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

MARCOS ANTONIO ALVES GONDIM

TRANSFORMADA NUMÉRICA MANOBRÁVEL DE FOURIER:

definição e aplicação em cifragem de imagens

Recife

2019

MARCOS ANTONIO ALVES GONDIM

TRANSFORMADA NUMÉRICA MANOBRÁVEL DE FOURIER:

definição e aplicação em cifragem de imagens

Tese submetida 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

2019

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

G637t Gondim, Marcos Antonio Alves.
Transformada numérica manobrável de Fourier: definição e aplicação em cifragem de imagens / Marcos Antonio Alves Gondim. – 2019.
83 folhas, il., gráfs., tabs.

Orientador: Prof. Dr. Juliano Bandeira Lima.

Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2019.
Inclui Referências.

1. Engenharia Elétrica. 2. Transformada discreta manobrável de Fourier. 3. Transformada numérica de Fourier. 4. Transformada numérica manobrável de Fourier. 5. Trigonometria sobre corpos finitos. 6. Cifragem de imagens. I. Lima, Juliano Bandeira. (Orientador). II. Título.

UFPE

621.3 CDD (22. ed.) BCTG/2019-362

MARCOS ANTONIO ALVES GONDIM

TRANSFORMADA NUMÉRICA MANOBRÁVEL DE FOURIER:
definição e aplicação em cifragem de imagens

Tese submetida 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.

Aprovado em: 05 / 07 / 2019 .

BANCA EXAMINADORA

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

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

Prof. Dr. Daniel Pedro Bezerra Chaves (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Gilson Jeronimo da Silva Junior (Examinador Externo)
Universidade de Pernambuco

Prof. Dr. José Rodrigues de Oliveira Neto (Examinador Externo)
Universidade Federal de Pernambuco

Dedico este trabalho ao meu avô João Alves da Silva.

AGRADECIMENTOS

Sou grato primeiramente à Deus por minha vida e por ter me presenteado com o desejo de aprender mais e questionar sempre.

Ao orientador Prof. Juliano Bandeira, pelo exemplo de pessoa, de comprometimento e dedicação, exercendo seu papel de forma admirável e inspiradora. Sou grato também por ter me acolhido no programa de pós-graduação como aluno de dedicação parcial, acreditando no meu comprometimento com a pesquisa e a conciliação com as minhas atividades profissionais.

À minha família, em especial à minha esposa Gemma Gondim, por acreditar em mim mais do que qualquer outra pessoa, pelo companheirismo e pela partilha de uma vida juntos. Agradeço também à minha mãe, Eugenia Alves, pelo amor e dedicação incondicionais.

Sou grato aos professores Ricardo Campello e Hélio Magalhães a quem muito admiro. Aos professores Gilson Jerônimo e Daniel chaves pelas contribuições feitas no momento da qualificação. E aos colegas do Grupo de Pesquisa em Processamento de Sinais, em especial à José de Oliveira Neto.

RESUMO

A contribuição central desta tese é a definição de uma transformada numérica manobrável de Fourier (SFNT, do inglês *steerable Fourier number transform*). A SFNT pode ser vista como uma generalização da transformada numérica de Fourier, sendo obtida pela rotação, empregando funções trigonométricas sobre corpos finitos, de pares de vetores de base específicos desta transformada. O estabelecimento da SFNT preenche uma lacuna importante na teoria das transformadas discretas, pois, até então, as chamadas transformadas manobráveis haviam sido definidas apenas sobre os números reais e complexos. À definição da SFNT encontram-se associados diversos resultados intermediários interessantes e também inéditos, como a proposição e a caracterização de uma função tangente sobre corpos finitos e a introdução de uma versão da transformada numérica de Hilbert diferente da que se encontra documentada na literatura. No que diz respeito à aplicação, esta tese descreve um esquema para cifragem de imagens baseado na SFNT; os fundamentos do referido esquema são (i) a utilização de ângulos de rotação determinados por uma chave-secreta e (ii) a combinação em série entre duas etapas de transformação aplicadas a blocos da imagem e uma etapa de permutação aplicada à imagem completa. Comparações com esquemas no estado-da-arte neste cenário indicam que a técnica proposta provê benefícios relacionados à segurança, complexidade computacional e representação das imagens cifradas.

Palavras-chave: Transformada discreta manobrável de Fourier. Transformada numérica de Fourier. Transformada numérica manobrável de Fourier. Trigonometria sobre corpos finitos. Cifragem de imagens.

ABSTRACT

The central contribution of this thesis is the definition of a steerable Fourier number transform (SFNT). The SFNT can be viewed as a generalization of the Fourier number transform, being obtained by rotating, using finite field trigonometric functions, specific pairs of basis vectors of such a transform. The establishment of the SFNT fulfills an important gap in the theory of discrete transforms, since, until then, the so-called steerable transforms had been defined over real and complex numbers only. Several interesting and also new intermediary results are associated to the definition of the SFNT, such as the proposition and the characterization of a finite field tangent function, and the introduction of a version of the Hilbert number transform different from that archived in the literature. With respect to applications, this thesis describes an image encryption scheme based on the SFNT; the fundamentals of the referred scheme are (i) utilizing rotation angles determined by a secret-key and (ii) combining in a serial manner two block-based image transformation stages and one permutation stage applied to the whole image. Comparisons with state-of-the-art schemes in this scenario indicate that the proposed technique provides benefits related to security, computational complexity and representation of ciphered images.

Keywords: Steerable discrete Fourier transform. Fourier number transform. Steerable Fourier number transform. Trigonometry over finite fields. Image encryption.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

bpp	Bits por pixel
CNT	Transformada numérica do cosseno (Cosine number transform)
DCT	Transformada discreta do cosseno (Discrete cosine transform)
DFT	Transformada discreta de Fourier (Discrete Fourier transform)
DFrFT	Transformada discreta de Fourier fracionária (Discrete fractional Fourier transform)
DSP_G	Processamento digital de sinais sobre grafos (Digital signal processing on graphs)
DSP	Processamento digital de sinais (Digital signal processing)
FFHT	Transformada de Hartley sobre corpos finitos (Finite field Hartley transform)
FFTT	Transformada trigonométrica sobre corpos finitos (Finite field trigonometric transforms)
FNT	Transformada numérica de Fourier (Fourier number transform)
FT	Transformada de Fourier (Fourier transform)
FrFT	Transformada fracionária de Fourier (Fractional Fourier transform)
FrFNT	Transformada numérica fracionária de Fourier (Fractional Fourier number transform)
GFT	Transformada de Fourier sobre grafos (Graph Fourier transform)
HiNT	Transformada numérica de Hilbert (Hilbert number transform)

HNT	Transformada numérica de Hartley (Hartley number transform)
H-SSP	Hyperchaos with selfshrinking perturbance
LSB	Bit menos significativo (Least significant bit)
NPCR	Taxa do número de pixels alterados (Number of pixels change rate)
SDFT	Transformada discreta manobrável de Fourier (Steerable discrete Fourier transform)
SFNT	Transformada numérica manobrável de Fourier (Steerable Fourier number transform)
SNT	Transformada numérica do seno (Sine number transform)
UACI	Média unificada da mudança de intensidade (Unified average changing intensity)

LISTA DE SÍMBOLOS

$\mathbf{F}$	Matriz de transformação da FNT.
$\mathbf{F}_{\alpha,\theta}$	Matriz de transformação da SFNT.
$\mathrm{GI}(p)$	Conjunto dos inteiros Gaussianos módulo p.
$\mathrm{GF}(p)$	Corpo finito com p elementos.
$\mathcal{G}$	Grafo $\mathcal{G}$.
ν	Conjunto de vértices ν de um grafo.
ε	Conjunto de arestas ε de um grafo.
$*$	Conjugado transposto de uma matriz.
$\mathbf{H}$	Matriz da transformada numérica de Hartley.
$\overline{H}$	Entropia normalizada.
L	Matriz Laplaciana de um grafo $\mathcal{G}$.
$\mathbf{R}_\theta$	Matriz de rotação definida a partir de um ângulo θ.
$\boldsymbol{\alpha}$	Vetor contendo todos os elementos em relação aos quais os cossenos e senos em corpos finitos de ângulos de rotação são calculados.
$\boldsymbol{\theta}$	Vetor contendo todos os ângulos empregados nas rotações dos pares de autovetores de $\mathbf{F}$.
$\tilde{\beta}_r$	Função de ponderação empregada na definição de transformadas trigonométricas sobre corpos finitos.
$\tilde{\gamma}_r$	Função de ponderação empregada na definição de transformadas trigonométricas sobre corpos finitos.
Φ	Matriz contendo em suas colunas um conjunto de autovetores do Laplaciano do grafo $\mathcal{G}$.
ζ	Elemento pertencente a $\mathrm{GI}(p)$.
Λ	Matriz diagonal cujos elementos são autovalores da transformada de Fourier.
r_{xy}	Coeficiente de correlação.

$\mathrm{E}(x)$	Esperança.
$\mathrm{var}(x)$	Variância.
$\mathrm{cov}(x, y)$	Covariância.
$\otimes$	Produto de Kronecker.

SUMÁRIO

1 INTRODUÇÃO

As transformadas discretas são ferramentas matemáticas bem difundidas e com várias aplicações importantes, sobretudo na área de processamento digital de sinais (OPPENHEIM; SCHAFER; BUCK, 2010). Dentre essas ferramentas, a mais conhecida é a transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*), a qual possui diversas propriedades já muito bem caracterizadas e aplicabilidade consolidada em diversos cenários práticos. Transformadas discretas do cosseno, do seno e de Hartley, por exemplo, também foram definidas, tendo sido investigadas e utilizadas há várias décadas em diferentes contextos (AHMED; NATARAJAN; RAO, 1974; RAO; YIP, 1990; BRACEWELL, 1983; MARTUCCI, 1994).

Usualmente, transformadas como as mencionadas são definidas sobre os números reais ou complexos, mapeando uma estrutura discreta (um vetor de comprimento finito que representa um sinal de tempo discreto ou uma matriz que representa uma imagem digital, por exemplo), cujos elementos se encontram sobre esses corpos infinitos noutra estrutura com as mesmas dimensões no chamado domínio da transformada. O fato é que transformadas discretas também podem ser definidas sobre estruturas algébricas finitas e, em particular, sobre corpos finitos. No campo do processamento digital de sinais, essa possibilidade tem sido considerada desde a década de 1970, quando se introduziu a transformada de Fourier sobre corpos finitos (POLLARD, 1971). Uma série de variantes dessa transformada foi apresentada desde então, o que viabilizou, inclusive, aplicações às quais as transformadas correspondentes definidas sobre os reais não se adequariam. Dentre as aplicações das transformadas sobre corpos finitos, podem ser mencionadas (i) a caracterização de códigos corretores de erro e o projeto de algoritmos para decodificação nesse contexto (BLAHUT, 1983; BLAHUT, 1979; FEKRI et al., 2005) (ii) o cálculo eficiente de convoluções lineares, evitando erros de truncamento e uso de aritmética de ponto flutuante (LIMA, 2015; TOIVONEN; HEIKKILÄ, 2006; RUBANOV et al., 1998; LI, 1990; SHU; TIANREN, 1988) (iii) o processamento de sinais no domínio cifrado (PEDROUZO-ULLOA; TRONCOSO-PASTORIZA; PÉREZ-GONZÁLEZ, 2017), (iv) a inserção / extração de marcas d'água em imagens digitais (TAMORI; AOKI; YAMAMOTO, 2002; CINTRA et al., 2009), (v) a cifragem de imagens digitais (LIMA; MADEIRO; SALES, 2015; LIMA; NOVAES, 2014) e (vi) o projeto de sequências multinível para espalhamento espectral (OLIVEIRA; CAMPELLO DE SOUZA; KAUFFMAN, 1999; OLIVEIRA; CAMPELLO DE SOUZA, 2000; LIMA; CAMPELLO DE SOUZA; PANARIO, 2011; LIMA; CAMPELLO DE SOUZA; PANARIO, 2008).

Além da transformada de Fourier, têm sido definidas sobre corpos finitos transformadas do cosseno, do seno, de Hartley, wavelet, bem como versões fracionárias de algumas dessas ferramentas (CAMPELLO DE SOUZA; OLIVEIRA, 2000; CAMPELLO DE SOUZA et al., 2004; LIMA; SOUZA, 2011; LIMA; CAMPELLO DE SOUZA, 2010; FEKRI et al., 2006; FEKRI; MERSEREAU; SCHAFER, 1999; LIMA; SOUZA, 2013). Quando o mapeamento

induzido por uma dessas transformadas lida apenas com elementos num corpo finito primo (ou corpo finito base, fazendo um contraponto ao que seria um corpo de extensão), ela recebe o nome de transformada numérica (DIMITROV; COOKLEV; DONEVSKY, 1995; CAMPELLO DE SOUZA; OLIVEIRA; PALMA, 2001).

1.1 MOTIVAÇÃO

Uma das motivações para definição de novas transformadas sobre corpos finitos é a possibilidade de preencher lacunas teóricas, acompanhando a proposição de novas transformadas definidas sobre os números reais ou complexos e realizando paralelos relacionados às propriedades e à aplicabilidade dessas ferramentas. Diante disso, observou-se que, em trabalhos recentes, têm sido propostas transformadas discretas que podem ser classificadas, empregando uma terminologia geral, como direcionáveis (ZENG; FU, 2008; XU; ZENG; WU, 2010; CHANG; GIROD, 2008; COHEN et al., 2010). Tais transformadas recorrem a alguma estratégia que permite que estas sejam orientadas e melhor se adéquem ao sinal que se deseja processar. No caso, por exemplo, em que se aplique uma transformada discreta do cosseno (DCT, do inglês *discrete cosine transform*) a um bloco de imagem digital com a finalidade de realizar compressão, a possibilidade de direcionamento permite que a transformada seja "realinhada" e acompanhe as descontinuidades contidas no bloco em questão, proporcionando maior compactação de energia (FRACASTORO; FOSSON; MAGLI, 2017).

No cenário das transformadas direcionáveis recém-introduzidas, merece destaque a transformada discreta manobrável de Fourier (SDFT, do inglês *steerable discrete Fourier transform*) (FRACASTORO; MAGLI, 2017), a qual possui relação com a transformada de Fourier sobre grafos (GFT, do inglês *graph Fourier transform*) (SHUMAN et al., 2013; SANDRYHAILA; MOURA, 2013c; SHUMAN; RICAUD; VANDERGHEYNST, 2012; SARDELLITTI; BARBAROSSA; LORENZO, 2017; DERI; MOURA, 2017; SHUMAN; FARAJI; VANDERGHEYNST, 2016). A GFT é uma transformada discreta para sinais sobre grafos arbitrários; dependendo do grafo que se considere, a GFT coincide com uma transformada discreta para sinais sobre domínios regulares (um sinal de tempo discreto ou uma imagem digital), como é o caso da DFT ou o da DCT. De modo mais específico, para definição da SDFT, é construída uma nova base a partir da rotação de pares de vetores de base da DFT (linhas da matriz da DFT). Cada um desses pares é formado por vetores de base da DFT que se encontram associados ao mesmo autovalor do Laplaciano de um grafo em ciclo com N vértices, com o qual se pode relacionar o domínio dos sinais de tempo discreto com N pontos (FRACASTORO; MAGLI, 2017).

Estimulada pelo cenário acima delineado, esta tese apresenta como proposta central a definição de uma transformada manobrável de Fourier sobre corpos finitos, a qual é identificada como transformada numérica manobrável de Fourier (SFNT, do inglês *steerable Fourier number transform*). As principais motivações para realização deste trabalho são a existência de lacunas teóricas relacionadas ao tema em questão e que podem ser preenchidas com a definição que

Tabela 1 – Algumas das principais transformadas discretas e sobre corpos finitos propostas na literatura.

Transformada	Reais ou Complexos	Corpo Finito
Fourier	(COOLEY; LEWIS; WELCH, 1969)	(POLLARD, 1971)
Fracionária de Fourier	(CANDAN; KUTAY; OZAKTAS, 2000)	(LIMA; CAMPELLO DE SOUZA, 2010)
Manobrável de Fourier	(FRACASTORO; MAGLI, 2017)	Esta tese
Cosseno	(AHMED; NATARAJAN; RAO, 1974)	(CAMPELLO DE SOUZA et al., 2004)
Manobrável do Cosseno	(FRACASTORO; FOSSON; MAGLI, 2017)	–
Seno	(MARTUCCI, 1994)	(CAMPELLO DE SOUZA et al., 2005)
Hartley	(BRACEWELL, 1983)	(CAMPELLO DE SOUZA et al., 1998)

Fonte: O Autor, 2019.

se pretende realizar, e a possibilidade de se introduzir novos métodos, baseados na SFNT, em áreas como segurança da informação e comunicação. Para que o leitor possa se situar melhor com respeito a isso, a Tabela 1 apresenta uma visão condensada de algumas das principais transformadas discretas e sobre corpos finitos até então propostas na literatura. As referências indicadas na tabela são exemplos de trabalhos em que as respectivas transformadas podem ser encontradas, não representando, necessariamente, o trabalho em que elas foram originalmente definidas.

1.2 OBJETIVOS

O objetivo geral deste trabalho é definir uma transformada numérica manobrável de Fourier, estabelecida sobre corpos finitos, a qual represente, pela metodologia empregada em sua construção, uma versão análoga à transformada discreta manobrável de Fourier estabelecida sobre os números complexos. Neste sentido, os seguintes objetivos específicos podem ser elencados:

- Investigar os fundamentos da trigonometria e das transformadas sobre corpos finitos, avaliando a possibilidade e/ou necessidade de introdução de novos conceitos visando à definição ou aplicação da SFNT;
- Introduzir uma transformada numérica de Fourier manobrável (tanto para o caso unidimensional quanto para o bidimensional), a qual apresente analogia com a SDFT, e caracterizar esta ferramenta com relação aos seus principais aspectos;
- Explorar as possibilidades de desdobramentos da definição da SFNT que levem à definição de novas ferramentas no cenário das transformadas numéricas;
- Propor um esquema para cifragem de imagens baseado na SFNT, avaliar suas propriedades e compará-lo a outros esquemas em relação a aspectos como segurança e complexidade.

1.3 ESTRUTURA DA TESE E CONTRIBUIÇÕES

Esta tese está organizada da seguinte forma:

- No Capítulo 1, é feita uma introdução ao tema central do trabalho, sendo apresentados os principais motivos para o seu desenvolvimento, bem como seus objetivos, contribuições e estrutura de capítulos.

- No Capítulo 2, é apresentada uma breve revisão sobre conceitos básicos da Teoria dos Grafos. Tal revisão fornece ao leitor suporte para entendimento da definição da transformada de Fourier sobre grafos e da transformada discreta manobrável de Fourier (FRACASTORO; MAGLI, 2017), apresentadas no mesmo capítulo.

- No capítulo 3, são apresentados os principais resultados relacionados à trigonometria sobre corpos finitos e às transformadas numéricas[1]. Embora a maior parte do material deste capítulo seja de revisão, a primeira contribuição original desta tese é apresentada[2]: (i) a definição de uma função tangente sobre corpos finitos. São estudadas algumas propriedades dessa função, as quais têm relação com a aplicação da transformada numérica manobrável de Fourier descrita no capítulo seguinte, e desenvolvidos alguns exemplos. (ii) Além disso, é apresentada uma nova proposição relacionada às simetrias da transformada numérica de Fourier, quando esta emprega como núcleo um inteiro Gaussiano sobre um corpo finito; essa proposição tem papel importante na relação entre a SFNT e a transformada numérica de Hilbert.

- No Capítulo 4, apresenta-se a contribuição principal deste trabalho: (iii) a definição da transformada numérica manobrável de Fourier; são discutidos os resultados intermediários necessários a tal definição, como a determinação dos autovalores do Laplaciano do grafo em ciclo (caso unidimensional) e do Laplaciano do grafo toroidal (caso bidimensional), bem como suas multiplicidades. Por meio de exemplos, ilustra-se a construção da SFNT e de sua versão bidimensional. Apresenta-se, no contexto de corpos finitos, o conceito de ângulo de rotação ótimo. (iv) Propõe-se uma definição para a transformada numérica de Hilbert diferente da que se encontra documentada na literatura e discute-se uma maneira de chegar a tal definição empregando a SFNT.

- No Capítulo 5, é discutida a aplicação da SFNT em Criptografia. (v) Precisamente, o que se faz é descrever um esquema para cifragem de imagens digitais que combina dois

[1] Deste ponto em diante, as transformadas sobre corpos finitos são quase sempre identificadas como transformadas numéricas, uma vez que, nesta tese, não são consideradas transformadas sobre extensões arbitrárias de corpos finitos; apenas transformadas envolvendo vetores e matrizes cujos elementos se encontram em corpos finitos primos ou em conjuntos de inteiros Gaussianos sobre corpos finitos primos são consideradas. Nesses casos, não se faz necessário empregar uma aritmética módulo um polinômio, mas apenas uma aritmética módulo um número primo ou uma aritmética que "imita" a aritmética dos números complexos avaliados módulo um número primo.

[2] Ao longo desta seção, as principais contribuições originais desta tese são indicadas por meio de uma numeração em algarismos romanos.

blocos em que se aplica a 2D-SFNT e um bloco que permuta os pixels da imagem. Por meio de experimentos computacionais e do cálculo de métricas comumente empregadas na literatura, verifica-se que o esquema proposto preenche requisitos de robustez contra os principais ataques criptográficos. Além disso, conduz-se uma discussão que sugere que o esquema também é seguro com respeito a ataques criptográficos clássicos e realiza-se uma comparação com outros esquemas recentemente propostos na literatura; ao passo em que se mantém seguro, o método de cifragem proposto pode ser menos complexo que outras técnicas, em termos de operações aritméticas necessárias à sua implementação, e facilita a representação das imagens cifradas.

- No Capítulo 6, são apresentadas as considerações conclusivas desta tese, indicadas direções para a realização de pesquisas futuras e listado o artigo científico resultante do desenvolvimento deste trabalho.

2 TRANSFORMADA DISCRETA MANOBRÁVEL DE FOURIER

Neste capítulo, são revisados alguns dos principais conceitos relacionados à Teoria dos Grafos. Esses conceitos são, então, utilizados na apresentação da transformada de Fourier sobre grafos (GFT, do inglês *graph Fourier transform*), uma ferramenta central no recém-introduzido Processamento Digital de Sinais sobre grafos (DSP$_G$, do inglês *digital signal processing on graphs*) (ORTEGA et al., 2018; SANDRYHAILA; MOURA, 2013b; SANDRYHAILA; MOURA, 2014c; SANDRYHAILA; MOURA, 2014a; SANDRYHAILA; MOURA, 2013c; SHUMAN et al., 2013; GIRAULT; GONCALVES; FLEURY, 2015; FRACASTORO; MAGLI, 2017). Considera-se, em particular, a GFT associada a um grafo em ciclo, a qual coincide com a transformada discreta de Fourier ordinária (DFT). Tal observação é empregada na definição da transformada discreta manobrável de Fourier (SDFT, do inglês *steerable discrete Fourier transform*), a qual é descrita na parte final deste capítulo.

No que segue, a transformada discreta de Fourier unitária de um vetor $\mathbf{x} = (x(n))$, $x(n) \in \mathbb{C}$, $n = 0, 1, \ldots, N-1$, é o vetor $\mathbf{X} = (X(k))$, $X(k) \in \mathbb{C}$, $k = 0, 1, \ldots, N-1$, com componentes dadas por

$$X(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n) \omega_N^{kn},$$

em que $\omega_N = e^{-i\frac{2\pi}{N}}$. Matricialmente, a DFT de $\mathbf{x}$ pode ser expressa por

$$\mathbf{X} = \mathbf{F}\mathbf{x},$$

em que a matriz de transformação $\mathbf{F}$ possui componentes na k-ésima linha e n-ésima coluna

$$F(k, n) = \frac{1}{\sqrt{N}} \omega_N^{kn},$$

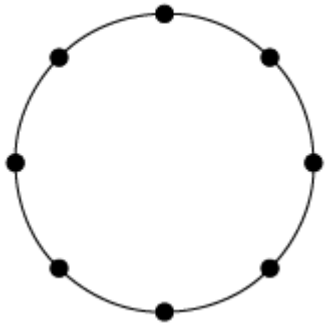
$k, n = 0, 1, \ldots, N-1$.

2.1 DEFINIÇÕES BÁSICAS SOBRE GRAFOS

Um grafo é denotado por $\mathcal{G} = (\nu, \varepsilon)$, em que ν é um conjunto de vértices (ou nós) com $|\nu| = N$ e $\varepsilon \subset \nu \times \nu$ é um conjunto de arestas, conforme ilustrado pela Figura 1. A matriz de adjacência $A(\mathcal{G}) \in \mathbb{R}^{N \times N}$ de um grafo é tal que $A(\mathcal{G})_{ij} = 1$, se houver uma aresta entre os nós i e j; caso contrário, $A(\mathcal{G})_{ij} = 0$. A matriz de grau $D(\mathcal{G})$ é uma matriz diagonal cujo elemento na i-ésima posição é igual ao número de arestas incidentes no vértice i. A matriz Laplaciana de um grafo é definida por $L(\mathcal{G}) = D(\mathcal{G}) - A(\mathcal{G})$. Como $L(\mathcal{G})$ é uma matriz real e simétrica (admitindo que o respectivo grafo é não-direcionado), ela será diagonalizada por uma matriz ortogonal, de maneira que se pode escrever

$$L(\mathcal{G}) = \Phi \Lambda \Phi^{\mathrm{H}}, \tag{2.1}$$

Figura 1 – Grafo em ciclo $\mathcal{C}_8$



Fonte: O Autor, 2019.

em que $\Phi \in \mathbb{R}^{N \times N}$ é uma matriz contendo em suas colunas um conjunto de autovetores de $L(\mathcal{G})$, Λ é uma matriz diagonal contendo os respectivos autovalores e H denota o transposto Hermitiano.

Um sinal $\mathbf{x} \in \mathbb{R}^N$ sobre um grafo pode ser interpretado como estando no *domínio dos vértices*, correspondendo a uma função real e definida nos nós do grafo $\mathcal{G}$, de modo que x_i, $i = 1, 2, \ldots, N$, é o valor do sinal sobre o nó $i \in \varepsilon$. A partir dos autovetores de $L(\mathcal{G})$, define-se a transformada de Fourier $\hat{\mathbf{x}} \in \mathbb{R}^N$ de um sinal $\mathbf{x} \in \mathbb{R}^N$ sobre um grafo como (FRACASTORO; MAGLI, 2017; ORTEGA et al., 2018)

$$\hat{\mathbf{x}} = \Phi^H \mathbf{x}. \tag{2.2}$$

A GFT inversa é calculada por

$$\mathbf{x} = \Phi \hat{\mathbf{x}}. \tag{2.3}$$

Há abordagens para definição da GFT diferentes daquela apresentada nas últimas equações; o que muda, fundamentalmente, é a matriz associada ao grafo que se emprega na expansão espectral dada em (2.1). É possível utilizar, em vez da matriz Laplaciana, a própria matriz de adjacência, conforme apresentado em (SANDRYHAILA; MOURA, 2014b). De qualquer forma, essa ferramenta, que corresponde a uma generalização da DFT ordinária, tem desempenhado um papel de grande relevância no contexto do DSP$_G$, sendo empregada na descrição de técnicas de filtragem, de amostragem e de análise espectral no cenário mencionado (ORTEGA et al., 2018).

2.2 A GFT PARA GRAFOS EM CICLO

Um caso particularmente interessante para definição da GFT é aquele em que se considera um grafo em ciclo não-direcionado e com N vértices, o qual é denotado por $\mathcal{C}_N$.

