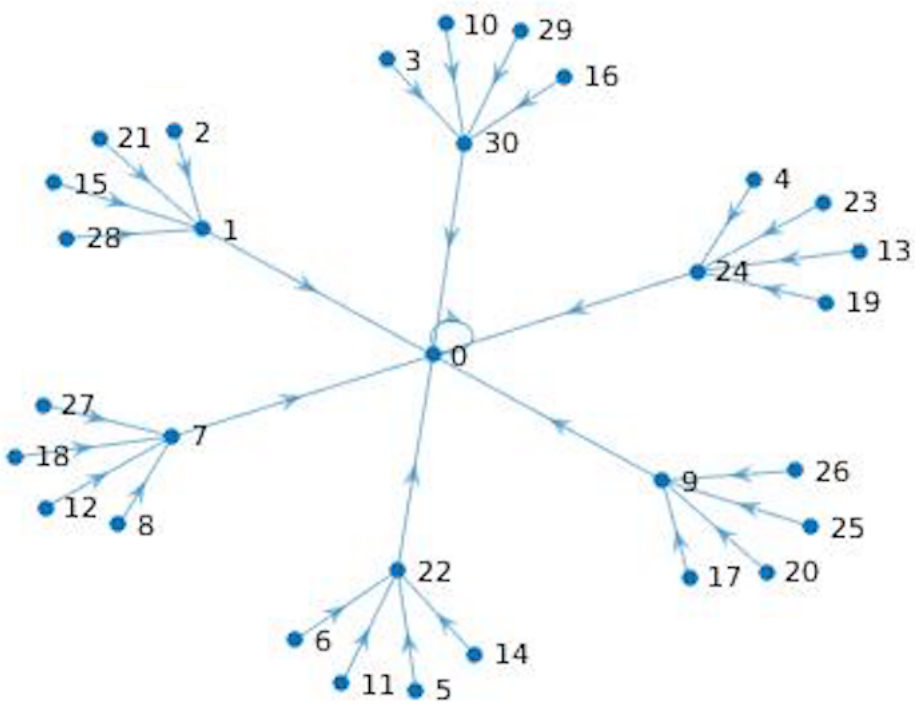
O item 2 decorre de uma das propriedades de $\varphi(\cdot)$. Mais especificamente, se escrevermos na forma irredutível todas as frações com denominador m de $\frac{1}{m}$ a $\frac{m}{m}$, teremos como denominadores todos os divisores de m e o número de frações com denominador d será dado por $\varphi(d)$. A divisão por 2 em $\frac{\varphi(N_x)}{2}$ se deve ao fato de estarmos contando apenas metade das referidas frações com determinado denominador d, à medida em que se faz $y = 1, \ldots, q + 1$, mas se

Figura 3 – Grafo funcional do mapa C_5 sobre $\mathbb{F}_{157}$, contendo 36, 4 e 6 ciclos de comprimento 4, 2 e 1 respectivamente. O mapa em questão é denominado como uma Permutação.



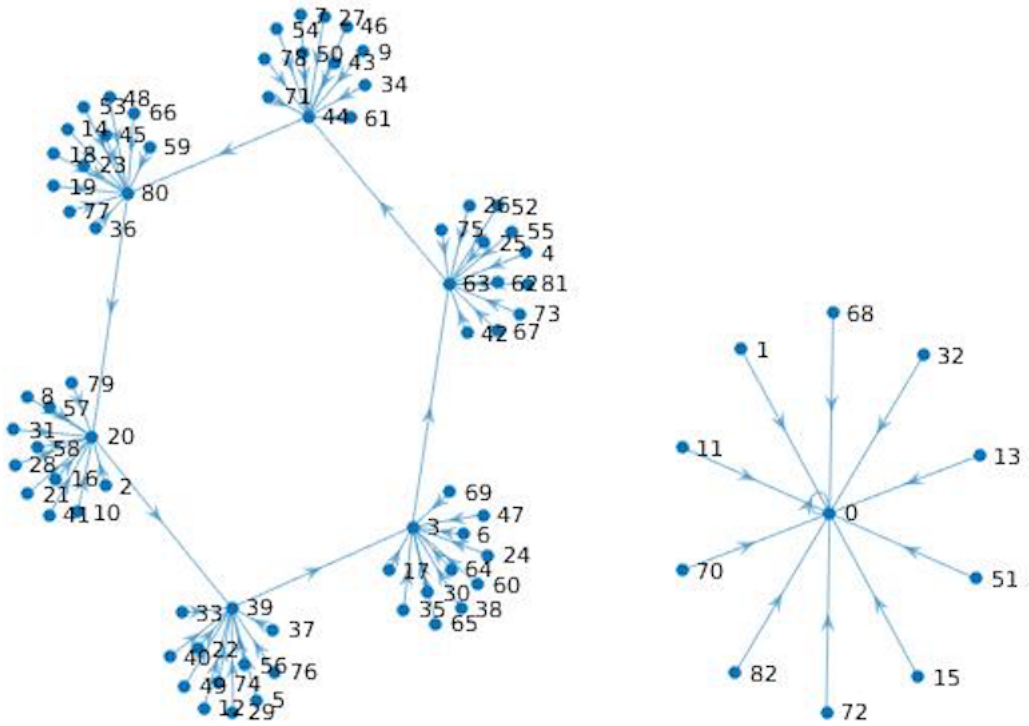
Fonte: O Autor (2023)

Figura 4 – Grafo funcional do mapa C_{12} sobre $\mathbb{F}_{31}$, contendo 1 de comprimento 1 e o mapa não é uma permutação.



Fonte: O Autor (2023)

Figura 5 – Grafo funcional do mapa C_{12} sobre $\mathbb{F}_{83}$, contendo 1 e 1 ciclo de comprimento 6 e 1 respectivamente. O mapa não é considerado uma permutação.



Fonte: O Autor (2023)

tem $m = \mathrm{ord}(\zeta) = 2(q+1)$; $N_0 = 2$ e $N_\infty = 4$ são considerados à parte em função do que se observou na demonstração da primeira parte da proposição. □

No resultado a seguir, que decorre diretamente das proposições 3.3 e 3.4, são indicados quantos ciclos com um certo comprimento o grafo funcional de C_n possui.

Proposição 3.5. *Seja* $\mathbb{N}_n = \{N_x, x \in \mathbb{F}_q^*, x \text{ é periódico com respeito a } C_n\}$ *o conjunto de valores de* N_x *obtidos conforme as Proposições 3.3 e 3.4. Obtenha, para cada elemento de* $\mathbb{N}_n$*, a ordem multiplicativa* π_{N_x} *de* n *módulo* $N_x/2$*, se* N_x *for par, ou módulo* N_x*, se* N_x *for ímpar. Suponha que, para exatos* k *elementos* $N_{x_1}, N_{x_2}, \ldots, N_{x_k}$ *de* $\mathbb{N}_n$*, tenha-se* $\pi = \pi_{N_{x_1}} = \pi_{N_{x_2}} = \cdots = \pi_{N_{x_k}}$*. Então, o grafo de* C_n *possui*

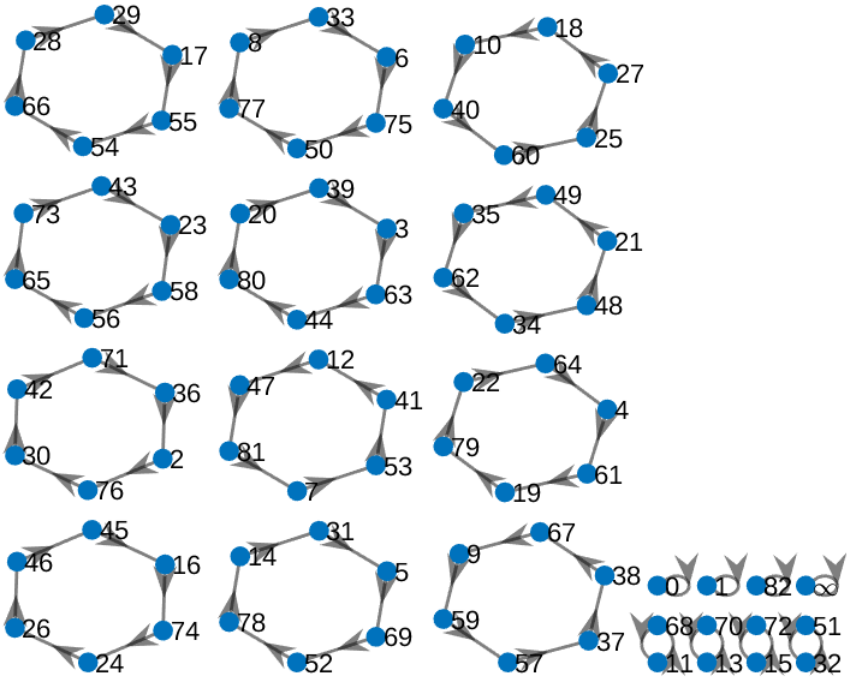
$$\sum_{r=1}^{k} \frac{\varphi(N_{x_r})}{2\pi}$$

ciclos com comprimento igual a π*, além de dois pontos fixos em* $x = 0$ *e* $x = \infty$*.*

Exemplo 3.1. *Neste exemplo, ilustra-se o uso dos resultados derivados nesta seção para obtenção da estrutura em ciclos do grafo funcional de* C_5 *sobre* $\mathbb{F}_{83}$*. Os possíveis valores de* N_x *são* $2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 84, 168$ *(Proposição 3.4, primeira parte); os períodos correspondentes são* $1, 2, 1, 2, 6, 1, 2, 6, 6, 2, 6, 6, 6, 6, 6$ *(Proposição 3.3); as quantidades de elementos com esses períodos são, respectivamente,* $1, 1, 1, 1, 3, 2, 2, 3, 6, 4, 6, 6, 12, 12, 24$

(Proposição 3.4, segunda parte). Usando os valores obtidos e a Proposição 3.5, conclui-se que o grafo do mapa em questão possui $12, 4$ *e* 4 *ciclos com comprimentos* $6, 2$ *e* 1*, respectivamente. Tal estrutura é apresentada na Figura 6, em que são incluídos, também, os valores de* x *associados a cada vértice.*

Figura 6 – Grafo funcional do mapa C_5 sobre $\mathbb{F}_{83}$, contendo 12, 4 e 3 ciclos de comprimento 6, 2 e 1. O mapa é considerado uma permutação.



