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

JOSÉ RODRIGUES DE OLIVEIRA NETO

CONSTRUÇÃO DE AUTOVETORES DE TRANSFORMADAS DISCRETAS DE FOURIER: novos métodos e aplicações

Recife

2019

JOSÉ RODRIGUES DE OLIVEIRA NETO

CONSTRUÇÃO DE AUTOVETORES DE TRANSFORMADAS DISCRETAS DE FOURIER: novos métodos e aplicações

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.

Coorientador: Prof. Dr. Daniel Panario.

Recife

2019

Catalogação na fonte
Bibliotecária Valdicéa Alves, CRB-4 / 1260

O48c Oliveira Neto, José Rodrigues de.
Construção de autovetores de transformadas discretas de Fourier: novos métodos e aplicações / José Rodrigues de Oliveira Neto - 2019.
135folhas, Il.; Tabs.; Abr.; Siglas. e Simb.

Orientador: Prof. Dr. Juliano Bandeira Lima.
Coorientador: Prof. Dr. Daniel Panario.

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

1. Engenharia Elétrica. 2. Transformada fracionária de Fourier. 3. Transformada fracionária numérica de Fourier. 4. Autovetores do tipo Hermite-Gaussiano. 5. Representação compacta de sinais. 6. Cifragem de imagens. Lima, Juliano Bandeira (Orientador). II. Panario, Daniel. III. Título.

UFPE

621.3 CDD (22. ed.) BCTG/2019 - 45

Universidade Federal de Pernambuco
Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE TESE DE DOUTORADO DE

JOSÉ RODRIGUES DE OLIVEIRA NETO

TÍTULO

"CONSTRUÇÃO DE AUTOVETORES DE TRANSFORMADAS DISCRETAS DE FOURIER: NOVOS MÉTODOS E APLICAÇÕES"

A comissão examinadora composta pelos professores: JULIANO BANDEIRA LIMA, DES/UFPE; RICARDO MENEZES CAMPELLO DE SOUZA, DES/UFPE; DANIEL PEDRO BEZERRA CHAVES, DES/UFPE; FRANCISCO MADEIRO BERNARDINO JÚNIOR, POLI/UPE e EDUARDO SHIRLIPPE GÓES LEANDRO, DM/UFPE, sob a presidência do primeiro, consideram o candidato **JOSÉ RODRIGUES DE OLIVEIRA NETO** **APROVADO**.

Recife, 23 de janeiro de 2019.

MARCELO CABRAL CAVALCANTI
Coordenador do PPGEE

JULIANO BANDEIRA LIMA
Orientador e Membro Titular Interno

FRANCISCO MADEIRO BERNARDINO JÚNIOR
Membro Titular Externo

RICARDO MENEZES CAMPELLO DE SOUZA
Membro Titular Interno

EDUARDO SHIRLIPPE GÓES LEANDRO
Membro Titular Externo

DANIEL PEDRO BEZERRA CHAVES
Membro Titular Interno

Dedico esse trabalho à minha família.

AGRADECIMENTOS

Primeiramente agradeço à minha família: Jó, Valderio, Walber, Walderio, Roberta, aos meus avós, tios, tias, primos-irmãos..., eu os amo muito.

Aos amigos que permanecem tão próximos, embora às vezes distantes geograficamente: Thiego, Rafael, Vitu, Diego, Amr, todos do RPG e Pizza, Primos Unidos e Conselho S.T.P.A.. Aos amigos que fiz no Canadá e que me mostraram que pessoas boas e dispostas a ajudar existem em qualquer lugar do mundo: Felipe, Lucas, Thaís, Jéssica, Andrey, Gustavo, Diego e Hellen.

Ao meu orientador Prof. Juliano, por ter me aceitado como orientando, mesmo eu tendo trabalhado em áreas diferentes durante toda a minha vida acadêmica; para ficar apenas no campo acadêmico: o senhor é o exemplo de pesquisador, professor e orientador que pretendo tentar seguir. Ao meu coorientador Prof. Daniel, por toda a ajuda e ensinamentos, principalmente durante o intercâmbio no Canadá, espero que continuemos a trabalhar juntos.

Aos professores e colaboradores do Grupo de Pesquisa em Processamento de Sinais, que influenciaram e ajudaram tanto nos resultados desse trabalho, quanto na minha formação; em especial aos colaboradores Ravi, Verusca e Marcos e aos professores Ricardo Campello e Gilson Jerônimo que ajudaram diretamente neste trabalho.

A todos os professores que participaram da minha formação, começando por minha mãe, minha primeira professora.

A todos os técnicos e funcionários da UFPE que participaram da minha estadia de mais de uma década nesta universidade, principalmente os do DES, que foi minha casa pela maior parte desses anos.

Ao CNPq e a CAPES pelo suporte financeiro a este trabalho.

RESUMO

Neste trabalho, são investigados métodos baseados em fórmulas fechadas para construção de autovetores de transformadas discretas de Fourier definidas (i) sobre o corpo dos reais e (ii) sobre corpos finitos. No primeiro caso, os métodos investigados, que empregam principalmente as chamadas matrizes geradoras, foram utilizados na definição de transformadas fracionárias discretas de Fourier (DFrFT) usando autovetores do tipo Hermite-Gaussiano (HGL). Com respeito a esses autovetores, foi apontada a convergência de suas componentes para amostras das funções Hermite-Gaussianas contínuas (HGF) correspondentes e foram propostas soluções para algumas restrições relacionadas à sua construção. A DFrFT proposta foi aplicada aos cenários de filtragem e de representação compacta de sinais no domínio fracionário e, nesses contextos, apresentou benefícios com relação a outras abordagens descritas na literatura. Em particular, demonstrou-se que a DFrFT em questão pode ser calculada de forma exata e aproximada com complexidade aritmética de 50% a 80% menor que a de outras DFrFT baseadas na auto-decomposição da matriz da transformada discreta de Fourier. Em relação ao estudo sobre corpos finitos, foi apresentado um método, também baseado em matrizes geradoras, para construção de autovetores da transformada numérica de Fourier (FNT). Foi proposto um método para criação dessas matrizes a partir de parâmetros escolhidos; exemplos específicos foram apresentados. Foi proposta uma metodologia, baseada nas referidas matrizes, para construção de bases ortogonais de autovetores da FNT, a partir das quais se pôde definir versões fracionárias dessa transformada. A transformada fracionária numérica definida foi então utilizada no cenário de cifragem de imagem, em que medidas para caracterização de robustez a ataques criptográficos indicaram seu potencial de uso prático; comparações com diversos trabalhos correlatos existentes na literatura revelaram benefícios do esquema proposto com relação à flexibilidade e à segurança, por exemplo.

Palavras-chave: Transformada fracionária de Fourier. Transformada fracionária numérica de Fourier. Autovetores do tipo Hermite-Gaussiano. Representação compacta de sinais. Cifragem de imagens.

ABSTRACT

In this work, we investigate methods to construct closed-form eigenvectors of discrete Fourier transforms defined (i) over the real field and (ii) over finite fields. Regarding the real-valued case, we construct discrete fractional Fourier transforms (DFrFT) using the so-called generating matrices and recently introduced closed-form Hermite-Gaussian-like (HGL) eigenvectors; we discuss the convergence of the components of such eigenvectors to samples of the corresponding continuous Hermite-Gaussian functions (HGF) and propose solutions to deal with some restrictions related to their construction. The proposed DFrFT is applied to the scenarios of filtering and compact representation of signals in the fractional domain and, in these contexts, it presents benefits when compared to other approaches described in the literature. In particular, we have shown that the referred DFrFT, or its proposed rounded version, can be calculated with arithmetic complexity 50% to 80% lower than other eigendecomposition-based DFrFT. In the finite field framework, a method based on generating matrices for the construction of Fourier number transform (FNT) eigenvectors is presented. We explain how to create such matrices from chosen parameters and present illustrative examples. Based on these matrices, a methodology to construct orthogonal bases of FNT eigenvectors is introduced and fractional versions of this transform are defined. The defined fractional transform is then used in the image encryption scenario, where metrics for characterizing the robustness of the scheme against cryptographic attacks indicated its potential for practical usage; a comparison with several related works revealed advantages of the proposed scheme regarding flexibility and security, for instance.

Keywords: Fractional Fourier transform. Fracional Fourier number transforms. Hermite-Gaussian-like eigenvectors. Compact signal representation. Image encryption.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

bpp	Bits per pixel
DFT	Discrete Fourier transform
DFrFT	Discrete fractional Fourier transform
FNT	Fourier number transform
FT	Fourier transform
FrFT	Fractional Fourier transform
FrFNT	Fractional Fourier number transform
HGF	Hermite-Gaussian function
HGL	Hermite-Gaussian-like
MFrFNT	Multiple-parameter fractional Fourier number transform
NPCR	Number of pixels change rate
LI	Linearmente independente
LSB	Least significant bit
SNR	Signal-to-noise ratio
UACI	Unified average changing intensity

LISTA DE SÍMBOLOS

Λ	Matriz diagonal cujos elementos são autovalores da transformada de Fourier (p. 56).
Γ	Transformada de Arnold (p. 97).
$\{\mathbf{\Phi}_m\}$	Base ortonormal de autovetores HGL da DFT (p. 30) e sua contraparte em corpos finitos, a base ortogonal de autovetores HGL da FNT (p. 79).
$\psi_m(t)$	Função Hermite-Gaussiana de ordem m.
a	Ordem fracionária (p. 56).
$\mathbf{a}$	Vetor de ordens fracionárias (p. 97).
A_N	Número total de adições para o cálculo da DFrFT de comprimento N (p. 67).
$\{\mathbf{c}_m^{\perp}\}$	Base ortonormal de autovetores HGL da DFT (p. 46).
$\mathrm{cov}(x, y)$	Covariância (p. 105).
$\{\mathbf{e}_m^{\perp}\}$	Base ortogonal de autovetores da FNT (p. 101).
$\mathbf{E}$	Matriz cujas colunas são formadas por uma base ortonormal de autovetores da transformada de Fourier (p. 56).
$E(x)$	Esperança (p. 105).
$\mathbb{F}_q$	Corpo finito de característica q.
$\{\mathbf{g}_m^{\perp}\}$	Base ortogonal de autovetores HGL da FNT (p. 81).
$\{\hat{\mathbf{g}}_m^{\perp}\}$	Base ortonormal de autovetores HGL da DFT (p. 34).
$\overline{H}$	Entropia normalizada (p. 108).
i	Raiz quadrada de menos um.
I_N	Sequência $I_N := \{-M+1, -M+2, \ldots, -M+N\}$, $M = \left\lfloor \frac{N+1}{2} \right\rfloor$.
$\#\{j\}$	Multiplicidade do autovalor $j = \{1, -i, -1, i\}$ da FNT.
M_N	Número total de multiplicações para o cálculo da DFrFT de comprimento N (p. 66).
$M_{\mathbf{A}}$	Numero total de elementos que podem ser escolhidos em uma matriz $\mathbf{A}$ (p. 100) e (p. 101).

N	Comprimento da transformada.
r_{xy}	Coeficiente de correlação (p. 105).
$S(k)$	Sequência definida na Definição 2.1 (p. 29).
$S_\zeta(k)$	Sequência definida na Definição 4.3 (p. 78).
var(x)	Variância (p. 105).

SUMÁRIO

1 INTRODUÇÃO

O campo de processamento digital de sinais sempre se beneficiou de uma estreita conexão entre a teoria e aplicações práticas em novas tecnologias. O apelo para o uso de transformadas discretas em aplicações do processamento de sinais vem do fato de essas transformadas possuírem algoritmos eficientes para o seu cálculo e implementação possível em sistemas digitais (SCHAFER; OPPENHEIM, 1999; COOLEY; TUKEY, 1965).

A transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*) é o mais conhecido exemplo de uma classe geral de transformadas de comprimento finito, cujas expressões de análise e síntese, na forma unitária, podem ser escritas, respectivamente, como

$$\mathbf{X}[k] := \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \mathbf{x}[n]\phi_k^*[n]$$

e

$$\mathbf{x}[n] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathbf{X}[k]\phi_k[n], \quad k, n = 0, 1, \ldots, N-1; \tag{1.1}$$

as sequências $\phi_k[n]$ se referem a uma base ortogonal, i.e.,

$$\frac{1}{N} \sum_{n=0}^{N-1} \phi_k[n]\phi_m^*[n] = \begin{cases} 1, & m = k, \\ 0, & m \neq k. \end{cases}$$

No caso da DFT, essa base é composta pelas sequências de exponenciais complexas, $e^{i2\pi nk/N}$. O uso de diferentes bases ortogonais nas expressões dadas em (1.1) leva à definição de outras transformadas como, por exemplo, a transformada de Walsh-Hadamard (ELLIOTT; RAO, 1982), aplicável à codificação de imagens, reconhecimento de padrões e filtragem (SUNDARARAJAN; AHMAD, 1998); a transformada de Hartley (BRACEWELL, 1983) usada, entre outras aplicações, em sistemas de cifragem de imagens (LIN, 2013); a transformada do cosseno (AHMED; NATARAJAN; RAO, 1974; RAO; YIP, 1990) vastamente utilizada em padrões de compressão de imagens e vídeo (WALLACE, 1992; MPEG, 1994; HEVC, 2013; POURAZAD et al., 2012); e as transformadas wavelet (DAUBECHIES, 1990; SHENG, 2010), ou "ondaletas", empregadas, por exemplo, em sistemas de compressão de imagens como o padrão JPEG 2000 (SKODRAS; CHRISTOPOULOS; EBRAHIMI, 2001).

O estudo das transformadas sobre corpos finitos teve início na década de 1970, quando John M. Pollard apresentou o artigo "*The fast Fourier transform in a finite field*" (POLLARD, 1971). No referido trabalho, o matemático britânico trouxe a definição da transformada de Fourier sobre corpos finitos, enfatizando a existência de algoritmos rápidos para o seu cálculo.

Nesse contexto, é relevante lembrar que um corpo $\mathbb{F}$, ou $< F, +, . >$, é uma estrutura algébrica composta de um conjunto F, que contém ao menos dois elementos, e duas operações definidas (comumente chamadas de adição "+" e multiplicação "."), para a qual os seguintes axiomas são satisfeitos (BLAHUT, 2010):

(i) o conjunto F e a operação de adição formam um grupo abeliano, $< F, + >$;

(ii) o conjunto F é fechado sob a multiplicação e o subconjunto dos elementos não nulos de F, juntamente com a operação de multiplicação, forma o grupo abeliano, $< F^*, . >$;

(iii) a lei distributiva, $(a + b)c = ac + bc$, é válida para todos a,b e c pertencentes ao corpo.

Em um corpo, é convencional denotar a identidade da operação adição por '0'; denotar o inverso aditivo de a por $-a$; chamar de '1' o elemento identidade da multiplicação; e denotar o inverso multiplicativo de a por a^{-1}. Quando o corpo possui um número q finito de elementos, é chamado de corpo finito e é denotado por $\mathbb{F}_q$ ou $GF(q)$ (do inglês *Galois Field*), em homenagem ao matemático francês Évariste Galois (1811-1832) (BLAHUT, 2010).

Dependendo da característica do corpo finito, as operações sobre um corpo $\mathbb{F}_q$ podem envolver adições e multiplicações módulo um número primo apenas; neste caso, a aplicação de operadores matemáticos definidos sobre corpos finitos se mostra atrativa por não requerer operações de ponto flutuante. Além disso, as referidas operações modulares podem ser implementadas com deslocamentos, reduzindo o esforço computacional para estes cálculos (BLAHUT, 2010; TOIVONEN; HEIKKILA, 2006; AGARWAL; BURRUS, 1974; DESCHAMPS, 2009; DE OLIVEIRA NETO; LIMA, 2018).

Embora o estudo das transformadas sobre corpos finitos possua várias particularidades no seu desenvolvimento, geralmente ele é guiado pela existência de transformadas análogas já definidas no corpo dos reais. Neste sentido, após o trabalho de Pollard, versões em corpos finitos das transformadas clássicas foram definidas e estudadas. Esse é o caso da transformada de Hartley (CAMPELLO DE SOUZA et al., 1998a; CAMPELLO DE SOUZA; H. M. DE OLIVEIRA; KAUFFMAN, 2000), cujas aplicações incluem o projeto de sistemas de multiplexação digital, sistemas de múltiplo acesso e sequências digitais para espalhamento espectral multinível (CAMPELLO DE SOUZA; H. M. DE OLIVEIRA; KAUFFMAN, 2000; DE OLIVEIRA; CAMPELLO DE SOUZA; KAUFFMAN, 1999; MIRANDA; DE OLIVEIRA, 2001; DE OLIVEIRA; MIRANDA; CAMPELLO DE SOUZA, 2001). Por sua vez, a transformada wavelet sobre corpos finitos foi apresentada na metade da década de 1990 (POOR, 1996), possuindo aplicabilidade em códigos corretores de erro e sistemas criptográficos (FEKRI et al., 2006; CHAN; FEKRI, 2004).

Em 2004, foi introduzida uma primeira transformada do cosseno sobre corpos finitos (CAMPELLO DE SOUZA et al., 2004), a qual se baseia em funções trigonométricas definidas sobre essas estruturas algébricas, sendo seguida pela publicação da transformada do seno sobre corpos finitos (CAMPELLO DE SOUZA et al., 2005). A partir desses trabalhos,

posteriores estudos apresentaram outros sete tipos de transformadas do cosseno e sete tipos de transformadas do seno definidas sobre corpos finitos (LIMA; CAMPELLO DE SOUZA, 2011). Foram investigadas, ainda, as autoestruturas dessa família de transformadas (LIMA; CAMPELLO DE SOUZA; PANARIO, 2011) e, mais recentemente, propostos algoritmos rápidos visando o seu cálculo eficiente (LIMA, 2015; DE OLIVEIRA NETO; LIMA, 2018). Tais estudos têm sido estimulados pela sua aplicabilidade em sistemas de marca d'água frágil (CINTRA et al., 2009) e esquemas de cifragem de imagens (LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015).

O estudo da autoestrutura das transformadas discretas sobre os reais (DICKINSON; STEIGLITZ, 1982; CLARY; MUGLER, 2003; GUREVICH; HADANI, 2009) ampliou os horizontes de aplicação dessas ferramentas e originou novas linhas de pesquisa. Uma das linhas atualmente em expansão é a das transformadas fracionárias, as quais correspondem, basicamente, a uma generalização em que se permite aplicar a um sinal potências não-inteiras do operador associado às respectivas transformadas ordinárias (SEJDIĆ; DJUROVIĆ; STANKOVIĆ, 2011; BULTHEEL; SULBARAN, 2004; WEI; RAN, 2011). A aplicabilidade das transformadas fracionárias pode ser ilustrada por meio de trabalhos recentes da área de processamento de sinais de radar (ELGAMEL; SORAGHAN, 2011; SINGH; DATCU, 2013), processamento de sinais geofísicos (MIAH; POTTER, 2014), processamento de imagens médicas (XU; WANG; CHEN, 2016), reconhecimento de padrões (CHEN et al., 2014), entre outros. A transformada fracionária mais conhecida é a de Fourier, originalmente caracterizada no cenário de sinais de variável contínua, mas também amplamente estudada em suas versões discretas.

Um dos trabalhos de destaque relacionado à transformada discreta fracionária de Fourier (DFrFT, do inglês *discrete fractional Fourier transform*) é o desenvolvido por Pei e Yeh (PEI; YEH, 1997), em que se empregou o conceito de matrizes comutantes da DFT bem como resultados acerca de sua autoestrutura (DICKINSON; STEIGLITZ, 1982). Mais especificamente, denotando por $\mathbf{F}$ a matriz da DFT de comprimento N, em que $F(k,n) = e^{-i2\pi nk/N}$, escreve-se

$$\mathbf{F} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^T,$$

em que as colunas da matriz $\mathbf{E}$ são formadas por autovetores da matriz $\mathbf{F}$ e cujos autovalores formam a matriz diagonal $\mathbf{\Lambda}$. Assim, define-se o operador transformada fracionária $\mathbf{F}^a = \mathbf{E}\mathbf{\Lambda}^a\mathbf{E}^T$, em que $a \in \mathbb{R}$ (CANDAN; KUTAY; OZAKTAS, 2000). Devido à existência de diferentes formas de expandir espectralmente a matriz $\mathbf{F}$, dado que esta possui autovalores repetidos, diferentes definições para a DFrFT vêm sendo apresentadas. Particular interesse existe em empregar autovetores do tipo Hermite-Gaussiano em tal expansão, visto que esses seriam análogos às funções Hermite-Gaussianas contínuas sobre as quais se expande o operador (integral) da transformada de Fourier e se define, deste modo, a versão fracionária dessa transformada; uma DFrFT assim construída seria, então, uma generalização da DFT no mesmo sentido em que a FrFT corresponde a uma generalização da transformada de Fourier ordinária (PEI; YEH, 1997; CANDAN; KUTAY; OZAKTAS, 2000).

Continuando o trabalho apresentado em (PEI; YEH, 1997), Candan et al. (CANDAN; KUTAY; OZAKTAS, 2000) apresentaram uma nova definição para a DFrFT, solucionando algumas questões teóricas deixadas no trabalho anterior e apresentando um novo método para cálculo dos autovetores da DFT também baseado na matriz comutante da DFT apresentada em (DICKINSON; STEIGLITZ, 1982). Mais recentemente, Serbes e Durak-Ata apresentaram uma nova forma para escolha e cálculo dos autovetores a partir da matriz da DFT centralizada, usando esse conjunto de vetores para definir uma transformada fracionária discreta (SERBES; DURAK-ATA, 2011).

Em 2009, Pei e Chang apresentaram uma forma sistemática para construir autovetores da DFT utilizando uma matriz geradora, $\mathbf{S}$, tal que a partir de um autovetor $\mathbf{v}$, relacionado a um autovalor λ, calcula-se outro autovetor $\mathbf{v}' = \mathbf{S}\mathbf{v}$, relacionado ao autovalor $\lambda' = \lambda^{1/2}$. No mesmo trabalho, foi ainda apresentada uma nova matriz que comuta com a matriz da DFT, $\mathbf{S}^{\mathbf{T}}\mathbf{S}$ (PEI; CHANG, 2009). Utilizando o trabalho anterior, em (PEI; CHANG, 2016), Pei e Chang apresentaram aproximações para vetores Hermite-Gaussianos de ordens mais altas a partir de uma generalização do vetor Hermite-Gaussiano de ordem zero apresentado por Kong (KONG, 2008).

Também motivado por (KONG, 2008), o matemático Alexey Kuznetsov construiu um novo algoritmo para o cálculo dos autovetores da DFT a partir de fórmulas fechadas. Ele, inicialmente, demonstrou a convergência dos primeiros vetores gerados para as respectivas funções Hermite-Gaussianas contínuas (KUZNETSOV, 2015) e, em um trabalho posterior, provou que a convergência é válida para todo o conjunto (KUZNETSOV; KWASNICKI, 2018).

Nos últimos anos, também foram definidas transformadas fracionárias sobre corpos finitos (PEI; WEN; DING, 2011; LIMA; CAMPELLO DE SOUZA, 2012; LIMA; CAMPELLO DE SOUZA, 2013; LIMA; LIMA; CAMPELLO DE SOUZA, 2017; LIMA; CAMPELLO DE SOUZA, 2016). Dentre as diversas abordagens empregadas com esta finalidade, merece destaque aquela proposta por Lima e Campello de Souza em 2016, que, estendendo resultados apresentados em (KUZNETSOV, 2015), descreve procedimentos sistemáticos para construção de uma base de autovetores da transformada numérica de Fourier[1], define uma transformada fracionária relacionada a esses autovetores e demonstra sua aplicabilidade em um esquema de cifragem de imagens (LIMA; CAMPELLO DE SOUZA, 2016). Diante do exposto, é motivação para a escrita desta tese a possibilidade de contribuir com avanços na área de transformadas fracionárias, visando, em particular, à caracterização de técnicas para construção de autovetores de transformadas discretas de Fourier.

[1] A partir deste ponto, as transformadas de Fourier sobre corpos finitos serão identificadas como transformadas numéricas de Fourier. Essa terminologia é usualmente empregada quando transformadas definidas sobre corpos finitos primos, e não sobre corpos de extensão, são consideradas; este é o caso que se assume na maioria dos desenvolvimentos apresentados nesta tese. Além disso, este é o jargão que costuma ser empregado na comunidade de processamento de sinais, diferentemente do que acontece, por exemplo, na comunidade interessada em códigos corretores de erros, onde o uso de transformadas sobre corpos de extensão é mais corriqueiro (BLAHUT, 2003; BLAHUT, 2010).

1.1 OBJETIVOS

Objetivo geral:

O objetivo geral deste trabalho é desenvolver técnicas para construção de autovetores de transformadas discretas de Fourier definidas sobre o corpo dos reais e sobre corpos finitos, visando preencher lacunas teóricas relacionadas à caracterização dessas ferramentas matemáticas e aplicar os métodos estudados na definição de novas transformadas fracionárias sobre as referidas estruturas algébricas.

Objetivos específicos:

Os objetivos específicos desta proposta são:

1. Sistematizar a construção de autovetores da transformada discreta de Fourier a partir de fórmulas fechadas recentemente apresentadas na literatura (PEI; CHANG, 2016; KUZNETSOV, 2015), visando fornecer soluções para lacunas teóricas deixadas nos respectivos trabalhos;
2. Estender ao cenário de corpos finitos técnicas originalmente aplicadas à construção de autovetores da transformada discreta de Fourier, baseadas em matrizes geradoras (PEI; CHANG, 2009; PEI; CHANG, 2016);
3. Empregar as técnicas para construção de autovetores das transformadas discretas investigadas na obtenção de bases para a definição de transformadas fracionárias neste cenário;
4. Propor algoritmos rápidos para calcular de forma eficiente as transformadas fracionárias definidas a partir das bases mencionadas no objetivo específico 3, comparando a sua complexidade com a de algoritmos utilizados na computação de transformadas fracionárias baseadas noutras abordagens (OZAKTAS et al., 1996; CANDAN; KUTAY; OZAKTAS, 2000; PEI; CHANG, 2009; PEI; WEN; DING, 2011; LIMA; CAMPELLO DE SOUZA, 2012; LIMA; CAMPELLO DE SOUZA, 2013; KUZNETSOV, 2015; LIMA; LIMA; CAMPELLO DE SOUZA, 2017; LIMA; CAMPELLO DE SOUZA, 2016);
5. Realizar uma investigação a respeito de cenários em que as transformadas e os autovetores construídos são potencialmente aplicáveis. Estes cenários incluem, por exemplo, criptografia, representação compacta de sinais no domínio fracionário, comunicações, etc.

1.2 ESTRUTURA DO DOCUMENTO E CONTRIBUIÇÕES

O documento está estruturado da seguinte forma:

- No Capítulo 2, é apresentado o estudo sobre os métodos de construção de autovetores HGL da DFT a partir de fórmulas fechadas. É investigada a relação entre os métodos

dados em (KUZNETSOV, 2015; PEI; CHANG, 2016) e apresentadas soluções para lacunas teóricas deixadas no trabalho (PEI; CHANG, 2016). É apresentada uma família de matrizes geradoras e descrito como construir, empregando tal família, a autobase HGL da DFT proposta em (KUZNETSOV, 2015). Os conjuntos de autovetores considerados são utilizados para definir transformadas fracionárias discretas de Fourier; a aplicabilidade dessas transformadas em cenários práticos, como o da filtragem de sinais no domínio fracionário de Fourier, é avaliada por meio de simulações computacionais. Os resultados obtidos são comparáveis àqueles conseguidos empregando outras definições da DFrFT.

- No Capítulo 3, é introduzido um método com complexidade aritmética reduzida para o cálculo de uma das DFrFT definidas no Capítulo 2. A abordagem proposta explora as propriedades dos autovetores HGL da DFT introduzidos no capítulo anterior, que são usados para definir a DFrFT; além disso, uma estratégia de arredondamento que possibilita diminuir ainda mais a complexidade aritmética do cálculo da transformada é apresentada. Até onde o autor dessa tese tem conhecimento, o número de multiplicações e o de adições envolvidos no procedimento proposto são menores que quaisquer outros necessários ao cálculo de uma DFrFT baseada na autodecomposição da matriz da DFT. Mais especificamente, tomando por referência o algoritmo proposto em (MAJORKOWSKA-MECH; CARIOW, 2017), o número de adições é reduzido em cerca de 50% e o de multiplicações em até 65%. Os resultados são validados por meio de experimentos computacionais em que a aplicação da transformada fracionária na filtragem e na representação compacta de sinais no domínio fracionário é considerada.

- No Capítulo 4, é apresentado um método baseado em matrizes geradoras para a construção de autovetores da transformada numérica de Fourier (FNT, do inglês *Fourier number transform*). Define-se uma matriz geradora específica e, usando-a, demonstra-se como construir uma base ortogonal de autovetores do tipo Hermite-Gaussiano da FNT, que podem ser usados para definir uma transformada fracionária numérica de Fourier (FrFNT, do inglês *fractional Fourier number transform*). Em relação à autobase construída, são discutidos os principais aspectos e são realizadas comparações com bases construídas por outros métodos encontrados na literatura. Mais especificamente, a referida autobase é obtida usando fórmulas fechadas, não possui ambiguidades acerca da ordenação dos autovetores e permite que se evitem, considerando certos parâmetros como comprimento e característica do corpo finito em que a respectiva transformada fracionária é definida, cálculos em corpos de extensão.

- No Capítulo 5, é descrito um esquema de cifragem de imagens baseado na transformada fracionária multiparamétrica numérica de Fourier (MFrFNT, do inglês *multiple-parameter fractional Fourier number transform*). Para definir a MFrFNT, é introduzido um procedimento sistemático para construção de uma base de autovetores da FNT com parâmetros escolhidos. Testes para avaliar a robustez do sistema são realizados e os resultados sugerem

que o esquema proposto pode resistir aos ataques criptográficos usualmente considerados na literatura relacionada. Além disso, demonstra-se que o método proposto pode ser facilmente ajustado para lidar com diferentes tipos de imagem e que envolve um número maior de parâmetros livres do que outras técnicas de cifragem de imagem que também se baseiam em transformadas numéricas.

- No Capítulo 6, são revisitadas de forma sumária as principais contribuições do trabalho, elencados possíveis desdobramentos desta tese em trabalhos futuros e listadas as publicações relacionadas às investigações realizadas.
- No Apêndice A, são apresentadas as provas de algumas proposições do Capítulo 2.

2 TRANSFORMADA FRACIONÁRIA DISCRETA DE FOURIER BASEADA EM AUTOVETORES DO TIPO HERMITE-GAUSSIANO DA DFT

A transformada fracionária de Fourier (FrFT, do inglês *fractional Fourier transform*) tem sido aplicada em cenários práticos relacionados a óptica, processamento de sinais, comunicações, criptografia, mecânica quântica, etc. (NAMIAS, 1980; WEIMANN et al., 2016; LOHMANN, 1993; OZAKTAS; ZALEVSKY; KUTAY, 2001; LIU; SHERIDAN, 2013; ALMEIDA, 1994; WEI; LI, 2016; LIMA; NOVAES, 2014; WANG et al., 2016; TAO; MENG; WANG, 2011; ZHAO et al., 2016c; LU; XIAO; WEI, 2016; PELICH et al., 2016). A FrFT para funções de variáveis contínuas ou, considerando o jargão empregado na área de processamento de sinais, para sinais de tempo contínuo, é normalmente definida a partir da autodecomposição do operador transformada de Fourier (FT, do inglês *Fourier transform*). Mais especificamente, em (CANDAN; KUTAY; OZAKTAS, 2000), a FrFT é definida, para $0 < |a| < 2$, por meio da integral

$$\mathcal{F}^a f(t_a) = \int_{-\infty}^{\infty} K_a(t_a, t) f(t) dt,$$

em que

$$K_a(t_a, t) = K_\alpha \mathrm{e}^{i\pi\left(t_a^2 \cot(\alpha) - 2t_a t \csc(\alpha) + t^2 \cot(\alpha)\right)},$$

$\alpha = a\pi/2$ e $K_\alpha = \mathrm{e}^{\left(-i(\pi \mathrm{sgn}(\alpha)/4 - \alpha/2)/|\mathrm{sen}(\alpha)|^{0,5}\right)}$. O núcleo $K_a(t_a, t)$ é definido separadamente para $a = 0$ e $a = \pm 2$ como $K_0(t_a, t) = \delta(t_a - t)$ e $K_{\pm 2}(t_a, t) = \delta(t_a + t)$. A definição pode ser estendida para fora do intervalo $[-2, 2]$ notando que $\mathcal{F}^{4l+a} f(t_a) = \mathcal{F}^a f(t_a)$ para qualquer inteiro l. O núcleo é conhecido por possuir expansão espectral

$$K_a(t_a, t) = \sum_{k=0}^{\infty} \psi_k(t_a) \mathrm{e}^{\left(-i\frac{\pi}{2}ka\right)} \psi_k(t),$$

em que $\psi_k(t)$ é a k-ésima função Hermite-Gaussiana, e t_a denota a variável no domínio da transformada fracionária de Fourier de **ordem fracionária** a (CANDAN; KUTAY; OZAKTAS, 2000). Com isso, utiliza-se as funções Hermite-Gaussianas (HGF, do inglês *Hermite-Gaussian functions*), que constituem uma família canônica de autofunções da FT, diretamente no núcleo da transformada fracionária de Fourier.

Nas últimas décadas, várias estratégias para o cálculo digital da FrFT têm sido propostas (OZAKTAS et al., 1996; PEI; YEH; TSENG, 1999; CANDAN; KUTAY; OZAKTAS, 2000; PEI; HSUE; DING, 2006; SANTHANAN; SANTHANAN, 2007; BHATTA; SANTHANAM, 2015; HANNA; SEIF; AHMED, 2004; SERBES; DURAK-ATA, 2011). Idealmente, um método com tal propósito deve preencher os seguintes requisitos: (i) aproximar numericamente a FrFT, (ii) manter as propriedades da FrFT (ex. aditividade de índices e redução para FT quando a ordem fracionária é 1) e (iii) possuir algoritmos rápidos para o seu cálculo. Provavelmente, o método mais popular de cálculo digital da FrFT é o proposto em (OZAKTAS et al., 1996), em

que o núcleo da transformação é expresso como uma sucessão de operadores que podem ser discretizados e eficientemente calculados. De forma geral, este método cumpre os requisitos (i) e (iii), mas falha em satisfazer o (ii).

A FrFT também pode ser calculada a partir de versões discretas dessa transformada. Neste caso, é definida a transformada fracionária discreta de Fourier (DFrFT, do inglês *discrete fractional Fourier transform*), que generaliza a transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*) no mesmo sentido em que a FrFT generaliza a FT. Esta classe de transformadas normalmente emprega a expansão espectral da matriz da DFT N-dimensional, $\mathbf{F} = (F(k,n))$, cujo elemento na $(k+1)$-ésima linha e na $(n+1)$-ésima coluna é $F(k,n) = \frac{1}{\sqrt{N}} e^{-i\frac{2\pi}{N}kn}$, $k, n = 0, 1, \ldots, N-1$, $i := \sqrt{-1}$. Esta expansão é expressa como

$$\mathbf{F} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^T, \tag{2.1}$$

em que $\mathbf{E}$ é a matriz cujas colunas formam uma base ortonormal de autovetores da DFT para o $\mathbb{R}^N$, $\mathbf{\Lambda}$ é a matriz diagonal em que os elementos são os autovalores correspondentes da DFT (ver a Tabela 1 (MCCLELLAN; PARKS, 1972)) e $\mathbf{E}^T$ é a matriz transposta da matriz $\mathbf{E}$. Isso permite escrever

$$\mathbf{F}^a = \mathbf{E}\mathbf{\Lambda}^a\mathbf{E}^T, \tag{2.2}$$

que corresponde à matriz da DFrFT com ordem fracionária $a \in \mathbb{R}$.

Logo, dado um vetor $\mathbf{x}$ de comprimento N, com componentes $x(n) \in \mathbb{C}$, sua transformada fracionária relacionada à ordem fracionária a é o vetor $\mathbf{X}^{(a)}$ de comprimento N, com componentes $X^{(a)}(k) \in \mathbb{C}$, calculado por

$$\mathbf{X}^{(a)} = \mathbf{F}^a\mathbf{x} = \mathbf{E}\mathbf{\Lambda}^a\mathbf{E}^T\mathbf{x}. \tag{2.3}$$

Tabela 1 – Multiplicidade dos autovalores da matriz $N \times N$ da DFT.

N	1	$-i$	-1	i
$4L$	$L+1$	L	L	$L-1$
$4L+1$	$L+1$	L	L	L
$4L+2$	$L+1$	L	$L+1$	L
$4L+3$	$L+1$	$L+1$	$L+1$	L

Fonte: (MCCLELLAN; PARKS, 1972)

O ponto-chave da abordagem descrita acima é obter o conjunto de autovetores da DFT usados na matriz $\mathbf{E}$. Para definir uma DFrFT que cumpra o requisito (i), os autovetores devem ser versões discretas análogas das HGF contínuas. Neste sentido, vários métodos visando à construção desses autovetores têm sido propostos (PEI; YEH; TSENG, 1999; CANDAN;

KUTAY; OZAKTAS, 2000; PEI; HSUE; DING, 2006; SANTHANAN; SANTHANAN, 2007; BHATTA; SANTHANAM, 2015; HANNA; SEIF; AHMED, 2004; SERBES; DURAK-ATA, 2011)[1]. Estes métodos normalmente são baseados em matrizes comutantes com $\mathbf{F}$, entre os quais se encontra a bem conhecida matriz $\mathbf{S}$ e diversos tipos de matrizes tri-diagonalizáveis (PEI; YEH; TSENG, 1999; CANDAN; KUTAY; OZAKTAS, 2000; PEI; HSUE; DING, 2006; SANTHANAN; SANTHANAN, 2007; BHATTA; SANTHANAM, 2015). Outros métodos empregam o Teorema Espectral para decompor a matriz $\mathbf{F}$ e construir projeções ortogonais das quais os autovetores da DFT são obtidos (HANNA; SEIF; AHMED, 2004; SERBES; DURAK-ATA, 2011). Em ambas as abordagens (matrizes comutantes e decomposição espectral), a construção dos autovetores depende de procedimentos com fórmulas não-fechadas, que podem levar à perda de acurácia e indesejáveis efeitos numéricos.

Em publicações recentes, procedimentos para construção dos referidos autovetores da DFT a partir de fórmulas fechadas têm sido desenvolvidos (KUZNETSOV, 2015; PEI; CHANG, 2016). Essas abordagens são baseadas na generalização do trabalho de Kong (KONG, 2008), em que são apresentadas expressões analíticas para os vetores HGL de ordem zero e de ordem um para $N = 4L+1$. Mais especificadamente, em (KUZNETSOV, 2015), é descrito um método para construção de uma base ortonormal de autovetores HGL da DFT a partir de fórmulas fechadas. O autor demonstra que os primeiros oito autovetores convergem para as HGF correspondentes e conjectura que os demais vetores também convergem; em publicação posterior (KUZNETSOV; KWASNICKI, 2018), os autores provam a convergência para todos os autovetores. Em (PEI; CHANG, 2016), os autores empregam o vetor HGL de ordem zero (KONG, 2008) e o método dado em (PEI; CHANG, 2009) para construir vetores HGL para $N = 4L + 1$; os argumentos dados pelos autores para classificar estes vetores como HGL são equivalentes aos apresentados em (KUZNETSOV, 2015). Contudo, nenhuma demonstração sobre a possível convergência para as HGF contínuas correspondentes é apresentada.

Neste capítulo, são investigadas características dos autovetores HGL da DFT propostos em (KUZNETSOV, 2015) e (PEI; CHANG, 2016); discute-se a convergência desses autovetores e explica-se como estes autovetores podem ser usados para definir a DFrFT. Após a Seção 2.1, que contém uma revisão concisa de (KUZNETSOV, 2015) e (PEI; CHANG, 2016), descreve-se a relação entre esses dois trabalhos e apresenta-se, nesse contexto, as contribuições do presente trabalho.

i Na Seção 2.2, são caracterizados os autovetores HGL da DFT construídos de acordo com (PEI; CHANG, 2016), esclarecendo aspectos relacionados à sua independência linear e explicando como usá-los para obter uma base ortonormal. Também é introduzida uma abordagem *híbrida*, combinando os métodos dados em (KUZNETSOV, 2015)

[1] Existe ainda uma recente abordagem em que uma DFrFT randômica é definida (HSUE; CHANG, 2015a; KANG; ZHANG; TAO, 2015a; ANNABY; RUSHDI; NEHARY, 2016a); no entanto, os autovetores empregados nessas técnicas não são do tipo Hermite-Gaussiano, por isso não são considerados neste capítulo.

e (PEI; CHANG, 2016). Esta nova abordagem permite utilizar o método das matrizes geradoras (PEI; CHANG, 2009) para construir bases de autovetores HGL da DFT para $N = 4L + 3$, $N = 4L$ e $N = 4L + 2$, casos não cobertos por (PEI; CHANG, 2016).

ii Na Seção 2.3, é feita uma comparação em relação à aproximação numérica entre as HGF contínuas e os vetores construídos na Seção 2.2 e os propostos em (KUZNETSOV, 2015) e (PEI; CHANG, 2016). Também é introduzida uma nova matriz geradora, a qual é utilizada para construção de autovetores HGL da DFT que aproximam as HGF contínuas melhor que as abordagem anteriormente descritas.

iii Na Seção 2.4, uma família de matrizes geradoras é definida. Utilizando essa família de matrizes e vetores sementes construídos segundo a abordagem descrita em (KUZNETSOV, 2015), é proposto um método para geração de uma autobase HGL da DFT. Além do mais, é provado que essa base é a mesma apresentada em (KUZNETSOV, 2015).

iv Na Seção 2.5, é descrito como utilizar os autovetores investigados nas seções anteriores para definir uma DFrFT de acordo com (2.2). As DFrFT propostas são empregadas na transformação de um sinal discreto padrão e na filtragem no domínio fracionário. Os resultados são comparados com os obtidos por meio dos métodos dados em (OZAKTAS et al., 1996) e (CANDAN; KUTAY; OZAKTAS, 2000). De forma geral, é mostrado que os métodos discutidos neste capítulo podem ser utilizados em cenários práticos sem perdas significativas de precisão.

2.1 TRABALHOS RELACIONADOS

Recentemente, foram propostas duas interessantes abordagens para a construção de autovetores HGL da DFT a partir de fórmulas fechadas (KUZNETSOV, 2015; PEI; CHANG, 2016). Ambos os métodos são baseados na generalização do vetor $\mathbf{f}_0$, proposto em (KONG, 2008), cujas componentes $f_0(n)$, $n = 0, 1, \ldots, N-1$, são calculadas a partir de

$$f_0(n) = \prod_{s=L+1}^{2L} \left[\cos\left(n\frac{2\pi}{N}\right) - \cos\left(s\frac{2\pi}{N}\right) \right], \tag{2.4}$$

para $N = 4L + 1$. De acordo com (KONG, 2008), o vetor $\mathbf{f}_0$ pode ser visto como a contraparte discreta da HGF contínua de ordem zero basicamente devido à coincidência entre a forma do vetor e aquela da função contínua correspondente. Na sequência da seção, é explicado como o vetor $\mathbf{f}_0$ pode ser generalizado para produzir versões discretas dilatadas de sinais Gaussianos contínuos, as quais são utilizadas para criação de autovetores HGL da DFT.

2.1.1 Autovetores HGL a partir de Combinações Lineares de Sinais Gaussianos Dilatados Discretos

Em (KUZNETSOV, 2015), uma versão centralizada e unitária da DFT foi utilizada, em que um vetor $\mathbf{x} = (x(n))$ é mapeado em um vetor $\mathbf{X} = (X(k))$ de acordo com

$$X(k) := \frac{1}{\sqrt{N}} \sum_{n \in I_N} x(n) e^{-i\frac{2\pi}{N}kn}, \;\; k \in I_N,$$

em que $I_N := \{-M+1, -M+2, \ldots, -M+N\}$, $M = \left\lfloor \frac{N+1}{2} \right\rfloor$. A única diferença entre a versão centralizada e a não-centralizada da DFT é o conjunto dos valores dos índices n e k considerados em cada transformada. Estes conjuntos de N índices podem ser tratados de uma maneira cíclica, ou seja, as duas transformadas são essencialmente a mesma. Para simplificar a notação e deixar o texto mais conciso, não será mencionado explicitamente qual das transformadas está sendo considerada. O cálculo de $\mathbf{X}$ pode ser expresso como $\mathbf{X} = \mathbf{F}\mathbf{x}$, em que a componente na $(k+M)$-ésima linha e na $(n+M)$-ésima coluna da matriz de transformação $\mathbf{F}$ é dada por $F(k+M, n+M) = e^{-i\frac{2\pi}{N}kn}$. A abordagem considera o *suporte próprio*, $\mathrm{supp}(\mathbf{x})$, de um vector $\mathbf{x}$, que corresponde ao conjunto de todos os índices $n \in I_N$ tal que $x(n) \neq 0$. Isso é usado para definir o *comprimento* de um vetor $\mathbf{x}$ como

$$l(\mathbf{x}) := \max\{m - n + 1 : m, n \in \mathrm{supp}(\mathbf{x})\}.$$

Relaciona-se o comprimento de um vetor $\mathbf{x}$ e da sua DFT $\mathbf{F}\mathbf{x}$ por meio da inequação

$$l(\mathbf{x}) + l(\mathbf{F}\mathbf{x}) \geq N + 1. \tag{2.5}$$

A inequação acima, que é uma contraparte discreta do princípio da incerteza (DE OLIVEIRA, 2007), segue do Teorema 1 em (KONG, 2008). Em (KUZNETSOV, 2015), os vetores de simetria par/ímpar que têm o valor $l(\mathbf{x}) + l(\mathbf{F}\mathbf{x})$ menor possível são ditos *ótimos* e existem em número dado pelo teorema a seguir.

Teorema 2.1. *(KUZNETSOV, 2015) Assumindo que $N \geq 3$,*

i. Se $N = 2K+1$, existem apenas $K+1$ vetores pares não-nulos que satisfazem $l(\mathbf{u}) + l(\mathbf{F}\mathbf{u}) = N+1$ e apenas K vetores ímpares não-nulos satisfazendo $l(\mathbf{v}) + l(\mathbf{F}\mathbf{v}) \leq N+3$.

ii. Se $N = 2K$, existem apenas $K-1$ vetores pares não-nulos que satisfazem $u(K) = (Fu)(K) = 0$ e $l(\mathbf{u}) + l(\mathbf{F}\mathbf{u}) \leq N+2$ e apenas $K-1$ vetores ímpares não-nulos satisfazendo $l(\mathbf{v}) + l(\mathbf{F}\mathbf{v}) \leq N+2$.

Em (KUZNETSOV, 2015), expressões explícitas para os vetores descritos no Teorema 2.1 são dadas para todos os valores de N. A seguir, descreve-se como construir esses vetores para $N = 4L+1$.

Teorema 2.2. *(KUZNETSOV, 2015)*

i. Os vetores de simetria par $\{\mathbf{u}_m\}_{-L\leq m\leq L}$ *descritos no Teorema 2.1 são dados por*

$$u_m(n) := N2^{L+m}\prod_{s=L-m+1}^{2L}\left[\cos\left(n\frac{2\pi}{N}\right)-\cos\left(s\frac{2\pi}{N}\right)\right],\ \ n\in I_N. \tag{2.6}$$

ii. Os vetores de simetria ímpar $\{\mathbf{v}_m\}_{-L\leq m\leq L-1}$ *descritos no Teorema 2.1 são dados por*

$$v_m(n) := \operatorname{sen}\left(n\frac{2\pi}{N}\right)u_m(n),\ \ n\in I_N. \tag{2.7}$$

Os vetores $\{\mathbf{u}_m\}_{-L\leq m\leq L}$ *e* $\{\mathbf{v}_m\}_{-L\leq m\leq L+1}$ *são linearmente independentes (LI).*

Também é definido em (KUZNETSOV, 2015), a sequência $\{S(k)\}_{k\geq 0}$ como se segue:

Definição 2.1. (KUZNETSOV, 2015) A sequência $\{S(k)\}_{k\geq 0}$, é definida como

$$S(0) := 1,$$
$$S(k) := \prod_{j=1}^{k} 2\operatorname{sen}\left(\frac{\pi j}{N}\right),\quad \text{para } k>1.$$

Em que a sequência satisfaz:

i. $S(k) = N$, para $k > N$.

ii. $S(k)S(N-k-1) = N$, para $0 \leq k \leq N-1$.

Examinando (2.6), verifica-se que $\mathbf{u}_m$ é uma generalização do vetor $\mathbf{f}_0$ descrito por Kong (KONG, 2008). Mais especificamente, para $m = 0$, $\mathbf{u}_0$ é um múltiplo escalar do vetor $\mathbf{f}_0$ dado em (2.4) (os índices n das componentes de $\mathbf{u}_0$ devem ser calculados módulo N). Os vetores $\mathbf{u}_m$ e $\mathbf{v}_m$ descritos no Teorema 2.2 correspondem às versões discretas dos sinais Hermite-Gaussianos dilatados de ordem zero e um, respectivamente. Em (KUZNETSOV, 2015), é mostrado que a DFT de $\mathbf{u}_m$ (resp. $\mathbf{v}_m$), dada por $\mathbf{F}\mathbf{u}_m$ (resp. $\mathbf{F}\mathbf{v}_m$), é o produto de $\mathbf{u}_{-m}$ (resp. $\mathbf{v}_{-m-1}$) por uma constante, que é precisamente determinada pelo autor. Combinando linearmente esses vetores com suas DFT, constrói-se a base dada a seguir.

Corolário 2.1. *(KUZNETSOV, 2015) Os* N *vetores*

$$\mathbf{w}_m = \mathbf{u}_m + \mathbf{F}\mathbf{u}_m,\ \ 0\leq m\leq L \tag{2.8}$$
$$\mathbf{x}_m = \mathbf{v}_m + i\mathbf{F}\mathbf{v}_m,\ \ 0\leq m\leq L-1, \tag{2.9}$$
$$\mathbf{y}_m = -\mathbf{u}_{m+1} + \mathbf{F}\mathbf{u}_{m+1},\ \ 0\leq m\leq L-1, \tag{2.10}$$
$$\mathbf{z}_m = -\mathbf{v}_m + i\mathbf{F}\mathbf{v}_m,\ \ 0\leq m\leq L-1, \tag{2.11}$$

formam uma base de autovetores da DFT para o $\mathbb{R}^N$.

A partir da base dada no Corolário 2.1, são construídos os seguintes vetores.

Definição 2.2. Os N vetores $\{\Phi_m\}_{0\leq m\leq N-1}$ são definidos como $\Phi_{4m} = \tilde{\mathbf{w}}_m$, $\Phi_{4m+1} = \tilde{\mathbf{x}}_m$, $\Phi_{4m+2} = \tilde{\mathbf{y}}_m$ e $\Phi_{4m+3} = \tilde{\mathbf{z}}_m$, em que $\{\tilde{\mathbf{w}}_m\}_{0\leq m\leq L}$, $\{\tilde{\mathbf{x}}_m\}_{0\leq m\leq L-1}$, $\{\tilde{\mathbf{y}}_m\}_{0\leq m\leq L-1}$ e $\{\tilde{\mathbf{z}}_m\}_{0\leq m\leq L-1}$ são vetores unitários obtidos aplicando o algoritmo de Gram-Schmidt a $\{\mathbf{w}_m\}_{0\leq m\leq L}$, $\{\mathbf{x}_m\}_{0\leq m\leq L-1}$, $\{\mathbf{y}_m\}_{0\leq m\leq L-1}$ e $\{\mathbf{z}_m\}_{0\leq m\leq L-1}$, respectivamente.