Um exemplo deste tipo de grafo, com 8 vértices e denotado por $\mathcal{C}_8$, tem sua estrutura exibida na Figura 1.

A matriz de adjacência deste tipo de grafo e, consequentemente, sua matriz Laplaciana, que é dada por

$$L(\mathcal{C}_N) = \begin{bmatrix} 2 & -1 & \cdots & 0 & -1 \\ -1 & 2 & -1 & \cdots & 0 \\ \vdots & -1 & 2 & \cdots & \vdots \\ 0 & \dots & \dots & \ddots & -1 \\ -1 & 0 & \dots & -1 & 2 \end{bmatrix}, \tag{2.4}$$

são casos particulares de matrizes circulantes. Essas últimas são bem conhecidas no contexto de processamento digital de sinais (SHUMAN; FARAJI; VANDERGHEYNST, 2016), sendo empregadas na descriçao de operações fundamentais como filtragem e reconstrução de sinais (SANDRYHAILA; MOURA, 2013a; EKAMBARAM; FANTI; AYAZIFAR, 2013).

Mais precisamente, uma matriz circulante $\mathbf{C}$ é construída a partir de um vetor

$$\mathbf{c} = [c_0 \quad c_1 \ \cdots \ c_{N-2} \quad c_{N-1}]$$

que aparece em sua primeira coluna. As colunas seguintes da matriz correspondem à primeira coluna sucessiva e ciclicamente deslocada para baixo, resultando em

$$\mathbf{C} = \begin{bmatrix} c_0 & c_{N-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{N-1} & \cdots & c_2 \\ \vdots & c_1 & c_0 & \cdots & \vdots \\ c_{N-2} & \dots & \dots & \ddots & c_{N-1} \\ c_{N-1} & c_{N-2} & \dots & c_1 & c_0 \end{bmatrix}. \tag{2.5}$$

Um resultado bastante conhecido do DSP clássico é que as linhas da matriz $\mathbf{F}$ da DFT com dimensões $N \times N$, as quais são dadas por

$$\mathbf{v}^k = \frac{1}{\sqrt{N}}[1 \ \ \omega_k \quad \omega_k^2 \ \dots \ \omega_k^{N-1}], \qquad k = 0, 1, \dots, N-1,$$

em que

$$\omega_k{}^n = e^{-i\frac{2\pi}{N}kn},$$

formam uma base ortogonal de autovetores de qualquer matriz circulante com as mesmas dimensões (FRACASTORO; MAGLI, 2017). Este fato, que decorre da propriedade de convolução cíclica da DFT (OPPENHEIM; SCHAFER; BUCK, 2010), permite expressar a matriz circulante $\mathbf{C}$ como

$$\mathbf{C} = \mathbf{F}\mathbf{\Lambda}\mathbf{F}^H, \tag{2.6}$$

em que $\mathbf{F}$ é a matriz com $\mathbf{v}^k$ e $k = 0, 1, \dots, N-1$, em sua k-ésima linha e Λ é uma matriz diagonal contendo os respectivos autovalores.

Assim, as linhas da matriz da DFT compõem uma base de autovetores válida para definição da GFT de um grafo $\mathcal{C}_N$. Os autovalores λ_k, $k = 0, 1, \ldots, N-1$, de $\mathbf{C}$, dispostos ao longo da diagonal de $\mathbf{\Lambda}$, podem ser obtidos por

$$\mathbf{\Lambda} = \mathbf{F}^H \mathbf{C} \mathbf{F}. \tag{2.7}$$

Da última equação, λ_k é calculado por

$$\lambda_k = \sum_{n=0}^{N-1} c_{N-n} \omega_k^n = c_0 + c_{N-1}\omega_k + \cdots + c_1 \omega_k^{N-1}. \tag{2.8}$$

Fazendo $\mathbf{C} = L(\mathcal{C}_N)$, tem-se $c_j = 0$, $j = 2, 3, \ldots, N-2$, e, portanto, a última equação se desenvolve como

$$\lambda_k = 2 - e^{i\frac{2\pi}{N}k} - e^{-i\frac{2\pi}{N}k}$$
$$\lambda_k = 2 - 2\cos\frac{2k\pi}{N}.$$

Os autovalores λ_k de $\mathbf{C} = L(\mathcal{C}_N)$ são tais que

$$\lambda_k = \lambda_{N-k}, \tag{2.9}$$

$k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$. Se N for par, λ_0 e $\lambda_{\frac{N}{2}}$ terão multiplicidade algébrica 1 e os outros autovalores terão multiplicidade algébrica 2. Como os autovetores de $L(\mathcal{C}_N)$ são ortogonais, a multiplicidade geométrica de cada autovalor será igual à respectiva multiplicidade algébrica; equivalentemente, a dimensão do autoespaço associado a cada autovalor λ_k, $k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$, será igual a 2 e os vetores de base da DFT não serão a única base de autovetores de $L(\mathcal{C}_N)$.

2.3 A TRANSFORMADA DISCRETA MANOBRÁVEL DE FOURIER

Nesta seção, é revisada a definição da transformada discreta de Fourier manobrável (SDFT, do inglês *steerable discrete Fourier transform*) (FRACASTORO; MAGLI, 2017). Para tanto, é enunciado o corolário a seguir, o qual consolida o principal resultado apresentado na última seção.

Corolário 2.1. *A transformada discreta de Fourier pode ser utilizada para o cálculo da GFT de um grafo em ciclo; todavia, as linhas da matriz da DFT não compõem o único conjunto de autovetores possível para a construção de* Φ^H.

Para cada autovalor λ_k, $k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$, há dois autovetores associados $\mathbf{v}^{(k)}$ e $\mathbf{v}^{(N-k)}$ que, sendo rotacionados por um ângulo θ_k, resultam em dois novos autovetores $\mathbf{v}^{(k)'}$ e $\mathbf{v}^{(N-k)'}$. Mais precisamente, tem-se

$$\begin{bmatrix} \mathbf{v}^{(k)'} \\ \mathbf{v}^{(N-k)'} \end{bmatrix} = \begin{bmatrix} \cos\theta_k & \operatorname{sen}\theta_k \\ -\operatorname{sen}\theta_k & \cos\theta_k \end{bmatrix} \cdot \begin{bmatrix} \mathbf{v}^{(k)} \\ \mathbf{v}^{(N-k)} \end{bmatrix}, \tag{2.10}$$

em que θ_k é um ângulo de rotação no intervalo $[0, 2\pi]$. Substituindo, em $\mathbf{F}$, os autovetores originais por suas respectivas versões rotacionadas, obtém-se uma nova matriz de transformação, a qual é denotada por $\mathbf{F}_{\boldsymbol{\theta}}$, em que $\boldsymbol{\theta} = [\theta_1 \ \theta_2 \ \ldots \ \theta_m] \in \mathbb{R}^m$, com $m = \lceil \frac{N}{2} \rceil - 1$, denota o vetor contendo todos os ângulos usados para rotacionar os pares de autovetores. À referida matriz de transformação está associada a transformada discreta de Fourier manobrável, a qual assume diferentes versões à medida em que cada ângulo θ_k em $\boldsymbol{\theta}$ é ajustado.

Assim, pode-se escrever a matriz de transformação da SDFT como

$$\mathbf{F}_{\boldsymbol{\theta}} = \mathbf{R}_{\boldsymbol{\theta}}\mathbf{F}, \tag{2.11}$$

em que $\mathbf{R}_{\boldsymbol{\theta}} \in \mathbb{R}^{N \times N}$ é uma matriz contendo os elementos de todas as matrizes de rotação convenientemente organizados; além disso, tem-se $\mathbf{F}_{\mathbf{0}} = \mathbf{F}$, em que $\mathbf{0}$ denota o vetor nulo com comprimento m. A SDFT de um vetor $\mathbf{x}$, para um conjunto de ângulos de rotação especificados no vetor $\boldsymbol{\theta}$, é então dada por

$$\mathbf{X}_{\boldsymbol{\theta}} = \mathbf{F}_{\boldsymbol{\theta}}\mathbf{x} = \mathbf{R}_{\boldsymbol{\theta}}\mathbf{F}\mathbf{x} = \mathbf{R}_{\boldsymbol{\theta}}\mathbf{X}. \tag{2.12}$$

A última equação indica que $\mathbf{X}_{\boldsymbol{\theta}}$ pode ser obtido calculando-se, inicialmente, $\mathbf{X}$, a DFT de $\mathbf{x}$, e, em seguida, multiplicando o resultado pela matriz de rotações $\mathbf{R}_{\boldsymbol{\theta}}$.

2.4 TRANSFORMADA DISCRETA MANOBRÁVEL DE FOURIER BIDIMENSIONAL

As componentes de $\mathbf{X} = (X(k,l))$, $X(k,l) \in \mathbb{C}$, $k = 0, 1, \ldots, N_1 - 1$, $l = 0, 1, \ldots, N_2 - 1$, são computadas pela DFT bidimensional (2D-DFT) de um sinal $\mathbf{x} = (x(m,n))$, $x(m,n) \in \mathbb{C}$, $m = 0, 1, \ldots, N_1 - 1$, $n = 0, 1, \ldots, N_2 - 1$ e podem ser obtidas por meio da expressão

$$X(k,l) = \frac{1}{\sqrt{N_1 N_2}} \sum_{m=0}^{N_1-1} \sum_{n=0}^{N_2-1} x(m,n) e^{-i2\pi\left(\frac{km}{N_1} + \frac{ln}{N_2}\right)}. \tag{2.13}$$

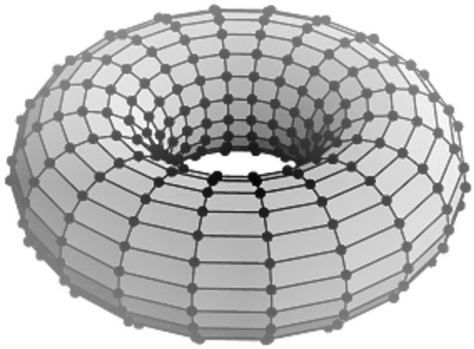
Matricialmente, em função da separabilidade do núcleo da transformada, o cálculo 2D-DFT de $\mathbf{x}$ pode ser expresso como

$$\mathbf{X} = \mathbf{F}_1 \mathbf{x} \mathbf{F}_2^T, \tag{2.14}$$

em que $\mathbf{F}_1$ e $\mathbf{F}_2$ denotam, respectivamente, as matrizes da (1D-)DFT com dimensões $N_1 \times N_1$ e $N_2 \times N_2$.

Em (FRACASTORO; MAGLI, 2017), mostra-se que os vetores de base da 2D-DFT constituem uma possível autobase do Laplaciano de um grafo toroidal (vide Figura 2). De maneira geral, um grafo toroidal $\mathcal{T}_{N_1 N_2}$, com $|\nu| = N_1 N_2$, pode ser visto como o resultado do produto de grafos $\mathcal{C}_{N_1} \times \mathcal{C}_{N_2}$, em que $\mathcal{C}_{N_i}$ é um grafo em ciclo com N_i vértices. Fazendo $N_1 = N_2 = N$, pode-se, de modo similar ao caso unidimensional, denotar por $\mathbf{v}^{(r)}$, $r = 0, 1, \ldots, N - 1$, os autovetores de $\mathcal{C}_N$, e por λ_r os respectivos autovalores. Assim, os autovalores de $L(\mathcal{T}_{NN})$, o Laplaciano de $\mathcal{T}_{NN}$, são expressos por $\mu_{r,s} = \mu_{s,r} = \lambda_r + \lambda_s$; os respectivos autovetores são dados

Figura 2 – Grafo toroidal $\mathcal{T}_{20,20}$.



Fonte: O Autor, 2019.

por $\mathbf{u}^{(r,s)} = \mathbf{v}^{(r)} \otimes \mathbf{v}^{(r)}$, em que o símbolo $\otimes$ denota o produto de Kronecker entre os operandos, isto é, a componente na posição (m, n) de $\mathbf{u}^{(r,s)}$ é calculada por $u^{(r,s)}(m, n) = v^{(r)}(m)v^{(s)}(n)$, $m, n = 0, 1, \ldots, N-1$ (FRACASTORO; MAGLI, 2017).

As multiplicidades dos autovalores $\mu_{r,s}$ se enquadram, então, nos seguintes casos:

- Os autovalores $\mu_{r,s}$, $r, s = 1, 2, \ldots, N/2 - 1$, $r \neq s$, têm multiplicidade 8, uma vez que $\mu_{r,s} = \mu_{s,r} = \mu_{r,N-s} = \mu_{N-s,r} = \mu_{s,N-r} = \mu_{N-r,s} = \mu_{N-r,N-s} = \mu_{N-s,N-r}$;
- Os autovalores $\mu_{r,r}$, $r = 1, 2, \ldots, N/2 - 1$, têm multiplicidade 4 uma vez que $\mu_{r,r} = \mu_{r,N-r} = \mu_{N-r,sr} = \mu_{N-r,N-r}$;
- Os autovalores $\mu_{r,s}$, $r = 0, N/2$ e $s = 1, 2, \ldots, N/2 - 1$ (ou $r = 1, 2, \ldots, N/2 - 1$ e $s = 0, N/2$), têm multiplicidade 4 uma vez que $\mu_{r,s} = \mu_{s,r} = \mu_{r,N-s} = \mu_{N-s,r}$ ($\mu_{r,s} = \mu_{s,r} = \mu_{N-r,s} = \mu_{s,N-r}$);
- Os autovalores $\mu_{0,N/2} = \mu_{N/2,0}$ têm multiplicidade 2;
- Os autovalores $\mu_{0,0}$ e $\mu_{N/2,N/2}$ têm multiplicidade 1.

Consideram-se pares de autovalores da forma $\mu_{r,s}$ e $\mu_{s,r}$ $(r \neq s)$ e seus respectivos autovetores $\mathbf{u}^{(r,s)}$ e $\mathbf{u}^{(s,r)}$, que são vetores de base específicos da 2D-DFT com dimensão $N \times N$. A cada um desses pares de autovetores, é aplicada uma rotação a fim de obter um novo par de autovetores no mesmo autoespaço. Se as componentes dos autovetores $\mathbf{u}^{(r,s)}$ e $\mathbf{u}^{(s,r)}$ forem dispostas de forma unidimensional, como vetores-linha com dimensão $1 \times N^2$, o respectivo novo par de autovetores $\mathbf{u}^{(r,s)'}$ e $\mathbf{u}^{(s,r)'}$ é calculado por

$$\begin{bmatrix} \mathbf{u}^{(r,s)'} \\ \mathbf{u}^{(s,r)'} \end{bmatrix} = \begin{bmatrix} \cos(\theta_{r,s}) & \text{sen}(\theta_{r,s}) \\ -\text{sen}(\theta_{r,s}) & \cos(\theta_{r,s}) \end{bmatrix} \begin{bmatrix} \mathbf{u}^{(r,s)} \\ \mathbf{u}^{(s,r)} \end{bmatrix}. \tag{2.15}$$

em que $\theta_{r,s}$ é um ângulo com valor no intervalo $[0, 2\pi]$.

Substituindo os pares originais de autovetores por aqueles resultantes das rotações, obtém-se uma nova base, à qual está associada a transformada discreta manobrável de Fourier bidimensional (os autovetores associados aos autovalores com multiplicidades iguais a 1 e aqueles identificados pelo par de índices r, s, $r = s$, não são alterados). Convertendo uma matriz $\mathbf{X}$, com dimensões $N \times N$ e cuja 2D-SDFT se queira calcular, numa estrutura unidimensional com dimensões $N^2 \times 1$, o cálculo da referida transformada pode ser expresso matricialmente de modo semelhante ao apresentado em (2.11) e (2.12); neste caso, o vetor $\boldsymbol{\theta}$ de ângulos de rotação será formado por $N(N-1)/2$ componentes (não sofrem rotações os vetores de base indexados por $r = s$) e a matriz de rotação $\mathbf{R}_{\boldsymbol{\theta}}$ possuirá dimensões $N^2 \times N^2$. Mais especificamente, o cálculo de $\mathbf{X}_{\boldsymbol{\theta}} = (X_{\boldsymbol{\theta}}(r,s))$, $r, s = 0, 1, \ldots, N-1$, pode ser feito utilizando (2.14) para, inicialmente, calcular $\mathbf{X}$, a 2D-DFT de $\mathbf{x}$, e, em seguida, multiplicando o resultado pela matriz de rotações $\mathbf{R}_{\boldsymbol{\theta}}$, de modo que se tenha

$$\begin{bmatrix} X_{\boldsymbol{\theta}}(r,s) \\ X_{\boldsymbol{\theta}}(s,r) \end{bmatrix} = \begin{bmatrix} \cos(\theta_{r,s}) & \operatorname{sen}(\theta_{r,s}) \\ -\operatorname{sen}(\theta_{r,s}) & \cos(\theta_{r,s}) \end{bmatrix} \begin{bmatrix} X(r,s) \\ X(s,r) \end{bmatrix}. \tag{2.16}$$

Os autores de (FRACASTORO; MAGLI, 2017) discutem de forma bastante preliminar algumas possíveis aplicações da SDFT; a transformada pode ser usada para filtrar a componente par ou a componente ímpar de um sinal, o que pode ser útil na representação de sinais (GNUTTI; GUERRINI; LEONARDI, 2015). Além disso, empregando a SDFT, pode-se calcular a transformada de Hilbert, a qual permite calcular a fase local e a amplitude de um sinal. Tais cálculos, por sua vez, possuem aplicação em detecção de *edges* e extração de características em imagens (KOVESI, 1999; CARNEIRO; JEPSON, 2002). Por fim, os autores sugerem que a SDFT pode ser aplicada em criptografia (BIANCHI; BIOGLIO; MAGLI, 2016; ZHANG et al., 2016).

3 TRIGONOMETRIA EM CORPOS FINITOS E TRANSFORMADAS NUMÉRICAS

Neste capítulo, são apresentadas as principais definições relacionadas à trigonometria em corpos finitos. Embora a maior parte deste conteúdo seja revisivo, ele conta com pelo menos uma contribuição original: a definição da função tangente sobre corpos finitos e de sua inversa; alguns resultados relacionados à caracterização dessa função são também derivados. A trigonometria em corpos finitos é fundamental para o estudo de ferramentas como a transformada numérica de Fourier (FNT, do inglês *Fourier number transform*) (POLLARD, 1971; BLAHUT, 2010), a transformada numérica de Hartley (HNT, do inglês *Hartley number transform*) e as transformadas numéricas trigonométricas, as quais incluem transformadas numéricas do cosseno (CNT, do inglês *cosine number transform*) e transformadas numéricas do seno (SNT, do inglês *sine number transform*) (CAMPELLO DE SOUZA et al., 1998; CAMPELLO DE SOUZA; OLIVEIRA, 2000; CAMPELLO DE SOUZA; OLIVEIRA; PALMA, 2001; LIMA; SOUZA, 2011; SILVA et al., 2002). As definições dessas transformadas e algumas de suas propriedades também são revisadas nas próximas seções. O conteúdo apresentado neste capítulo é empregado na proposição das contribuições centrais desta tese, as quais são desenvolvidas a partir do Capítulo 4.

3.1 TRIGONOMETRIA EM CORPOS FINITOS

Os primeiros conceitos relacionados à trigonometria em corpos finitos foram estabelecidos com a finalidade de definir uma transformada de Hartley sobre essas estruturas (CAMPELLO DE SOUZA et al., 1998; SILVA et al., 2002). Em trabalhos posteriores, novas ideias foram acrescentadas e empregadas na criação de outras ferramentas matemáticas com diversas aplicações (LIMA; SOUZA, 2011; LIMA; CAMPELLO DE SOUZA; PANARIO, 2011; LIMA; SOUZA, 2013; CINTRA et al., 2009). A seguir, são apresentados os principais resultados acerca dessa teoria e, em particular, definidas as funções trigonométricas sobre corpos finitos, as quais desempenham um papel central nesse contexto. As demonstrações de proposições omitidas no texto que segue podem ser encontradas nas referências supracitadas.

Definição 3.1. O conjunto de inteiros Gaussianos sobre $\mathrm{GF}(p)$, com p ímpar, é o conjunto $\mathrm{GI}(p)$ com elementos na forma $a + bi$, em que $a, b \in \mathrm{GF}(p)$ e i^2 é um não-resíduo quadrático sobre $\mathrm{GF}(p)$.

Um elemento $\zeta \in \mathrm{GI}(p)$ pode ser visto como um elemento complexo com partes real e imaginária dadas por $\mathfrak{R}\{\zeta\} = a$ e $\mathfrak{I}\{\zeta\} = b$, respectivamente. Neste sentido, $\zeta^* = a - bi$ denota o conjugado complexo em corpo finito de $\zeta = a + bi$.

Definição 3.2. O conjunto unimodular de $\mathrm{GF}(p)$ é o conjunto $\mathrm{G}_{1,p}$ de elementos $a + bi \in \mathrm{GI}(p)$, em que $\zeta \cdot \zeta^* = (a + bi) \cdot (a - bi) = a^2 - b^2 i^2 \equiv 1 \pmod{p}$.

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

Proposição 3.1. *A estrutura* $\langle \mathrm{G}_{1,p}, \cdot \rangle$ *é um grupo cíclico de ordem* $p + 1$.

Definição 3.3. Seja $\zeta \in \mathrm{GI}(p)$ um elemento com ordem multiplicativa denotada por $\mathrm{ord}(\zeta)$. O cosseno e o seno sobre corpos finitos de um ângulo relacionado a ζ^x, a x-ésima potência de ζ, são respectivamente definidos como

$$\cos_\zeta(x) = \frac{\zeta^x + \zeta^{-x}}{2} \tag{3.1}$$

e

$$\mathrm{sen}_\zeta(x) = \frac{\zeta^x - \zeta^{-x}}{2i}, \tag{3.2}$$

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

As expressões (3.1) e (3.2) são calculadas módulo p. O conjunto de todos os possíveis valores do cosseno sobre um corpo finito em relação a zeta ζ é denotado por $\mathbb{C}_\zeta$; o conjunto de todos os possíveis valores do seno sobre corpos finitos em relação a ζ é denotado por $\mathbb{S}_\zeta$. Tais funções mantêm propriedades semelhantes às das respectivas funções no corpo dos reais. Como exemplo, tem-se a propriedade do círculo unitário, que pode ser escrita como

$$\cos^2_\zeta(x) - i^2 \mathrm{sen}^2_\zeta(x) \equiv 1 \pmod{p}, \tag{3.3}$$

e a fórmula de Euler

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

Note que, se $p \equiv 3 \pmod 4$ e $i = \sqrt{-1}$, (3.3) se torna semelhante à identidade trigonométrica fundamental clássica. As propriedades de simetria das funções seno e cosseno são preservadas no contexto de corpo finito, isto é, $\cos_\zeta(-x) = \cos_\zeta(x)$ e $\mathrm{sen}_\zeta(-x) = -\mathrm{sen}_\zeta(x)$.

Proposição 3.2. *O cosseno e o seno sobre corpos finitos de um ângulo relacionado a* ζ^x*, em que* $\zeta \in \mathrm{G}_{1,p}$*, podem ser expressos, respectivamente, como*

$$\cos_\zeta(x) = \mathfrak{R}\{\zeta^x\}$$

e

$$\mathrm{sen}_\zeta(x) = \mathfrak{I}\{\zeta^x\},$$

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

O lema a seguir é um resultado desenvolvido nesta tese e é empregado no estabelecimento de proposições a serem apresentadas posteriormente.

Lema 3.1. *Se* $\zeta = a + bi \in \mathrm{GI}(p)$ *tem ordem multiplicativa* $\mathrm{ord}(\zeta) = 2(p + 1)$*, então* $\zeta^{-1} = -\zeta^*$.

Demonstração. Devido à Proposição 3.1, sabe-se que $\zeta^2 = (a^2 + i^2b^2) + (2ab)i$ é unimodular. Por consequência, $\zeta^{-2} = (\zeta^2)^* = (a^2 + i^2b^2) - (2ab)i = (-a + bi)^2$ e o resultado segue. □

A proposição a seguir é um resultado desenvolvido nesta tese.

Proposição 3.3. *Seja $\zeta \in \mathrm{GI}(p)$ um elemento com ordem multiplicativa $\mathrm{ord}(\zeta) = 2(p + 1)$ e $\zeta_1 = \zeta^2$. O cosseno e seno sobre corpo finito do ângulo relacionado a ζ^x é puramente "real" (i. e., pertence a $\mathrm{GF}(p)$), se x for par, ou puramente "imaginário" (i. e., tem a forma $b'i$, $b' \in \mathrm{GF}(p)$), se x for ímpar.*

Demonstração. Se x for par, ele pode ser escrito como $x = 2y$. Portanto, uma vez que $\zeta_1 = \zeta^2$, o cosseno e o seno sobre corpo finito do ângulo relacionado a ζ^x correspondem, respectivamente, ao cosseno e ao seno sobre corpo finito do ângulo relacionado a ζ_1^y, o qual, devido a Proposição 3.2, pertence a $\mathrm{GF}(p)$ (ζ_1 tem ordem multiplicativa $\mathrm{ord}(\zeta_1) = p + 1$, isto é, é um gerador de $\mathrm{G}_{1,p}$). Se x for ímpar, ele pode ser escrito como $x = 2y + 1$ e, assim,

$$\mathrm{sen}_\zeta(x) = \mathrm{sen}_\zeta(2y + 1) = \frac{\zeta^{2y+1} - \zeta^{-2y-1}}{2i} = \frac{\zeta_1^y\zeta - \zeta_1^{-y}\zeta^{-1}}{2i}. \tag{3.4}$$

Assumindo que $\zeta_1^y = a + bi$, $a, b \in \mathrm{GI}(p)$, que também é unimodular, tem-se que $\zeta_1^{-y} = a - bi$. Adicionalmente, assumindo que $\zeta = c+di$, $c, d \in \mathrm{GF}(p)$, obtém-se, do Lema 3.1, $\zeta^{-1} = -c+di$. Usando-se (3.4), obtém-se

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

o qual é puramente "imaginário". Um desenvolvimento similar é obtido para o cosseno sobre corpo finito. □

3.1.1 Função Tangente sobre Corpos Finitos

Nesta seção, é introduzida a função tangente sobre corpos finitos. Alguns resultados relacionados a esta função são derivados e sua função inversa é caracterizada. Além de preencher uma lacuna teórica na trigonometria sobre corpos finitos, essa função tangente é empregada no cálculo do chamado "ângulo ótimo", que pode indicar a rotação aplicada a um par de vetores de base da transformada numérica de Fourier, para definição da transformada numérica manobrável de Fourier (Capítulo 4).

Definição 3.4. Seja $\zeta \in \mathrm{GI}(p)$ um elemento com ordem multiplicativa denotada por $\mathrm{ord}(\zeta)$. A tangente sobre corpos finitos do ângulo relacionado a ζ^x é definida como

$$\mathrm{tan}_\zeta(x) = \frac{\mathrm{sen}_\zeta(x)}{\mathrm{cos}_\zeta(x)} = \frac{1}{i}\frac{\zeta^x - \zeta^{-x}}{\zeta^x + \zeta^{-x}}, \tag{3.5}$$

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

Diferentemente do cosseno e do seno sobre corpos finitos, a função tangente definida é $\left(\frac{\mathrm{ord}(\zeta)}{2}\right)$-periódica; dado um número inteiro k, isso pode ser verificado calculando

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

Uma vez que $\zeta^{k\frac{\mathrm{ord}(\zeta)}{2}} = \zeta^{-k\frac{\mathrm{ord}(\zeta)}{2}} = (-1)^k$, tem-se $\tan_\zeta\left(x + k\frac{\mathrm{ord}(\zeta)}{2}\right) = \tan_\zeta(x)$. Pode-se também verificar que a tangente sobre corpos finitos tem simetria ímpar, isto é, $\tan_\zeta(-x) = -\tan_\zeta(x)$. O conjunto de todos os possíveis valores das tangentes sobre corpos finitos em relação a ζ é denotado por $\mathbb{T}_\zeta$. O seguinte lema mostra que o cômputo da tangente no intervalo dado na Definição 3.4 produz exatamente $\mathrm{ord}(\zeta)/2$ valores diferentes.