Fonte: O Autor (2023)

Quando C_n não é uma permutação sobre $\mathbb{F}_q$, há elementos $x \in \mathbb{F}_q$ que não são periódicos. Isso sugere considerar a definição a seguir (GASSERT, 2014).

Definição 3.3. *Um elemento* $x \in \mathbb{F}_q$ *é pré-periódico com respeito a* C_n*, o que se escreve como* $\mathrm{pper}_{C_n,\mathbb{F}_q}(x) = \rho$*, se houver números inteiros mínimos* $\rho \geq 0$ *e* $\pi \geq 1$ *tais que* $C_{n^{\rho+\pi}}(x) = C_{n^\rho}(x)$*. Além disso, se* $\rho > 0$*, então* x *é estritamente pré-periódico.*

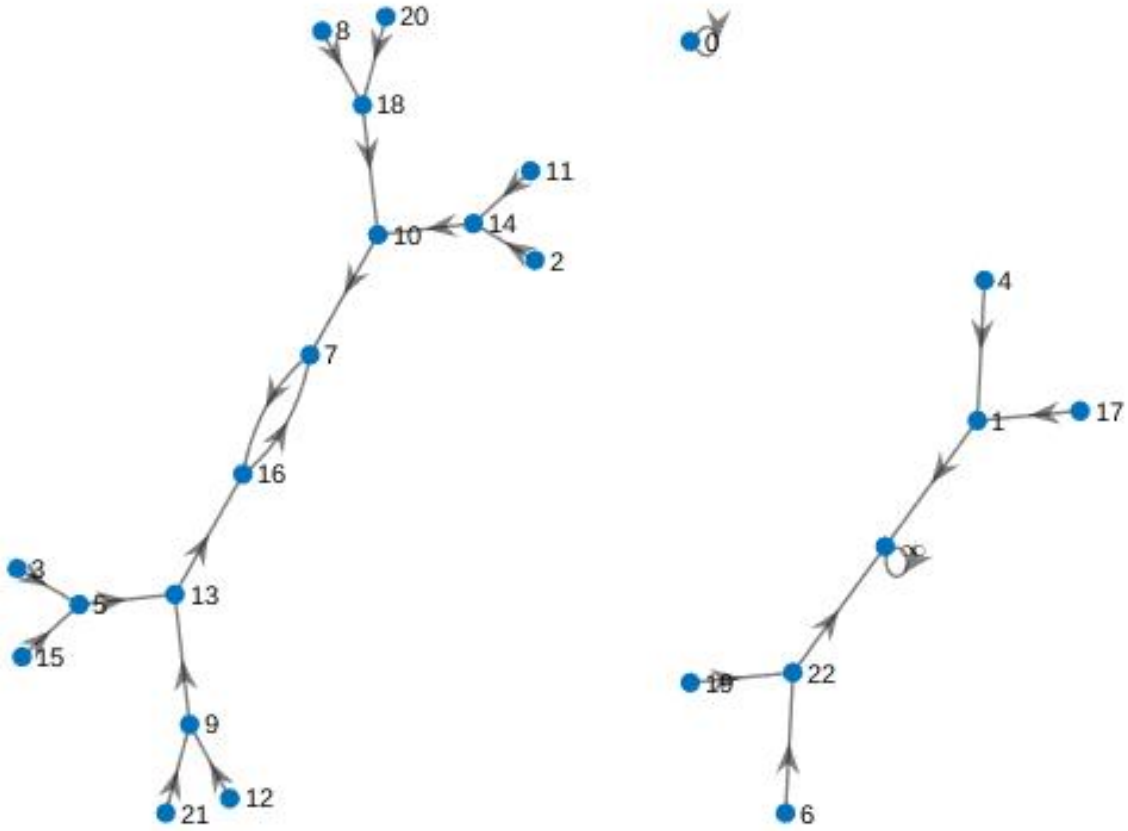
Observe que, se $\rho = 0$, então x é periódico com relação a C_n (vide Definição 2.6). A proposição a seguir caracteriza os elementos pré-periódicos com respeito a um mapa C_n.

Proposição 3.6. *Um elemento* $x \in \mathbb{F}_q^*$*, com* $N_x = \frac{2(q+1)}{mdc(2(q+1),y)}$ *para algum* $y = 1, \ldots, q$*, é estritamente pré-periódico com relação a* C_n *se e somente se* $\mathrm{mdc}(n, N_x/2) \neq 1$*, se* N_x *for par, ou* $\mathrm{mdc}(n, N_x) \neq 1$*, se* N_x *for ímpar. Além disso, se* x *for estritamente pré-periódico, seu pré-período* ρ *é igual ao menor número inteiro positivo* ν *tal que* $N_{x'} = \frac{2(q+1)}{\mathrm{mdc}(2(q+1),n^\nu y)}$ *se encontra associado a algum* x' *periódico e seu período é dado conforme a Proposição 3.3, substituindo* N_x *por* $N_{x'}$*.*

Demonstração. A primeira parte da proposição decorre diretamente da Proposição 2.9. Para determinar o pré-período, o que se busca é o primeiro elemento na sequência $x' = C_{n^\nu}(x)$, $\nu = 1, 2, \ldots$ que seja periódico ou, simplesmente, o valor de $N_{x'}$ correspondente a esse elemento. Das definições de $C_n(x)$, $\eta(x)$ e N_x (vide Proposição 2.9) e da Proposição 3.4, conclui-se que $\eta(C_{n^\nu}(x)) = \eta(x') = \zeta^{n^\nu \arctan_\zeta(x)}$ e, portanto, $N_{C_{n^\nu}(x)} = N_{x'} = \frac{2(q+1)}{\mathrm{mdc}(2(q+1), n^\nu \arctan_\zeta(x))}$, de onde segue o resultado da segunda parte da proposição. □

Exemplo 3.2. *Neste exemplo, ilustra-se o uso dos resultados derivados nesta seção para obtenção da estrutura em ciclos do grafo funcional de C_2 sobre $\mathbb{F}_{23}$. Os possíveis valores de N_x, com x periódico, são $2, 3, 4, 6$ (Proposição 3.4, primeira parte) e os períodos correspondentes são $1, 2, 1, 2$ (Proposição 3.3); as quantidades de elementos com esses períodos são, respectivamente, $1, 1, 1, 1$ (Proposição 3.4, segunda parte). Os possíveis valores de N_x, com x estritamente pré-periódico, são $8, 12, 16, 24, 48$, os pré-períodos correspondentes são $1, 1, 2, 2, 3$ e os períodos correspondentes são $1, 2, 1, 2, 2$ (Proposição 3.6); as quantidades de elementos com esses pré-períodos e períodos são, respectivamente, $2, 2, 4, 4, 8$. O grafo funcional do mapa em questão é apresentado na Figura 7, em que estão incluídos, também, os valores de x associados a cada vértice.*

Figura 7 – Grafo funcional de C_2 sobre $\mathbb{F}_{23}$ contendo 2 e 1 ciclos de comprimento 2 e 1. O mapa não é considerado uma permutação.



Fonte: O Autor (2023)

4 MAPAS TANGENTE-CHEBYSHEV DO TERCEIRO TIPO SOBRE CORPOS FINITOS

Neste capítulo é introduzida uma nova definição relacionada aos mapas tangente-Chebyshev sobre corpos finitos. Mais especificamente, é proposto um novo tipo desses mapas, cuja definição possui certa analogia com a definição dos polinômios de Chebyshev do terceiro tipo sobre corpos finitos (LIMA; PANARIO; CAMPELLO DE SOUZA, 2014). Assim, para evitar ambiguidades e entendimento errôneo por parte do leitor, é importante esclarecer que, a partir deste ponto do texto, o mapa considerado nos capítulos anteriores deste trabalho será identificado como mapa tangente-Chebyshev simplesmente ou mapa tangente-Chebyshev do primeiro tipo; o novo mapa é identificado como mapa tangente-Chebyshev do terceiro tipo. Na seção a seguir, são introduzidas algumas proposições preliminares sobre trigonometria em corpos finitos (CAMPELLO DE SOUZA et al., 1998a; LIMA; PANARIO; CAMPELLO DE SOUZA, 2014; LIMA; PANARIO; CAMPELLO DE SOUZA, 2010b; LIMA; PANARIO; CAMPELLO DE SOUZA, 2010a), necessárias especificamente ao desenvolvimento do conteúdo apresentado neste capítulo.

4.1 RESULTADOS PRELIMINARES SOBRE TRIGONOMETRIA EM CORPOS FINITOS

Nesta seção, são desenvolvidos alguns resultados sobre trigonometria em corpos finitos empregados nas proposições associadas aos mapas tangente-Chebyehsv do terceiro tipo. Os referidos resultados são inspirados no que já se tem de forma bem estabelecida para a trigonometria clássica; em todo caso, podem ser considerados contribuições secundárias desta tese, visto que ainda não haviam sido abordados na literatura.

Proposição 4.1 (Tangente da soma de dois arcos)**.** *Sejam $\zeta \in \mathbb{I}_q$ e i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$. Então,*

$$\tan_\zeta(x+y) = \frac{\tan_\zeta(x) + \tan_\zeta(y)}{1 + \tan_\zeta(x)\tan_\zeta(y)i^2}. \tag{28}$$

Demonstração. A proposição pode ser demonstrada considerando (3) e (4) para escrever

$$\tan_\zeta(x+y) = \frac{\operatorname{sen}_\zeta(x)\cos_\zeta(y) + \operatorname{sen}_\zeta(y)\cos_\zeta(x)}{\cos_\zeta(x)\cos_\zeta(y) + i^2\operatorname{sen}_\zeta(x)\operatorname{sen}_\zeta(y)}. \tag{29}$$

A prova é concluída dividindo o numerador e o denominador da última expressão pelo fator $\cos_\zeta(x)\cos_\zeta(y)$. □

Proposição 4.2 (Tangente do arco metade)**.** *Sejam $\zeta \in \mathbb{I}_q$ e i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$. Então,*

$$\tan_\zeta(x/2) = \frac{1 \pm \sqrt{1 - i^2\tan_\zeta^2(x)}}{i^2\tan_\zeta(x)}. \tag{30}$$

Demonstração. Da Proposição 4.1, fazendo $x = y$, escreve-se

$$\tan_\zeta(2x) = \frac{2\tan_\zeta(x)}{1 + i^2\tan_\zeta^2(x)}. \tag{31}$$

A partir de 4.1, fazendo $\tan_\zeta(2x) = a$ e $\tan_\zeta(x) = y$, pode-se escrever

$$i^2ay^2 - 2y + a = 0, \tag{32}$$

cuja solução é

$$y = \frac{1 \pm \sqrt{1 - i^2a^2}}{i^2a}. \tag{33}$$

Na expressão acima, substituindo y e a pelas respectivas expressões em termos de tangentes e, por fim, substituindo x e $2x$ por $x/2$ e x, correspondentemente, conclui-se a prova. □

Proposição 4.3. *Sejam $\zeta \in \mathbb{I}_q$ e i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$. Então,*

$$\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right) = \frac{1 \pm \sqrt{1 - i^2x^2}}{i^2x}. \tag{34}$$

Demonstração. A demonstração é feita empregando diretamente a Proposição 4.2 e considerando o fato de que $\tan_\zeta(\arctan_\zeta(x)) = x$. □

4.2 MAPAS TANGENTE-CHEBYSHEV DO TERCEIRO TIPO

A seguir, propõe-se uma definição para mapas tangente-Chebyshev do terceiro tipo. Naturalmente, a definição é inspirida na dos polinômios de Chebyshev do terceiro tipo e estabelecida de modo análogo à dos mapas tangente-Chevbyshev do primeiro tipo. A definições se originam da substituição, na expressão trigonométrica dos polinômios de Chebyshev do primeiro tipo sobre corpos finitos, da função cosseno sobre corpos finitos (e de sua inversa) pela função tangente sobre corpos finitos[1].