Finalmente, os seguintes resultados são estabelecidos.

Teorema 2.3. *(KUZNETSOV, 2015)*

i. Os vetores $\{\Phi_m\}_{0\leq m\leq N-1}$ formam a base ortonormal de autovetores da DFT para o $\mathbb{R}^N$ de modo que: para todo $0 \leq m \leq N-1$, $\mathbf{F}\Phi_m = (-i)^m\Phi_m$;

ii. Para $0 \leq m \leq 7$,

$$\max_{-2L\leq n\leq 2L} |\epsilon^{-\frac{1}{2}}\phi_m(n) - \psi_m(\epsilon n)| \to 0 \text{ com } N \to +\infty,$$

em que $\epsilon := \sqrt{2\pi/N}$ e ψ_m é a função Hermite-Gaussiana contínua de m-ésima ordem.

Outros resultados apresentados em (KUZNETSOV, 2015) sugerem a convergência no Teorema 2.3 (ii) não restrita aos primeiros oito vetores. Além do mais, para $0 \leq m \leq N-1$, o vetor Φ_m deve ter exatamente m mudanças de sinal (CANDAN; KUTAY; OZAKTAS, 2000).

Se $N = 4L+3$, os vetores pares $\{\mathbf{u}_m\}_{-L\leq m\leq L+1}$ e os vetores ímpares $\{\mathbf{v}_m\}_{-L\leq m\leq L}$ descritos no Teorema 2.1 são construídos a partir de

$$u_m(n) = N2^{L+m} \prod_{s=L-m+2}^{2L+1} \left[\cos\left(n\frac{2\pi}{N}\right) - \cos\left(s\frac{2\pi}{N}\right)\right], \quad n \in I_N, \tag{2.12}$$

e $v_m(n) := \text{sen}\left(n\frac{2\pi}{N}\right) u_m(n)$, $n \in I_N$. Estes vetores e suas DFT são linearmente combinados para formar a base de autovetores da DFT $\mathbf{w}_m = \mathbf{u}_{m+1} + \mathbf{F}\mathbf{u}_{m+1}$, $0 \leq m \leq L$, $\mathbf{x}_m = \mathbf{v}_m + i\mathbf{F}\mathbf{v}_m$, $0 \leq m \leq L$, $\mathbf{y}_m = -\mathbf{u}_{m+1} + \mathbf{F}\mathbf{u}_{m+1}$, $0 \leq m \leq L$, e $\mathbf{z}_m = -\mathbf{v}_{m+1} + i\mathbf{F}\mathbf{v}_{m+1}$, $0 \leq m \leq L-1$. A base ortonormal de autovetores HGL $\{\Phi_m\}_{0\leq m\leq N-1}$ é obtida por meio de procedimento análogo ao descrito na Definição 2.2.

Se $N = 4L$, os vetores pares $\{\mathbf{u}_m\}_{-L\leq m\leq L}$ e os vetores ímpares $\{\mathbf{v}_m\}_{-L+1\leq m\leq L-1}$ descritos no Teorema 2.1 são construídos a partir de

$$u_m(n) = N2^{L+m}\cos\left(n\frac{\pi}{N}\right)^2 \prod_{s=L-m+1}^{2L-1} \left[\cos\left(n\frac{2\pi}{N}\right) - \cos\left(s\frac{2\pi}{N}\right)\right],$$
$$-L+1 \leq m \leq L,\ n \in I_N, \tag{2.13}$$

$u_{-L}(n) := 2L$ e $v_m(n) := \tan\left(n\frac{\pi}{N}\right) u_m(n),\ n \in I_N$. Estes vetores e suas DFT são então combinados linearmente para formar a base de autovetores $\mathbf{w}_m = \mathbf{u}_m + \mathbf{F}\mathbf{u}_m,\ 0 \le m \le L-1$, $\mathbf{w}_L = \mathbf{u}_L + 2N^{\frac{1}{2}}\mathbf{u}_{-L}$, $\mathbf{x}_m = \mathbf{v}_m + i\mathbf{F}\mathbf{v}_m,\ 0 \le m \le L-1$, $\mathbf{y}_m = -\mathbf{u}_{m+1} + \mathbf{F}\mathbf{u}_{m+1},\ 0 \le m \le L-2$, $\mathbf{y}_{L-1} = -\mathbf{u}_L + 2N^{\frac{1}{2}}\mathbf{u}_{-L}$ e $\mathbf{z}_m = -\mathbf{v}_{m+1} + i\mathbf{F}\mathbf{v}_{m+1},\ 0 \le m \le L-2$. A base ortonormal de autovetores HGL $\{\Phi_m\}_{0\le m\le N,\, m\neq N-1}$ é obtida por meio de procedimento análogo ao descrito na Definição 2.2.

Se $N = 4L+2$, os vetores pares $\{\mathbf{u}_m\}_{-L\le m\le L+1}$ e os vetores ímpares $\{\mathbf{v}_m\}_{-L+1\le m\le L}$ descritos no Teorema 2.1 são construídos a partir de

$$\begin{aligned} u_m(n) =& N2^{L+m}\cos\left(n\frac{\pi}{N}\right)^2 \prod_{s=L-m+2}^{2L}\left[\cos\left(n\frac{2\pi}{N}\right) - \cos\left(s\frac{2\pi}{N}\right)\right], \\ & -L+1 \le m \le L+1,\ n \in I_N, \end{aligned} \tag{2.14}$$

$u_{-L}(n) := 2L+1$ e $v_m(n) := \tan\left(n\frac{\pi}{N}\right) u_m(n),\ n \in I_N$. Estes vetores e suas DFT são então combinados linearmente para formar a base de autovetores $\mathbf{w}_m = \mathbf{u}_{m+1} + \mathbf{F}\mathbf{u}_{m+1}, 0 \le m \le L-1$, $\mathbf{w}_L = \mathbf{u}_{L+1} + 2N^{\frac{1}{2}}\mathbf{u}_{-L}$, $\mathbf{x}_m = \mathbf{v}_{m+1} + i\mathbf{F}\mathbf{v}_{m+1},\ 0 \le m \le L-1$, $\mathbf{y}_m = -\mathbf{u}_{m+1} + \mathbf{F}\mathbf{u}_{m+1},\ 0 \le m \le L-1$, $\mathbf{y}_L = -\mathbf{u}_{L+1} + 2N^{\frac{1}{2}}\mathbf{u}_{-L}$ e $\mathbf{z}_m = -\mathbf{v}_{m+1} + i\mathbf{F}\mathbf{v}_{m+1},\ 0 \le m \le L-1$. A base ortonormal de autovetores HGL $\{\Phi_m\}_{0\le m\le N,\, m\neq N-1}$ é obtida por meio de procedimento análogo ao descrito na Definição 2.2.

2.1.2 Autovetores HGL usando Matrizes Geradoras

Em (PEI; CHANG, 2016), Pei e Chang generalizaram (2.4) definindo, para $N = 4L+1$, os vetores $\mathbf{h}_m$, $m = 0, 1, \ldots, 2L$, cujas componentes são computadas de acordo com

$$h_m(n) = \prod_{s=m+1}^{2L}\left[\cos\left(n\frac{2\pi}{N}\right) - \cos\left(s\frac{2\pi}{N}\right)\right], \tag{2.15}$$

para $n = 0, 1, \ldots, N-1$. Observa-se que $\mathbf{h}_L = \mathbf{f}_0$ e, considerando (2.6), conclui-se que, para $-L \le m \le L$ e $n \in I_N$,

$$h_{L-m}(n \pmod N) = \frac{u_m(n)}{N2^{L+m}}. \tag{2.16}$$

Em (PEI; CHANG, 2016), é mostrado que

$$\mathbf{F}\mathbf{h}_m = c_m \cdot \mathbf{h}_{2L-m},$$

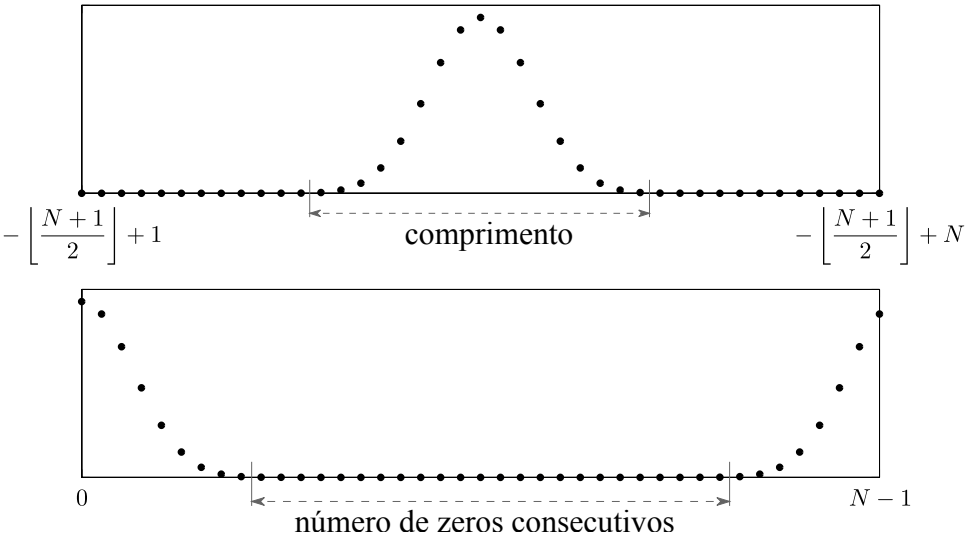
mas a constante c_m não é especificada.

Os autores denotam por $\mathcal{N}(\mathbf{x})$ o número máximo de zeros consecutivos em um vetor $\mathbf{x}$ de N pontos, que é considerado ótimo se

$$\mathcal{N}(\mathbf{x}) + \mathcal{N}(\mathbf{F}\mathbf{x}) = N-1. \tag{2.17}$$

A condição dada em (2.17) é um *complemento* daquela derivada em (2.5) e aplicada em (KUZNETSOV, 2015). Isso é ilustrado na Figura 1, em que versões normalizadas dos vetores $\mathbf{u}_0$ e $\mathbf{h}_L$ são plotadas e o critério de otimalidade é enfatizado. Os autores mostram que os vetores $\mathbf{h}_m$ são ótimos de acordo com (2.17) e, além do mais, provam que estes vetores são únicos, não-negativos e mantêm a propriedade de *forma de sino*. Estas características, que imitam de certa forma as características dos sinais Gaussianos dilatados de tempo contínuo, são então usadas como argumento para nomear os referidos vetores como funções Gaussianas discretas.

Figura 1 – Ilustração do comprimento de um vetor e número de zeros consecutivos, empregados para definir os critérios de otimalidade em (KUZNETSOV, 2015) e (PEI; CHANG, 2016), respectivamente.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

Deste ponto em diante, os autores seguem passos completamente diferentes dos propostos em (KUZNETSOV, 2015); eles não apresentam vetores análogos a $\mathbf{v}_m$, descritos no Teorema 2.1 e construídos de acordo com o Teorema 2.2. Consequentemente, não é construída uma base de autovetores da DFT para $\mathbb{R}^N$ diretamente dos vetores $\mathbf{h}_m$. Por outro lado, Pei e Chang empregam o *método de matrizes geradoras* (PEI; CHANG, 2009) para construção de autovetores HGL da DFT. Mais especificamente, uma matriz geradora é definida como:

Definição 2.3. A matriz $\mathbf{S_A}$ é definida como

$$\mathbf{S_A} = \gamma^{\frac{1}{2}}\mathbf{F}^{-1}\mathbf{A}\mathbf{F} + \mathbf{A}, \tag{2.18}$$

em que $\mathbf{A}$ é uma matriz que satisfaz $\mathbf{F}^2\mathbf{A}\mathbf{F}^2 = \lambda\mathbf{A}$.

Tais matrizes geradoras possuem a propriedade de que, se $\mathbf{x}$ é um autovetor da DFT com autovalor $\lambda_\mathbf{x}$, então $\mathbf{S_A}\mathbf{x}$ é outro autovetor da DFT com autovalor $\gamma^{\frac{1}{2}}\lambda_\mathbf{x}$. Este procedimento pode ser repetido para gerar vários outros autovetores da DFT multiplicando potências da matriz $\mathbf{S_A}$ pelo autovetor $\mathbf{x}$, que funciona como um vetor *semente*.

Com a proposta de gerar autovetores com suporte próprio compacto (comprimento menor que o comprimento dos vetores, N), em (PEI; CHANG, 2016), os autores propõem usar o método descrito acima utilizando a matriz diagonal $\mathbf{A} = \overline{\mathbf{T}}$, cujo elemento na $(n+1)$-ésima linha e na $(n+1)$-ésima coluna, $n = 0, 1, \ldots, N-1$, é

$$\overline{T}(n,n) = \text{sen}\left(n\frac{2\pi}{N}\right).$$

A matriz $\overline{\mathbf{T}}$ satisfaz $\mathbf{F}^2\overline{\mathbf{T}}\mathbf{F}^2 = -\overline{\mathbf{T}}$ e, escolhendo $\lambda^{\frac{1}{2}} = -i$ em (2.18), tem-se

$$\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F} = \begin{bmatrix} 0 & -\frac{i}{2} & & & & & \frac{i}{2} \\ \frac{i}{2} & 0 & -\frac{i}{2} & & & & \\ & \frac{i}{2} & 0 & \ddots & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & -\frac{i}{2} & \\ & & & & \frac{i}{2} & 0 & -\frac{i}{2} \\ -\frac{i}{2} & & & & & \frac{i}{2} & 0 \end{bmatrix}.$$

Portanto, se um autovetor *semente* $\mathbf{x}$ tem $2L$ zeros consecutivos, tal qual $\mathbf{h}_L$, então $\mathbf{S}_{\overline{\mathbf{T}}}\mathbf{x}$ terá pelo menos $2L-2$ zeros consecutivos, $\mathbf{S}^2_{\overline{\mathbf{T}}}\mathbf{x}$ terá pelo menos $2L-4$ zeros consecutivos, e assim por diante.

Em (PEI; CHANG, 2016), os autores argumentam que a matriz geradora

$$\mathbf{S}_{\overline{\mathbf{T}}} = -i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F} + \overline{\mathbf{T}} \tag{2.19}$$

aproxima o chamado operador de criação (FEYNMAN, 1998)

$$a^\dagger = -\frac{d}{dt} + t,$$

que relaciona dois sinais Hermite-Gaussianos consecutivos por

$$\psi_{m+1}(t) = a^\dagger \frac{\psi_m(t)}{\sqrt{2(m+1)}}.$$

Isso é justificado pelo fato de que, desde que $\text{sen}(t) \simeq t$ para t pequeno, $\overline{\mathbf{T}}$ aproxima a matriz diagonal $\mathbf{T} = \mathbf{diag}(0, 1, 2, \ldots, -2, -1)$ proposta em (PEI; CHANG, 2009). Adicionalmente, $i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F}$ aproxima o operador diferencial $\frac{d}{dt}$, desde que $\mathcal{F}\{\frac{d}{dt}\} = i\Omega$ no caso contínuo ($\mathcal{F}$ denota o operador transformada de Fourier e Ω é a variável no domínio da transformada). Isso é usado para investigar a conexão entre os autovetores HGL construídos a partir do método das matrizes geradoras utilizando $\mathbf{S}_{\overline{\mathbf{T}}}$ e os sinais Hermite-Gaussianos dilatados correspondentes. Finalmente, os autores sugerem alguns cenários de aplicação para o método proposto.

2.2 CARACTERIZAÇÃO DOS AUTOVETORES HGL DA DFT A PARTIR DE DE MATRIZES GERADORAS

Como revisado na Seção 2.1.2, o método de matrizes geradoras pode ser usado recursivamente para construir autovetores HGL de uma matriz $N \times N$ da DFT, $N = 4L + 1$. Isso é alcançado usando-se $\mathbf{g}_0 = \mathbf{h}_L$ como autovetor *semente* e calculando, para $m = 1, 2, \ldots, N-1$,

$$\mathbf{g}_m = \mathbf{S}_{\overline{\mathbf{T}}}\mathbf{g}_{m-1}. \tag{2.20}$$

Como previamente explicitado, $\mathbf{g}_0 = \mathbf{h}_L$ é uma versão escalonada de $\mathbf{u}_0$ (ver (2.16)). Considerando (2.8), para $m = 0$, mostra-se que $\mathbf{w}_0 = 2\mathbf{u}_0$ (KUZNETSOV, 2015) e, além do mais,

$$\frac{\mathbf{g}_0}{\|\mathbf{g}_0\|} = \frac{\mathbf{w}_0}{\|\mathbf{w}_0\|} = \tilde{\mathbf{w}}_0 = \frac{\mathbf{u}_0}{\|\mathbf{u}_0\|} = \Phi_0. \tag{2.21}$$

Uma relação análoga a (2.21) pode ser estabelecida para $\mathbf{g}_1$. Para $m = 0$, (2.9) fornece

$$\mathbf{x}_0 = \mathbf{v}_0 + i\mathbf{F}\mathbf{v}_0. \tag{2.22}$$

Do Teorema 2.2 (ii), é sabido que $\mathbf{v}_0 = \overline{\mathbf{T}}\mathbf{u}_0$ e, desde que $\mathbf{F}\overline{\mathbf{T}} = -\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F}^2$ e $\mathbf{F}\mathbf{u}_0 = \mathbf{u}_0$, (2.22) pode ser reescrito como

$$\begin{aligned}\mathbf{x}_0 &= \overline{\mathbf{T}}\mathbf{u}_0 + i\mathbf{F}\overline{\mathbf{T}}\mathbf{u}_0 = \overline{\mathbf{T}}\mathbf{u}_0 - i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F}(\mathbf{F}\mathbf{u}_0) \\ &= (-i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F} + \overline{\mathbf{T}})\mathbf{u}_0 = \mathbf{S}_{\overline{\mathbf{T}}}\mathbf{u}_0.\end{aligned}$$

Além de que, tem-se

$$\frac{\mathbf{g}_1}{\|\mathbf{g}_1\|} = \frac{\mathbf{x}_0}{\|\mathbf{x}_0\|} = \tilde{\mathbf{x}}_0 = \Phi_1. \tag{2.23}$$

Relações análogas à (2.21) e (2.23) não podem ser estabelecidas para $\mathbf{g}_m$ e Φ_m, $m = 2, 3, \ldots, N-1$. Isso significa que o conjunto de autovetores HGL derivado em (PEI; CHANG, 2016) não é simplesmente uma versão escalonada do derivado em (KUZNETSOV, 2015). Isso sugere a necessidade de realizar uma caracterização mais completa do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$. Resultados relacionados a tal caracterização são desenvolvidos nas seções a seguir.

2.2.1 A Autoestrutura de $\mathbf{S}_{\overline{\mathbf{T}}}$

A autoestrutura da matriz $\mathbf{S}_{\overline{\mathbf{T}}}$ está relacionada com a independência linear do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$. Mais especificamente, os seguintes resultados podem ser considerados.

Proposição 2.1. *Se o conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ é linearmente independente, o polinômio mínimo de $\mathbf{S}_{\overline{\mathbf{T}}}$ tem grau igual a $N = 4L + 1$.*

Prova. *O conjunto* $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ *é linearmente independente se e somente se*

$$\begin{aligned} c_0\mathbf{g}_0 + c_1\mathbf{g}_1 + \cdots + c_{N-1}\mathbf{g}_{N-1} &= \mathbf{0}, \\ c_0\mathbf{g}_0 + c_1\mathbf{S}_{\overline{\mathbf{T}}}\mathbf{g}_0 + \cdots + c_{N-1}\mathbf{S}_{\overline{\mathbf{T}}}^{N-1}\mathbf{g}_0 &= \mathbf{0}, \\ c_0\mathbf{I} + c_1\mathbf{S}_{\overline{\mathbf{T}}} + \cdots + c_{N-1}\mathbf{S}_{\overline{\mathbf{T}}}^{N-1} &= \mathbf{0}, \end{aligned}$$

o que requer $c_m = 0$, $m = 0, 1, \ldots, N-1$; $\mathbf{I}$ *é a matriz identidade* $N \times N$. *Tal requisito, aplicado na última igualdade, implica que o grau mínimo de um polinômio não-nulo cuja matriz* $\mathbf{S}_{\overline{\mathbf{T}}}$ *é uma raiz é* $N = 4L + 1$. ■

De acordo com a Proposição 2.1, a independência linear do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ requer a coincidência entre o polinômio mínimo e o polinômio característico de $\mathbf{S}_{\overline{\mathbf{T}}}$. Isso sugere uma investigação acerca do polinômio característico de $\mathbf{S}_{\overline{\mathbf{T}}}$, à qual os seguintes fatos são relacionados.

Proposição 2.2. *O determinante de* $\mathbf{S}_{\overline{\mathbf{T}}}$ *é* $\det(\mathbf{S}_{\overline{\mathbf{T}}}) = 0$.

Prova. *Ver Apêndice A.* ■

Proposição 2.3. *Se* $m \not\equiv 0 \pmod 4$, *o traço de* $\mathbf{S}_{\overline{\mathbf{T}}}^m$ *é* $\operatorname{tr}\left(\mathbf{S}_{\overline{\mathbf{T}}}^m\right) = 0$.

Prova. *Ver Apêndice A.* ■

Os coeficientes do polinômio característico de $\mathbf{S}_{\overline{\mathbf{T}}}$,

$$p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda) = b_N\lambda^N + b_{N-1}\lambda^{N-1} + \cdots + b_1\lambda + b_0, \tag{2.24}$$

podem ser expressos como (PENNISI, 1987)

$$\begin{aligned} b_N &= (-1)^N, \quad b_{N-1} = -(-1)^N\tau_1, \\ b_{N-2} &= -\frac{1}{2}\left[b_{N-1}\tau_1 + (-1)^N\tau_2\right], \\ b_{N-3} &= -\frac{1}{3}\left[b_{N-2}\tau_1 + b_{N-1}\tau_2 + (-1)^N\tau_3\right], \ldots, \\ b_1 &= -\frac{1}{N-1}\left[b_2\tau_1 + b_3\tau_2 + \cdots + b_{N-1}\tau_{N-2} + (-1)^N\tau_{N-1}\right], \\ b_0 &= -\frac{1}{N}\left[b_1\tau_1 + b_2\tau_2 + \cdots + b_{N-1}\tau_{N-1} + (-1)^N\tau_N\right] \\ &= (-1)^N\det(\mathbf{S}_{\overline{\mathbf{T}}}) = 0, \end{aligned}$$

em que $\tau_m = \operatorname{tr}\left(\mathbf{S}_{\overline{\mathbf{T}}}^m\right)$, $m = 1, 2, \ldots, N$. Combinando as expressões para os coeficientes de $p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda)$ e a Proposição 2.3, conclui-se que, para $m = 0, 1, \ldots, N$, se $m \not\equiv 1 \pmod 4$, $b_m = 0$. Além de que, (2.24) pode ser reescrito como

$$\begin{aligned} p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda) &= b_N\lambda^N + b_{N-4}\lambda^{N-4} + \cdots + b_1\lambda \\ &= \lambda(b_N\lambda^{N-1} + b_{N-4}\lambda^{N-5} + \cdots + b_5\lambda^4 + b_1). \end{aligned}$$

Isso permite inferir os seguintes fatos acerca dos autovalores da matriz $\mathbf{S}_{\overline{\mathbf{T}}}$:

1. Zero é um autovalor simples de $\mathbf{S}_{\overline{\mathbf{T}}}$;

2. Devido à não-simetria[2] de $\mathbf{S}_{\overline{\mathbf{T}}}$, seus outros autovalores são complexos, com parte real diferente de zero (GOLUB; LOAN, 1996);

3. Desde que todos o coeficientes não-nulos de $\lambda^{-1}p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda)$ são aqueles relacionados a λ^{4m}, $m = 0, 1, \ldots, L$, se λ_j é um autovalor de $\mathbf{S}_{\overline{\mathbf{T}}}$, $-\lambda_j$ também é um autovalor de $\mathbf{S}_{\overline{\mathbf{T}}}$. Isso significa que um autovalor λ_j necessariamente determina mais três autovalores, λ_j^*, $-\lambda_j$ e $-\lambda_j^*$; em que $*$ indica o conjugado de um número complexo.

4. Seja $\{\lambda_j, \lambda_j^*, -\lambda_j, -\lambda_j^*\}$, $j = 1, 2, \ldots, L_1$, $L_1 \leq L$, o conjunto de autovalores distintos de $\mathbf{S}_{\overline{\mathbf{T}}}$. Se $\lambda_j = c_j + d_j i$, então escreve-se

$$b_{N-1} = \sum_{j=1}^{L_1} 2\mu_j(-c_j^2 + d_j^2),$$

em que μ_j é a multiplicidade de λ_j. Então, uma das possibilidades que dá $b_{N-1} = 0$ é $c_j = \pm d_j$, $j = 1, 2, \ldots, L_1$.

Para $N = 4L + 1$, $L = 1, 2, \ldots, 128$, foram verificados computacionalmente os fatos descritos acima, incluindo a verificação de que todos os autovalores não-nulos de $\mathbf{S}_{\overline{\mathbf{T}}}$ são únicos. Isso é ilustrado na Figura 2, em que é mostrada a distribuição dos autovalores de $\mathbf{S}_{\overline{\mathbf{T}}}$ no plano complexo, para $N = 5, 9, 13$ e 17. Isso significa que, pelo menos para os valores de N testados, o polinômio mínimo de $\mathbf{S}_{\overline{\mathbf{T}}}$ possui grau N e, além disso, de acordo com a Proposição 2.1, o conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ pode ser linearmente independente.

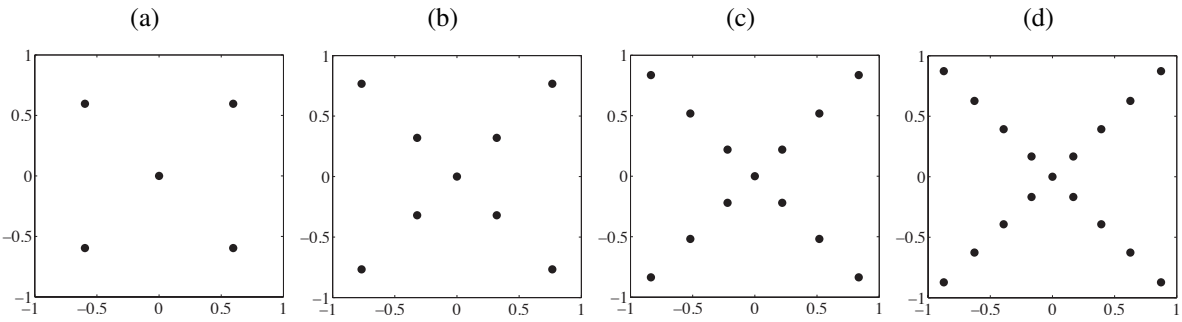
A independência linear do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$, para $N = 4L+1$, $L = 1, 2, \ldots, 128$, foi verificada computacionalmente. Isso teve que ser feito porque a condição estabelecida pela Proposição 2.1 é necessária, mas não suficiente. Neste caso, o autovetor *semente* $\mathbf{g}_0 = \mathbf{h}_L$ é um vetor cíclico de $\mathbf{S}_{\overline{\mathbf{T}}}$ (HOFFMAN; KUNZE, 1971). De outra forma, se $\mathbf{g}_0$ fosse uma autovetor de $\mathbf{S}_{\overline{\mathbf{T}}}$, por exemplo, mesmo que o polinômio mínimo tivesse grau N, o conjunto de autovetores gerados seria linearmente dependente.

2.2.2 Ortogonalizando o Conjunto de Autovetores HGL

Embora o conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ seja linearmente independente, ele não é ortogonal. Isso pode ser visto considerando $E_1 = \{\mathbf{g}_{4m}\}_{m=0,1,\ldots,L}$, $E_{-i} = \{\mathbf{g}_{4m+1}\}_{m=0,1,\ldots,L-1}$, $E_{-1} = \{\mathbf{g}_{4m+2}\}_{m=0,1,\ldots,L-1}$ e $E_i = \{\mathbf{g}_{4m+3}\}_{m=0,1,\ldots,L-1}$, os autoespaços relacionados aos autovalores 1, $-i$, -1 e i da DFT, respectivamente. Qualquer autovetor em E_1 ou E_{-1} possui simetria par, portanto, é ortogonal a qualquer autovetor em E_i ou E_{-i}, que possui simetria ímpar. Qualquer autovetor em E_1 pode ser expresso por $\mathbf{e}_1 = \mathbf{e} + \mathbf{E}$, em que $\mathbf{e}$ e $\mathbf{E}$ são um vetor com simetria par

[2] De fato, $\mathbf{S}_{\overline{\mathbf{T}}}$ é a soma entre uma matriz quase-simétrica e uma matriz diagonal.

Figura 2 – Distribuição dos autovalores de $\mathbf{S}_{\overline{\mathbf{T}}}$ no plano complexo, para (a) $N = 5$, (b) $N = 9$, (c) $N = 13$ e (d) $N = 17$.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

e sua DFT correspondente, respectivamente (MCCLELLAN; PARKS, 1972); autovetores em E_{-1} podem ser expressos por $\mathbf{e}_{-1} = \mathbf{e} - \mathbf{E}$. Então, o produto interno entre $\mathbf{e}_1$ e $\mathbf{e}_{-1}$ é

$$\begin{aligned}\langle \mathbf{e}_1, \mathbf{e}_{-1} \rangle &= \langle \mathbf{e} + \mathbf{E}, \mathbf{e} - \mathbf{E} \rangle \\ &= \langle \mathbf{e}, \mathbf{e} \rangle - \langle \mathbf{e}, \mathbf{E} \rangle + \langle \mathbf{E}, \mathbf{e} \rangle - \langle \mathbf{E}, \mathbf{E} \rangle \\ &= \langle \mathbf{e}, \mathbf{e} \rangle - \langle \mathbf{F}\,\mathbf{e}, \mathbf{F}\,\mathbf{e} \rangle = \langle \mathbf{e}, \mathbf{e} \rangle - \langle \mathbf{e}, \mathbf{e} \rangle = 0.\end{aligned}$$

Por outro lado, o produto interno entre dois autovetores sobre o mesmo autoespaço pode não ser zero. Isso sugere a aplicação de algum processo de ortogonalização em cada autoespaço. Após aplicar o algoritmo de ortogonalização de Gram-Schmidt em E_1, E_{-i}, E_{-1} e E_i, são obtidos os autoespaços $E_1^{\perp} = \{\hat{\mathbf{g}}_{4m}^{\perp}\}_{m=0,1,\ldots,L}$, $E_{-i}^{\perp} = \{\hat{\mathbf{g}}_{4m+1}^{\perp}\}_{m=0,1,\ldots,L-1}$, $E_{-1}^{\perp} = \{\hat{\mathbf{g}}_{4m+2}^{\perp}\}_{m=0,1,\ldots,L-1}$ e $E_i^{\perp} = \{\hat{\mathbf{g}}_{4m+3}^{\perp}\}_{m=0,1,\ldots,L-1}$, respectivamente, e a base ortonormal a $\{\hat{\mathbf{g}}_m^{\perp}\}_{m=0,1,\ldots,N-1}$ de autovetores HGL da DFT.

2.2.3 Caso $N = 4L + 3$

Se $N = 4L + 3$, a construção de um conjunto de autovetores HGL usando a matriz geradora $\mathbf{S}_{\overline{\mathbf{T}}}$ requer considerar um autovetor *semente* um pouco diferente do empregado para $N = 4L + 1$. Mais especificamente, deve-se usar o vetor $\mathbf{g}_0 = \mathbf{w}_0 = \mathbf{u}_1 + \mathbf{F}\mathbf{u}_1$, em que $\mathbf{u}_1$ tem suas componentes calculadas por (2.12). Também, para $N = 4L + 3$, a independência linear do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$, construído de maneira análoga à explicada no começo da Seção 2.2, requer a coincidência entre o polinômio mínimo e o polinômio característico de $\mathbf{S}_{\overline{\mathbf{T}}}$ (Proposição 2.1); neste caso, também tem-se $\det(\mathbf{S}_{\overline{\mathbf{T}}}) = 0$ (Proposição 2.2) e $\mathrm{tr}\left(\mathbf{S}_{\overline{\mathbf{T}}}^m\right) = 0$, se $m \not\equiv 0 \pmod 4$ (Proposição 2.3). Isso permite expressar o polinômio característico de $\mathbf{S}_{\overline{\mathbf{T}}}$ por

$$\begin{aligned}p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda) &= b_N\lambda^N + b_{N-1}\lambda^{N-1} + \cdots + b_1\lambda + b_0 \\ &= b_N\lambda^N + b_{N-4}\lambda^{N-4} + \cdots + b_3\lambda^3 \\ &= \lambda^3(b_N\lambda^{N-1} + b_{N-4}\lambda^{N-5} + \cdots + b_7\lambda^4 + b_3),\end{aligned}$$

e concluir que zero é um autovalor de $\mathbf{S}_{\overline{\mathbf{T}}}$ com multiplicidade 3. Os outros fatos relacionados aos autovalores de $\mathbf{S}_{\overline{\mathbf{T}}}$ são análogos aos estabelecidos para $N = 4L + 1$.

Para $N = 4L + 3$, $L = 1, 2, \ldots, 128$, foi verificado computacionalmente que os autovalores não-nulos de $\mathbf{S}_{\overline{\mathbf{T}}}$ são únicos. Isso significa que, pelo menos para os valores testados de N, o polinômio mínimo de $\mathbf{S}_{\overline{\mathbf{T}}}$ é $q_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda) = \lambda^{-s} p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda)$, sendo $s \in \{0, 1, 2\}$. De fato, verifica-se que $q_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda) = p_{\mathbf{S}_{\overline{\mathbf{T}}}}(\lambda)$, isso é, $s = 0$ e, portanto, $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ pode ser um conjunto linearmente independente. Para os valores mencionados de N, a independência linear foi comprovada por métodos computacionais. Enfim, após a ortonormalização do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N-1}$ de acordo com o processo descrito previamente, é obtido o conjunto ortonormal de N autovetores HGL da DFT $\{\hat{\mathbf{g}}_m^{\perp}\}_{m=0,1,\ldots,N-1}$.

2.2.4 Caso N par

Comparado com os casos prévios, se N é par, fatores adicionais têm que ser considerados para construção de um conjunto ortonormal de autovetores HGL usando o método de matrizes geradoras. Primeiramente, para $N = 4L$ e $N = 4L + 2$, deve-se usar como autovetores semente, respectivamente, $\mathbf{g}_0 = \mathbf{u}_0$, cujas componentes são calculadas por (2.13), e $\mathbf{g}_0 = \mathbf{w}_0 = \mathbf{u}_1 + \mathbf{F}\mathbf{u}_1$, em que $\mathbf{u}_1$ tem suas componentes calculadas por (2.14). Das Proposições 2.2 e 2.3, que também são válidas para N par, mostra-se que o polinômio característico de $\mathbf{S}_{\overline{\mathbf{T}}}$ tem zero como um autovalor com multiplicidade 4 e 2, para $N = 4L$ e $N = 4L + 2$, respectivamente. Também se verificou computacionalmente que, para $N = 2K$, $K = 2, 3, \ldots, 256$, os autovalores não-nulos de $\mathbf{S}_{\overline{\mathbf{T}}}$ são simples e o polinômio mínimo de cada uma das matrizes coincide com seu polinômio característico.

Embora a autoestrutura de $\mathbf{S}_{\overline{\mathbf{T}}}$ para N par seja, em certo sentido, análoga aquela para N ímpar, no caso par, a construção de um conjunto de autovetores HGL da DFT precisa levar em conta particularidades da autoestrutura da DFT: se $N = 4L$, as dimensões dos autoespaços relacionados aos autovalores 1, $-i$, -1 e i são, respectivamente, $L + 1$, L, L e $L - 1$; se $N = 4L + 2$, as dimensões dos autoespaços relacionados aos autovalores 1, $-i$, -1 e i são, respectivamente, $L+1$, L, $L+1$ e L (ver Tabela 1, p. 25). Devido a isso, poder-se-ia inicialmente gerar o conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N}$, que é linearmente dependente, e remover o vetor $\mathbf{g}_{N-1}$, como uma tentativa de obter um conjunto linearmente independente e consistente com as dimensões dos autoespaços mencionadas acima. Contudo, observa-se que tal remoção de vetor não causa efeito na independência linear do conjunto $\{\mathbf{g}_m\}_{m=0,1,\ldots,N}$, uma vez que o vetor $\mathbf{g}_N$, que pode ser visto como o "causador" dessa dependência, e o vetor $\mathbf{g}_{N-1}$ são relacionados a autovetores diferentes.

Neste trabalho, é proposta a seguinte solução para a restrição discutida acima: os primeiros autovetores do conjunto serão construídos de acordo com o método descrito na Seção 2.1.1

para $N = 4L$ ou $N = 4L + 2$, isso é,

$$\mathbf{g}_0 = \mathbf{w}_0, \quad \mathbf{g}_1 = \mathbf{x}_0, \quad \mathbf{g}_2 = \mathbf{y}_0, \quad \mathbf{g}_3 = \mathbf{z}_0, \quad \mathbf{g}_4 = \mathbf{w}_1.$$

Os vetores restantes são construídos de acordo com $\mathbf{g}_m = \mathbf{S}_{\mathbf{T}}^{m-4}\mathbf{g}_{m-1}$, $m = 5, 6, \ldots, N$. O conjunto $\{\mathbf{g}_m\}_{m=4,5,\ldots,N}$ pode ser linearmente independente, desde que contenha no máximo $N + 1$ vetores gerados ciclicamente. Após a exclusão do vetor $\mathbf{g}_{N-1}$ do conjunto e unindo o resultado com $\{\mathbf{g}_m\}_{m=0,1,2,3}$, que contém vetores que não foram ciclicamente gerados, obtém-se o conjunto não-ortogonal e possivelmente linearmente independente $\{\mathbf{g}_m\}_{m=0,1,\ldots,N,\, m\neq N-1}$. De fato, para $N = 2K$, $K = 2, 3, \ldots, 256$, foi computacionalmente verificado que o conjunto formado é linearmente independente. Daí, aplica-se a ortonormalização para obter o conjunto completo de N autovetores HGL da DFT $\{\hat{\mathbf{g}}_m^{\perp}\}_{m=0,1,\ldots,N,\, m\neq N-1}$.

2.3 COMPARAÇÕES NUMÉRICAS E UMA MATRIZ GERADORA DE ORDEM MAIS ALTA

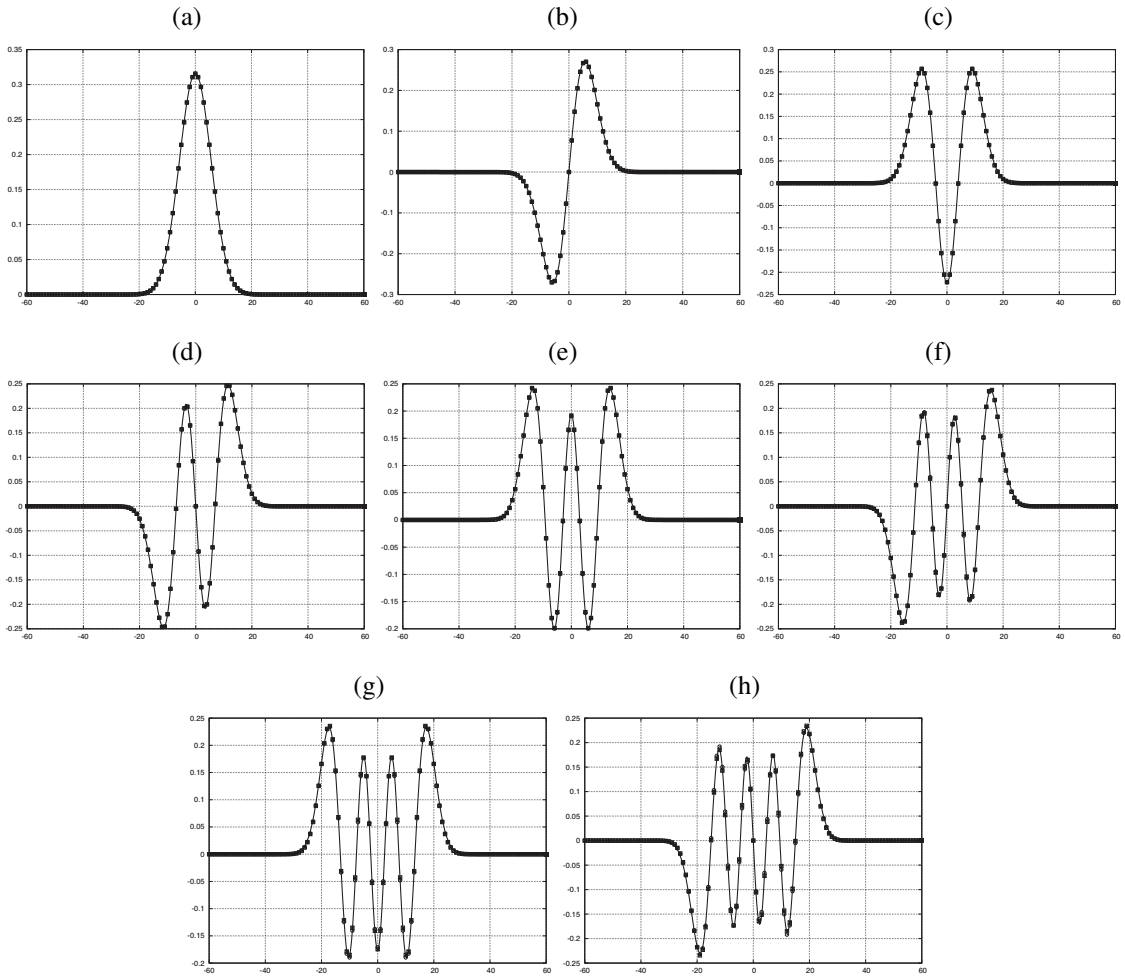
Nesta seção, são apresentados vários resultados que permitem avaliar o quanto os autovetores HGL considerados neste trabalho aproximam amostras dos sinais Hermite-Gaussianos contínuos. Mais especificamente, são considerados os conjuntos de autovetores HGL provenientes de (KUZNETSOV, 2015) e (PEI; CHANG, 2016), e também a versão ortogonalizada dos últimos, que é caracterizada na Seção 2.2. Deve-se lembrar que os m-ésimos vetores obtidos por meio desses métodos são respectivamente denotados por Φ_m, $\hat{\mathbf{g}}_m$ (foram considerados vetores normalizados) e $\hat{\mathbf{g}}_m^{\perp}$.

Na Figura 3, são plotadas as componentes dos primeiros oito autovetores dos conjuntos mencionados, para $N = 201$, junto com o sinal Hermite-Gaussiano contínuo correspondente. Observa-se que não há diferenças significativas entre os três métodos. Contudo, isso ocorre porque foram considerados autovetores de baixa ordem. Se o gráfico para $m = 7$ for examinado em detalhes (Figura 3h), observa-se que algumas componentes de $\hat{\mathbf{g}}_7$ parecem se derivar de $\psi_7(t)$ mais que as componentes correspondentes de Φ_7 e $\hat{\mathbf{g}}_7^{\perp}$[3]. Esta tendência é reforçada se for considerado $m = 16$, como mostrado na Figura 4; as componentes de $\hat{\mathbf{g}}_{16}$ claramente se desviam de $\psi_{16}(t)$ mais que as componentes correspondentes de Φ_{16} e $\hat{\mathbf{g}}_{16}^{\perp}$.

O desvio entre as componentes dos autovetores HGL e as amostras dos sinais Hermite-Gaussianos contínuos correspondentes pode ser também visualizado a partir do gráfico do erro médio quadrático, para $m = 0, 1, \ldots, N - 1$, como na Figura 5. Nesta figura, se vê que os vetores $\hat{\mathbf{g}}_m^{\perp}$ produzem o melhor resultado, pelo menos para m variando de 0 a 110; em geral, este resultado é observável para m variando de 0 para um número próximo de $N/2$. Na mesma figura, observa-se um crescimento e decrescimento na curva relacionada a $\hat{\mathbf{g}}_m^{\perp}$. Uma possível explicação para o fenômeno é o fato do suporte próprio dos vetores $\hat{\mathbf{g}}_m$ mudar de $N - 2$ para N, quando

[3] Embora na versão impressa deste trabalho possa ser difícil identificar certas nuances das figuras, na versão digital, que possibilita aumentar as figuras, estas diferenças se tornam mais perceptíveis.

Figura 3 – Amostras dos autovetores HGL Φ_m ($\square$), $\hat{\mathbf{g}}_m$ ($\bigcirc$) e $\hat{\mathbf{g}}_m^{\perp}$ ($\times$), para $N = 201$, e os sinais Hermite-Gaussianos contínuos correspondentes $\psi_m(t)$ (linhas), $m = 0, 1, \ldots, 7$, no intervalo $n = -60, -59, \ldots, 59, 60$.

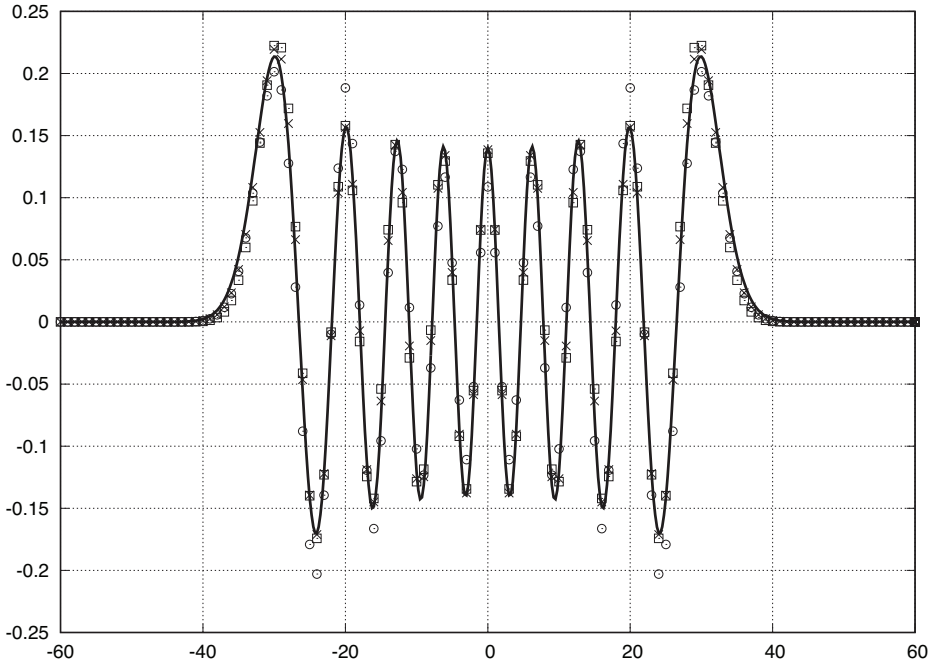


Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

$m = \lfloor N/4 \rfloor - 1$ muda para $m = \lfloor N/4 \rfloor$. Isso pode impactar no processo de ortogonalização do referido conjunto de vetores, sendo este fato verificado para todos os valores de N testados. Para autovetores de ordem mais alta ($m \geq \frac{2N}{3}$), o erro médio parece não seguir uma tendência, e nenhum dos métodos para construção de autovetores se destaca dos outros. Se for considerado $N \neq 4L + 1$, resultados similares são observados. Como exemplo, na Figura 6 são mostradas as componentes dos oito primeiros autovetores HGL para $N = 256$, junto com os sinais Hermite-Gaussianos contínuos correspondentes; já na Figura 7, também para $N = 256$, é plotado o erro médio entre as componentes dos autovetores HGL e amostras dos sinais Hermite-Gaussianos contínuos correspondentes.

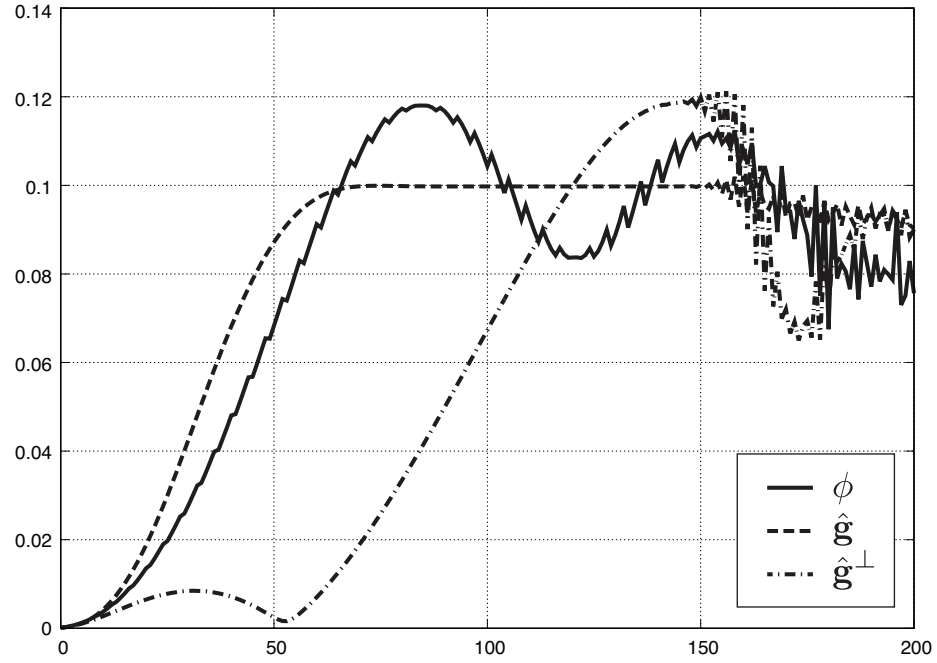
Embora uma prova formal da convergência dos autovetores HGL a amostras dos sinais Hermite-Gaussianos correspondentes não esteja disponível, com base em evidências numéricas, é razoável conjecturar que tal convergência é verdadeira. Um modo conciso de ilustrar este fato é considerando o erro médio quadrático entre as componentes de um dado autovetor HGL e

Figura 4 – Amostras dos autovetores HGL Φ_{16} ($\square$), $\hat{\mathbf{g}}_{16}$ ($\bigcirc$) e $\hat{\mathbf{g}}_{16}^{\perp}$ ($\times$), para $N = 201$, e o sinal Hermite-Gaussiano contínuo correspondente $\psi_{16}(t)$ (linha), no intervalo $n = -60, -59, \ldots, 59, 60$.