Lema 3.2. *Seja* $\zeta \in \mathrm{GI}(p)$ *um elemento com ordem multiplicativa* $\mathrm{ord}(\zeta)$. *Para* $0 \leq x, y \leq \frac{\mathrm{ord}(\zeta)}{2} - 1$,

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

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

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

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

Proposição 3.4. *Se* $\zeta \in \mathrm{GI}(p)$ *é um elemento com ordem multiplicativa* $\mathrm{ord}(\zeta) = 2(p+1)$, *então* $\mathbb{T}_\zeta = \mathbb{F}_p \cup \infty$.

Demonstração. Considerando a periodicidade da função tangente sobre corpos finitos e o Lema 3.2, sabe-se que $\tan_\zeta(x)$ produz exatamente $p + 1$ diferentes resultados. Devido à Proposição 3.3, sabe-se que p destes resultados estão em $\mathrm{GF}(p)$, uma vez que as funções cosseno e seno correspondentes, para um dado x, são simultaneamente puramente "reais" ou puramente "imaginárias". Isto é, os referidos resultados são todos elementos de $\mathrm{GF}(p)$. A única exceção é o resultado obtido quando $x = \frac{\mathrm{ord}(\zeta)}{4}$, que resulta em $\cos_\zeta\left(\frac{\mathrm{ord}(\zeta)}{4}\right) = 0$ e, consequentemente, $\tan_\zeta\left(\frac{\mathrm{ord}(\zeta)}{4}\right) = \infty$. □

Exemplo 3.1. *Neste exemplo, ilustra-se o cálculo de todos os valores de seno, cosseno e tangente sobre corpos finitos em relação ao elemento* $\zeta = 2 + 3i \in \mathrm{GI}(7)$, $i^2 = 6$, *e considerando o intervalo* $x = 0, 1, \ldots, 7$ *(vide Tabela 2); o elemento tem ordem multiplicativa* $\mathrm{ord}(\zeta) = 2(p+1) = 16$. *Como ilustração da Proposição 3.4, na tabela, pode-se observar que as colunas relacionadas à função tangente são formadas por todos os elementos de* $\mathrm{GF}(7)$.

Tabela 2 – Valores calculados do seno, cosseno e tangente sobre um corpo finito em relação ao elemento $\zeta = 2 + 3i \in \mathrm{GI}(7)$, em que $\mathrm{ord}(\zeta) = 2(p+1) = 16$, $i^2 = 6$, e considerando o intervalo $x = 0, 1, \ldots, 7$.

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	Inf
5	4i	5i	5
6	5	5	1
7	5i	4i	3

Fonte: O Autor, 2019.

Exemplo 3.2. *Neste exemplo, ilustra-se o cálculo de todos os valores de seno, cosseno e tangente sobre corpos finitos em relação ao elemento* $\zeta = 191 + 225i \in \mathrm{GI}(257)$*,* $i^2 = 3$*, e considerando o intervalo* $x = 0, 1, \ldots, 257$ *(vide Tabela 3); o elemento tem ordem multiplicativa* $\mathrm{ord}(\zeta) = 2(p+1) = 516$*. Como ilustração da Proposição 3.4, na tabela, pode-se observar que as colunas relacionadas à função tangente são formadas por todos os elementos de* $\mathrm{GF}(257)$*.*

A partir de (3.5), pode-se derivar uma expressão fechada para a função tangente sobre corpos finitos inversa, a qual é denotada por $\arctan_\zeta(x)$, se ela for calculada com relação a um elemento $\zeta \in \mathrm{GI}(p)$. Na referida equação, substitui-se $\tan_\zeta(x)$ e x por x e $y = \arctan_\zeta(x)$, respectivamente; então, obtém-se o desenvolvimento

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

e, finalmente,

$$y = \arctan_\zeta(x) = \frac{1}{2}\log_\zeta\left(\frac{1 + ix}{1 - ix}\right). \tag{3.6}$$

3.2 A TRANSFORMADA NUMÉRICA DE FOURIER

Nesta seção, é revisada a definição da transformada numérica de Fourier. Na literatura voltada a aplicações em processamento de sinais, o uso do termo "numérica" remete a um caso particular da transformada de Fourier sobre corpos finitos, em que as componentes dos vetores envolvidos e o núcleo da transformada se encontram no chamado corpo base, isto é, $\mathrm{GF}(p)$ (POLLARD, 1971; SHU; TIANREN, 1988; RUBANOV et al., 1998; DIMITROV; COOKLEV; DONEVSKY, 1995; GUDVANGEN, 2006); noutras palavras, não são considerados corpos de extensão. A definição aqui apresentada assume que os vetores envolvidos e o núcleo

Tabela 3 – Valores calculados com $\zeta = 191 + 225i \in \mathrm{GI}(257)$, $\mathrm{ord}(\zeta) = 2(p+1) = 516$, $i^2 = 3$.

x	$\mathrm{sen}_\zeta(x)$	$\cos_\zeta(x)$	$\tan_\zeta(x)$	x	$\mathrm{sen}_\zeta(x)$	$\cos_\zeta(x)$	$\tan_\zeta(x)$	x	$\mathrm{sen}_\zeta(x)$	$\cos_\zeta(x)$	$\tan_\zeta(x)$
0	$0+0i$	$1+0i$	0	86	$249+0i$	$129+0i$	241	172	$249+0i$	$128+0i$	16
1	$0+22i$	$0+32i$	81	87	$0+12i$	$0+2i$	6	173	$0+247i$	$0+227i$	86
2	$112+0i$	$232+0i$	160	88	$256+0i$	$255+0i$	129	174	$144+0i$	$23+0i$	118
3	$0+207i$	$0+167i$	229	89	$0+181i$	$0+127i$	222	175	$0+231i$	$0+217i$	142
4	$54+0i$	$221+0i$	127	90	$58+0i$	$228+0i$	255	176	$4+0i$	$7+0i$	74
5	$0+165i$	$0+99i$	173	91	$0+190i$	$0+73i$	242	177	$0+25i$	$0+231i$	88
6	$15+0i$	$26+0i$	50	92	$185+0i$	$167+0i$	155	178	$170+0i$	$141+0i$	65
7	$0+24i$	$0+23i$	191	93	$0+85i$	$0+78i$	123	179	$0+61i$	$0+55i$	174
8	$224+0i$	$21+0i$	182	94	$201+0i$	$160+0i$	141	180	$234+0i$	$139+0i$	59
9	$0+177i$	$0+36i$	112	95	$0+186i$	$0+139i$	238	181	$0+9i$	$0+103i$	45
10	$93+0i$	$209+0i$	239	96	$45+0i$	$57+0i$	109	182	$209+0i$	$105+0i$	95
11	$0+121i$	$0+233i$	177	97	$0+124i$	$0+168i$	117	183	$0+3i$	$0+192i$	253
12	$9+0i$	$66+0i$	152	98	$119+0i$	$74+0i$	144	184	$110+0i$	$8+0i$	78
13	$0+198i$	$0+136i$	232	99	$0+39i$	$0+199i$	181	185	$0+98i$	$0+63i$	230
14	$228+0i$	$89+0i$	17	100	$173+0i$	$98+0i$	146	186	$202+0i$	$9+0i$	51
15	$0+2i$	$0+163i$	82	101	$0+239i$	$0+162i$	57	187	$0+237i$	$0+256i$	20
16	$156+0i$	$110+0i$	193	102	$226+0i$	$166+0i$	54	188	$70+0i$	$56+0i$	194
17	$0+216i$	$0+195i$	96	103	$0+90i$	$0+182i$	153	189	$0+131i$	$0+244i$	69
18	$196+0i$	$65+0i$	90	104	$92+0i$	$83+0i$	94	190	$153+0i$	$18+0i$	137
19	$0+249i$	$0+110i$	56	105	$0+144i$	$0+247i$	37	191	$0+152i$	$0+137i$	33
20	$67+0i$	$238+0i$	10	106	$57+0i$	$53+0i$	132	192	$247+0i$	$72+0i$	7
21	$0+184i$	$0+216i$	77	107	$0+163i$	$0+61i$	108	193	$0+236i$	$0+102i$	219
22	$52+0i$	$114+0i$	23	108	$142+0i$	$94+0i$	89	194	$90+0i$	$237+0i$	124
23	$0+60i$	$0+141i$	159	109	$0+187i$	$0+44i$	197	195	$0+127i$	$0+160i$	208
24	$160+0i$	$230+0i$	213	110	$39+0i$	$130+0i$	26	196	$136+0i$	$157+0i$	122
25	$0+157i$	$0+187i$	185	111	$0+253i$	$0+52i$	79	197	$0+96i$	$0+122i$	5
26	$172+0i$	$208+0i$	243	112	$221+0i$	$88+0i$	58	198	$49+0i$	$137+0i$	36
27	$0+57i$	$0+18i$	46	113	$0+13i$	$0+183i$	170	199	$0+213i$	$0+165i$	34
28	$235+0i$	$164+0i$	3	114	$219+0i$	$96+0i$	187	200	$241+0i$	$189+0i$	227
29	$0+77i$	$0+198i$	186	115	$0+125i$	$0+50i$	131	201	$0+48i$	$0+109i$	215
30	$157+0i$	$73+0i$	62	116	$137+0i$	$252+0i$	24	202	$237+0i$	$179+0i$	165
31	$0+205i$	$0+105i$	210	117	$0+162i$	$0+144i$	226	203	$0+214i$	$0+39i$	190
32	$139+0i$	$41+0i$	41	118	$127+0i$	$154+0i$	136	204	$245+0i$	$113+0i$	150
33	$0+210i$	$0+206i$	11	119	$0+256i$	$0+203i$	119	205	$0+46i$	$0+254i$	156
34	$89+0i$	$190+0i$	248	120	$195+0i$	$15+0i$	13	206	$106+0i$	$82+0i$	158
35	$0+89i$	$0+132i$	209	121	$0+145i$	$0+243i$	8	207	$0+56i$	$0+111i$	151
36	$37+0i$	$225+0i$	39	122	$146+0i$	$124+0i$	196	208	$109+0i$	$156+0i$	32
37	$0+223i$	$0+133i$	21	123	$0+204i$	$0+240i$	245	209	$0+238i$	$0+107i$	228
38	$117+0i$	$125+0i$	40	124	$215+0i$	$210+0i$	154	210	$98+0i$	$85+0i$	110
39	$0+69i$	$0+157i$	43	125	$0+192i$	$0+93i$	143	211	$0+123i$	$0+193i$	235
40	$24+0i$	$207+0i$	164	126	$155+0i$	$170+0i$	205	212	$131+0i$	$220+0i$	184
41	$0+182i$	$0+241i$	85	127	$0+219i$	$0+250i$	189	213	$0+37i$	$0+9i$	204
42	$225+0i$	$62+0i$	157	128	$2+0i$	$28+0i$	202	214	$34+0i$	$223+0i$	256
43	$0+83i$	$0+129i$	166	129	$0+166i$	$0+0i$	inf	215	$0+83i$	$0+128i$	91
44	$34+0i$	$34+0i$	1	130	$2+0i$	$229+0i$	55	216	$225+0i$	$195+0i$	100
45	$0+37i$	$0+248i$	53	131	$0+219i$	$0+7i$	68	217	$0+182i$	$0+16i$	172
46	$131+0i$	$37+0i$	73	132	$155+0i$	$87+0i$	52	218	$24+0i$	$50+0i$	93
47	$0+123i$	$0+64i$	22	133	$0+192i$	$0+164i$	114	219	$0+69i$	$0+100i$	214
48	$98+0i$	$172+0i$	147	134	$215+0i$	$47+0i$	103	220	$117+0i$	$132+0i$	217
49	$0+238i$	$0+150i$	29	135	$0+204i$	$0+17i$	12	221	$0+223i$	$0+124i$	236
50	$109+0i$	$101+0i$	225	136	$146+0i$	$133+0i$	61	222	$37+0i$	$32+0i$	218
51	$0+56i$	$0+146i$	106	137	$0+145i$	$0+14i$	249	223	$0+89i$	$0+125i$	48
52	$106+0i$	$175+0i$	99	138	$195+0i$	$242+0i$	244	224	$89+0i$	$67+0i$	9
53	$0+46i$	$0+3i$	101	139	$0+256i$	$0+54i$	138	225	$0+210i$	$0+51i$	246
54	$245+0i$	$144+0i$	107	140	$127+0i$	$103+0i$	121	226	$139+0i$	$216+0i$	216
55	$0+214i$	$0+218i$	67	141	$0+162i$	$0+113i$	31	227	$0+205i$	$0+152i$	47
56	$237+0i$	$78+0i$	92	142	$137+0i$	$5+0i$	233	228	$157+0i$	$184+0i$	195
57	$0+48i$	$0+148i$	42	143	$0+125i$	$0+207i$	126	229	$0+77i$	$0+59i$	71
58	$241+0i$	$68+0i$	30	144	$219+0i$	$161+0i$	70	230	$235+0i$	$93+0i$	254
59	$0+213i$	$0+92i$	223	145	$0+13i$	$0+74i$	87	231	$0+57i$	$0+239i$	211
60	$49+0i$	$120+0i$	221	146	$221+0i$	$169+0i$	199	232	$172+0i$	$49+0i$	14
61	$0+96i$	$0+135i$	252	147	$0+253i$	$0+205i$	178	233	$0+157i$	$0+70i$	72
62	$136+0i$	$100+0i$	135	148	$39+0i$	$127+0i$	231	234	$160+0i$	$27+0i$	44
63	$0+127i$	$0+97i$	49	149	$0+187i$	$0+213i$	60	235	$0+60i$	$0+116i$	98
64	$90+0i$	$20+0i$	133	150	$142+0i$	$163+0i$	168	236	$52+0i$	$143+0i$	234
65	$0+236i$	$0+155i$	38	151	$0+163i$	$0+196i$	149	237	$0+184i$	$0+41i$	180
66	$247+0i$	$185+0i$	250	152	$57+0i$	$204+0i$	125	238	$67+0i$	$19+0i$	247
67	$0+152i$	$0+120i$	224	153	$0+144i$	$0+10i$	220	239	$0+249i$	$0+147i$	201
68	$153+0i$	$239+0i$	120	154	$92+0i$	$174+0i$	163	240	$196+0i$	$192+0i$	167
69	$0+131i$	$0+13i$	188	155	$0+90i$	$0+75i$	104	241	$0+216i$	$0+62i$	161
70	$70+0i$	$201+0i$	63	156	$226+0i$	$91+0i$	203	242	$156+0i$	$147+0i$	64
71	$0+237i$	$0+1i$	237	157	$0+239i$	$0+95i$	200	243	$0+2i$	$0+94i$	175
72	$202+0i$	$248+0i$	206	158	$173+0i$	$159+0i$	111	244	$228+0i$	$168+0i$	240
73	$0+98i$	$0+194i$	27	159	$0+39i$	$0+58i$	76	245	$0+198i$	$0+121i$	25
74	$110+0i$	$249+0i$	179	160	$119+0i$	$183+0i$	113	246	$9+0i$	$191+0i$	105
75	$0+3i$	$0+65i$	4	161	$0+124i$	$0+89i$	140	247	$0+121i$	$0+24i$	80
76	$209+0i$	$152+0i$	162	162	$45+0i$	$200+0i$	148	248	$93+0i$	$48+0i$	18
77	$0+9i$	$0+154i$	212	163	$0+186i$	$0+118i$	19	249	$0+177i$	$0+221i$	145
78	$234+0i$	$118+0i$	198	164	$201+0i$	$97+0i$	116	250	$224+0i$	$236+0i$	75
79	$0+61i$	$0+202i$	83	165	$0+85i$	$0+179i$	134	251	$0+24i$	$0+234i$	66
80	$170+0i$	$116+0i$	192	166	$185+0i$	$90+0i$	102	252	$15+0i$	$231+0i$	207
81	$0+25i$	$0+26i$	169	167	$0+190i$	$0+184i$	15	253	$0+165i$	$0+158i$	84
82	$4+0i$	$250+0i$	183	168	$58+0i$	$29+0i$	2	254	$54+0i$	$36+0i$	130
83	$0+231i$	$0+40i$	115	169	$0+181i$	$0+130i$	35	255	$0+207i$	$0+90i$	28
84	$144+0i$	$234+0i$	139	170	$256+0i$	$2+0i$	128	256	$112+0i$	$25+0i$	97
85	$0+247i$	$0+30i$	171	171	$0+12i$	$0+255i$	251	257	$0+22i$	$0+225i$	176

Fonte: O Autor, 2019.

da transformada podem se encontrar no conjunto $\mathrm{GI}(p)$, que, em função do possível isomorfismo com $\mathrm{GF}(p^2)$, pode ser um corpo de extensão (CAMPELLO DE SOUZA et al., 1998; SILVA et al., 2002; LIMA; CAMPELLO DE SOUZA, 2006). De qualquer forma, como a aritmética na referida estrutura pode ser realizada de forma análoga àquela empregada nos números complexos usuais, sem a necessidade de realizar explicitamente operações módulo um polinômio, esta tese mantém a nomenclatura "numérica" para identificar a transformada; tal escolha é, também, uma tentativa de alinhar a terminologia empregada neste trabalho com a de outros trabalhos com os quais pode se relacionar o mesmo.

Definição 3.5. Seja $\zeta \in \mathrm{GI}(p)$ um elemento cuja ordem multiplicativa é $\mathrm{ord}(\zeta) = N$. A transformada numérica de Fourier unitária (FNT) do vetor $\mathbf{x} = (x(n))$, $x(n) \in \mathrm{GI}(p)$, $n = 0, 1, \ldots, N-1$, é o vetor $\mathbf{X} = (X(k))$, $X(k) \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, com componentes dadas por

$$X(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\zeta^{kn}. \tag{3.7}$$

A invertibilidade da FNT é provida pelo seguinte lema.

Lema 3.3. *Um elemento $\zeta \in \mathrm{GI}(p)$ de ordem multiplicativa $\mathrm{ord}(\zeta) = N$ satisfaz*

$$\sum_{m=0}^{N-1} \zeta^{km} = \begin{cases} N, & \textit{se } k = 0, \\ 0, & \textit{se } k = 1, 2, \ldots, N-1. \end{cases} \tag{3.8}$$

Usando o Lema 3.3, pode-se mostrar que as componentes de um vetor $\mathbf{x}$ são recuperadas a partir das componentes de sua FNT por

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k)\zeta^{-kn}.$$

Empregando a notação matricial, pode-se escrever

$$\mathbf{X} = \mathbf{F}\mathbf{x}, \tag{3.9}$$

em que $\mathbf{F}$ é a matriz de transformação da FNT[1], cujo elemento na k-ésima linha e na n-ésima coluna é dado por

$$F(k, n) = \sqrt{N^{-1}}\zeta^{kn}. \tag{3.10}$$

Exemplo 3.3. *Como exemplo, considere o elemento $\zeta = 4 \in \mathrm{GF}(257)$, com ordem multiplicativa $\mathrm{ord}(4) = 8$. Empregando o referido núcleo, define-se uma FNT cuja matriz $\mathbf{F}$ é dada por*

[1] Embora no Capítulo 2, $\mathbf{F}$ tenha sido usado também para denotar a matriz da DFT, deste ponto em diante na tese, tal símbolo identificará a matriz da FNT apenas.

$$\mathbf{F} = \begin{bmatrix} 242 & 242 & 242 & 242 & 242 & 242 & 242 & 242 \\ 242 & 197 & 17 & 68 & 15 & 60 & 240 & 189 \\ 242 & 17 & 15 & 240 & 242 & 17 & 15 & 240 \\ 242 & 68 & 240 & 197 & 15 & 189 & 17 & 60 \\ 242 & 15 & 242 & 15 & 242 & 15 & 242 & 15 \\ 242 & 60 & 17 & 189 & 15 & 197 & 240 & 68 \\ 242 & 240 & 15 & 17 & 242 & 240 & 15 & 17 \\ 242 & 189 & 240 & 60 & 15 & 68 & 17 & 197 \end{bmatrix}.$$

Se a FNT de um vetor com componentes pertencentes a $\mathrm{GF}(p)$ for definida empregando-se como núcleo um elemento $\omega \in \mathrm{G}_{1,p}$, as seguintes propriedades de simetria serão satisfeitas.

Proposição 3.5. *Seja* $\mathbf{X} = (X(k))$, $X(k) \in \mathrm{GI}(p)$, $k = 0, \ldots, N-1$, *a transformada numérica de Fourier do vetor* $\mathbf{x} = (x(n))$, $x(n) \in \mathrm{GF}(p)$, $n = 0, \ldots, N-1$. *Tem-se*

1. $\Re\{X(k)\} = \Re\{X(N-k) \pmod N\}$;
2. $\Im\{X(k)\} = -\Im\{X(N-k) \pmod N\}$.

Demonstração. Usando a fórmula de Euler, pode-se escrever $\omega^{kn} = \cos_\omega(kn) + i\mathrm{sen}_\omega(kn)$ e, uma vez que ω é unimodular, devido à Proposição 3.2, sabe-se que $\Re\{\omega^{kn}\} = \cos_\omega(kn)$ e $\Im\{\omega^{kn}\} = \mathrm{sen}_\omega(kn)$. Dessa maneira, tem-se

$$\begin{aligned} \Re\{X(k)\} &= \Re\left\{\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\omega^{kn}\right\} = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\Re\{\omega^{kn}\} \\ &= \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\cos_\omega(kn). \end{aligned}$$

Devido à simetria par da função cosseno, a última equação pode ser reescrita como

$$\begin{aligned} \Re\{X(k)\} &= \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\cos_\omega(-kn) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\Re\{\omega^{-kn}\} \\ &= \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\Re\{\omega^{(N-k)n}\} = \Re\{X(N-k)\}. \end{aligned}$$

Isso conclui a prova da parte real $\Re\{X(k)\}$ da Proposição 3.5. A prova da parte imaginária $\Im\{X(k)\}$, que é omitida, pode ser desenvolvida usando passos similares e considerando o fato de que a função seno possui simetria ímpar. □

A Proposição 3.5 será empregada no Capítulo 4, na definição da transformada numérica de Hilbert, a qual possui relação com a transformada numérica manobrável de Fourier.

3.2.1 Convolução em Corpos Finitos

A convolução é uma operação de grande relevância no estudo de processamento de sinais e sua aplicação a vetores cujos elementos pertencem a um corpo finito é, também, comumente considerada (BLAHUT, 2010; SHU; TIANREN, 1988; RUBANOV et al., 1998; DIMITROV; COOKLEV; DONEVSKY, 1995; TOIVONEN; HEIKKILÄ, 2006). A equação que descreve a convolução cíclica entre sinais em $\mathrm{GF}(p)$ é a mesma empregada para a convolução cíclica no corpo dos reais, a não ser pelo fato de que, no corpo finito, todas as operações são avaliadas módulo p. Assim, a convolução cíclica (ou circular) de comprimento N entre dois vetores $\mathbf{g}$ e $\mathbf{d}$ com componentes $g(n)$ e $d(n)$ resulta no vetor $\mathbf{s} = \mathbf{g} \star_N \mathbf{d}$ com componentes calculadas por

$$s(n) = \sum_{m=0}^{N-1} g(m)d((n-m) \pmod N) \pmod p. \tag{3.11}$$

Uma das formas de se computar a convolução cíclica de sinais em $\mathrm{GF}(p)$ é utilizar a transformada numérica de Fourier com o teorema da convolução. Mais especificamente, tem-se

$$S(k) = G(k)D(k), \tag{3.12}$$

em que

$$G(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} g(n)\zeta^{kn} \tag{3.13}$$

e

$$D(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} d(n)\zeta^{kn}. \tag{3.14}$$

O resultado da convolução é obtido por meio do cômputo da FNT inversa de $\mathbf{S}$, isto é,

$$s(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} S(k)\zeta^{-kn}. \tag{3.15}$$

3.2.2 Transformada Numérica de Fourier Bidimensional

Versões bidimensionais da transformada numérica de Fourier podem ser definidas a partir de uma simples extensão do caso unidimensional apresentado. A definição da 2D-FNT é dada a seguir.

Definição 3.6. Sejam $\zeta_1 \in \mathrm{GI}(p)$ e $\zeta_2 \in \mathrm{GI}(p)$ elementos cujas ordens multiplicativas são dadas por $\mathrm{ord}(\zeta_1) = N_1$ e $\mathrm{ord}(\zeta_2) = N_2$, respectivamente. A transformada numérica de Fourier bidimensional da matriz $\mathbf{x} = (x(n,m))$, $x(n,m) \in \mathrm{GI}(p)$, $n = 0, 1, \ldots, N_1 - 1$, $m = 0, 1, \ldots, N_2 - 1$, é a matriz $\mathbf{X} = (X(r,s))$, $X(r,s) \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N_1 - 1$, $l = 0, 1, \ldots, N_2 - 1$, com componentes dadas por

$$X(r,s) = \frac{1}{\sqrt{N_1 N_2}} \sum_{n=0}^{N_1-1} \sum_{m=0}^{N_2-1} x(n,m)\zeta_1^{rn}\zeta_2^{sm}. \tag{3.16}$$

De modo análogo ao que se fez para o caso unidimensional, pode-se mostrar que as componentes de $\mathbf{x}$ são recuperadas a partir das componentes de sua FNT por

$$x(n,m) = \frac{1}{\sqrt{N_1 N_2}} \sum_{r=0}^{N_1-1} \sum_{s=0}^{N_2-1} X(r,s)\zeta_1^{-rn}\zeta_2^{-sm}.$$

Considerando o caso particular em que $\zeta = \zeta_1 = \zeta_2$ e, consequentemente, $N = N_1 = N_2$, é possível expressar o cálculo da 2D-FNT matricialmente como

$$\mathbf{X} = \mathbf{F}\mathbf{x}\mathbf{F}^T, \tag{3.17}$$

em que $\mathbf{F}$ é a matriz de transformação da FNT unidimensional com núcleo dado por ζ e T denota a transposição do respectivo argumento; noutras palavras, como a FNT é uma transformada separável, sua versão bidimensional corresponde a calcular a FNT (unidimensional) de todas as colunas de $\mathbf{x}$ e depois de todas as linhas da matriz que se obtiver como resultado da primeira operação.

3.3 OUTRAS TRANSFORMADAS NUMÉRICAS

A seguir são apresentadas algumas transformadas numéricas, que foram avaliadas no decorrer da pesquisa, em relação a possibilidade de defini-las sobre estruturas algébricas finitas.

3.3.1 Transformada Numérica de Hartley

Em (CAMPELLO DE SOUZA et al., 1998), introduziu-se a transformada de Hartley sobre corpos finitos (FFHT, do inglês *finite field Hartley transform*). Posteriormente, versões numéricas dessa transformada foram apresentadas e algumas de suas aplicações foram investigadas (CAMPELLO DE SOUZA; OLIVEIRA; PALMA, 2001; SILVA et al., 2002). Nesta seção, de modo análogo ao que se fez na Seção 3.2, é apresentada uma versão dessa ferramenta nomeada simplesmente por transformada numérica de Hartley (HNT, do inglês *Hartley number transform*), a qual, conforme definido a seguir, é construída com base num elemento $\zeta \in \mathrm{GI}(p)$.