[1] A ausência, até o momento, de uma definição para mapas tangente-Chebyshev do segundo e do quarto tipos sobre corpos finitos explica-se pelo fato de não se ter concebido uma função que esteja para a tangente sobre corpos finitos como o seno está para o cosseno na trigonometria clássica (considerando alguma analogia baseada na satisfação de propriedades e identidades trigonométricas básicas). Sem tal definição, não se aplica as expressões

$$U_n(x) = \frac{\mathrm{sen}_\zeta((n+1)\arccos_\zeta(x))}{\mathrm{sen}_\zeta(\arccos_\zeta(x))}$$

e

$$W_n(x) = \frac{\mathrm{sen}_\zeta\left(\left(n+\frac{1}{2}\right)\arccos_\zeta(x)\right)}{\mathrm{sen}_\zeta\left(\frac{1}{2}\arccos_\zeta(x)\right)},$$

dos polinômios de Chebyshev do segundo e do quarto tipos sobre corpos finitos, respectivamente, a abordagem descrita.

Definição 4.1. *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*

$$E_n(x) = \frac{\tan_\zeta\left(\left(n+\frac{1}{2}\right)\arctan_\zeta(x)\right)}{\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)}, \tag{35}$$

em que $\zeta \in \mathbb{I}_q$ e $x \in \mathbb{T}_\zeta$.

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 4.4. *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*

$$E_{n+1}(x) = \frac{E_n(x) + x[c(x)]^{-1}}{1 + i^2 x c(x) E_n(x)}, \tag{36}$$

em que $c(x) = \tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)$.

Demonstração. Empregando a Definição 4.1, a Proposição 4.1 e a substituição indicada no final do enunciado da proposição em questão, pode-se escrever

$$\begin{aligned} E_{n+1}(x) &= \frac{\tan_\zeta\left(\left(n+1+\frac{1}{2}\right)\arctan_\zeta(x)\right)}{\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)}\frac{1}{c(x)} \\ &= \frac{\tan_\zeta\left(\left(n+\frac{1}{2}\right)\arctan_\zeta(x)\right) + \tan_\zeta\left((1)\arctan_\zeta(x)\right)}{1 + i^2\tan_\zeta\left((n)\arctan_\zeta(x)\right)\tan_\zeta\left((1)\arctan_\zeta(x)\right)}\frac{1}{c(x)} \\ &= \frac{\tan_\zeta\left(\left(n+\frac{1}{2}\right)\arctan_\zeta(x)\right) + x}{1 + i^2 x\tan_\zeta\left(\left(n+\frac{1}{2}\right)\arctan_\zeta(x)\right)}\frac{1}{c(x)}, \end{aligned}$$

multiplicando por $\frac{c(x)}{c(x)}$ tem-se

$$E_{n+1}(x) = \frac{E_n(x) + x[c(x)]^{-1}}{1 + i^2 x c(x) E_n(x)}.$$

□

Observe que o termo $c(x)$ na última proposição independe de n. Assim, se desejar avaliar $E_n(x)$ para valores específicos de n e x, empregando a relação de recorrência apresentada, o termo $c(x)$ só precisa ser calculado uma vez; daí por diante, quando da aplicação propriamente dita da recorrência até que se alcance o valor de n em questão, o referido termo pode ser tratado como se fosse uma constante. Também nesse contexto, observa-se, a partir da Proposição 4.3, que o cálculo de $c(x)$ envolve a extração de uma raiz quadrada sobre $\mathbb{F}_q$. Assim, ainda que $x \in \mathbb{F}_q$, é possível que $c(x) \in \mathbb{I}_q \backslash \mathbb{F}_q$. Detalhes sobre essa possibilidade são discutidos na sequência deste capítulo. Em todo caso, utilizando a Proposição 4.4, pode-se fornecer, por exemplo, as seguintes

expressões de mapas tangente-Chebyshev do terceiro tipo:

$$E_0(x) = 1, \tag{37}$$

$$E_1(x) = \frac{1 + x[c(x)]^{-1}}{1 + i^2 x c(x)}, \tag{38}$$

$$E_2(x) = \frac{1 + 2x[c(x)]^{-1} + i^2x^2}{1 + 2i^2 x c(x) + i^2x^2}, \tag{39}$$

$$E_3(x) = \frac{1 + 3x[c(x)]^{-1} + 3i^2x^2 + i^2x^3[c(x)]^{-1}}{1 + 3i^2 x c(x) + 3i^2x^2 + i^4x^3c(x)}, \tag{40}$$

$$E_4(x) = \frac{1 + 4x[c(x)]^{-1} + 6i^2x^2 + 4i^2x^3[c(x)]^{-1} + i^4x^4}{1 + 4i^2 x c(x) + 6i^2x^2 + 4i^4x^3c(x) + i^4x^4}. \tag{41}$$

Para ilustrar os resultados derivados na parte inicial deste capítulo, faz-se necessária uma regra que permita prover sem ambiguidade o valor da raiz quadrada envolvida no cálculo de $c(x)$. Em princípio, poder-se pensar em remover da expressão mais à direita em

$$c(x) = \tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right) = \frac{1 \pm \sqrt{1 - i^2x^2}}{i^2x}$$

o sinal "$\pm$", substituindo-o simplesmente por "$+$" e escolhendo uma das duas raízes segundo algum critério adicional. Porém, tal ação imporia a $c(x)$ uma simetria ímpar, o que não é coerente com a escrita trigonométrica da mesma expressão. Mais especificamente, embora se verifique a simetria (ímpar)

$$\arctan_\zeta(x) \equiv -\arctan_\zeta(-x \pmod p) \pmod{p+1},$$

a divisão por 2 no argumento da função tangente, que também possui simetria ímpar, torna $c(x)$ assimétrica. Isso sugere que sejam considerados valores diferentes da raiz quadrada em questão para x e $-x \pmod p$, o que, deste ponto em diante, é feito conforme a regra a seguir:

- Se $0 \leq x \leq \frac{p-1}{2}$, então $c(x) = \frac{1+\sqrt{1-i^2x^2}}{i^2x}$, em que $0 \leq \sqrt{1-i^2x^2} \leq \frac{p-1}{2}$ ou $0 \leq i^{-1}\sqrt{1-i^2x^2} \leq \frac{p-1}{2}$;
- Se $\frac{p+1}{2} \leq x \leq p-1$, então $c(x) = \frac{1\pm\sqrt{1-i^2x^2}}{i^2x}$, em que $\frac{p+1}{2} \leq \sqrt{1-i^2x^2} \leq p-1$ ou $\frac{p+1}{2} \leq i^{-1}\sqrt{1-i^2x^2} \leq p-1$.

Observe que as desigualdades cujos termos centrais são multiplicados por i^{-1}, em cada um dos itens acima. São necessárias porque o termo sob a raiz pode não ser um resíduo quadrático, o que resultaria em um elemento em um corpo de extensão, de modo que se tenha $\sqrt{1-i^2x^2} = di$, $d \in \mathbb{F}_p$.

O exemplo a seguir retoma o Exemplo 2.1 e considera a regra acima descrita.

Exemplo 4.1. *Neste exemplo, avalia-se, para todo $x \in \mathbb{T}_\zeta$, em que $\zeta = 2 + 3i \in \mathbb{I}_7$, $i^2 \equiv -1 \pmod 7$ e $\mathrm{ord}(\zeta) = 2(p+1) = 16$, o mapa tangente-Chebyshev do terceiro tipo*

$$E_3(x) = \frac{1 + 3x[c(x)]^{-1} - 3x^2 - x^3[c(x)]^{-1}}{1 - 3x c(x) - 3x^2 + x^3c(x)}. \tag{42}$$

Na Tabela 3, são apresentados inicialmente todos os valores de $\tan_\zeta(x)$*, de* $\arctan_\zeta(x)$ *e de*

$$c(x) = \tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right) = \frac{-1+\sqrt{1+x^2}}{x},$$

para $x \in \mathbb{T}_\zeta$*. Com relação a esta última função, chama atenção o aparecimento de valores* $c(x) \in \mathbb{I}_q \backslash \mathbb{F}_q$*; conforme comentado anteriormente, isso está associado ao cálculo da raiz quadrada na avaliação da função em questão. Naturalmente, este fato tem repercussão no cálculo de* $E_3(x)$*, que fornece os valores apresentados na última coluna da tabela.*

Tabela 3 – Valores para as funções tangente, arco-tangente e $E_3(x)$ relacionadas ao elemento $\zeta = 2+3i \in \mathbb{I}_7$, em que $\mathrm{ord}(\zeta) = 2(q+1) = 16$, $i^2 \equiv -1 \pmod 7$ e $x = 0, 1, \ldots, 7$.

x	$\tan_\zeta(x)$	$\arctan_\zeta(x)$	c(x)	$E_3(x)$
0	0	0	0	1
1	4	6	2	6
2	6	3	$3+5i$	$5+5i$
3	2	7	$2+3i$	$2+2i$
4	∞	1	$5+4i$	$2+2i$
5	5	5	$4+2i$	$5+5i$
6	1	2	5	6
7	3	–	–	–
∞	–	4	6	1

Fonte: O Autor (2023)