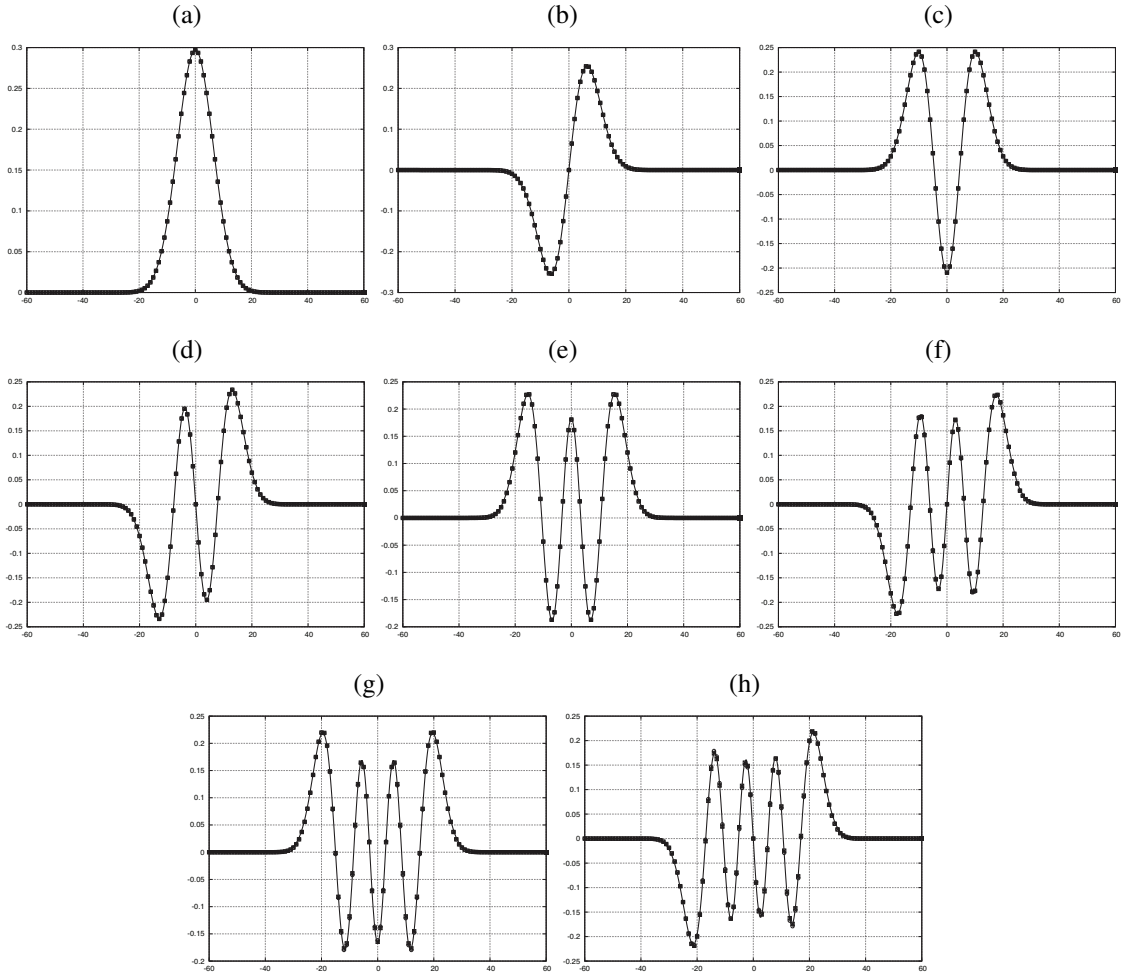
Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

Figura 5 – Raiz do erro médio quadrático entre os autovetores HGL Φ_m, $\hat{\mathbf{g}}_m$, $\hat{\mathbf{g}}_m^{\perp}$, para $N = 201$ e amostras dos sinais Hermite-Gaussianos contínuos correspondentes $\psi_m(t)$, em que $m = 0, 1, \ldots, 200$.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

Figura 6 – Amostras dos autovetores HGL Φ_m ($\square$), $\hat{\mathbf{g}}_m$ ($\bigcirc$) e $\hat{\mathbf{g}}_m^{\perp}$ ($\times$), para $N = 256$, e amostras dos sinais Hermite-Gaussianos contínuos correspondentes $\psi_m(t)$ (linhas), $m = 0, 1, \ldots, 7$, no intervalo $n = -60, -59, \ldots, 59, 60$.



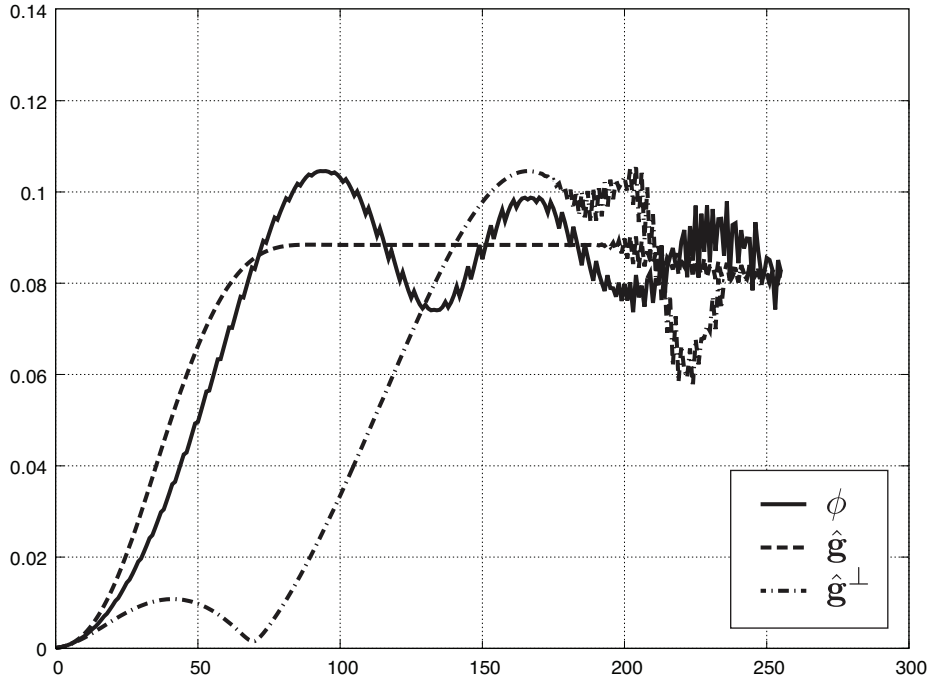
Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

amostras do sinal Hermite-Gaussiano contínuo correspondente para vários valores de N. Na Figura 8, isso é feito para o autovetor de ordem $m = 24$, para $N = 20R + 5$, $R = 1, 2, \ldots, 20$. Na figura, observa-se com clareza que o erro se aproxima de zero à medida que N cresce; aparentemente, esta característica independe da ordem do autovetor HGL considerado. Por outro lado, a taxa de convergência muda de acordo com o método de construção do autovetor HGL que está sendo avaliado. Mais precisamente, a convergência dos autovetores HGL ortogonalizados $\hat{\mathbf{g}}_m^{\perp}$ parece ser mais rápida que a dos outros dois métodos.

2.3.1 Uma Matriz Geradora de Ordem mais Alta

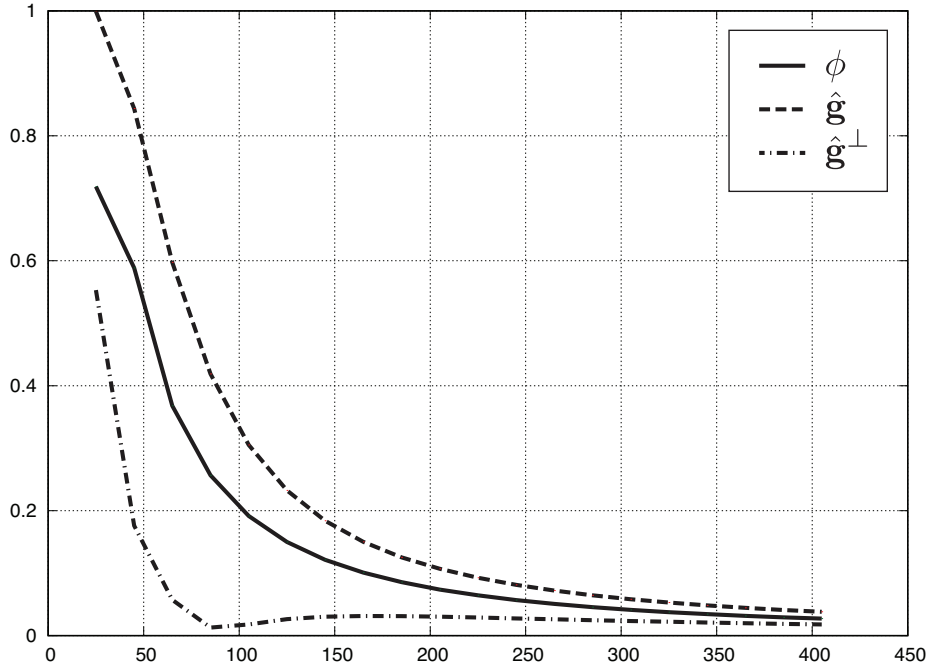
Como explicado na Seção 2.1.2, diferentes matrizes geradoras podem ser empregadas para produzir recursivamente autovetores da DFT; se for desejado que as componentes desses autovetores aproximem amostras das funções Hermite-Gaussianas contínuas, o vetor *semente*

Figura 7 – Raiz do erro médio quadrático entre os autovetores HGL Φ_m, $\hat{\mathbf{g}}_m$, $\hat{\mathbf{g}}_m^{\perp}$ e amostras dos sinais Hermite-Gaussianos contínuos correspondentes $\psi_m(t)$, para $N = 256$, $m = 0, 1, \ldots, 256$, $m \neq 255$.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

Figura 8 – Raiz do erro médio quadrático entre os autovetores HGL Φ_{24}, $\hat{\mathbf{g}}_{24}$, $\hat{\mathbf{g}}_{24}^{\perp}$ e amostras do sinal Hermite-Gaussiano contínuo correspondente $\psi_{24}(t)$, para $N = 20R + 5$, $R = 1, 2, \ldots, 20$.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

deve ser $\mathbf{g}_0$ e a matriz geradora deve aproximar o operador de criação. Neste sentido, usa-se, por exemplo, a matriz diagonal $\mathbf{A} = \overline{\overline{\mathbf{T}}}$, cujo elemento na $(n+1)$-ésima linha e na $(n+1)$-ésima coluna, $n = 0, 1, \ldots, N-1$, é

$$\overline{\overline{T}}(n,n) = \frac{1}{6}\left[8\,\text{sen}\left(n\frac{2\pi}{N}\right) - \text{sen}\left(n\frac{4\pi}{N}\right)\right].$$

Utilizando $\overline{\overline{\mathbf{T}}}$, que satisfaz $\mathbf{F}^2\overline{\overline{\mathbf{T}}}\mathbf{F}^2 = -\overline{\overline{\mathbf{T}}}$ e, em (2.18), utilizando $\gamma^{\frac{1}{2}} = -i$, é obtida a matriz geradora

$$\mathbf{S}_{\overline{\overline{\mathbf{T}}}} = -i\mathbf{F}^{-1}\overline{\overline{\mathbf{T}}}\mathbf{F} + \overline{\overline{\mathbf{T}}},$$

em que

$$i\mathbf{F}^{-1}\overline{\overline{\mathbf{T}}}\mathbf{F} = \begin{bmatrix} 0 & \frac{8}{12} & -\frac{1}{12} & & & \frac{1}{12} & -\frac{8}{12} \\ -\frac{8}{12} & 0 & \frac{8}{12} & -\frac{1}{12} & & & \frac{1}{12} \\ \frac{1}{12} & -\frac{8}{12} & 0 & \ddots & \ddots & & \\ & \frac{1}{12} & \ddots & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & \ddots & \frac{8}{12} & -\frac{1}{12} \\ -\frac{1}{12} & & & \ddots & -\frac{8}{12} & 0 & \frac{8}{12} \\ \frac{8}{12} & -\frac{1}{12} & & & \frac{1}{12} & -\frac{8}{12} & 0 \end{bmatrix}.$$

A matriz $i\mathbf{F}^{-1}\overline{\overline{\mathbf{T}}}\mathbf{F}$ corresponde à versão matricial da aproximação de quarta ordem da primeira derivada (LYNCH, 2005):

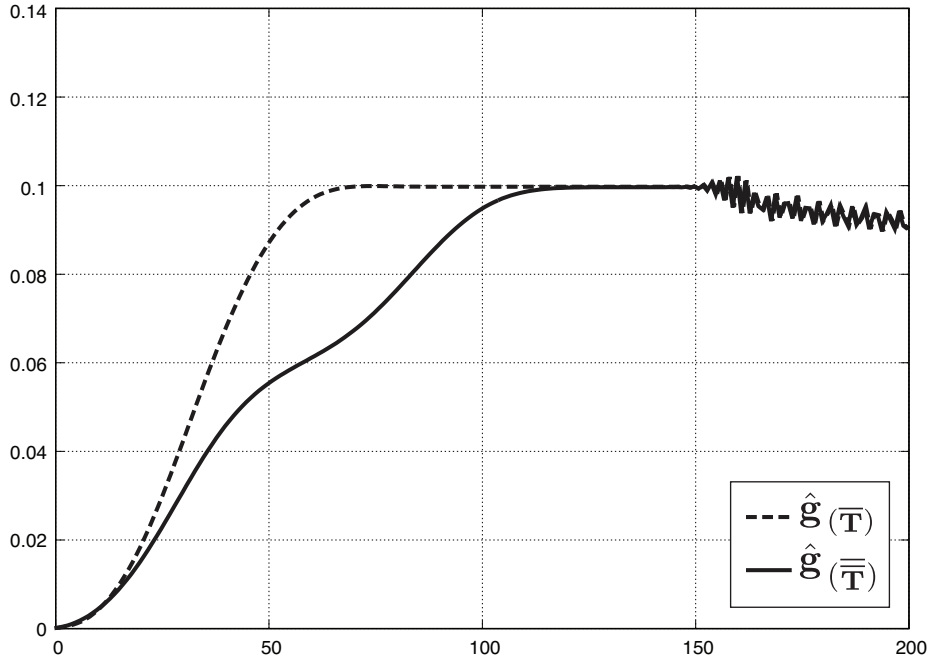
$$\left.\frac{df(x)}{dx}\right|_{\text{contínuo}} \approx \left.\frac{18f(x-2) - 8f(x-1) + f(x) - 8f(x+1) + 18f(x+2)}{12}\right|_{\text{discreto}}.$$

A autoestrutura de $\mathbf{S}_{\overline{\overline{\mathbf{T}}}}$ é similar à de $\mathbf{S}_{\overline{\mathbf{T}}}$, que foi analisada na Seção 2.2.1. Desde que o autovetor *semente* $\mathbf{g}_0$ possui $2K$ zeros consecutivos, $\mathbf{g}_1 = \mathbf{S}_{\overline{\overline{\mathbf{T}}}}\mathbf{g}_0$ terá $2K-4$ zeros consecutivos, $\mathbf{g}_2 = \mathbf{S}^2_{\overline{\overline{\mathbf{T}}}}\mathbf{g}_0$ terá $2K-8$ zeros consecutivos, e assim por diante. Tal número de zeros consecutivos é comunicado para a versão ortonormalizada de cada autovetor. Na Figura 9, como esperado, observa-se que o conjunto de autovetores HGL de 201 pontos $\hat{\mathbf{g}}_m$ construídos usando $\overline{\overline{\mathbf{T}}}$, aproxima as amostras dos sinais Hermite-Gaussianos contínuos correspondentes melhor que os construídos usando $\overline{\mathbf{T}}$. Isso também é válido para os demais valores de N. Naturalmente, tal aproximação pode ser melhor se forem consideradas aproximações de ordem mais alta para a primeira derivada na definição da matriz geradora.

2.4 UMA FAMÍLIA DE MATRIZES GERADORAS DE AUTOVETORES HGL DA DFT

Nesta seção, é introduzida uma família de matrizes geradoras de autovetores da DFT. Além disso, é mostrado que, se um conjunto específico de autovetores é utilizado como autovetores semente, uma base de autovetores HGL da DFT é obtida. Mais especificamente, mostra-se

Figura 9 – Erro RMS entre os autovetores $\hat{\mathbf{g}}_m$, construídos utilizando as matrizes geradoras $\overline{\mathbf{T}}$ e $\overline{\overline{\mathbf{T}}}$, e amostras dos sinais Hermite-Gaussianos contínuos correspondentes $\psi_m(t)$, para $N = 201$, $m = 0, 1, \ldots, 200$.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

que essa base de autovetores HGL da DFT é a proposta em (KUZNETSOV, 2015), no entanto, construída de uma forma recursiva mais simples.

Seja $\{\mathbf{C}_m\}_{0\leq m\leq N-1}$ um conjunto de matrizes diagonais definidas por

$$\mathbf{C}_m = \operatorname{diag}\left(2\cos\left(\frac{2\pi n}{N}m\right)\right), \quad n \in I_N, \quad 0 \leq m \leq N-1,$$

as quais satisfazem $\mathbf{F}^2\mathbf{C}_m\mathbf{F}^2 = \mathbf{C}_m$. Então, se $\mathbf{v}$ é um autovetor de $\mathbf{F}$ com autovalor λ, $\mathbf{v}_{\mathbf{C}_m} = \mathbf{S}_{\mathbf{C}_m}\mathbf{v}$ também é um autovetor de $\mathbf{F}$ com o mesmo autovalor λ.

Na sequência desse texto, $\mathbf{w}_0$, $\mathbf{x}_0$, $\mathbf{y}_0$ e $\mathbf{z}_0$ denotam os primeiros autovetores dos autoespaços relacionados aos autovalores 1, $-i$, -1 e i de $\mathbf{F}$, respectivamente, obtidos de (KUZNETSOV, 2015); $\#\{\lambda\}$ indica a multiplicidade do autovalor λ. A partir deste ponto, serão descritos os resultados para $N \equiv 1 \pmod 4$. Resultados semelhantes para os outros valores de N são encontrados de forma semelhante.

Definição 2.4. Seja $\mathbf{c}_0 = \mathbf{w}_0$, $\mathbf{c}_1 = \mathbf{x}_0$, $\mathbf{c}_2 = \mathbf{y}_0$ e $\mathbf{c}_3 = \mathbf{z}_0$. O conjunto de autovetores da DFT

$\{\mathbf{c}_m\}_{0\leq m\leq N-1}$ é obtido a partir de

$$\begin{aligned}
\mathbf{c}_{4m} &= \mathbf{S}_{\mathbf{C}_m}\mathbf{c}_0, \quad m = 1, 2, \ldots, \#\{1\} - 1,\\
\mathbf{c}_{4m+1} &= \mathbf{S}_{\mathbf{C}_m}\mathbf{c}_1, \quad m = 1, 2, \ldots, \#\{-i\} - 1,\\
\mathbf{c}_{4m+2} &= \mathbf{S}_{\mathbf{C}_m}\mathbf{c}_2, \quad m = 1, 2, \ldots, \#\{-1\} - 1,\\
\mathbf{c}_{4m+3} &= \mathbf{S}_{\mathbf{C}_m}\mathbf{c}_3, \quad m = 1, 2, \ldots, \#\{i\} - 1.
\end{aligned}$$

Na Definição 2.4, cada subconjunto $\{\mathbf{c}_{4m+l}\}_{0\leq m\leq \#\{(-i)^l\}-1}$ é composto por autovetores relacionados aos autovalores $(-i)^l$, $0 \leq l \leq 3$. O teorema mostrado a seguir é a principal contribuição desta seção.

Teorema 2.4. *O conjunto $\{\mathbf{c}_m^{\perp}\}_{0\leq m\leq N-1}$, obtido após a ortonormalização de cada um dos subconjuntos de autovetores construídos usando a Definição 2.4, é a base de autovetores HGL da DFT $\{\Phi_m\}_{0\leq m\leq N-1}$ descrita em (KUZNETSOV, 2015).*

O Teorema 2.4 pode ser provado demostrando que os autovetores de cada subconjunto construído a partir da Definição 2.4 são combinações lineares dos vetores que compõem os autoespaços da base descrita em (KUZNETSOV, 2015) (antes do processo de ortogonalização). Para demostrar isso, primeiramente os vetores $\{\mathbf{c}_m\}_{0\leq m\leq N-1}$ são renomeados como

$$\begin{aligned}
\{\mathbf{w}'_m\}_{0\leq m\leq(\#\{1\}-1)} &= \{\mathbf{c}_{4m}\}_{0\leq m\leq(\#\{1\}-1)},\\
\{\mathbf{x}'_m\}_{0\leq m\leq(\#\{-i\}-1)} &= \{\mathbf{c}_{4m+1}\}_{0\leq m\leq(\#\{-i\}-1)},\\
\{\mathbf{y}'_m\}_{0\leq m\leq(\#\{-1\}-1)} &= \{\mathbf{c}_{4m+2}\}_{0\leq m\leq(\#\{-1\}-1)},\\
\{\mathbf{z}'_m\}_{0\leq m\leq(\#\{i\}-1)} &= \{\mathbf{c}_{4m+3}\}_{0\leq m\leq(\#\{i\}-1)}.
\end{aligned}$$

Além do mais, os lemas descritos a seguir são importantes para a continuidade da prova do Teorema 2.4.

Lema 2.1. *Os vetores do conjunto $\{\mathbf{c}_m\}_{0\leq m\leq N-1}$ podem ser expressos como*

$$\begin{aligned}
\mathbf{w}'_m &= \mathbf{C}_m\mathbf{w}_0 + \mathbf{F}\mathbf{C}_m\mathbf{w}_0,\\
\mathbf{x}'_m &= \mathbf{C}_m\mathbf{x}_0 + i\mathbf{F}\mathbf{C}_m\mathbf{x}_0,\\
\mathbf{y}'_m &= \mathbf{C}_m\mathbf{y}_0 - \mathbf{F}\mathbf{C}_m\mathbf{y}_0,\\
\mathbf{z}'_m &= \mathbf{C}_m\mathbf{z}_0 - i\mathbf{F}\mathbf{C}_m\mathbf{z}_0.
\end{aligned}$$

Prova. *Desde que* $\mathbf{w}'_m$ *é um autovetor da DFT associado com o autovalor* 1*, tem-se*

$$\begin{aligned}
\mathbf{w}'_m &= \mathbf{S}_{\mathbf{C}_m}\mathbf{w}_0 \text{ , em que } \quad \mathbf{S}_{\mathbf{C}_m} = \mathbf{F}^{-1}\mathbf{C}_m\mathbf{F} + \mathbf{C}_m, \\
\mathbf{w}'_m &= \mathbf{F}^{-1}\mathbf{C}_m\mathbf{F}\mathbf{w}_0 + \mathbf{C}_m\mathbf{w}_0, \\
\mathbf{F}\mathbf{w}'_m &= \mathbf{F}(\mathbf{F}^{-1}\mathbf{C}_m\mathbf{F}\mathbf{w}_0 + \mathbf{C}_m\mathbf{w}_0) = \mathbf{C}_m\mathbf{F}\mathbf{w}_0 + \mathbf{F}\mathbf{C}_m\mathbf{w}_0, \\
\mathbf{w}'_m &= \mathbf{C}_m\mathbf{w}_0 + \mathbf{F}\mathbf{C}_m\mathbf{w}_0.
\end{aligned}$$

A prova para $\mathbf{x}'_m$*,* $\mathbf{y}'_m$ *e* $\mathbf{z}'_m$ *segue os mesmos passos.* ■

Lema 2.2. *Os vetores* $\mathbf{C}_m\mathbf{u}_n$ *e* $\mathbf{C}_m\mathbf{v}_n$*,* $n < m$*, podem ser expressos respectivamente como*

$$\mathbf{C}_m\mathbf{u}_n = \mathbf{u}_{m+n} + \alpha_{m+n-1}\mathbf{u}_{m+n-1} + \cdots + \alpha_n\mathbf{u}_n \tag{2.25}$$

e

$$\mathbf{C}_m\mathbf{v}_n = \mathbf{v}_{m+n} + \alpha_{m+n-1}\mathbf{v}_{m+n-1} + \cdots + \alpha_n\mathbf{v}_n, \tag{2.26}$$

em que os $\{\alpha_k\}_{n\leq k\leq m+n-1}$ *são constantes.*

Prova. *Assume-se que* $m = n + 1$ *e considera-se o fato de que*

$$u_m(k) = \left(2\cos\left(\frac{2\pi k}{N}\right) - 2\cos\left(\frac{2\pi(3L+m)}{N}\right)\right)u_{m-1}(k),$$

conforme demonstrado em (KUZNETSOV, 2015). A última equação pode ser reescrita como

$$u_m(k) = (C_1(k) - e_m)u_{m-1}(k), \tag{2.27}$$

em que $C_m(k) = 2\cos\left(\frac{2\pi k}{N}m\right)$ *e* $e_m = 2\cos\left(\frac{2\pi(3L+m)}{N}\right)$*. Além do mais,*

$$C_1(k)u_{m-1}(k) = u_m(k) + e_m u_{m-1}(k) \tag{2.28}$$

e, desde que $v_m(k) = \sin\left(\frac{2\pi k}{N}\right)u_m(k)$*, tem-se que*

$$C_1(k)v_{m-1}(k) = v_m(k) + e_m v_{m-1}(k). \tag{2.29}$$

Similarmente, para $m = n + 2$*, obtém-se que*

$$\begin{aligned}
u_m(k) &= (C_1(k) - e_m)(C_1(k) - e_{m-1})u_{m-2}(k) \\
&= (C_2(k) - C_1(k)(e_m + e_{m-1}) + e_m e_{m-1} + 2)u_{m-2}(k).
\end{aligned}$$

Se usada a identidade trigonométrica

$$\cos(a)\cos(b) = \frac{1}{2}(\cos(a+b) + \cos(a-b)), \tag{2.30}$$

escreve-se a seguinte igualdade:

$$u_m(k) = (C_2(k) - C_1(k)(e_m + e_{m-1}) + e_m e_{m-1} + 2)u_{m-2}(k).$$

Usando (2.28) na última igualdade, tem-se

$$u_m(k) = C_2(k)u_{m-2}(k) - (e_m + e_{m-1})(u_{m-1}(k) + e_m u_{m-2}(k)) + (e_m e_{m-1} + 2)u_{m-2}(k),$$
$$C_2(k)u_{m-2}(k) = u_m(k) + (e_m + e_{m-1})u_{m-1}(k) + (e_m e_{m-1} - 2)u_{m-2}(k).$$

Aplicando recursivamente o produto de dois cossenos (2.30) e (2.28) (resp. (2.29)), $\mathbf{C}_m\mathbf{u}_n$ *(resp.* $\mathbf{C}_m\mathbf{v}_n$*),* $n < m$*, podem ser escritos em termos dos vetores do conjunto* $\{\mathbf{u}_k\}_{n\leq k\leq m+n}$ *(resp.* $\{\mathbf{v}_k\}_{n\leq k\leq m+n}$*), como mostrado em (2.25) (resp. (2.26)).* ■

Proposição 2.4. *Seja* $d_n = N^{-\frac{1}{2}}S(2L + 2n)$*. Para* $0 \leq n \leq 2L$*, (i)* $d_n d_{-n} = 1$ *e (ii)* $d_0 = 1$*.*

Prova. *(i) Para* $0 \leq n \leq 2L$*, tem-se*

$$\begin{aligned} d_n d_{-n} &= N^{-\frac{1}{2}}S(2L + 2n)N^{-\frac{1}{2}}S(2L - 2n) \\ &= N^{-1}S(2L + 2n)S(2L - 2n). \end{aligned}$$

Utilizando a substituição $k = 2L+2n$ *e o fato que* $S(k)S(N-k-1) = N$ *(KUZNETSOV, 2015), obtém-se*

$$d_n d_{-n} = N^{-1}S(k)S(N - k - 1) = N^{-1}N = 1.$$

(ii) Para $0 \leq n \leq 2L$*, usando* $S(k)S(N - k - 1) = N$ *com* $k = 2L$*, conclui-se* $S(2L) = N^{\frac{1}{2}}$*. Além do mais,* $d_0 = N^{-\frac{1}{2}}S(2L) = N^{-\frac{1}{2}}N^{\frac{1}{2}} = 1$*.*

■

Proposição 2.5. *Seja* $\delta_n = N^{-\frac{1}{2}}S(2L + 2n + 1)$*. Para* $0 \leq n \leq 2L$*,* $\delta_n\delta_{-n-1} = 1$*.*

Prova. *Pode-se escrever*

$$\begin{aligned} \delta_n\delta_{-n-1} &= N^{-\frac{1}{2}}S(2L + 2n + 1)N^{-\frac{1}{2}}S(2L - 2n - 2 + 1) \\ &= N^{-1}S(2L + 2n + 1)S(2L - 2n - 1). \end{aligned}$$

Usando a substituição $k = 2L + 2n + 1$*, tem-se*

$$\delta_n\delta_{-n-1} = N^{-1}S(k)S(N - k - 1) = N^{-1}N = 1.$$

■

Expressões para $\mathbf{w}_0$, $\mathbf{x}_0$, $\mathbf{y}_0$ e $\mathbf{z}_0$ podem ser reescritas usando d_n (Proposição 2.4) e δ_n (Proposição 4.4) como

$$\mathbf{w}_0 = \mathbf{u}_0 + d_0\mathbf{u}_0 = 2\mathbf{u}_0, \qquad \mathbf{x}_0 = \mathbf{v}_0 + \delta_0\mathbf{v}_{-1},$$
$$\mathbf{y}_0 = -\mathbf{u}_1 + d_1\mathbf{u}_{-1}, \qquad \mathbf{z}_0 = -\mathbf{v}_0 + \delta_0\mathbf{v}_{-1}.$$

Usando o Lema 2.1, $\mathbf{y}'_m$ pode ser reescrito como

$$\begin{aligned}\mathbf{y}'_m &= \mathbf{C}_m\mathbf{y}_0 - \mathbf{F}\mathbf{C}_m\mathbf{y}_0 \\ &= \mathbf{C}_m(-\mathbf{u}_1 + d_1\mathbf{u}_{-1}) - \mathbf{F}\mathbf{C}_m(-\mathbf{u}_1 + d_1\mathbf{u}_{-1}).\end{aligned}$$

Usando (2.25) na última igualdade, obtém-se

$$\begin{aligned}\mathbf{y}'_m =& -(\mathbf{u}_{m+1} + \alpha_m\mathbf{u}_m + \cdots + \alpha_1\mathbf{u}_1)+ \\ &+ d_1(\mathbf{u}_{m-1} + \beta_{m-2}\mathbf{u}_{m-2} + \cdots + \beta_{-1}\mathbf{u}_{-1})+ \\ &- \mathbf{F}\,(-(\mathbf{u}_{m+1} + \alpha_m\mathbf{u}_m + \cdots + \alpha_1\mathbf{u}_1) + \\ &+ d_1(\mathbf{u}_{m-1} + \beta_{m-2}\mathbf{u}_{m-2} + \cdots + \beta_{-1}\mathbf{u}_{-1})), \\ \mathbf{y}'_m =& -\mathbf{u}_{m+1} - \alpha_m\mathbf{u}_m + (d_1 - \alpha_{m-1})\mathbf{u}_{m-1} + \cdots + \\ &+ (d_1\beta_k - \alpha_k)\mathbf{u}_k + \cdots + d_1\beta_0\mathbf{u}_0 + d_1\beta_{-1}\mathbf{u}_{-1}+ \\ &- \mathbf{F}(-\mathbf{u}_{m+1} - \alpha_m\mathbf{u}_m + (d_1 - \alpha_{m-1})\mathbf{u}_{m-1} + \cdots + \\ &+ (d_1\beta_k - \alpha_k)\mathbf{u}_k + \cdots + d_1\beta_0\mathbf{u}_0 + d_1\beta_{-1}\mathbf{u}_{-1}).\end{aligned}$$

Implementando a multiplicação por $\mathbf{F}$ na segunda parte da equação acima, obtém-se

$$\begin{aligned}\mathbf{y}'_m =& -\mathbf{u}_{m+1} - \alpha_m\mathbf{u}_m + (d_1 - \alpha_m)\mathbf{u}_{m-1} + \cdots + \\ &+ (d_1\beta_k - \alpha_k)\mathbf{u}_k + \cdots + d_1\beta_0\mathbf{u}_0 + d_1\beta_{-1}\mathbf{u}_{-1}+ \\ &+ d_{m+1}\mathbf{u}_{-m-1} - \alpha_m d_m\mathbf{u}_{-m} + \cdots + \\ &- (d_1\beta_k - \alpha_k)d_k\mathbf{u}_{-k} + \cdots + d_1\beta_0 d_0\mathbf{u}_0 + d_1\beta_{-1}d_{-1}\mathbf{u}_1.\end{aligned}$$

Utilizando a Proposição 2.4(i) e 2.4(ii), os termos relacionados $\mathbf{u}_k$ e $\mathbf{u}_{-k}$, $0 \leq k \leq m$, podem ser agrupados em

$$\begin{aligned}\mathbf{y}'_m =& (-\mathbf{u}_{m+1} + d_m\mathbf{u}_{-m-1}) - \alpha_m(-\mathbf{u}_m + d_m\mathbf{u}_{-m})+ \\ &\cdots + (d_1\beta_k - \alpha_k)(-\mathbf{u}_k + d_k\mathbf{u}_{-k})+ \\ &\cdots + (d_1\beta_1 - \alpha_1)(\mathbf{u}_1 - d_1\mathbf{u}_{-1}) + (d1\beta_0 - d1\beta_0)\mathbf{u}_0+ \\ &+ (d_1\beta_{-1}\mathbf{u}_{-1} - \beta_{-1}\mathbf{u}_1), \\ \mathbf{y}'_m =& (-\mathbf{u}_{m+1} + d_m\mathbf{u}_{-m-1}) - \alpha_m(-\mathbf{u}_m + d_m\mathbf{u}_{-m})+ \\ &\cdots + (d_1\beta_k - \alpha_k)(-\mathbf{u}_k + d_k\mathbf{u}_{-k})+ \\ &\cdots + (\alpha_1 - \beta_{-1} - d_1\beta_1)(-\mathbf{u}_1 + d_1\mathbf{u}_{-1}), \\ \mathbf{y}'_m =& \mathbf{y}_m - \alpha_m\mathbf{y}_{m-1} + \cdots + (d_1\beta_{k+1} - \alpha_{k+1})\mathbf{y}_k+ \\ &\cdots + (\alpha_1 - \beta_{-1} - d_1\beta_1)\mathbf{y}_0.\end{aligned}$$

Na última equação, o vetor $\mathbf{y}'_m$ é expresso como a combinação linear dos vetores $\{\mathbf{y}_k\}_{0\leq k\leq m}$. Usando os resultados intermediários, e utilizando passos análogos aos apresentados, obtém-se resultados equivalentes para os vetores $\mathbf{w}'_m$, $\mathbf{x}'_m$ e $\mathbf{z}'_m$. Assim conclui-se a prova do Teorema 2.4.

■

2.5 TRANSFORMADA FRACIONÁRIA DISCRETA DE FOURIER BASEADA EM AUTOVETORES HGL DA DFT OBTIDOS POR FÓRMULAS FECHADAS

Como descrito anteriormente, uma transformada fracionária discreta de Fourier pode ser definida por meio da expansão espectral da matriz da DFT de dimensão N, $\mathbf{F}$. Usando esta metodologia, escreve-se a matriz da DFrFT com ordem fracionária $a \in \mathbb{R}$ como em (2.2). Nesta seção, é investigado o uso dos conjuntos ortogonais de autovetores HGL, oriundos dos métodos previamente estudados neste trabalho, como colunas da matriz $\mathbf{E}$ em (2.2). De acordo com as evidências apresentadas na Seção 2.3, tais autovetores aproximam amostras de sinais Hermite-Gaussianos e, portanto, é esperado que as DFrFT correspondentes aproximem numericamente a FrFT. Adicionalmente, os referidos autovetores HGL são construídos a partir de expressões fechadas e a DFrFT correspondente se conforma às principais propriedades da FrFT (aditividade de índices e redução à transformada ordinária quando a ordem fracionária é igual a 1).

Os autovetores HGL empregados em (2.2) são os construídos usando a abordagem de combinações lineares, $\{\Phi_m\}_{0\leq m\leq N-1}$, e aquela obtida a partir da ortonormalização do conjunto construído usando o método de matrizes geradoras, $\{\hat{\mathbf{g}}_m^{\perp}\}_{0\leq m\leq N-1}$. Com o intuito de ilustrar os resultados produzidos por estas DFrFT, estas transformadas foram aplicadas a um pulso retangular discreto padrão, como mostrado na Figura 10. Para comparar os resultados obtidos usando estas abordagens da DFrFT, também foram calculadas a transformada do pulso retangular por meio dos métodos propostos em (OZAKTAS et al., 1996) e (CANDAN; KUTAY; OZAKTAS, 2000).

Na Figura 10, foi usado $N = 315$ e foi esboçada a magnitude da DFrFT do pulso retangular discreto para $a \in \{0{,}25, 0{,}50, 0{,}75, 1{,}00\}$. Inspecionando as Figuras 10a – 10c, observa-se que os gráficos produzidos usando os autovetores $\{\hat{\mathbf{g}}_m^{\perp}\}_{0\leq m\leq N-1}$ (método de matrizes geradoras) e aqueles obtidos usando (OZAKTAS et al., 1996) e (CANDAN; KUTAY; OZAKTAS, 2000) são bem próximos; por outro lado, o gráfico produzido usando-se os autovetores $\{\Phi_m\}_{0\leq m\leq N-1}$ (método de combinações lineares) exibe pequenos desvios dos mencionados anteriormente, bem como pequenas flutuações em intervalos em que as outras abordagens são predominantemente planas. Estas diferenças, que refletem em algum sentido no erro médio quadrático que foi discutido na Seção 2.3, podem ser consequência do fato de os autovetores Φ_m possuírem suporte próprio mais compacto que os autovetores $\hat{\mathbf{g}}_m^{\perp}$ e os dados em (CANDAN; KUTAY; OZAKTAS, 2000); noutras palavras, um grande número de componentes consecutivas $\Phi_m(n)$ de Φ_m, $m = 0, 1, \ldots, N-1$, para n em torno de $\left\lfloor \frac{N}{2} \right\rfloor \pmod N$, é zero, enquanto que as amostras dos sinais Hermite-Gaussianos correspondentes $\psi_m(t)$, $m = 0, 1, \ldots, N-1$, são não nulas. Isso é ilustrado na Figura 11, em que as componentes nulas dos autovetores Φ_m de 21 pontos e $\hat{\mathbf{g}}_m^{\perp}$, $m = 0, 1, \ldots, 20$, bem como suas simetrias são enfatizadas. Se $a = 1{,}00$, todas as abordagens produzem o mesmo resultado (ver Figura 10d), isso é, a DFT de um pulso retangular. De qualquer forma, após o cálculo do erro entre cada DFrFT considerada na Figura 10 e a amostra da FrFT

Tabela 2 – Raiz do erro médio quadrático entre amostras da FrFT contínua e as DFrFT consideradas na Figura 10.

a	0,25	0,50	0,75	1,00
Ozaktas (OZAKTAS et al., 1996)	0,0357	0,0364	0,0451	0,1426
Candan (CANDAN; KUTAY; OZAKTAS, 2000)	0,0366	0,0381	0,0453	0,1426
$\{\hat{\mathbf{g}}_m^{\perp}\}$	0,0359	0,0379	0,0495	0,1426
$\{\Phi_m\}$	0,0400	0,0472	0,0510	0,1426

Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

contínua de um pulso retangular[4], não foi verificado nenhuma diferença significativa entre os métodos, como indica a Tabela 2.

Outra maneira de comparar as diferentes abordagens da DFrFT é considerar a aplicação no cenário de filtragem no domínio fracionário. Com este propósito, para $0 \leq t \leq 40$, adicionou-se a um sinal Gaussiano

$$x(t) = e^{-\frac{(t-30)^2}{20}} \tag{2.31}$$

o sinal *chirp*

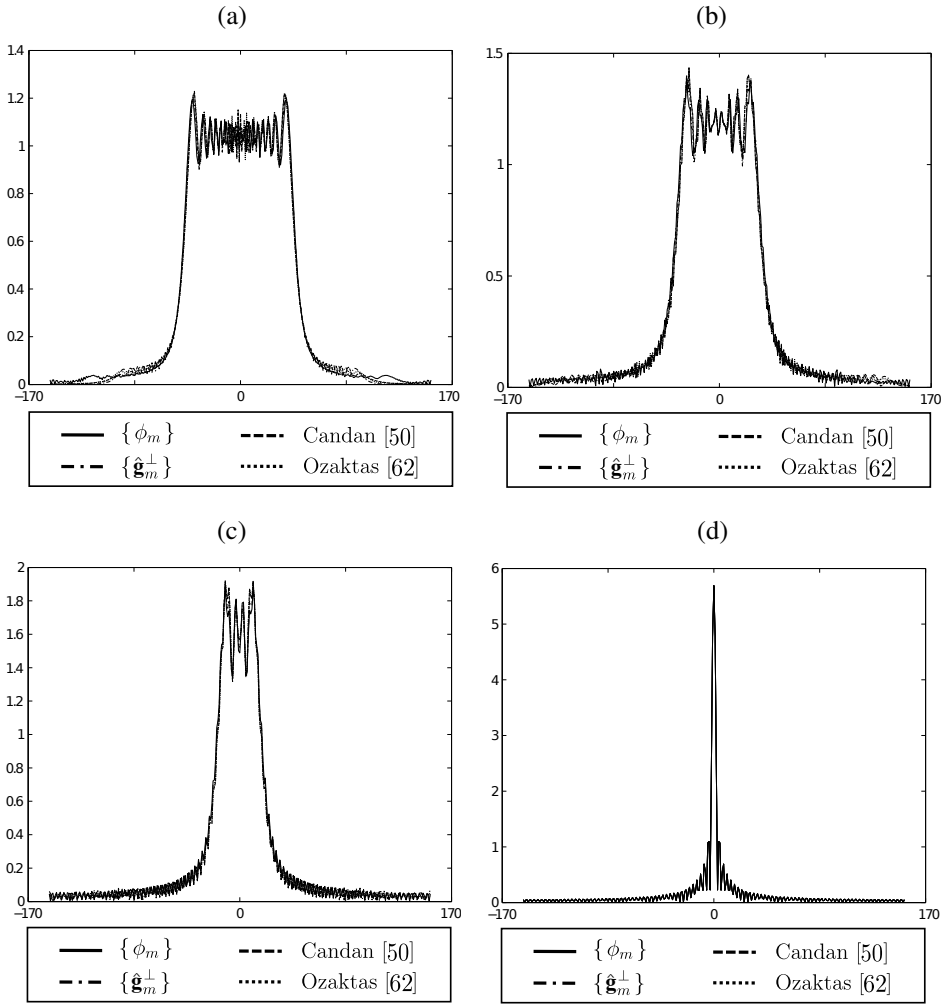
$$c(t) = 0{,}1e^{i\left(\frac{t^2}{10}-2t\right)}.$$

O sinal resultante foi então discretizado com um frequência de amostragem $f_s = \frac{315}{40}$ Hz; este valor foi escolhido para produzir um sinal de tempo discreto com 315 amostras. Desta maneira, as mesmas DFrFT empregadas para calcular a transformada do pulso retangular puderam ser utilizadas. Após aplicar a DFrFT, o sinal resultante no domínio fracionário foi multiplicado por um filtro rejeita-faixa. Por fim, a DFrFT inversa correspondente foi aplicada.

Na Figura 12a, é mostrado o sinal Gaussiano adicionado do sinal *chirp*. Nas Figuras 12b e 12c, para cada abordagem da DFrFT considerada previamente nesta seção, são mostrados respectivamente o sinal no domínio fracionário antes e depois da multiplicação pelo filtro rejeita-faixa; a ordem fracionária usada foi $a = 3{,}100$ para todas as abordagens da DFrFT, exceto para aquela baseada nos autovetores Φ_m, que utiliza $a = 3{,}088$. Tal diferença foi empiricamente imposta por prover um resultado melhor que o usando $a = 3{,}100$. Mesmo assim, os resultados obtidos pelas outras abordagens parecem mais precisos e contêm menos flutuações. Por outro lado, os resultados obtidos usando a abordagem de combinações lineares apresentou alguns desvios em relação ao resultado *correto*. Contudo, como mostrado na Figura 12d, os sinais Gaussianos filtrados exibem uma forma satisfatória para todas as abordagens da DFrFT. Esta

[4] A forma integral da FrFT foi aproximada por um somatório com um número de termos consideravelmente maior que $N = 315$ (OZAKTAS et al., 1996).

Figura 10 – Magnitude da DFrFT de 315 pontos de um pulso retangular de tempo discreto; as transformadas foram definidas usando quatro diferentes abordagens: Candan (CANDAN; KUTAY; OZAKTAS, 2000), Ozaktas (OZAKTAS et al., 1996), $\{\Phi_m\}$ e $\{\hat{\mathbf{g}}_m^{\perp}\}$.

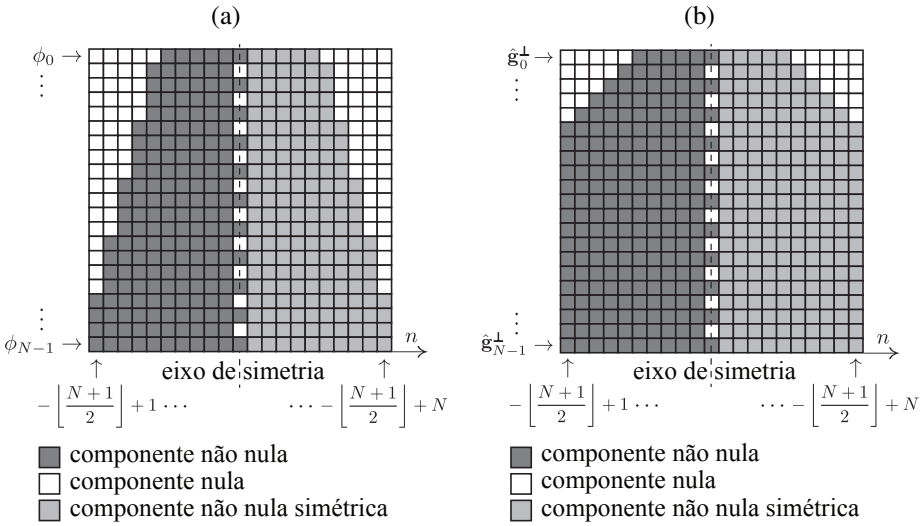


Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

conclusão é ratificada por meio do cálculo da razão sinal-ruído (SNR, do inglês *signal-to-noise ratio*) para cada uma das curvas mostradas na Figura 12d, usando como referência o sinal Gaussiano (2.31); todos os valores de SNR ficaram em torno de 210 dB.

Os resultados que foram descritos acima também podem ser apreciados obtendo a distribuição de Wigner dos sinais nos domínios original e fracionário (LOHMANN, 1993). Isso é possível devido ao fato da aplicação da transformada fracionária de Fourier corresponder a uma rotação da distribuição de Wigner, o que permite estimar a ordem fracionária necessária para aplicar a filtragem. Na Figura 13a, é mostrada a distribuição de Wigner do sinal Gaussiano adicionado do sinal *chirp*. O sinal Gaussiano é relacionado à elipse com aspecto achatado; o sinal *chirp* corresponde predominantemente aos pontos azuis claros e escuros em torno da elipse. Na Figura 13b, para cada abordagem da DFrFT, é mostrada a distribuição de Wigner do sinal no

Figura 11 – Ilustração enfatizando a simetria e as componentes nulas dos autovetores construídos utilizando (a) combinações lineares e (b) o método de matrizes geradoras ($N = 21$). Cada linha está relacionada a um autovetor; os quadrados representam suas respectivas componentes.

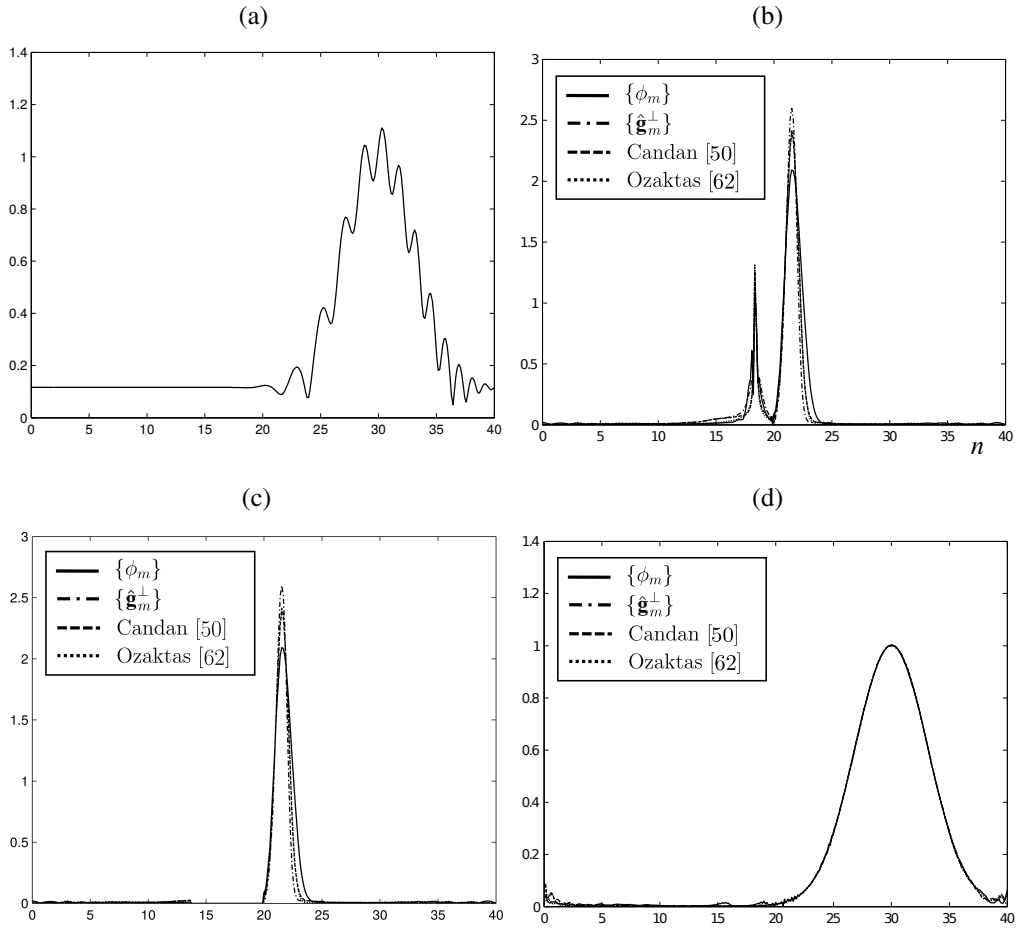


Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

domínio fracionário. Idealmente, a ordem fracionária usada para cada DFrFT deve prover uma separação da elipse que representa o sinal Gaussiano do conteúdo relacionado ao sinal *chirp* por meio de uma linha vertical imaginária. O resultado de tal separação é mostrado na Figura 13c, e na Figura 13d, é apresentada a distribuição de Wigner do sinal Gaussiano recuperado no domínio original. Comparando estas figuras, a maior distinção relacionada às diferentes abordagens da DFrFT é a pequena deformação na elipse relacionada ao sinal Gaussiano, quando é aplicada a abordagem de combinações lineares. No entanto, isso não parece crucial para recuperar o sinal Gaussiano com uma forma aceitável (ver Figura 18d).

Embora as DFrFT definidas nesta seção aproximem numericamente a FrFT e obedeçam suas propriedades, algoritmos sistemáticos para o cálculo rápido dessas transformadas ainda não estão disponíveis. Isso significa que, à primeira vista, multiplicar $\mathbf{F}^a$ por um vetor N-dimensional requer $\mathcal{O}(N^2)$ operações aritméticas. Contudo, é factível presumir que algumas peculiaridades dos autovetores HGL podem ser exploradas para desenvolver algoritmos com complexidade reduzida para valores específicos de N (potências de dois, por exemplo). Tal possibilidade se deve basicamente à simetria dos autovetores e ao fato de que várias componentes desses vetores serem nulas (especialmente se for utilizado o método de combinações lineares, como mostrado na Figura 11). Detalhes sobre a factibilidade desta ideia são discutidos no Capítulo 3.