Definição 3.7. Seja $\zeta \in \mathrm{GI}(p)$ um elemento cuja ordem multiplicativa é $\mathrm{ord}(\zeta) = N$. A transformada numérica de Hartley do vetor $\mathbf{x} = (x(n))$, $x(n) \in \mathrm{GI}(p)$, $n = 0, 1, \ldots, N-1$, é o vetor $\mathbf{X}_H = (X_H(k))$, $X_H(k) \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, com componentes dadas por

$$X_H(k) = \sum_{n=0}^{N-1} x(n)\mathrm{cas}_\zeta(kn), \tag{3.18}$$

em que $\mathrm{cas}_\zeta(kn) = \cos_\zeta(kn) + \mathrm{sen}_\zeta(kn)$.

A HNT inversa é obtida utilizando-se a expressão da própria HNT, ou seja, aplicando duas vezes a transformada de Hartley a um vetor $\mathbf{x}$, obtém-se como resultado o próprio vetor.

Equivalentemente, pode-se afirmar que a transformada de Hartley é uma involução, conforme indicado pelo teorema a seguir.

Teorema 3.1. *A transformada numérica de Hartley inversa do vetor* $\mathbf{X}_H = (X_H(k))$, $X_H(k) \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, *possui componentes dadas por (CAMPELLO DE SOUZA et al., 1998)*

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X_H(k) \mathrm{cas}_\zeta(kn), \tag{3.19}$$

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

A equação matricial da HNT é dada por

$$\mathbf{X}_H = \mathbf{H}\mathbf{x}, \tag{3.20}$$

em que $H(k, n) = \mathrm{cas}_\zeta(kn)$, $k, n = 0, 1, \ldots, N-1$.

3.3.2 Transformadas Numéricas do Cosseno e do Seno

Nesta seção, são apresentadas de forma sumária as transformadas trigonométricas unitárias sobre corpos finitos (FFTT, do inglês *finite field trigonometric transforms*), as quais incluem 8 transformadas do cosseno e 8 transformadas do seno (LIMA; SOUZA, 2011). De modo análogo ao que se tem feito noutras seções desta tese, essas transformadas são identificadas, respectivamente, como transformada numérica do cosseno (CNT, do inglês *cosine number transform*) e da transformada numérica do seno (SNT, do inglês *sine number transform*).

A construção das FFTT possui certa analogia com a das transformações trigonométricas discretas (MARTUCCI, 1994). O procedimento, que é baseado no cálculo de transformadas de Fourier de versões simetricamente estendidas de uma sequência (ou vetor), leva à definição dos diversos tipos de transformada à medida em que se combina tipos par e ímpar das referidas extensões.

Em geral, qualquer FFTT de uma sequência $\mathbf{x} = (x(n))$, $(x(n)) \in \mathrm{GI}(p)$, $n = 0, 1, \ldots, N-1$, é uma sequência $\mathbf{X} = (X(k)), X(k) \in \mathrm{GI}(p)$, obtida pela equação matricial

$$\mathbf{X} = \mathbf{M}\mathbf{x}, \tag{3.21}$$

em que M é a matriz de transformação. Os elementos dessa matriz são calculados de acordo com a primeira coluna da Tabela 4 ou da Tabela 5, em que as funções de ponderação $\tilde{\beta}_r$ e $\tilde{\gamma}_r$ são dadas por

$$\tilde{\beta}_r \equiv \begin{cases} \sqrt{2^{-1}} \pmod p, & r = 0 \text{ or } N, \\ 1, & r = 1, 2, \ldots, N-1 \end{cases} \tag{3.22}$$

e

$$\tilde{\gamma}_r \equiv \begin{cases} 1, & r = 0, 1, \ldots, N-2, \\ \sqrt{2^{-1}} \pmod{p}, & r = N-1. \end{cases} \tag{3.23}$$

Tabela 4 – Elementos das matrizes das transformadas sobre corpos finitos do cosseno unitárias.

Elementos da matriz de transformação	Dimensão da matriz
$C_{1e}(k,n) = (\sqrt{2/N})\ \tilde{\beta}_n\ \tilde{\beta}_k \cos_\zeta(kn)$	$n, k = 0, 1, \ldots, N$
$C_{2e}(k,n) = (\sqrt{2/N})\ \tilde{\beta}_k \cos_\zeta\left(k\left(n+\frac{1}{2}\right)\right)$	$n, k = 0, 1, \ldots, N-1$
$C_{3e}(k,n) = (\sqrt{2/N})\ \tilde{\beta}_n \cos_\zeta\left(\left(k+\frac{1}{2}\right)n\right)$	$n, k = 0, 1, \ldots, N-1$
$C_{4e}(k,n) = (\sqrt{2/N})\ \cos_\zeta\left(\left(k+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\right)$	$n, k = 0, 1, \ldots, N-1$
$C_{1o}(k,n) = (2/\sqrt{2N-1})\ \tilde{\beta}_n\ \tilde{\beta}_k \cos_\zeta(kn)$	$n, k = 0, 1, \ldots, N-1$
$C_{2o}(k,n) = (2/\sqrt{2N-1})\ \tilde{\gamma}_n\ \tilde{\beta}_k \cos_\zeta\left(k\left(n+\frac{1}{2}\right)\right)$	$n, k = 0, 1, \ldots, N-1$
$C_{3o}(k,n) = (2/\sqrt{2N-1})\ \tilde{\beta}_n\ \tilde{\gamma}_k \cos_\zeta\left(\left(k+\frac{1}{2}\right)n\right)$	$n, k = 0, 1, \ldots, N-1$
$C_{4o}(k,n) = (2/\sqrt{2N-1})\ \cos_\zeta\left(\left(k+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\right)$	$n, k = 0, 1, \ldots, N-2$

Fonte: O Autor, 2019.

As dimensões de $\mathbf{x}$, $\mathbf{X}$ e $\mathbf{M}$ são especificadas na segunda coluna das referidas tabelas, em que o intervalo nos índices k (linha) e n (coluna) são mostrados. As matrizes de transformação do cosseno e do seno são identificadas como $\mathbf{C}$ e $\mathbf{S}$, respectivamente; os subíndices e e o indicam que as transformadas foram construídas, respectivamente, a partir de extensões com simetria par e com simetria ímpar.

Tabela 5 – Elementos das matrizes das transformadas sobre corpos finitos do seno unitárias .

Elementos da matriz de transformação	Dimensão da matriz
$S_{1e}(k,n) = (\sqrt{2/N})\,\mathrm{sen}_\zeta(kn)$	$n,k = 1,2,\ldots,N-1$
$S_{2e}(k,n) = (\sqrt{2/N})\,\tilde{\beta}_k \mathrm{sen}_\zeta\left(k\left(n+\frac{1}{2}\right)\right)$	$n = 0,1,\ldots,N-1$ $k = 1,2,\ldots,N$
$S_{3e}(k,n) = (\sqrt{2/N})\,\tilde{\beta}_i \mathrm{sen}_\zeta\left(\left(k+\frac{1}{2}\right)n\right)$	$n = 1,2,\ldots,N$ $k = 0,1,\ldots,N-1$
$S_{4e}(k,n) = (\sqrt{2/N})\,\mathrm{sen}_\zeta\left(\left(k+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\right)$	$n,k = 0,1,\ldots,N-1$
$S_{1o}(k,n) = (2/\sqrt{2N-1})\,\mathrm{sen}_\zeta(kn)$	$n,k = 1,2,\ldots,N-1$
$S_{2o}(k,n) = (2/\sqrt{2N-1})\,\mathrm{sen}_\zeta\left(k\left(n+\frac{1}{2}\right)\right)$	$n = 0,1,\ldots,N-2$ $k = 1,2,\ldots,N-1$
$S_{3o}(k,n) = (2/\sqrt{2N-1})\,\mathrm{sen}_\zeta\left(\left(k+\frac{1}{2}\right)n\right)$	$n = 1,2,\ldots,N-1$ $k = 0,1,\ldots,N-2$
$S_{4o}(k,n) = (2/\sqrt{2N-1})\,\tilde{\gamma}_n\,\tilde{\gamma}_k \mathrm{sen}_\zeta\left(\left(k+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\right)$	$n,k = 0,1,\ldots,N-1$

Fonte: O Autor, 2019.

4 TRANSFORMADAS NUMÉRICAS MANOBRÁVEIS

Neste capítulo, é apresentada a contribuição principal deste trabalho: a definição de uma transformada numérica manobrável de Fourier (SFNT, do inglês *steerable Fourier number transform*). Essa ferramenta corresponde a uma versão definida sobre corpos finitos da transformada discreta manobrável de Fourier apresentada no Capítulo 2 (FRACASTORO; MAGLI, 2017). Aspectos relacionados ao cálculo da SFNT e de sua aplicação empregando ângulos ótimos são abordados. Além disso, é apresentada uma nova definição para a transformada numérica de Hilbert (HiNT, do inglês Hilbert number transform); a motivação para introdução da HiNT, como resultado intermediário desta tese, vem do fato de ela poder ser calculada a partir de uma SFNT definida utilizando ângulos e rotações apropriadas.

4.1 TRANSFORMADA NUMÉRICA DE FOURIER MANOBRÁVEL

O ponto de partida para a definição da SFNT é considerar um grafo em ciclo $\mathcal{C}_N$, como o apresentado na Figura 1, e avaliar a expansão espectral de sua matriz Laplaciana L sobre determinado corpo finito $\mathrm{GF}(p)$. Tal procedimento admite uma interpretação semelhante àquela considerada na definição da transformada de Fourier sobre um grafo, conforme exposto no Capítulo 2. Mais precisamente, o Laplaciano de $\mathcal{C}_N$ avaliado sobre $\mathrm{GF}(p)$ é dado pela matriz circulante

$$L(\mathcal{C}_N) = \mathrm{circ}([2 \;\; -1 \;\; \cdots \;\; -1]) \equiv \mathrm{circ}([2 \;\; p-1 \;\; \cdots \;\; p-1]) \;(\mathrm{mod}\;\; p).$$

Como consequência da propriedade de convolução cíclica da FNT (vide Capítulo 3), a sua matriz diagonaliza qualquer matriz circulante (naturalmente, com elementos no mesmo corpo em que a transformada se encontra definida) e, em particular, $L(\mathcal{C}_N)$. Assim, pode-se afirmar que as linhas de $\mathbf{F}$ constituem um conjunto ortogonal de autovetores de $L(\mathcal{C}_N)$, o que permite que se escreva

$$L(\mathcal{C}_N) = \mathbf{F}^* \mathbf{\Lambda} \mathbf{F}. \tag{4.1}$$

Na última equação, $*$ denota o tranposto conjugado da matriz $\mathbf{F}$ e $\mathbf{\Lambda}$ é uma matriz diagonal com os autovalores de $L(\mathcal{C}_N)$, os quais são calculados a seguir.

Proposição 4.1. *Os autovalores da matriz $L(\mathcal{C}_N)$ são*

$$\lambda_k = 2 - 2\cos_\zeta(k), \quad k = 0, 1, \ldots, N-1, \tag{4.2}$$

em que $\zeta \in \mathrm{GI}(p)$ é um elemento de ordem multiplicativa $\mathrm{ord}(\zeta) = N$.

Demonstração. O fato de que os autovalores de qualquer matriz circulante corresponde à transformada de Fourier de sua primeira linha é bem conhecido (BLAHUT, 2010; MERRI,

1998). Assim, para obter os λ_k, calcula-se

$$\lambda_k = \sum_{n=0}^{N-1} c(n)\zeta^{kn},$$

com $c(0) = 2$, $c(1) = c(N-1) = -1$ e $c(n) = 0$ para $n = 2, 3, \ldots, N-2$. Dessa forma, no somatório da última equação, apenas três termos serão não-nulos. Considerando a definição do cosseno sobre corpos finitos, isso fornece

$$\lambda_k = 2 - \zeta^k - \zeta^{-k} = 2 - 2\cos_\zeta(k).$$

□

Os autovalores obtidos através da Proposição 4.1 têm multiplicidades iguais a 1 ou 2. Mais especificamente, tem-se:

- Se N for ímpar, os autovalores $\lambda_k = \lambda_{N-k},\ k = 1, \ldots, \frac{N-1}{2}$, terão multiplicidade igual a 2; o autovalor λ_0 terá multiplicidade igual a 1.
- Se N for par, os autovalores $\lambda_k = \lambda_{N-k},\ k = 1, \ldots, \frac{N}{2} - 1$ terão multiplicidade igual a 2; os autovalores λ_0 e $\lambda_{\frac{N}{2}}$ terão multiplicidade igual a 1.

Como consequência do que se acabou de discutir, de modo análogo ao que se observa na construção da SDFT, os autovetores associados aos autovalores λ_k, isto é, as linhas da matriz $\mathbf{F}$, geram autoespaços com dimensão máxima igual a 2. Isso ratifica o fato de que, também no cenário de corpos finitos, as linhas de $\mathbf{F}$, denotadas por $\mathbf{v}_k$, $k = 0, 1, \ldots, N-1$, não constituem a única base de autovetores de $L(\mathcal{C}_N)$; outras dessas bases podem ser derivadas, a partir da primeira, aplicando rotações a pares de autovetores associados ao mesmo autovalor λ_k. No presente contexto, as referidas rotações são aplicadas mediante o uso das funções trigonométricas em corpos finitos, isto é, empregando o operador

$$\mathbf{R}_{\alpha_k}(\theta_k) = \begin{bmatrix} \cos_{\alpha_k}\theta_k & \mathrm{sen}_{\alpha_k}\theta_k \\ -\mathrm{sen}_{\alpha_k}\theta_k & \cos_{\alpha_k}\theta_k \end{bmatrix}, \tag{4.3}$$

em que $\alpha_k \in \mathrm{GI}(p)$ e $\theta_k \in \mathbb{Z}_{\mathrm{ord}(\alpha_k)}$[1], $k = 1, 2, \ldots, \lceil \frac{N}{2} \rceil - 1$ (não é necessário especificar os pares α_0, θ_0 e, se N for par, $\alpha_{\frac{N}{2}}, \theta_{\frac{N}{2}}$, pois λ_0 e $\lambda_{\frac{N}{2}}$ possuem multiplicidade unitária e, assim, os respectivos autovetores não são rotacionados).

Observe que os elementos α_k, em relação aos quais os cossenos e senos são calculados, podem ser distintos para diferentes valores de k e também não precisam coincidir com o elemento ζ, utilizado no núcleo da transformada numérica de Fourier que se está manobrando. Isso eleva o número de parâmetros que se pode escolher para definir uma certa SFNT. Naturalmente, se se desejar simplificar tal escolha, pode-se fazer $\alpha_k = \alpha$ ou mesmo $\alpha_k = \zeta$, $k = 1, 2, \ldots, \lceil \frac{N}{2} \rceil - 1$.

[1] $\mathbb{Z}_{\mathrm{ord}(\alpha_k)}$ denota o conjunto de inteiros módulo $\mathrm{ord}(\alpha_k)$.

Assim, dos autovetores $\mathrm{v}^{(k)}$ e $\mathrm{v}^{(N-k)}$, associados a um autovalor $\lambda_k = \lambda_{N-k}$ com multiplicidade algébrica igual a 2, obtém-se um novo par de autovetores $\mathrm{v}^{(k)'}$ e $\mathrm{v}^{(N-k)'}$ por

$$\begin{bmatrix} \mathrm{v}^{(k)'} \\ \mathrm{v}^{(N-k)'} \end{bmatrix} = \begin{bmatrix} \cos_{\alpha_k} \theta_k & \mathrm{sen}_{\alpha_k} \theta_k \\ -\mathrm{sen}_{\alpha_k} \theta_k & \cos_{\alpha_k} \theta_k \end{bmatrix} \cdot \begin{bmatrix} \mathrm{v}^{(k)} \\ \mathrm{v}^{(N-k)} \end{bmatrix}, \tag{4.4}$$

$k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$. Esse novo par de autovetores substitui o par original na composição da matriz de transformação de Fourier; os autovetores associados a autovalores com multiplicidade igual a 1 (serão, no máximo, dois desses autovetores) não são alterados. Com isso, obtém-se uma nova matriz, que é denotada por $\mathbf{F}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ e que identifica a transformada numérica de Fourier manobrável; $\boldsymbol{\theta} = (\theta_k)$, $k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$, é um vetor contendo todos os ângulos empregados nas rotações dos pares de autovetores de $\mathbf{F}$ e $\boldsymbol{\alpha} = (\alpha_k)$, $k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$, é um vetor contendo todos os elementos em relação aos quais os cossenos e senos dos referidos ângulos são calculados. A definição da SFNT é sumarizada a seguir.

Definição 4.1. Seja $\mathbf{x}$ um vetor com comprimento N e com componentes sobre $\mathrm{GI}(p)$, e seja $\mathbf{F}$ a matriz $N \times N$ de uma transformada numérica de Fourier com núcleo $\zeta \in \mathrm{GI}(p)$, em que $\mathrm{ord}(\zeta) = N$; a k-ésima linha de $\mathbf{F}$ é denotada por $\mathbf{v}^{(k)}$, $k = 0, 1, \ldots, N-1$. A transformada numérica manobrável de Fourier de $\mathbf{x}$, com ângulos de rotação $\boldsymbol{\theta} = (\theta_k)$ associados aos elementos $\boldsymbol{\alpha} = (\alpha_k)$, $k = 1, \ldots, \lceil \frac{N}{2} \rceil - 1$, generalizando a transformada à qual a matriz $\mathbf{F}$ está relacionada, é calculada por

$$\mathbf{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}} = \mathbf{F}_{\boldsymbol{\alpha},\boldsymbol{\theta}} \mathbf{x},$$

em que a k-ésima e a $(N-k)$-ésima linhas de $\mathbf{F}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ são denotadas respectivamente por $\mathbf{v}^{(k)'}$ e $\mathbf{v}^{(N-k)'}$ e calculadas de acordo com (4.4); além disso, $\mathbf{v}^{(0)'} = \mathbf{v}^{(0)}$ e, se N for par, $\mathbf{v}^{(N/2)'} = \mathbf{v}^{(N/2)}$.

A matriz $\mathbf{F}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ da SFNT pode ser decomposta como

$$\mathbf{F}_{\boldsymbol{\alpha},\boldsymbol{\theta}} = \mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}} \mathbf{F}, \tag{4.5}$$

em que $\mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ é uma matriz contendo todos os cossenos e senos sobre corpos finitos utilizados nas rotações dos pares de autovetores, tomados de operadores como aquele dado em (4.3) e convenientemente distribuídos ao longo das linhas e colunas da referida matriz.

Para N ímpar, a matriz $\mathbf{R}_{\boldsymbol{\alpha},\theta}$ tem a forma

$$\mathbf{R}_{\boldsymbol{\alpha},\theta} = \begin{bmatrix} 1 & & & & & & \\ & \cos_{\alpha_1}\theta_1 & & & & \operatorname{sen}_{\alpha_1}\theta_1 & \\ & & \ddots & & \iddots & & \\ & & & \cos_{\alpha_{\frac{N-1}{2}}}\theta_{\frac{N-1}{2}} & \operatorname{sen}_{\alpha_{\frac{N-1}{2}}}\theta_{\frac{N-1}{2}} & & \\ & & & -\operatorname{sen}_{\alpha_{\frac{N-1}{2}}}\theta_{\frac{N-1}{2}} & \cos_{\alpha_{\frac{N-1}{2}}}\theta_{\frac{N-1}{2}} & & \\ & & \iddots & & \ddots & & \\ & -\operatorname{sen}_{\alpha_1}\theta_1 & & & & \cos_{\alpha_1}\theta_1 & \\ & & & & & & 1 \end{bmatrix}. \quad (4.6)$$

Para N par, a matriz $\mathbf{R}_{\boldsymbol{\alpha},\theta}$ tem a forma

$$\mathbf{R}_{\boldsymbol{\alpha},\theta} = \begin{bmatrix} 1 & & & & & & \\ & \cos_{\alpha_1}\theta_1 & & & & \operatorname{sen}_{\alpha_1}\theta_1 & \\ & & \ddots & & \iddots & & \\ & & & \cos_{\alpha_{\frac{N}{2}-1}}\theta_{\frac{N}{2}-1} & \operatorname{sen}_{\alpha_{\frac{N}{2}-1}}\theta_{\frac{N}{2}-1} & & \\ & & & 1 & & & \\ & & & -\operatorname{sen}_{\alpha_{\frac{N}{2}-1}}\theta_{\frac{N}{2}-1} & \cos_{\alpha_{\frac{N}{2}-1}}\theta_{\frac{N}{2}-1} & & \\ & & \iddots & & \ddots & & \\ & -\operatorname{sen}_{\alpha_1}\theta_1 & & & & \cos_{\alpha_1}\theta_1 & \end{bmatrix}. \quad (4.7)$$

O cálculo da transformada numérica manobrável de Fourier $\mathbf{X}$ de um vetor $\mathbf{x}$ com comprimento N e elementos sobre um corpo finito pode, para um conjunto específico de ângulos de rotação armazenados num vetor θ, ser expresso por

$$\mathbf{X}_{\boldsymbol{\alpha},\theta} = \mathbf{F}_{\boldsymbol{\alpha},\theta}\mathbf{x} = \mathbf{R}_{\boldsymbol{\alpha},\theta}\mathbf{F}\mathbf{x}. \quad (4.8)$$

Da última equação, é possível observar que a complexidade aritmética envolvida no cálculo da SFNT pouco difere daquela envolvida no cálculo da respectiva FNT. O número de operações de adição e multiplicação necessárias ao cômputo de $\mathbf{F}\mathbf{x}$ pode ser, por exemplo, igual a $\mathcal{O}(N \log_2 N)$, se N for uma potência de 2; isso é alcançável empregando algoritmos de dizimação no tempo ou na frequência, que, embora originalmente introduzidos no contexto da transformada discreta de Fourier (OPPENHEIM; SCHAFER; BUCK, 2010), também são aplicáveis no cenário das transformadas numéricas (BLAHUT, 2010). O cálculo do produto entre $\mathbf{R}_{\boldsymbol{\alpha},\theta}$ e $\mathbf{F}\mathbf{x}$ requer, no máximo, mais $2N-2$ multiplicações e $N-1$ adições, o que significa que a complexidade aritmética total envolvida no cálculo da SFNT se mantém $\mathcal{O}(N \log_2 N)$.

A matriz da SFNT inversa $\mathbf{F}^{-1}_{\boldsymbol{\alpha},\theta}$ deve ser tal que

$$\mathbf{F}^{-1}_{\boldsymbol{\alpha},\theta}\mathbf{F}_{\boldsymbol{\alpha},\theta} = \mathbf{I},$$

em que $\mathbf{I}$ é a matriz identidade. Dessa forma, tem-se

$$\mathbf{F}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{-1} = \mathbf{F}^{-1}\mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{-1} = \mathbf{F}^{-1}\mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{T}.$$

A complexidade aritmética envolvida no cálculo da SFNT inversa é, portanto, similar àquela envolvida no cálculo da SFNT direta.

Exemplo 4.1. *Neste exemplo, define-se uma SFNT com comprimento $N = 8$ empregando o elemento $\zeta = 4 \in \mathrm{GF}(257)$. O vetor a ser transformado é*

$$\mathbf{x} = [200 \quad 41 \quad 3 \quad 101 \quad 77 \quad 8 \quad 65 \quad 250]$$

e os ângulos de rotação são $\boldsymbol{\theta} = [2 \quad 18 \quad 210]$, todos relacionados ao elemento $\alpha = \alpha_k = 191 + 225i$, $k = 1, 2, 3$. Pode-se tomar a matriz $\mathbf{F}$ da FNT do Exemplo 3.3 e calcular

$$\mathbf{X} = \mathbf{F}\mathbf{x}^T = [133 \quad 152 \quad 212 \quad 113 \quad 54 \quad 218 \quad 200 \quad 104]. \tag{4.9}$$

A matriz de rotação $\mathbf{R}_{\boldsymbol{\theta}}$ (o subíndice $\boldsymbol{\alpha}$ é omitido) foi construída a partir dos valores dos senos e cossenos dos ângulos que compõem o vetor $\boldsymbol{\theta}$ que, por sua vez, foram obtidos da Tabela 3 (página 32). Essa matriz é dada por

$$\mathbf{R}_{\boldsymbol{\theta}} = \begin{bmatrix}
1 & & & & & & & \\
& \cos_\alpha(2) & & & & & & \mathrm{sen}_\alpha(2) \\
& & \cos_\alpha(18) & & & & \mathrm{sen}_\alpha(18) & \\
& & & \cos_\alpha(210) & \mathrm{sen}_\alpha(210) & & & \\
& & & & 1 & & & \\
& & & -\mathrm{sen}_\alpha(210) & \cos_\alpha(210) & & & \\
& & -\mathrm{sen}_\alpha(18) & & & & \cos_\alpha(18) & \\
& -\mathrm{sen}_\alpha(2) & & & & & & \cos_\alpha(2)
\end{bmatrix}$$

$$= \begin{bmatrix}
1 & & & & & & & \\
& 232 & & & & & & 112 \\
& & 65 & & & & 196 & \\
& & & 85 & 98 & & & \\
& & & & 1 & & & \\
& & & -98 & 85 & & & \\
& & -196 & & & & 65 & \\
& -112 & & & & & & 232
\end{bmatrix}.$$

A SFNT é obtida calculando-se

$$\mathbf{X}_{\boldsymbol{\theta}} = \mathbf{R}_{\boldsymbol{\theta}}\mathbf{X} = [133 \quad 138 \quad 244 \quad 129 \quad 54 \quad 3 \quad 147 \quad 165].$$

4.1.1 A SFNT Bidimensional

A construção de uma SFNT bidimensional (2D-SFNT) pode ser realizada de modo análogo à da SFNT unidimensional. Para isso, considera-se o grafo resultante do produto $\mathcal{C}_{N_1} \times \mathcal{C}_{N_2}$ entre dois grafos em ciclo com N_1 e N_2 vértices, respectivamente, o qual corresponde a um grafo toroidal com $N_1 N_2$ vértices, que aqui é denotado por $\mathcal{T}_{N_1,N_2}$. Faz-se necessário avaliar de que maneira se organizam os autovetores associados a um mesmo autovalor do Laplaciano deste grafo a fim de aplicar as rotações que têm sido consideradas ao longo desta seção.

Sem perda de generalidade, considere $N = N_1 = N_2$. Dos Teoremas 2 e 3 em (FRACASTORO; MAGLI, 2017), que também são válidos no caso de corpos finitos, sabe-se que os vetores de base da 2D-FNT constituem uma base de autovetores de $L(\mathcal{T}_{N,N})$. Como consequência da forma como $\mathcal{T}_{N,N}$ é construído (produto entre dois grafos em ciclo), os autovalores do seu Laplaciano, conforme (FRACASTORO; FOSSON; MAGLI, 2017), podem ser expressos por

$$\mu_{r,s} = \mu_{s,r} = \lambda_r + \lambda_s,$$

$r, s = 0, 1, \ldots, N-1$, em que os λ_r e λ_s são os autovalores dos grafos em ciclo $\mathcal{C}_N$ (de cujo Laplaciano os vetores de base da FNT unidimensional constituem uma base de autovetores). As multiplicidades dos autovalores $\mu_{r,s}$, para N par, se enquadram, então, nos seguintes casos:

- Os autovalores $\mu_{r,s}$, em que $1 \leq r, s = 1, 2, \ldots, N/2-1$ e $r \neq s$, têm multiplicidade algébrica 8, uma vez que $\mu_{r,s} = \mu_{s,r} = \mu_{r,N-s} = \mu_{N-s,r} = \mu_{N-r,s} = \mu_{s,N-r} = \mu_{N-r,N-s} = \mu_{N-s,N-r}$;
- Os autovalores $\mu_{r,r}$, em que $r = 1, 2, \ldots, N/2-1$, têm multiplicidade algébrica 4 uma vez que $\mu_{r,r} = \mu_{r,N-r} = \mu_{N-r,r} = \mu_{N-r,N-r}$;
- Os autovalores $\mu_{r,s}$, em que $r = 0, N/2$ e $s = 1, 2, \ldots, N/2-1$ (ou $r = 1, 2, \ldots, N/2-1$ e $s = 0, N/2$), têm multiplicidade 4 uma vez que $\mu_{r,s} = \mu_{s,r} = \mu_{r,N-s} = \mu_{N-s,r}$ ($\mu_{r,s} = \mu_{s,r} = \mu_{N-r,s} = \mu_{s,N-r}$);
- Os autovalores $\mu_{0,N/2} = \mu_{N/2,0}$ têm multiplicidade 2;
- Os autovalores $\mu_{0,0}$ e $\mu_{N/2,N/2}$ têm multiplicidade 1.