O fato comentado na parte final do exemplo acima pode ser explicado sob outra perspectiva. Para isso, considera-se (35), a qual pode ser reescrita como

$$E_n(x) = \frac{\tan_\zeta\left(\left(\frac{2n+1}{2}\right)\arctan_\zeta(x)\right)}{\tan_\zeta\left(\left(\frac{1}{2}\right)\arctan_\zeta(x)\right)} \tag{43}$$

$$= \frac{\tan_{\zeta^{\frac{1}{2}}}\left((2n+1)\arctan_\zeta(x)\right)}{\tan_{\zeta^{\frac{1}{2}}}\left(\arctan_\zeta(x)\right)}. \tag{44}$$

Na última equação, observa-se que o cálculo de $E_n(x)$ envolve (ainda que implicitamente, caso o referido cálculo seja realizado empregando alguma das fórmulas não-trigonométricas apresentadas) a avaliação de uma função tangente sobre corpos finitos com relação ao elemento $\zeta^{\frac{1}{2}} = \pm\sqrt{\zeta}$. Como $\mathrm{ord}(\zeta) = 2(q+1)$, pode-se assumir que $\zeta^{\frac{1}{2}} = \pm\sqrt{\zeta}$ corresponde à raiz quadrada de ζ com ordem multiplicativa $\mathrm{ord}(\zeta^{\frac{1}{2}}) = 4(q+1)$. Assim, considerando a Proposição 2.4, sabe-se que $\tan_{\zeta^{\frac{1}{2}}}(\cdot)$ provê valores que não se encontram em $\mathbb{F}_q$. Mais precisamente, uma tangente calculada com relação a $\zeta^{\frac{1}{2}}$ provê valores em $\mathbb{F}_q$, se e somente se o respectivo argumento for par; isso porque, escrevendo tal argumento como $2m$, tem-se

$$\tan_{\zeta^{\frac{1}{2}}}(2m) = \tan_\zeta(m) \in \mathbb{F}_q,$$

o que não se consegue, se o referido argumento for ímpar. Em suma, considerando (44) e o fato de $(2n+1)$ ser ímpar, para que se tenha $E_n(x) \in \mathbb{F}_q$, é necessário e suficiente que $\arctan_\zeta(x)$ seja par. Essa condição pode ser verificada no último exemplo, observando, na Tabela 3, em que apenas os valores pares ao longo da coluna $\arctan_\zeta(x)$ levam a valores $E_3(x) \in \mathbb{F}_q$.

Em seguida, são dadas duas proposições em que os mapas tangente-Chebyshev do terceiro tipo são relacionados aos do primeiro tipo.

Proposição 4.5. *Sejam $\zeta \in \mathbb{I}_q$, i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$ e $n \in \mathbb{N}$. Então,*

$$E_n(x) = [c(x)]^{-1} \frac{1 \pm \sqrt{1 - i^2 C_{2n+1}^2(x)}}{i^2 C_{2n+1}(x)}. \tag{45}$$

Demonstração. (35) pode ser reescrita como

$$E_n(x) = \frac{\tan_\zeta\left(\frac{1}{2}(2n+1)\arctan_\zeta(x)\right)}{c(x)}.$$

Aplicando a Proposição 4.2 ao numerador da última expressão, obtém-se

$$E_n(x) = \frac{1}{c(x)} \frac{1 \pm \sqrt{1 - i^2 \tan_\zeta^2((2n+1)\arctan_\zeta(x))}}{i^2 \tan_\zeta((2n+1)\arctan_\zeta(x))},$$

e empregando a Definição 2.5, conclui-se a demonstração. □

Proposição 4.6. *Sejam $\zeta \in \mathbb{I}_q$, i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$ e $n \in \mathbb{N}$. Então,*

$$E_n(x) = \frac{C_{2n+1}\left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}\right)}{\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}} = \frac{C_{2n+1}(c(x))}{c(x)}. \tag{46}$$

Demonstração. Empregando a Definição 2.5, tem-se

$$\frac{C_{2n+1}\left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}\right)}{\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}} = \frac{\tan_\zeta\left((2n+1)\arctan_\zeta\left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}\right)\right)}{\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}}. \tag{47}$$

Considerando a Proposição 4.3, a última expressão pode ser reescrita como

$$\frac{C_{2n+1}\left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}\right)}{\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}} = \frac{\tan_\zeta\left((2n+1)\arctan_\zeta\left(\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)\right)\right)}{\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)} \tag{48}$$

$$= \frac{\tan_\zeta\left((2n+1)\frac{1}{2}\arctan_\zeta(x)\right)}{\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)}, \tag{49}$$

e o resultado segue. □

A última proposição pode ser empregada na obtenção de uma expressão explícita para os mapas tangente-Chebyshev do terceiro tipo; considerando também (11), escreve-se diretamente

$$E_n(x) = \frac{\sum_{k=0}^{\lfloor 2n/2 \rfloor} \binom{2n+1}{2k+1} i^{2k} \left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x} \right)^{2k+1}}{\sum_{k=0}^{\lfloor (2n+1)/2 \rfloor} \binom{2n+1}{2k} i^{2k} \left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x} \right)^{2k}} \frac{1}{\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x}} \tag{50}$$

$$= \frac{\sum_{k=0}^{n} \binom{2n+1}{2k+1} i^{2k} \left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x} \right)^{2k}}{\sum_{k=0}^{n} \binom{2n+1}{2k} i^{2k} \left(\frac{1 \pm \sqrt{1-i^2x^2}}{i^2 x} \right)^{2k}} \tag{51}$$

$$= \frac{\sum_{k=0}^{n} \binom{2n+1}{2k+1} i^{2k} \left(c(x) \right)^{2k}}{\sum_{k=0}^{n} \binom{2n+1}{2k} i^{2k} \left(c(x) \right)^{2k}}. \tag{52}$$

Observe que, fixado o valor de i, a última equação provê uma maneira de expressar $E_n(x)$ como uma função racional de $c(x)$, diferentemente do que se obtém empregando a relação de recorrência dada na Proposição 4.4; esta última provê expressões em que o numerador e o denominador possuem termos cruzando $c(x)$, $[c(x)]^{-1}$ e potências de x. Utilizando (52), produz-se, por exemplo,

$$E_0(x) = 1, \tag{53}$$

$$E_1(x) = \frac{3 + i^2c^2(x)}{1 + 3i^2c^2(x)}, \tag{54}$$

$$E_2(x) = \frac{5 + 10i^2c^2(x) + i^4c^4(x)}{1 + 10i^2c^2(x) + 5i^4c^4(x)}, \tag{55}$$

$$E_3(x) = \frac{7 + 35i^2c^2(x) + 21i^4c^4(x) + i^6c^6(x)}{1 + 21i^2c^2(x) + 35i^4c^4(x) + 7i^6c^6(x)}, \tag{56}$$

$$E_4(x) = \frac{9 + 84i^2c^2(x) + 126i^4c^4(x) + 36i^6c^6(x) + i^8c^8(x)}{1 + 36i^2c^2(x) + 126i^4c^4(x) + 84i^6c^6(x) + 9i^8c^8(x)}. \tag{57}$$

Exemplo 4.2. *Neste exemplo, considera-se* $\zeta = 3 + 6i \in \mathbb{I}_{23}$, $i^2 \equiv -1 \pmod{23}$ *e* $\operatorname{ord}(\zeta) = 2(p+1) = 48$, *e avalia-se o mapa tangente-Chebyshev do terceiro tipo*

$$E_2(x) = \frac{\tan_\zeta \left(\frac{5 \arctan_\zeta(x)}{2} \right)}{\tan_\zeta \left(\frac{\arctan_\zeta(x)}{2} \right)} = \frac{5 + 13c^2(x) + c^4(x)}{1 + 13c^2(x) + 5c^4(x)}, \tag{58}$$

para todos os valores de $x \in \mathbb{T}_\zeta$ *para os quais* $\arctan_\zeta(x)$ *é par. Na Tabela 4, são apresentados inicialmente todos os valores de* $\tan_\zeta(x)$, *de* $\arctan_\zeta(x)$ *e de*

$$c(x) = \tan_\zeta \left(\frac{1}{2} \arctan_\zeta(x) \right) = \frac{-1 + \sqrt{1 + x^2}}{x}.$$

4.2.1 Polos e Zeros

A seguir, são determinados os polos e zeros do mapa E_n.

Tabela 4 – Valores para as funções tangente, arco-tangente e $c(x)$ relacionadas ao elemento $\zeta = 3 + 6i \in \mathbb{I}_{23}$, em que $\mathrm{ord}(\zeta) = 2(q+1) = 48$, $i^2 \equiv -1 \pmod{23}$.

x	$\tan_\zeta(x)$	$\arctan_\zeta(x)$	$c(x)$	$E_2(x)$
0	0	0	0	1
1	11	18	4	10
5	15	10	15	13
7	20	8	10	22
9	4	22	21	13
10	5	4	14	2
13	2	20	5	12
14	18	2	11	16
16	16	16	7	22
18	1	14	20	16
22	9	6	6	7
23	12	-	-	-
∞	-	12	22	1

Fonte: O Autor (2023)

Proposição 4.7. *Os zeros $r_k \in \mathbb{F}_q$ do mapa tangente-Chebyshev do terceiro tipo sobre $\mathbb{F}_q$ são dados por*

$$r_k = \begin{cases} \tan(k(q+1)), \\ \tan((2k+1)(q+1)). \end{cases} \tag{59}$$

em que k é qualquer número inteiro tal que $k(q+1)/n$ também é um número inteiro.

Demonstração. Desenvolvendo $E_n(x)$, tem-se

$$E_n(x) = \frac{\mathrm{sen}((n+1/2)\arctan(x)))\cos(\arctan(x)/2)}{\cos((n+1/2)\arctan(x)))\mathrm{sen}(\arctan(x)/2)} \tag{60}$$

Para r_k ser um zero de E_n, é preciso que $\mathrm{sen}((n+1/2)\arctan(x)))\cos(\arctan(x)/2) = 0$ ou, de modo equivalente, $(n+1/2)\arctan(x) \equiv 0 \pmod{(q+1)}$ ou $\arctan(x)/2 \equiv \left(\frac{q+1}{2}\right) \pmod{(q+1)}$. Noutras palavras, isso significa que $(n+1/2)\arctan_\zeta(r_k) = k(q+1)$, $k \in \mathbb{Z}$, ou que $\arctan_\zeta(r_k) = (2k+1)(q+1)$, $k \in \mathbb{Z}$e o resultado segue. □

Proposição 4.8. *Os polos $s_k \in \mathbb{F}_q$ do mapa tangente-Chebyshev do terceiro sobre $\mathbb{F}_q$ são dados por*

$$r_k = \begin{cases} \tan\left[\frac{(2k+1)(q+1)}{2n+1}\right], \\ \tan\left[2k(q+1)\right]. \end{cases} \tag{61}$$

em que k é qualquer inteiro tal que $(2k+1)(q+1)/2n$ também é um inteiro.