Figura 12 – Filtragem de sinais por meio da DFrFT: (a) domínio original; (b) domínio fracionário; (c) domínio fracionário após a filtragem rejeita-faixa; (d) domínio original do sinal filtrado; usando quatro diferentes abordagens: Candan (CANDAN; KUTAY; OZAKTAS, 2000), Ozaktas (OZAKTAS et al., 1996), $\{\Phi_m\}$ e $\{\hat{\mathbf{g}}_m^{\perp}\}$.

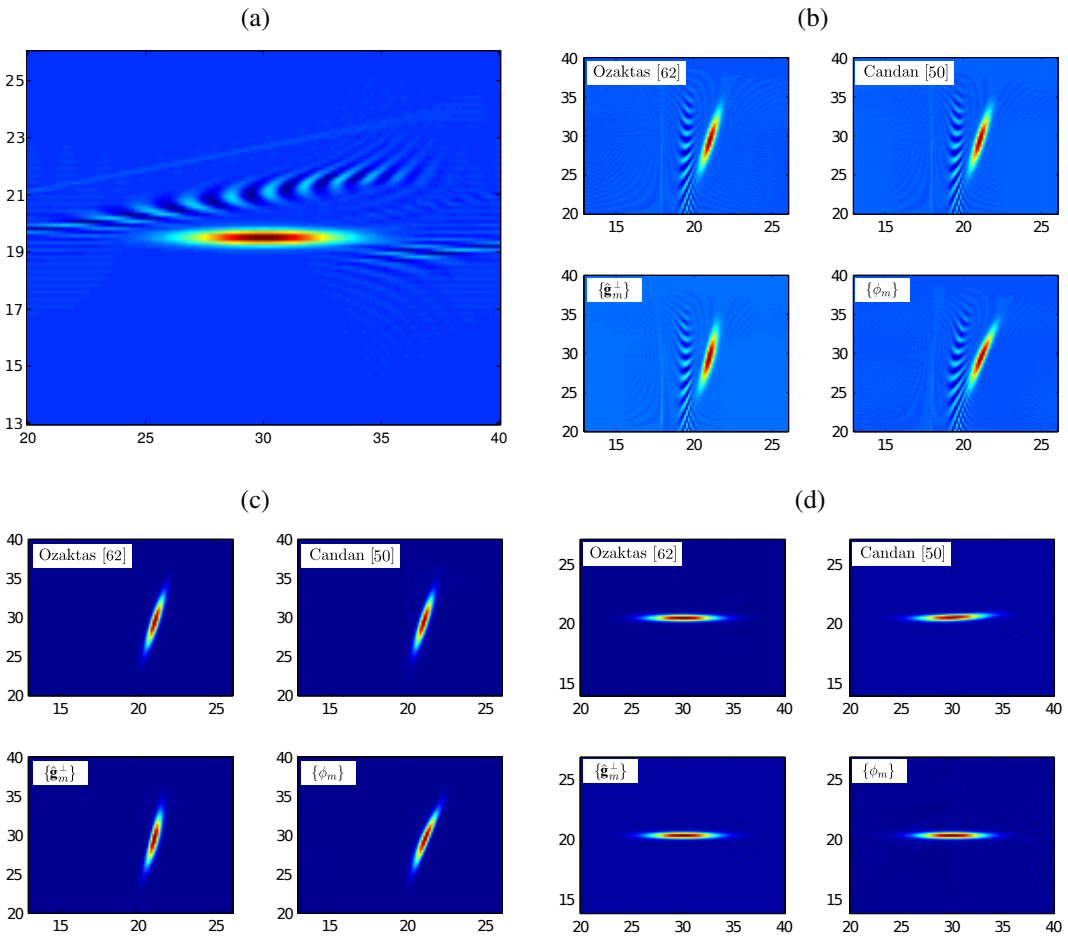


Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

2.6 CONSIDERAÇÕES

Neste capítulo, foram investigadas propriedades dos autovetores do tipo Hermite-Gaussiano construídos por fórmulas fechadas. Vários aspectos acerca do método de matrizes geradoras para construção destes autovetores foram esclarecidos e paralelos entre esta metodologia e a proposta em (KUZNETSOV, 2015) foram traçados. Combinando estes métodos, um procedimento sistemático para construção de bases de autovetores HGL para qualquer valor de N foi proposto e vários resultados numéricos foram apresentados e analisados. Estes resultados sugerem que as componentes de tais autovetores HGL aproximam amostras dos sinais Hermite-Gaussianos contínuos correspondentes e, portanto, seu uso na expansão espectral da matriz da DFT permite fracionarizar este operador de maneira análoga à utilizada na definição da FrFT. Ainda, foi apresentada uma família de matrizes geradoras e, empregando-a, foi proposto um método recursivo para construção da autobase HGL da DFT dada em (KUZNETSOV, 2015). Por fim, na

Figura 13 – Distribuição de Wigner do sinal no: (a) domínio original; (b) domínio fracionário; (c) domínio fracionário após a filtragem rejeita-faixa; (d) domínio original do sinal filtrado; usando quatro diferentes abordagens: Candan (CANDAN; KUTAY; OZAKTAS, 2000), Ozaktas (OZAKTAS et al., 1996), $\{\Phi_m\}$ e $\{\hat{\mathbf{g}}_m^{\perp}\}$.



Fonte: (DE OLIVEIRA NETO; LIMA, 2017)

Seção 2.5, as DFrFT apresentadas são aplicadas e seus resultados são discutidos e comparados com definições clássicas encontradas na literatura.

3 CÁLCULO DA TRANSFORMADA FRACIONÁRIA DISCRETA DE FOURIER COM COMPLEXIDADE ARITMÉTICA REDUZIDA

Como descrito no Capítulo 2 desta tese, a transformada fracionária de Fourier (FrFT, do inglês *fractional Fourier transform*) tem sido vastamente investigada e empregada em várias aplicações (OZAKTAS; ZALEVSKY; KUTAY, 2001; WEIMANN et al., 2016; LIU; SHERIDAN, 2013; WEI; LI, 2016; LIMA; NOVAES, 2014; WANG et al., 2016; TAO; MENG; WANG, 2011; ZHAO et al., 2016c; LU; XIAO; WEI, 2016; PELICH et al., 2016). Esta transformada corresponde a uma generalização da respectiva transformada ordinária, em que potências não-inteiras do operador transformada de Fourier podem ser consideradas. Neste contexto, uma questão central diz respeito ao cálculo digital eficiente da transformada. O método mais popular para computar a FrFT digitalmente é o proposto em (OZAKTAS et al., 1996), em que a transformada é aproximada por uma sucessão de operadores discretos cuja aplicação a um sinal envolve complexidade aritmética $\mathcal{O}(N\log(N))$, no entanto existem limitações quanto à manutenção das propriedades da FrFT (ver texto introdutório do Capítulo 2).

Outra possibilidade é a definição da transformada fracionária discreta de Fourier, DFrFT, em que se obtém um operador matricial $\mathbf{F}^a$, $a \in \mathbb{R}$, em que $\mathbf{F}$ é o operador DFT em sua forma matricial como descrito no Capítulo 2.

Isso é normalmente feito considerando a autodecomposição de $\mathbf{F}$, que permite escrever

$$\mathbf{F}^a = \mathbf{E}\Lambda^a\mathbf{E}^T. \tag{3.1}$$

Na equação acima, se $\mathbf{E}$ for uma matriz ortogonal tendo em sua k-ésima coluna um autovetor HGL da DFT, o produto da matriz $\mathbf{F}^a$ por um sinal possui resultado numericamente próximo ao obtido quando comparado ao resultado obtido pelo cálculo da FrFT (de tempo contínuo) do mesmo sinal. Na verdade, existem várias outras abordagens para definir uma DFrFT (PEI; YEH; TSENG, 1999; HANNA; SEIF; AHMED, 2004; HANNA; SEIF; AHMED, 2006; HANNA; SEIF; AHMED, 2008; HANNA, 2012; SERBES; DURAK-ATA, 2011). Em particular, se a expansão espectral em (3.1) for empregada com uma autobase de autovetores que não sejam HGL (PEI; WEN; DING, 2008; HSUE; CHANG, 2015a; KANG; ZHANG; TAO, 2015a; ANNABY; RUSHDI; NEHARY, 2016a), a aproximação à transformada de tempo contínuo não é provida; nestes casos, embora a transformada obtida tenha interesse para aplicações (tais como cifragem de imagem, por exemplo), ela não corresponde a uma versão discreta *verdadeira* da FrFT.

Existem duas principais abordagens para construção de autovetores HGL da DFT. A primeira é a baseada em matrizes comutantes com a matriz $\mathbf{F}$ e depende de fórmulas não-fechadas (CANDAN; KUTAY; OZAKTAS, 2000; PEI; HSUE; DING, 2006; SANTHANAN; SANTHANAN, 2007; HANNA; SEIF; AHMED, 2008; PEI; WEN; DING, 2008; WEI et

al., 2011; WEI; LI, 2014; SERBES; DURAK-ATA, 2011; BHATTA; SANTHANAM, 2015; CANDAN, 2007); neste caso, mesmo se for assumido que os referidos autovetores são gerados *off-line* (ou seja, são gerados anteriormente ao seu uso, de forma que o esforço necessário para o seu cálculo não interfere na complexidade aritmética), o produto da matriz da DFrFT resultante $\mathbf{F}^a$ por um vetor envolve $\mathcal{O}(N^2)$ operações aritméticas (PEI; CHANG, 2016). A segunda abordagem é baseada em expressões analíticas (de fórmulas fechadas) combinada com o método das matrizes geradoras (KONG, 2008; KUZNETSOV, 2015; DE OLIVEIRA NETO; LIMA, 2017; KUZNETSOV; KWASNICKI, 2018; DE OLIVEIRA NETO; LIMA; PANARIO, 2018a), que foi descrita no Capítulo 2; também neste caso, a estrutura da matriz da DFrFT resultante $\mathbf{F}^a$ não favorece sua multiplicação por um vetor com complexidade sub-quadrática. Por outro lado, tem-se observado que algumas propriedades dos autovetores gerados utilizando a abordagem em questão permite calcular a DFrFT correspondente com considerável redução da complexidade aritmética; isso se deve principalmente ao número de componentes dos referidos autovetores cujos valores são zero, o que resulta num número menor de adições e multiplicações requeridas para o cálculo da transformada.

Neste capítulo, será introduzida uma metodologia que utiliza a característica mencionada acima para computar com complexidade aritmética reduzida a DFrFT baseada na autodecomposição do operador da DFT ordinária[1] de um vector $\mathbf{x}$ cujas componentes são números complexos. Em vez de considerar particularidades da estrutura da matriz e atacar diretamente o problema de realizar o produto $\mathbf{F}^a\mathbf{x}$, a abordagem descrita neste capítulo considera primeiramente a multiplicação sequencial à esquerda de $\mathbf{x}$ por $\mathbf{E}^T$, $\mathbf{\Lambda}^a$ e $\mathbf{E}$. É demonstrado que a complexidade multiplicativa do método proposto é similar à apresentada em (MAJORKOWSKA-MECH; CARIOW, 2017)[2], sendo, de forma geral, um pouco menor. Por outro lado, a complexidade aditiva é reduzida para menos da metade da do algoritmo proposto em (MAJORKOWSKA-MECH; CARIOW, 2017). Além disso, é introduzida uma estratégia de arredondamento que reduz consideravelmente o número de multiplicações requeridas pelo método proposto, sem comprometer o desempenho do ponto de vista prático (como mostrado na Seção 3.2, p. 69); para $N = 512$, por exemplo, o número de multiplicações necessárias é reduzida para um terço do original.

As contribuições contidas neste capítulo são sumarizadas a seguir:

i Nas Seções 3.1.1 e 3.1.2, é explicado como as simetrias, o suporte próprio compacto e as componentes repetidas dos autovetores HGL da DFT podem ser explorados para reduzir o número de multiplicações e adições necessárias para o cálculo da DFrFT correspondente;

[1] A partir daqui, este método será referenciado apenas como "DFrFT baseada em autodecomposição" por questões de síntese.

[2] Partindo da literatura especializada, o método dado em (MAJORKOWSKA-MECH; CARIOW, 2017) é o que requer a menor complexidade aritmética para o cálculo da DFrFT baseada na autodecomposição do operador ordinário. Por isso, ao longo deste capítulo, esta é a principal referência usada para comparação dos resultados alcançados com o método proposto neste trabalho.

ii Na Seção 3.1.3, é introduzida a estratégia de arredondamento baseada no fato de que, quando N cresce, várias componentes dos autovetores HGL da DFT possuem valores muito próximos a zero e, assim, podem ser tratadas como zero para propósitos práticos. Isso também reduz a complexidade aritmética envolvida no cálculo da DFrFT;

iii Na Seção 3.1.4, é explicado como contar o número de operações aritméticas necessárias para aplicar o método proposto;

iv Na Seção 3.1.5, são comparados os resultados providos pelo método proposto e por outros métodos encontrados na literatura para o cálculo da DFrFT baseada na autodecomposição. Se nenhum arredondamento for feito, a técnica proposta requer um número de multiplicações um pouco menor e metade ou menos do número de adições quando comparada com o até então mais eficiente método (MAJORKOWSKA-MECH; CARIOW, 2017). Se a estratégia de arredondamento discutida na Seção 3.1.3 for aplicada, até 65% das multiplicações podem ser evitadas;

v Na Seção 3.2, os resultados são validados a partir de experimentos computacionais em que a filtragem e a representação compacta de sinais no domínio fracionário são considerados. Verifica-se que, mesmo quando a estratégia de arredondamento é utilizada, o desempenho da DFrFT aplicada não é comprometido. Particularmente, é demonstrado que, em cenários em que a busca de uma ordem fracionária ideal tem que ser realizada, o número de multiplicações e adições pode ser reduzido em até 80%.

3.1 CÁLCULO DA DFRFT COM COMPLEXIDADE ARITMÉTICA REDUZIDA

Nesta seção, é introduzido o método proposto para o cálculo eficiente da DFrFT descrita na Seção 2.5, definida empregando a base de autovetores construída segundo o método descrito na Seção 2.4. É considerada a expansão espectral da matriz $\mathbf{F}^a$, como mostrado em (3.1), e é contado o número de multiplicações e adições necessárias para obter $\mathbf{X}^{(a)}$, a DFrFT de um vetor de entrada $\mathbf{x}$ cujas componentes são números complexos, por meio da realização do produto

$$\mathbf{X}^{(a)} = (\mathbf{E}\Lambda^a\mathbf{E}^T)\mathbf{x}.$$

Na expressão acima, tem-se que $\mathbf{x}$ é sequencialmente multiplicado à esquerda por $\mathbf{E}^T$, Λ^a e $\mathbf{E}$, produzindo os vetores intermediários

$$\mathbf{x}' = \mathbf{E}^T\mathbf{x}, \tag{3.2}$$

$$\mathbf{x}'' = \Lambda^a\mathbf{x}', \tag{3.3}$$

$$\mathbf{X}^{(a)} = \mathbf{E}\mathbf{x}''; \tag{3.4}$$

o ponto-chave do método proposto é considerar algumas propriedades dos autovetores HGL da DFT da autobase $\{\Phi_m\}_{0\leq m\leq N-1}$, que são estabelecidas e discutidas a seguir.

3.1.1 Simetrias e Suporte Próprio Compacto

É bem conhecido o fato de que qualquer autovetor da DFT possui simetria par ou simetria ímpar. Mais especificadamente, autovetores relacionados aos autovalores ± 1 e $\pm i$ são, respectivamente, de simetria par e de simetria ímpar (MCCLELLAN; PARKS, 1972). Se esta propriedade for considerada, o cálculo do produto escalar entre um vetor de $\{\Phi_m\}_{0 \leq m \leq N-1}$ e o vetor de entrada $\mathbf{x}$, que é a multiplicação entre uma coluna de $\mathbf{E}^T$ e $\mathbf{x}$ no produto matriz-vetor $\mathbf{x}' = \mathbf{E}^T\mathbf{x}$ em (3.2), pode ser realizado utilizando cerca de $N/2$ multiplicações. Esta propriedade também pode ser utilizada no produto matricial $\mathbf{X}^{(a)} = \mathbf{E}\mathbf{x}''$ em (3.4), em que um efeito similar em termos de multiplicações salvas é conseguido. Operações de adição também são salvas devido à simetria dos autovetores, porque algumas adições entre termos simetricamente posicionados de $\mathbf{x}$ e $\mathbf{x}''$ podem ser pré-calculadas.

Devido à desigualdade (2.5), os autovetores $\{\Phi_m\}_{0 \leq m \leq N-1}$ tem o que é conhecido como *suporte próprio compacto*. No contexto deste trabalho, isso significa que estes autovetores começam e terminam com sequências de componentes nulas, entre as quais aparecem as componentes não-nulas. Este fato é ilustrado na Figura 14, em que as componentes não-nulas de cada um dos autovetores HGL da DFT de comprimento $N = 16$ são representadas como quadrados brancos ao longo do eixo n; a simetria de cada vetor também é representada. Em geral, se Φ_m possuir simetria par, o número de componentes não-nulas é, no máximo[3],

$$\text{nonzero}(\Phi_m) = 2\lfloor (N + m + 2)/4 \rfloor + 1;$$

Se Φ_m possuir simetria ímpar, tal número é, no máximo,

$$\text{nonzero}(\Phi_m) = 2\lfloor (N + m + 2)/4 \rfloor.$$

Combinada com a simetria, esta propriedade permite economizar ainda mais operações aritméticas nos produtos matriciais (3.2) e (3.4). Para ser mais preciso, o cálculo do produto escalar entre um autovetor de simetria par Φ_m e um vetor de entrada $\mathbf{x}$ pode ser realizado usando no máximo

$$\lfloor (N + m + 2)/4 \rfloor + 1 \tag{3.5}$$

multiplicações; similarmente, se Φ_m possuir simetria ímpar, este número é

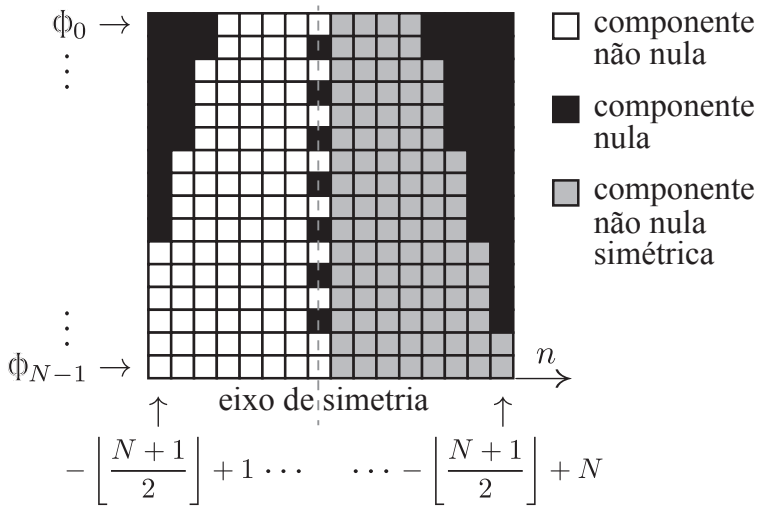
$$\lfloor (N + m + 2)/4 \rfloor. \tag{3.6}$$

3.1.2 Componentes Repetidas

Deixando as simetrias à parte, verifica-se que alguns autovetores $\Phi_m = [\phi_m(n)]$, $n \in I_N$, possuem componentes com valores absolutos repetidos. Isso também pode ser levado em

[3] As exceções são os vetores Φ_{N-2} e Φ_{N-1}, para os quais tem-se $\text{nonzero}(\Phi_m) = N$; estes casos serão tratados separadamente ao longo do desenvolvimento.

Figura 14 – "Imagem" da matriz $\mathbf{E}^T$, $N = 16$, em que simetrias e componentes nulas dos autovetores HGL da DFT podem ser observadas.



Fonte: Produzido pelos autores.

consideração para reduzir a complexidade aritmética envolvida nos produtos matriciais em (3.2) e (3.4). Por exemplo, considere os seguintes vetores para $N = 8$, que são escritos no formato transposto para melhor visualização[4]:

$$\Phi_2^T = \begin{bmatrix} 0{,}168278385 \\ 0{,}574538345 \\ 0{,}168278385 \\ -0{,}475963149 \\ 0{,}168278385 \\ 0{,}574538345 \\ 0{,}168278385 \\ 0{,}000000000 \end{bmatrix}; \quad \Phi_3^T = \begin{bmatrix} -0{,}353553391 \\ -0{,}500000000 \\ 0{,}353553391 \\ 0{,}000000000 \\ -0{,}353553391 \\ 0{,}500000000 \\ 0{,}353553391 \\ 0{,}000000000 \end{bmatrix}.$$

Desde que $\phi_2(-3) = \phi_2(-1)$, ao invés de requerer 4 multiplicações, o produto $\langle \Phi_2, \mathbf{x} \rangle$ requer 3 multiplicações. Uma redução similar pode ser realizada no cálculo de $\langle \Phi_3, \mathbf{x} \rangle$, porque $\phi_3(-3) = -\phi_3(-1)$. Essa característica é também observada para valores maiores de N. Para, por exemplo, $N = 128$, tem-se $\phi_{123}(2) = \phi_{123}(60)$.

Adicionalmente, considerando-se o formato peculiar de Φ_{N-1} e Φ_{N-2} (ver Definição 2.4, p. 45). Com exceção da última componente, isto é, a $(-M + N)$-ésima componente, os referidos vetores são formados por componentes com o mesmo valor absoluto de sinal alternado. Novamente, como exemplo, os autovetores Φ_6 e Φ_7 para $N = 8$ são ilustrados como dito

[4] Embora as componentes dos autovetores sejam exibidas com nove casas decimais apenas, elas são na verdade armazenadas no formado de ponto flutuante com precisão dupla, isso é, 11 e 52 bits são usados para o expoente e a mantissa, respectivamente.

Tabela 3 – Autovetores Φ_m que têm componentes não-nulas com valores repetidos (simetrias à parte) e o respectivo número de componetes não-nulas com valores absolutos distintos $\mathbf{d}_m$.

N	m	$\mathbf{d}_m$
8	$2, 3, 6, 7$	$3, 2, 2, 2$
16	$2, 3, 7, 11, 13, 14, 15$	$5, 3, 5, 5, 5, 2, 2$
32	$2, 3, 27, 29, 30, 31$	$9, 8, 9, 9, 2, 2$
64	$3, 7, 11, 59, 61, 62, 63$	$16, 17, 18, 17, 17, 2, 2$
128	$123, 125, 126, 127$	$33, 33, 2, 2$
256	$251, 253, 254, 255$	$65, 65, 2, 2$
512	$507, 509, 510, 511$	$129, 129, 2, 2$

Fonte: Produzido pelos autores.

anteriormente:

$$\Phi_6^T = \begin{bmatrix} 0{,}310937912 \\ -0{,}310937912 \\ 0{,}310937912 \\ -0{,}310937912 \\ 0{,}310937912 \\ -0{,}310937912 \\ 0{,}310937912 \\ 0{,}568527312 \end{bmatrix}; \quad \Phi_7^T = \begin{bmatrix} -0{,}214883126 \\ 0{,}214883126 \\ -0{,}214883126 \\ 0{,}214883126 \\ -0{,}214883126 \\ 0{,}214883126 \\ -0{,}214883126 \\ 0{,}822664388 \end{bmatrix}.$$

Esta característica, que também é verificada para valores maiores de N, permite calcular o produto de Φ_{N-1} ou Φ_{N-2} por $\mathbf{x}$ usando apenas 2 multiplicações.

Com base na discussão acima, foi realizada uma busca, para $N = 2^k$, $3 \leq k \leq 9$, como a intenção de encontrar todos os autovetores com componentes repetidas (simetrias à parte). Denotando por $\mathbf{R}_N$ o conjunto de índices de tais autovetores para um dado N, o número $\mathbf{d}_m$ de componentes não-nulas de Φ_m, $m \in \mathbf{R}_N$, com valores absolutos distintos foi calculado. O resultado, que é mostrado na Tabela 3, é considerado em seções futuras deste capítulo, uma vez que a quantidade $\mathbf{d}_m$ corresponde ao número de multiplicações necessárias para realizar o produto $\langle \Phi_m, \mathbf{x} \rangle$.

3.1.3 Questões Relacionadas à Precisão

A execução do método para geração da autobase HGL da DFT $\{\Phi_m\}_{0 \leq m \leq N-1}$ mostrada na Seção 2.4 requer considerar alguns aspectos de precisão numérica. Isso ocorre principalmente devido ao fato do método envolver operações de natureza recursiva (por exemplo, o processo de ortogonalização), que são susceptíveis ao acúmulo de erros de arredondamento; obviamente, isso se torna crítico à medida que N cresce. Por esta razão, o cálculo *off-line* para geração dessa autobase é realizado empregando aritmética de múltipla precisão[5]. Isso garante uma correta

[5] Os autovetores são gerados no SageMath, que possui uma biblioteca interna que lida com aritmética de múltipla precisão.

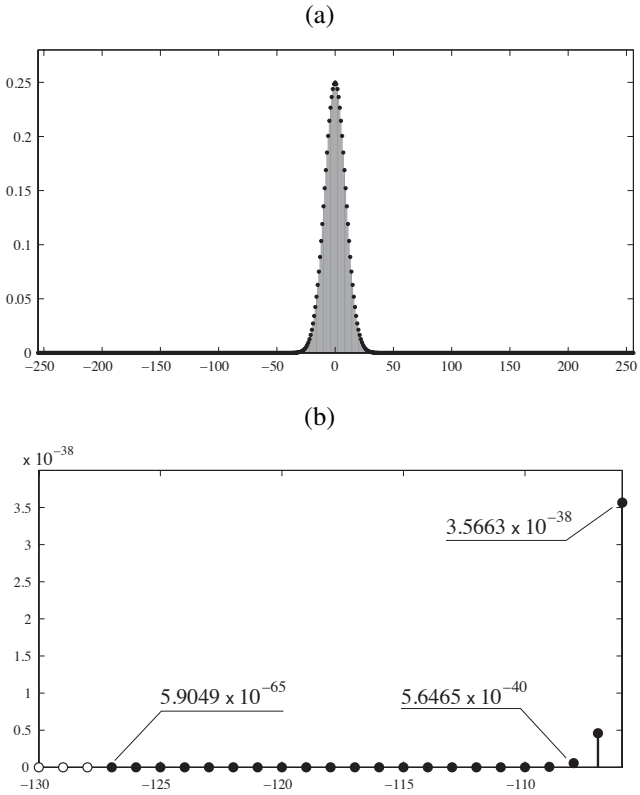
construção dos autovetores, que podem conter componentes cuja magnitude é muito próxima de zero assim como componentes cujas magnitudes são muito próximas entre si.

Para ilustrar esta característica, considere o autovetor Φ_0 para $N = 512$ (ver Figura 15). Devido a (2.5), é sabido que $\phi_0(n)$ é zero nos intervalos $-255 \leq n \leq -129$ e $129 \leq n \leq 256$. Contudo, observando a Figura 15a, tal sequência de componentes nulas parece se estender até quase a parte central do eixo horizontal, em que o sinal Gaussiano discreto cresce e decai. Esta percepção equivocada é produzida devido ao fato de que Φ_0 possui componentes muito próximas de zero, isso pode ser visto na Figura 15b. Uma característica similar pode ser observada para autovetores Φ_m, $m \neq 0$, embora perca força à medida em que m cresce; isso ocorre porque o comprimento do autovetor se torna cada vez maior e os autovetores HGL da DFT possuem mais variações abruptas entre componentes consecutivas.

De qualquer forma, a questão da precisão aritmética pode ser explorada para reduzir a complexidade aritmética envolvida nos produtos matriz-vetor em (3.2) e (3.4); neste caso, o que se propõe fazer é simplesmente arredondar os valores das componentes dos autovetores em uma certa casa decimal. A primeira consequência de tal procedimento é que o comprimento do vetor irá diminuir; componentes que estão na borda do suporte próprio do autovetor, mas que possuem valores muito próximos de zero, podem se tornar efetivamente zero após o arredondamento. Então, o número de operações envolvendo o produto matriz-vetor pode ser reduzido. Como segunda consequência, após o arredondamento, componentes não-nulas que possuem magnitudes muito próximas entre si podem assumir o mesmo valor; neste caso, elas podem ser tratadas como componentes repetidas, que, como explicado na Seção 3.1.2, também podem ser exploradas para reduzir a complexidade aritmética. Na Figura 16, são providas "imagens" da matriz $\mathbf{E}^T$, $N = 512$, antes e após o arredondamento; o efeito das componentes zeradas dos autovetores HGL da DFT pode ser visto observando as regiões em branco (componentes não-nulas) e em preto (componentes nulas) ao longo das linhas da Figura 16a, Figura 16b e Figura 16c para matriz não-arredondada, arredondada na nona casa decimal e arredondada na terceira casa decimal, respectivamente; na última, os pontos pretos dentro da região com contorno em forma de parábola representam as várias componentes que não-estão na fronteira do suporte próprio do autovetor, mas que foram zeradas após o arredondamento (veja a visão ampliada da área quadrada selecionada da figura).

Naturalmente, dependendo do quão rigoroso o arredondamento proposto é aplicado, isso pode trazer efeitos indesejáveis. As versões arredondadas dos autovetores Φ_m podem não ser um autovetor da DFT para um certo nível de precisão; consequentemente, a versão arredondada do conjunto $\{\Phi_m\}_{0 \leq m \leq N-1}$ pode não ser uma autobase ortogonal da DFT, ou nem mesmo uma base. Desta maneira, a aplicação da transformada correspondente, identificada deste ponto em diante como **DFrFT arredondada proposta**, em um dado cenário prático pode não prover a acurácia necessária. Para um dado N, a tarefa é escolher uma casa decimal em que as componentes dos autovetores podem ser arredondadas, fornecendo uma redução não

Figura 15 – Componentes do autovetor Φ_0 $(N = 512)$ nos intervalos (a) $-255 \leq n \leq 256$ e (b) $-130 \leq n \leq -106$; em (b), componentes nulas são identificadas por círculos brancos.



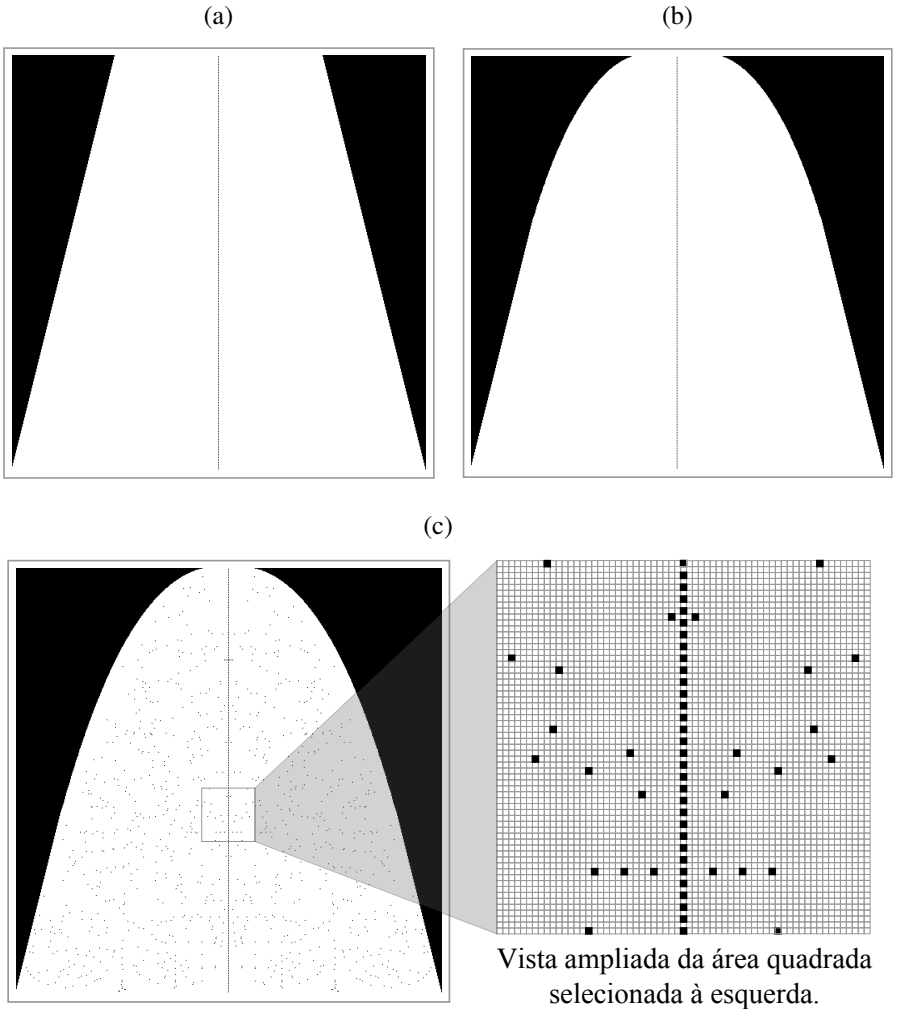
Fonte: Produzido pelos autores.

negligenciável na complexidade aritmética do cálculo da transformada e sem o comprometimento do desempenho da transformada quando o processamento de um dado sinal é realizado para um propósito específico. Estas premissas são consideradas nas seções seguintes desse capítulo.

3.1.4 Número de Multiplicações e Adições

Nesta seção, é quantificado o impacto que as propriedades e estratégias discutidas nas Seções 3.1.1, 3.1.2 e 3.1.3 têm na redução da complexidade aritmética envolvida no cálculo da DFrFT considerada neste trabalho. Para ilustrar como isso é realizado, são inicialmente

Figura 16 – Imagens da matriz $\mathbf{E}^T$, $N = 512$, para (a) matriz sem arredondamento, (b) com arredondamento na nona casa decimal e (c) com arredondamento na terceira casa decimal; regiões pretas e brancas representam componentes nulas e não-nulas, respectivamente.



Fonte: Produzido pelos autores.

fornecidos detalhes acerca do cálculo da DFrFT para $N = 8$, para a qual se tem

$$\mathbf{E}^T = \begin{bmatrix} 0 & A & B & C & B & A & 0 & 0 \\ 0 & D & E & 0 & -E & -D & 0 & 0 \\ F & G & F & H & F & G & F & 0 \\ I & J & -I & 0 & I & J & -I & 0 \\ K & L & M & N & M & L & K & 0 \\ O & P & Q & 0 & -Q & -P & -O & 0 \\ R & -R & R & -R & R & -R & R & S \\ T & -T & T & -T & T & -T & T & U \end{bmatrix},$$

em que

$$A = 0{,}1434, \quad B = 0{,}4896, \quad C = 0{,}6924, \quad D = -0{,}4082,$$
$$E = -0{,}5774, \quad F = 0{,}1683, \quad G = 0{,}5745, \quad H = -0{,}4760,$$
$$I = -0{,}3536, \quad J = -0{,}5000, \quad K = 0{,}5734, \quad L = 0{,}0805,$$
$$M = -0{,}2985, \quad N = 0{,}3888, \quad O = -0{,}6124, \quad P = 0{,}2887,$$
$$Q = -0{,}2041, \quad R = 0{,}3109, \quad S = 0{,}5685, \quad T = -0{,}2149,$$
$$U = 0{,}8227;$$

também se tem

$$\Lambda^a = \mathrm{diag}\left([\lambda_0^a \quad \lambda_1^a \quad \cdots \quad \lambda_7^a]\right),$$

em que $\lambda_0^a = 1$, $\lambda_n^a = e^{-i\frac{\pi}{2}na}$, para $1 \leq n \leq 6$, e $\lambda_7^a = e^{-i\frac{\pi}{2}8a}$.

O número de multiplicações necessárias para calcular $\mathbf{x}' = \mathbf{E}^T\mathbf{x}$ como em (3.2) é o número de componentes não-nulas de $\mathbf{E}$ com valores absolutos distintos, isso é, 21 (neste passo, tem-se a multiplicação de um número real por um complexo); este também é o número de multiplicações necessárias para o cálculo de $\mathbf{X}^{(a)} = \mathbf{E}\mathbf{x}''$ como indicado em (3.4). O produto $\mathbf{x}'' = \Lambda^a\mathbf{x}'$ em (3.3) requer 7 multiplicações entre dois números complexos (a multiplicação por $\lambda_0^a = 1$ é trivial). Pode ser verificado que o número de adições complexas necessárias para obter $\mathbf{x}'$ é igual 22; este número é alcançado contando-se o número de elementos não-nulos com valores distintos em cada vetor (linhas de $\mathbf{E}^T$), pré-computando adições $x(n) + x(-n)$, $n = -3, -2, -1$, e observando que o número de adições pode ser reduzido ainda mais quando componentes com valores repetidos são levadas em consideração (ver Seção 3.1.2). O número de adições complexas necessárias para realizar $\mathbf{E}\mathbf{x}''$ é 24; isso pode ser verificado observando que, uma vez que o produto da n-ésima linha de $\mathbf{E}$, $n = 0, 1, 2$, por $\mathbf{x}''$ é calculado, o produto entre a $(8 - n - 2)$-ésima linha de $\mathbf{E}$ e $\mathbf{x}''$ pode ser obtido utilizando apenas uma adição. Também é pré-calculado $Rx(3) + Tx(4)$, então mais três adições são necessárias para calcular $X^{(a)}(0)$ e uma adição a mais é necessária para calcular $X^{(a)}(4)$.

Assumindo que (i) uma multiplicação entre uma número real e um complexo é realizada usando duas multiplicações reais, (ii) uma multiplicação entre dois números complexos é realizada usando três multiplicações reais e cinco adições reais, e (iii) uma adição entre dois números complexos é realizada usando duas adições reais, conclui-se que

$$\mathbf{M}_8 = 2 \times (21 + 21) + 3 \times 7 = 105$$

e

$$\mathbf{A}_8 = 5 \times 7 + 2 \times 22 + 2 \times 24 = 127 \tag{3.7}$$

multiplicações e adições reais, respectivamente, são necessárias para calcular a transformada; o termo 5×7 em (3.7) corresponde ao número de adições reais necessárias para calcular as multiplicações entre números complexos em $\mathbf{x}'' = \Lambda^a\mathbf{x}'$.

A complexidade multiplicativa $\mathbf{M}_N$ para calcular a DFrFT de N pontos pode ser obtida considerando (3.5), (3.6) e a possível ocorrência de componentes repetidas (ver Seção 3.1.2 e Tabela 3); também é considerado que o produto matriz-vetor em (3.3) requer $N-1$ multiplicações complexas. Em geral, tem-se

$$\begin{aligned}\mathbf{M}_N = 2\times 2\times \sum_{\substack{m \text{ par};\\ m\notin \mathbf{R}_N}} \left(\lfloor (N+m+2)/4\rfloor + 1\right) + 2\times 2\times \sum_{\substack{m \text{ ímpar};\\ m\notin \mathbf{R}_N}} \lfloor (N+m+2)/4\rfloor \\ +2\times 2\times \sum_{m\in \mathbf{R}_N} \mathbf{d}_m + 3\times (N-1).\end{aligned} \tag{3.8}$$

Por simplicidade, a fórmula da complexidade aditiva é derivada a seguir considerando apenas as componentes repetidas em Φ_{N-2} e Φ_{N-1}, e negligenciando o que pode ocorrer em outros autovetores (ver Tabela 3); isso não deve ter um impacto significativo na complexidade aritmética total do método proposto. Denotando por $\mathbf{A}'_N$ o número de adições reais para obter $\mathbf{x}' = \mathbf{E}^T\mathbf{x}$, tem-se

$$\begin{aligned}\mathbf{A}'_N = 2\times 2\times \left(\tfrac{N}{2}-1\right) + 2\times \sum_{m \text{ par}} \left(\lfloor (N+m+2)/4\rfloor\right) \\ +2\times \sum_{\substack{m \text{ ímpar};\\ m\neq N-1}} \left(\lfloor (N+m+2)/4\rfloor - 1\right) + 2.\end{aligned} \tag{3.9}$$

Em (3.9), o primeiro termo é relacionado ao pré-cálculo de $x(n)+x(-n)$, $n=-N/2+1,\ldots,-1$; o segundo e terceiro termos são relacionados ao número de elementos não-nulos com valores absolutos distintos (simetrias são consideradas, mas as repetições são exploradas como explicado na Seção 3.1.2 apenas para $m=N-1$). Uma vez que $x'(N/2-1)$ é calculado, $x'(N/2)$ pode ser calculado com uma adição complexa a mais (as duas adições reais no final da última equação). O número de adições reais vindas de $\mathbf{x}''=\Lambda^a\mathbf{x}'$ é

$$\mathbf{A}''_N = 5\times (N-1). \tag{3.10}$$

Finalmente, denotando por $\mathbf{A}'''_N$ o número de adições reais necessárias para obtenção de $\mathbf{X}^{(a)} = \mathbf{E}\mathbf{x}''$, tem-se

$$\begin{aligned}\mathbf{A}'''_N = 2\times 6 + 2\times \sum_{\substack{k=1\\ N>8}}^{\frac{N}{4}-2} (6+4k-1) + 2\times (N-1)\times \left(\lfloor (N+2)/4\rfloor\right) \\ +2\left(\tfrac{N}{2}-1\right)+2.\end{aligned} \tag{3.11}$$

Em (3.11), o primeiro termo é relacionado ao cálculo do produto entre a 0-ésima coluna de $\mathbf{E}^T$ (0-ésima linha de $\mathbf{E}$) e $\mathbf{x}''$. Isso também inclui uma adição necessária para realizar o produto entre a $(N-2)$-ésima coluna de $\mathbf{E}^T$ e $\mathbf{x}''$, assim, uma adição é necessária para pré-calcular

$$\phi_{N-2}(N/2)x''(N/2-1) + \phi_{N/2}(N/2)x''(N-1);$$

o somatório no segundo termo conta o número de adições necessárias para calcular o produto entre a n-ésima, $n = 1, 2, \ldots, N/4-2$, coluna da $\mathbf{E}^T$ e $\mathbf{x}''$ (é incluída uma adição necessária para calcular o produto entre a $(N-n-2)$-ésima coluna de $\mathbf{E}^T$ e $\mathbf{x}''$); no terceiro termo, é contado o número de adições necessárias para realizar o produto entre a n-ésima, $n = N/4-1, \ldots, N/2-2$, coluna de $\mathbf{E}^T$ e $\mathbf{x}''$ (é incluída uma adição necessária para realizar o produto entre a $(N-n-2)$-ésima coluna de $\mathbf{E}^T$ e $\mathbf{x}''$); por fim, no quarto e quinto termos, são contados, respectivamente, o número de adições necessárias para realizar o produto entre a $(N/2-1)$-ésima e a $(N-1)$-ésima coluna de $\mathbf{E}^T$ e $\mathbf{x}''$. Assim, o total de adições reais necessárias para o cálculo da DFrFT é

$$\mathbf{A}_N = \mathbf{A}'_N + \mathbf{A}''_N + \mathbf{A}'''_N. \tag{3.12}$$

Se a estratégia de arredondamento descrita na Seção 3.1.3 for empregada, as fórmulas (3.8) e (3.12) não podem ser usadas para obter a complexidade aritmética envolvida no cálculo da DFrFT correspondente. Isso é devido ao fato que tal estratégia produz um decréscimo no suporte de alguns autovetores, por anular componentes cujo valor absoluto era bem próximo a zero antes do arredondamento. Como não é possível prever o quanto o suporte do vetor será diminuído, dada a casa decimal em que o arredondamento é realizado, recorreu-se a um programa de computador para contar o número de multiplicações e adições necessárias para calcular a DFrFT arredondada. De qualquer forma, premissas similares às que têm sido consideradas nesta seção são empregadas em tal contagem. Mais especificamente, o número de multiplicações para calcular a transformada continua relacionado ao número de componentes não-nulas com valores absolutos distintos na versão arredondada de $\mathbf{E}$ (componentes repetidas, simetrias à parte, também são consideradas), o número de adições pode ser obtido considerando os pré-cálculos que foram observados nesta seção e assim por diante.

3.1.5 Análise Comparativa

Nesta seção, são apresentados os números de multiplicações e adições necessárias para calcular a DFrFT proposta para vários valores de N e é realizada a comparação com os números requeridos por outros métodos. Além da complexidade envolvida no cálculo exato da transformada (sem arredondamento), foi considerado o envolvido na versão arredondada da transformada (cujo arredondamento em diferentes casas decimais é indicado). Também é considerado o cálculo de uma DFrFT baseada em autodecomposição pelo método direto, o método dado em (PEI; YEH, 2001)[6] e a proposta em (MAJORKOWSKA-MECH; CARIOW, 2017); este último método é, até então, o método com menor complexidade aritmética documentado na literatura.

Os referidos números são mostrados nas Tabelas 4 e 5. A complexidade multiplicativa do método proposto (sem arredondamento) é próxima da apresentada em (MAJORKOWSKA-

[6] O método dado em (PEI; YEH, 2001) é baseado no cálculo da DFrFT de comprimento N por meio do cálculo de uma transformada fracionária do cosseno e uma transformada fracionária do seno com comprimentos $N/2+1$ e $N/2-1$, respectivamente.

Tabela 4 – Número de multiplicações reais necessárias para o cálculo da DFrFT de N pontos utilizando diferentes abordagens (os números entre parênteses indicam a casa decimal em que foi realizado o arredondamento).

N	direto	PEI[1]	M-M[2]	proposto	proposto (arredondamento)
8	192	117	102	105	–
16	768	417	390	377	–
32	3.072	1.593	1.542	1.521	–
64	12.288	6.249	6.150	6.093	5.997 ($4^{\underline{a}}$) 5.625 ($3^{\underline{a}}$)
128	49.152	24.777	24.582	24.473	23.385 ($4^{\underline{a}}$) 19.749 ($3^{\underline{a}}$)
256	196.608	98.697	98.310	98.073	88.397 ($4^{\underline{a}}$) 59.297 ($3^{\underline{a}}$)
512	786.432	393.993	393.222	392.729	315.317 ($4^{\underline{a}}$) 139.653 ($3^{\underline{a}}$)

[1](PEI; YEH, 2001).

[2](MAJORKOWSKA-MECH; CARIOW, 2017).

Fonte: Produzido pelos autores.

MECH; CARIOW, 2017), sendo, em geral, um pouco menor. Por outro lado, a complexidade aditiva é reduzida para menos de metade da necessária em (MAJORKOWSKA-MECH; CARIOW, 2017). Em relação à transformada arredondada proposta, são apresentados nas tabelas os números para arredondamentos efetuados na quarta e terceira casas decimais apenas. A razão para isso é que, para valores altos de N, é observado que a mudança entre as diferenças relativas entre a complexidade multiplicativa associada ao arredondamento nessas duas casas decimais e a associada ao cálculo da transformada exata é mais perceptível. Por exemplo, o número de multiplicações da DFrFT arredondada proposta na quarta e terceira casas decimais respectivamente correspondem aproximadamente a 90% e 60% de M_{256}; para $N = 512$, os referidos números correspondem aproximadamente a 80% e 36% de M_{512}. Estas reduções são significativas, uma vez que o custo computacional de um algoritmo é normalmente concentrado na realização de operações de multiplicação. Também se verifica que o procedimento de arredondamento produz significativa redução na complexidade aditiva apenas se uma única casa decimal for preservada (até 90% de redução para $N = 512$). São mostradas nas Figuras 17a e 17b, as porcentagens que representam os números de multiplicações e adições necessárias para calcular a DFrFT arredondada, para arredondamento em diferentes casas decimais, em relação ao valor para o cálculo da transformada proposta sem arredondamento.

Tabela 5 – Número de adições reais necessárias para o cálculo da DFrFT de N pontos utilizando diferentes abordagens (os números entre parênteses indicam a casa decimal em que foi realizado o arredondamento).

N	direto	PEI[1]	M-M[2]	proposto	proposto (arredondamento)
8	432	279	270	131	–
16	1.760	987	990	455	–
32	7.104	3.747	3.774	1.691	–
64	28.544	14.643	14.718	6.459	6.395 ($4^{\underline{a}}$) 6.339 ($3^{\underline{a}}$)
128	114.432	57.939	58.110	25.211	24.531 ($4^{\underline{a}}$) 24.251 ($3^{\underline{a}}$)
256	458.240	230.547	230.910	99.579	95.199 ($4^{\underline{a}}$) 94.143 ($3^{\underline{a}}$)
512	1.833.984	919.827	920.574	395.771	372.967 ($4^{\underline{a}}$) 368.827 ($3^{\underline{a}}$)

[1](PEI; YEH, 2001).
[2](MAJORKOWSKA-MECH; CARIOW, 2017).

Fonte: Produzido pelos autores.

3.2 SIMULAÇÕES COMPUTACIONAIS

Nesta seção, são consideradas duas aplicações da DFrFT: filtragem e representação compacta de sinais no domínio fracionário de Fourier (DE OLIVEIRA NETO; LIMA, 2017; DE OLIVEIRA NETO; LIMA; PANARIO, 2018a; SERBES, 2017). O propósito desta seção é validar, por meio de simulações, o emprego da transformada considerada ao longo deste capítulo (incluindo a versão arredondada) em tais cenários; mais especificamente, a intenção é mostrar que é possível utilizar a DFrFT calculada com complexidade aritmética reduzida sem comprometimento de desempenho.

3.2.1 Filtragem no Domínio Fracionário

Para avaliar a aplicabilidade da DFrFT proposta no cenário de filtragem no domínio fracionário, é considerado o sinal Gaussiano

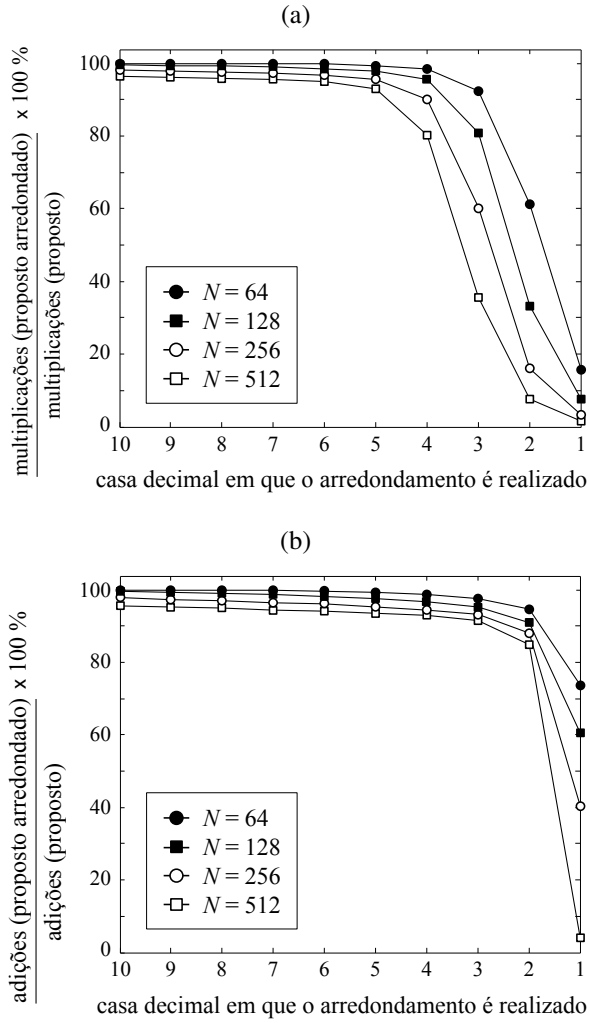
$$x(t) = e^{-\frac{(t-30)^2}{20}}, \quad 0 \leq t \leq 40,$$

ao qual o sinal *chirp*

$$c(t) = 0{,}1e^{i\left(\frac{t^2}{10}-2t\right)}$$

é adicionado. O sinal resultando é então amostrado com frequência $f_s = \frac{256}{40}$ Hz, produzindo um sinal de tempo discreto com $N = 256$ amostras. Após aplicar a DFrFT, é realizada a multiplicação por um filtro rejeita-faixa no domínio fracionário. Por fim, a DFrFT inversa correspondente é aplicada e a diferença entre o sinal reconstruído e a versão de tempo discreto de $x(t)$ é medida

Figura 17 – (a) Relação entre o número de multiplicações necessárias para o cálculo da DFrFT arredondada e a não arredondada propostas; (b) a mesma relação para o número de adições.