Os casos para N ímpar podem ser caracterizados a partir do que já se verificou para N par. Dos casos analisados, vê-se que o espectro de $L(\mathcal{T}_{N,N})$ possui autovalores com multiplicidades maiores que 2, o que permitiria definir rotações em mais de duas dimensões. Por ora, considerar-se-ão apenas rotações em duas dimensões, como no caso da SFNT unidimensional, o que exige o agrupamento dos autovalores em duplas. Isso é conseguido considerando pares de autovalores da forma $\mu_{s,r}$ e $\mu_{r,s}$ $(r \neq s)$ e seus respectivos autovetores $\mathbf{u}^{(r,s)}$ e $\mathbf{u}^{(s,r)}$, que são vetores de base específicos da 2D-FNT com dimensão N^2; é a cada um desses pares de autovetores que é aplicada uma rotação, a fim de obter um novo par de autovetores no mesmo autoespaço. Se

as componentes dos autovetores $\mathbf{u}^{(r,s)}$ e $\mathbf{u}^{(s,r)}$ forem dispostas de forma unidimensional, como vetores-linha com dimensão $1 \times N^2$, o respectivo novo par de autovetores $\mathbf{u}^{(r,s)'}$ e $\mathbf{u}^{(s,r)'}$ é calculado por

$$\begin{bmatrix} \mathbf{u}^{(r,s)'} \\ \mathbf{u}^{(s,r)'} \end{bmatrix} = \begin{bmatrix} \cos_{\alpha_{r,s}}(\theta_{r,s}) & \text{sen}_{\alpha_{r,s}}(\theta_{r,s}) \\ -\text{sen}_{\alpha_{r,s}}(\theta_{r,s}) & \cos_{\alpha_{r,s}}(\theta_{r,s}) \end{bmatrix} \begin{bmatrix} \mathbf{u}^{(r,s)} \\ \mathbf{u}^{(s,r)} \end{bmatrix}. \tag{4.10}$$

Na última expressão, os cossenos e senos dos ângulos $\theta_{r,s}$ são calculados com relação aos elementos $\alpha_{r,s} \in \text{GI}(p)$, $r = 0, \ldots, N-2$, $s = r+1, \ldots, N-1$, isto é, até $N(N-1)/2$ ângulos podem ser especificados. Substituindo os pares originais de autovetores por aqueles resultantes das rotações, obtém-se uma nova base, à qual está associada a transformada numérica manobrável de Fourier bidimensional (os autovetores associados aos autovalores com multiplicidades iguais a 1 e aqueles identificados pelo par de índices r, s, $r = s$, não são alterados). A matriz de transformação da 2D-SFNT pode ser denotada por $\mathbf{F}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$, em que $\boldsymbol{\alpha} = (\alpha_{r,s})$ e $\boldsymbol{\theta} = (\theta_{r,s})$, $r = 0, \ldots, N-2$, $s = r+1, \ldots, N-1$.

A matriz $\mathbf{F}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ da 2D-SFNT possui dimensões $N^2 \times N^2$ e pode ser decomposta como

$$\mathbf{F}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}} = \mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}} \mathbf{F}^{(2D)}, \tag{4.11}$$

em que $\mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ é uma matriz contendo todos os cossenos e senos sobre corpos finitos utilizados nas rotações dos pares de autovetores, tomados de operadores como aquele dado em (4.3) e convenientemente distribuídos ao longo das linhas e colunas da referida matriz; $\mathbf{F}^{(2D)}$ é a matriz com dimensões também $N^2 \times N^2$ da transformada numérica de Fourier bidimensional (escrevendo dessa forma, a 2D-FNT é calculada por meio de um produto matricial entre a referida matriz e uma versão vetorizada, com dimensões $1 \times N^2$, da estrutura bidimensional cuja transformada se deseja obter).

O cálculo de $\mathbf{X}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$, que é a 2D-SFNT de uma estrutura bidimensional $\mathbf{x}$ com dimensões $N \times N$ e elementos sobre um corpo finito, pode, para um conjunto específico de ângulos de rotação armazenados em $\boldsymbol{\theta}$, ser expresso por

$$\mathbf{X}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}} = \mathbf{F}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}} \mathbf{x} = \mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}} \mathbf{F}^{(2D)} \mathbf{x}; \tag{4.12}$$

novamente, a forma como a última equação é escrita indica que os elementos de $\mathbf{x}$ estão dispostos de modo unidimensional, como um vetor coluna com comprimento N^2. De outra forma, pode-se, inicialmente, calcular a 2D-FNT de $\mathbf{x}$ (vide Capítulo 3), substituir o resultado no lugar de $\mathbf{F}^{(2D)}\mathbf{x}$ (também considerando uma disposição unidimensional dos elementos) e, finalmente, aplicar a matriz de rotações $\mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$.

Procedendo de modo análogo ao caso unidimensional, demonstra-se que a matriz da 2D-SFNT inversa $\left[\mathbf{F}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}})\right]^{-1}$ é dada por

$$\left[\mathbf{F}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}})\right]^{-1} = \left[\mathbf{F}^{(2D)}\right]^{-1} \left[\mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}\right]^{-1} = \left[\mathbf{F}^{(2D)}\right]^{-1} \left[\mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}\right]^{T}. \tag{4.13}$$

No caso da aplicação deste operador a uma estrutura bidimensional $\mathbf{X}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$, pode-se, em primeiro lugar, calcular o produto entre a matriz de rotação inversa $\left[\mathbf{R}^{(2D)}_{\boldsymbol{\alpha},\boldsymbol{\theta}}\right]^T$ e a versão vetorizada da estrutura mencionada e, em seguida, calcular a 2D-FNT inversa.

Para que a composição e a disposição dos operadores envolvidos no cálculo de uma 2D-SFNT fiquem mais claras, considere o cálculo dessa transformada com dimensões $N \times N = 4 \times 4 = 16$. Os ângulos de rotação são armazenados em $\boldsymbol{\theta} = (\theta_{r,s})$ e estão relacionados aos elementos $\boldsymbol{\alpha} = (\alpha_{r,s})$, $r = 0, \ldots, 2$, $s = r + 1, \ldots, 3$. A estrutura bidimensional $\mathbf{x} = (x_{mn})$, $m, n = 0, 1, \ldots, 3$, cuja 2D-SFNT se pretende calcular é

$$\mathbf{x} = \begin{bmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{bmatrix}. \tag{4.14}$$

A 2D-FNT de $\mathbf{x}$ é obtida por $\mathbf{X}^{(2D)} = \mathbf{F}\mathbf{x}\mathbf{F}^T$ e pode ser expressa como

$$\mathbf{X}^{(2D)} = \begin{bmatrix} X_{00} & X_{01} & X_{02} & X_{03} \\ X_{10} & X_{11} & X_{12} & X_{13} \\ X_{20} & X_{21} & X_{22} & X_{23} \\ X_{30} & X_{31} & X_{32} & X_{33} \end{bmatrix}. \tag{4.15}$$

Assumindo que a versão linearizada de $\mathbf{X}^{(2D)}$ é dada por

$$\mathbf{X}^{(2D)} = \begin{bmatrix} X_{00} \\ X_{11} \\ X_{22} \\ X_{33} \\ X_{01} \\ X_{02} \\ X_{03} \\ X_{12} \\ X_{13} \\ X_{23} \\ X_{32} \\ X_{31} \\ X_{21} \\ X_{30} \\ X_{20} \\ X_{10} \end{bmatrix}, \tag{4.16}$$

a matriz de rotações $\mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)}$ é dada por

$$\mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \begin{bmatrix} 1 & & & & & & & & & & & & \\ & 1 & & & & & & & & & & & \\ & & 1 & & & & & & & & & & \\ & & & 1 & & & & & & & & & \\ & & & & \cos_{\alpha_{0,1}}(\theta_{0,1}) & & & & & & & \operatorname{sen}_{\alpha_{0,1}}(\theta_{0,1}) & \\ & & & & & \ddots & & & & & \iddots & & \\ & & & & & & \cos_{\alpha_{2,3}}(\theta_{2,3}) & \operatorname{sen}_{\alpha_{2,3}}(\theta_{2,3}) & & & & & \\ & & & & & & -\operatorname{sen}_{\alpha_{2,3}}(\theta_{2,3}) & \cos_{\alpha_{2,3}}(\theta_{2,3}) & & & & & \\ & & & & & \iddots & & & & & \ddots & & \\ & & & & -\operatorname{sen}_{\alpha_{0,1}}(\theta_{0,1}) & & & & & & & \cos_{\alpha_{0,1}}(\theta_{0,1}) & \end{bmatrix}.$$

Assim, a versão linearizada de $\mathbf{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)}\mathbf{X}^{(2D)}$ resulta em

$$\mathbf{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \begin{bmatrix} X_{00} \\ X_{11} \\ X_{22} \\ X_{33} \\ X_{01}\cos_{\alpha_{0,1}}(\theta_{0,1}) + X_{10}\operatorname{sen}_{\alpha_{0,1}}(\theta_{0,1}) \\ X_{02}\cos_{\alpha_{0,2}}(\theta_{0,2}) + X_{20}\operatorname{sen}_{\alpha_{0,2}}(\theta_{0,2}) \\ X_{03}\cos_{\alpha_{0,3}}(\theta_{0,3}) + X_{30}\operatorname{sen}_{\alpha_{0,3}}(\theta_{0,3}) \\ X_{12}\cos_{\alpha_{1,2}}(\theta_{1,2}) + X_{21}\operatorname{sen}_{\alpha_{1,2}}(\theta_{1,2}) \\ X_{13}\cos_{\alpha_{1,3}}(\theta_{1,3}) + X_{31}\operatorname{sen}_{\alpha_{1,3}}(\theta_{1,3}) \\ X_{23}\cos_{\alpha_{2,3}}(\theta_{2,3}) + X_{32}\operatorname{sen}_{\alpha_{2,3}}(\theta_{2,3}) \\ X_{32}\cos_{\alpha_{2,3}}(\theta_{2,3}) - X_{23}\operatorname{sen}_{\alpha_{2,3}}(\theta_{2,3}) \\ X_{31}\cos_{\alpha_{1,3}}(\theta_{1,3}) - X_{13}\operatorname{sen}_{\alpha_{1,3}}(\theta_{1,3}) \\ X_{21}\cos_{\alpha_{1,2}}(\theta_{1,2}) - X_{12}\operatorname{sen}_{\alpha_{1,2}}(\theta_{1,2}) \\ X_{30}\cos_{\alpha_{0,3}}(\theta_{0,3}) - X_{30}\operatorname{sen}_{\alpha_{0,3}}(\theta_{0,3}) \\ X_{20}\cos_{\alpha_{0,2}}(\theta_{0,2}) - X_{20}\operatorname{sen}_{\alpha_{0,2}}(\theta_{0,2}) \\ X_{10}\cos_{\alpha_{0,1}}(\theta_{0,1}) - X_{10}\operatorname{sen}_{\alpha_{0,1}}(\theta_{0,1}) \end{bmatrix}, \tag{4.17}$$

a qual, reorganizada em duas dimensões, fornece

$$\mathrm{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \begin{bmatrix} X_{00} & X_{01}\cos_{\alpha_{0,1}}(\theta_{0,1}) + X_{10}\operatorname{sen}_{\alpha_{0,1}}(\theta_{0,1}) & X_{02}\cos_{\alpha_{0,2}}(\theta_{0,2}) + X_{20}\operatorname{sen}_{\alpha_{0,2}}(\theta_{0,2}) & X_{03}\cos_{\alpha_{0,3}}(\theta_{0,3}) + X_{30}\operatorname{sen}_{\alpha_{0,3}}(\theta_{0,3}) \\ X_{10}\cos_{\alpha_{0,1}}(\theta_{0,1}) - X_{10}\operatorname{sen}_{\alpha_{0,1}}(\theta_{0,1}) & X_{11} & X_{12}\cos_{\alpha_{1,2}}(\theta_{1,2}) + X_{21}\operatorname{sen}_{\alpha_{1,2}}(\theta_{1,2}) & X_{13}\cos_{\alpha_{1,3}}(\theta_{1,3}) + X_{31}\operatorname{sen}_{\alpha_{1,3}}(\theta_{1,3}) \\ X_{20}\cos_{\alpha_{0,2}}(\theta_{0,2}) - X_{20}\operatorname{sen}_{\alpha_{0,2}}(\theta_{0,2}) & X_{21}\cos_{\alpha_{1,2}}(\theta_{1,2}) - X_{12}\operatorname{sen}_{\alpha_{1,2}}(\theta_{1,2}) & X_{22} & X_{23}\cos_{\alpha_{2,3}}(\theta_{2,3}) + X_{32}\operatorname{sen}_{\alpha_{2,3}}(\theta_{2,3}) \\ X_{30}\cos_{\alpha_{0,3}}(\theta_{0,3}) - X_{30}\operatorname{sen}_{\alpha_{0,3}}(\theta_{0,3}) & X_{31}\cos_{\alpha_{1,3}}(\theta_{1,3}) - X_{13}\operatorname{sen}_{\alpha_{1,3}}(\theta_{1,3}) & X_{32}\cos_{\alpha_{2,3}}(\theta_{2,3}) - X_{23}\operatorname{sen}_{\alpha_{2,3}}(\theta_{2,3}) & X_{33} \end{bmatrix}.$$

Exemplo 4.2. *Neste exemplo, define-se uma 2D-SFNT com dimensões* $N \times N = 4 \times 4 = 16$*, empregando o elemento* $\zeta = 16 \in \mathrm{GF}(257)$*, cuja ordem multiplicativa é* $\mathrm{ord}(\zeta) = 4$*. A matriz de rotação* $\mathbf{R}_{\boldsymbol{\theta}}^{(2D)}$ *é construída a partir dos senos e cossenos dos ângulos calculados em relação ao elemento* $\alpha = \alpha_k = 191 + 225i$ *(vide Tabela 3). Os ângulos de rotação são*

$\boldsymbol{\theta} = [16 \quad 92 \quad 104 \quad 180 \quad 4 \quad 200]$ *e a estrutura bidimensional* $\mathbf{x}$ *cuja transformada se deseja calcular é*

$$\mathbf{x} = \begin{bmatrix} 1 & 130 & 80 & 45 \\ 20 & 254 & 92 & 50 \\ 46 & 78 & 99 & 160 \\ 20 & 80 & 121 & 200 \end{bmatrix}. \tag{4.18}$$

Utilizando a matriz da FNT unidimensional com núcleo $\zeta = 16$*,*

$$\mathbf{F} = \begin{bmatrix} 128 & 128 & 128 & 128 \\ 128 & 249 & 129 & 8 \\ 128 & 129 & 128 & 129 \\ 128 & 8 & 129 & 249 \end{bmatrix}, \tag{4.19}$$

calcula-se a 2D-FNT de $\mathbf{x}$ *por*

$$\mathbf{X}^{(2D)} = \mathbf{F}\mathbf{x}\mathbf{F}^T = \begin{bmatrix} 112 & 79 & 256 & 154 \\ 141 & 54 & 109 & 165 \\ 79 & 136 & 36 & 13 \\ 181 & 241 & 19 & 28 \end{bmatrix}. \tag{4.20}$$

A versão linearizada de $\mathbf{X}^{(2D)}$ *é escrita como*

$$\mathbf{X}^{(2D)} = \begin{bmatrix} 112 \\ 54 \\ 36 \\ 28 \\ 79 \\ 256 \\ 154 \\ 109 \\ 165 \\ 13 \\ 19 \\ 241 \\ 136 \\ 181 \\ 79 \\ 141 \end{bmatrix}. \tag{4.21}$$

A matriz de rotação é dada por

$$\mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 110 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 156 \\ 0 & 0 & 0 & 0 & 0 & 167 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 185 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 83 & 0 & 0 & 0 & 0 & 0 & 0 & 92 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 139 & 0 & 0 & 0 & 0 & 234 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 221 & 0 & 0 & 54 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 189 & 241 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -241 & 189 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -54 & 0 & 0 & 221 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -234 & 0 & 0 & 0 & 0 & 139 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -92 & 0 & 0 & 0 & 0 & 0 & 0 & 83 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -185 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 167 & 0 \\ 0 & 0 & 0 & 0 & -156 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 110 \end{bmatrix},$$

de modo que se tem

$$\mathbf{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} \mathbf{X}^{(2D)} = \begin{bmatrix} 112 \\ 54 \\ 36 \\ 28 \\ 103 \\ 56 \\ 136 \\ 201 \\ 135 \\ 97 \\ 201 \\ 147 \\ 80 \\ 84 \\ 14 \\ 102 \end{bmatrix}. \tag{4.22}$$

Reorganizando $\mathbf{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)}$ *como uma estrutura bidimensional, obtém-se*

$$\mathbf{X}_{\boldsymbol{\alpha},\boldsymbol{\theta}}^{(2D)} = \begin{bmatrix} 112 & 103 & 56 & 136 \\ 102 & 54 & 201 & 135 \\ 14 & 80 & 36 & 97 \\ 84 & 147 & 201 & 28 \end{bmatrix}, \tag{4.23}$$

que é a 2D-SFNT de $\mathbf{x}$.

4.2 ÂNGULO ÓTIMO

Conforme exposto na última seção, o cálculo de uma SFNT pode ser visto como a aplicação de rotações a vetores, ou pares de coeficientes de uma FNT, em espaços bidimensionais. Em função disso, é possível escolher tais ângulos de modo que um coeficiente em cada um dos referidos pares seja anulado; esses são os chamados ângulos ótimos. Esta ideia foi explorada no contexto da transformada discreta manobrável do cosseno, em (FRACASTORO; FOSSON; MAGLI, 2017), com a finalidade de realizar compressão de imagens e vídeos. Mais especificamente, no referido artigo, os autores propõem estratégias que permitem diminuir a taxa em bits por pixel de codificação de uma imagem (ou vídeo), informando, na verdade, ângulos de rotação sub-ótimos, que fazem com que um coeficiente em cada par de coeficientes rotacionado se aproxime de zero, o que proporciona uma representação mais esparsa no domínio da transformada.

No presente cenário, imagina-se que possíveis aplicações do uso de ângulos ótimos no cálculo da SFNT se encontrem num escopo diferente do descrito acima; tal suposição se deve ao fato de que, à medida em que um coeficiente é anulado (e seu valor não precisa ser informado a um decodificador, onde a transformada inversa é calculada), é necessário, em contrapartida, informar sem erro o ângulo utilizado para alcançar tal resultado, pois o fato de se estar empregando operações aritméticas módulo p não viabiliza resultados aproximados (referidos acima como sub-ótimos). Em todo caso, o ângulo ótimo relacionado a um par de coeficientes X_1 e X_2 de uma transformada numérica de Fourier pode ser definido como

$$\theta^{(\text{opt})} = \arctan_\alpha\left(\frac{X_2}{X_1}\right). \tag{4.24}$$

Observe que, considerando a função tangente sobre corpos finitos inversa e a Proposição 3.4 (vide Capítulo 3), garante-se que, se α for um elemento com ordem multiplicativa $\operatorname{ord}(\alpha) = 2(p+1)$, o ângulo ótimo será sempre calculável, para quaisquer valores $X_1, X_2 \in \mathrm{GF}(p)$. Empregando a matriz de rotação sobre corpos finitos que tem sido considerada neste capítulo, verifica-se facilmente que a versão rotacionada de X_2 será $X_2' = 0$, ao passo em que X_1', a versão rotacionada de X_1, pode permanecer não-nula.

Exemplo 4.3. *Neste exemplo, define-se uma SFNT a partir de uma FNT cujo núcleo é o elemento* $\zeta = 4 \in \mathrm{GF}(257)$*, tal que* $\operatorname{ord}(\zeta) = 8$*. A ideia é ilustrar o emprego de ângulos ótimos na matriz de rotação para obtenção da transformada de*

$$\mathbf{x} = [200 \quad 41 \quad 3 \quad 101 \quad 77 \quad 8 \quad 65 \quad 250].$$

A FNT de $\mathbf{x}$ *é dada por*

$$\mathbf{X} = [171 \quad 36 \quad 113 \quad 138 \quad 223 \quad 103 \quad 128 \quad 17].$$

Os ângulos ótimos são, então, o resultado da função tangente sobre corpos finitos inversa avaliada em

$$17(36)^{-1} \equiv 79 \,(\mathrm{mod}\, 257), \quad 128(113)^{-1} \equiv 199 \,(\mathrm{mod}\, 257) \quad \textit{e} \quad 103(138)^{-1} \equiv 92 \,(\mathrm{mod}\, 257).$$

Empregando o elemento $\alpha = \alpha_k = 191 + 225i$, pode-se recorrer à Tabela 3 para obter os valores dos ângulos ótimos; estes são armazenados em

$$\theta = [111 \quad 146 \quad 56],$$

o que fornece a matriz de rotações

$$\mathbf{R}_\theta = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 52i & 0 & 0 & 0 & 0 & 0 & 253i \\ 0 & 0 & 169 & 0 & 0 & 0 & 221 & 0 \\ 0 & 0 & 0 & 78 & 0 & 237 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -237 & 0 & 78 & 0 & 0 \\ 0 & 0 & -221 & 0 & 0 & 0 & 169 & 0 \\ 0 & -253i & 0 & 0 & 0 & 0 & 0 & 52i \end{bmatrix}. \tag{4.25}$$

Daí, obtém-se a SFNT de $\mathbf{x}$*, que é dada por*

$$\mathbf{X}_\theta = \mathbf{R}_\theta \mathbf{X}^T = [171 \quad 5i \quad 97 \quad 223 \quad 223 \quad 0 \quad 0 \quad 0].$$

Exemplo 4.4. *Neste exemplo, define-se uma 2D-SFNT com dimensões $N \times N = 4 \times 4 = 16$, com base nos dados do Exemplo 4.2. Mais uma vez, a ideia é ilustrar como são obtidos os ângulos ótimos que serão utilizados na matriz de rotação para obtenção da transformada da estrutura bidimensional* $\mathbf{x}$ *dada em (4.18). De (4.20), sabe-se que os ângulos ótimos são o resultado da função tangente sobre corpos finitos inversa avaliada em*

$$141(79)^{-1} \equiv 223 \,(\mathrm{mod}\, 257), \quad 79(256)^{-1} \equiv 178 \,(\mathrm{mod}\, 257), \quad 181(154)^{-1} \equiv 123 \,(\mathrm{mod}\, 257),$$

$$136(109)^{-1} \equiv 138 \,(\mathrm{mod}\, 257), \quad 241(165)^{-1} \equiv 246 \,(\mathrm{mod}\, 257) \quad e \quad 19(13)^{-1} \equiv 41 \,(\mathrm{mod}\, 257),$$

Empregando o elemento $\alpha = \alpha_k = 191 + 225i$, pode-se recorrer à Tabela 3 para obter os valores dos ângulos ótimos, os quais são dados respectivamente por

$$59, \quad 147, \quad 93, \quad 139, \quad 225, \quad e \quad 32.$$

Assim, a matriz de rotação é dada por

$$\mathbf{R}_{\theta}^{(2D)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 92i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 213i \\ 0 & 0 & 0 & 0 & 0 & 205i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 253i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 78i & 0 & 0 & 0 & 0 & 0 & 0 & 85i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 54i & 0 & 0 & 0 & 0 & 256i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 51i & 0 & 0 & 210i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 139 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -139 & 41 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -210i & 0 & 0 & 51i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -256i & 0 & 0 & 0 & 0 & 54i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -85i & 0 & 0 & 0 & 0 & 0 & 0 & 78i & 0 & 0 \\ 0 & 0 & & 0 & 0 & -253i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 205i & 0 \\ 0 & 0 & 0 & 0 & -213i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 92i \end{bmatrix}$$

e o resultado da sua multiplicação pela versão linearizada de $\mathbf{X}^{(2D)}$ *fornece*

$$\mathbf{X}_{\theta}^{(2D)} = \mathbf{R}_{\theta}^{(2D)}\mathbf{X}^{(2D)} = \begin{bmatrix} 112 \\ 54 \\ 36 \\ 28 \\ 36i \\ 250i \\ 155i \\ 96i \\ 172i \\ 90 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{4.26}$$

Reorganizando $\mathbf{X}_{\theta}^{(2D)}$ *como uma estrutura bidimensional, obtém-se*

$$\mathbf{X}_{\alpha,\theta}^{(2D)} = \begin{bmatrix} 112 & 36i & 250i & 155i \\ 0 & 54 & 96i & 172i \\ 0 & 0 & 36 & 90 \\ 0 & 0 & 0 & 28 \end{bmatrix}. \tag{4.27}$$

4.3 A TRANSFORMADA NUMÉRICA DE HILBERT

Nesta seção, apresenta-se uma nova definição para a transformada numérica de Hilbert (HiNT, do inglês *Hilbert number transform*). A abordagem proposta é uma espécie de versão sobre corpos finitos da transformada discreta de Hilbert como definida em (OPPENHEIM; SCHAFER; BUCK, 2010). Esta última, por sua vez, corresponde a uma extensão bastante intuitiva da transformada de Hilbert para sinais de tempo contínuo (COHEN et al., 2010). A versão anteriormente proposta, em (KAK, 2014), é uma versão sobre corpos finitos da transformada discreta de Hilbert como definida em (KAK, 1970). Inicialmente, define-se o que seria o sinal analítico de um vetor $\mathbf{x}$ no presente contexto:

Definição 4.2. Seja $\mathbf{X} = (X(k))$, $X(k) \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, a transformada numérica de Fourier do vetor $\mathbf{x} = (x(n))$, $x(n) \in \mathrm{GF}(p)$, $n = 0, 1, \ldots, N-1$. O sinal analítico de $\mathbf{x}$, denotado por $\mathbf{X}_{a,c}$ é o sinal cujas componentes são dadas por

$$X_{a,c}(k) = \begin{cases} 2X(k), & k = 1 \ldots, \frac{N}{2} - 1, \\ X(k), & k = 0, \frac{N}{2}, \\ 0, & k = \frac{N}{2} + 1, \ldots, N-1, \end{cases} \tag{4.28}$$

para N par.

O sinal analítico é, então, usado para definir a transformada numérica de Hilbert como a seguir.

Definição 4.3. Seja $\mathbf{x}_{a,c} = \Re\{\mathbf{x}_{a,c}\} + \Im\{\mathbf{x}_{a,c}\}i = (x_{a,c}(n))$, $x_{a,c}(n) \in \mathrm{GI}(p)$, $n = 0, 1, \ldots, N-1$, a transformada numérica de Fourier inversa de $\mathbf{X}_{a,c} = (X_{a,c}(k))$, $X_{a,c}(k) \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, o sinal analítico de $\mathbf{x}$. A transformada numérica de Hilbert de $\mathbf{x}$ corresponde a $\mathbf{X}_h = \Im\{\mathbf{x}_{a,c}\}$.