Demonstração. Para s_k ser um polo de E_n, é preciso que

$$\cos((n+1/2)\arctan(x)))\mathrm{sen}(\arctan(x)/2) = 0,$$

ou, de modo equivalente, $(n + 1/2)\arctan(x) \equiv \left(\frac{q+1}{2}\right) \pmod{(q+1)}$ ou $\arctan(x)/2 \equiv 0 \pmod{(q+1)}$. Noutras palavras, isso significa que $(n + 1/2)\arctan_\zeta(r_k) = (2k+1)(q+1)$, ou que $\arctan_\zeta(r_k) = k(q+1)$, $k \in \mathbb{Z}$ e segue o resultado. $\square$

5 ESTUDO PRELIMINAR DE APLICAÇÃO

5.1 CIGRAGEM DE CHAVE PÚBLICA BASEADO NOS POLINÔMIOS TANGENTE-CHEBYSHEV DO TIPO I

A criptografia moderna é conhecida como a ciência da segurança da informação, que teve inicio com o artigo *Communication Theory of Secrecy Systems* (SHANNON, 1949), porém, esta área ficou realmente conhecida com a publicação do artigo *New Directions in Cryptograph* (DIFFIE; HELLMAN, 1976). Diffie e Hellman demonstraram, pela primeira vez, que uma comunicação secreta é possível sem a transferência da chave secreta, o que se entitula como criptografia de chave pública.

Em um sistema de criptografia de chave pública, cada entidade A tem uma chave pública e e uma chave privada d. Em sistemas computacionais, a tarefa de computar d dado e é inviável. A chave pública define uma transformação de cifragem E_e, enquanto a chave privada define uma transformação de cifragem D_d. Se Alice pretende mandar uma mensagem M para Bob, Alice usa a chave pública de Bob para realizar a transformação de cifragem $C = E_e(M)$ para obter o texto cifrado, e transmite C para Bob. Para ler a mensagem, Bob utiliza a sua chave privada para realizar a transformação $M = D_d(C)$, obtendo assim, a mensagem original.

Embora os polinômios de Chebyshev tenham propriedades caóticas, que são adequadas para fins criptográficos, eles não fornecem segurança e explorando a definição de polinômios de Chebyshev, e manipulando-os algebricamente , pode recuperar o texto cifrado (KOCAREV, 2011). Com o propósito de evitar essa falha, Ning (NING; LIU; HE, 2006) a definição de polinômios de Chebyshev para corpos finitos foi expandida, evitando dessa forma a vulnerabilidade sobre o intervalo $[-1, 1]$, em que se tem uma boa propriedade unilateral (NING; LIU; HE, 2006). Em (LIMA; CAMPELLO DE SOUZA; PANARIO, 2008), foi introduzida uma nova definição dos polinômios de Chebyshev sobre corpos finitos, baseada na trigonometria em corpos finitos (CAMPELLO DE SOUZA et al., 1998b), o que permitiu o estudo sobre segurança do algoritmo proposto em (NING; LIU; HE, 2006).

Polinômios de Chebyshev definidos sobre corpos finitos têm sido bastante utilizados como parte de criptossistemas de chave pública (HUE; HOANG; BRAEKEN, 2017; YOSHIOKA, 2018c; YOSHIOKA, 2020; CLAUDIO; PANARIO, 2019; WEI; SHANG; WENZHENG, 2021; KRITSANAPONG; CHALIDA, 2021). Por causa das semelhanças entre os mapas tangente-Chebyshev e os polinômios de Chebyshev sobre corpo finito proposto por Lima (LIMA; CAMPELLO DE SOUZA; PANARIO, 2008), é esperado que um criptossistema de chave pública utilizando os mapas tangente-Chebyshev tenha resultados semelhantes. Seguindo o procedimento proposto em (NING; LIU; HE, 2006), o procedimento de criação de um sistema de criptografia de chave pública é dividido em três partes.

5.1.1 Geração do par de chaves

Para Alice obter o par de chaves, é necessário o seguinte procedimento:

1. Seleciona-se aleatoriamente um número $s \in \mathbb{Z}$, sendo $s \neq 0, 1$, e $x \in \mathbf{F}_q$, sendo $x \neq 0, 1$, e computa-se $C_s(x)$.

2. Denomina-se s como a chave privada de Alice e $(x, C_s(x))$ como a chave pública.

5.1.2 Cifrando a mensagem

Assume-se que Bob deseja enviar uma mensagem $M \in \mathbf{F}_q$, sendo $M \neq 0$, para Alice. Para tal, o procedimento é o seguinte:

1. Seleciona-se um inteiro $r \in \mathbb{Z}$, $r \neq 0, 1$;

2. A partir da chave pública de Alice $(x, C_s(x)$ computa-se $C_r(x)$, em que $C_{rs}(x) = C_r(C_s(x))$ e $X = MC_{rs}(x) \bmod \quad f(y)$, sendo $f(y)$ um polinômio primitivo.

3. Envia-se o texto cifrado $T = (C_r(x), X)$ para Alice.

5.1.3 Decifrando a mensagem

Após receber a mensagem, para poder ler o conteúdo, Alice segue o seguinte procedimento:

1. Utiliza a chave privada s para computar $C_{sr}(x) = C_s(C_r(x))$;

2. Recupera-se a mensagem M computando $M = X(C_{sr}(x))^{-1}$.

Devido a propriedade de semigrupo dos polinômios tangente-Chebyshev, a mensagem M é recuperada corretamente (NING; LIU; HE, 2006).

5.1.4 Análise de segurança do algortimo

De maneira similar à (LIMA; PANARIO; CAMPELLO DE SOUZA, 2010b), presume-se que o algoritmo é seguro por causa da não existência de definições trigonométricas para efetuar o ataque descrito em (BERGAMO et al., 2005). Nesta seção o ataque descrito por Bergamo é aplicado para os polinômios tangente-Chebyshev para $q \equiv 3 (\bmod\ 4)$, e é demonstrado que a solução envolve o problema do logaritmo discreto.

Para recuperar a mensagem M, dado a chave pública de Alice $(x, C_s(x))$ e o texto cifrado $C_r(x), X$, é necessário seguir o seguinte procedimento:

1. Computar r' de modo que $C_{r'}(x) = C_r(x)$;

2. Avaliar $C_{r's}(x) = C_{r'}(C_s(x))$;

3. Recuperar a mensagem $M = X(C_{r's}(x))^{-1}$.

Este procedimento é sempre válido, dado que, se $C_{r'}(x) = C_r(x)$, então

$$\begin{aligned} C_{rs}(x) &= C_{sr}(x) = C_s(C_r(x)) \\ &= C_s(C_{r's}(x)) = C_{r's}(C_s(x)). \end{aligned}$$

O cálculo de r' é sumarizado no seguinte resultado.

Lema 5.1. *Para cada par $x, C_r(x)$, o inteiro r' satisfaz $C_{r'}(x) = C_r(x)$ se, somente se,*

$$r' = \arctan_\zeta((C_r(x))\,(\arctan_\zeta(x))^{-1}\,(\mathrm{mod}\ N), \tag{62}$$

para $N = ord(\zeta)$.

Prova. *Assume-se que*

$$r' = \arctan_\zeta(C_r(x))(\arctan_\zeta(x))^{-1}(\mathrm{mod}\ N).$$

A partir da Definição 2.5,

$$C_{r'}(x) = \tan_\zeta(r' \arctan_\zeta(x)),$$

substituindo r' tem-se

$$\begin{aligned} C_{r'}(x) &= \tan_\zeta(\arctan_\zeta(C_r(x))(\arctan_\zeta(x))^{-1} \arctan_\zeta(x) \\ &= \tan_\zeta(\arctan_\zeta(C_r(x))) = C_r(x). \end{aligned}$$

Por outro lado, assumindo que $C_{r'}(x) = C_r(x)$, tem-se

$$C_{r'}(x) = \tan_\zeta(r' \arctan_\zeta(x) = C_r(x).$$

Aplicando a função $\arctan_\zeta$ em ambos os lados da igualdade, tem-se

$$\arctan_\zeta(\tan_\zeta(r' \arctan_\zeta(x))) = \arctan_\zeta(C_r(x)). \tag{63}$$

Seja $y = \arctan_\zeta(w)$. A partir de (2.3), a função trigonometrica tangente em corpo finito tem simetria ímpar, i.e.,

$$\tan_\zeta(-x) = -\tan_\zeta(x). \tag{64}$$

Devido à periodicidade da função $\tan_\zeta$, se $\tan_\beta = w$, tem-se que $\beta = y(\mathrm{mod}\ N)$. Portanto (63) se mantém se, somente se,

$$r' = \arctan_\zeta(C_r(x))(\arctan_\zeta(x))^{-1}(\mathrm{mod}\ N).$$

■

Diferentemente dos ataques contra criptossistemas baseados nos polinômios de Chebyshev clássicos, sobre corpos finitos, o Lemma 5.1 resulta em somente um valor de r'. Portanto, não é preciso considerar aspectos de precisão ou resolver qualquer sistema linear de equações modulares.

Contudo, a computação de r' em (62) depende da restrição sobre a existência da função inversa da tangente. Aplicando (6) em (62) tem-se

$$r' = \frac{1}{2}\log_\zeta \frac{\frac{1}{2}\log_\zeta \frac{1+ix}{1-ix} + iC_r(x)}{\frac{1}{2}\log_\zeta \frac{1+ix}{1-ix} - iC_r(x)}. \tag{65}$$

Noutras palavras, dado um texto cifrado, para recuperar a mensagem original, sem o conhecimento da chave privada, é necessário computar r', o que envolve resolver o problema do logaritmo discreto.