Fonte: Produzido pelos autores.

pela raiz quadrada do erro médio quadrático (RMSE, do inglês *root-mean-square error*). É usada como referência a DFrFT que utiliza a autobase HGL da DFT definida em (CANDAN; KUTAY; OZAKTAS, 2000), que é identificada como Candan-DFrFT e cujo cálculo pode ser realizado usando o algoritmo proposto em (MAJORKOWSKA-MECH; CARIOW, 2017), por exemplo. Poderiam ter sido escolhidos como referência, diferentes abordagens da DFrFT; contudo, embora tais escolhas poderiam trazer alguma melhoria na performance em termos de acurácia, a complexidade aritmética envolvida no cálculo da transformada, que é o aspecto que mais interessa a este trabalho, no melhor dos casos não mudaria. Também foi realizado o mesmo procedimento empregando a DFrFT proposta (versões exata e arredondada), cujo cálculo pode ser realizado com complexidade aritmética reduzida como explicado na Seção 3.1.

Na Figura 18a, é mostrado o sinal Gaussiano somado ao sinal *chirp*. Nas Figuras 18b

Tabela 6 – Filtragem no domínio fracionário de Fourier: RMSE e complexidade aritmética relacionada à reconstrução de um sinal Gaussiano de comprimento $N = 256$ após a remoção de um sinal aditivo *chirp* por meio de uma filtro rejeita-faixas.

DFrFT	RMSE*	Multiplicações ($\times 10^4$)	Adições ($\times 10^4$)
Candan-DFrFT	0,0170	9,8310	23,0910
proposta	0,0102	9,8073	9,9579
proposta (arred. $6^{\underline{a}}$)	0,0102	9,4793	9,6367
proposta (arred. $3^{\underline{a}}$)	0,0106	5,9297	9,4143

*Para servir de referência, o RMSE para o sinal antes da filtragem é 0,0873.
Fonte: Produzido pelos autores.

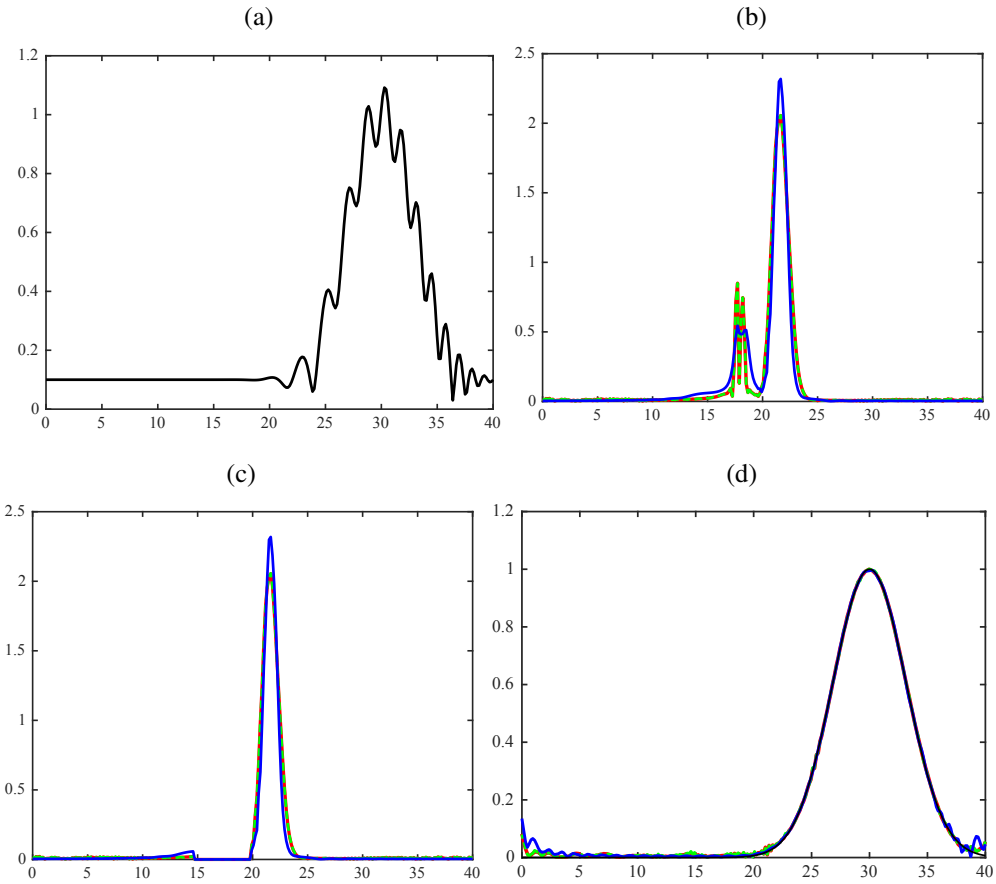
e Fig. 18c, são mostrados respectivamente os sinais no domínio fracionário antes e após a multiplicação por um filtro rejeita-faixa; além do resultado alcançado utilizando a Candan-DFrFT para $a = 3{,}100$, são mostrados nessas figuras os resultados obtidos para a DFrFT proposta, para $a = 3{,}088$, após o arredondamento na sexta e terceira casas decimais. A curva para a DFrFT proposta exata não é mostrada porque ela não é visualmente distinguível da DFrFT arredondada proposta na sexta casa decimal. Como mostrado na Figura 18d, a forma do sinal Gaussiano reconstruído é satisfatória para todos os casos. Esta conclusão é ratificada pelo cálculo do RMSE para cada uma das DFrFT utilizadas, que possuem valores claramente menores quando comparados com o valor do RMSE do sinal antes da filtragem (ver Tabela 6) e cujas diferenças parecem ser devido a menores ou maiores flutuações que ocorrem em intervalos em que o sinal recuperado deveria ser zero.

Na Tabela 6, também são dadas as complexidades aritméticas envolvidas no cálculo de cada uma das DFrFT comparadas. O primeiro ponto de destaque nos valores apresentados é o número de multiplicações necessárias para aplicar a filtragem usando a DFrFT arredondada proposta na terceira casa decimal, que é em torno de 40% menor que a requerida por todas as outras transformadas. Em segundo lugar, observa-se que o número de adições envolvidas no cálculo da DFrFT proposta (com e sem arredondamento) é menos da metade do que é necessário na abordagem do Candan quando calculada pelo algoritmo dado em (MAJORKOWSKA-MECH; CARIOW, 2017). Em resumo, conclui-se que a DFrFT proposta pode ser utilizada para filtragem do sinal em questão; este procedimento envolve menor complexidade aritmética do que as outras DFrFT baseadas em autodecomposição calculadas por meio do algoritmo dado em (MAJORKOWSKA-MECH; CARIOW, 2017).

3.2.2 Representação Compacta no Domínio Fracionário

Como segundo exemplo de aplicação, é considerada a representação do sinal em forma compacta no domínio fracionário, que tem sido útil na restauração de sinais (SERBES; DURAK-

Figura 18 – Sinal filtrado por meio da transformada fracionária discreta de Fourier: (a) domínio original; (b) domínio fracionário; (c) domínio fracionário após a filtragem rejeita-faixa; (d) domínio original após a filtragem rejeita-faixa. Preto: Gaussiana + *chirp* em (a), e sinal Gaussiano (d); azul: Candan-DFrFT (CANDAN; KUTAY; OZAKTAS, 2000); vermelho: DFrFT proposta (arredondada na $6^{\underline{a}}$ casa decimal); verde pontilhada: DFrFT proposta (arredondada na $3^{\underline{a}}$ casa decimal).



Fonte: Produzido pelos autores.

ATA, 2009), amostragem esparsa (BU et al., 2015), estimação de taxa *chirp* (ZHENG; SHI, 2010), e análise tempo-frequência (LU; XIAO; WEI, 2016; NGUYEN et al., 2017; SEJDIC; DJUROVIC; STANKOVIC, 2011), por exemplo. Aqui é revisitada a aplicação do método da menor norma (MNM, do inglês *minimum norm method*) proposto em (SERBES, 2017), que permite achar a ordem fracionária ótima $a_{\text{opt.}}$ que leva um sinal de interesse para um domínio fracionário de Fourier em que sua representação seja a mais compacta possível. Utiliza-se como medida de compactação a norma-ℓ_1; é adotada uma estratégia de busca de modo que o menor número possível de transformações precisem ser calculadas. A norma-ℓ_1 de um vetor $\mathbf{v} = [v(0), \ldots, v(N-1)]$ é definida em (SERBES, 2017) por:

$$||\mathbf{v}||_1 := \sum_{n=0}^{N-1} |v(n)|.$$

O sinal utilizado nos experimentos é o *chirp* de duas componentes dada por

$$s(t) = A_0 e^{i\pi(m_0 t^2 + 2f_0 t)} + A_1 e^{i\pi(m_1 t^2 + 2f_1 t)},$$

em que $m_0 = 0{,}1$ e $m_1 = 0{,}4$ são as *taxas de chirp*, $f_0 = 0{,}1$ e $f_1 = -0{,}1$ são as *frequências de deslocamento*, e $A_0 = 1$ e $A_1 = 1$ são as *amplitudes complexas*. O sinal $s(t)$ é amostrado para produzir o sinal de tempo discreto de comprimento $N = 512$. As configurações para a aplicação do MNM são as mesmas usadas na Seção III.A de (SERBES, 2017), então, 55 transformadas fracionárias de Fourier são calculadas até que se encontre a ordem fracionária ótima. Na Tabela 7, são mostrados os resultados do MNM aplicado em três diferentes modos:

i É usada a Candan-DFrFT (CANDAN; KUTAY; OZAKTAS, 2000);

ii É usada a DFrFT proposta;

iii É usada a DFrFT arredondada proposta (na terceira casa decimal) para realizar a busca e, uma vez que a ordem fracionária ótima é encontrada, a versão exata da mesma transformada é usada para calcular a transformada do sinal, tendo como objetivo assegurar uma melhor reconstrução do sinal.

Na tabela, observa-se que, embora as ordens fracionárias ótimas encontradas por meio do MNM são relativamente próximas entre si, a norma-ℓ_1 no domínio da DFrFT proposta (modos (ii) e (iii)) é menor que a no domínio da Candan-DFrFT (modo (i) acima); de qualquer forma, em todos os casos, o objetivo de representar o sinal de forma mais compacta foi claramente alcançado. Em particular, é notável o que fato que, mesmo quando a busca pela ordem fracionária ótima é realizada usando a transformada arredondada (modo (iii) acima), é encontrado um valor quase igual ao encontrado quando comparado com a respectiva transformada não arredondada (modo (ii) acima). Na Figura 19, em que a magnitude quadrática do sinal $s(t)$ é plotada para o sinal no domínio original e no domínio fracionário utilizando a ordem fracionária ótima encontrada, tem-se uma noção visual do resultado alcançado.

Uma vez que a DFrFT considerada no modo (i) pode ser calculada usando o algoritmo dado em (MAJORKOWSKA-MECH; CARIOW, 2017), o número correspondente ao total de multiplicações e adições envolvidas na aplicação do MNM pode ser calculado, para $N = 512$, usando as Tabelas 4 e 5. Tais números são respectivamente dados por

$$55 \times 393.222 \approx 2{,}1627 \times 10^7$$

e

$$55 \times 920.574 \approx 5{,}0631 \times 10^7.$$

Diferentemente da transformada empregada no modo (i), a DFrFT proposta usada nos modos (ii) e (iii) permite pré-calcular o produto entre $\mathbf{E}^T$ (ou sua versão arredondada) e o sinal a ser transformado, como em (3.2), e para cada ordem fracionária avaliada durante o processo de busca são

Tabela 7 – Aplicação do método da norma mínima para o sinal *chirp* bi-componente usando (i) Candan-DFrFT (CANDAN; KUTAY; OZAKTAS, 2000) calculada pelo algoritmo dado em (MAJORKOWSKA-MECH; CARIOW, 2017), (ii) DFrFT proposta não arredondada e (iii) uma combinação entre a DFrFT proposta com e sem arredondamento (o arredondamento foi realizado na terceira casa decimal).

Modo	$a_{\text{opt.}}$	Norma-ℓ_1^*	Multiplicações $(\times 10^7)$	Adições $(\times 10^7)$
(i)	1,1861	377,9506	2,1627	5,0631
(ii)	1,1141	317,7685	1,1037	1,1151
(iii)	1,1185	317,7684	0,4344	1,0792

*Como referência, a norma-ℓ_1 do sinal no domínio original (tempo) é 681,3125.

Fonte: Produzido pelos autores.

necessárias novas operações aritméticas apenas no cálculo dos produtos matriz-vetor (3.3) e (3.4). Esta estratégia provê uma economia de aproximadamente metade das multiplicações e adições contada na Seção 3.1.4. Mais especificamente, com base nas explicações dadas e considerando os termos nos somatórios em (3.8) e (3.12), são obtidos os números de multiplicações e adições aplicando o MNM no modo (ii) respectivamente como

$$195.598 + 55 \times 197.131 \approx 1{,}1037 \times 10^7$$

e

$$196.608 + 55 \times 199.163 \approx 1{,}1151 \times 10^7.$$

De forma análoga, o MNM aplicado no modo (iii) requer

$$69.060 + 55 \times 70.593 + 392.729 \approx 4{,}3444 \times 10^6$$

multiplicações e

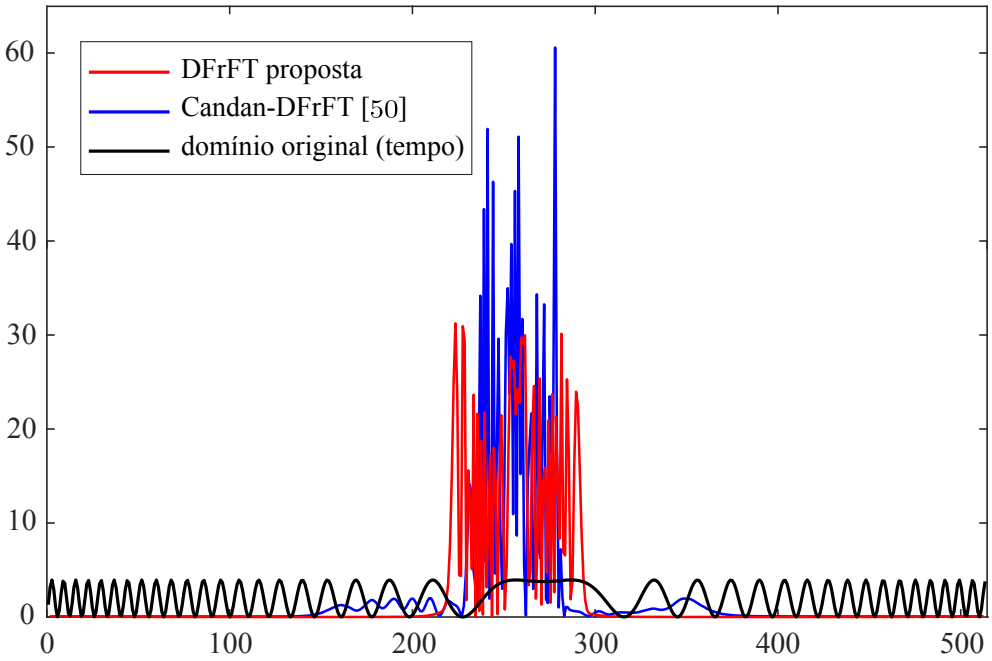
$$183.136 + 55 \times 185.691 + 395.771 \approx 1{,}0792 \times 10^7$$

adições. A partir dos resultados mostrados acima, que também são mostrados na Tabela 7, conclui-se que cerca de 50% das multiplicações e 78% das adições são economizadas, se o MNM for aplicado no modo (ii) ao invés do modo (i); se o modo (iii) for usado, comparando com o modo (i), cerca de 80% das multiplicações e 79% das adições são salvas. Isso sugere que a DFrFT arredondada proposta pode ser utilizada durante a busca da ordem fracionária ótima no MNM, provendo benefícios significativos do ponto de vista de complexidade computacional e velocidade.

3.3 CONSIDERAÇÕES

Neste capítulo, foi introduzido um método para cálculo eficiente de uma transformada fracionária discreta de Fourier baseada na autodecomposição do operador da transformada de

Figura 19 – Magnitude quadrática do sinal *chirp* bi-componente no domínio original (tempo) e no domínio fracionário utilizando o método da menor norma.



Fonte: Produzido pelos autores.

Fourier ordinária. Esta abordagem provê uma significativa redução na complexidade aritmética, quando comparada com outros métodos do estado-da-arte, sendo aplicável em determinados cenários práticos. Foi demonstrado que a transformada proposta pode ser aplicada empregando uma estratégia de arredondamento das componentes dos autovetores do tipo Hemite-Gaussiano usados para definir a transformada, permitindo uma economia de 50% a 80% no número de multiplicações e adições envolvidas no referido cálculo, ao mesmo tempo em que um desempenho satisfatório é mantido.

4 AUTOVETORES DO TIPO HERMITE-GAUSSIANO DA TRANSFORMADA NUMÉRICA DE FOURIER A PARTIR DE MATRIZES GERADORAS

A transformada numérica de Fourier (FNT, do inglês *Fourier number transform*) tem sido vastamente estudada nas últimas décadas. Aplicações que envolvem esta transformada incluem cálculo rápido de convoluções sem erros de arredondamento, cifragem de imagem, comunicação multiusuário, códigos corretores de erro e processamento de sinais no domínio cifrado (AGARWAL; BURRUS, 1974; RUBANOV et al., 1998; BOUSSAKTA; HOLT, 1999; SONG et al., 2014b; TOIVONEN; HEIKKILA, 2006; LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; ZHAO et al., 2016a; PEDROUZO-ULLOA; TRONCOSO-PASTORIZA; PÉREZ-GONZÁLEZ, 2017). Mais recentemente, transformadas numéricas fracionárias de Fourier (FrFNT, do inglês *fractional Fourier number transform*) têm sido apresentadas na literatura (PEI; WEN; DING, 2011; LIMA; CAMPELLO DE SOUZA, 2012; LIMA; CAMPELLO DE SOUZA, 2016; LIMA; LIMA; CAMPELLO DE SOUZA, 2017). Assim como ocorre com as transformadas fracionárias definidas sobre o corpo dos complexos ou dos reais, a FrFNT é normalmente baseada na expansão espectral da matriz da transformada ordinária correspondente. Seja $\mathbf{F}$ a matriz da FNT, a sua expansão espectral é dada por

$$\mathbf{F} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^T,$$

em que $\mathbf{E}$ é uma matriz quadrada cujas colunas são formadas por um conjunto ortonormal de autovetores de $\mathbf{F}$ e seus respectivos autovalores estão dispostos na matriz diagonal $\mathbf{\Lambda}$. A autoestrutura da FNT é análoga à da DFT (BIRTWISTLE, 1982; MCCLELLAN; PARKS, 1972); seus autovalores são $\{1, -1, i, -i\}$, em que $i^2 \equiv -1 \pmod{p}$, em que p é um primo ímpar, e as multiplicidades dos autovalores dependem do valor de N como mostrado na Tabela 8. A matriz da FrFNT pode ser obtida então como

$$\mathbf{F}^a = \mathbf{E}\mathbf{\Lambda}^a\mathbf{E}^T, \tag{4.1}$$

em que a *ordem fracionária* é denotada por $a = \frac{a_1}{a_2}$, em que $a_1 \in \mathbb{Z}$ e $a_2 \in \mathbb{Z}^*$.

Tabela 8 – Multiplicidade dos autovetores da matriz da FNT $N \times N$.

N	$\#\{1\}$	$\#\{-i\}$	$\#\{-1\}$	$\#\{i\}$
$4L$	$L+1$	L	L	$L-1$
$4L+1$	$L+1$	L	L	L
$4L+2$	$L+1$	L	$L+1$	L
$4L+3$	$L+1$	$L+1$	$L+1$	L

Fonte: (BIRTWISTLE, 1982)

Existem diferentes formas de construir um conjunto ortonormal de autovetores da FNT para ser usado como colunas da matriz $\mathbf{E}$ (PEI; WEN; DING, 2011; LIMA; CAMPELLO DE SOUZA, 2012; LIMA; CAMPELLO DE SOUZA, 2016). Normalmente, estes métodos são extensões para corpos finitos de abordagens primeiramente apresentadas no corpo dos reais (PEI; WEN; DING, 2008; CANDAN; KUTAY; OZAKTAS, 2000; KUZNETSOV, 2015). Em particular, Lima e Campello de Souza apresentaram um método para construção de autovetores do tipo Hermite-Gaussiano (HGL) da FNT a partir de fórmulas fechadas (LIMA; CAMPELLO DE SOUZA, 2016). O trabalho é a contraparte em corpos finitos da abordagem apresentada em (KUZNETSOV, 2015). A partir de combinações lineares de vetores Gaussianos dilatados, o método produz autovetores HGL da FNT que podem ser dispostos numa ordem específica como colunas da matriz E. Deste modo, esta abordagem evita ambiguidades e gera uma base única de autovetores da FNT que é usada para definir a FrFNT e empregada pelos autores em um sistema de cifragem de imagens.

Em (PEI; CHANG, 2009), Pei e Chang propõem um método de matrizes geradoras para construção de autovetores da DFT. Em (PEI; CHANG, 2016), o método de matrizes geradoras é utilizado para construir autovetores HGL da DFT utilizando uma matriz geradora específica. No Capítulo 2, são removidas algumas restrições da metodologia apresentada em (PEI; CHANG, 2016) e são apresentados dois métodos para construção de uma base de autovetores HGL da DFT (DE OLIVEIRA NETO; LIMA, 2017; DE OLIVEIRA NETO; LIMA; PANARIO, 2018a).

Neste capítulo, é apresentado o método das matrizes geradoras para construção de autovetores da FNT e indicado como escolher alguns de seus parâmetros para obter-se uma base de autovetores do tipo Hermite-Gaussiano. Além do mais, é mostrado que essa base coincide com o conjunto obtido em (LIMA; CAMPELLO DE SOUZA, 2016). Utilizando a abordagem descrita neste capítulo, este conjunto pode ser gerado a partir de apenas quatro vetores *sementes* e dispensa a computação prévia dos vetores Gaussianos dilatados mencionados anteriormente.

Após essa introdução, na Seção 4.1, são apresentadas algumas definições matemáticas necessárias para o entendimento do método proposto. Nas Seções 4.2, 4.3 e 4.4 são dadas as principais contribuições deste capítulo, como elencado a seguir.

i Na Seção 4.2.1, o método de construção de autovetores da FNT a partir de matrizes geradoras é apresentado;

ii Na Seção 4.2.2, é apresentado um novo algoritmo para construção da base proposta em (LIMA; CAMPELLO DE SOUZA, 2016).

iii Na Seção 4.3, é mostrado um exemplo específico para ilustrar a construção da base a partir de matrizes geradoras; é usada essa base na definição da FrFNT.

iv Na Seção 4.4, são discutidos aspectos relevantes do método proposto comparando com as outras técnicas encontradas na literatura.

v Na Seção 4.5, é apresentado um resumo do capítulo.

4.1 PRELIMINARES MATEMÁTICAS

Nesta seção, são dadas algumas definições matemáticas que são necessárias ao longo deste capítulo.

4.1.1 Transformada numérica de Fourier centralizada

Neste trabalho, foi considerada a versão centralizada da transformada numérica de Fourier.

Definição 4.1. Seja $\mathbf{x}$ uma sequência de N pontos, cujas componentes $x(n)$ estão em um corpo finito $\mathbb{F}_p$, em que p é um primo ímpar; a **transformada numérica de Fourier** de $\mathbf{x}$ é calculada módulo p por

$$X(k) := \frac{1}{\sqrt{N}} \sum_{n \in I_N} x(n)\alpha^{-nk}\,, \quad k \in I_N\,, \tag{4.2}$$

em que $\alpha \in \mathbb{F}_p$ é um elemento com ordem multiplicativa denotada por $\mathrm{ord}(\alpha) = N$, $\mathbf{X}$ é uma sequência de N-pontos cujas as componentes $X(k)$ estão sobre $\mathbb{F}_p$ e $I_N := \{-M+1, -M+2, \cdots, -M+N\}$, $M = \left\lfloor \frac{N+1}{2} \right\rfloor$.

4.1.2 Funções trigonométricas sobre corpos finitos

Definição 4.2. Seja $\zeta \in \mathbb{F}_p$ um elemento com ordem multiplicativa $\mathrm{ord}(\zeta) = N$. O seno e o cosseno sobre corpos finitos de um arco relacionado com ζ são computados módulo p, respectivamente, por

$$\mathrm{sen}_\zeta(x) := \frac{\zeta^x - \zeta^{-x}}{2i} \quad \text{e} \quad \cos_\zeta(x) := \frac{\zeta^x + \zeta^{-x}}{2}, \tag{4.3}$$

em que $x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$ e $i^2 \equiv -1 (\mathrm{mod}\ p)$ (CAMPELLO DE SOUZA et al., 1998b; LIMA; CAMPELLO DE SOUZA; PANARIO, 2011).

4.1.3 Autovetores do tipo Hermite-Gaussiano da transformada numérica de Fourier a partir de fórmulas fechadas

Nesta seção, são sumarizadas algumas contribuições de (LIMA; CAMPELLO DE SOUZA, 2016). Utilizando as funções trigonométricas mostradas na Definição 4.2, os autores definiram a sequência S_ζ como a seguir.

Definição 4.3. Seja $\alpha \in \mathbb{F}_p$ um elemento com ord$(\alpha) = N$, $\zeta = \sqrt{\alpha}$ e ord$(\zeta) = 2N$. A sequência $S_\zeta(k)$ é definida por $S_\zeta(0) := 1$ e

$$S_\zeta(k) := \prod_{n=1}^{k} 2\,\text{sen}_\zeta(n), \quad k > 1. \tag{4.4}$$

Proposição 4.1. *(LIMA; CAMPELLO DE SOUZA, 2016) A sequência $S_\zeta(k)$ satisfaz as seguintes propriedades:*

(i) $S_\zeta(k) = 0$, *para* $k \geq N$;

(ii) $S_\zeta(k)S_\zeta(N-k-1) = N$, *para* $0 \leq k \leq N-1$.

Além disso, em (LIMA; CAMPELLO DE SOUZA, 2016), descreve-se como construir os conjuntos de vetores $\mathbf{u}$ e $\mathbf{v}$ a partir da sequência S_ζ para todos os valores de N. Como ilustração, são mostrados a seguir as expressões para $N = 4L + 1$.

Teorema 4.1. *(LIMA; CAMPELLO DE SOUZA, 2016) Para $N = 4L + 1$, os vetores com simetria par $\{\mathbf{u}_n\}_{-L\leq n\leq L}$ e os vetores com simetria ímpar $\{\mathbf{v}_n\}_{-L\leq n\leq L-1}$ são construídos como:*

1. $u_n(k) := S_\zeta(3L+n+k)S_\zeta(3L+n-k)$, $k \in I_N$. *Estes vetores formam um conjunto linearmente independente e satisfazem*

$$\mathbf{F}\mathbf{u}_j = \mathbf{U}_j = N^{-1/2}S_\zeta(2L+2j)\mathbf{u}_{-j}. \tag{4.5}$$

2. $v_n(k) := sen_\zeta(2k)S_\zeta(3L+n+k)S_\zeta(3L+n-k)$, $k \in I_N$. *Estes vetores formam um conjunto linearmente independente e satisfazem*

$$\mathbf{F}\mathbf{v}_j = \mathbf{V}_j = -iN^{-1/2}S_\zeta(2L+2j+1)\mathbf{v}_{-j-1}. \tag{4.6}$$

combina-se linearmente esses vetores com suas FNT, construindo a base indicada a seguir.

Corolário 4.1. *(LIMA; CAMPELLO DE SOUZA, 2016) Os N vetores*

$$\begin{aligned}
&\mathbf{w}_n = \mathbf{u}_n + \mathbf{U}_n, && 0 \leq n \leq L,\\
&\mathbf{x}_n = \mathbf{v}_n + i\mathbf{V}_n, && 0 \leq n \leq L-1,\\
&\mathbf{y}_n = -\mathbf{u}_{n+1} + \mathbf{U}_{n+1}, && 0 \leq n \leq L-1 \quad e\\
&\mathbf{z}_n = -\mathbf{v}_n + i\mathbf{V}_n, && 0 \leq n \leq L-1,
\end{aligned}$$

formam uma base de autovetores da FNT.

Uma base ortonormal é construída aplicando o algoritmo de Gram-Schmidt aos conjuntos $\{\mathbf{w}_n\}_{0\leq n\leq L}$, $\{\mathbf{x}_n\}_{0\leq n\leq L-1}$, $\{\mathbf{y}_n\}_{0\leq n\leq L-1}$ e $\{\mathbf{z}_n\}_{0\leq n\leq L-1}$, formando os conjuntos $\{\mathbf{w}_n^{\perp}\}_{0\leq n\leq L}$, $\{\mathbf{x}_n^{\perp}\}_{0\leq n\leq L-1}$, $\{\mathbf{y}_n^{\perp}\}_{0\leq n\leq L-1}$ e $\{\mathbf{z}_n^{\perp}\}_{0\leq n\leq L-1}$. Estes vetores são organizados como $\Phi_{4n} = \mathbf{w}_n^{\perp}$, $0 \leq n \leq L$, $\Phi_{4n+1} = \mathbf{x}_n^{\perp}$, $0 \leq n \leq L-1$, $\Phi_{4n+2} = \mathbf{y}_n^{\perp}$, $0 \leq n \leq L-1$, e $\Phi_{4n+3} = \mathbf{z}_n^{\perp}$, $0 \leq n \leq L-1$, produzindo a base ortonormal de autovetores da FNT $\{\Phi_m^{\perp}\}_{0\leq m\leq N-1}$.

Embora neste texto apenas estejam transcritas as expressões para $N = 4L+1$, os autores de (LIMA; CAMPELLO DE SOUZA, 2016) mostram no artigo o procedimento para construção da base para todos os valores de N. Como esta abordagem é uma extensão do método descrito em (KUZNETSOV, 2015), eles nomearam estes vetores como autovetores HGL da FNT.

4.2 AUTOBASE DA TRANSFORMADA NUMÉRICA DE FOURIER A PARTIR DE MATRIZES GERADORAS

Nesta seção, é apresentada a principal contribuição deste capítulo.

4.2.1 Matrizes para geração de autovetores da FNT

A seguir, é introduzido o conceito de *matrizes geradoras* para construção de autovetores da FNT. Este método é uma extensão para corpos finitos do algoritmo descrito em (PEI; CHANG, 2009) para construção de autovetores da DFT.

Seja $\mathbf{F}$ a matriz da FNT de N pontos e $\mathbf{A}$ uma matriz quadrada $N \times N$ que satisfaz $\mathbf{F}^2\mathbf{A}\mathbf{F}^2 = \gamma\mathbf{A}$, em que γ é uma constante. A *matriz geradora* $\mathbf{S_A}$ é definida como

$$\mathbf{S_A} = \gamma^{\frac{1}{2}}\mathbf{F}^{-1}\mathbf{A}\mathbf{F} + \mathbf{A} \tag{4.7}$$

e satisfaz a seguinte propriedade:

Proposição 4.2. *Se* $\mathbf{x}$ *é um autovetor da FNT com autovalor* $\lambda_{\mathbf{x}}$*, então* $\mathbf{x}' = \mathbf{S_A}\mathbf{x}$ *também é um autovetor da FNT com autovalor* $\lambda_{\mathbf{x}'} = \gamma^{\frac{1}{2}}\lambda_{\mathbf{x}}$.

Prova. *Desde que* $\mathbf{F}^4$ *é a matriz identidade, tem-se o seguinte desenvolvimento:*

$$\begin{aligned}
\mathbf{F}\mathbf{x}' &= \mathbf{F}(\mathbf{S_A}\mathbf{x}) \\
&= \mathbf{F}(\gamma^{\frac{1}{2}}\mathbf{F}^{-1}\mathbf{A}\mathbf{F} + \mathbf{A})\mathbf{x} \\
&= (\gamma^{\frac{1}{2}}\mathbf{A}\mathbf{F} + \mathbf{F}\mathbf{A})\mathbf{x} = (\gamma^{\frac{1}{2}}\mathbf{A}\mathbf{F} + \mathbf{F}^{-1}\mathbf{F}^2\mathbf{A}\mathbf{F}^4)\mathbf{x} \\
&= (\gamma^{\frac{1}{2}}\mathbf{A}\mathbf{F} + \mathbf{F}^{-1}\gamma\mathbf{A}\mathbf{F}^2)\mathbf{x} = (\gamma^{\frac{1}{2}}\mathbf{A} + \mathbf{F}^{-1}\gamma\mathbf{A}\mathbf{F})\mathbf{F}\mathbf{x} \\
&= \gamma^{\frac{1}{2}}(\mathbf{A} + \gamma^{\frac{1}{2}}\mathbf{F}^{-1}\mathbf{A}\mathbf{F})\mathbf{F}\mathbf{x} = \gamma^{\frac{1}{2}}\mathbf{S_A}\lambda_{\mathbf{x}}\mathbf{x} \\
&= \gamma^{\frac{1}{2}}\lambda_{\mathbf{x}}\mathbf{x}'.
\end{aligned}$$

■

Isto é, a partir de autovetores *sementes*, constrói-se outros autovetores com autovalores conhecidos. Na seção seguinte, é descrito como construir uma autobase HGL ortogonal da FNT utilizando uma matriz geradora específica.

4.2.2 Base de autovetores HGL da FNT a partir de matrizes geradoras

Seja $\mathbf{C}$ a matriz diagonal cujo elemento na $(k+M)$-ésima linha e na $(k+M)$-ésima coluna é dado por $2\cos_\alpha(k)$, $k \in I_N$, em que $\alpha \in \mathbb{F}_p$ tem ordem multiplicativa $\text{ord}(\alpha) = N$ e $I_N := \{-M+1, -M+2, \ldots, -M+N\}$, $M = \left\lfloor \frac{N+1}{2} \right\rfloor$. Desde que $\mathbf{C}$ satisfaz $\mathbf{F}^2\mathbf{C}\mathbf{F}^2 = \mathbf{C}$, $\mathbf{S_C} = \mathbf{F}^{-1}\mathbf{C}\mathbf{F} + \mathbf{C}$ é a matriz geradora dada por

$$\mathbf{S_C} = \begin{bmatrix} 2\cos_\alpha(-M+1) & 1 & 0 & \cdots & 1 \\ 1 & 2\cos_\alpha(-M+2) & 1 & \cdots & 0 \\ 0 & 1 & 2\cos_\alpha(-M+3) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 2\cos_\alpha(-M+N) \end{bmatrix},$$

em que $M = \left\lfloor \frac{N+1}{2} \right\rfloor$.

Definição 4.4. Seja $\{\mathbf{g}_0 = \mathbf{w}_0, \mathbf{g}_1 = \mathbf{x}_0, \mathbf{g}_2 = \mathbf{y}_0, \mathbf{g}_3 = \mathbf{z}_0\}$ uma conjunto de vetores semente. O conjunto $\{\mathbf{g}_m\}_{0 \le m \le N-1}$ de autovetores HGL da transformada numérica de Fourier é construído aplicando recursivamente a matriz geradora $\mathbf{S_C}$ como se segue:

$$\begin{aligned} \mathbf{g}_{4n} &= \mathbf{S_C}\mathbf{g}_{4(n-1)}, \quad n = 1, 2, \ldots, \#\{1\} - 1, \\ \mathbf{g}_{4n+1} &= \mathbf{S_C}\mathbf{g}_{4(n-1)+1}, \quad n = 1, 2, \ldots, \#\{-i\} - 1, \\ \mathbf{g}_{4n+2} &= \mathbf{S_C}\mathbf{g}_{4(n-1)+2}, \quad n = 1, 2, \ldots, \#\{-1\} - 1, \\ \mathbf{g}_{4n+3} &= \mathbf{S_C}\mathbf{g}_{4(n-1)+3}, \quad n = 1, 2, \ldots, \#\{i\} - 1, \end{aligned}$$

em que $\#\{1\}$, $\#\{-i\}$, $\#\{-1\}$ e $\#\{i\}$ são as multiplicidades dos autovetores 1, $-i$, -1 e i, respectivamente, como mostrado na Tabela 8.

Teorema 4.2. *O conjunto $\{\mathbf{g}_m^\perp\}_{0 \le m \le N-1}$ obtido aplicando o algoritmo de Gram-Schmidt a cada um dos subconjuntos construídos usando a Definição 4.4 é uma versão escalonada do conjunto $\{\phi_m^\perp\}_{0 \le m \le N-1}$ proposto em (LIMA; CAMPELLO DE SOUZA, 2016).*

A prova do Teorema 4.2 requer alguns lemas descritos a seguir. A prova se desenvolve mostrando-se que é possível escrever os vetores construídos utilizando o algoritmo proposto na Definição 4.4 como uma combinação linear dos vetores dos conjuntos $\{\mathbf{w}_n\}_{0 \le n \le (\#\{1\}-1)}$, $\{\mathbf{x}_n\}_{0 \le n \le (\#\{-i\}-1)}$, $\{\mathbf{y}_n\}_{0 \le n \le (\#\{-1\}-1)}$ e $\{\mathbf{z}_n\}_{0 \le n \le (\#\{i\}-1)}$. De fato, apenas a prova para $N = 4L+1$ é apresentada, uma vez que a prova para os demais valores de N segue os mesmos passos.

Primeiramente, os vetores do conjunto $\{\mathbf{g}_n\}_{0\leq n\leq N-1}$ são renomeados para

$$\begin{aligned}
\{\mathbf{w}_n^{'}\}_{0\leq n\leq(\#\{1\}-1)} &= \{\mathbf{g}_{4n}\}_{0\leq n\leq(\#\{1\}-1)},\\
\{\mathbf{x}_n^{'}\}_{0\leq n\leq(\#\{-i\}-1)} &= \{\mathbf{g}_{4n+1}\}_{0\leq n\leq(\#\{-i\}-1)},\\
\{\mathbf{y}_n^{'}\}_{0\leq n\leq(\#\{-1\}-1)} &= \{\mathbf{g}_{4n+2}\}_{0\leq n\leq(\#\{-1\}-1)},\\
\{\mathbf{z}_n^{'}\}_{0\leq n\leq(\#\{i\}-1)} &= \{\mathbf{g}_{4n+3}\}_{0\leq n\leq(\#\{i\}-1)}.
\end{aligned}$$

Além do mais, os seguintes resultados são necessários:

Lema 4.1. *Os vetores do conjunto* $\{\mathbf{g}_m\}_{0\leq m\leq N-1}$ *podem ser escritos em função da matriz* $\mathbf{C}$ *de acordo com*

$$\begin{aligned}
\mathbf{w}'_n &= \mathbf{C}\mathbf{w}'_{n-1} + \mathbf{F}\mathbf{C}\mathbf{w}'_{n-1},\\
\mathbf{x}'_n &= \mathbf{C}\mathbf{x}'_{n-1} + i\mathbf{F}\mathbf{C}\mathbf{x}'_{n-1},\\
\mathbf{y}'_n &= \mathbf{C}\mathbf{y}'_{n-1} - \mathbf{F}\mathbf{C}\mathbf{y}'_{n-1},\\
\mathbf{z}'_n &= \mathbf{C}\mathbf{z}'_{n-1} - i\mathbf{F}\mathbf{C}\mathbf{z}'_{n-1}.
\end{aligned}$$

Prova. *Desde que* $\mathbf{w}'_n$ *é um autovetor da FNT com autovalor* $\lambda_{\mathbf{w}'_n} = 1$*, tem-se*

$$\begin{aligned}
\mathbf{w}'_n &= \mathbf{S}_{\mathbf{C}}\mathbf{w}'_{n-1} = \mathbf{F}^{-1}\mathbf{C}\mathbf{F}\mathbf{w}'_{n-1} + \mathbf{C}\mathbf{w}'_{n-1},\\
\mathbf{F}\mathbf{w}'_n &= \mathbf{F}(\mathbf{F}^{-1}\mathbf{C}\mathbf{F}\mathbf{w}'_{n-1} + \mathbf{C}\mathbf{w}'_{n-1}) = \mathbf{C}\mathbf{F}\mathbf{w}'_{n-1} + \mathbf{F}\mathbf{C}\mathbf{w}'_{n-1},\\
\lambda_{\mathbf{w}'_n}\mathbf{w}'_n &= \mathbf{C}\lambda_{\mathbf{w}'_{n-1}}\mathbf{w}'_{n-1} + \mathbf{F}\mathbf{C}\mathbf{w}'_{n-1},\\
\mathbf{w}'_n &= \mathbf{C}\mathbf{w}'_{n-1} + \mathbf{F}\mathbf{C}\mathbf{w}'_{n-1}.
\end{aligned}$$

A prova para $\mathbf{x}'_n$*,* $\mathbf{y}'_n$ *e* $\mathbf{z}'_n$ *segue os mesmos passos.* ■

Da definição dos vetores $\mathbf{u}_n$ e $\mathbf{v}_n$ no Teorema 4.1, pode-se renomear d_n e δ_n como

$$d_n = N^{-\frac{1}{2}}S_\zeta(2L+2n), \tag{4.8}$$

$$\delta_n = N^{-\frac{1}{2}}S_\zeta(2L+2n+1). \tag{4.9}$$

Proposição 4.3. *Para* $0\leq n\leq 2L$*,* d_n *satisfaz,*

(i) $d_n d_{-n} = 1$*,*

(ii) $d_0 = 1$.

Prova. *Utilizando a Propriedade 4.1(ii) da sequência S_ζ, isso é, $S_\zeta(k)S_\zeta(N-k-1)=N$, tem-se*

(i) Para $0 \leq n \leq 2L$, usando (4.8):

$$d_n d_{-n} = N^{-\frac{1}{2}} S_\zeta(2L+2n) N^{-\frac{1}{2}} S_\zeta(2L-2n) = N^{-1} S_\zeta(2L+2n) S_\zeta(2L-2n).$$

Aplicando a substituição $k = 2L+2n$, tem-se

$$d_n d_{-n} = N^{-1} S_\zeta(k) S_\zeta(N-k-1) = N^{-1} N = 1.$$

(ii) Para $0 \leq n \leq 2L$, usando a Propriedade 4.1(ii), $S_\zeta(k)S_\zeta(N-k-1)=N$, e aplicando a substituição $k = 2L$,

$$S_\zeta(2L) S_\zeta(2L) = N, \quad S_\zeta(2L) = N^{\frac{1}{2}}.$$

Então, $d_0 = N^{-\frac{1}{2}} S_\zeta(2L) = N^{-\frac{1}{2}} N^{\frac{1}{2}} = 1$.

■

Por outro lado, δ_n definido em (4.9) satisfaz a seguinte propriedade:

Proposição 4.4. *Para $0 \leq n \leq 2L$, $\delta_n \delta_{-n-1} = 1$.*

Prova. *Considerando-se o desenvolvimento a seguir:*

$$\begin{aligned} \delta_n \delta_{-n-1} &= N^{-\frac{1}{2}} S_\zeta(2L+2n+1) N^{-\frac{1}{2}} S_\zeta(2L-2n-2+1) \\ &= N^{-1} S_\zeta(2L+2n+1) S_\zeta(2L-2n-1). \end{aligned}$$

Daí, aplica-se a substituição $k = 2L+2n+1$, obtendo-se como resultado

$$\delta_n \delta_{-n-1} = N^{-1} S_\zeta(k) S_\zeta(N-k-1) = N^{-1} N = 1.$$

■

Substituindo (4.8) e (4.9) nas expressões para $\mathbf{w}_n$, $\mathbf{x}_n$, $\mathbf{y}_n$ e $\mathbf{z}_n$, tem-se

$$\begin{aligned} \mathbf{w}_n &= \mathbf{u}_n + d_n \mathbf{u}_{-n}, \\ \mathbf{x}_n &= \mathbf{v}_n + \delta_n \mathbf{v}_{-n-1}, \\ \mathbf{y}_n &= -\mathbf{u}_{n+1} + d_n \mathbf{u}_{-n-1}, \\ \mathbf{z}_n &= -\mathbf{v}_n + \delta_n \mathbf{v}_{-n-1}. \end{aligned}$$

Utilizando o Teorema 4.1, escreve-se $\mathbf{u}_n$ como uma função de $\mathbf{u}_{n-1}$, uma vez que $u_n(k)$ satisfaz

$$\begin{aligned}
&S_\zeta(3L+n+k)S_\zeta(3L+n-k) = \\
&= 2\text{sen}_\zeta\,(3L+n+k)\,2\text{sen}_\zeta\,(3L+n-k)\,S_\zeta(3L+n-1+k)S_\zeta(3L+n-1-k) \\
&= 2\text{sen}_\zeta\,(3L+n+k)\,2\text{sen}_\zeta\,(3L+n-k)\,u_{n-1}(k) \\
&= (2\cos_\zeta\,(2k) - 2\cos_\zeta\,(2(3L+n)))\,u_{n-1}(k).
\end{aligned}$$

Renomeando $C(k) = 2\cos_\zeta\,(2k) = 2\cos_\alpha\,(k)$ e $c_n = 2\cos_\zeta\,(2(3L+n)) = 2\cos_\alpha\,(3L+n)$, pode-se escrever $\mathbf{u}_n$ como uma função de $\mathbf{u}_{n-1}$,

$$u_n(k) = [C(k) - c_n]u_{n-1}(k) \quad \text{e} \quad C(k)u_{n-1}(k) = u_n(k) + c_n u_{n-1}(k).$$

Um argumento similar também se aplica para $v_n(k)$; escrevendo as expressões na forma vetorial, obtém-se para $\mathbf{u}_n$ e $\mathbf{v}_n$

$$\mathbf{C}\mathbf{u}_{n-1} = \mathbf{u}_n + c_n\mathbf{u}_{n-1}, \quad \mathbf{C}\mathbf{v}_{n-1} = \mathbf{v}_n + c_n\mathbf{v}_{n-1}. \tag{4.10}$$

A partir daqui, será descrito como escrever $\mathbf{w}_n^{'}$ como função do conjunto $\{\mathbf{w}_j\}_{0\leq j\leq n}$. Primeiramente, usa-se o Lema 4.1 para mostrar o caso $n = 1$:

$$\mathbf{w}_1^{'} = \mathbf{C}\mathbf{w}_0^{'} + \mathbf{F}\mathbf{C}\mathbf{w}_0^{'}.$$

Desde que $\mathbf{w}_0^{'} = \mathbf{w}_0$, tem-se

$$\mathbf{w}_1' = \mathbf{C}\mathbf{w}_0 + \mathbf{F}\mathbf{C}\mathbf{w}_0 = \mathbf{C}(\mathbf{u}_0 + d_0\mathbf{u}_0) + \mathbf{F}\mathbf{C}(\mathbf{u}_0 + d_0\mathbf{u}_0).$$

Utilizando as Propriedades 4.3*(i)* e 4.3*(ii)* e aplicando (4.10), tem-se

$$\begin{aligned}
\mathbf{w}_1' &= 2(\mathbf{C}\mathbf{u}_0 + \mathbf{F}\mathbf{C}\mathbf{u}_0) \\
&= 2[(\mathbf{u}_1 + c_1\mathbf{u}_0) + \mathbf{F}(\mathbf{u}_1 + c_1\mathbf{u}_0)] = 2[(\mathbf{u}_1 + c_1\mathbf{u}_0) + (d_1\mathbf{u}_{-1} + c_1d_0\mathbf{u}_0)] \\
&= 2[(\mathbf{u}_1 + d_1\mathbf{u}_{-1}) + (c_1\mathbf{u}_0 + c_1d_0\mathbf{u}_0)] = 2\mathbf{w}_1 + 2c_1\mathbf{w}_0.
\end{aligned}$$

Aplicando um procedimento análogo, chega-se nas expressões para $\mathbf{x}_1'$, $\mathbf{y}_1'$ e $\mathbf{z}_1'$, obtendo

$$\begin{aligned}
\mathbf{x}_1' &= \mathbf{x}_1 + (c_1 + \delta_0 + c_0)\mathbf{x}_0, \\
\mathbf{y}_1' &= \mathbf{y}_1 + (c_2 + c_0)\mathbf{y}_0, \\
\mathbf{z}_1' &= \mathbf{z}_1 + (c_1 - \delta_0 + c_0)\mathbf{z}_0.
\end{aligned}$$

Continuando, $\mathbf{w}_{n-1}^{'}$, $1 < n \leq (\#\{1\} - 1)$, pode ser escrito como uma combinação linear dos vetores $\{\mathbf{w}_j\}_{0\leq j\leq n-1}$ como

$$\mathbf{w}_{n-1}^{'} = \beta_{n-1}\mathbf{w}_{n-1} + \beta_{n-2}\mathbf{w}_{n-2} + \cdots + \beta_1\mathbf{w}_1 + \beta_0\mathbf{w}_0,$$

em que $\{\beta_j\}_{0\leq j\leq n-1}$ são constantes. Novamente, utilizando o Lema 4.1, escreve-se

$$\begin{aligned}\mathbf{w}'_n =&\mathbf{C}\mathbf{w}'_{n-1} + \mathbf{F}\mathbf{C}\mathbf{w}'_{n-1}\\ =&\mathbf{C}(\beta_{n-1}\mathbf{u}_{n-1} + \beta_{n-2}\mathbf{u}_{n-2} + \cdots + \beta_1\mathbf{u}_1 + 2\beta_0\mathbf{u}_0 + \beta_1 d_1\mathbf{u}_{-1}\\ &+ \cdots + \beta_{n-2}d_{n-2}\mathbf{u}_{-n+2} + \beta_{n-1}d_{n-1}\mathbf{u}_{-n+1})\\ &+ \mathbf{F}\mathbf{C}(\beta_{n-1}\mathbf{u}_{n-1} + \beta_{n-2}\mathbf{u}_{n-2} + \cdots + \beta_1\mathbf{u}_1 + 2\beta_0\mathbf{u}_0 + \beta_1 d_1\mathbf{u}_{-1}\\ &+ \cdots + \beta_{n-2}d_{n-2}\mathbf{u}_{-n+2} + \beta_{n-1}d_{n-1}\mathbf{u}_{-n+1}).\end{aligned}$$

Utilizando (4.10) e aplicando a FNT no segundo termo do lado direito da expressão acima ($\mathbf{F}\mathbf{C}\mathbf{w}'_{n-1}$), agrupa-se os termos relacionados a $\mathbf{u}_j$ e $\mathbf{u}_{-j}$, $0 \leq j \leq n$, como se segue:

$$\begin{aligned}\mathbf{w}'_n =&\beta_{n-1}(\mathbf{u}_n + d_n\mathbf{u}_{-n}) + [\beta_{n-1}c_n + \beta_{n-2} + \beta_{n-1}c_{-n+2}](\mathbf{u}_{n-1} + d_{n-1}\mathbf{u}_{-n+1})\\ &+ \cdots + [\beta_j(c_{j+1} + c_{-j+1}) + \beta_{j-1} + \beta_{j+1}d_{j+1}d_{-j}](\mathbf{u}_j + d_j\mathbf{u}_{-j})\\ &+ \cdots + [\beta_1 c_2 + 2\beta_0 + \beta_1 c_0](\mathbf{u}_1 + d_1\mathbf{u}_{-1}) + [2\beta_0 c_1 + \beta_1 d_1](\mathbf{u}_0 + d_0\mathbf{u}_0).\end{aligned}$$

Então, expressa-se $\mathbf{w}'_n$ como função do conjunto $\{\mathbf{w}_j\}_{0\leq j\leq n}$:

$$\begin{aligned}\mathbf{w}'_n =& \beta_{n-1}\mathbf{w}_n + [\beta_{n-1}c_n + \beta_{n-2} + \beta_{n-1}c_{-n+2}]\mathbf{w}_{n-1}\\ &+ \cdots + [\beta_j(c_{j+1} + c_{-j+1}) + \beta_{j-1} + \beta_{j+1}d_{j+1}d_{-j}]\mathbf{w}_j\\ &+ \cdots + [\beta_1 c_2 + 2\beta_0 + \beta_1 c_0]\mathbf{w}_1 + [2\beta_0 c_1 + \beta_1 d_1]\mathbf{w}_0.\end{aligned}$$

O mesmo procedimento pode ser aplicado para os demais valores de N, assim como para $\mathbf{x}'_n$, $\mathbf{y}'_n$ e $\mathbf{z}'_n$. Deste modo, após aplicar o algoritmo de Gram-Schmidt, tem-se

$$\begin{aligned}\mathbf{w}'^{\perp}_n &= \beta_{n-1}\mathbf{w}^{\perp}_n,\\ \mathbf{x}'^{\perp}_n &= \beta_{n-1}\mathbf{x}^{\perp}_n,\\ \mathbf{y}'^{\perp}_n &= \beta_{n-1}\mathbf{y}^{\perp}_n,\\ \mathbf{z}'^{\perp}_n &= \beta_{n-1}\mathbf{z}^{\perp}_n,\end{aligned}$$

para $0 \leq n \leq (\#\{j\} - 1)$, em que $j \in \{1, -i, -1, i\}$. Isso completa a prova do Teorema 4.2. ■

O método para construção da autobase HGL da FNT $\{\mathbf{g}^{\perp}_m\}_{0\leq m\leq N-1}$ pode ser resumido nos passos descritos na Tabela 9.