Exemplo 4.5. *Neste exemplo, ilustra-se a definição de uma transformada numérica de Hilbert de comprimento* 8 *sobre* $\mathrm{GF}(7)$. *Inicialmente, constrói-se uma transformada numérica de Fourier*

usando $\zeta = 2 + 2i \in \mathrm{G}_{1,7}$, $i = \sqrt{-1}$, *como núcleo. A matriz da FNT é, então, dada por*

$$\mathbf{F} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2+2i & i & 5+2i & 6 & 5+5i & 6i & 2+5i \\ 1 & i & 6 & 6i & 1 & i & 6 & 6i \\ 1 & 5+2i & 6i & 2+2i & 6 & 2+5i & i & 5+5i \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5+5i & i & 2+5i & 6 & 2+2i & 6i & 5+2i \\ 1 & 6i & 6 & i & 1 & 6i & 6 & i \\ 1 & 2+5i & 6i & 5+5i & 6 & 5+2i & i & 2+2i \end{bmatrix} \tag{4.29}$$

e a matriz da FNT inversa é

$$\mathbf{F}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2+5i & 6i & 5+5i & 6 & 5+2i & 1i & 2+2i \\ 1 & 6i & 6 & i & 1 & 6i & 6 & i \\ 1 & 5+5i & i & 2+5i & 6 & 2+2i & 6i & 5+2i \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5+2i & 6i & 2+2i & 6 & 2+5i & i & 5+5i \\ 1 & i & 6 & 6i & 1 & i & 6 & 6i \\ 1 & 2+2i & i & 5+2i & 6 & 5+5i & 6i & 2+5i \end{bmatrix}. \tag{4.30}$$

A FNT do vetor

$$\mathbf{x} = [1 \quad 3 \quad 0 \quad 5 \quad 5 \quad 3 \quad 6i \quad 4] \tag{4.31}$$

é dada por

$$\mathbf{X} = [6 \quad 1+3i \quad 4i \quad 5+i \quad 4 \quad 5+6i \quad 3i \quad 1+4i]. \tag{4.32}$$

Observe que as simetrias das partes real e imaginária de $\mathbf{X}$ *estão de acordo com o que é estabelecido na Proposição 3.5. O sinal analítico relacionado a* $\mathbf{x}$ *é, assim, dado por*

$$\mathbf{X}_{a,c} = [6 \quad 2+6i \quad i \quad 3+2i \quad 4 \quad 0 \quad 0 \quad 0], \tag{4.33}$$

o qual possui

$$\mathbf{x}_{a,c} = [1+2i \quad 3+5i \quad 0 \quad 5+3i \quad 5 \quad 3+2i \quad 6+5i \quad 4+4i] \tag{4.34}$$

como sua FNT inversa. A HiNT de $\mathbf{x}$ *é, portanto,*

$$\mathbf{X}_h = \Im\{\mathbf{x}_{a,c}\} = [2 \quad 5 \quad 0 \quad 3 \quad 0 \quad 2 \quad 5 \quad 4]. \tag{4.35}$$

4.3.1 Definindo a HiNT a partir da SFNT

Alternativamente, a transformada numérica de Hilbert pode ser calculada usando a transformada numérica de Fourier manobrável. Mais especificamente, a seguinte proposição é válida.

Proposição 4.2. *Seja $\alpha \in \mathrm{GI}(p)$ um elemento tal que $8|\mathrm{ord}(\alpha)$ e seja $\theta = \frac{\mathrm{ord}(\alpha)}{8}$. A transformada numérica de Hilbert de $\mathbf{x} \in \mathrm{GI}(p)$ pode ser calculada de acordo com*

$$\mathbf{X}_h = \mathfrak{I}\left\{\widetilde{\mathbf{F}}^H_{\boldsymbol{\alpha},\boldsymbol{\theta}}\mathbf{F}_{\boldsymbol{\alpha},-\boldsymbol{\theta}}\mathbf{x}\right\}, \tag{4.36}$$

em que $\boldsymbol{\alpha}$ e $\boldsymbol{\theta}$ denotam, respectivamente, os vetores α e θ, constantes e de comprimento $\lceil N/2-1 \rceil$, tendo α e θ como suas componentes, o símbolo $\widetilde{}$ em $\widetilde{\mathbf{F}}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$ indica que esta matriz é calculada considerando o operador de rotação imprópria em corpos finitos

$$\widetilde{\mathbf{R}}_\alpha(\theta) = \begin{bmatrix} \cos_\alpha\theta & \sin_\alpha\theta \\ \sin_\alpha\theta & -\cos_\alpha\theta \end{bmatrix} \tag{4.37}$$

e $\{\cdot\}^H$ denota a transposição Hermitiana do argumento.

Demonstração. Sem perda de generalidade, assumamos que N é par. Pode-se escrever

$$\widetilde{\mathbf{F}}^H_{\boldsymbol{\alpha},\boldsymbol{\theta}} = \left[\begin{bmatrix} 1 & & & & & & & & \\ & \cos_\alpha\theta & & & & & & \sin_\alpha\theta & \\ & & \ddots & & & & \iddots & & \\ & & & \cos_\alpha\theta & & \sin_\alpha\theta & & & \\ & & & & 1 & & & & \\ & & & \sin_\alpha\theta & & -\cos_\alpha\theta & & & \\ & & \iddots & & & & \ddots & & \\ & \sin_\alpha\theta & & & & & & -\cos_\alpha\theta & \end{bmatrix}\mathbf{F}\right]^H$$

$$= \mathbf{F}^H \begin{bmatrix} 1 & & & & & & & & \\ & \cos_\alpha\theta & & & & & & \sin_\alpha\theta & \\ & & \ddots & & & & \iddots & & \\ & & & \cos_\alpha\theta & & \sin_\alpha\theta & & & \\ & & & & 1 & & & & \\ & & & \sin_\alpha\theta & & -\cos_\alpha\theta & & & \\ & & \iddots & & & & \ddots & & \\ & \sin_\alpha\theta & & & & & & -\cos_\alpha\theta & \end{bmatrix}.$$

Seja $\mathbf{X}$ a FNT de $\mathbf{x}$. Observando que $\cos_\alpha(-\theta) = \cos_\alpha\theta$ e $\sin_\alpha(-\theta) = -\sin_\alpha\theta$, também se pode escrever

$$\mathbf{F}_{\boldsymbol{\alpha},-\boldsymbol{\theta}}\mathbf{x} = \begin{bmatrix} 1 & & & & & & & \\ & \cos_\alpha\theta & & & & & & -\sin_\alpha\theta \\ & & \ddots & & & & \iddots & \\ & & & \cos_\alpha\theta & & -\sin_\alpha\theta & & \\ & & & & 1 & & & \\ & & & \sin_\alpha\theta & & \cos_\alpha\theta & & \\ & & \iddots & & & & \ddots & \\ & \sin_\alpha\theta & & & & & & \cos_\alpha\theta \end{bmatrix} \begin{bmatrix} X(0) \\ X(1) \\ \vdots \\ X(N-2) \\ X(N-1) \end{bmatrix}.$$

Usando (3.3) e assumindo que $\mathbf{y} = \widetilde{\mathbf{F}}^H_{\boldsymbol{\alpha},\boldsymbol{\theta}}\mathbf{F}_{\boldsymbol{\alpha},-\boldsymbol{\theta}}\mathbf{x}$, tem-se

$$\begin{aligned} \mathbf{y} &= \mathbf{F}^H \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & -1 & & \\ & & & & & \ddots & \\ & & & & & & -1 \end{bmatrix} \begin{bmatrix} X(0) \\ X(1) \\ \vdots \\ X(N-2) \\ X(N-1) \end{bmatrix} \\ &= \mathbf{F}^H \begin{bmatrix} X(0) \\ \vdots \\ X\left(\frac{N}{2}\right) \\ -X\left(\frac{N}{2}+1\right) \\ \vdots \\ -X(N-1) \end{bmatrix}. \end{aligned}$$

Definindo $\mathbf{X}' = [X(0) \ \ldots \ X\left(\frac{N}{2}\right) \ -X\left(\frac{N}{2}+1\right) \ldots \ -X(N-1)]$ e assumindo que a FNT considerada em nosso desenvolvimento é definida usando um elemento ω como núcleo, da última equação, a n-ésima componente de $\mathbf{y}$ pode ser expressa como

$$\begin{aligned} y(n) &= \sum_{k=0}^{N-1} X'(k)\omega^{-kn} \\ &= X'(0) + (-1)^n X'(N/2) + \sum_{k=1}^{N/2-1} X'(k)\omega^{-kn} + \sum_{k=N/2+1}^{N-1} X'(k)\omega^{-kn}. \end{aligned}$$

Após a realização de uma substituição de variável no segundo somatório, a última equação pode ser reescrita como

$$y(n) = X'(0) + (-1)^n X'(N/2) + \sum_{k=1}^{N/2-1} \left[X'(k)\omega^{-kn} + X'(N-k)\omega^{kn}\right].$$

Devido à Proposição 3.5, sabe-se que $X'(N-k) = -X'^{*}(k)$. Além disso, para $k = 0, \ldots, N/2$, tem-se $X(k) = X'(k)$. Portanto, a última equação pode ser reescrita como

$$\begin{aligned} y(n) &= X'(0) + (-1)^n X'(N/2) + \sum_{k=1}^{N/2-1} \left[X'(k)\omega^{-kn} - \left(X'(k)\omega^{-kn}\right)^*\right] \\ &= X(0) + (-1)^n X(N/2) + \sum_{k=1}^{N/2-1} 2\Im\left\{X(k)\omega^{-kn}\right\} i \end{aligned}$$

e, consequentemente, sua parte imaginária é dada por

$$\Im\{y(n)\} = \sum_{k=1}^{N/2-1} 2\Im\left\{X(k)\omega^{-kn}\right\}.$$

Por outro lado, considerando a Definição 4.2, as componentes da FNT inversa do sinal analítico de $\mathbf{x}$ podem ser expressas como

$$\begin{aligned} x_{a,c}(n) &= \sum_{k=0}^{N-1} X_{a,c}(k)\omega^{-kn} = \sum_{k=0}^{N/2} X_{a,c}(k)\omega^{-kn} \\ &= X(0) + (-1)^n X(N/2) + \sum_{k=1}^{N/2-1} 2X(k)\omega^{-kn}. \end{aligned}$$

Uma vez que a parte imaginária de $x_{a,c}(n)$ coincide com a de $y(n)$, para $n = 0, \ldots, N-1$, a proposição é satisfeita. □

Até o momento em que se finalizou a escrita desta tese, não haviam sido investigadas aplicações da transformada numérica de Hilbert proposta. Pretende-se realizar tal investigação em trabalhos futuros, juntamente com uma caracterização mais ampla da HiNT e com o estabelecimento de suas propriedades.

5 APLICAÇÃO DA TRANSFORMADA NUMÉRICA DE FOURIER MANOBRÁVEL

Neste capítulo, é discutida a aplicação da SFNT em cifragem de imagens. Mais especificamente, introduz-se um esquema de criptografia de imagens cuja base é uma versão bidimensional da transformação proposta; as propriedades do método são discutidas e seu desempenho é comparado ao de outras técnicas neste cenário. A escolha dessa aplicação para investigar o uso prático da SFNT foi motivada, principalmente, pelo crescente interesse, nas últimas décadas, no desenvolvimento de técnicas para proteção multimídia, entre as quais se encontram os esquemas de criptografia (TAMORI; AOKI; YAMAMOTO, 2002; CINTRA et al., 2009; LIMA; NOVAES, 2014; LIMA; SOUZA; LIMA, 2014; LIMA; MADEIRO; SALES, 2015; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017).

Como exemplos de esquemas de cifragem de imagens recentemente propostos, podem ser brevemente descritos os seguintes. Em (HUA; ZHOU, 2017), uma cifra que utiliza filtragem de imagem e criptografia baseada em blocos é introduzida; o método emprega máscaras geradas aleatoriamente e a operação de filtragem de imagens para espalhar pequenas alterações nas imagens para os *pixels* da imagem cifrada. Em (HUA et al., 2018), os autores apresentam um algoritmo de criptografia de imagens baseado em um mapa bidimensional de acoplamento senoidal; também são desenvolvidos um novo método para permutar rapidamente os *pixels* da imagem e um algoritmo de difusão para espalhamento de pequenas alterações na imagem cifrada resultante. Em (HUA; YI; ZHOU, 2018), é descrito um esquema de criptografia para proteger imagens médicas usando embaralhamento de alta velocidade e difusão adaptativa dos *pixels*; tal método provê resultados que satisfazem diversos requisitos de segurança associados ao fato de que se permite cifrar uma mesma imagem em diferentes imagens cifradas, mesmo quando se está usando a mesma chave secreta.

O esquema de criptografia de imagens proposto nesta tese pode ser melhor comparado àqueles que também utilizam uma transformação linear em uma das etapas do processo de cifragem. A ideia principal por trás desse tipo de esquema é empregar, entre outros blocos construtivos, uma transformação discreta parametrizável cuja matriz muda de acordo com uma chave secreta. A classe de transformadas mais conhecida nesse contexto é a das transformadas fracionárias. Tais transformadas correspondem a uma generalização das transformadas ordinárias correspondentes, em que uma potência arbitrária do operador matricial de transformação pode ser computada. Em (ANNABY; RUSHDI; NEHARY, 2016), por exemplo, os autores propõem um esquema de criptografia de imagens baseado em transformadas discretas de Fourier fracionárias geradas por matrizes aleatórias. Em (KANG; TAO, 2018), uma transformada fracionária de Hartley de múltiplos parâmetros é definida e um esquema de criptografia de imagem coloridas baseado em tal ferramenta é proposto; os autores demonstram que o seu algoritmo é simples, seguro, sensível a mudanças nas chaves e robusto a possíveis ataques. Em (KANG; MING; TAO,

2018), sugere-se uma técnica similar baseada em uma transformada angular discreta fracionária de múltiplos parâmetros. Outros esquemas baseados em transformadas fracionárias são descritos em (KANG; ZHANG; TAO, 2015; GAO et al., 2018; ZHAO et al., 2016; YOUSSEF, 2008). Além de atender aos diversos requisitos de segurança, mostra-se que o esquema proposto nesta tese fornece benefícios relacionados à complexidade aritmética, quando comparado àqueles baseados em transformadas fracionárias complexas ou reais, além de utilizar um número reduzido de etapas no processo de cifragem.

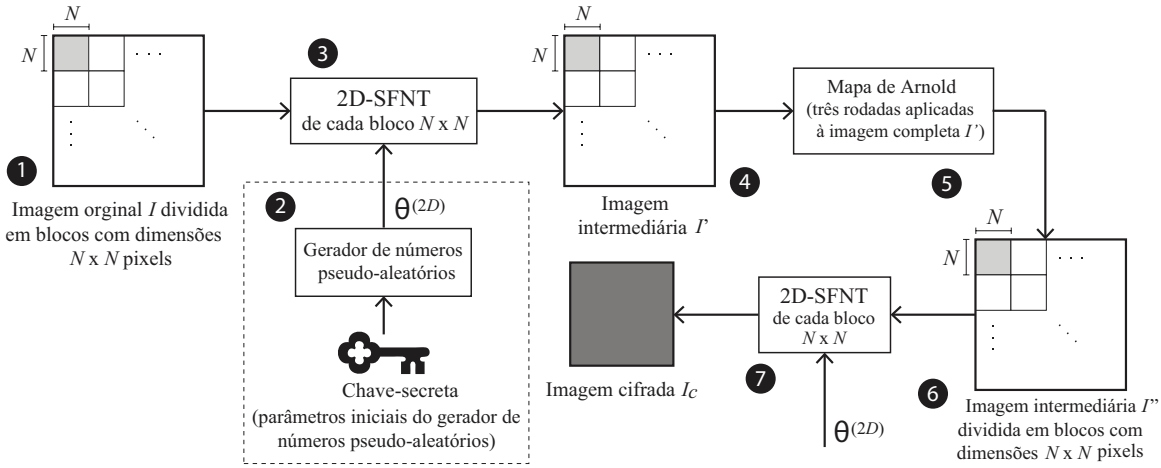
5.1 ESQUEMA PROPOSTO

A transformada numérica manobrável de Fourier utilizada no esquema proposto é a bidimensional, uma vez que se está interessado em aplicá-la a imagens. Assume-se que a 2D-SFNT será aplicada a uma imagem digital quadrada e que os ângulos de rotação usados na definição da transformada podem ser escolhidos arbitrariamente ou, no contexto de cifragem, ser determinados por uma chave secreta. Deve-se escolher o valor do número primo p, que caracteriza o corpo finito $\mathrm{GF}(p)$ em que a 2D-SFNT é definida. Os *pixels* das imagens assumem valores inteiros entre $[P_{min}$,$P_{max}]$ e, a partir destes valores, pode-se escolher $p \geq P_{max} - P_{min} + 1$. Este critério de escolha de p evita que dois diferentes valores sejam tratados como sendo o mesmo, após a redução módulo p. Os parâmetros P_{min} e P_{max} são públicos e devem ser armazenados para permitir a correta reconstrução da imagem após a aplicação da transformada inversa. Neste capítulo, tem-se $p = 257$, considerando que se vai tratar imagens em escala de cinza com *pixels* codificados em 8 bits, isto é, assumindo valores inteiros no intervalo $[0, 255]$. Todavia, a condição geral de escolha de p descrita acima é importante, pois há classes de imagens em que tal faixa de valores pode ser bem mais ampla; é o caso, por exemplo, de imagens médicas armazenadas no formato DICOM (DICOM, 2019). A definição propriamente dita da 2D-SFNT sobre $\mathrm{GF}(p)$ requer, ainda, escolher $\zeta \in \mathrm{GF}(p)$, cuja ordem é $\mathrm{ord}(\zeta) = N$. Isto determina o tamanho $N \times N$ da transformada e, consequentemente, as dimensões das imagens ou dos blocos de imagens a serem processadas.

O esquema proposto emprega ângulos (em corpos finitos) armazenados no vetor $\boldsymbol{\theta}^{(2D)}$ e gerados utilizando-se uma chave secreta. O procedimento para cifragem de uma imagem I é descrito no diagrama de blocos da Figura 3 e inclui os seguintes passos:

1. Dividir I em blocos com dimensões $N \times N$ *pixels*;
2. Usar uma chave secreta para gerar o vetor $\boldsymbol{\theta}^{(2D)}$ de comprimento $N(N-1)/2$;
3. Calcular a 2D-SFNT de cada bloco da imagem I utilizando o vetor $\boldsymbol{\theta}^{(2D)}$ gerado no passo 2;
4. Obter uma imagem intermediária I' proveniente dos blocos transformados no passo 3;

Figura 3 – Diagrama de bloco do esquema de criptografia proposto com os números de cada passo da cifragem.



Fonte: O Autor, 2019.

5. Embaralhar os *pixels* de I' aplicando três rodadas da transformada de Arnold (*Arnold cat map*) (CHEN et al., 2013), obtendo como resultado a segunda imagem intemediária I'';

6. Dividir I'' em blocos com dimensões $N \times N$ *pixels*;

7. Computar a 2D-SFNT de cada bloco de I'' usando o mesmo vetor $\theta^{(2D)}$ e obter a imagem cifrada I_c.

Os dois princípios relacionados à segurança de criptossistemas de chave-secreta, difusão e a confusão (SHANNON, 1949), são contemplados ao longo das etapas descritas (a difusão está relacionada à redução da redundância da informação e a confusão objetiva tornar mais complexa a relação entre o texto claro e o cifrado). No esquema proposto, a aplicação da 2D-SFNT a blocos das imagens provê confusão e a aplicação da transformada de Arnold à imagem intermediária I' completa, combinada com uma nova etapa de transformação pela 2D-SFNT, provê difusão ao esquema; a permutação entre as posições de *pixels* de blocos diferentes na imagem intermediária I' utilizando o mapa de Arnold (passo 5 da Figura 3), antes da segunda rodada de transformação com a 2D-SFNT, faz com que o esquema seja não-linear. A decifragem é realizada quando se aplica os passos anteriormente descritos na ordem inversa, ou seja, do passo 7 ao 1, utilizando a 2D-SFNT inversa nos passos 7 e 3 e a transfomação inversa de Arnold no passo 5.

No esquema proposto, é definido que uma chave-secreta é usada para gerar o vetor $\theta^{(2D)}$ que contém ângulos em corpo finito (ver o passo 2). Entretanto, tal vetor pode não ser adequado para ser usado diretamente como a chave do esquema. Se $N = 128$, por exemplo, $\theta^{(2D)}$ deveria ter $128 \times 127/2 = 8.128$ componentes; se cada um desses componentes pertencer ao intervalo $[0, 127]$, $\theta^{(2D)}$ seria representado por $8.128 \times \log_2 128 = 8.128 \times 7 = 56.896$ ***bits***, que é um número muito grande para ser armazenado e compartilhado, quando comparado com outros esquemas de criptografia simétrica (SMART, 2012). Assim, na prática, $\theta^{(2D)}$ pode ser obtido usando-se geradores de números aleatórios baseados em caos (STOJANOVSKI; PIHL;

KOCAREV, 2001; STOJANOVSKI; KOCAREV, 2001; BEIRAMI; NEJATI; CALLEGARI, 2014; LIU; MIAO, 2016). Tem-se mostrado que, entre outras propriedades, tais geradores são altamente sensíveis às suas condições iniciais, o que constitui uma característica essencial para sua utilização como chave-secreta. Além disso, estes geradores fornecem um tamanho adequado para o espaço de chaves, sendo apropriados para fins criptográficos. Para ser mais específico, consideraremos como exemplo o gerador caótico H-SSP (*hyperchaos with self-shrinking perturbance*) dado em (LIU; MIAO, 2016); a cardinalidade de seu espaço de chaves é $\sim 2^{M+13P}$, em que M é o número de registros e P é a precisão usada no processo de geração. Escolher os parâmetros M e P de modo que se tenha $M + 13P > 256$ é suficiente para produzir um vetor $\theta^{(2D)}$ seguro.

5.2 EXPERIMENTOS COMPUTACIONAIS E ANÁLISE DE SEGURANÇA

Nos experimentos realizados, foram cifradas 141 imagens em escala de cinza com dimensões 512×512 *pixels* [1]. Foi considerado o corpo finito $\mathrm{GF}(257)$ porque $p = 257$ é o menor primo que contempla o intervalo $[0, 255]$. Foram escolhidos $N = \mathrm{ord}(\zeta) = 128$ e o elemento $\zeta = \alpha = \alpha_k = 9$ para calcular as funções trigonométricas do corpo finito e definir as transformações necessárias nos passos de cifragem / decifragem da imagem[2]. O vetor $\theta^{(2D)}$ foi gerado aleatoriamente e tem $128 \times \frac{127}{2} = 8.128$ componentes inteiros pertencentes ao intervalo $[0, 127]$.

O comportamento estatístico das imagens cifradas pode ser avaliado pelo cálculo do coeficiente de correlação entre dois *pixels* adjacentes (a adjacência pode ser horizontal, vertical ou diagonal) e pelo cálculo da entropia. O cômputo do coeficiente de correlação é feito por meio da seleção aleatória de P *pixels* da imagem a partir de (AKHSHANI et al., 2010)

$$r_{xy} = \frac{\mathrm{Cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{5.1}$$

em que

$$\mathrm{Cov}(x, y) = \frac{1}{P}\sum_{i=1}^{P}(x_i - E(x))(y_i - E(y)), \tag{5.2}$$

$$\mathrm{D}(x) = \frac{1}{P}\sum_{i=1}^{P}(x_i - E(x))^2, \tag{5.3}$$

e

$$\mathrm{E}(x) = \frac{1}{P}\sum_{i=1}^{P} x_i; \tag{5.4}$$

[1] As imagens foram obtidas do banco de dados de imagens USC-SIPI, volumes *Textures*, *Aerials* e *Miscellaneous*, e convertidos para o formato mencionado (USC-SIPI,).

[2] Imagens de um tamanho diferente de 512×512 podem ser cifradas combinando preenchimento com zeros e o uso de blocos de imagem (e também 2D-SFNT) com dimensões diferentes de 128×128.

x_i é o valor do i-ésimo *pixel* selecionado e y_i é o valor do *pixel* adjacente correspondente. Espera-se que uma imagem, antes de ser submetida à cifragem baseada na 2D-SFNT, tenha coeficiente de correlação próximo de 1 e, após o processo de cifragem, tenha coeficiente de correlação o mais próximo possível de 0.

O cálculo das entropias das imagens é realizado avaliando-se o número de diferentes valores que os p *pixels* da imagem podem assumir. Denotando por N_i a quantidade de *pixels* da imagem que assumem o valor $i = 0, 1, \ldots, p-1$ e por N^2 o número total de *pixels* da imagem, a entropia da imagem é calculada por

$$H = \sum_{i=0}^{p-1} \frac{N_i}{N} \log_2 \frac{N}{N_i}. \tag{5.5}$$

Como nos experimentos realizados tem-se $p = 257$, o valor máximo da entropia de uma imagem transformada seria $\log_2 257$ [3]. Assim, para facilitar a avaliação do que seria uma entropia elevada (ou baixa), define-se uma entropia normalizada $\overline{H}$ que é dada por (YANG et al., 2015; LIMA; MADEIRO; SALES, 2015)

$$\overline{H} = \frac{H}{\log_2 p}. \tag{5.6}$$

Se as intensidades dos *pixels* forem equiprováveis, a entropia normalizada deve ser igual a 1.

Conforme pode ser visto na Figura 4, as imagens cifradas resultantes têm um aspecto completamente ruidoso, não retendo vestígios visuais das imagens originais correspondentes (na figura, são apresentados quatro exemplos de imagens empregadas nos experimentos; todas as outras apresentaram resultados similares). Observa-se também que, independentemente do histograma antes da cifragem, os valores de *pixel* de cada imagem cifrada são uniformemente distribuídos. Como esperado, esse comportamento qualitativo tem relação com as medidas numéricas apresentadas, isto é, o coeficiente de correlação (LIMA; NOVAES, 2014) e a entropia normalizada (YANG et al., 2015). Os resultados para as imagens originais e cifradas são exibidos na Tabela 6. Os valores sugerem que ataques estatísticos contra o esquema proposto não seriam efetivos.

Também foram realizados testes do esquema proposto em relação ao ataque diferencial. Isso foi feito calculando o NPCR (*Number of Changing Pixel Rate*) e a UACI (*Unified Averaged Changed Intensity*) (WU; NOONAN; AGAIAN, 2011; LIMA; NOVAES, 2014; LIMA; LIMA; CAMPELLO DE SOUZA, 2016). Sejam $I_1(n,k)$ e $I_2(n,k)$ os valores dos *pixels* na posição (n,k) de duas imagens cifradas $\mathbf{I}_1$ e $\mathbf{I}_2$, respectivamente, com imagens originais correspondentes diferentes apenas no bit menos significativo (LSB, do inglês *least significant bit*) de um *pixel*. Seja $D(n,k)$ definido por

$$D(n,k) := \begin{cases} 0, & I_1(n,k) = I_2(n,k), \\ 1, & \text{caso contrário.} \end{cases}$$

[3] Para as imagens originais, a entropia máxima seria 8, uma vez que imagens monocromáticas com 256 níveis de cinza estão sendo consideradas.