Exemplo 5.1. *Seja a chave pública de Alice* $(x, C_s(x))$ *e o texto cifrado* $T = (C_r(x), X)$*, em que* $X = MC_{rs}(x)$*. É possível mostrar como um adversário computa* $C_{rs}(x)$ *e recupera a mensagem* M*.*

O corpo considerado é $\mathbf{F}_{43}$*. Além disso,* $x = 38$ *e* $s = 25$*. A partir de (2.4), computa-se* $C_s(x)$*. Alice entrega sua chave pública* $(x, C_s)(x) = (38, 21)$ *para Bob. Bob escolhe* $r = 32$ *para cifrar a mensagem* M *e computa* $C_r(x) = 15$*. Com isto, Bob chega em* $C_r(C_s(x))$*. Para um adversário recuperar a mensagem cifrada, este deve deter o valor de* r*, ou seja, deve computar um* $r' = r$ *usando o Lema (62). Utilizando a (62), é possível obter*

$$\begin{aligned} r' &= \arctan(C_r(x))(\arctan(x)^{-1}(\text{mod } 44) = \arctan(15)(\arctan(38)^{-1}(\text{mod } 44) \\ &= 16^{-1}(\text{mod } 44) = 16 \times 35(\text{mod } 44) = 32. \end{aligned}$$

O texto original enviado por Bob pode ser recuperado a partir de $M = X(C_{32}(C_s(x)))^{-1}(\text{mod } 43)$

5.2 CONCLUSÕES

Neste capítulo, é apresentada a investigação sobre possível aplicações do mapa tangente-Chebyshev do primeiro tipo. Analisou-se de forma preliminar o uso dos mapas tangente-Chebyshev do primeiro tipo em um sistema de cifragem de chave pública. Apresentou-se uma análise de segurança, a qual indica a possibilidade de utilização dos mapas nessa aplicação. Em função da propriedade de semigrupo, demonstrou-se que a quebra de um sistema deste tipo envolve o problema do logaritmo discreto, o que sugere que, dependendo dos parâmetros escolhidos, seu uso prático pode ser viável.

6 CONCLUSÕES

Neste capítulo são apresentadas as considerações finais da tese desenvolvida. Para isso, são elencadas a seguir as contribuições originais do trabalho realizado:

1. Partindo de um estudo sobre os recém-introduzidos mapas racionais tangente-Chebysyhev sobre corpos finitos, foram estabelecidas novas propriedades desses mapas. Mais especificamente, foram propostos resultados relativos aos pontos fixos dos mapas tangente-Chebysyhev e às suas relações com as funções de Rédei e com a transformação de Möbius.

2. Foram estabelecidas diversas proposições associadas aos grafos funcionais dos mapas tangente-Chebysyhev, e indicados aspectos interessantes concernentes a essas representações.

3. Foi introduzida a definição de um novo tipo de mapa racional tangente-Chebysyhev sobre corpos finitos, o qual possui analogia com os polinômios de Chebyshev do terceiro tipo; propriedades básicas desses mapas, como o seu cálculo por equações de recorrência, sua relação com os mapas do primeiro tipo e seus zeros e polos, foram estabelecidas.

4. Foi realizada uma investigação preliminar a respeito do uso dos mapas tangente-Chebysyhev para cifragem de chave pública.

6.1 CONTINUIDADE DA PESQUISA

Embora a tese apresentada contenha, conforme delineado na última seção, contribuições teóricas originais e sugestões consistentes de cenários em que a teoria desenvolvida pode ser aplicada, ela abre, também, margem para realização de novas pesquisas. Estas contribuições podem ser útil para outros estudantes e mesmo para o autor da tese, considerando a perspectiva de continuidade do seu envolvimento com a Academia. Assim, as seguintes direções e sugestões de temas para trabalhos futuros podem ser listadas:

1. Ampliação dos resultados acerca dos grafos funcionais associados aos mapas tangente-Chebysyhev do primeiro tipo, indicando como tal caracterização se relaciona com propriedades já estabelecidas para esses mapas e utilizando-a para o estabelecimento de novas propriedades nesse contexto.

2. Estabelecimento de novas propriedades dos mapas racionais tangente-Chebysyhev do terceiro tipo, o que deve incluir, por exemplo, propriedades de permutação, de involução e caracterização dos respectivos grafos funcionais.

3. Realização de novos estudos sobre a possibilidade de definir mapas racionais tangente-Chebysyhev do segundo e do quarto tipo e, consequentemente, de estudar as suas propriedades.

4. Investigar o uso dos mapas tangente-Chebysyhev em entrelaçadores empregados em codificação de canal, mais especificamente os códigos turbo.

5. Consolidação dos resultados referentes ao uso dos mapas tangente-Chebyshev em entrelaçadores empregados em esquemas de criptografia de chave pública.

6. Avaliação do uso dos mapas tangente-Chebyshev como blocos reponsáveis pelo *embaralhamento* de símbolos em esquemas de criptografia de chave secreta.

6.2 ARTIGO ASSOCIADO A ESTA TESE

O seguinte artigo em periódico internacional resultou desta tese:
FIGUEIREDO, RAVI B.D.; LIMA, J. B.. Tangent-Chebyshev maps over finite fields: New properties and functional graphs. Cryptography and Communications - Discrete Structures Boolean Functions and Sequences, p. 1-10, 2022. DOI: https://doi.org/10.1007/s12095-022-00565-8

REFERÊNCIAS

BARBIER, M.; CHEBALLAH, H.; BARS, J. M. On the computation of the möbius transform. **Theoretical Computer Science**, v. 809, p. 171 – 188, 2020. ISSN 0304-3975. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0304397519307674>. Citado na página 28.

BELLINI, E.; MURRU, N. An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics. **Finite Fields and Their Applications**, Academic Press, v. 39, p. 179–194, may 2016. ISSN 1071-5797. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S1071579716000198>. Citado na página 27.

BERGAMO, P. et al. Security of public-key cryptosystems based on Chebyshev polynomials. **IEEE Trans. Circuits Syst. I, Reg. Papers**, v. 52, n. 7, p. 1382–1393, July 2005. Citado 2 vezes nas páginas 22 e 47.

BORS, A.; PANARIO, D.; WANG, Q. **Functional graphs of generalized cyclotomic mappings of finite fields**. 2023. Citado na página 29.

BURTON, D. M. **Elementary Number Theory**. 7th. ed. [S.l.]: McGraw-Hill Science/Engineering/Math, 2010. Citado na página 26.

CAMPELLO DE SOUZA, R. M. et al. Trigonometry in finite fields and a new Hartley transform. In: IEEE. **Proc. IEEE Int. Symp. Inf. Theory**. [S.l.], 1998. p. 293. Citado 3 vezes nas páginas 15, 16 e 37.

CAMPELLO DE SOUZA, R. M. C. et al. Trigonometry in finite fields and a new Hartley transform. In: **Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on**. [S.l.: s.n.], 1998. p. 293. Citado na página 46.

CAPAVERDE, J.; MASUDA, A. M.; RODRIGUES, V. M. Rédei permutations with cycles of the same length. **Designs, Codes and Cryptography**, v. 88, n. 12, p. 2561–2579, Dec 2020. ISSN 1573-7586. Disponível em: <https://doi.org/10.1007/s10623-020-00801-3>. Citado na página 29.

CHARPIN, P.; MESNAGER, S.; SARKAR, S. Involutions over the Galois field $\mathbb{F}_{2^n}$. **IEEE Transactions on Information Theory**, v. 62, n. 4, p. 2266–2275, April 2016. Citado na página 24.

CHENGQING, L. et al. The graph structure of the generalized discrete arnold's cat map. **IEEE Transactions on Computers**, v. 71, n. 2, p. 364–377, 2022. Citado na página 29.

CHEONG, K. Y.; KOSHIBA, T. More on security of public-key cryptosystems based on Chebyshev polynomials. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 54, n. 9, p. 795–799, September 2007. Citado na página 22.

CLAUDIO, Q.; PANARIO, D. The graph structure of Chebyshev polynomials over finite fields and applications. **Designs, Codes and Cryptography**, v. 87, n. 2, p. 393–416, 2019. ISSN 1573-7586. Disponível em: <https://doi.org/10.1007/s10623-018-0545-7>. Citado na página 46.

DA SILVA NETO, E. F.; LIMA, J. B. Audio encryption based on the cosine number transform. **Multimedia Tools and Applications**, v. 75, n. 14, p. 8403–8418, July 2016. Citado na página 15.

DICKSON, L. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. **Annals of Mathematics**, Annals of Mathematics, v. 11, n. 1/6, p. 65–120, 1896. ISSN 0003486X. Disponível em: <http://www.jstor.org/stable/1967217>. Citado na página 12.

DIFFIE, W.; HELLMAN, M. New directions in cryptography. **IEEE Transactions on Information Theory**, v. 22, n. 6, p. 644–654, 1976. Citado na página 46.

DING, C.; ZHOU, Z. Binary cyclic codes from explicit polynomials over gf(2m). **Discrete Mathematics**, v. 321, p. 76 – 89, 2014. ISSN 0012-365X. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0012365X13005311>. Citado na página 12.

EDOUARD, L. Théorie des fonctions numériques simplement périodiques. **American Journal of Mathematics**, Johns Hopkins University Press, v. 1, n. 2, p. 184–196, 1878. ISSN 00029327, 10806377. Disponível em: <http://www.jstor.org/stable/2369308>. Citado na página 29.

FAN, X. A classification of permutation polynomials of degree 7 over finite fields. **Finite Fields and Their Applications**, v. 59, p. 1 – 21, 2019. ISSN 1071-5797. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071579719300449>. Citado na página 12.

FIGUEIREDO, R. B. D.; LIMA, J. B. Fractional angular transform: a number-theoretic approach. **Electronics Letters**, v. 55, n. 6, p. 322–325, March 2019. Citado na página 15.

GASSERT, A. T. Chebyshev action on finite fields. **Discrete Mathematics**, v. 315-316, p. 83 – 94, 2014. ISSN 0012-365X. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0012365X1300441X>. Citado na página 34.

GUPTA, R.; SHARMA, R. K. On permutation polynomials over finite fields of characteristic 2. **Journal of Algebra and Its Applications**, v. 15, n. 07, p. 1650133, 2016. Disponível em: <https://doi.org/10.1142/S0219498816501334>. Citado na página 12.

HERMITE, C. Sur les fonctions de sept lettre. **C. R. Acad. Sci.**, v. 57, p. 750–757, 1863. Citado na página 12.

HOU, X.-D. Permutation polynomials over finite fields — a survey of recent advances. **Finite Fields and Their Applications**, v. 32, p. 82 – 119, 2015. ISSN 1071-5797. Special Issue : Second Decade of FFA. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071579714001117>. Citado na página 12.