4.3 UM EXEMPLO

Nesta seção, é dado um exemplo ilustrativo no qual autovetores HGL da FNT são contruídos de acordo com o método proposto neste capítulo. Seguindo os passos sumarizados na Tabela 9, escolhe-se $p = 73$, $\alpha = 2$, $\zeta = 41$ e $N = 9$ (passo 1). A sequência

$$S_\zeta = \{1, 67, 24, 7, 3, 43, 46, 35, 9\}$$

Tabela 9 – Resumo da construção da autobase HGL da FNT a partir do método de matrizes geradoras.

1.	Escolher as constantes: p, α, $\zeta = \sqrt{\alpha}$, $N = 4L+1, M = \left\lfloor \frac{N+1}{2} \right\rfloor$, $I_N = \{-M+1, \ldots, -M+N\}$.
2.	Construir a sequência $S_\zeta(k), 1 \leq k \leq N-1$: $S_\zeta(0) = 1\,, S_\zeta(k) = \prod_{n=1}^{k} 2\text{sen}_\zeta(n)$.
3.	Construir os vetores $\{\mathbf{u}_n\}_{-1\leq n\leq 1}$ e $\{\mathbf{v}_n\}_{-1\leq n\leq 0}$, $k \in I_N$: $u_n(k) = S_\zeta(3L+n+k)S_\zeta(3L+n-k)\,, \mathbf{F}\mathbf{u}_n = \mathbf{U}_n = N^{-1/2}S_\zeta(2L+2n)\mathbf{u}_{-n}$, $v_n(k) = \text{sen}_\zeta u_n(k)\,, \mathbf{F}\mathbf{v}_n = \mathbf{V}_n = -iN^{-1/2}S_\zeta(2L+2n+1)\mathbf{v}_{-n-1}$.
4.	Construir os autovetores *semente*: $\mathbf{g}_0 = \mathbf{u}_0 + \mathbf{U}_0\,, \mathbf{g}_1 = \mathbf{v}_0 + i\mathbf{V}_0\,, \mathbf{g}_2 = -\mathbf{u}_1 + \mathbf{U}_1\,, \mathbf{g}_3 = -\mathbf{v}_0 + i\mathbf{V}_0$.
5.	Construir a matriz geradora $\mathbf{S_C}$, $k \in I_N$: $C(k+M, k+M) = 2\cos_\alpha(k), \quad \mathbf{S_C} = \mathbf{F}^{-1}\mathbf{C}\mathbf{F} + \mathbf{C}$.
6.	Construir a autobase $\{\mathbf{g}_m\}_{0\leq m\leq N-1}$: $\mathbf{g}_{4n} = \mathbf{S_C}\mathbf{g}_{4(n-1)}, \mathbf{g}_{4n+1} = \mathbf{S_C}\mathbf{g}_{4(n-1)+1}, \mathbf{g}_{4n+2} = \mathbf{S_C}\mathbf{g}_{4(n-1)+2}, \mathbf{g}_{4n+3} = \mathbf{S_C}\mathbf{g}_{4(n-1)+3}$.
7.	Obter $\{\mathbf{g}_m^\perp\}_{0\leq m\leq N-1}$ aplicando o algoritmo de Gram-Schmidt ao conjunto $\{\mathbf{g}_m\}_{0\leq m\leq N-1}$.

Fonte: (DE OLIVEIRA NETO; LIMA; PANARIO, 2018b).

é construída (passo 2, Tabela 9), assim como os vetores (passo 3, Tabela 9)

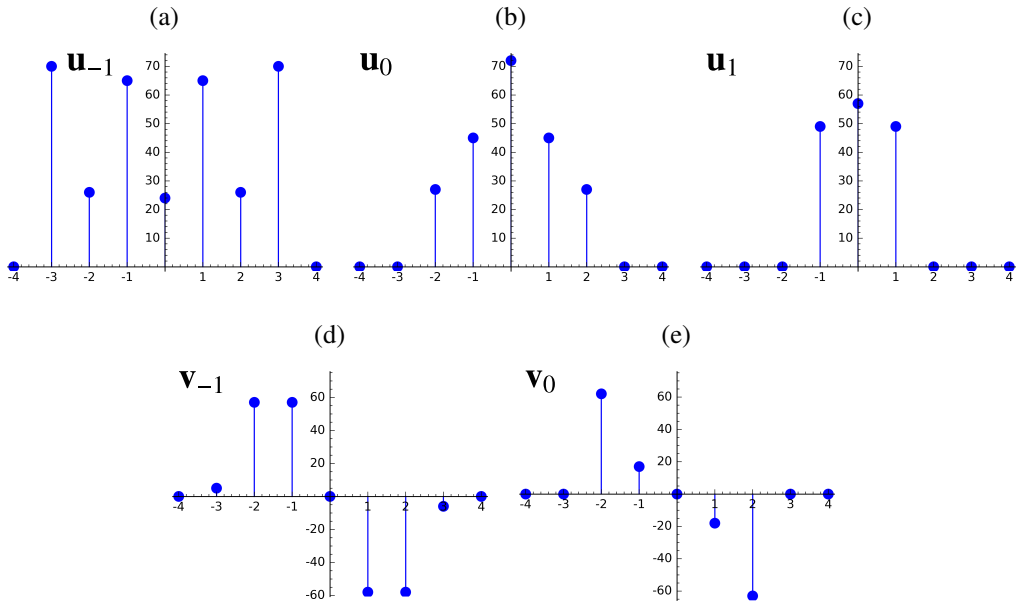
$$
\begin{aligned}
\mathbf{u}_{-1} &= [0 \quad 70 \quad 26 \quad 65 \quad 24 \quad 65 \quad 26 \quad 70 \quad 0], \\
\mathbf{u}_0 &= [0 \quad 0 \quad 27 \quad 45 \quad 72 \quad 45 \quad 27 \quad 0 \quad 0], \\
\mathbf{u}_1 &= [0 \quad 0 \quad 0 \quad 49 \quad 57 \quad 49 \quad 0 \quad 0 \quad 0], \\
\mathbf{v}_{-1} &= [0 \quad 5 \quad 57 \quad 57 \quad 0 \quad 16 \quad 16 \quad 68 \quad 0], \\
\mathbf{v}_0 &= [0 \quad 0 \quad 62 \quad 17 \quad 0 \quad 56 \quad 11 \quad 0 \quad 0].
\end{aligned}
$$

Tais vetores são plotados na Figura 20. Nesta figura, as amostras dos vetores são plotadas de maneira a enfatizar a simetria de cada vetor, embora em corpos finitos não seja possível classificar um número como sendo "positivo" ou "negativo". Neste sentido, levando em consideração o simétrico aditivo módulo 73, é fácil notar na figura que os vetores $\{\mathbf{u}_n\}_{-1\leq n\leq 1}$ e $\{\mathbf{v}_n\}_{-1\leq n\leq 0}$ possuem simetria par e ímpar, respectivamente.

Os autovetores *semente* $\mathbf{g}_n$, $n = 0, 1, 2, 3$, são construídos de acordo com o passo 4 (Tabela 9) e são dados por

$$
\begin{aligned}
\mathbf{g}_0 &= [0 \quad 0 \quad 54 \quad 17 \quad 71 \quad 17 \quad 54 \quad 0 \quad 0]\,, \\
\mathbf{g}_1 &= [0 \quad 23 \quad 3 \quad 31 \quad 0 \quad 42 \quad 70 \quad 50 \quad 0]\,, \\
\mathbf{g}_2 &= [0 \quad 27 \quad 58 \quad 23 \quad 19 \quad 23 \quad 58 \quad 27 \quad 0]\,, \\
\mathbf{g}_3 &= [0 \quad 23 \quad 25 \quad 70 \quad 0 \quad 3 \quad 48 \quad 50 \quad 0].
\end{aligned}
$$

Figura 20 – Vetores: (a) $\mathbf{u}_{-1}$, (b) $\mathbf{u}_0$, (c) $\mathbf{u}_1$, (d) $\mathbf{v}_{-1}$, e (e) $\mathbf{v}_0$.



Fonte: (DE OLIVEIRA NETO; LIMA; PANARIO, 2018b)

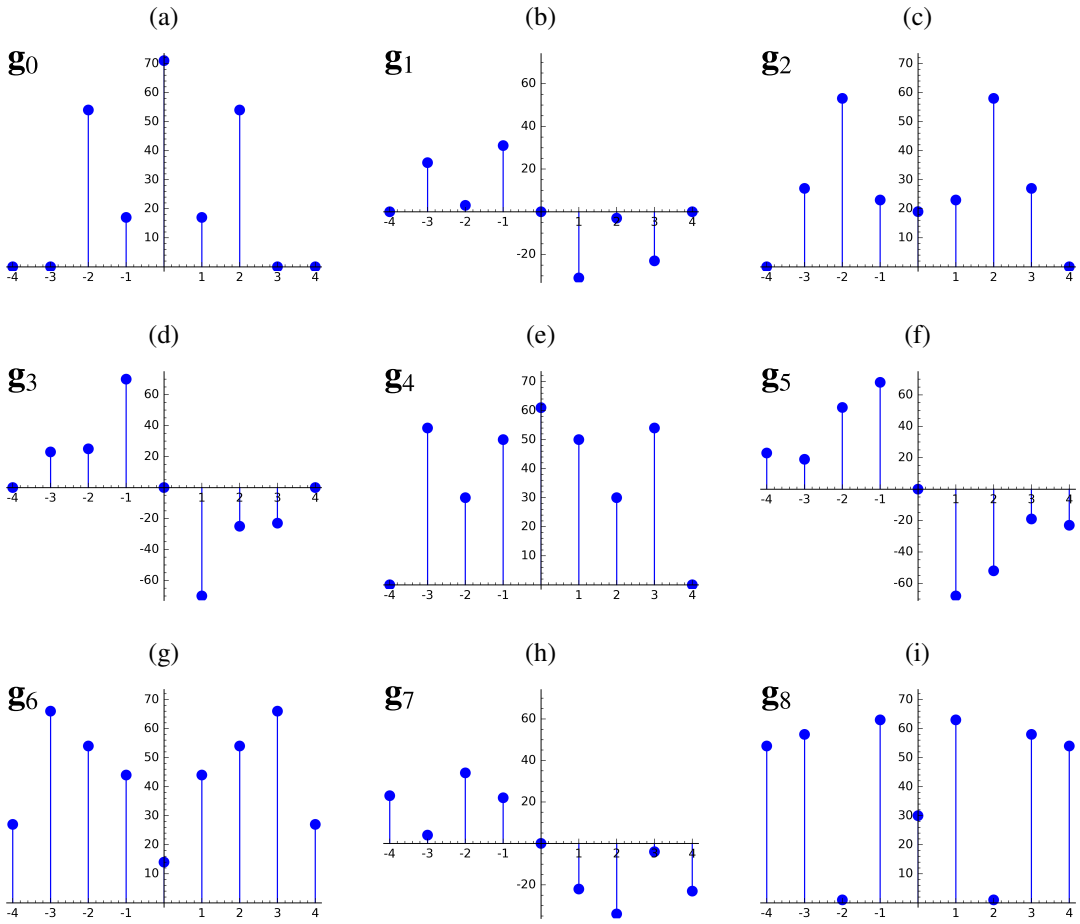
A matriz geradora $\mathbf{S_C}$, construída de acordo com o passo 5 (Tabela 9), é dada por

$$\mathbf{S_C} = \begin{bmatrix} 48 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 72 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 59 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 39 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 39 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 59 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 72 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 48 \end{bmatrix}.$$

Usando $\mathbf{S_C}$ e os autovetores *semente*, a autobase $\{\mathbf{g}_m\}_{0\leq m\leq 8}$ é construída de acordo com o passo 6 (Tabela 9). Após a ortogonalização desses vetores (passo 7, Tabela 9), é obtida a autobase $\{\mathbf{g}_m^{\perp}\}_{0\leq m\leq 8}$, cujos vetores são

$$\begin{aligned}
\mathbf{g}_0^{\perp} &= [\ 0 \quad 0 \quad 54 \quad 17 \quad 71 \quad 17 \quad 54 \quad 0 \quad 0], \\
\mathbf{g}_1^{\perp} &= [\ 0 \quad 23 \quad 3 \quad 31 \quad 0 \quad 42 \quad 70 \quad 50 \quad 0], \\
\mathbf{g}_2^{\perp} &= [\ 0 \quad 27 \quad 58 \quad 23 \quad 19 \quad 23 \quad 58 \quad 27 \quad 0], \\
\mathbf{g}_3^{\perp} &= [\ 0 \quad 23 \quad 25 \quad 70 \quad 0 \quad 3 \quad 48 \quad 50 \quad 0], \\
\mathbf{g}_4^{\perp} &= [\ 0 \quad 54 \quad 30 \quad 50 \quad 61 \quad 50 \quad 30 \quad 54 \quad 0], \\
\mathbf{g}_5^{\perp} &= [23 \quad 19 \quad 52 \quad 68 \quad 0 \quad 5 \quad 21 \quad 54 \quad 50], \\
\mathbf{g}_6^{\perp} &= [27 \quad 66 \quad 54 \quad 44 \quad 14 \quad 44 \quad 54 \quad 66 \quad 27], \\
\mathbf{g}_7^{\perp} &= [23 \quad 4 \quad 34 \quad 33 \quad 0 \quad 51 \quad 39 \quad 69 \quad 50], \\
\mathbf{g}_8^{\perp} &= [54 \quad 58 \quad 1 \quad 63 \quad 30 \quad 63 \quad 1 \quad 58 \quad 54].
\end{aligned}$$

Figura 21 – Autovetores: (a) $\mathbf{g}_0^{\perp}$, (b) $\mathbf{g}_1^{\perp}$, (c) $\mathbf{g}_2^{\perp}$, (d) $\mathbf{g}_3^{\perp}$, (e) $\mathbf{g}_4^{\perp}$, (f) $\mathbf{g}_5^{\perp}$, (g) $\mathbf{g}_6^{\perp}$, (h) $\mathbf{g}_7^{\perp}$, e (i) $\mathbf{g}_8^{\perp}$.



Fonte: (DE OLIVEIRA NETO; LIMA; PANARIO, 2018b)

Estes vetores são plotados na Figura 21. Também nesta figura, observa-se a simetria par ou ímpar dos vetores com índices pares ou ímpares, respectivamente. Os autovetores HGL podem ser dispostos como colunas da matriz $\mathbf{E}$ em (4.1) e, dada uma ordem fracionária a, a matriz $\mathbf{F}^a$ da FrFNT correspondente é obtida. Considerando, por exemplo, as matrizes $\mathbf{F}^a$, para $a = \frac{1}{2}$ e $a = \frac{1}{3}$, tem-se

$$\mathbf{F}^{\frac{1}{2}} = \begin{bmatrix} 57 & 21 & 45 & 22 & 62 & 34 & 37 & 63 & 9 \\ 21 & 32 & 71 & 18 & 72 & 21 & 37 & 41 & 63 \\ 45 & 71 & 59 & 41 & 20 & 21 & 25 & 37 & 37 \\ 22 & 18 & 41 & 67 & 4 & 23 & 21 & 21 & 34 \\ 62 & 72 & 20 & 4 & 26 & 4 & 20 & 72 & 62 \\ 34 & 21 & 21 & 23 & 4 & 67 & 41 & 18 & 22 \\ 37 & 37 & 25 & 21 & 20 & 41 & 59 & 71 & 45 \\ 63 & 41 & 37 & 21 & 72 & 18 & 71 & 32 & 21 \\ 9 & 63 & 37 & 34 & 62 & 22 & 45 & 21 & 57 \end{bmatrix}$$

e

$$\mathbf{F}^{\frac{1}{3}} = \begin{bmatrix} 67 & 60 & 15 & 3 & 56 & 57 & 52 & 30 & 22 \\ 60 & 36 & 42 & 48 & 48 & 0 & 42 & 70 & 30 \\ 15 & 42 & 44 & 65 & 60 & 13 & 28 & 42 & 52 \\ 3 & 48 & 65 & 28 & 46 & 53 & 13 & 0 & 57 \\ 56 & 48 & 60 & 46 & 4 & 46 & 60 & 48 & 56 \\ 57 & 0 & 13 & 53 & 46 & 28 & 65 & 48 & 3 \\ 52 & 42 & 28 & 13 & 60 & 65 & 44 & 42 & 15 \\ 30 & 70 & 42 & 0 & 48 & 48 & 42 & 36 & 60 \\ 22 & 30 & 52 & 57 & 56 & 3 & 15 & 60 & 67 \end{bmatrix}.$$

Na Figura 22, são plotadas as FrFNT dos vetores

$$\begin{aligned} \mathbf{x}_\delta &= [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0], \\ \mathbf{x}_\mathbf{w} &= [0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0], \\ \mathbf{x}_\mathbf{u} &= [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1], \end{aligned}$$

calculadas utilizando $\mathbf{F}^{\frac{1}{2}}$ e $\mathbf{F}^{\frac{1}{3}}$. As referidas transformadas são dadas por

$$\begin{aligned} \mathbf{X}_\delta^{\left(\frac{1}{2}\right)} &= [62 \quad 72 \quad 20 \quad 4 \quad 26 \quad 4 \quad 20 \quad 72 \quad 62], \\ \mathbf{X}_\mathbf{w}^{\left(\frac{1}{2}\right)} &= [54 \quad 0 \quad 20 \quad 10 \quad 1 \quad 10 \quad 20 \quad 0 \quad 54], \\ \mathbf{X}_\mathbf{u}^{\left(\frac{1}{2}\right)} &= [59 \quad 15 \quad 67 \quad 30 \quad 38 \quad 6 \quad 17 \quad 68 \quad 61], \\ \mathbf{X}_\delta^{\left(\frac{1}{3}\right)} &= [56 \quad 48 \quad 60 \quad 46 \quad 4 \quad 46 \quad 60 \quad 48 \quad 56], \\ \mathbf{X}_\mathbf{w}^{\left(\frac{1}{3}\right)} &= [37 \quad 34 \quad 64 \quad 59 \quad 70 \quad 59 \quad 64 \quad 34 \quad 37], \\ \mathbf{X}_\mathbf{u}^{\left(\frac{1}{3}\right)} &= [71 \quad 44 \quad 49 \quad 23 \quad 68 \quad 44 \quad 7 \quad 15 \quad 55]. \end{aligned}$$

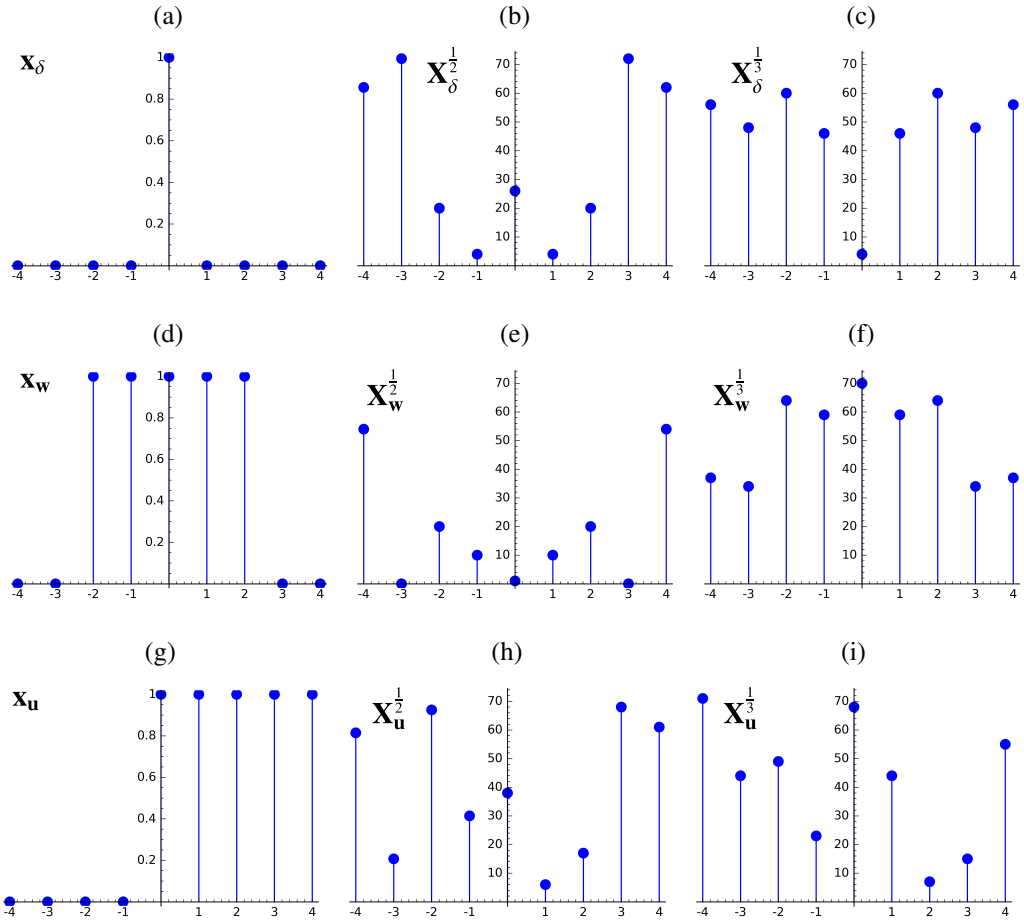
4.4 DISCUSSÃO

Nesta seção, são discutidos alguns aspectos importantes do método proposto neste capítulo e do conjunto de autovetores HGL da FNT $\{\mathbf{g}_m^{\perp}\}_{0\leq m\leq N-1}$. Primeiramente, são levantadas possibilidades relacionadas à complexidade aritmética envolvida no cálculo da FrFNT definida utilizando o referido conjunto. Em sequência, são apresentadas propriedades do método de matrizes geradoras, comparando com outras abordagens no mesmo contexto.

4.4.1 Complexidade aritmética

À primeira vista, a complexidade do cálculo de uma FrFNT definida utilizando a autobase proposta neste capítulo é $\mathcal{O}(N^2)$. Contudo, conjectura-se que uma complexidade menor pode ser obtida aplicando o método dado em (MAJORKOWSKA-MECH; CARIOW, 2017). Este método depende basicamente das simetrias da matriz de transformação e, embora tenha sido desenvolvido para o cálculo da DFrFT, é possível estender o algoritmo para o cenário dos corpos

Figura 22 – Vetores: (a) $\mathbf{x}_\delta$, (d) $\mathbf{x_w}$ e (g) $\mathbf{x_u}$; respectivas FrFNT para $a = \frac{1}{2}$: (b) $\mathbf{X}_\delta^{\left(\frac{1}{2}\right)}$, (e) $\mathbf{X_w}^{\left(\frac{1}{2}\right)}$ e (h) $\mathbf{X_u}^{\left(\frac{1}{2}\right)}$; e para $a = \frac{1}{3}$: (c) $\mathbf{X}_\delta^{\left(\frac{1}{3}\right)}$, (f) $\mathbf{X_w}^{\left(\frac{1}{3}\right)}$ e (i) $\mathbf{X_u}^{\left(\frac{1}{3}\right)}$.



Fonte: (DE OLIVEIRA NETO; LIMA; PANARIO, 2018b)

finitos. No intuito de fornecer uma ilustração preliminar de tal possibilidade, considera-se a matriz $\mathbf{F}^{\frac{1}{2}}$ da FrFNT construída no exemplo da Seção 4.3. Sua versão não-centralizada[1] $\bar{\mathbf{F}}^{\frac{1}{2}}$ pode ser escrita como

$$\bar{\mathbf{F}}^{\frac{1}{2}} = \begin{bmatrix} b & c & d & e & f & f & e & d & c \\ c & g & h & i & j & k & l & l & m \\ d & h & n & o & q & r & r & s & l \\ e & i & o & t & l & u & v & r & l \\ f & j & q & l & w & x & u & r & k \\ f & k & r & u & x & w & l & q & j \\ e & l & r & v & u & l & t & o & i \\ d & l & s & r & r & q & o & n & h \\ c & m & l & l & k & j & i & h & g \end{bmatrix},$$

em que $b = 26$, $c = 4$, $d = 20$, $e = 72$, $f = 62$, $g = 67$, $h = 41$, $i = 18$, $j = 22$, $k = 34$, $l = 21$, $m = 23$, $n = 59$, $o = 71$, $q = 45$, $r = 37$, $s = 25$, $t = 32$, $u = 63$, $v = 41$,

[1] O método proposto em (MAJORKOWSKA-MECH; CARIOW, 2017) considera transformadas não-centralizadas, que podem ser obtidas aplicando um deslocamento circular nas linhas e colunas da matriz da transformada centralizada.

$w = 57$ e $x = 9$. A simetria de $\bar{\mathbf{F}}^{\frac{1}{2}}$ e o fato de que ela apresenta apenas 22 entradas distintas podem ser explorados com o intuito de efetuar eficientemente o produto entre esta matriz e um vetor cuja FrFNT deseja-se calcular (a estratégia pode ser similar à apresentada no Exemplo 1 de (MAJORKOWSKA-MECH; CARIOW, 2017) e explicada na Seção 4 do mesmo artigo). Mais precisamente, deve-se poder efetuar este produto utilizando no máximo 41 multiplicações e 56 adições em $\mathbb{F}_{73}$ (ver Tabela 4 em (MAJORKOWSKA-MECH; CARIOW, 2017)). Por outro lado, o método direto requer 81 multiplicações e 72 adições.

A possibilidade descrita acima ainda necessita de maiores estudos, isto deve ser parte de um trabalho futuro. A extensão de outras estratégias, como a descrita em (LIU et al., 2014), para corpos finitos não parece ser tão clara, devido ao fato de que algumas operações não devem ter um equivalente em corpos finitos (multiplicação por sinal *chirp*, por exemplo). De qualquer forma, diferentemente da DFrFT, as aplicações da FrFNT envolvem apenas aritmética com números inteiros. Isso permite implementar em casos específicos multiplicações por meio de adições e deslocamentos de bits (ver por exemplo (BLAHUT, 2003; BLAHUT, 2010; DE OLIVEIRA NETO; LIMA, 2018)).

4.4.2 Propriedades e comparações com outros autovetores da FNT

Na Seção 4.2.1, é demonstrado que o método de matrizes geradoras pode ser usado recursivamente para construção de autovetores da FNT. A partir da escolha da matriz $\mathbf{A}$ satisfazendo $\mathbf{F}^2\mathbf{A}\mathbf{F}^2 = \gamma\mathbf{A}$ e um autovetor semente, autovetores da FNT, relacionados a autovalores possivelmente diferentes, podem ser obtidos. Os autovetores gerados podem constituir uma base que pode ser utilizada na definição da FrFNT (esta possibilidade assim como um sistema de cifragem de imagens é descrito no Capítulo 5). Na Seção 4.2.2, é demonstrado que, se $\mathbf{A} = \mathbf{C}$ e autovetores específicos são escolhidos, é obtida a autobase HGL da FNT apresentada em (LIMA; CAMPELLO DE SOUZA, 2016). Neste contexto, é relevante listar algumas das propriedades do método, indicando quando eles são especificamente relacionados com o conjunto HGL $\{\mathbf{g}_m^{\perp}\}_{0 \leq m \leq N-1}$:

1. O método de matrizes geradoras utiliza fórmulas fechadas e não requer, por exemplo, o emprego de algoritmos para achar raízes de polinômios sobre corpos finitos;

2. Diferentes conjuntos de autovetores da FNT podem ser obtidos modificando a matriz geradora utilizada, assim como os vetores semente. Consequentemente, se o conjunto obtido for uma base, diferentes FrFNT podem ser definidas;

3. Autovetores com componentes em corpos de extensão podem ser evitados, escolhendo matrizes geradoras e autovetores semente com componentes apenas em $\mathbb{F}_p$. Isso significa que todas as operações envolvidas na geração dos autovetores são feitas utilizando aritmética módulo p;

4. A autobase HGL da FNT $\{\mathbf{g}_m^{\perp}\}_{0\leq m\leq N-1}$ contém vetores com sequências de componentes nulas em suas extremidades, o que pode ser visto como uma espécie de *suporte próprio compacto*[2]. Isso pode ser útil no desenvolvimento de algoritmos rápidos para geração dessas autobases e do cálculo das FrFNT correspondentes;

5. Os vetores $\{\mathbf{g}_m^{\perp}\}_{0\leq m\leq N-1}$ são claramente ordenados. Isso evita ambiguidades relacionadas à sequência em que eles são arranjados como colunas da matriz $\mathbf{E}$ em (4.1), quando uma FrFNT específica é definida.

Os autovetores da FNT obtidos a partir do método das matrizes geradoras podem ser comparados com aqueles construídos usando outras duas técnicas. Em (PEI; WEN; DING, 2011), os autores estenderam para corpos finitos o método descrito em (PEI; WEN; DING, 2008), que é baseado nas sequências de Legendre generalizadas completas (CGLS, do inglês *complete generalized Legendre sequences*); em (LIMA; CAMPELLO DE SOUZA, 2012), o método apresentado em (CANDAN; KUTAY; OZAKTAS, 2000) é estendido para corpos finitos e os autovetores são derivados empregando uma matriz que comuta com a matriz da FNT[3]. Na Tabela 10, uma comparação entre os métodos é sumarizada; os aspectos considerados na tabela, basicamente, levam em consideração as propriedades 1-5 descritas anteriormente, indicando quando elas são satisfeitas pelos métodos comparados. O método descrito em (LIMA; CAMPELLO DE SOUZA, 2012), por exemplo, não utiliza fórmulas fechadas para construção dos autovetores da FNT, envolvendo algoritmos para encontrar raízes de polinômios (característicos) sobre um corpo finito; se essas raízes estiverem num corpo de extensão, são obtidos autovetores cujas componentes também pertencem a um corpo de extensão. O cálculo de uma FrFNT definida utilizando tais autovetores requer uma aritmética de maior complexidade que a calculada sobre um corpo base. Dados N e $\alpha \in \mathbb{F}_p$, a técnica descrita em (PEI; WEN; DING, 2011) produz um único conjunto de autovetores (não-HGL) da FNT; isso significa que, diferentemente do que é verificado pelo método proposto neste capítulo (ver propriedade 2), o único parâmetro livre na FrFNT baseada na abordagem CGLS é a ordem fracionária a.

4.5 CONSIDERAÇÕES

Neste capítulo, foi descrito um método para construção de autovetores da transformada numérica de Fourier utilizando matrizes geradoras. Foi proposto um algoritmo para construção de uma base de autovetores do tipo Hermite-Gaussiano da FNT partindo de uma matriz gera-

[2] Ver o vetor $\mathbf{g}_0^{\perp}$ na Seção 4.3, por exemplo; ele possui dois zeros consecutivos em suas extremidades e, além do mais, seu suporte tem comprimento 5. Em geral, se $N = 4L + 1$, o vetor $\mathbf{g}_0^{\perp}$ tem suporte igual a $2L + 1$. O suporte cresce com m para $\{\mathbf{g}_m^{\perp}\}_{1\leq m\leq N-5}$, alcançando seu máximo, isso é, N, para $\{\mathbf{g}_m^{\perp}\}_{N-4\leq m\leq N-1}$ (ver vetores $\{\mathbf{g}_m^{\perp}\}_{1\leq m\leq 8}$ no já mencionado exemplo).

[3] Em (LIMA; LIMA; CAMPELLO DE SOUZA, 2017), outra transformada fracionária numérica de Fourier é apresentada. No entanto, a abordagem emprega funções de matrizes e não requer a construção de autovetores da matriz da transformada ordinária correspondente. Este é o motivo pelo qual ela não foi considerada na análise comparativa feita nesta seção.

Tabela 10 – Comparação entre os diferentes métodos de construção de autovetores da FNT.

	Proposto	PEI[1]	LIMA[2]
Os autovetores são de fórmula fechada	×	×	
Dados N e $\alpha \in \mathbb{F}_p$, diferentes conjuntos de autovetores podem ser construídos	×		
Autovetores em corpos de extensão podem ser evitados	×	×	
Autovetores HGL da FNT podem ser obtidos	×*		×
Os autovetores podem ser ordenados sem ambiguidades	×	×	
Autovetores de *suporte próprio compacto* podem ser obtidos	×*		

*Estas propriedades são satisfeitas pelo conjunto $\{\mathbf{g}_m^{\perp}\}_{0 \leq m \leq N-1}$ gerado pelo método proposto.
[1](PEI; WEN; DING, 2011).
[2](LIMA; CAMPELLO DE SOUZA, 2012).

Fonte: (DE OLIVEIRA NETO; LIMA; PANARIO, 2018b)

dora específica e foi provado que esta base é uma versão escalonada do conjunto apresentado em (LIMA; CAMPELLO DE SOUZA, 2016).

5 PROJETO DE UMA TRANSFORMADA FRACIONÁRIA MULTIPARAMÉTRICA NUMÉRICA DE FOURIER E SUA APLICAÇÃO EM CIFRAGEM DE IMAGENS

Nas últimas décadas, diversas técnicas voltadas para segurança da informação multimídia têm sido desenvolvidas (LI et al., 2008; DEB et al., 2013; LEE; TSAI, 2014; CHEN et al., 2016; QIAN; ZHANG, 2016; BOYADJIS et al., 2017; WU et al., 2017; ZHANG et al., 2017; GE; QIAN; WANG, 2018; LIU; LIN; YUAN, 2018). Neste contexto, várias investigações têm tido como foco a construção de esquemas de cifragem de imagem, muitas das quais são baseadas nas chamadas transformadas fracionárias (PEI; WEN; DING, 2008; PEI; HSUE, 2009; KANG; ZHANG; TAO, 2015b; HSUE; CHANG, 2015b; LIU et al., 2015; ANNABY; RUSHDI; NEHARY, 2016b; TAO; MENG; WANG, 2010; PEI; HSUE, 2006; KANG; TAO; ZHANG, 2016; TAO; LANG; WANG, 2009; KANG; MING; TAO, 2018; KANG; TAO, 2018; LIU; LIU, 2007; SINGH; SINHA, 2008; LIU et al., 2012; LANG, 2012; RAN et al., 2014; LANG, 2015; ELHOSENY et al., 2016; ZHAO et al., 2016b; LI et al., 2015; VAISH; KUMAR, 2017). A segurança desses sistemas é relacionada com a ordem fracionária, que pode ser escolhida de acordo com uma chave secreta. Transformadas numéricas também desempenham um papel importante neste cenário (LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017); elas são exploradas principalmente devido à alta sensibilidade a pequenas modificações nos operandos, característica inerente das operações aritméticas modulares, o que é interessante do ponto de vista criptográfico. Em particular, alguns esquemas de criptografia são baseados em transformadas fracionárias numéricas (PEI; WEN; DING, 2011; LIMA; NOVAES, 2014; LIMA; CAMPELLO DE SOUZA, 2016; LIMA; LIMA; CAMPELLO DE SOUZA, 2017), e transformadas multiparamétricas fracionárias, definidas sobre os reais ou complexos (PEI; HSUE, 2006; KANG; TAO; ZHANG, 2016; TAO; LANG; WANG, 2009; KANG; MING; TAO, 2018; KANG; TAO, 2018), em que a *única* ordem fracionária é substituída por um vetor com *múltiplas* ordens fracionárias usadas como chave secreta.

Ao contrário do que ocorre em algumas definições da DFrFT (ver Capítulo 2), em certos cenários práticos, a busca por uma definição da transformada que aproxime numericamente a transformada fracionária contínua não é necessária. Isso é verificado, por exemplo, na definição de transformadas fracionárias randômicas discretas. Nesta classe de transformadas fracionárias discretas, que também tem sido empregada em esquemas de cifragem, um conjunto de autovetores com vários parâmetros escolhidos é usado para definir a transformada (PEI; WEN; DING, 2008; PEI; HSUE, 2009; KANG; ZHANG; TAO, 2015b).

Neste capítulo, é apresentado um novo algoritmo para definir uma classe de autovetores da transformada numérica de Fourier; esses vetores são então usados para definir uma transformada fracionária multiparamétrica numérica de Fourier (MFrFNT, do inglês *multiple-parameter*

fractional Fourier number transform). O algoritmo proposto emprega o conceito de matrizes geradoras, originalmente apresentado para construção de autovetores da DFT (PEI; CHANG, 2009; PEI; CHANG, 2016; DE OLIVEIRA NETO; LIMA, 2017). Ao longo do Capítulo 4, é explicado como este conceito de matrizes geradoras pode ser estendido para o cenário de corpos finitos, permitindo a construção de autovetores da FNT (DE OLIVEIRA NETO; LIMA; PANARIO, 2018b). Aqui, é introduzido um método para criação das referidas matrizes a partir de parâmetros escolhidos e, usando essas matrizes, é dado um procedimento sistemático para construção de uma base ortogonal de autovetores da FNT empregada na definição da MFrFNT. Esta transformada multiparamétrica é então usada como o núcleo de um esquema de cifragem de imagem, que também inclui um estágio de embaralhamento de pixels baseado na transformação de Arnold. Comparando com outros esquemas de cifragem de imagem que empregam transformadas numéricas, o método proposto envolve um número de parâmetros livres substancialmente maior e conta com uma transformada fracionária definida apenas por meio de fórmulas fechadas.

O restante do capítulo é organizado como segue.

i Na Seção 5.1, são apresentadas algumas definições matemáticas necessárias no decorrer do trabalho.

ii Na Seção 5.2, é descrito o método usado para construção da base de autovetores ortogonais da FNT utilizada na definição da MFrFNT. Um novo algoritmo para definir matrizes geradoras a partir de parâmetros é apresentado, tendo como ênfase o número de elementos que se pode escolher. A partir dessas matrizes, é apresentado um método para construção de uma base ortogonal de autovetores da FNT.

iii Na Seção 5.3, é introduzido o esquema de cifragem de imagens baseado na MFrFNT; são descritas suas características assim como os passos necessários para cifragem e decifragem.

iv Na Seção 5.4, são mostrados os resultados das simulações feitas para avaliar a robustez do sistema proposto. Isso é feito utilizando métricas encontradas na literatura relacionada (LIU; LIU, 2007; SINGH; SINHA, 2008; LIU et al., 2012; LANG, 2012; RAN et al., 2014; LANG, 2015; ELHOSENY et al., 2016; ZHAO et al., 2016b; LI et al., 2015; VAISH; KUMAR, 2017; PEI; WEN; DING, 2008; PEI; HSUE, 2009; TAO; MENG; WANG, 2010; HSUE; CHANG, 2015b; LIU et al., 2015; KANG; ZHANG; TAO, 2015b; KANG; TAO; ZHANG, 2016; ANNABY; RUSHDI; NEHARY, 2016b; PEI; HSUE, 2006; PEI; WEN; DING, 2011; LIMA; NOVAES, 2014; LIMA; CAMPELLO DE SOUZA, 2016; LIMA; LIMA; CAMPELLO DE SOUZA, 2017; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017; LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; ECRYPT II, 2012; TAO; LANG; WANG, 2009; WU; NOONAN; AGAIAN, 2011).

v Na Seção 5.5, é explicado como o esquema pode ser ajustado para diferentes tipos de imagem.

vi Na Seção 5.6, algumas considerações sobre o capítulo são apresentadas.

5.1 PRELIMINARES MATEMÁTICAS

Nesta seção, são apresentadas algumas definições relacionadas a trabalhos anteriores que serão úteis ao logo deste capítulo.

5.1.1 Transformada fracionária numérica de Fourier

A expansão espectral da matriz $\mathbf{F}$ da FNT é dada por

$$\mathbf{F} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^T,$$

em que $\mathbf{E}$ é uma matriz quadrada cujas colunas formam um conjunto ortogonal de autovetores de $\mathbf{F}$ e a matriz diagonal $\mathbf{\Lambda}$ é formada pelos autovalores correspondentes. A autoestrutura da FNT é análoga à da DFT (MCCLELLAN; PARKS, 1972; BIRTWISTLE, 1982); logo, seus autovetores são $\{1, -1, i, -i\}$, em que $i^2 \equiv -1 \pmod p$, com multiplicidades mostradas na Tabela 8, p. 76.

Outra forma de escrever a expansão espectral de $\mathbf{F}$ é

$$\mathbf{F} = \tilde{\mathbf{E}}\mathbf{D}\mathbf{\Lambda}\tilde{\mathbf{E}}^T, \tag{5.1}$$

em que $\tilde{\mathbf{E}}$ é uma matriz quadrada cujas colunas formam um conjunto ortogonal de autovetores de $\mathbf{F}$, os respectivos autovalores são os elementos da diagonal da matriz diagonal $\mathbf{\Lambda}$, e $\mathbf{D}$ é uma matriz diagonal cujos elementos são o inverso do quadrado da norma dos autovetores correspondentes na matriz $\tilde{\mathbf{E}}$. Esta abordagem é apresentada em (LIMA; CAMPELLO DE SOUZA, 2016) e evita que os elementos da transformada caiam sobre um corpo de extensão [1].

A partir de (5.1), defini-se a matriz da FrFNT como

$$\mathbf{F}^a = \tilde{\mathbf{E}}\mathbf{D}\mathbf{\Lambda}^a\tilde{\mathbf{E}}^T, \tag{5.2}$$

em que a é a ordem fracionária, e $a = \frac{b}{c}$, $b \in \mathbb{Z}$ e $c \in \mathbb{Z}^*$.

5.1.2 Transformada fracionária multiparamétrica numérica de Fourier

Transformadas fracionárias multiparamétricas têm sido definidas sobre o corpo dos reais (KANG; TAO; ZHANG, 2016; PEI; HSUE, 2006; TAO; LANG; WANG, 2009). Em tais abordagens, a ordem fracionária é substituída por um vetor de ordens fracionárias. Sobre corpos

[1] Isso poderia ocorrer porque a operação de radiciação, necessária à normalização dos autovetores, não é fechada em $\mathbb{F}_p$.

finitos, seja $\mathbf{a}$ um vetor de ordens fracionárias com componentes $a_j = \frac{b_j}{c_j}$, $1 \leq j \leq N$, em que $b_j \in \mathbb{Z}$ e $c_j \in \mathbb{Z}^*$. Os elementos de $\mathbf{a}$ são os expoentes de cada um dos elementos da diagonal de $\mathbf{\Lambda}$, isso é,

$$\mathbf{\Lambda^a} = \begin{bmatrix} \lambda_{1,1}^{a_1} & 0 & \cdots & 0 \\ 0 & \lambda_{2,2}^{a_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{N,N}^{a_N} \end{bmatrix}.$$

A transformada fracionária multiparamétrica numérica de Fourier (MFrFNT, do inglês *multiple-parameter fractional Fourier number transform*) de um vetor $\mathbf{x}$ é então definida por

$$\mathbf{X^{(a)}} = \mathbf{F^a x} = \mathbf{\tilde{E} D \Lambda^a \tilde{E}}^T \mathbf{x}. \tag{5.3}$$

5.1.3 Construção de autovetores da FNT a partir de sequências randômicas

Um algoritmo conhecido para construção de autovetores da DFT emprega vetores com simetria par para gerar autovetores relacionados aos autovetores 1 ou -1, e vetores com simetria ímpar para gerar autovetores relacionados com os autovalores i ou $-i$ (MCCLELLAN; PARKS, 1972). É possível usar uma estratégia similar para construir autovetores da FNT com autovalores desejados (BIRTWISTLE, 1982).

Seja $\mathbf{d}_e$ um vetor com simetria par com componentes $d_e(k) \in \mathbb{F}_p$, $k \in I_N$, e FNT dada por $\mathbf{D}_e = \mathbf{F d}_e$; seja $\mathbf{d}_o$ um vetor com simetria ímpar com componentes $d_o(k) \in \mathbb{F}_p$, $k \in I_N$, e FNT dada por $\mathbf{D}_o = \mathbf{F d}_o$. Constrói-se autovetores $\mathbf{v}_j$ da FNT relacionados com os autovalores $j \in \{1, -1, i, -i\}$, em que $i^2 \equiv -1 \pmod p$, por meio de (MCCLELLAN; PARKS, 1972)

$$\mathbf{v}_1 = \mathbf{d}_e + \mathbf{D}_e, \qquad \mathbf{v}_{-1} = \mathbf{d}_e - \mathbf{D}_e,$$
$$\mathbf{v}_i = \mathbf{d}_o - i\mathbf{D}_o, \qquad \mathbf{v}_{-i} = \mathbf{d}_o + i\mathbf{D}_o.$$

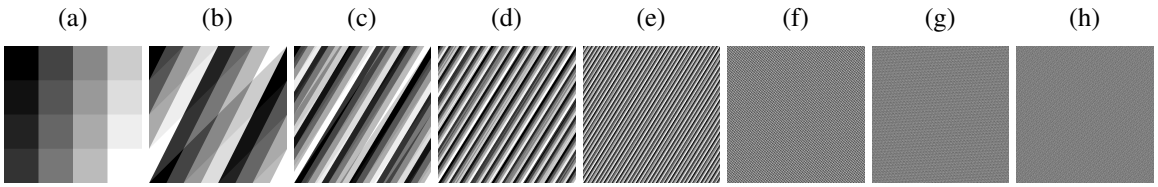
Por sua vez, pode-se construir vetores de N pontos com simetria par ou ímpar a partir de sequências randômicas com $\frac{N-1}{2}$ elementos, se N é ímpar, ou $\frac{N}{2} - 2$ elementos, se N é par[2].

5.1.4 Transformada de Arnold

A transformada de Arnold $\mathbf{\Gamma}$ é uma transformação linear sobre os índices x e y de um pixel $I(x, y)$ de uma imagem $\mathbf{I}$ (ARNOLD; AVEZ, 1968; SVANSTROM, 2014), em que $0 \leq x \leq N_r$, $0 \leq y \leq N_c$, em que N_r e N_c são os números de linhas e colunas da imagem, respectivamente. Isto é, se a transformação for aplicada nos índices x e y de um pixel $I(x, y)$, são obtidos novos índices $x^{'}$ e $y^{'}$ relacionados à nova posição do pixel $I(x^{'}, y^{'})$. Esta transformação

[2] Estes valores podem ser facilmente definidos observando os graus de liberdade na construção de um vetor com simetria par ou ímpar.

Figura 23 – (a) Imagem teste. Imagem teste após aplicar a transformada de Arnold com: (b) 1, (c) 2, (d) 3, (e) 4, (f) 5, (g) 6, (h) 7 iterações.



Fonte: Produzido pelos autores.

é definida por

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \mathbf{\Gamma} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N),$$

e sua inversa $\mathbf{\Gamma}^{-1}$ é dada por

$$\begin{bmatrix} x \\ y \end{bmatrix} = \mathbf{\Gamma}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} (\text{mod } N) = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N),$$

em que N é o número de linhas e colunas da imagem (neste caso, é assumido que a imagem possui o mesmo número de linhas e colunas). Esta transformação pode ser aplicada recursivamente, resultando em uma imagem mais embaralhada (ARNOLD; AVEZ, 1968; SVANSTROM, 2014). Nas Figuras 23b-23h são mostradas versões embaralhadas da imagem teste mostrada na Figura 23a, que possui dimensões de 512×512 pixels, utilizando a transformada de Arnold com $1, 2, \ldots, 7$ iterações, respectivamente. A imagem teste é constituída de 16 subimagens de 128×128 pixels. Cada subimagem é formada por pixels que possuem um único valor, contudo, este valor é diferente para cada uma das subimagens. Iste é feito para mostrar que os pixels de cada uma das subimagens são espalhados por todas as outras subimagens após 3 iterações da transformada de Arnold. Esta propriedade é usada no esquema de cifragem de imagens proposto na Seção 5.3.

5.2 MÉTODO DE MATRIZES GERADORAS PARA CONSTRUÇÃO DE AUTOVETORES DA FNT

No Capítulo 4, foi apresentado o conceito de matriz geradora de autovetores da FNT, mostrou-se que, dados uma matriz geradora $\mathbf{S_A} = \gamma^{\frac{1}{2}}\mathbf{F}^{-1}\mathbf{A}\mathbf{F} + \mathbf{A}$ e um autovetor $\mathbf{v}$, o vetor $\mathbf{v}' = \mathbf{S_A}\mathbf{v}$ também é um autovetor da FNT com autovalor conhecido, podendo esse procedimento ser repetido recursivamente. Utilizando o algoritmo descrito na Seção 5.1.3 constrói-se autovetores semente com autovalores desejados. Adicionalmente a isso, nesta seção, é apresentado um método para construção da matriz $\mathbf{A}$ que será utilizado para definir um algoritmo para geração de um conjunto ortogonal de autovetores da FNT.

5.2.1 Método de construção de uma matriz geradora

Para definir uma matriz geradora $\mathbf{S_A}$, é necessário determinar uma matriz $\mathbf{A}$ que satisfaça

$$\mathbf{F}^2\mathbf{A}\mathbf{F}^2 = \gamma\mathbf{A}. \tag{5.4}$$

Analisando (5.4), vê-se que os elementos de $\mathbf{F}^2$ são dependentes do comprimento N ser par ou ímpar, de acordo com

$$\mathbf{F}^2_{N\times N} = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix},$$

para $N = 2P + 1$ e

$$\mathbf{F}^2_{N\times N} = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 1 & 0 & 0 \\ \vdots & \vdots & \iddots & & \vdots & \vdots \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{bmatrix},$$

para $N = 2P$.