Tabela 6 – Resultados dos experimentos: coeficiente de correlação (r), entropia normalizada ($\bar{H}$), NPCR$_d$ and UACI$_d$ (teste de ataque diferencial) e NPCR$_s$ (teste de sensibilidade da chave); o símbolo ($'$) é usado para imagens cifradas.

	r	r'	$\bar{H}$	$\bar{H}'$	NPCR$_d$	UACI$_d$	NPCR$_s$
min	0,02624	0,00001	0,06246	0,99989	99,56	33,27	99,57
max	1,00000	0,00837	0,95488	0,99993	99,65	33,66	99,65

Define-se

$$\mathrm{NPCR} = \frac{\sum_{n,k} D(n,k)}{N_r \times N_c} \times 100\%$$

e

$$\mathrm{UACI} = \frac{1}{N_r \times N_c}\left[\frac{\sum_{n,k} |I_1(n,k) - I_2(n,k)|}{p-1}\right] \times 100\%,$$

em que N_r e N_c denotam, respectivamente, os números de linhas e de colunas das imagens envolvidas.

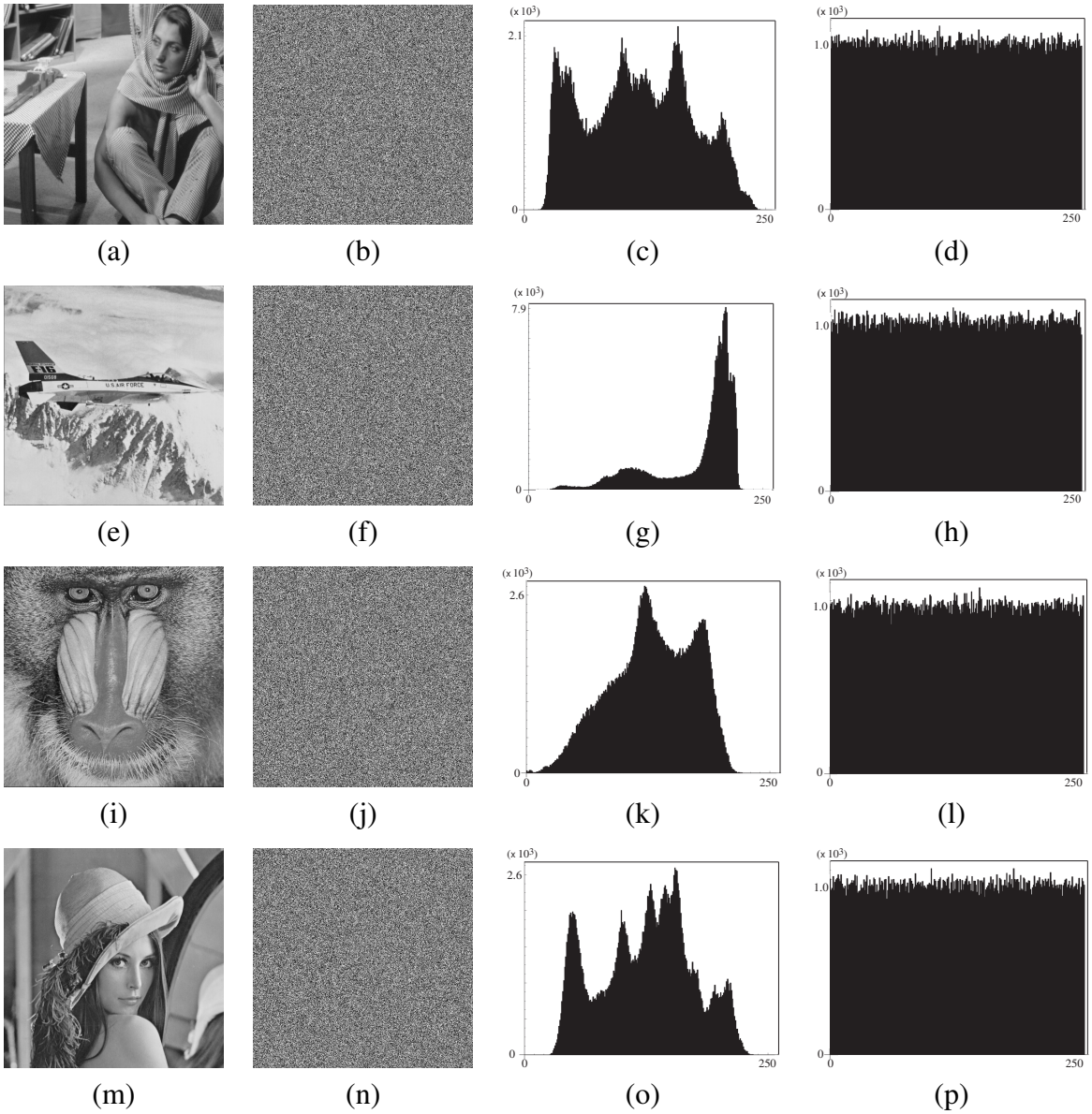
Nos nossos testes, para cada uma das 141 imagens, foram geradas 100 imagens modificadas em um LSB de um *pixel* escolhido aleatoriamente. A versão cifrada de cada imagem original, identificada por $\mathbf{I}_1$, e a versão cifrada da imagem modificada correspondente, identificada como $\mathbf{I}_2$, foram usadas para calcular o NPCR e o UACI para cada uma das 100 imagens modificadas. Os valores mínimo e máximo, obtidos após considerar todas as imagens de teste são mostrados na Tabela 6. Os valores são muito próximos dos teóricos esperados (NPCR $\approx 99{,}61\%$, UACI $\approx 33{,}46\%$) (WU; NOONAN; AGAIAN, 2011).

Finalmente, foi avaliada a sensibilidade do nosso esquema a pequenas alterações no vetor θ^{2D}. Isso foi feito mediante 100 realizações do seguinte experimento para cada uma das imagens originais: (i) cifrar uma imagem I usando o vetor $\theta^{(2D)}$ de ângulos de corpo finito e obter a imagem cifrada I_c; (ii) escolher aleatoriamente um bit entre aqueles utilizados em $\theta^{(2D)}$ e invertê-lo, obtendo um vetor minimamente modificado $\tilde{\theta}^{(2D)}$; (iii) usar $\tilde{\theta}^{(2D)}$ para aplicar as etapas de decifragem em I_c e obter $\tilde{I}$; (iv) comparar $\tilde{I}$ e I calculando o NPCR. O resultado, também mostrado na Tabela 6, indica que o esquema é altamente sensível a mudanças em $\theta^{(2D)}$. Conforme discutido anteriormente, $\theta^{(2D)}$ tem comprimento (8.128×7) e, consequentemente, é suficientemente grande para inviabilizar um ataque direto; de acordo com o que já se enfatizou, $\theta^{(2D)}$ pode ser obtido por meio de geradores de números aleatórios, cuja sensibilidade e tamanho do espaço-chave têm se mostrado adequados (STOJANOVSKI; KOCAREV, 2001; STOJANOVSKI; PIHL; KOCAREV, 2001; BEIRAMI; NEJATI; CALLEGARI, 2014; LIU; MIAO, 2016).

5.2.1 Robustez a Ataques Clássicos

As simulações e estudos realizados indicam que o esquema proposto pode resistir a ataques criptográficos clássicos, como ataques de texto-claro conhecido e ataques de texto-claro

Figura 4 – Exemplos de imagens utilizadas nos experimentos; as colunas da esqueda para a direita correspondem respectivamente a imagem original, imagem cifrada, histograma original e histograma após cifragem.



Fonte: O Autor, 2019.

escolhido (CPA, do inglês *chosen plaintext attack*). Para realizar o CPA, o adversário poderia escolher, por exemplo, uma imagem tendo apenas uma de suas sub-imagens correspondente à matriz identidade (passo 1 da Figura 3), como uma tentativa de revelar a matriz da 2D-SFNT que é dependente da chave-secreta (passo 3 da Figura 3). Para ser mais preciso, denote a referida sub-imagem como $\mathbf{I}_{r,c}$. Após o passo 2 do procedimento de criptografia, obtém-se

$$\mathbf{I}^{\mathbf{1}}_{r,c} = \mathbf{R}^{(2D)}_{\boldsymbol{\theta}} \mathbf{F} \mathbf{I}_{r,c} \mathbf{F}^T.$$

Na última equação, se $\mathbf{I}_{r,c}$ for igual a matriz identidade, tem-se

$$\mathbf{I}^{\mathbf{1}}_{r,c} = \mathbf{R}^{(2D)}_{\boldsymbol{\theta}} \mathbf{F} \mathbf{F}^T,$$

em que

$$\mathbf{F}\mathbf{F}^T = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 \\ 0 & 0 & \iddots & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Como a multiplicação de $\mathbf{R}^{(2D)}_{\boldsymbol{\theta}}$ por $\mathbf{F}\mathbf{F}^T$ representa uma simples permutação dos elementos da primeira matriz, esta seria conhecida pelo adversário e, assim, a SFNT aplicada nos passos 3 e 7 da cifragem estaria revelada; observe que, se se supuser que o valor de $\alpha = \alpha_k$, o elemento com relação ao qual os cossenos e senos da matriz de rotação são calculados, é público, o adversário poderia explicitar, inclusive, os ângulos de rotação propriamente ditos (embora isso não seja exatamente necessário para tentativa de quebra do esquema). Independentemente disso, uma vez que o adversário não tem acesso às sub-imagens calculadas no passo 3 da cifragem (Figura 3) e que compõem a imagem intermediária I' no passo 4, a qual, na sequência, passa por um estágio de permutação (passo 5) e por uma segunda rodada de transformação baseada em sub-imagem (passo 6), a estratégia descrita acima se reduz a um ataque de força bruta e suas possibilidades de sucesso são consideravelmente comprometidas.

Outro CPA poderia ser tentado escolhendo como texto-claro uma imagem em que todas as sub-imagens $\mathbf{I}_{r,c}$, $r, c = 1, \ldots, 4$, são iguais. Neste caso, todas as sub-imagens transformadas $\mathbf{I^1}_{r,c}$, $r, c = 1, \ldots, 4$, no passo 2 do procedimento de cifragem também seriam iguais. Consequentemente, a permutação envolvendo entradas de diferentes sub-imagens $\mathbf{I^1}_{r,c}$ no passo 4 seria equivalente a aplicar uma permutação a cada sub-imagem de uma maneira isolada. Dessa forma, mesmo após a segunda transformação no passo 6, a relação entre uma sub-imagem $\mathbf{I}'_{r,c}$ e a respectiva sub-imagem $\mathbf{I}_{r,c}$ seria linear e o sistema poderia ser quebrado. Uma maneira muito simples de evitar esse ataque é usar diferentes ângulos de rotação na transformação das sub-imagens no passo 2 (e também no passo 6). Na verdade, poder-se-ia partir de um mesmo conjunto de ângulos de rotação e deslocar ciclicamente as posições dos ângulos nesse conjunto à medida em que diferentes sub-imagens fossem transformadas pela SFNT na cifragem.

Além do ajuste acima descrito, outras estratégias poderiam ser empregadas para melhorar a capacidade do esquema proposto de resistir à CPA. Um conjunto de ângulos de rotação dependente da imagem original (texto-claro) e de parâmetros externos poderia ser usado, por exemplo. Nesse caso, um adversário teria maior dificuldade de obter informações úteis à quebra do sistema por meio de comparações entre o texto-claro e o texto-cifrado simplesmente (CHAI et al., 2019; HU et al., 2017; MURUGAN; GOUNDER, 2016). Em suma, considerando as investigações realizadas até a conclusão desta tese, é razoável admitir que o esquema proposto apresenta robustez a ataques criptográficos clássicos.

5.3 COMPARAÇÃO COM OUTROS ESQUEMAS DE CIFRAGEM

O esquema de cifragem proposto pode ser comparado a outros métodos considerando os seguintes aspectos:

Segurança. A segurança do esquema proposto foi avaliada usando métricas e métodos comumente aceitos na literatura. Sob este aspecto, nossos resultados são comparáveis aos mostrados em (YANG et al., 2015; KAUR; KUMAR, 2018; KANG; TAO, 2018; KANG; MING; TAO, 2018; ANNABY; RUSHDI; NEHARY, 2016; LIMA; MADEIRO; SALES, 2015; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017) conforme exibido na Tabela 7. Na tabela, foi utilizado texto em negrito para destacar os dois melhores resultados para cada métrica. Para ser mais específico, foram considerados os maiores espaços de chave[4], os valores máximos mais baixos dos coeficientes de correlação, as médias entre os valores máximo e mínimo do NPCR_d e UACI_d mais próximos aos valores teóricos de tais métricas e os valores mínimos mais altos de entropias normalizadas. Pode-se observar que os resultados fornecidos pelo esquema proposto estão sempre entre os melhores, embora outros métodos tenham atingido valores satisfatórios do ponto de vista da segurança. Como alternativas para aumentar ainda mais a segurança do nosso esquema, pode-se usar conjuntos diferentes $\boldsymbol{\theta}^{(2D)}$ para transformar cada bloco nos passos 3 e 7 da cifragem, ou empregar um vetor não-constante $\boldsymbol{\alpha}$, contendo os elementos em relação aos quais são calculados os cossenos e senos da matriz de rotação.

Sensibilidade. Como todas as operações aritméticas realizadas na cifragem de uma imagem pelo esquema proposto são realizadas módulo p, o método é altamente sensível a modificações tanto nos parâmetros secretos quanto nas imagens originais ou cifradas. Em outras palavras, pode-se dizer que, se a aritmética módulo p é usada, uma pequena mudança em um vetor (mudança de 1 bit em um de seus componentes, por exemplo) não leva necessariamente a uma pequena alteração no resultado da 2D-SFNT; isso se deve à redução modular aplicada durante o cálculo da transformação (combinações lineares dos componentes do vetor, usando

[4] Na Tabela 7, foi indicado como tamanho do espaço de chaves $2^{256}-2^{56.896}$ porque, como discutido anteriormente, o vetor $\boldsymbol{\theta}^{(2D)}$, usado na parametrização da 2D-SFNT, pode ser produzido por um gerador de números aleatórios, cujas condições iniciais desempenham o papel de chave-secreta ou tomadas como a própria chave-secreta (mesmo que tal chave seja relativamente grande). Em resumo, isso significa que o esquema proposto fornece flexibilidade na escolha da chave-secreta e atende simultaneamente aos respectivos requisitos de segurança.

adições e multiplicações módulo p). Tal comportamento favorece a obtenção de um certo nível de segurança usando menos estágios de criptografia do que métodos baseados em operações complexas e reais (KANG; ZHANG; TAO, 2015; HSUE; CHANG, 2015; GAO et al., 2018; KANG; MING; TAO, 2018; KANG; TAO, 2018; ANNABY; RUSHDI; NEHARY, 2016). Neste contexto, os métodos citados podem ser mais susceptíveis a tipos específicos de ataques [5] (ZHAO et al., 2016; YOUSSEF, 2008).

Complexidade computacional. A 2D-SFNT, que constitui o núcleo do método de criptografia proposto, é de fácil construção e pode ser eficientemente calculada como um produto entre uma matriz esparsa de funções trigonométricas de corpo finito e uma versão linearizada da 2D-FNT da estrutura bidimensional processada (sub-imagem). Tal produto envolve $\mathcal{O}(N^2)$ operações aritméticas e a 2D-FNT ordinária pode ser computada usando-se, por exemplo, algoritmos rápidos de dizimação no tempo originalmente projetados para computar a 2D-DFT com complexidade $\mathcal{O}(N \log_2 N)$[6]. Em contraste, outras transformadas empregadas em cifragem de imagem são normalmente construídas usando procedimentos que envolvem fórmulas não-fechadas e requerem, no caso bidimensional, $\mathcal{O}(N^3)$ operações aritméticas complexas ou reais para serem computadas (KANG; ZHANG; TAO, 2015; HSUE; CHANG, 2015; GAO et al., 2018; KANG; MING; TAO, 2018).

Uma transformada fracionária discreta, por exemplo, cuja matriz de transformação ordinária pode ser genericamente denotada por $\mathbf{M}$, é geralmente definida por meio da expansão espectral

$$\mathbf{M} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^{-1},$$

em que $\mathbf{V}$ tem em suas colunas um conjunto ortogonal de autovetores de $\mathbf{M}$ e $\mathbf{\Lambda}$ é uma matriz diagonal que contém os respectivos autovalores. Isso nos permite obter a matriz da transformada fracionária discreta correspondente como

$$\mathbf{M}^a = \mathbf{V}\mathbf{\Lambda}^a\mathbf{V}^{-1};$$

e a ordem fracionária $a \in \mathbb{R}$ é comumente empregada como o parâmetro secreto em aplicações de criptografia de imagens. O ponto-chave para expandir espectralmente $\mathbf{M}$ é a construção do conjunto de autovetores para ser usado como colunas de $\mathbf{V}$. Isso normalmente é realizado usando fórmulas não-fechadas, o que impede que a transformação seja calculada com complexidade subquadrática. Uma comparação quantitativa em relação a esse aspecto pode ser realizada considerando o estágio de transformação de um esquema de criptografia de imagens semelhante ao nosso (passo 3 ou passo 7 na Figura 3), onde é preciso computar 16 transformadas bidimensionais

[5] Foi avaliado um esquema similar ao nosso, porém empregando a SDCT real (FRACASTORO; FOSSON; MAGLI, 2017), no lugar do 2D-SFNT. Entre outros problemas, o esquema apresentou várias deficiências relacionadas à sensibilidade e segurança necessárias para uma técnica de criptografia de imagens.

[6] Vários algoritmos rápidos para computar a DFT são adaptáveis à FNT e, consequentemente, à versão bidimensional dessa transformada. Além disso, dependendo da característica de $\mathrm{GF}(p)$, algoritmos livres de multiplicação podem ser usados para calcular a transformada (BLAHUT, 2010).

com comprimento 128×128 (DE OLIVEIRA NETO, 2019). Se a 2D-SFNT for utilizada, a complexidade multiplicativa será da ordem de

$$\mathbf{C}_{\text{2D-SFNT}} = 16 \times (2 \times 128) \times (128 \log_2 128) = 7 \times 2^{19}$$

operações aritméticas módulo p. Se a transformada fracionária for usada, a complexidade multiplicativa será da ordem

$$\mathbf{C}_{\text{frac.}} = 16 \times (2 \times 128) \times (128^2) = 128 \times 2^{19}$$

operações aritméticas. Ou seja, mesmo que se empregue uma transformada fracionária sobre corpos finitos, o que poderia eliminar algum custo adicional associado à realização de operações de ponto flutuante (com valor complexo ou real) em vez de executar as de ponto fixo (módulo p), $\mathbf{C}_{\text{frac.}}$ terá uma complexidade quase 20 vezes maior que $\mathbf{C}_{\text{2D-SFNT}}$.

Representação da imagem. Naturalmente, as imagens cifradas produzidas pelo nosso esquema têm componentes inteiras. Portanto, se $p = 257$, os correspondentes valores dos *pixels* estão no intervalo $[0, 256]$ e não poderão ser representados usando uma codificação usual de 8 bits. De qualquer forma, alternativas simples poderiam ser adotadas para contornar essa restrição. Pode-se representar, por exemplo, cada inteiro no intervalo $[0, 254]$ usando um byte no intervalo $[00000000, 11111110]$, correspondentemente, e o byte 11111111 seria usado como um tipo de *flag*, que seria seguido pelo "nono" bit 0 para representar o valor decimal 255 ou pelo "nono" bit 1 para representar o valor decimal 256. Assumindo que os símbolos (valores dos *pixels*) em uma imagem cifrada são equiprováveis, o número médio de bits por *pixel* na representação proposta seria dado por $(255 \times 8 + 2 \times 9)/257 = 8{,}0077821012$. Isso significa que o número de bits adicionais devido à criptografia é insignificante. Além disso, como nenhum arredondamento é necessário, se a chave correta for empregada, a imagem recuperada na decifragem é idêntica à imagem original correspondente. Por outro lado, a criptografia de imagens usando transformadas definidas em corpos infinitos precisa lidar com estratégias de preservação da realidade (para evitar que apareçam números complexos na imagem cifrada) e de trucamento (KANG; MING; TAO, 2018; KANG; TAO, 2018; ANNABY; RUSHDI; NEHARY, 2016; VENTURINI; DUHAMEL, 2004); isso pode levar a problemas relacionados a precisão e aumentar consideravelmente a taxa de bits das imagens codificadas, caso representações de ponto-flutuante sejam utilizadas.

Tabela 7 – Comparação com os métodos existentes: dimensão do espaço de chaves, coeficiente de correlação (r), NPCR$_d$ e UACI$_d$ (teste de ataque diferencial) e entropia normalizada ($\overline{H}$); o símbolo ($'$) indica imagens cifradas e o símbolo "$-$" em algumas entradas da tabela indica que a métrica de segurança correspondente não é claramente fornecida pelos autores do referido documento. O texto em negrito é usado para destacar os dois melhores resultados para cada métrica.

Método	Espaço de Chave	$\lvert r' \rvert$	NPCR$_d$	UACI$_d$	$\overline{H}'$
Proposto	$\mathbf{2^{256} - 2^{56.896}}$	$\mathbf{0{,}00001 - 0{,}00837}$	$\mathbf{99{,}56 - 99{,}65}$	$\mathbf{33{,}27 - 33{,}66}$	$\mathbf{0{,}99989 - 0{,}99993}$
(YANG et al., 2015)	2^{325}	$0{,}00136 - 0{,}00859$	$99{,}64 - 99{,}68$	$33{,}40 - 33{,}66$	$0{,}99982 - 0{,}99998$
(KAUR; KUMAR, 2018)	$\mathbf{2^{26.952}}$	$\mathbf{0{,}00010 - 0{,}00730}$	$99{,}67 - 99{,}70$	$32{,}58 - 33{,}66$	$0{,}99963 - 0{,}99976$
(KANG; TAO, 2018)	–	$0{,}00010 - 0{,}00910$	$99{,}86 - 100{,}00$	$26{,}16 - 33{,}34$	–
(KANG; MING; TAO, 2018)	$\approx 2^{325}$	$0{,}00016 - 0{,}00842$	$99{,}99 - 100{,}00$	$33{,}30 - 33{,}34$	–
(ANNABY; RUSHDI; NEHARY, 2016)	–	$0{,}00982 - 0{,}39088$	$100{,}00$	$33{,}24 - 33{,}45$	$0{,}99965 - 0{,}99967$
(LIMA; MADEIRO; SALES, 2015)	2^{160}	$0{,}00010 - 0{,}01320$	$99{,}58 - 99{,}99$	$33{,}19 - 33{,}56$	$0{,}99820 - 0{,}99990$
(MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017)	2^{71}	$0{,}00010 - 0{,}00910$	$\mathbf{99{,}54 - 99{,}71}$	$\mathbf{33{,}44 - 33{,}52}$	$\mathbf{0{,}99997 - 0{,}99999}$

Fonte: O Autor, 2019.

6 CONCLUSÕES

Neste capítulo, são apresentadas as principais conclusões desta tese e sugeridas direções para o desenvolvimento de trabalhos futuros. Realizando um paralelo com o que fora colocado como objetivo geral a ser alcançado pela execução deste trabalho, ratifica-se que se conseguiu definir uma transformada numérica manobrável de Fourier, a qual corresponde a uma versão em corpos finitos da transformada discreta manobrável de Fourier, de modo análogo àquele em que a transformada numérica de Fourier (FNT) corresponde à transformada discreta de Fourier. Tal definição, que representa uma generalização da FNT, preencheu uma lacuna teórica importante no âmbito das transformadas aplicáveis ao processamento digital de sinais, vindo acompanhada da derivação de diversos outros resultados inéditos e importantes. Nesse contexto, as seguintes contribuições específicas podem ser elencadas:

1. Definiu-se uma função tangente sobre corpos finitos. Foram estudadas algumas propriedades dessa função, como a periodicidade, e foi estabelecida e caracterizada a sua função inversa. Esses conceitos têm utilidade na forma como a transformada numérica manobrável de Fourier é aplicada, quando é utilizado o conceito de ângulo ótimo.

2. Foi apresentada uma nova proposição relacionada às simetrias da transformada numérica de Fourier, quando esta emprega como núcleo um inteiro Gaussiano sobre um corpo finito; essa proposição tem papel importante na relação entre a SFNT e a transformada numérica de Hilbert.

3. Foi introduzido um operador de rotação bidimensional baseado em funções trigonométricas sobre corpos finitos. Com isso, pôde-se definir a transformada numérica manobrável de Fourier, bem como sua versão bidimensional. Foram desenvolvidos vários exemplos em que a construção dessas transformadas foi ilustrada e sua complexidade aritmética foi avaliada.

4. Foi introduzido, no contexto de corpos finitos, o conceito de ângulo de rotação ótimo e, empregando os resultados relacionados à função tangente sobre corpos finitos, indicou-se como obter tal ângulo.

5. Foi proposta uma nova definição para a transformada numérica de Hilbert (HiNT), com base na nova proposição sobre as simetrias da transformada numérica de Fourier; foi demonstrado como obter a HinT a partir da SFNT.

6. Foi proposto um esquema para cifragem de imagens baseado na 2D-SFNT. Foram analisados os diversos aspectos desse esquema, tendo sido verificada a sua segurança contra os principais tipos de ataques criptográficos e indicadas suas vantagens em relação a outras técnicas no estado-da-arte no mesmo contexto.

7. Como resultado desta tese, foi publicado no periódico “Signal Processing: Image Communication” (Qualis A1 em Engenharias IV; fator de impacto 2,073) o artigo intitulado “Steerable Fourier number transform with application to image encryption” (Maio/2019, Volume 74, p. 89-95). O autor desta tese é o primeiro autor do artigo, que foi escrito em coautoria com o seu orientador e com o Prof. Dr. José Rodrigues de Oliveira Neto. No trabalho, é apresentada a definição da transformada numérica manobrável de Fourier e descrita a sua aplicação em cifragem de imagens. A análise de segurança apresentada nesta tese e a sua comparação com outras ténicas úteis no mesmo cenário também são apresentadas no trabalho.

6.1 CONTINUIDADE DA PESQUISA

Neste momento, torna-se importante indicar o que pode ser refinado dos resultados obtidos e o que ainda pode ser pesquisado. Com este propósito, é possível elencar as seguintes atividades a serem realizadas após defesa da tese:

- Estudo de propriedades da SFNT: mesmo para a transformada discreta manobrável de Fourier, ainda não foram estudadas de modo sistemático as suas propriedades. Assim, constitui uma lacuna importante a caracterização da SFNT também sob esse aspecto. O fato é que, como a SFNT pode ser calculada por meio de uma FNT seguida da aplicação de rotações, talvez não sejam encontradas exatamente propriedades novas para essa transformada, mas apenas extensões das propriedades já estabelecidas para a FNT. De qualquer maneira, é relevante pensar no que acontece, por exemplo, com a propriedade de convolução no domínio da SFNT; trabalhos futuros devem levar em consideração desenvolvimentos neste sentido.

- Investigação sobre a possibilidade de se definir uma SFNT tridimensional: embora possa parecer trivial, a extensão da SFNT ao caso tridimensional demanda a visitação cuidadosa dos diversos passos expostos no Capítulo 4 desta tese para as versões 1D e 2D dessa transformada. Especificamente, é necessário elucidar a forma que teria o grafo resultante do produto entre três grafos em ciclo e determinar as multiplicidades dos autovalores do respectivo Laplaciano. Se houver autovalores com multiplicidades maiores que 2, novas opções de rotação são criadas, elevando os graus de liberdade nas manobras impostas à base original. Tais possibilidades precisam ser bem estudadas e descritas de forma sistemática e organizada.