HUE, T. T. K.; HOANG, T. M.; BRAEKEN, A. Lightweight signcryption scheme based on discrete chebyshev maps. In: **2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)**. [S.l.: s.n.], 2017. p. 43–47. Citado na página 46.

IOANNIS, D.; GEORGIOS, T.; FEDERICO, M. The möbius transform effect in singular systems of differential equations. **Applied Mathematics and Computation**, v. 361, p. 338 – 353, 2019. ISSN 0096-3003. Citado na página 28.

JELÍNEK, V. et al. On the growth of the möbius function of permutations. **Journal of Combinatorial Theory, Series A**, v. 169, p. 105121, 2020. ISSN 0097-3165. Citado na página 28.

KOCAREV, L.; TASEV, Z. Public-key encryption based on Chebyshev maps. In: **Proc. IEEE Int. Symp. Circuits Syst.** [S.l.: s.n.], 2003. v. 3, p. 28–31. Citado na página 22.

KOCAREV, S. L. L. **Chaos-based Cryptography**. [S.l.]: Springer-Verlag Berlin Heidelberg, 2011. v. 1. ISBN 978-3-642-20542-2. Citado na página 46.

KRITSANAPONG, S.; CHALIDA, S. Increasing security to public key cryptography for point-to-point communication. **Journal of Discrete Mathematical Sciences and Cryptography**, Taylor and Francis, v. 0, n. 0, p. 1–15, 2021. Disponível em: <https://doi.org/10.1080/09720529.2021.1930656>. Citado na página 46.

LAIGLE-CHAPUY, Y. Permutation polynomials and applications to coding theory. **Finite Fields and Their Applications**, v. 13, n. 1, p. 58 – 70, 2007. ISSN 1071-5797. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071579705000705>. Citado na página 12.

LEHMER, D. H. An extended theory of lucas' functions. **Annals of Mathematics**, Annals of Mathematics, v. 31, n. 3, p. 419–448, 1930. ISSN 0003486X. Disponível em: <http://www.jstor.org/stable/1968235>. Citado na página 29.

LENORE, B.; MANUEL, B.; MICHAEL, S. A simple unpredictable pseudo-random number generator. **SIAM J. Comput.**, v. 15, p. 364–383, 1986. Citado na página 29.

LI, J.; CHANDLER, D. B.; XIANG, Q. Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. **Finite Fields and Their Applications**, v. 16, n. 6, p. 406 – 419, 2010. ISSN 1071-5797. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071579710000602>. Citado na página 12.

LI, L. et al. New classes of complete permutation polynomials. **Finite Fields and Their Applications**, v. 55, p. 177–201, 2019. ISSN 1071-5797. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1071579718301254>. Citado na página 12.

LIDL, R.; MULLEN, G. L.; TURNWALD, G. **Dickson Polynomials**. [S.l.]: Chapman and Hall/CRC, 1993. ISBN 0 582 09119 5. Citado na página 12.

LIMA, J.; BARONE, M.; CAMPELLO DE SOUZA, R. Cosine transforms over fields of characteristic 2. **Finite Fields and Their Applications**, v. 37, p. 265–284, 2016. ISSN 1071-5797. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1071579715001069>. Citado na página 58.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Fractional cosine and sine transforms over finite fields. **Linear Algebra and its Applications**, v. 438, n. 8, p. 3217–3230, April 2013. Citado na página 15.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M.; PANARIO, D. Security of public-key cryptosystems based on chebyshev polynomials over prime finite fields. p. 1843–1847, 2008. Citado na página 46.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. C. Tangent function and chebyshev-like rational maps over finite fields. **IEEE Transactions on Circuits and Systems II: Express Briefs**, p. 1–1, 2019. Citado 11 vezes nas páginas 13, 15, 16, 17, 18, 19, 21, 22, 23, 24 e 27.

LIMA, J. B.; PANARIO, D.; CAMPELLO DE SOUZA, R. M. Public-key encryption based on Chebyshev polynomials over GF(q). **Information Processing Letters**, v. 111, n. 2, p. 51–56, December 2010. Citado na página 22.

LIMA, J. B.; PANARIO, D.; CAMPELLO DE SOUZA, R. M. C. Public-key encryption based on Chebyshev polynomials over finite fields. **Information Processing Letters**, v. 111, n. 2, p. 51 – 56, 2010. ISSN 0020-0190. Citado 2 vezes nas páginas 12 e 37.

LIMA, J. B.; PANARIO, D.; CAMPELLO DE SOUZA, R. M. C. Public-key encryption based on chebyshev polynomials over gf(q). **Information Processing Letters**, v. 111, n. 2, p. 51 – 56, 2010. ISSN 0020-0190. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0020019010003170>. Citado 3 vezes nas páginas 12, 37 e 47.

LIMA, J. B.; PANARIO, D.; CAMPELLO DE SOUZA, R. M. C. A trigonometric approach for Chebyshev polynomials over finite fields. In: LARCHER, G. et al. (Ed.). **Applied Algebra and Number Theory**. Cambridge: Cambridge University Press, 2014. p. 255–279. Citado 4 vezes nas páginas 12, 15, 16 e 37.

LIU , Q.; SUN, Y.; ZHANG, W. Some classes of permutation polynomials over finite fields with odd characteristic. **Applicable Algebra in Engineering, Communication and Computing**, v. 29, n. 5, p. 409–431, Nov 2018. ISSN 1432-0622. Disponível em: <https://doi.org/10.1007/s00200-018-0350-6>. Citado na página 12.

MASON, J.; HANDSCOMB, D. C. **Chebyshev Polynomials**. [S.l.]: Chapman & Hall/CRC, 2003. ISBN 9780849303555. Citado na página 12.

MIKHAIL, M.; ABOUELSEOUD, Y.; ELKOBROSY, G. Two-phase image encryption scheme based on FFCT and fractals. **Security and Communication Networks**, p. 1–13, January 2017. Citado na página 15.

MULLEN, G. L.; PANARIO, D. **Handbook of Finite Fields**. [S.l.]: Chapman & Hall/CRC, 2013. Citado na página 22.

MURATOVIC-RIBIC, A.; PASALIC, E. A note on complete polynomials over finite fields and their applications in cryptography. **Finite Fields and Their Applications**, v. 25, p. 306 – 315, 2014. ISSN 1071-5797. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071579713001135>. Citado na página 12.

NADIR, M. A note on the use of rédei polynomials for solving the polynomial pell equation and its generalization to higher degrees. **The Ramanujan Journal**, v. 53, n. 3, p. 693–703, Dec 2020. ISSN 1572-9303. Disponível em: <https://doi.org/10.1007/s11139-019-00233-1>. Citado na página 27.

NING, H.; LIU, Y.; HE, D. Public key encryption algorithm based on chebyshev polynomials over finite fields. In: **2006 8th international Conference on Signal Processing**. [S.l.: s.n.], 2006. v. 4. Citado 2 vezes nas páginas 46 e 47.

PANARIO, D.; REIS, L. The functional graph of linear maps over finite fields and applications. **Designs, Codes and Cryptography**, v. 87, n. 2, p. 437–453, Mar 2019. ISSN 1573-7586. Disponível em: <https://doi.org/10.1007/s10623-018-0547-5>. Citado na página 29.

POLLARD, J. M. A monte carlo method for factorization. **BIT Numerical Mathematics**, v. 15, n. 3, p. 331–334, Sep 1975. ISSN 1572-9125. Disponível em: <https://doi.org/10.1007/BF01933667>. Citado na página 29.

POLLARD, M. J. Monte carlo methods for index computation $({mod} p)$. In: . [S.l.: s.n.], 1978. Citado na página 29.

QURESHI, C.; PANARIO, D. Rédei Actions on Finite Fields and Multiplication Map in Cyclic Group. **SIAM Journal on Discrete Mathematics**, v. 29, n. 3, p. 1486–1503, jan 2015. ISSN 0895-4801. Disponível em: <http://epubs.siam.org/doi/10.1137/140993338>. Citado na página 27.

SAKZAD, A. et al. Self-inverse interleavers based on permutation functions for turbo codes. In: **2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)**. [S.l.: s.n.], 2010. p. 22–28. Citado na página 28.

SCHWENK, J.; HUBER, K. Public key encryption and digital signatures based on permutation polynomials. **Electronics Letters**, v. 34, n. 8, p. 759–760, April 1998. Citado na página 12.

SHANNON, C. E. Communication theory of secrecy systems. **The Bell System Technical Journal**, v. 28, n. 4, p. 656–715, 1949. Citado na página 46.

SHIHUI, F. et al. A recursive construction of permutation polynomials over $\mathbb{F}_{q^2}$ with odd characteristic from rédei functions. **Designs, Codes and Cryptography**, v. 87, n. 7, p. 1481–1498, Jul 2019. ISSN 1573-7586. Disponível em: <https://doi.org/10.1007/s10623-018-0548-4>. Citado na página 27.

SUNGHAN, B.; BYUNGCHUL, C.; HWANYUP, J. Möbius function in short intervals for function fields. **Finite Fields and Their Applications**, v. 34, p. 235–249, 2015. ISSN 1071-5797. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1071579715000155>. Citado na página 28.

TESKE, E.; HUGH w. C. A note on shanks's chains of primes. In: BOSMA, W. (Ed.). **Algorithmic Number Theory**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000. p. 563–580. ISBN 978-3-540-44994-2. Citado na página 29.

WEI, P.; SHANG, S.; WENZHENG, L. An Improved Cryptanalysis Algorithm for Chebyshev Map-Based Discrete Logarithm Problem. In: WANG, G. et al. (Ed.). **Security, Privacy, and Anonymity in Computation, Communication, and Storage**. Cham: Springer International Publishing, 2021. p. 118–130. ISBN 978-3-030-68851-6. Citado na página 46.

YANBIN, Z.; QIANG, W.; WENHONG, W. On inverses of permutation polynomials of small degree over finite fields. **IEEE Transactions on Information Theory**, v. 66, n. 2, p. 914–922, 2020. Citado na página 12.

YOSHIOKA, D. Periodic properties of Chebyshev polynomial sequences over the residue ring $\mathbb{Z}/2^k\mathbb{Z}$. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 63, n. 8, p. 778–782, August 2016. Citado na página 22.

YOSHIOKA, D. Properties of chebyshev polynomials modulo p^k. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 65, n. 3, p. 386–390, March 2018. Citado na página 21.

YOSHIOKA, D. Properties of Chebyshev polynomials modulo p^k. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 65, n. 3, p. 386–390, March 2018. Citado na página 22.