Além do mais, a expressão (5.4) apenas reorganiza os elementos da matriz $\mathbf{A}$. Mais precisamente, se $\mathbf{B} = \mathbf{F}^2\mathbf{A}\mathbf{F}^2$, os elementos $b_{n,m}$ de $\mathbf{B}$ são dependentes dos elementos $a_{n,m}$ de $\mathbf{A}$, em que $n, m \in \{1, 2, ..., N\}$; se $N = 2P + 1$, tem-se

$$b_{n,m} = a_{(N+1)-n,(N+1)-m}, \tag{5.5}$$

e, se $N = 2P$, tem-se

$$b_{n,m} = \begin{cases} a_{n,m}, & \text{se } n = N \quad \text{e} \quad m = N, \\ a_{n,N-m}, & \text{se } n = N \quad \text{e} \quad m \neq N, \\ a_{N-n,m}, & \text{se } n \neq N \quad \text{e} \quad m = N, \\ a_{N-n,N-m}, & \text{se } n \neq N \quad \text{e} \quad m \neq N. \end{cases} \tag{5.6}$$

Esta dependência restringe o número de elementos de $\mathbf{A}$ que podem ser escolhidos. Como existem duas expressões para $b_{n,m}$, (5.5) e (5.6), o número $M_{\mathbf{A}}$ de elementos de livre escolha também possui duas expressões.

5.2.1.1 Caso $N = 2P + 1$

As relações entre as matrizes $\mathbf{A}$ e $\mathbf{B}$, expressas em (5.5), podem ser usadas para definir $\mathbf{A}$. Em (5.7), como exemplo, é apresentada uma matriz 5×5 em que as letras a a h são os elementos que podem ser escolhidos para $\gamma = \pm 1$:

$$\mathbf{A} = \left[\begin{array}{cc|c|cc} a & b & c & d & e \\ b & f & g & h & \gamma d \\ \hline c & g & 0 & \gamma g & \gamma c \\ \hline d & \gamma h & \gamma g & \gamma f & \gamma b \\ \gamma e & \gamma d & \gamma c & \gamma b & \gamma a \end{array}\right]. \tag{5.7}$$

Em (5.8), é mostrado $\mathbf{B} = \mathbf{F}^2\mathbf{A}\mathbf{F}^2$ para a matriz $\mathbf{A}$ em (5.7). Como desejado, tem-se que $\mathbf{B} = \gamma\mathbf{A}$:

$$\mathbf{B} = \left[\begin{array}{cc|c|cc} \gamma a & \gamma b & \gamma c & \gamma d & \gamma e \\ \gamma b & \gamma f & \gamma g & \gamma h & d \\ \hline \gamma c & \gamma g & 0 & g & c \\ \hline \gamma d & h & g & f & b \\ e & d & c & b & a \end{array}\right]. \tag{5.8}$$

De maneira mais geral, seja m_j o número de elementos que é possível escolher na j-ésima linha da matriz $\mathbf{A}$. Pode-se escrever o número $M_{\mathbf{A}}$ de elementos independentes de uma matriz $\mathbf{A}$ $N \times N$ por

$$M_{\mathbf{A}} = \sum_{j=1}^{N} m_j.$$

Para uma matriz $\mathbf{A}$ como a apresentada em (5.7), tem-se $m_1 = N$ elementos livres na primeira linha, $m_2 = m_1 - 2 = N - 2$ elementos livres na segunda linha e assim por diante até a linha $j = (N-1)/2$. Então, tem-se

$$\begin{aligned} M_{\mathbf{A}} &= \textstyle\sum_{j=1}^{\frac{N-1}{2}} (N - 2(j-1)) \\ &= \tfrac{(N+3)}{2} \cdot \tfrac{(N-1)}{2} = \tfrac{N^2+2N-3}{4}. \end{aligned} \tag{5.9}$$

5.2.1.2 Caso $N = 2P$

A matriz $\mathbf{A}$ para N par pode ser definida seguindo a mesma estratégia usada para N ímpar, para $\gamma = \pm 1$. Em (5.10), como exemplo, é mostrada a matriz 6×6 em que as letras de a

a l são os elementos que podem ser escolhidos:

$$\mathbf{A} = \left[\begin{array}{cc|c|cc|c} a & b & c & d & e & k \\ b & f & g & h & \gamma d & l \\ \hline c & g & 0 & \gamma g & \gamma c & 0 \\ \hline d & \gamma h & \gamma g & \gamma f & \gamma b & \gamma l \\ \gamma e & \gamma d & \gamma c & \gamma b & \gamma a & \gamma k \\ \hline i & j & 0 & \gamma j & \gamma i & 0 \end{array}\right]. \tag{5.10}$$

Em (5.11), é mostrada a matriz $\mathbf{B} = \mathbf{F}^2\mathbf{A}\mathbf{F}^2$ para a matriz $\mathbf{A}$ apresentada em (5.10). Como desejado, tem-se que $\mathbf{B} = \gamma\mathbf{A}$:

$$\mathbf{B} = \left[\begin{array}{cc|c|cc|c} \gamma a & \gamma b & \gamma c & \gamma d & \gamma e & \gamma k \\ \gamma b & \gamma f & \gamma g & \gamma h & d & \gamma l \\ \hline \gamma c & \gamma g & 0 & g & c & 0 \\ \hline \gamma d & h & g & f & b & l \\ e & d & c & b & a & k \\ \hline \gamma i & \gamma j & 0 & j & i & 0 \end{array}\right]. \tag{5.11}$$

Extrapolando para um matriz $\mathbf{A}_{N\times N}$ a partir de (5.10), observa-se que a submatriz formada pelas $N-1$ primeiras linhas e as $N-1$ primeiras colunas possuem a simetria mostrada em (5.7). Então, desde que $\frac{N-2}{2}$ elementos podem ser escolhidos na última coluna e na última linha, tem-se

$$M_{\mathbf{A}} = \sum_{j=1}^{\frac{N-2}{2}} (N-1-2(j-1)) + 2\left(\frac{N-2}{2}\right) = \frac{N^2+4N-12}{4}. \tag{5.12}$$

5.2.2 Construção de uma autobase ortogonal da FNT

Nesta seção, um algoritmo para construção de uma base ortogonal de autovetores da FNT é proposto utilizando a matriz geradora $\mathbf{S_A}$ definida como descrito na Seção 5.2.1 para $\gamma = 1$.

Definição 5.1. Seja $\{\mathbf{e}_0 = \mathbf{v}_1, \mathbf{e}_1 = \mathbf{v}_{-i}, \mathbf{e}_2 = \mathbf{v}_{-1}, \mathbf{e}_3 = \mathbf{v}_i\}$ um conjunto de *autovetores semente*, em que os autovetores $\mathbf{v}_j$ são construídos como descrito na Seção (5.1.3). O conjunto de autovetores da FNT $\{\mathbf{e}_m\}_{0\leq m\leq N-1}$ é construído aplicando recursivamente a matriz geradora $\mathbf{S_A}$ como:

$$\begin{aligned}
\mathbf{e}_{4n} &= \mathbf{S_A}\mathbf{e}_{4(n-1)}, \quad n = 1, 2, \ldots, \#\{1\} - 1, \\
\mathbf{e}_{4n+1} &= \mathbf{S_A}\mathbf{e}_{4(n-1)+1}, \quad n = 1, 2, \ldots, \#\{-i\} - 1, \\
\mathbf{e}_{4n+2} &= \mathbf{S_A}\mathbf{e}_{4(n-1)+2}, \quad n = 1, 2, \ldots, \#\{-1\} - 1, \\
\mathbf{e}_{4n+3} &= \mathbf{S_A}\mathbf{e}_{4(n-1)+3}, \quad n = 1, 2, \ldots, \#\{i\} - 1,
\end{aligned}$$

em que $\#\{1\}$, $\#\{-i\}$, $\#\{-1\}$ e $\#\{i\}$ são as multiplicidades dos autovalores 1, $-i$, -1 e i, respectivamente, mostrados na Tabela 8, p. 76.

O conjunto ortogonal $\{\mathbf{e}^{\perp}\}_{0\leq m\leq N-1}$ é construído aplicando o algoritmo de Gram-Schmidt em cada um dos autoespaços

$$\{\mathbf{e}_{4n}\}_{0\leq n\leq \#\{1\}-1},\ \{\mathbf{e}_{4n+1}\}_{0\leq n\leq \#\{-i\}-1},\ \{\mathbf{e}_{4n+2}\}_{0\leq n\leq \#\{-1\}-1} \text{ e } \{\mathbf{e}_{4n+3}\}_{0\leq n\leq \#\{i\}-1}.$$

É necessário verificar se os vetores do conjunto construído na Definição 5.1 são linearmente independentes (LI). A verificação pode ser feita checando se $\{\mathbf{e}^{\perp}\}_{0\leq m\leq N-1}$ contém algum vetor nulo. Se a condição de independência linear for satisfeita, usa-se o conjunto $\{\mathbf{e}^{\perp}\}_{0\leq m\leq N-1}$ como colunas de $\tilde{\mathbf{E}}$.

Os passos do algoritmo proposto estão sumarizados na Tabela 11.

Tabela 11 – Algoritmo para construção de uma autobase da FNT.

PASSO	DESCRIÇÃO
1	Definir uma matriz $\mathbf{A}$ seguindo o algoritmo da Seção 5.2.1, para $\gamma = 1$, e usá-la para definir a matriz geradora $\mathbf{S_A} = \mathbf{F}^{-1}\mathbf{A}\mathbf{F} + \mathbf{A}$.
2	Usar o algoritmo da Seção (5.1.3) para construir os *autovetores semente* $\{\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$, cujos autovalores são 1, $-i$, -1 e i, respectivamente.
3	Usar recursivamente $\mathbf{S_A}$ para construir o conjunto $\{\mathbf{e}_m\}_{0\leq m\leq N-1}$ como descrito na Definição 5.1.
4	Aplicar o algoritmo de Gram-Schmidt em cada um dos autoespaços e verificar se o conjunto $\{\mathbf{e}_m^{\perp}\}_{0\leq m\leq N-1}$ é LI. Se não for, repetir os passos 2, 3 e 4.

Fonte: Produzido pelos autores.

5.3 ESQUEMA DE CIFRAGEM DE IMAGENS BASEADA NA 2D-MFRFNT

O sistema de cifragem de imagens baseada na transformada multiparamétrica definida em (5.3) é descrito nesta seção. Este sistema cifra imagens em tons de cinza com dimensões de 512×512 pixels, codificados em 8 bits por pixel (bpp). A flexibilidade do sistema para trabalhar com diferentes tipos de imagens (diferentes dimensões e codificações) é abordada na Seção 5.5.

5.3.1 Uma MFrFNT sobre $\mathbb{F}_{257}$

No sistema proposto, é utilizado $p = 2^8 + 1 = 257$. Uma vez que o comprimento da transformada utilizada no sistema de cifragem é 128, é escolhido $\alpha = 13$, que satisfaz $\text{ord}(\alpha) = 128$, para construir a matriz $\mathbf{F}$ da FNT em (4.2). Para construir a matriz geradora $\mathbf{S_A}$, foi utilizado $\mathbf{A} = \mathbf{C}$, em que $\mathbf{C}$ é um matriz diagonal cujos elementos na $(k + M)$-ésima linha e na $(k + M)$-ésima coluna são dados por $2\cos_{\alpha}(k)$, $k \in I_N$, como definido na Seção 4.2.2.

Tabela 12 – Passos necessários para cifragem e decifragem de uma imagem pelo método proposto.

PASSO	CIFRAGEM	DECIFRAGEM
1	Dividir a imagem original $\mathbf{I}$ de 512×512 pixels, em 16 subimagens com 128×128 pixels: $\mathbf{I}_{r,c}$, $0 \leq r, c \leq 3$.	Dividir a imagem $\mathbf{I}^{'}$ de 512×512 pixels, em 16 subimagens com 128×128 pixels: $\mathbf{I}^{'}_{r,c}$, $0 \leq r, c \leq 3$;.
2	Aplicar a 2D-MFrFNT em cada uma das subimagens: $\mathbf{I^1}_{r,c} = \mathbf{F^a I}_{r,c}\mathbf{F^a}^T$, $0 \leq r, c \leq 3$.	Aplicar a 2D-MFrFNT em cada uma das subimagens: $\mathbf{I^2}_{r,c} = \mathbf{F^{a_d}} \mathbf{I}^{'}_{r,c} \mathbf{F^{a_d}}^T$, $0 \leq r, c \leq 3$, em que $\mathbf{a_d} \equiv -\mathbf{a} \pmod{p}$.
3	Construir a imagem intermediária $\mathbf{I^1}$ usando as subimagens $\mathbf{I^1}_{r,c}$, $0 \leq r, c \leq 3$.	Construir a imagem intermediária $\mathbf{I^2}$ usando as subimagens $\mathbf{I^2}_{r,c}$, $0 \leq r, c \leq 3$.
4	Realizar o embaralhamento dos pixels de $\mathbf{I^1}$ correspondente à aplicação da transformada de Arnold com 3 iterações, gerando a imagem intermediária $\mathbf{I^2}$.	Realizar o desembaralhamento dos pixels de $\mathbf{I^2}$ correspondente à aplicação da transformada de Arnold inversa com 3 iterações, gerando a imagem intermediária $\mathbf{I^1}$.
5	Dividir $\mathbf{I^2}$ em 16 subimagens 128×128 cada, $\mathbf{I^2}_{r,c}$, $0 \leq r, c \leq 3$.	Dividir $\mathbf{I^1}$ em 16 subimagens 128×128 cada, $\mathbf{I^1}_{r,c}$, $0 \leq r, c \leq 3$.
6	Aplicar novamente a 2D-MFrFNT a cada uma das subimagens: $\mathbf{I}^{'}_{r,c} = \mathbf{F^a I^2}_{r,c} \mathbf{F^a}^T$, $0 \leq r, c \leq 3$.	Aplicar novamente a 2D-MFrFNT a cada uma das subimagens: $\mathbf{I}_{r,c} = \mathbf{F^{a_d}} \mathbf{I^1}_{r,c} \mathbf{F^{a_d}}^T$, $0 \leq r, c \leq 3$, em que $\mathbf{a_d} \equiv -\mathbf{a} \pmod{p}$.
7	Construir a imagem cifrada $\mathbf{I}^{'}$ usando as subimagens $\mathbf{I}^{'}_{r,c}$, $0 \leq r, c \leq 3$.	Construir a imagem decifrada $\mathbf{I}$ usando as subimagens $\mathbf{I}_{r,c}$, $0 \leq r, c \leq 3$.

Fonte: Produzido pelos autores.

A sequência gerada randomicamente

$$\begin{aligned}\mathbf{d} = [&170,\ 141,\ 171,\ 0,\ 29,\ 115, 168,\ 131,\ 50,\ 216,\ 92,\ 52,\ 154,\ 127,\ 118,\ 244,\ 146,\ 228,\ 6,\\ &52,\ 222,\ 80,\ 120,\ 112,\ 216,\ 247,\ 121,\ 27,\ 228,\ 139,\ 83,\ 86,\ 171,\ 23,\ 207,\ 84,\ 190,\\ &190,\ 39,\ 182,\ 202,\ 28,\ 251,\ 220,\ 192,\ 177,\ 21,\ 247,\ 168,\ 1, 224,\ 163,\ 255,\ 239,\ 41,\\ &161,\ 61,\ 208,\ 53,\ 108,\ 58,\ 12,\ 149]\end{aligned}$$

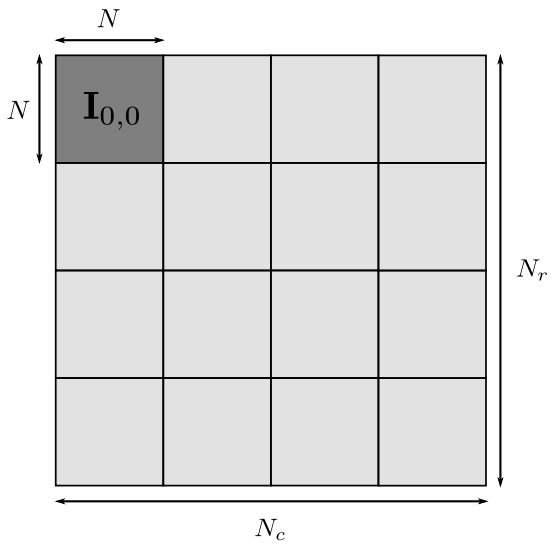
é usada para obter o vetor com simetria par $\mathbf{d}_e$ e o vetor com simetria ímpar $\mathbf{d}_o$ usados para construir os *vetores semente* $\{\mathbf{e}_n\}_{0 \leq n \leq 3}$.

Utiliza-se o algoritmo apresentado na Seção 5.2.2, para construção do conjunto $\{\mathbf{e}_m^{\perp}\}_{0 \leq m \leq N-1}$ usado na definição da matriz $\mathbf{F^a} = \tilde{\mathbf{E}}\mathbf{D}\mathbf{\Lambda^a}\tilde{\mathbf{E}}^T$. Neste caso, $\mathbf{a}$ é o vetor de ordens fracionárias com componentes $a_j = \frac{b_j}{c_j}$, para $1 \leq j \leq 128$. No sistema, valor de c_j é fixado em $c_j = c = 64$, de modo que $\mathbf{a} = \frac{1}{c}\mathbf{b}$ e o vetor $\mathbf{b}$ é a chave secreta do esquema. Em outras palavras, o vetor $\mathbf{b}$ é formado por cada um dos numeradores b_j de cada um dos elementos do vetor $\mathbf{a}$. Assumindo que cada componente b_j corresponde a um número inteiro de 0 a 63, a chave $\mathbf{b}$ possui $128 \times 6 = 768$ bits.

5.3.2 Esquema de Cifragem e Decifragem

Os passos necessários para cifragem e decifragem de uma imagem são apresentados na Tabela 12, em que $\mathbf{I}$ é uma imagem original, $\mathbf{I}^{'}$ é a imagem cifrada, e $\mathbf{I^1}$ e $\mathbf{I^2}$ são imagens intermediárias. As subimagens usadas nos passos intermediários são obtidas por uma divisão da imagem original como mostrado na Figura 24.

Figura 24 – Subimagens $\mathbf{I}_{r,c}$, $0 \leq r, c \leq 3$, de uma imagem $\mathbf{I}$.



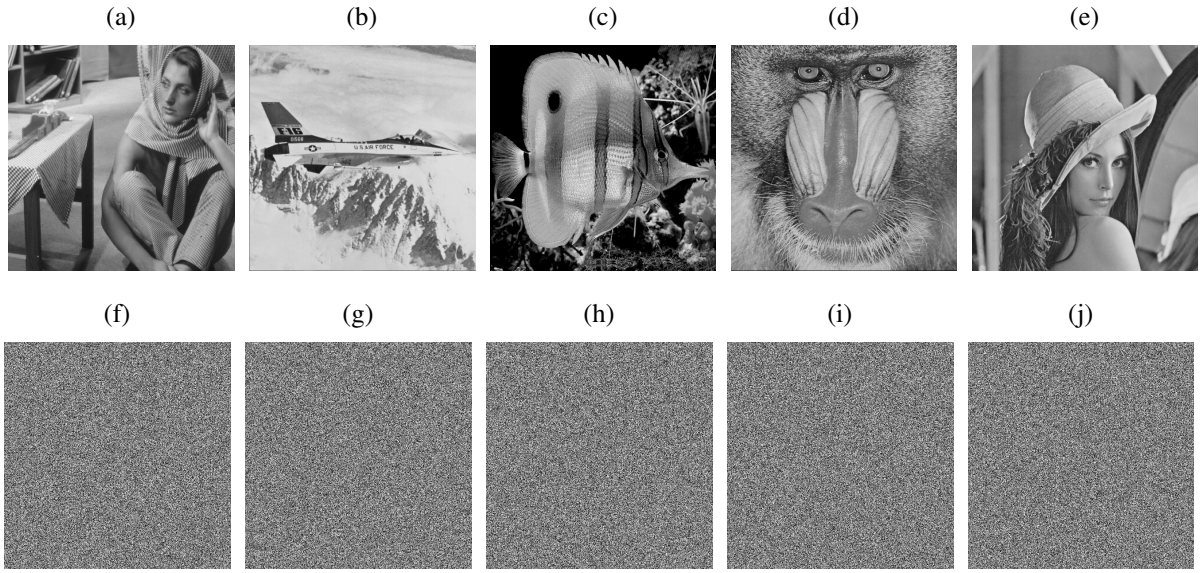
Fonte: Produzido pelos autores.

5.4 EXPERIMENTOS E ANÁLISES DE SEGURANÇA

Nesta seção, os testes realizados para caracterizar o esquema proposto e avaliar a sua segurança são apresentados. Foi utilizado o SageMath[3] para implementar o esquema de cifragem e foram utilizadas nos testes imagens padrão de tamanho 512×512 pixels em tons de cinza (DATASET. . . ,). Nas Figuras 25a-25e são mostradas as imagens originais: $\mathbf{I}_a$, $\mathbf{I}_b$, $\mathbf{I}_c$, $\mathbf{I}_d$ e $\mathbf{I}_e$; nas Figuras 25f-25j, são mostradas suas respectivas versões cifradas, $\mathbf{I}'_a$, $\mathbf{I}'_b$, $\mathbf{I}'_c$, $\mathbf{I}'_d$ e $\mathbf{I}'_e$. Nas seções seguintes são mostrados os testes realizados no sistema de cifragem proposto tendo como base os testes encontrados na literatura relacionada (LIU; LIU, 2007; SINGH; SINHA, 2008; LIU et al., 2012; LANG, 2012; RAN et al., 2014; LANG, 2015; ELHOSENY et al., 2016; ZHAO et al., 2016b; LI et al., 2015; VAISH; KUMAR, 2017; PEI; WEN; DING, 2008; PEI; HSUE, 2009; TAO; MENG; WANG, 2010; HSUE; CHANG, 2015b; LIU et al., 2015; KANG; ZHANG; TAO, 2015b; KANG; TAO; ZHANG, 2016; ANNABY; RUSHDI; NEHARY, 2016b; PEI; HSUE, 2006; PEI; WEN; DING, 2011; LIMA; NOVAES, 2014; LIMA; CAMPELLO DE SOUZA, 2016; LIMA; LIMA; CAMPELLO DE SOUZA, 2017; MIKHAIL; ABOUELSEOUD;

[3] SageMath é um *framework open source* escrito na linguagem de programação Phyton. Mais informações podem ser encontradas em: <http://www.sagemath.org/>.

Figura 25 – Imagens: (a)-(e) originais; (f)-(j) cifradas.



Fonte: Produzido pelos autores.

ELKOBROSY, 2017; LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; ECRYPT II, 2012; TAO; LANG; WANG, 2009; WU; NOONAN; AGAIAN, 2011; KANG; MING; TAO, 2018; KANG; TAO, 2018).

5.4.1 Análise estatísticas

Uma análise preliminar do esquema pode ser feita pela observação do histograma das imagens antes e após a cifragem (ver Figura 26). Analisando estes histogramas nota-se que, independentemente do histograma da imagem original, Figuras 26a-26e, o histograma da imagem cifrada correspondente possui aspecto próximo ao de uma distribuição uniforme, Figuras 26f-26j.

Informações adicionais podem ser adquiridas pelo cálculo do coeficiente de correlação entre pixels adjacentes da imagem. Seja x_n o valor do n-ésimo pixel, y_n o valor do n-ésimo pixel adjacente, P o número total de pixels da imagem, e $E(x)$ o valor esperado para um pixel, dado por

$$E(x) = \frac{1}{P}\sum_{n=1}^{P} x_n.$$

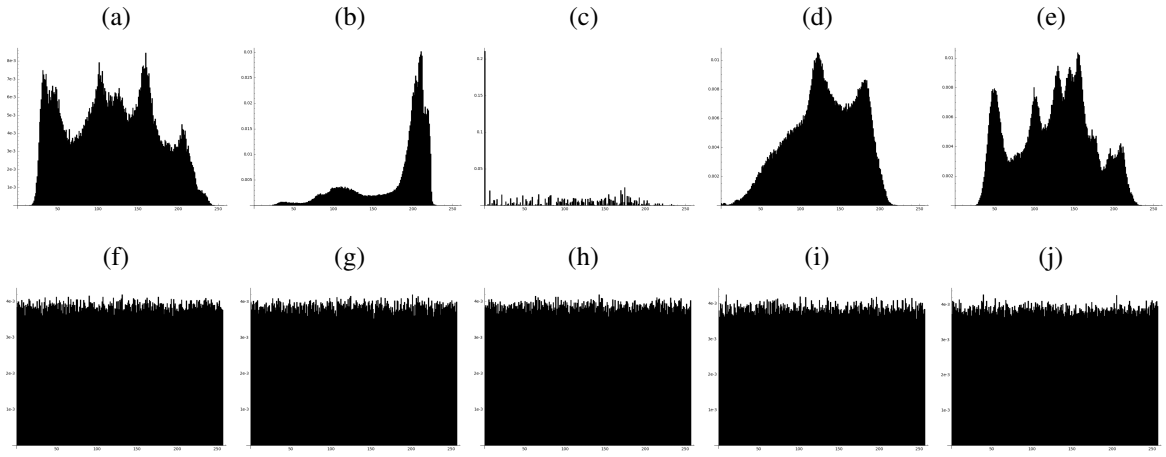
O coeficiente de correlação entre dois pixels adjacentes x e y, em que essa adjacência pode ser horizontal, vertical ou diagonal, é dado por

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{\text{var}(x)\text{var}(y)}},$$

em que

$$\text{cov}(x,y) = \frac{1}{P}\sum_{n=1}^{P}(x_n - E(x))(y_n - E(y)),$$

Figura 26 – Histogramas: (a)-(e) imagens originais; (f)-(j) imagens cifradas.



Fonte: Produzido pelos autores.

$$\text{var}(x) = \frac{1}{P}\sum_{n=1}^{P}(x_n - E(x))^2.$$

É esperado que o coeficiente de correlação de uma imagem original seja próximo de 1. Por outro lado, é desejável que o coeficiente de correlação entre os pixels da imagem cifrada seja próximo de 0. Na Tabela 13, são mostrados os valores calculados para cada um dos coeficientes de correlação para as imagens $\mathbf{I}_a$, $\mathbf{I}_b$, $\mathbf{I}_c$, $\mathbf{I}_d$ e $\mathbf{I}_e$, assim como para as suas respectivas versões cifradas. Como desejado, o valor para cada uma das imagens cifradas é próximo de zero com pelo menos duas casas decimais.

Tabela 13 – Coeficiente de correlação dos pixels das imagens originais (r_{xy}) e o correspondente das imagens cifradas (r'_{xy}); (v), (h) e (d) são relacionados à adjacência vertical, horizontal e diagonal, respectivamente.

Metric	$\mathbf{I}_a$	$\mathbf{I}_b$	$\mathbf{I}_c$	$\mathbf{I}_d$	$\mathbf{I}_e$
$r_{xy}(h)$	0,96261	0,95982	0,96176	0,75450	0,98748
$r'_{xy}(h)$	0,00293	0,00119	0,00124	−0,00084	−0,00089
$r_{xy}(v)$	0,89325	0,96793	0,95938	0,86947	0,97151
$r'_{xy}(v)$	0,00356	0,00162	0,00021	0,00281	−0,00284
$r_{xy}(d)$	0,88093	0,93160	0,93819	0,72204	0,96103
$r'_{xy}(d)$	0,00263	−0,00045	−0,00308	0,00257	0,00397

Fonte: Produzido pelos autores.

5.4.2 Robustez a ataques diferenciais

Para avaliar a robustez do esquema em relação a ataques diferenciais é necessário comparar imagens cifradas geradas a partir de imagens originais minimamente diferentes. Neste

caso, é desejável que as imagens cifradas sejam consideravelmente diferentes. Para medir essa diferença são utilizadas duas métricas: o taxa do número de pixels modificados (NPCR, do inglês *number of pixels change rate*), e a intensidade média de mudança unificada (UACI, do inglês *unified average changing intensity*) (WU; NOONAN; AGAIAN, 2011). Sejam $I^{'}(n,k)$ e $I^{''}(n,k)$ os valores dos pixels na (n,k)-ésima posição das imagens cifradas $\mathbf{I}^{'}$ e $\mathbf{I}^{''}$, respectivamente, com as imagens originais correspondentes diferindo em apenas um bit menos significativo (LSB, do inglês *least significant bit*) de um dos pixels da imagem. Seja $D(n,k)$ definido como

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

As métricas NPCR e UACI são definidas como

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

e

$$\mathbf{UACI} = \frac{1}{N_r \times N_c} \left[\frac{\sum_{n,k} |I^{'}(n,k) - I^{''}(n,k)|}{p-1} \right] \times 100\%,$$

em que N_r e N_c são o número de linhas e colunas, respectivamente.

Nos testes realizados, para cada uma das imagens originais $\mathbf{I}_a$, $\mathbf{I}_b$, $\mathbf{I}_c$, $\mathbf{I}_d$ e $\mathbf{I}_e$, foram geradas 100 imagens modificadas. Estas imagens modificadas diferem da imagem original apenas no LSB de apenas um pixel da imagem escolhido aleatoriamente. Utilizando a versão cifrada da imagem original $\mathbf{I}^{'}$ e a versão cifrada da imagem modificada correspondente $\mathbf{I}^{''}$ são calculados o NPCR e o UACI para cada uma das 100 imagens modificadas. Na Tabela 14, são mostrados os valores máximos, mínimos e médios para o NPCR e o UACI para as imagens $\mathbf{I}_a$, $\mathbf{I}_b$, $\mathbf{I}_c$, $\mathbf{I}_d$ e $\mathbf{I}_e$. Observa-se que os valores são próximos aos valores desejados: $\mathbf{NPCR} \approx 99{,}61\%$ e $\mathbf{UACI} \approx 33{,}46\%$ (WU; NOONAN; AGAIAN, 2011); mais especificamente, dentro dos valores limites indicados nas Tabelas I e II de (WU; NOONAN; AGAIAN, 2011) para imagens em tons de cinza de dimensões 512×512 com um grau de significância (*significance level*) de $0{,}001$.

5.4.3 Espaço de chaves e sensibilidade da chave

O espaço de chaves de um sistema de cifragem precisa ser grande o suficiente para tornar o ataque por força bruta impraticável. No sistema proposto, cada componente da chave secreta, os elementos do vetor $\mathbf{b}$, é uma palavra de 6 bits. Como o vetor $\mathbf{b}$ possui 128 elementos, a chave secreta possui 768 bits, que é consideravelmente maior que o valor mínimo sugerido na literatura (ECRYPT II, 2012).

Além de calcular o tamanho da chave secreta, é necessário verificar a sensibilidade da chave, sendo desejável que esta seja alta. Para isso, pode-se cifrar a imagem original com a chave secreta

$$\mathbf{b} = [\ 6 \quad 6 \quad 13 \quad \ldots \quad \underline{56} \quad \ldots \quad 24 \quad 24 \quad 44\ ],$$

Tabela 14 – Valores mínimo (min.), máximo (max.) e médio (avg.) do NPCR e do UACI obtidos nos experimentos.

Médida	$\mathbf{I}_a$	$\mathbf{I}_b$	$\mathbf{I}_c$	$\mathbf{I}_d$	$\mathbf{I}_e$
NPCR					
avg.	99,60950	99,61103	99,61015	99,61189	99,61077
min.	99,58649	99,58687	99,58000	99,58343	99,57161
max.	99,64523	99,64523	99,63875	99,63493	99,64943
UACI					
avg.	33,44647	33,50081	33,45211	33,46131	33,45628
min.	33,32290	33,41306	33,34930	33,34606	33,35870
max.	33,55878	33,57132	33,55477	33,56346	33,58874

Fonte: Produzido pelos autores.

por exemplo, e decifrar a imagem com uma chave com um bit de erro:

$$\mathbf{b}'' = [\ 6 \quad 6 \quad 13 \quad \ldots \quad \underline{57} \quad \ldots \quad 24 \quad 24 \quad 44\ ].$$

Nos testes realizados, foi utilizada uma chave gerada randomicamente para cifrar as imagens originais e a mesma chave com o LSB modificado de uma das componentes do vetor $\mathbf{b}$. A Figura 27 mostra os resultados: nas Figuras 27a-27e, são mostradas as imagens decifradas com a chave errada, $\mathbf{I}''_a$, $\mathbf{I}''_b$, $\mathbf{I}''_c$, $\mathbf{I}''_d$ e $\mathbf{I}''_e$, respectivamente, e nas Figuras 27f-27j são mostrados seus respectivos histogramas. Como desejado, observa-se que, se mudado apenas um bit menos significativo de uma das componentes da chave secreta, não é possível ter acesso a nenhuma parte da imagem original ou informação sobre a chave secreta.

A avaliação pode ser complementada pelo cálculo do NCPR, introduzido na Seção 5.4.2, entre a imagem original e imagem decifrada correspondente com uma chave com um bit de erro. A partir da chave correta, foram geradas 128 chaves com um bit errado, modificando o LSB de cada uma das componentes do vetor chave $\mathbf{b}$. Isso é, a primeira chave errada em um bit é gerada modificando o LSB da primeira componente do vetor $\mathbf{b}$, b_1; a segunda chave com um bit de erro é gerada modificando o LSB de b_2, e assim por diante. Na Tabela 15, são mostrados os valores mínimos, máximos e médios do NPCR calculado para cada uma das imagens $\mathbf{I}_a$, $\mathbf{I}_b$, $\mathbf{I}_c$, $\mathbf{I}_d$ e $\mathbf{I}_e$ e as respectivas 128 versões decifradas com as chaves com um bit de erro. Como desejado, todos os valores são próximos a 99.61% (acima do valor limite indicado na Tabela I em (WU; NOONAN; AGAIAN, 2011) para imagens em tons de cinza de dimensões 512×512 com um grau de significância de $0{,}001$).

5.4.4 Entropia Normalizada

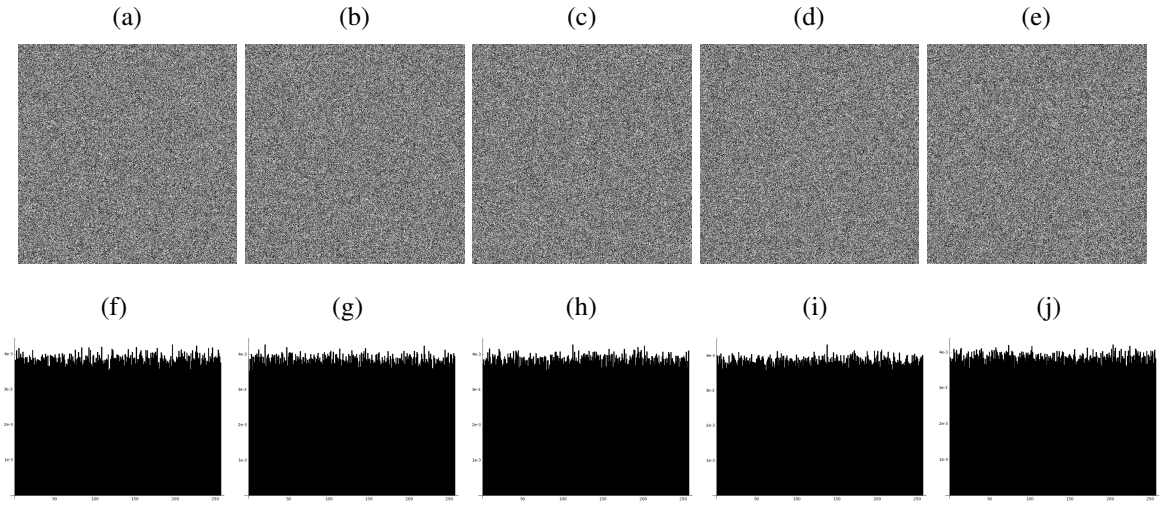
Dado que p é o número de diferentes valores que um pixel pode assumir no domínio da transformada empregada no presente esquema de cifragem, denota-se por N_n o número de

Tabela 15 – Valores mínimo (min.), máximo (max.) e médio (avg.) do NPCR obtido no experimento de sensibilidade da chave.

NPCR	$\mathbf{I}_a$	$\mathbf{I}_b$	$\mathbf{I}_c$	$\mathbf{I}_d$	$\mathbf{I}_e$
avg.	99,61189	99,61127	99,61140	99,60979	99,61109
min.	99,57275	99,57314	99,58191	99,57657	99,58344
max.	99,64409	99,63913	99,64294	99,64027	99,63493

Fonte: Produzido pelos autores.

Figura 27 – Imagens decifradas com uma chave com um bit de erro: (a)-(e) imagens; (f)-(j) histogramas.



Fonte: Produzido pelos autores.

pixels que assumem um valor específico n, $0 \leq n < p-1$, por N_T o total de pixels da imagem. A entropia da imagem é calculada por

$$H = \sum_{n=0}^{p-1} \frac{N_n}{N_T} \log_2 \frac{N_T}{N_n}.$$

O valor resultante da entropia pertence ao intervalo $[0; \log_2(p)]$.

Como os valores dos pixels das imagens originais se encontram no intervalo [0,255] (8 bpp) e os das imagens cifradas em [0,256], para comparar de forma equânime suas entropias, é usada a versão normalizada definida por

$$\overline{H} = \frac{\sum_{n=0}^{p-1} \frac{N_n}{N_T} \log_2 \frac{N_T}{N_n}}{\log_2 p}$$

e pertence ao intervalo $[0; 1]$.

É desejável que cada pixel da imagem cifrada tenha a mesma probabilidade de assumir qualquer um dos valores possíveis. Neste caso, a entropia normalizada terá um valor próximo

Tabela 16 – Entropia normalizada das imagens originais ($\overline{H}$), das imagens cifradas correspondentes ($\overline{H}^{'}$), e das imagens decifradas com uma chave com um bit de erro ($\overline{H}^{''}$).

Metric	$\mathbf{I}_a$	$\mathbf{I}_b$	$\mathbf{I}_c$	$\mathbf{I}_d$	$\mathbf{I}_e$
$\overline{H}$	0,95334	0,83412	0,75162	0,91910	0,93003
$\overline{H}^{'}$	0,99990	0,99991	0,99992	0,99991	0,99991
$\overline{H}^{''}$	0,99991	0,99992	0,99991	0,99992	0,99993

Fonte: Produzido pelos autores.

de 1. Na Tabela 16, são mostrados os valores calculados da entropia normalizada para as imagens originais ($\overline{H}$), cifradas ($\overline{H}^{'}$) e decifradas com uma chave com um bit de erro ($\overline{H}^{''}$) (ver Seção 5.4.3). Como desejado, os valores da entropia normalizada são próximos a 1 para as versões cifradas e decifradas com uma chave errada.

5.4.5 Robustez a ataques clássicos

As investigações realizadas sugerem que o esquema proposto é resistente aos ataques de texto-claro conhecido (imagem original conhecida) e texto-claro escolhido (imagem original escolhida). O adversário poderia, por exemplo, escolher uma imagem cujas subimagens correspondessem à matriz identidade, com o intuito de tentar revelar a matriz $\mathbf{F^a}$ da transformada que é dependente da chave secreta (Passo 2, Tabela 12). Contudo, desde que o adversário não tem acesso à imagem intermediária $\mathbf{I^1}$ (Passo 3, Tabela 12), que, na sequência, segue para um estágio de permutação (Passo 4, Tabela 12) e para a segunda rodada de transformações (Passo 6, Tabela 12), esta estratégia é reduzida ao caso de ataque por força bruta e a possibilidade de sucesso é consideravelmente reduzida. A segurança do esquema pode ser aumentada ainda mais combinando permutações e transformações de maneiras diferentes.

5.5 FLEXIBILIDADE DO ESQUEMA

Nas seções anteriores, foi apresentado o esquema proposto e suas partes. Nesta seção, para demonstrar a flexibilidade do sistema, é descrito como suas partes podem ser ajustadas para tratar tipos específicos de imagens. Entre as possibilidades, é mostrado como mudar o tamanho da chave e como usar o esquema para cifrar imagens com diferentes tamanhos. Além disso, o esquema proposto é comparado com outros sistemas de cifragem de imagem que utilizam transformadas fracionárias.

5.5.1 Flexibilidade do tamanho da chave secreta

Foi mostrado na Seção 5.4.3 que o esquema proposto utiliza uma chave de 768 bits, que é grande o suficiente para resistir contra ataques por força bruta (ECRYPT II, 2012). Contudo,

Tabela 17 – Métricas obtidas nos experimentos para o esquema trabalhando com uma chave secreta de 128 bits.

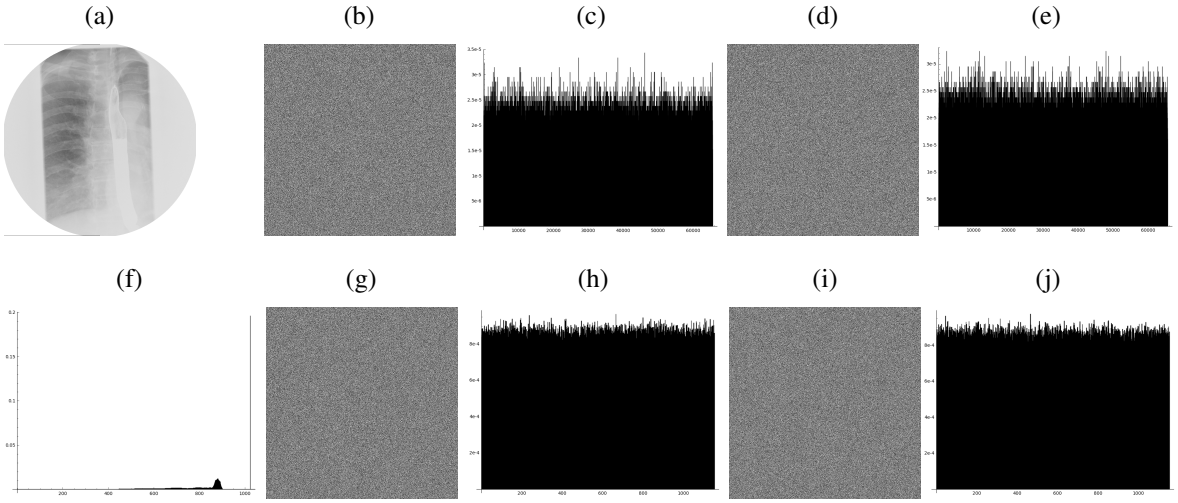
Medida	$\mathbf{I}_a$	$\mathbf{I}_b$	$\mathbf{I}_c$	$\mathbf{I}_d$	$\mathbf{I}_e$
Ataque Diferencial					
NPCR					
avg.	99,61277	99,61010	99,61106	99,61263	99,61130
min.	99,58839	99,58878	99,58267	99,58420	99,58725
max.	99,64447	99,64142	99,63684	99,64523	99,63989
UACI					
avg.	33,44941	33,45314	33,47074	33,46356	33,44975
min.	33,34999	33,36303	33,35508	33,35961	33,32841
max.	33,56247	33,54445	33,56679	33,57181	33,53861
Sensibilidade da Chave (NPCR)					
avg.	99,61156	99,61047	99,60995	99,60955	99,60708
min.	99,58534	99,58191	99,57771	99,57542	99,57428
max.	99,64638	99,63684	99,64066	99,63837	99,65362
Coeficiente de Correlação					
$r'_{xy}(h)$	0,00389	0,00371	−0,00082	0,00009	−0,00462
$r'_{xy}(v)$	−0,00425	−0,00175	0,00104	−0,00145	−0,00431
$r'_{xy}(d)$	−0,00641	0,00063	0,00073	−0,00225	−0,00121
Entropia Normalizada					
$\overline{H}'$	0,99992	0,99991	0,99991	0,99992	0,99992
$\overline{H}''$	0,99991	0,99991	0,99991	0,99992	0,99999

Fonte: Produzido pelos autores.

este tamanho de chave pode ser muito grande para alguns cenários práticos; ela pode ocupar, por exemplo, muito espaço de memória para ser salva em aplicações de baixo custo, ter um tempo de transmissão proibitivo etc. Este problema pode ser solucionado pelo uso de menos bits para representar os elementos do vetor chave secreta $\mathbf{b}$. Isso é, cada elemento b_j, $1 \leq j \leq N$, pode ser representado por uma palavra de k bits, $1 \leq k \leq 6$. Consequentemente, a chave terá um tamanho de $k \times 128$ bits.

De qualquer forma, deve-se evitar utilizar um elemento $b_j = 0$, porque, neste caso, tem-se $\lambda_{j,j}^{\frac{0}{c}} = 1$, o que pode representar uma fraqueza do sistema. Equivalentemente, deve-se apenas evitar que $a_j = \frac{b_j}{c} = 0$. Para $k = 1$, por exemplo, isso pode ser feito usando $a_j = \frac{1+b_j}{c}$. Neste caso, ainda se tem um bit por elemento do vetor chave $\mathbf{b}$, que é $b_j \in \{0, 1\}$, embora os valores efetivos usados no esquema se encontrem no conjunto $\{1, 2\}$. Para mostrar a força do esquema modificado, são mostradas na Tabela 17 as métricas obtidas para o esquema para $k = 1$.

Figura 28 – (a) Imagem no formato DICOM. (f) Histograma da imagem DICOM. Para os esquemas modificados para usar $p = 65537$ e $p = 1153$, respectivamente: (b) e (g) imagens cifradas; (c) e (h) histogramas da imagens cifradas; (d) e (i) imagens decifradas com uma chave com um bit de erro; (e) e (j) histogramas das imagens decifradas com uma chave com um bit de erro.



Fonte: Produzido pelos autores.

5.5.2 Imagens de tipos e tamanhos diferentes

Embora imagens com dimensões 512×512 e com 8 bpp sejam comuns em cenários práticos, existem vários padrões de imagem. Então, é interessante mostrar que o esquema proposto pode ser facilmente modificado para lidar com diferentes tipos e tamanhos de imagem. Imagens coloridas no padrão RGB, por exemplo, são compostas por 3 camadas, cada uma sendo responsável por representar a intensidade de uma das cores R(ed), G(reen) ou B(lue) (vermelho, verde ou azul em inglês, respectivamente). Para este tipo de imagem, apenas é necessário realizar cifragem/decifragem em cada uma das camadas da imagem. A mesma estratégia pode ser utilizada para outros padrões de imagem multicamada.

Por outro lado, para imagens cujos pixels são codificados em n-bits com $n > 8$, são necessárias maiores modificações. Por exemplo, imagens no padrão DICOM (DICOM...,) possuem cada pixel codificado em uma palavra de 16 bits. Uma modificação possível para o sistema é a utilização de $p = 2^{16} + 1 = 65537$; consequentemente, cada pixel cifrado será codificado em uma palavra de 17 bits. Como um exemplo, o esquema foi modificado para cifrar a imagem com 1024×1024 pixels no formato DICOM mostrado na Figura 28a. Foi empregado $p = 65537$, $\alpha = 13987$ com $\text{ord}(\alpha) = 128$, $\mathbf{A} = \mathbf{C}$ e o mesmo vetor $\mathbf{d}$ para construir os *autovetores sementes* para obter a MFrFNT de 128 pontos usada no esquema. A imagem original é dividida em 64 subimagens nos passos de transformação.

Para garantir que no passo de embaralhamento os pixels de cada uma das subimagens são espalhadas por todas as outras subimagens, é utilizado o embaralhamento correspondente

a aplicação da transformada de Arnold com 5 iterações. Nas Figuras 28b-28e, são mostrados os resultados para o esquema de cifragem modificado. Nas Figuras 28b e 28c, tem-se a versão cifrada da imagem e seu histograma; a versão decifrada com uma chave com um bit de erro e seu histograma são mostrados na Figura 28d e 28e, respectivamente.

Em cenários práticos, imagens DICOM podem usar menos que os 16 bits para codificar cada pixel (ver o histograma na Figura 28f). Por exemplo, na imagem testada, cada pixel usa apenas 10 bits. Então, é possível utilizar um primo p menor que 65537 no esquema, permitindo reduzir o número de bits necessários para codificar a imagem cifrada. Pode-se usar, por exemplo, $p = 3^2 \times 2^7 + 1 = 1153$. Neste caso, o esquema seria implementado com $N = 64$, $\alpha = 943$ com $\text{ord}(\alpha) = 64$, $c = 32$, a transformada de Arnold com 5 iterações, $\mathbf{A} = \mathbf{C}$ e

$$\begin{aligned}\mathbf{d} =&[8,\ 864,\ 879,\ 639,\ 658,\ 589,\ 110,\ 450,\ 457,\ 271,\ 457,\ 656,\ 732,\ 652,\ 72,\ 392,\ 598,\ 113,\\ &404,\ 547,\ 299,\ 532,\ 844,\ 520,\ 630,\ 891,\ 991,\ 749,\ 658,\ 51,\ 156]\end{aligned}$$

usado na construção dos *autovetores semente*. Como resultado, cada pixel da imagem cifrada é codificado em uma palavra de 11 bits, ao invés dos 16 bits da imagem original ou os 17 bits da solução prévia. Os resultados são mostrados nas Figuras 28g-28j. Nas Figuras 28g e 28h, são mostrados a imagem cifrada e seu histograma; a imagem decifrada com uma chave com um bit de erro e seu histograma são mostrados nas Figuras 28i e 28j, respectivamente.

5.5.3 Comparação com métodos existentes na literatura

Na Tabela 18, são apresentados concisamente os valores das medidas consideradas na análise do sistema proposto; elas são comparadas com as obtidas por algoritmos de cifragem de imagem encontrados na literatura e que também são baseados em transformadas fracionárias (LIU et al., 2015; ANNABY; RUSHDI; NEHARY, 2016b; KANG; MING; TAO, 2018; KANG; TAO, 2018; LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017; LIMA; NOVAES, 2014; LIMA; CAMPELLO DE SOUZA, 2016; LIMA; LIMA; CAMPELLO DE SOUZA, 2017). Nota-se que o método proposto possui resultados entre os melhores mostrados na tabela.

Além do mais, diferentemente dos esquemas baseados em transformadas definidas sobre o corpo dos reais ou complexos (LIU et al., 2015; ANNABY; RUSHDI; NEHARY, 2016b; KANG; MING; TAO, 2018; KANG; TAO, 2018), o esquema proposto neste trabalho não necessita de um estágio de arredondamento e sendo livre de erros de precisão. Esta propriedade, que se deve ao fato de todas as operações no algoritmo proposto serem feitas utilizando aritmética modular apenas, tem duas consequências: (i) se a chave estiver correta, a imagem original é perfeitamente recuperada a partir da imagem cifrada correspondente; (ii) a imagem cifrada possui apenas componentes inteiras usando um número de bits por pixel igual ao que é usado para representar a imagem original[4]. Isso elimina a necessidade de empregar estratégias de

[4] Se $p = 257$, por exemplo, como considerado na Seção 5.3 and 5.4, as imagens cifradas também podem ser

Tabela 18 – Comparação com outros esquemas de cifragem de imagem que também empregam transformadas fracionárias.