- Continuidade do estudo sobre a transformada numérica de Hilbert: nesta tese, propôs-se uma nova definição para a HiNT, porém, não foram estudadas propriedades nem investigadas aplicações em potencial para esta ferramenta. Assim, fica para trabalhos futuros um estudo aprofundado neste sentido. A perspectiva é que a referida transformada

possa ter aplicações também em criptografia e, eventualmente, noutras técnicas voltadas ao processamento de imagem.

- Relação entre a SFNT e outras transformadas numéricas: de forma semelhante ao que se obteve para a transformada numérica de Hilbert, pode-se estudar, em trabalhos futuros, a possibilidade de calcular outras transformadas numéricas a partir da SFNT construída com ângulos de rotação específicos. Isso deve auxiliar na caracterização mais completa da nova transformada e permitir identificá-la como uma versão generalizada de outras transformadas diferentes da de Fourier.

- Aplicação da SFNT com ângulo ótimo: nesta tese, demonstrou-se que é possível escolher ângulos de rotação que anulem cerca de metade dos coeficientes no cálculo de uma SFNT, levando a uma representação mais concentrada do vetor. Quando a transformada é definida sobre os reais ou complexos, uma estratégia como essa pode ser usada para realizar compressão de dados, porque há soluções aproximadas (ângulo sub-ótimo) e baseadas em otimização, que evitam que o que se esteja fazendo seja uma simples troca, para cálculo da transformada inversa, entre armazenar o coeficiente (anulado) e armazenar o ângulo de rotação. Todavia, tal possibilidade parece não factível no caso de corpos finitos, pois, em função da natureza das operações de aritmética modular, o ângulo ótimo exato deve ser guardado. Em investigações futuras, pode-se averiguar que particularidades possui o cálculo da SFNT com ângulo ótimo e que aplicações isso poderia ter.

- Definição de outras transformadas numéricas manobráveis: sobre os números reais, as únicas transformadas discretas manobráveis introduzidas foram a de Fourier e a do cosseno (relacionada à transformada discreta do cosseno do tipo 2) (FRACASTORO; MAGLI, 2017; FRACASTORO; FOSSON; MAGLI, 2017). Nesta linha, pretende-se investigar a possibilidade de se definir transformadas numéricas manobráveis de tipos diferentes da de Fourier. Existe um interesse particular em considerar a transformada numérica de Hartley em tal investigação (CAMPELLO DE SOUZA; OLIVEIRA, 2000; CAMPELLO DE SOUZA; OLIVEIRA; PALMA, 2001; CAMPELLO DE SOUZA et al., 1998); isso se deve aos fatos de essa transformada ainda não ter sido considerada mesmo no cenário dos números reais e de ela possuir propriedades similares às da transformada numérica de Fourier, o que deve permitir o aproveitamento de alguns resultados já derivados no presente trabalho.

- Definição da SFNT sobre corpos de característica 2 e corpos de extensão: nesta tese, foram consideradas transformadas definidas sobre $\mathrm{GF}(p)$ ou $\mathrm{GI}(p)$, em que p é um primo ímpar. Em investigações futuras, pode-se considerar SFNT definidas em corpos de extensão, o que pode abrir um leque para novos cenários de aplicação da ferramenta. Em particular, pode-se pensar em construir SFNT em corpos de característica 2. Neste caso, a principal dificuldade é definir as funções trigonométricas e, consequentemente, o operador de rotação; até existe

uma definição de função cosseno sobre corpos de característica 2 (LIMA; BARONE; CAMPELLO DE SOUZA, 2016), porém, a definição de seno é ausente em função de, nos referidos corpos, ainda não haver um artifício que permita distinguir a operação de adição da de diferença (vide Definição 3.3).

REFERÊNCIAS

AHMED, N.; NATARAJAN, T.; RAO, K. R. Discrete cosine transform. **IEEE Transactions on Computers**, C-23, n. 1, p. 90–93, Janeiro 1974. ISSN 0018-9340. Citado 2 vezes nas páginas 16 e 18.

AKHSHANI, A. et al. A novel scheme for image encryption based on 2D piecewise chaotic maps. **Optics Communications**, v. 283, n. 17, p. 3259–3266, Setembro 2010. Citado na página 63.

ANNABY, M. H.; RUSHDI, M. A.; NEHARY, E. A. Image encryption via discrete fractional Fourier-type transforms generated by random matrices. **Signal Processing: Image Communication**, v. 49, p. 25–46, Novembro 2016. Citado 5 vezes nas páginas 60, 68, 69, 70 e 71.

BEIRAMI, A.; NEJATI, H.; CALLEGARI, S. Fundamental performance limits of chaotic-map random number generators. In: **Proceedings of the 52nd Annual Allerton Conference on Communication, Control, and Computing**. Monticello, IL: [s.n.], 2014. p. 1126–1131. Citado 2 vezes nas páginas 63 e 65.

BIANCHI, T.; BIOGLIO, V.; MAGLI, E. Analysis of one-time random projections for privacy preserving compressed sensing. **IEEE Transactions on Information Forensics and Security**, v. 11, n. 2, p. 313–327, Fevereiro 2016. Citado na página 27.

BLAHUT, R. E. Transform techniques for error-control codes. **IBM J. Res. Dev.**, v. 23, p. 299–315, Maio 1979. Citado na página 16.

BLAHUT, R. E. **Theory and Practice of Error Control Codes**. [S.l.]: Addison-Wesley, 1983. Citado na página 16.

BLAHUT, R. E. **Fast Algorithms for Signal Processing**. [S.l.]: Cambridge University Press, 2010. Citado 6 vezes nas páginas 28, 36, 41, 42, 44 e 69.

BRACEWELL, R. N. Discrete Hartley transform. **Journal of the Optical Society of America**, OSA, v. 73, n. 12, p. 1832–1835, Dezembro 1983. Citado 2 vezes nas páginas 16 e 18.

CAMPELLO DE SOUZA, R.; OLIVEIRA, H. de; PALMA, L. E. Hartley number theoretic transforms. In: **Proc. IEEE Int. Symp. Information Theory**. Washington, DC: [s.n.], 2001. p. 210. Citado 4 vezes nas páginas 17, 28, 37 e 74.

CAMPELLO DE SOUZA, R. et al. A transformada discreta do seno em um corpo finito. In: **Anais do XXVIII Congresso Nacional de Matemática Aplicada e Computacional, São Paulo, Brasil**. [S.l.: s.n.], 2005. v. 53, p. 404–406. Citado na página 18.

CAMPELLO DE SOUZA, R. M.; OLIVEIRA, H. M. de. The complex Hartley transform over a finite field. In: FARNELL, P. G.; DARNELL, M.; HONARY, B. (Ed.). **Coding, Communications and Broadcasting**. 1st. ed. Hertfordshire: Research Studies Press, Jonh Wiley, 2000. p. 267–276. Citado 3 vezes nas páginas 16, 28 e 74.

CAMPELLO DE SOUZA, R. M. et al. The discrete cosine transform over prime finite fields. In: SOUZA, J. N. de; DINI, P.; LORENZ, P. (Ed.). **International Conference on Telecommunications**. Berlin: Springer, 2004. (Lecture Notes in Computer Science), p. 482–487. Citado 2 vezes nas páginas 16 e 18.

CAMPELLO DE SOUZA, R. M. et al. Trigonometry in finite fields and a new Hartley transform. In: IEEE. **Proc. IEEE Int. Symp. Information Theory (ISIT'98)**. [S.l.], 1998. p. 293. Citado 6 vezes nas páginas 18, 28, 34, 37, 38 e 74.

CANDAN, C.; KUTAY, M. A.; OZAKTAS, H. M. The discrete fractional Fourier transform. **IEEE Trans. Signal Process.**, v. 48, n. 5, p. 1329–1337, Maio 2000. Citado na página 18.

CARNEIRO, G.; JEPSON, A. D. Phase-based local features. In: **Proceedings of the 7th European Conference on Computer Vision-Part I**. London, UK: Springer-Verlag, 2002. (ECCV '02), p. 282–296. Citado na página 27.

CHAI, X. et al. A color image cryptosystem based on dynamic DNA encryption and chaos. **Signal Processing**, v. 155, n. 2, p. 44–62, February 2019. Citado na página 68.

CHANG, C. L.; GIROD, B. Direction-adaptive partitioned block transform for image coding. In: **Proc. IEEE International Conferecene on Image Processing**. [S.l.: s.n.], 2008. p. 145–148. Citado na página 17.

CHEN, F. et al. Period distribution of the generalized discrete Arnold cat map for $n = 2^e$. **IEEE Transactions on Information Theory**, v. 59, n. 5, p. 3249–3255, Maio 2013. Citado na página 62.

CINTRA, R. J. et al. Fragile watermarking using finite field trigonometrical transforms. **Signal Processing, Image Communication**, v. 24, p. 587–597, 2009. Citado 3 vezes nas páginas 16, 28 e 60.

COHEN, R. A. et al. Direction-adaptive transforms for coding prediction residuals. In: **Proc. IEEE International Conferecene on Image Processing**. [S.l.: s.n.], 2010. p. 185–188. Citado 2 vezes nas páginas 17 e 55.

COOLEY, J.; LEWIS, P.; WELCH, P. The finite Fourier transform. **IEEE Transactions on Audio and Electroacoustics**, v. 17, n. 2, p. 77–85, Junho 1969. Citado na página 18.

DE OLIVEIRA NETO, J. R. **Construção de autovetores de transformadas discretas de Fourier: novos métodos e aplicações.** 136 p. Dissertação (Doutorado em Engenharia Elétrica) — Universidade Federal de Pernambuco, 2019. Citado na página 70.

DERI, J. A.; MOURA, J. M. F. Spectral projector-based graph Fourier transforms. **IEEE Journal of Selected Topics in Signal Processing**, v. 11, n. 6, p. 785–795, 2017. Citado na página 17.

DICOM. DICOM - digital imaging and communications in medicine. 2019. Janeiro, 2018. Citado na página 61.

DIMITROV, V. S.; COOKLEV, T. V.; DONEVSKY, B. D. Number theoretic transforms over the golden section quadratic field. **IEEE Trans. on Signal Processing**, v. 43, n. 8, p. 1790–1797, Agosto 1995. Citado 3 vezes nas páginas 17, 32 e 36.

EKAMBARAM, V.; FANTI, G. C.; AYAZIFAR, B. Multiresolution graph signal processing via circulant structures. **IEEE Digital Signal Processing and Signal Processing Education Meeting (DSP/SPE)**, IEEE, v. 30, Outubro 2013. Disponível em: <http://ieeexplore.ieee.org/document/6642575/>. Citado na página 23.

FEKRI, F. et al. Block error correcting codes using finite-field wavelet transforms. **IEEE Trans. on Signal Processing**, v. 54, n. 3, p. 991–1004, 2006. Citado na página 16.

FEKRI, F.; MERSEREAU, R. M.; SCHAFER, R. W. Theory of wavelet transforms over finite fields. In: **Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing**. Phoenix, AZ: [s.n.], 1999. v. 3, p. 1213–1216. Citado na página 16.

FEKRI, F. et al. Convolutional codes using finite-field wavelets: time-varying codes and more. **IEEE Trans. on Signal Processing**, v. 53, n. 5, p. 1881–1896, Maio 2005. Citado na página 16.

FRACASTORO, G.; FOSSON, S. M.; MAGLI, E. Steerable discrete cosine transform. **IEEE Transactions on Image Processing**, v. 26, n. 1, p. 303–314, Janeiro 2017. ISSN 1057-7149. Citado 6 vezes nas páginas 17, 18, 46, 52, 69 e 74.

FRACASTORO, G.; MAGLI, E. Steerable discrete Fourier transform. **IEEE Signal Processing Letters**, IEEE, v. 24, p. 319 – 323, Março 2017. Citado 13 vezes nas páginas 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 41, 46 e 74.

GAO, Z. et al. Colour image encryption algorithm using one-time key and FrFT. **IET Image Processing**, v. 12, n. 4, p. 472–478, April 2018. Citado 2 vezes nas páginas 61 e 69.

GIRAULT, B.; GONCALVES, P.; FLEURY, E. Translation on graphs: An isometric shift operator. **IEEE Signal Processing Letters**, Institute of Electrical and Electronics Engineers (IEEE), v. 22, n. 12, p. 2416–2420, dec 2015. Disponível em: <https://doi.org/10.1109/lsp.2015.2488279>. Citado na página 21.

GNUTTI, A.; GUERRINI, F.; LEONARDI, R. Representation of signals by local symmetry decomposition. In: **2015 23rd European Signal Processing Conference (EUSIPCO)**. [S.l.: s.n.], 2015. p. 983–987. Citado na página 27.

GUDVANGEN, S. **Practical Applications of Number Theoretic Transforms**. 2006. Disponível em: <citeseer.ist.psu.edu/235814.html>. Citado na página 32.

HSUE, W. L.; CHANG, W. C. Real discrete fractional Fourier, Hartley, generalized Fourier and generalized Hartley transforms with many parameters. **IEEE Transactions on Circuits and Systems I: Regular Papers**, v. 62, n. 10, p. 2594–2605, Outubro 2015. Citado na página 69.

HU, T. et al. Chaotic image cryptosystem using DNA deletion and dna insertion. **Signal Processing**, v. 134, n. 5, p. 234–243, Maio 2017. Citado na página 68.

HUA, Z. et al. 2D logistic-sine-coupling map for image encryption. **Signal Processing**, v. 149, n. 8, p. 148–161, Agosto 2018. Citado na página 60.

HUA, Z.; YI, S.; ZHOU, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. **Signal Processing**, v. 144, n. 3, p. 134–144, Março 2018. Citado na página 60.

HUA, Z.; ZHOU, Y. Design of image cipher using block-based scrambling and image filtering. **Information Sciences**, v. 396, n. 8, p. 97–113, Agosto 2017. Citado na página 60.

KAK, S. The number theoretic Hilbert transform. **Circuits, Systems, and Signal Processing**, v. 33, n. 8, p. 2539–2548, Agosto 2014. Citado na página 55.

KAK, S. C. The discrete Hilbert transform. **Proceedings of the IEEE**, v. 58, n. 4, p. 585–586, April 1970. Citado na página 55.

KANG, X.; MING, A.; TAO, R. Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption. **IEEE Transactions on Circuits and Systems for Video Technology (accepted for publication, DOI: 10.1109/TCSVT.2018.2851983)**, 2018. Citado 5 vezes nas páginas 61, 68, 69, 70 e 71.

KANG, X.; TAO, R. Color image encryption using pixel scrambling operator and reality-preserving MPFRHT. **IEEE Transactions on Circuits and Systems for Video Technology (accepted for publication, DOI: 10.1109/TCSVT.2018.2859253)**, accepted for publication, 2018. Citado 5 vezes nas páginas 60, 68, 69, 70 e 71.

KANG, X.; ZHANG, F.; TAO, R. Multichannel random discrete fractional Fourier transform. **IEEE Signal Processing Letters**, v. 22, n. 9, p. 1340–1344, Setembro 2015. Citado 2 vezes nas páginas 61 e 69.

KAUR, M.; KUMAR, V. Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain. **IET Image Processing**, v. 12, n. 7, p. 1273–1283, Junho 2018. Citado 2 vezes nas páginas 68 e 71.

KOVESI, P. **Image Features from Phase Congruency**. 1999. Citado na página 27.

LI, W. The modified Fermat number transform and its application. In: **Proc. IEEE Int. Symp. Circuits Syst.** New Orleans, LA: [s.n.], 1990. v. 3, p. 2365–2368. Citado na página 16.

LIMA, J. Fast algorithm for computing cosine number transform. **Electronics Letters**, IET, v. 51, n. 20, p. 1570–1572, 2015. Citado na página 16.

LIMA, J.; SOUZA, R. C. de. Fractional cosine and sine transforms over finite fields. **Linear Algebra and Its Applications**, Elsevier, v. 438, n. 8, p. 3217–3230, 2013. Citado 2 vezes nas páginas 16 e 28.

LIMA, J. B.; BARONE, M.; CAMPELLO DE SOUZA, R. M. C. de. Cosine transforms over fields of characteristic 2. **Finite Fields and Their Applications**, Elsevier, v. 37, p. 265–284, 2016. Citado na página 75.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. New trigonometric transforms over prime finite fields for image filtering. In: **Proc. of the International Telecommunications Symposium**. Fortaleza, Brazil: [s.n.], 2006. Citado na página 34.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. The finite field fractional fourier transform. In: **Proc. IEEE Conference on Acoustics, Speech and Signal Processing**. [S.l.: s.n.], 2010. p. 3670–3673. Citado 2 vezes nas páginas 16 e 18.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M.; PANARIO, D. Blind sequence separation based on the eigenstructure of finite field transforms. In: . Rio de Janeiro, Brasil: [s.n.], 2008. Citado na página 16.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M.; PANARIO, D. The eigenstructure of finite fields trigonometric transforms. **Linear Algebra and its Applications**, v. 435, n. 8, p. 1956–1971, Outubro 2011. Citado 2 vezes nas páginas 16 e 28.

LIMA, J. B.; MADEIRO, F.; SALES, F. Encryption of medical images based on the cosine number transform. **Signal Processing: Image Communication**, Elsevier, v. 35, p. 1–8, 2015. Citado 5 vezes nas páginas 16, 60, 64, 68 e 71.

LIMA, J. B.; NOVAES, L. Image encryption based on the fractional Fourier transform over finite fields. **Signal Processing**, Elsevier, v. 94, p. 521–530, 2014. Citado 3 vezes nas páginas 16, 60 e 64.

LIMA, J. B.; SOUZA, R. M. C. Finite field trigonometric transforms. **Applicable Algebra in Engineering, Communication and Computing**, v. 22, n. 5-6, p. 393–411, Dezembro 2011. Citado 3 vezes nas páginas 16, 28 e 38.

LIMA, J. B.; SOUZA, R. M. C. de; LIMA, P. Fractional number-theoretic transforms based on matrix functions. In: IEEE. **Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on**. [S.l.], 2014. p. 2614–2618. Citado na página 60.

LIMA, P. H. E. S.; LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Fractional Fourier, Hartley, cosine and sine number-theoretic transforms based on matrix functions. **Circuits, Systems, and Signal Processing**, v. 36, n. 7, p. 2893–2916, Julho 2016. Citado na página 64.

LIU, L.; MIAO, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. **SpringerPlus**, v. 5, n. 289, p. 1–12, Março 2016. ISSN 2193-1801. Disponível em: <https://doi.org/10.1186/s40064-016-1959-1>. Citado 2 vezes nas páginas 63 e 65.

MARTUCCI, S. A. Symmetric convolution and the discrete sine and cosine transforms. **IEEE Trans. on Signal Processing**, v. 42, n. 5, p. 1038–1051, Maio 1994. Citado 3 vezes nas páginas 16, 18 e 38.

MERRI, R. Laplacian graph eigenvectors. **Linear Algebra and its Applications**, v. 278, n. 1, p. 221–236, 1998. Citado 2 vezes nas páginas 41 e 42.

MIKHAIL, M.; ABOUELSEOUD, Y.; ELKOBROSY, G. Two-phase image encryption scheme based on FFCT and fractals. **Security and Communication Networks**, v. 10, p. 1–13, Janeiro 2017. Citado 3 vezes nas páginas 60, 68 e 71.

MURUGAN, B.; GOUNDER, A. G. N. Image encryption scheme based on block-based confusion and multiple levels of diffusion. **IET Computer Vision**, v. 10, n. 6, p. 593–602, Junho 2016. Citado na página 68.

OLIVEIRA, H. M. de; CAMPELLO DE SOUZA, R. M. Orthogonal multilevel spreading sequence design. In: FARNELL, P. G.; DARNELL, M.; HONARY, B. (Ed.). **Coding, Communications and Broadcasting**. 1st. ed. Hertfordshire: Research Studies Press, Jonh Wiley, 2000. p. 291–303. Citado na página 16.

OLIVEIRA, H. M. de; CAMPELLO DE SOUZA, R. M.; KAUFFMAN, A. N. Efficient multiplex for band-limited channels: Galois-field multiple access. In: **Proc. of the Workshop on Coding and Criptography**. Cambridge, United Kingdom: [s.n.], 1999. p. 235–241. Citado na página 16.

OPPENHEIM, A. V.; SCHAFER, R. W.; BUCK, J. R. **Discrete-Time Signal Processing**. 3nd. ed. [S.l.]: Pierson Hall, 2010. Citado 4 vezes nas páginas 16, 23, 44 e 55.

ORTEGA, A. et al. Graph signal processing: overview, challenges, and applications. **Proceedings of the IEEE**, v. 106, n. 5, p. 808–828, Maio 2018. Citado 2 vezes nas páginas 21 e 22.

PEDROUZO-ULLOA, A.; TRONCOSO-PASTORIZA, J. R.; PÉREZ-GONZÁLEZ, F. Number theoretic transforms for secure signal processing. **IEEE Trans. Inf. Forensics Security**, v. 12, n. 5, p. 1125–1140, Maio 2017. Citado na página 16.

POLLARD, J. M. The fast Fourier transform in a finite field. **Math. Comput.**, v. 25, n. 114, p. 365–374, Abril 1971. Citado 4 vezes nas páginas 16, 18, 28 e 32.

RAO, K. R.; YIP, P. **Discrete Cosine Transform: Algorithms, Advantages, Applications**. San Diego, CA: Academic, 1990. Citado na página 16.

RUBANOV, N. S. et al. The modified number theoretic transform over the direct sum of finite fields to compute the linear convolution. **IEEE Trans. on Signal Processing**, v. 46, n. 3, p. 813–817, 1998. Citado 3 vezes nas páginas 16, 32 e 36.

SANDRYHAILA, A.; MOURA, J. Discrete signal processing on graphs: Graph filters. **IEEE International Conference on Acoustics, Speech, and Signal Processing**, IEEE, v. 30, 2013. Citado na página 23.

SANDRYHAILA, A.; MOURA, J. M. F. Discrete signal processing on graphs. **IEEE Transactions on Signal Processing**, v. 61, n. 7, p. 1644–1656, 2013. Citado na página 21.

SANDRYHAILA, A.; MOURA, J. M. F. Discrete signal processing on graphs: graph Fourier transform. In: **2013 IEEE International Conference on Acoustics, Speech and Signal Processing**. Institute of Electrical and Electronics Engineers (IEEE), 2013. Disponível em: <https://doi.org/10.1109%2Ficassp.2013.6638850>. Citado 2 vezes nas páginas 17 e 21.

SANDRYHAILA, A.; MOURA, J. M. F. Big data analysis with signal processing on graphs: Representation and processing of massive data sets with irregular structure. **IEEE Signal Process. Mag.**, IEEE, v. 31, n. 5, p. 80–90, 2014. Citado na página 21.

SANDRYHAILA, A.; MOURA, J. M. F. Big data analysis with signal processing on graphs: Representation and processing of massive data sets with irregular structure. **IEEE Signal Processing Magazine**, v. 31, n. 5, p. 80–90, Setembro 2014. Citado na página 22.

SANDRYHAILA, A.; MOURA, J. M. F. Discrete signal processing on graphs: Frequency analysis. **IEEE Transactions Signal Processing**, v. 62, n. 12, p. 3042–3054, Julho 2014. Citado na página 21.

SARDELLITTI, S.; BARBAROSSA, S.; LORENZO, P. D. On the graph Fourier transform for directed graphs. **IEEE Journal of Selected Topics in Signal Processing**, v. 11, n. 6, p. 796–811, Setembro 2017. Citado na página 17.

SHANNON, C. **The mathematical theory of communication.** Dissertação (University of Illinois Press) — University of Illinois, 1949. Citado na página 62.

SHU, W.; TIANREN, Y. Algorithm for linear convolution using number theoretic transforms. **Electronics Letters**, v. 24, n. 5, p. 249–250, 1988. Citado 3 vezes nas páginas 16, 32 e 36.

SHUMAN, D. I.; FARAJI, M. J.; VANDERGHEYNST, P. A multiscale pyramid transform for graph signals. **IEEE Transactions on Signal Processing**, v. 64, n. 8, p. 2119–2134, 2016. Citado 2 vezes nas páginas 17 e 23.

SHUMAN, D. I. et al. The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains. **IEEE Signal Processing Magazine**, v. 30, n. 3, p. 83–98, Maio 2013. Citado 2 vezes nas páginas 17 e 21.

SHUMAN, D. I.; RICAUD, B.; VANDERGHEYNST, P. A windowed graph Fourier transform. In: IEEE. **Statistical Signal Processing Workshop (SSP), 2012 IEEE**. [S.l.], 2012. p. 133–136. Citado na página 17.

SILVA, D. et al. A transformada numérica de hartley e grupos de inteiros gaussianos. **Journal of Communication and Information Systems**, v. 17, n. 1, p. 48–57, 2002. Citado 3 vezes nas páginas 28, 34 e 37.

SMART, N. **ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)**. [S.l.], 2012. Citado na página 62.

STOJANOVSKI, T.; KOCAREV, L. Chaos-based random number generators – part I: analysis. **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, v. 48, n. 3, p. 281–288, Março 2001. Citado 2 vezes nas páginas 63 e 65.

STOJANOVSKI, T.; PIHL, J.; KOCAREV, L. Chaos-based random number generators – part II: practical realization. **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, v. 48, n. 3, p. 382–385, Março 2001. Citado 2 vezes nas páginas 63 e 65.

TAMORI, H.; AOKI, N.; YAMAMOTO, T. A fragile digital watermarking technique by number theoretic transform. **IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences**, E85-A, n. 8, p. 1902–1904, Agosto 2002. Citado 2 vezes nas páginas 16 e 60.

TOIVONEN, T.; HEIKKILÄ, J. Video filtering with Fermat number theoretic transforms using residue number system. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 16, n. 1, p. 92–101, Janeiro 2006. Citado 2 vezes nas páginas 16 e 36.

USC-SIPI. <http://sipi.usc.edu/database/>. 2018. Citado na página 63.

VENTURINI, I.; DUHAMEL, P. Reality preserving fractional transforms. In: **Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)**. Montreal, Canada: [s.n.], 2004. p. 205–208. Citado na página 70.

WU, Y.; NOONAN, J. P.; AGAIAN, S. NPCR and UACI randomness tests for image encryption. **Cyber J.: J. Sci. Technol. J. Sel. Areas Telecommun**, p. 31–38, April 2011. Citado 2 vezes nas páginas 64 e 65.

XU, J.; ZENG, B.; WU, F. An overview of directional transforms in image coding. In: **Proc. IEEE Int. Symp. Circuits Syst.** [S.l.: s.n.], 2010. p. 3036–3039. Citado na página 17.

YANG, Y.-G. et al. Novel image encryption based on quantum walks. **Scientific Reports**, v. 5, p. 1–9, Janeiro 2015. Citado 3 vezes nas páginas 64, 68 e 71.

YOUSSEF, A. M. On the security of a cryptosystem based on multiple-parameters discrete fractional Fourier transform. **IEEE Signal Processing Letters**, v. 15, p. 77–78, Janeiro 2008. Citado 2 vezes nas páginas 61 e 69.

ZENG, B.; FU, J. Directional discrete cosine transforms - a new framework for image coding. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 18, n. 3, p. 305–313, Março 2008. Citado na página 17.

ZHANG, L. Y. et al. Bi-level protected compressive sampling. **IEEE Transactions on Multimedia**, v. 18, n. 9, p. 1720–1732, Sep. 2016. ISSN 1520-9210. Citado na página 27.

ZHAO, T. et al. Security of image encryption scheme based on multi-parameter fractional Fourier transform. **Optics Communications**, v. 376, p. 47–51, Outubro 2016. Citado 2 vezes nas páginas 61 e 69.