YOSHIOKA, D. Properties of chebyshev polynomials modulo p^k. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 65, n. 3, p. 386–390, 2018. Citado na página 46.

YOSHIOKA, D. Security of public-key cryptosystems based on chebyshev polynomials over F/p^kF. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 67, n. 10, p. 2204–2208, 2020. Citado na página 46.

APÊNDICE A – TRANSFORMADAS DO COSSENO DOS TIPOS III E IV EM CORPOS DE CARACTERÍSTICA 2

Este apêndice contém uma contribuição secundária desta tese, surgida em meio ao estudo de novos resultados relacionados à trigonometria sobre corpos finitos. Mais especificamente, introduz-se o Lema A.1, que complementa um resultado apresentado em (LIMA; BARONE; CAMPELLO DE SOUZA, 2016). No artigo em questão, são introduzidos quatro tipos de transformadas do cosseno sobre corpos finitos de característica 2; os autores afirmam que a demonstração da invertibilidade de tais transformadas pode ser realizada empregando o Lema 1, introduzido no mesmo trabalho. A definição cosseno em corpos finitos de característica 2 utilizada por Lima difere da definição utilizada neste trabalho e é definida da seguinte maneira,

Definição A.1. *Se um elemento $\zeta \in \mathbb{F}_{2^r}$ tem ordem multiplicativa ord(ζ), a função cosseno em corpo finito relacionado ao ângulo ζ é definido como*

$$\cos_\zeta(n) \coloneqq \zeta^n + \zeta^{-n}, \tag{66}$$

para $n \in \mathbb{Z}$.

O fato é que, para demonstrar a invertibilidade das transformadas dos tipos III e IV (cujas definições são reapresentadas neste apêndice), faz-se necessário o já mencionado Lema A.1, o qual é enunciado a seguir.

Lema A.1. *Se um elemento $\zeta \in \mathbb{F}_{2^r}$ tem ordem multiplicativa $2N-1$, então*

$$A = \sum_{k=1}^{N-1} \cos_\zeta((k+1/2)n) = \begin{cases} 0 & n = t(2N-1), \\ 1 = \cos_\zeta(n/2) & \textit{caso contrário.} \end{cases} \tag{67}$$

Demonstração. Como ζ tem ordem $(2N-1)$, tem-se $\zeta^{kt(2N-1)} = 1$, $t \in \mathbb{N}$, $k = 1, \ldots, N-1$. Para o caso em que $n = t(2N-1)$,

$$\zeta^{(k+1/2)t(2N-1)} + \zeta^{-(k+1/2)t(2N-1)} = 1 + 1 = 0 \pmod 2.$$

Caso contrário, a equação acima pode ser escrita da seguinte forma:

$$A = \zeta^{n/2}\left(\frac{\zeta^n(\zeta^{n(N-2)}-1}{\zeta^n-1}\right) + \zeta^{-n/2}\left(\frac{\zeta^{-n}(\zeta^{-n(N-2)}-1}{\zeta^n-1}\right) \tag{68}$$

$$= \zeta^{n/2}\left(\frac{\zeta^n(\zeta^{n(N-2)}-1}{\zeta^n-1}\right) + \zeta^{-n/2}\left(\frac{1-\zeta^{-n(N-2)}}{\zeta^n-1}\right) \tag{69}$$

$$= \frac{\zeta^{n(N-1/2)} - \zeta^{3n/2} + \zeta^{-n/2} - \zeta^{-n(N-3/2)}}{\zeta^n - 1} \tag{70}$$

$$= \frac{\zeta^n + 1 + \zeta^{-n/2}(\zeta^{2n}+1)}{\zeta^n - 1} \tag{71}$$

$$= 1 + \zeta^{-n/2}(\zeta^n + 1) \tag{72}$$

$$= 1 + \zeta^{n/2} + \zeta^{-n/2} = 1 + \cos_\zeta(n/2). \tag{73}$$

□

Definição A.2. *Seja $\zeta \in \mathbb{F}_{2^r}$ um elemento com ord$(\zeta) = 2N-1$. A transformada do cosseno do tipo III em corpos de caraterística 2 do vetor $\mathbf{x} = (x_i), x_n \in \mathbb{F}_{2^r}$, $i = 0, \ldots, N-1$ é o vetor $\mathbf{X} = (X_k) \in \mathbb{F}_{2^r}$ cujos componentes são definidos como*

$$X_k := \sum_{n=1}^{N-1} x_n \cos_\zeta((k+1/2)n), \tag{74}$$

$k = 0, 1, \ldots, N-1$.

Teorema A.1. *Seja $\zeta \in \mathbb{F}_{2^r}$ um elemento com ord$(\zeta) = 2N-1$. A transformada inversa do cosseno do tipo III em corpos de característica 2 do vetor $\mathbb{X} = (X_k)$, $X_k \in \mathbb{F}_{2^r}$, $k = 0, 1, \ldots, N-1$ é o vetor $\mathbf{x} = (x_n)$, $x_n \in \mathbb{F}_{2^r}$ cujos componentes são definidos como*

$$x_n = \sum_{k=0}^{N-2} X_k \cos_\zeta((k+1/2)n), \tag{75}$$

$n = 0, 1, \ldots, N-2$.

Demonstração. Substituindo a equação 74 na equação 75 (em que substituie-se o índice n por m), obtém-se a expressão

$$\begin{aligned}\hat{x}_m &= \sum_{k=0}^{N-2} \sum_{n=1}^{N-1} X_n \cos_\zeta((k+1/2)n) \cos_\zeta((k+1/2)m) \\ &= \sum_{n=1}^{N-1} X_n \sum_{k=0}^{N-1} \left[\cos_\zeta((k+1/2)(m+n)) + \cos_\zeta((k+1/2)(m-n))\right];\end{aligned}$$

retirando do somatório o caso $k = 0$,

$$\begin{aligned}\hat{x}_m = \sum_{n=1}^{N-1} X_n [\, &\cos_\zeta(1/2(m+n)) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m+n)) + \cos_\zeta(1/2(m-n)) + \\ &\sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m-n))].\end{aligned}$$

Para utilizar o lema A.1 é necessário avaliar o caso em que $m = n$, portanto, segue-se que

$$\begin{aligned}
\hat{x}_m &= x_m \left[\cos_\zeta(m) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)2m) + \cos_\zeta(0) + \sum_{k=1}^{N-2} \cos_\zeta(0) \right] \\
&+ \sum_{\substack{n=1 \\ n\neq m}}^{N-1} [\cos_\zeta((1/2)(m+n)) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m+n)) + \cos_\zeta(1/2(m-n)) \\
&+ \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m-n))] \\
&= x_m[\cos_\zeta(m) + 1 + \cos_\zeta(m) + 0 + 0] \\
&+ \sum_{\substack{n=1 \\ n\neq m}}^{N-1} [\cos_\zeta(\frac{m+n}{2}) + 1 + \cos_\zeta(\frac{m+n}{2}) + \cos_\zeta(\frac{m-n}{2}) + 1 + \cos_\zeta(\frac{m-n}{2})] \\
&= x_m.
\end{aligned}$$

□

Definição A.3. *Seja $\zeta \in \mathbb{F}_{2^r}$ um elemento com ord$(\zeta) = 2N - 1$. A transformada do cosseno do tipo IV em corpos de caraterística 2 do vetor $\mathbf{x} = (x_i)$,$x_n \in \mathbb{F}_{2^r}$ $i = 0, 1, \ldots, N-2$ é o vetor $\mathbf{X} = (X_k) \in \mathbb{F}_{2^r}$ cujos componentes são definidos como*

$$X_k := \sum_{n=0}^{N-2} x_n \cos_\zeta((k+1/2)(n+1/2)), \tag{76}$$

$k = 0, 1, \ldots, N-2$.

Teorema A.2. *Seja $\zeta \in \mathbb{F}_{2^r}$ um elemento com ord$(\zeta) = 2N - 1$. A transformada inversa do cosseno do tipo IV em corpos de característica 2 do vetor $\mathbb{X} = (X_k)$, $X_k \in \mathbb{F}_{2^r}$, $k = 0, 1, \ldots, N-1$ é o vetor $\mathbf{x} = (x_n)$, $x_n \in \mathbb{F}_{2^r}$ cujos componentes são definidos como*

$$x_n = \sum_{k=0}^{N-2} X_k \cos_\zeta((k+1/2)(n+1/2)), \tag{77}$$

$n = 0, 1, \ldots, N-2$.

Demonstração. Substituindo a equação 76 na equação 77 (onde se substitui o índice n por m), obtém-se a expressão

$$\begin{aligned}
\hat{x}_m &= \sum_{k=0}^{N-2} \sum_{n=1}^{N-1} X_n \cos_\zeta((k+1/2)(n+1/2)) \cos_\zeta((k+1/2)(m+1/2)) \\
&= \sum_{n=1}^{N-1} X_n \sum_{k=0}^{N-1} \Big[\cos_\zeta((k+1/2)(m+n+1)) + \cos_\zeta((k+1/2)(m-n)) \Big];
\end{aligned}$$

retirando do somatório o caso $k = 0$,

$$\hat{x}_m = \sum_{n=1}^{N-1} X_n \Big[\cos_\zeta((m+n+1)/2) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m+n+1)) + \cos_\zeta((m-n)/2) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m-n)) \Big].$$

Para utilizar o lema A.1 é necessário avaliar o caso em que $m = n$, portanto, segue-se que

$$\begin{aligned}
\hat{x}_m &= x_m \Big[\cos_\zeta((2m+1)/2) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(2m+1)) + \cos_\zeta(0) + \sum_{k=1}^{N-2} \cos_\zeta(0) \Big] \\
&+ \sum_{\substack{n=1 \\ n\neq m}}^{N-1} x_n \Big[\cos_\zeta((m+n+1)/2) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m+n+1)) \\
&+ \cos_\zeta((m-n)/2) + \sum_{k=1}^{N-2} \cos_\zeta((k+1/2)(m-n)) \Big] \\
&= x_m \Big[\cos_\zeta((2m+1)/2) + 1 + \cos_\zeta((2m+1)/2) + 0 + 0 \Big] \\
&+ \sum_{\substack{n=1 \\ n\neq m}}^{N-1} x_n \Big[\cos_\zeta(\frac{m+n+1}{2}) + 1 + \cos_\zeta(\frac{m+n+1}{2}) + \cos_\zeta(\frac{m-n}{2}) + 1 + \cos_\zeta(\frac{m-n}{2}) \Big] \\
&= x_m.
\end{aligned}$$

□