Algoritmos	Espaço de Chaves	$\lvert r'_{xy} \rvert$	$\mathbf{NPCR}_d$	$\mathbf{UACI}_d$	$\overline{H}'$
Proposto	$2^{128} - 2^{768}$	$0{,}00009 - 0{,}00641$	$99{,}57161 - 99{,}64943$	$33{,}32290 - 33{,}58874$	$0{,}99990 - 0{,}99999$
Ref.(LIU et al., 2015)	$51^{290\times290} \times 10^{15}$	$0{,}00450 - 0{,}04720$	–	–	–
Ref.(ANNABY; RUSHDI; NEHARY, 2016b)	–	$0{,}00982 - 0{,}39088$	100	$33{,}2440 - 33{,}4520$	$0{,}99965 - 0{,}99967$
Ref.(KANG; MING; TAO, 2018)	$\approx 2^{325}$	$0{,}00016 - 0{,}00842$	$99{,}9901 - 99{,}9981$	$33{,}3036 - 33{,}3403$	–
Ref.(KANG; TAO, 2018)	–	$0{,}00010 - 0{,}00910$	$99{,}8577 - 99{,}9977$	$26{,}1648 - 33{,}3389$	–
Ref.(LIMA; LIMA; MADEIRO, 2013)	$\approx 2^{118}$	$0{,}00000 - 0{,}00860$	$99{,}5716 - 99{,}6387$	$33{,}2941 - 33{,}6021$	$0{,}99990 - 0{,}99992$
Ref.(LIMA; MADEIRO; SALES, 2015)	2^{160}	$0{,}00010 - 0{,}01320$	$99{,}5750 - 99{,}9939$	$33{,}1915 - 33{,}5556$	$0{,}99820 - 0{,}99990$
Ref.(MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017)	2^{71}	$0{,}00010 - 0{,}00910$	$99{,}5449 - 99{,}7103$	$33{,}4448 - 33{,}5152$	$0{,}99997 - 0{,}99999$
Ref.(LIMA; NOVAES, 2014)	2^{140}	$0{,}00050 - 0{,}01680$	$98{,}1977 - 99{,}0686$	$32{,}9900 - 33{,}3013$	$0{,}99990 - 0{,}99991$
Ref.(LIMA; CAMPELLO DE SOUZA, 2016)	2^{192}	0,00650	99,6098	33,4853	0,99934
Ref.(LIMA; LIMA; CAMPELLO DE SOUZA, 2017)	2^{240}	0,00010	$99{,}6065 - 99{,}6307$	$33{,}4300 - 33{,}4765$	0,99990

Fonte: Produzido pelos autores.

preservação de realidade (não ter como resultado uma imagem com componentes complexas) e truncamento, e evita alta taxa de bits na representação das imagens cifradas. Finalmente, quando comparado com as abordagens definidas sobre corpos finitos (LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017; LIMA; NOVAES, 2014; LIMA; CAMPELLO DE SOUZA, 2016; LIMA; LIMA; CAMPELLO DE SOUZA, 2017), o sistema proposto possui possui medidas semelhantes, quando não melhores, e traz o estudo sobre a flexilidade em relação ao comprimento da chave, às dimensões da imagem e ao tipo de codificação, que não é abordado nas referências comparadas.

5.6 CONSIDERAÇÕES

Neste capítulo, foi introduzido um método baseado em matrizes geradoras para construir uma base ortogonal de autovetores da FNT a partir de parâmetros escolhidos. Foi mostrado como definir uma matriz geradora, apontando o número de elementos livres, que podem ser escolhidos, e como, utilizando esta matriz, pode-se construir uma base ortogonal. Esta autobase é usada para definir uma transformada fracionária multiparamétrica numérica de Fourier que é empregada em um esquema de cifragem de imagem. Utilizando métricas encontradas na literatura, foi avaliada a robustez do sistema proposto; os resultados sugerem que o sistema pode ser utilizado em cenários práticos.

representadas usando 8 bpp, como nas imagens originais; alguns poucos bits adicionais seriam suficientes para indicar a presença do pixel 256.

6 CONCLUSÕES

No presente trabalho, foram investigados métodos baseados em fórmulas fechadas para construção de autovetores de transformadas discretas de Fourier definidas sobre o corpo dos reais e sobre corpos finitos; entre os referidos métodos, receberam ênfase aqueles que empregam matrizes geradoras, a partir das quais diversos resultados foram derivados e para os quais várias aplicações foram apresentadas. As contribuições desta tese são sumarizadas a seguir:

1. Foram investigadas propriedades dos autovetores da DFT do tipo Hermite-Gaussiano construídos por fórmulas fechadas. Vários aspectos acerca do método de matrizes geradoras para construção destes autovetores (PEI; CHANG, 2009; PEI; CHANG, 2016) foram esclarecidos e paralelos entre esta metodologia e a proposta em (KUZNETSOV, 2015) foram traçados.

2. Combinando os métodos apresentados em (PEI; CHANG, 2016) e (KUZNETSOV, 2015), um procedimento sistemático para construção de bases de autovetores HGL para qualquer valor de N foi proposto e vários resultados numéricos foram apresentados e analisados.

3. Uma família de matrizes geradoras foi proposta e foi mostrado como utilizá-la para construir, de maneira mais simples, os autovetores apresentados em (KUZNETSOV, 2015).

4. Os autovetores HGL construídos foram utilizados na expansão espectral da matriz $\mathbf{F}$ da DFT e permitiram definir um operador fracionário $\mathbf{F}^a$ correspondente que representa uma versão discreta do operador transformada fracionária de Fourier (FrFT).

5. A fracionarização acima mencionada foi aplicada no cenário de filtragem de sinais no domínio fracionário; mostrou-se que os resultados obtidos são comparáveis àqueles resultantes do uso de outras abordagens encontradas na literatura.

6. Foi introduzido um método para o cálculo eficiente de uma transformada fracionária discreta de Fourier baseada na autodecomposição do operador transformada de Fourier ordinária. Esta abordagem provê uma significativa redução na complexidade aritmética, quando comparada com outros métodos do estado-da-arte, sendo aplicável em determinados cenários práticos.

7. Foi demonstrado que a transformada proposta pode ser aplicada empregando uma estratégia de arredondamento das componentes dos autovetores do tipo Hemite-Gaussiano usados para defini-la, permitindo uma economia de 50% a 80% no número de multiplicações e adições envolvidas no referido cálculo, ao mesmo tempo em que um desempenho satisfatório é mantido.

8. Os métodos propostos para o cálculo eficiente da transformada (com e sem arredondamento) foram empregados nos cenários práticos de filtragem e representação compacta de sinais no domínio fracionário. Os resultados indicaram que os métodos podem ser aplicados sem que o desempenho da transformada seja afetado de forma significativa.

9. Foi apresentado um método de matrizes geradoras para construção de autovetores da transformada numérica de Fourier.

10. Foi definida uma matriz geradora específica $\mathbf{S_C}$ e foi mostrado como, a partir dessa matriz, cria-se a base de autovetores do tipo Hermite-Gaussiano da FNT proposta em (LIMA; CAMPELLO DE SOUZA, 2016).

11. Foi apresentado um algoritmo para criação de matrizes geradoras a partir de parâmetros escolhidos. Foi apresentado um procedimento sistemático, que utiliza as referidas matrizes para a construção de uma base ortogonal de autovetores da FNT.

12. A base de autovetores mencionada foi então utilizada para definir uma MFrFNT; como exemplo de aplicação, foi proposto um esquema de cifragem de imagens. Utilizando medidas para testes de robustez encontrados na literatura, foi mostrado que o esquema tem potencial para ser empregado em cenários práticos.

6.1 TRABALHOS FUTUROS

A seguir, são elencados possíveis desdobramentos do trabalho apresentado:

- Apesar dos Capítulos 2 e 3 abordarem o uso da DFrFT proposta nos cenários de filtragem e representação compacta de sinais no domínio fracionário, outros cenários relacionados, por exemplo, às áreas de processamento de sinais, comunicações, código corretores de erro e criptografia podem ser avaliados (NAMIAS, 1980; WEIMANN et al., 2016; LOHMANN, 1993; OZAKTAS; ZALEVSKY; KUTAY, 2001; LIU; SHERIDAN, 2013; ALMEIDA, 1994; WEI; LI, 2016; LIMA; NOVAES, 2014; WANG et al., 2016; TAO; MENG; WANG, 2011; ZHAO et al., 2016c; LU; XIAO; WEI, 2016; PELICH et al., 2016).

- Encontram-se sob avaliação técnicas para melhorar a estratégia de arredondamento, proposta no Capítulo 3, para obter uma melhor relação entre precisão e complexidade aritmética da aplicação da transformada; o arredondamento pode ser realizado, por exemplo, em diferentes casas decimais para diferentes componentes de autovetores HGL.

- Atualmente, também tem sido considerada a possibilidade de desenvolver arquiteturas de *hardware* para a DFrFT proposta e a avaliação de seu desempenho em cenários distintos dos apresentados neste trabalho.

- As transformadas numéricas possuem uma vasta gama de aplicações além da cifragem de imagem, logo, é interessante estudar o uso das transformadas fracionárias numéricas propostas no Capítulo 4 em cenários tais como processamento de sinais no domínio cifrado (PEDROUZO-ULLOA; TRONCOSO-PASTORIZA; PÉFEZ-GONZÁLEZ, 2017), geração de sequências de espalhamento para canais de acesso múltiplo (SONG et al., 2014a), marca d'água frágil (CINTRA et al., 2009), entre outros.

- Assim como ocorre para transformadas fracionárias definidas sobre o corpo dos reais (ou complexos), também é de interesse propor arquiteturas de *hardware* para o cálculo eficiente das respectivas transformadas definidas sobre corpos finitos (BLAHUT, 2010; DE OLIVEIRA NETO; LIMA, 2018).

- A extensão do método de matrizes geradoras para outras transformadas numéricas, tais como a transformada de Hartley (CAMPELLO DE SOUZA et al., 1998a) e as transformadas trigonométricas (LIMA; CAMPELLO DE SOUZA, 2011) encontra-se sob avaliação. Este estudo terá como apoio trabalhos semelhantes sobre o domínio dos reais (FIGUEIREDO; LIMA; DE OLIVEIRA NETO, 2017a; FIGUEIREDO; LIMA; DE OLIVEIRA NETO, 2017b; LIMA; DE OLIVEIRA NETO; FIGUEIREDO, 2018; DE OLIVEIRA NETO; LIMA; PANARIO, 2018a).

6.2 ARTIGOS RELACIONADOS À TESE

Nesta seção, são listados os artigos publicados e submetidos ao longo do desenvolvimento deste trabalho. As publicações são apresentadas em ordem cronológica e os trabalhos cujo conteúdo é diretamente relacionado a esta tese são marcados em negrito.

Trabalhos publicados em periódicos

- **DE OLIVEIRA NETO, J. R.; LIMA, J. B. Discrete fractional Fourier transforms based on closed-form Hermite-Gaussian-like DFT eigenvectors. IEEE Transactions on Signal Processing, v. 65, n. 23, p. 6171 - 6184, Dec 2017.**

- LIMA, J. B.; DE OLIVEIRA NETO, J. R.; FIGUEIREDO, R. B. A unified approach for defining random discrete fractional transforms. **Optik**, v. 165, p. 388 – 394, 2018. ISSN 0030-4026.

- **DE OLIVEIRA NETO, J. R. de; LIMA, J. B.; PANARIO, D. A generating matrix method for constructing Hermite-Gaussian-like number-theoretic transform eigenvectors. Signal Processing, v. 152, p. 189 - 196, 2018. ISSN 0165-1684**.

- GONDIM, M. A. A; DE OLIVEIRA NETO, J. R.; LIMA, J. B., Steerable Fourier number transform with application to image encryption. **In: Signal Processing: Image Communication**. Aceito para publicação em 17 de Janeiro de 2019.

Trabalhos publicados em anais de eventos

- FIGUEIREDO, R. B. D.; LIMA, J. B.; DE OLIVEIRA NETO, J. R. Matrices generating eigenvectors for constructing fractional trigonometric transforms. **40th International Conference on Telecommunications and Signal Processing (TSP 2017)**, Jul 5-7, 2017, Barcelona, Spain.

- FIGUEIREDO, R. B. D.; LIMA, J. B.; DE OLIVEIRA NETO, J. R. Matrizes geradoras de autovetores para construção de transformadas de Hartley fracionárias. **XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT 2017)**, Sep 3-6, 2017, São Pedro, Brazil.

- **DE OLIVEIRA NETO, J. R.; LIMA, J. B.; PANARIO, D. A family of matrices for generating Hermite-Gaussian-Like DFT eigenvectors. In: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Apr 15-20, 2018. p. 4379–4383, Calgary, Canada.**

- DE OLIVEIRA NETO, J. R.; LIMA, J. B. Hardware architectures for computing 8-point cosine number transform. **In: 2018 IEEE International Symposium on Circuits and Systems (ISCAS)**. May 27-30, 2018. Florence, Italy.

Resumos expandidos publicados em anais de eventos

- **DE OLIVEIRA NETO, J. R.; LIMA, J. B.; PANARIO, D. Matrices for generating eigenvectors of number-theoretic transforms. 2017 5th Global Conference on Signal and Information Processing (GlobalSIP 2017), Nov 14-16, 2017, Montreal, Canada.**

Trabalhos submetidos a periódicos

- **DE OLIVEIRA NETO, J. R.; LIMA, J. B.; PANARIO, D., The design of a novel multiple-parameter fractional number-theoretic transform and its application to image encryption. In: IEEE Transactions on Circuits and Systems for Video Technology. submetido em 22 de agosto de 2018.**

- **DE OLIVEIRA NETO, J. R.; LIMA, J. B.; DA SILVA JR., G. J.; CAMPELLO DE SOUZA, R. M., Computation of an eigendecomposition-based discrete fractional Fourier transform with reduced arithmetic complexity. In: IEEE Transactions on Signal Processing. submetido em 21 de novembro de 2018.**

REFERÊNCIAS

AGARWAL, R.; BURRUS, C. Fast convolution using Fermat number transforms with applications to digital filtering. **IEEE Transactions on Acoustics, Speech, and Signal Processing**, v. 22, n. 2, p. 87–97, Apr 1974. ISSN 0096-3518. Citado 2 vezes nas páginas 18 e 76.

AHMED, N.; NATARAJAN, T.; RAO, K. R. Discrete cosine transform. **IEEE Transactions on Computers**, C-23, n. 1, p. 90–93, Jan 1974. ISSN 0018-9340. Citado na página 17.

ALMEIDA, L. B. The fractional Fourier transform and time-frequency representations. **IEEE Transactions on Signal Processing**, v. 42, n. 11, p. 3084–3091, Nov 1994. Citado 2 vezes nas páginas 24 e 117.

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, Nov 2016. Citado 2 vezes nas páginas 26 e 56.

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, n. Supplement C, p. 25–46, 2016. ISSN 0923-5965. Citado 6 vezes nas páginas 94, 95, 104, 105, 113 e 114.

ARNOLD, V.; AVEZ, A. **Ergodic Problems of Classical Mechanics**. Benjamin: [s.n.], 1968. Citado 2 vezes nas páginas 97 e 98.

BHATTA, I.; SANTHANAM, B. A comparative study of commuting matrix approaches for the discrete fractional Fourier transform. In: **Proc. IEEE Signal Processing and Signal Processing Education Workshop**. Salt Lake City, UT: [s.n.], 2015. Citado 5 vezes nas páginas 24, 25, 26, 56 e 57.

BIRTWISTLE, D. T. The eigenstructure of the number theoretic transforms. **Signal Processing**, v. 4, n. 4, p. 287–294, Jul 1982. Citado 3 vezes nas páginas 76, 96 e 97.

BLAHUT, R. E. **Algebraic codes for data transmission**. [S.l.]: Cambridge University Press, 2003. ISBN 0521553741. Citado 2 vezes nas páginas 20 e 91.

BLAHUT, R. E. **Fast Algorithms for Signal Processing**. [S.l.]: Cambridge University Press, 2010. ISBN 0521190495. Citado 4 vezes nas páginas 18, 20, 91 e 118.

BOUSSAKTA, S.; HOLT, A. In: HAWKES, P. W. (Ed.). **Number Theoretic Transforms and their Applications in Image Processing**. [S.l.]: Elsevier, 1999, (Advances in Imaging and Electron Physics, Supplement C). p. 1 – 90. Citado na página 76.

BOYADJIS, B. et al. Extended selective encryption of H.264/AVC (CABAC)- and HEVC-encoded video streams. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 27, n. 4, p. 892–906, Apr 2017. Citado na página 94.

BRACEWELL, R. N. Discrete Hartley transform. **Journal of the Optical Society of America**, OSA, v. 73, n. 12, p. 1832–1835, Dec 1983. Citado na página 17.

BU, H. et al. A novel SAR imaging algorithm based on compressed sensing. **IEEE Geoscience and Remote Sensing Letters**, v. 12, n. 5, p. 1003–1007, May 2015. Citado na página 72.

BULTHEEL, A.; SULBARAN, H. E. M. Computation of the fractional Fourier transform. **Applied and Computational Harmonic Analysis**, Elsevier BV, v. 16, n. 3, p. 182–202, May 2004. Citado na página 19.

CAMPELLO DE SOUZA, M. M. et al. The discrete cosine transform over prime finite fields. In: **Telecommunications and Networking - 11th International Conference on Telecommunications**. Fortaleza, Brazil: Springer Berlin Heidelberg, 2004. p. 482–487. ISBN 978-3-540-27824-5. Citado na página 18.

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

CAMPELLO DE SOUZA, R. M. et al. Trigonometry in finite fields and a new Hartley transform. In: **1998 IEEE International Symposium on Information Theory, Proceedings.** [S.l.: s.n.], 1998. p. 293. Citado 2 vezes nas páginas 18 e 118.

CAMPELLO DE SOUZA, R. M. et al. Trigonometry in finite fields and a new hartley transform. In: **Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252)**. [S.l.: s.n.], 1998. p. 293. Citado na página 78.

CAMPELLO DE SOUZA, R. M.; H. M. DE OLIVEIRA; KAUFFMAN, A. N. The complex finite field Hartley transform. In: HERTFORDSHIRE (Ed.). **Coding, Communications and Broadcasting**. [S.l.]: Research Studies Press (RSP), John Wiley, 2000. p. 267–276. Citado na página 18.

CANDAN, C. On higher order approximations for Hermite-Gaussian functions and discrete fractional Fourier transforms. **IEEE Signal Processing Letters**, v. 14, n. 10, p. 699–702, Oct 2007. ISSN 1070-9908. Citado 2 vezes nas páginas 56 e 57.

CANDAN, C.; KUTAY, M. A.; OZAKTAS, H. M. The discrete fractional Fourier transform. **IEEE Transactions on Signal Processing**, v. 48, n. 5, p. 1329–1337, May 2000. ISSN 1053-587X. Citado 21 vezes nas páginas 19, 20, 21, 24, 25, 26, 27, 30, 50, 51, 52, 54, 55, 56, 57, 70, 72, 73, 74, 77 e 92.

CHAN, K. S.; FEKRI, F. A block cipher cryptosystem using wavelet transforms over finite fields. **IEEE Transactions on Signal Processing**, v. 52, n. 10, p. 2975–2991, Oct 2004. ISSN 1053-587X. Citado na página 18.

CHEN, S. et al. Automatic detection of object-based forgery in advanced video. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 26, n. 11, p. 2138–2151, Nov 2016. Citado na página 94.

CHEN, X. et al. Maneuvering target detection via radon-fractional Fourier transform-based long-time coherent integration. **IEEE Transactions on Signal Processing**, v. 62, n. 4, p. 939–953, Feb 2014. ISSN 1053-587X. Citado na página 19.

CINTRA, R. J. et al. Fragile watermarking using finite field trigonometrical transforms. **Signal Processing: Image Communication**, v. 24, p. 587–597, Aug 2009. Citado 2 vezes nas páginas 19 e 118.

CLARY, S.; MUGLER, D. H. Shifted Fourier matrices and their tridiagonal commutors. **SIAM Journal on Matrix Analysis and Applications**, v. 24, n. 3, p. 809–821, 2003. Citado na página 19.

COOLEY, J. W.; TUKEY, J. W. An algorithm for the machine calculation of complex Fourier series. **Mathematics of Computation**, American Mathematical Society, v. 19, n. 90, p. 297–301, 1965. ISSN 00255718, 10886842. Citado na página 17.

DATASET of standard 512X512 grayscale test Images. <http://decsai.ugr.es/cvg/CG/base.htm>. Accessed: 2017-05-11. Citado na página 104.

DAUBECHIES, I. The wavelet transform, time-frequency localization and signal analysis. **IEEE Transactions on Information Theory**, v. 36, n. 5, p. 961–1005, Sep 1990. ISSN 0018-9448. Citado na página 17.

DE OLIVEIRA, H. M. **Análise de Fourier e Wavelets: sinais estacionários e não estacionários**. Recife: Editora Universitária, UFPE, 2007. Citado na página 28.

DE OLIVEIRA, H. M.; CAMPELLO DE SOUZA, R. M.; KAUFFMAN, A. N. Efficient multiplex for band-limited channels. In: **Proceedings of the Workshop on Coding and Cryptography - WCC '99**. Paris: [s.n.], 1999. p. 235–241. Citado na página 18.

DE OLIVEIRA, H. M.; MIRANDA, J. P. C. L.; CAMPELLO DE SOUZA, R. M. Spread-spectrum based on finite field Fourier transforms. In: **Proceedings of the ICSECIT - International Conference on Systems Engineering**. Punta Arenas: [s.n.], 2001. v. 1. Citado na página 18.

DE OLIVEIRA NETO, J. R.; LIMA, J. B. Discrete fractional Fourier transforms based on closed-form Hermite-Gaussian-like DFT eigenvectors. **IEEE Transactions on Signal Processing**, v. 65, n. 23, p. 6171–6184, Dec 2017. Citado 16 vezes nas páginas 32, 37, 40, 41, 42, 43, 45, 51, 52, 53, 54, 55, 57, 69, 77 e 95.

DE OLIVEIRA NETO, J. R.; LIMA, J. B. Hardware architectures for computing 8-point cosine number transform. In: **2018 IEEE International Symposium on Circuits and Systems (ISCAS)**. [S.l.: s.n.], 2018. p. 1–5. ISSN 2379-447X. Citado 4 vezes nas páginas 18, 19, 91 e 118.

DE OLIVEIRA NETO, J. R.; LIMA, J. B.; PANARIO, D. A family of matrices for generating Hermite-Gaussian-Like DFT eigenvectors. In: **2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)**. [S.l.: s.n.], 2018. p. 4379–4383. ISSN 2379-190X. Citado 4 vezes nas páginas 57, 69, 77 e 118.

DE OLIVEIRA NETO, J. R.; LIMA, J. B.; PANARIO, D. A generating matrix method for constructing Hermite-Gaussian-like number-theoretic transform eigenvectors. **Signal Processing**, v. 152, p. 189 – 196, Nov 2018. ISSN 0165-1684. Citado 6 vezes nas páginas 86, 87, 88, 90, 93 e 95.

DEB, S. et al. Hardware implementation of a digital watermarking system for video authentication. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 23, n. 2, p. 289–301, Feb 2013. Citado na página 94.

DESCHAMPS, J.-P. **Hardware Implementation of Finite-Field Arithmetic (Electronic Engineering)**. [S.l.]: McGraw-Hill Education, 2009. ISBN 9780071545822. Citado na página 18.

DICKINSON, B.; STEIGLITZ, K. Eigenvectors and functions of the discrete Fourier transform. **IEEE Transactions on Acoustics, Speech, and Signal Processing**, v. 30, n. 1, p. 25–31, Feb 1982. ISSN 0096-3518. Citado 2 vezes nas páginas 19 e 20.

DICOM - Digital Imaging and Communications in Medicine. <http://www.dicomstandard.org/>. January, 2018. Citado na página 112.

ECRYPT II. **ECRYPT II Yearly Report on Algorithms and Keysizes (2011–2012)**. 2nd. ed. [S.l.], 2012. European Network of Excellence in Cryptology II. Citado 5 vezes nas páginas 95, 104, 105, 107 e 110.

ELGAMEL, S. A.; SORAGHAN, J. Enhanced monopulse tracking radar using optimum fractional Fourier transform. **IET Radar, Sonar Navigation**, v. 5, n. 1, p. 74–82, Jan 2011. ISSN 1751-8784. Citado na página 19.

ELHOSENY, H. M. et al. The effect of fractional Fourier transform angle in encryption quality for digital images. **Optik - International Journal for Light and Electron Optics**, v. 127, n. 1, p. 315 – 319, Jan 2016. ISSN 0030 - 4026. Citado 4 vezes nas páginas 94, 95, 104 e 105.

ELLIOTT, D. F.; RAO, K. R. Book; Book/Illustrated. **Fast transforms : algorithms, analyses, applications**. [S.l.]: New York : Academic Press, 1982. ISBN 0122370805. Citado na página 17.

FEKRI, F. et al. Block error correcting codes using finite-field wavelet transforms. **IEEE Transactions on Signal Processing**, v. 54, n. 3, p. 991–1004, Mar 2006. ISSN 1053-587X. Citado na página 18.

FEYNMAN, R. **Statistical Mechanics: A Set of Lectures**. Boulder, CO, USA: Westview Press, 1998. Citado na página 33.

FIGUEIREDO, R. D. B.; LIMA, J. L.; DE OLIVEIRA NETO, J. R. Matrices generating eigenvectors for constructing fractional trigonometric transforms. In: **40th International Conference on Telecommunications and Signal Processing (TSP 2017)**. [S.l.: s.n.], 2017. Citado na página 118.

FIGUEIREDO, R. D. B.; LIMA, J. L.; DE OLIVEIRA NETO, J. R. Matrizes geradoras de autovetores para construção de transformadas de Hartley fracionárias. In: **XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT 2017)**. [S.l.: s.n.], 2017. Citado na página 118.

GE, H.; QIAN, Z.; WANG, J. A high capacity multi-level approach for reversible data hiding in encrypted images. **IEEE Transactions on Circuits and Systems for Video Technology**, PP, p. 1–11, Jul 2018. Citado na página 94.

GOLUB, G. H.; LOAN, C. F. V. **Matrix Computations**. 3rd. ed. [S.l.]: Johns Hopkins University Press, 1996. Citado na página 36.

GUREVICH, S.; HADANI, R. On the diagonalization of the discrete Fourier transform. **Applied and Computational Harmonic Analysis**, v. 27, n. 1, p. 87 – 99, Jul 2009. ISSN 1063-5203. Citado na página 19.

HANNA, M. T. Direct sequential evaluation of optimal orthonormal eigenvectors of the discrete Fourier transform matrix by constrained optimization. **Digital Signal Processing**, v. 22, n. 4, p. 681 – 689, Jul 2012. ISSN 1051-2004. Citado na página 56.

HANNA, M. T.; SEIF, N. P. A.; AHMED, W. A. E. M. Hermite-Gaussian-like eigenvectors of the discrete Fourier transform matrix based on the singular-value decomposition of its orthogonal projection matrices. **IEEE Transactions on Circuits and Systems I: Regular Papers**, v. 51, n. 11, p. 2245–2254, Nov 2004. Citado 4 vezes nas páginas 24, 25, 26 e 56.

HANNA, M. T.; SEIF, N. P. A.; AHMED, W. A. E. M. Hermite-Gaussian-like eigenvectors of the discrete Fourier transform matrix based on the direct utilization of the orthogonal projection matrices on its eigenspaces. **IEEE Transactions on Signal Processing**, v. 54, n. 7, p. 2815–2819, Jul 2006. ISSN 1053-587X. Citado na página 56.

HANNA, M. T.; SEIF, N. P. A.; AHMED, W. A. E. M. Discrete fractional Fourier transform based on the eigenvectors of tridiagonal and nearly tridiagonal matrices. **Digital Signal Processing**, v. 18, n. 5, p. 709–727, Sep 2008. Citado 2 vezes nas páginas 56 e 57.

HAZEWINKEL, M. **Trace of a square matrix. Encyclopedia of Mathematics**. [S.l.]: Springer, 2001. <https://www.encyclopediaofmath.org/index.php/Trace_of_a_square_matrix>. Citado na página 133.

HEVC. **High efficiency video coding: Recommendation ITU-T H.265**. [S.l.], 2013. International Telecommunication Union. Citado na página 17.

HOFFMAN, K. M.; KUNZE, R. **Linear Algebra**. 2nd. ed. [S.l.]: Pearson, 1971. Citado na página 36.

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, Oct 2015. Citado 2 vezes nas páginas 26 e 56.

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, Oct 2015. ISSN 1549-8328. Citado 4 vezes nas páginas 94, 95, 104 e 105.

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**, PP, p. 1–13, Jul 2018. Citado 5 vezes nas páginas 94, 104, 105, 113 e 114.

KANG, X.; TAO, R. Color image encryption using pixel scrambling operator and reality-preserving MPFRHT. **IEEE Transactions on Circuits and Systems for Video Technology**, PP, p. 1–13, Jul 2018. Citado 5 vezes nas páginas 94, 104, 105, 113 e 114.

KANG, X.; TAO, R.; ZHANG, F. Multiple-parameter discrete fractional transform and its applications. **IEEE Transactions on Signal Processing**, v. 64, n. 13, p. 3402–3417, Jul 2016. ISSN 1053-587X. Citado 5 vezes nas páginas 94, 95, 96, 104 e 105.

KANG, X.; ZHANG, F.; TAO, R. Multichannel random discrete fractional Fourier transform. **IEEE Signal Processing Letters**, v. 22, n. 9, p. 1340–1344, Sep 2015. Citado 2 vezes nas páginas 26 e 56.

KANG, X.; ZHANG, F.; TAO, R. Multichannel random discrete fractional Fourier transform. **IEEE Signal Processing Letters**, v. 22, n. 9, p. 1340–1344, Sep 2015. ISSN 1070-9908. Citado 4 vezes nas páginas 94, 95, 104 e 105.

KONG, F. N. Analytic expressions of two discrete Hermite-Gauss signals. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 55, n. 1, p. 56–60, Jan 2008. ISSN 1549-7747. Citado 6 vezes nas páginas 20, 26, 27, 28, 29 e 57.

KUZNETSOV, A. Explicit Hermite-type eigenvectors of the discrete Fourier transform. **SIAM. J. Matrix Anal. & Appl.**, Society for Industrial & Applied Mathematics (SIAM), v. 36, n. 4, p. 1443–1464, Jan 2015. Citado 20 vezes nas páginas 20, 21, 22, 26, 27, 28, 29, 30, 32, 34, 39, 45, 46, 47, 48, 54, 57, 77, 80 e 116.

KUZNETSOV, A.; KWASNICKI, M. Minimal Hermite-type eigenbasis of the discrete Fourier transform. **Journal of Fourier Analysis and Applications**, p. 1–27, Jan 2018. Citado 3 vezes nas páginas 20, 26 e 57.

LANG, J. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform. **Optics Communications**, v. 285, n. 10, p. 2584 – 2590, Jul 2012. ISSN 0030-4018. Citado 4 vezes nas páginas 94, 95, 104 e 105.

LANG, J. Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain. **Optics Communications**, v. 338, n. Supplement C, p. 181 – 192, Mar 2015. ISSN 0030-4018. Citado 4 vezes nas páginas 94, 95, 104 e 105.

LEE, Y. L.; TSAI, W. H. A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 24, n. 4, p. 695–703, Apr 2014. Citado na página 94.

LI, S. et al. Cryptanalysis of an image scrambling scheme without bandwidth expansion. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 18, n. 3, p. 338–349, Mar 2008. Citado na página 94.

LI, Y. et al. Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform. **Optics and Lasers in Engineering**, v. 72, n. Supplement C, p. 18 – 25, Sep 2015. ISSN 0143-8166. Citado 4 vezes nas páginas 94, 95, 104 e 105.

LIMA, J. B. Fast algorithm for computing cosine number transform. **Electronics Letters**, v. 51, n. 20, p. 1570–1572, Oct 2015. ISSN 0013-5194. Citado na página 19.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Finite field trigonometric transforms. **Applicable Algebra in Engineering, Communication and Computing**, v. 22, n. 5-6, p. 393–411, Dec 2011. Citado 2 vezes nas páginas 19 e 118.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. The fractional Fourier transform over finite fields. **Signal Processing**, v. 92, n. 2, p. 465 – 476, Feb 2012. ISSN 0165-1684. Citado 6 vezes nas páginas 20, 21, 76, 77, 92 e 93.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Fractional cosine and sine transforms over finite fields. **Linear Algebra and its Applications**, v. 438, n. 8, p. 3217 – 3230, 2013. ISSN 0024-3795. Citado 2 vezes nas páginas 20 e 21.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Closed-form Hermite–Gaussian-like number-theoretic transform eigenvectors. **Signal Processing**, v. 128, n. Complete, p. 409–416, Nov 2016. Citado 19 vezes nas páginas 20, 21, 76, 77, 78, 79, 80, 81, 91, 93, 94, 95, 96, 104, 105, 113, 114, 115 e 117.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M.; PANARIO, D. The eigenstructure of finite field trigonometric transforms. **Linear Algebra and its Applications**, v. 435, n. 8, p. 1956 – 1971, Oct 2011. ISSN 0024-3795. Citado 2 vezes nas páginas 19 e 78.

LIMA, J. B.; DE OLIVEIRA NETO, J. R.; FIGUEIREDO, R. B. A unified approach for defining random discrete fractional transforms. **Optik - International Journal for Light and Electron Optics**, v. 165, p. 388 – 394, Jul 2018. ISSN 0030-4026. Citado na página 118.

LIMA, J. B.; LIMA, E. A. O.; MADEIRO, F. Image encryption based on the finite field cosine transform. **Signal Processing: Image Communication**, v. 28, n. 10, p. 1537–1547, Nov 2013. Citado 9 vezes nas páginas 19, 76, 94, 95, 104, 105, 113, 114 e 115.

LIMA, J. B.; MADEIRO, F.; SALES, F. J. R. Encryption of medical images based on the cosine number transform. **Signal Processing: Image Communication**, Elsevier BV, v. 35, p. 1–8, Jul 2015. Citado 9 vezes nas páginas 19, 76, 94, 95, 104, 105, 113, 114 e 115.

LIMA, J. B.; NOVAES, L. F. G. Image encryption based on the fractional Fourier transform over finite fields. **Signal Processing**, v. 94, n. 1, p. 521–530, Jan 2014. Citado 10 vezes nas páginas 24, 56, 94, 95, 104, 105, 113, 114, 115 e 117.

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, p. 2893–2016, Nov 2017. Citado 11 vezes nas páginas 20, 21, 76, 92, 94, 95, 104, 105, 113, 114 e 115.

LIN, K. T. Image encryption using Arnold transform technique and Hartley transform domain. In: **2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing**. [S.l.: s.n.], 2013. p. 84–87. Citado na página 17.

LIU, S. et al. Sparse discrete fractional Fourier transform and its applications. **IEEE Transactions on Signal Processing**, v. 62, n. 24, p. 6582–6595, Dec 2014. Citado na página 91.

LIU, S.; SHERIDAN, J. T. Optical encryption by combining image scrambling techniques in fractional Fourier domains. **Optics Communications**, v. 287, p. 73–80, Jan 2013. Citado 3 vezes nas páginas 24, 56 e 117.

LIU, X. L.; LIN, C. C.; YUAN, S. M. Blind dual watermarking for color images' authentication and copyright protection. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 28, n. 5, p. 1047–1055, May 2018. Citado na página 94.

LIU, Y. et al. Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation. **Multimedia Tools and Applications**, v. 74, n. 9, p. 3171–3182, May 2015. Citado 6 vezes nas páginas 94, 95, 104, 105, 113 e 114.

LIU, Z.; LIU, S. Double image encryption based on iterative fractional Fourier transform. **Optics Communications**, v. 275, n. 2, p. 324 – 329, Jul 2007. ISSN 0030-4018. Citado 4 vezes nas páginas 94, 95, 104 e 105.

LIU, Z. et al. Image encryption by using local random phase encoding in fractional Fourier transform domains. **Optik - International Journal for Light and Electron Optics**, v. 123, n. 5, p. 428 – 432, Mar 2012. ISSN 0030-4026. Citado 4 vezes nas páginas 94, 95, 104 e 105.

LOHMANN, A. W. Image rotation, Wigner rotation, and the fractional Fourier transform. **Journal of the Optical Society of America**, v. 10, n. 10, p. 2181–2186, Oct 1993. Citado 3 vezes nas páginas 24, 52 e 117.

LU, G.; XIAO, M.; WEI, P. Adaptive short time fractional Fourier transform for time-frequency segmentation. **Electronics Letters**, v. 52, n. 8, p. 615–617, Apr 2016. Citado 4 vezes nas páginas 24, 56, 72 e 117.

LYNCH, D. R. **Numerical Partial Differential Equations for Environmental Scientists and Engineers: A First Practical Course**. Boston, MA: Springer US, 2005. Citado na página 44.

MAJORKOWSKA-MECH, D.; CARIOW, A. A low-complexity approach to computation of the discrete fractional Fourier transform. **Circuits, Systems, and Signal Processing**, v. 36, n. 10, p. 4118–4144, Oct 2017. Citado 13 vezes nas páginas 22, 57, 58, 67, 68, 69, 70, 71, 73, 74, 89, 90 e 91.

MCCLELLAN, J.; PARKS, T. Eigenvalue and eigenvector decomposition of the discrete Fourier transform. **IEEE Transactions on Audio and Electroacoustics**, v. 20, n. 1, p. 66–74, Mar 1972. Citado 6 vezes nas páginas 25, 37, 59, 76, 96 e 97.

MIAH, K. H.; POTTER, D. K. Geophysical signal parameterization and filtering using the fractional Fourier transform. **IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing**, v. 7, n. 3, p. 845–852, Mar 2014. ISSN 1939-1404. Citado na página 19.

MIKHAIL, M.; ABOUELSEOUD, Y.; ELKOBROSY, G. Two-phase image encryption scheme based on FFCT and fractals. **Security and Communication Networks**, Hindawi, p. 1–13, Jan 2017. Citado 7 vezes nas páginas 94, 95, 104, 105, 113, 114 e 115.

MIRANDA, J. P. C. L.; DE OLIVEIRA, H. M. On Galois-division multiple access systems: Figures of merit and performance evaluation. In: **Proceedings of the 19 Brazilian Telecommunication Symposium**. CE,Fortaleza: [s.n.], 2001. Citado na página 18.

MPEG, . **Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video**. [S.l.], 1994. International Organisation for Standardisation, ISO. Citado na página 17.

NAMIAS, V. The fractional order Fourier transform and its application in quantum mechanics. **Journal of the Institute of Mathematics and its Applications**, v. 25, p. 241–265, 1980. Citado 2 vezes nas páginas 24 e 117.

NGUYEN, Y. T. H. et al. Sparse reconstruction of time-frequency representation using the fractional Fourier transform. In: **Proc. International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)**. Da Nang, Vietnan: [s.n.], 2017. p. 16–20. Citado na página 72.

OZAKTAS, H. M. et al. Digital computation of the fractional Fourier transform. **IEEE Transactions on Signal Processing**, v. 44, n. 9, p. 2141–2150, Sep 1996. ISSN 1053-587X. Citado 9 vezes nas páginas 21, 24, 27, 50, 51, 52, 54, 55 e 56.

OZAKTAS, H. M.; ZALEVSKY, Z.; KUTAY, M. A. **The Fractional Fourier transform: with Applications in Optics and Signal Processing**. [S.l.]: John Wiley & Sons, 2001. Citado 3 vezes nas páginas 24, 56 e 117.

PEDROUZO-ULLOA, A.; TRONCOSO-PASTORIZA, J. R.; PÉREZ-GONZÁLEZ, F. Number theoretic transforms for secure signal processing. **IEEE Transations on Information Forensics Security**, v. 12, n. 5, p. 1125–1140, May 2017. Citado na página 76.

PEDROUZO-ULLOA, A.; TRONCOSO-PASTORIZA, J. R.; PÉFEZ-GONZÁLEZ, F. Number theoretic transforms for secure signal processing. **IEEE Transactions on Information Forensics and Security**, v. 12, n. 5, p. 1125–1140, May 2017. ISSN 1556-6013. Citado na página 118.

PEI, S.; HSUE, W.; DING, J. Discrete fractional Fourier transform based on new nearly tridiagonal commuting matrices. **IEEE Transactions on Signal Processing**, v. 54, n. 10, p. 3815–3828, Oct 2006. Citado 5 vezes nas páginas 24, 25, 26, 56 e 57.

PEI, S. C.; CHANG, K. W. Generating matrix of discrete Fourier transform eigenvectors. In: **2009 IEEE International Conference on Acoustics, Speech and Signal Processing**. [S.l.: s.n.], 2009. p. 3333–3336. ISSN 1520-6149. Citado 10 vezes nas páginas 20, 21, 26, 27, 32, 33, 77, 80, 95 e 116.

PEI, S. C.; CHANG, K. W. Optimal discrete Gaussian function: The closed-form functions satisfying Tao's and Donoho's uncertainty principle with Nyquist bandwidth. **IEEE Transactions on Signal Processing**, v. 64, n. 12, p. 3051–3064, Jun 2016. ISSN 1053-587X. Citado 14 vezes nas páginas 20, 21, 22, 26, 27, 31, 32, 33, 34, 39, 57, 77, 95 e 116.

PEI, S.-C.; HSUE, W.-L. The multiple-parameter discrete fractional Fourier transform. **IEEE Signal Processing Letters**, v. 13, n. 6, p. 329–332, Jun 2006. ISSN 1070-9908. Citado 5 vezes nas páginas 94, 95, 96, 104 e 105.

PEI, S. C.; HSUE, W. L. Random discrete fractional Fourier transform. **IEEE Signal Processing Letters**, v. 16, n. 12, p. 1015–1018, Dec 2009. ISSN 1070-9908. Citado 4 vezes nas páginas 94, 95, 104 e 105.

PEI, S. C.; WEN, C. C.; DING, J. J. Closed-form orthogonal DFT eigenvectors generated by complete generalized Legendre sequence. **IEEE Transactions on Circuits and Systems I: Regular Papers**, v. 55, n. 11, p. 3469–3479, Dec 2008. ISSN 1549-8328. Citado 8 vezes nas páginas 56, 57, 77, 92, 94, 95, 104 e 105.

PEI, S. C.; WEN, C. C.; DING, J. J. Closed-form orthogonal number theoretic transform eigenvectors and the fast fractional NTT. **IEEE Transactions on Signal Processing**, v. 59, n. 5, p. 2124–2135, May 2011. ISSN 1053-587X. Citado 10 vezes nas páginas 20, 21, 76, 77, 92, 93, 94, 95, 104 e 105.

PEI, S.-C.; YEH, M.-H. Improved discrete fractional Fourier transform. **Opt. Lett.**, OSA, v. 22, n. 14, p. 1047–1049, Jul 1997. Citado 2 vezes nas páginas 19 e 20.

PEI, S.-C.; YEH, M.-H. The discrete fractional cosine and sine transforms. **IEEE Transactions on Signal Processing**, v. 49, n. 6, p. 1198–1207, Jun 2001. Citado 3 vezes nas páginas 67, 68 e 69.

PEI, S.-C.; YEH, M.-H.; TSENG, C.-C. Discrete fractional Fourier transform based on orthogonal projections. **IEEE Transaction on Signal Processing**, v. 47, n. 5, p. 1335–1348, May 1999. Citado 4 vezes nas páginas 24, 25, 26 e 56.

PELICH, R. et al. Vessel refocusing and velocity estimation on SAR imagery using the fractional Fourier transform. **IEEE Transactions on Geoscience and Remote Sensing**, v. 54, n. 3, p. 1670–1684, Mar 2016. Citado 3 vezes nas páginas 24, 56 e 117.

PENNISI, L. L. Coefficients of the characteristic polynomial. **Mathematics Magazine**, v. 60, n. 1, p. 31–33, Feb 1987. Citado na página 35.

POLLARD, J. M. The fast Fourier transform in a finite field. **Mathematics of Computation**, American Mathematical Society (AMS), v. 25, n. 114, p. 365–365, May 1971. Citado na página 17.

POOR, H. V. Finite-field wavelet transforms. In: CHOUINARD, J.-Y.; FORTIER, P.; GULLIVER, T. A. (Ed.). **Information Theory and Applications II: 4th Canadian Workshop Lac Delage, Québec, Canada**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996. p. 225–238. ISBN 978-3-540-70647-2. Citado na página 18.

POURAZAD, M. T. et al. HEVC: The new gold standard for video compression: How does HEVC compare with H.264/AVC. **IEEE Consumer Electronics Magazine**, v. 1, n. 3, p. 36–46, Jul 2012. ISSN 2162-2248. Citado na página 17.

QIAN, Z.; ZHANG, X. Reversible data hiding in encrypted images with distributed source encoding. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 26, n. 4, p. 636–646, Apr 2016. Citado na página 94.

RAN, Q. et al. Vector power multiple-parameter fractional Fourier transform of image encryption algorithm. **Optics and Lasers in Engineering**, v. 62, n. Supplement C, p. 80 – 86, Nov 2014. ISSN 0143-8166. Citado 4 vezes nas páginas 94, 95, 104 e 105.

RAO, K. R.; YIP, P. **Discrete Cosine Transform: Algorithms, Advantages, Applications**. San Diego, CA: Academic Press, 1990. Citado na página 17.

RUBANOV, N. S. et al. The modified number theoretic transform over the direct sum of finite fields to compute the linear convolution. **IEEE Transactions on Signal Processing**, v. 46, n. 3, p. 813–817, Mar 1998. ISSN 1053-587X. Citado na página 76.

SANTHANAN, B.; SANTHANAN, T. S. Discrete Gauss-Hermite functions and eigenvectors of the centered discrete Fourier transform. In: **IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)**. [S.l.: s.n.], 2007. v. 3, p. 1385–1388. Citado 5 vezes nas páginas 24, 25, 26, 56 e 57.

SCHAFER, A. V. .; OPPENHEIM, R. W. **Discrete-time Signal Processing, 3rd**. [S.l.]: Prentice Hall, 1999. ISBN 8131704920. Citado na página 17.

SEJDIĆ, E.; DJUROVIĆ, I.; STANKOVIĆ, L. Fractional Fourier transform as a signal processing tool: An overview of recent developments. **Signal Processing**, Elsevier BV, v. 91, n. 6, p. 1351–1369, Jun 2011. Citado na página 19.

SEJDIC, E.; DJUROVIC, I.; STANKOVIC, L. Fractional Fourier transform as a signal processing tool: overview of recent developments. **Signal Processing**, v. 91, n. 6, p. 1351–1369, Jun 2011. Citado na página 72.

SERBES, A. Compact fractional Fourier domains. **IEEE Signal Processing Letters**, v. 24, n. 4, p. 427–431, April 2017. Citado 3 vezes nas páginas 69, 72 e 73.

SERBES, A.; DURAK-ATA, L. Optimum signal and image recovery by the method of alternating projections in fractional Fourier domains. **Communications in Nonlinear Science and Numerical Simulation**, v. 15, n. 3, p. 675–689, Mar 2009. Citado na página 72.

SERBES, A.; DURAK-ATA, L. The discrete fractional Fourier transform based on the DFT matrix. **Signal Processing**, v. 91, n. 3, p. 571 – 581, Mar 2011. ISSN 0165-1684. Advances in Fractional Signals and Systems. Citado 6 vezes nas páginas 20, 24, 25, 26, 56 e 57.

SHENG, Y. **Wavelet Transform**. 3th. ed. [S.l.]: CRC Press, 2010. Transforms and Applications Handbook. ISBN 1420066528. Citado na página 17.

SINGH, J.; DATCU, M. SAR image categorization with log cumulants of the fractional Fourier transform coefficients. **IEEE Transactions on Geoscience and Remote Sensing**, v. 51, n. 12, p. 5273–5282, Dec 2013. ISSN 0196-2892. Citado na página 19.

SINGH, N.; SINHA, A. Optical image encryption using fractional Fourier transform and chaos. **Optics and Lasers in Engineering**, v. 46, n. 2, p. 117 – 123, Feb 2008. ISSN 0143-8166. Citado 4 vezes nas páginas 94, 95, 104 e 105.

SKODRAS, A.; CHRISTOPOULOS, C.; EBRAHIMI, T. The JPEG 2000 still image compression standard. **IEEE Signal Processing Magazine**, v. 18, n. 5, p. 36–58, Sep 2001. ISSN 1053-5888. Citado na página 17.

SONG, G. et al. Finite field spreading for multiple-access channel. **IEEE Transactions on Communications**, v. 62, n. 3, p. 1001–1010, Mar 2014. ISSN 0090-6778. Citado na página 118.

SONG, G. et al. Finite field spreading for multiple-access channels. **IEEE Trans. Commun.**, v. 62, n. 3, p. 1001–1010, Mar 2014. Citado na página 76.

SUNDARARAJAN, D.; AHMAD, M. O. Fast computation of the discrete Walsh and Hadamard transforms. **IEEE Transactions on Image Processing**, v. 7, n. 6, p. 898–904, Jun 1998. ISSN 1057-7149. Citado na página 17.

SVANSTROM, F. **Properties of a generalized sArnold's discrete cat map**. Dissertação (Mestrado) — Department of Mathematics of Linnaeus University, Sweden, Jun 2014. Citado 2 vezes nas páginas 97 e 98.

TAO, R.; LANG, J.; WANG, Y. The multiple-parameter discrete fractional Hadamard transform. **Optics Communications**, v. 282, n. 8, p. 1531 – 1535, Apr 2009. ISSN 0030-4018. Citado 5 vezes nas páginas 94, 95, 96, 104 e 105.

TAO, R.; MENG, X. Y.; WANG, Y. Image encryption with multiorders of fractional Fourier transforms. **IEEE Transactions on Information Forensics and Security**, v. 5, n. 4, p. 734–738, Dec 2010. ISSN 1556-6013. Citado 4 vezes nas páginas 94, 95, 104 e 105.

TAO, R.; MENG, X.-Y.; WANG, Y. Transform order division multiplexing. **IEEE Transactions on Signal Processing**, v. 59, n. 2, p. 598–609, Feb 2011. Citado 3 vezes nas páginas 24, 56 e 117.

TOIVONEN, T.; HEIKKILA, 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, Jan 2006. ISSN 1051-8215. Citado 2 vezes nas páginas 18 e 76.

VAISH, A.; KUMAR, M. Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. **Optik - International Journal for Light and Electron Optics**, v. 145, n. Supplement C, p. 273 – 283, Sep 2017. ISSN 0030-4026. Citado 4 vezes nas páginas 94, 95, 104 e 105.

WALLACE, G. K. The JPEG still picture compression standard. **IEEE Transactions on Consumer Electronics**, v. 38, n. 1, p. xviii–xxxiv, Feb 1992. ISSN 0098-3063. Citado na página 17.

WANG, T. et al. Security coded OFDM system based on multiorder fractional Fourier transform. **IEEE Communications Letters**, v. 20, p. 2474–2477, Sep 2016. Citado 3 vezes nas páginas 24, 56 e 117.

WEI, D.; LI, Y. Novel tridiagonal commuting matrices for types I, IV, V, VIII DCT and DST matrices. **IEEE Signal Processing Letters**, v. 21, n. 4, p. 483–487, Apr 2014. ISSN 1070-9908. Citado 2 vezes nas páginas 56 e 57.

WEI, D.; LI, Y.-M. Generalized sampling expansions with multiple sampling rates for lowpass and bandpass signals in the fractional Fourier transform domain. **IEEE Transactions on Signal Processing**, v. 64, n. 18, p. 4861–4874, Sep 2016. Citado 3 vezes nas páginas 24, 56 e 117.

WEI, D.; RAN, Q. Multiplicative filtering in the fractional Fourier domain. **Signal, Image and Video Processing**, Springer Science, Business Media, v. 7, n. 3, p. 575–580, Sep 2011. Citado na página 19.

WEI, D. Y. et al. Fractionalisation of an odd time odd frequency DFT matrix based on the eigenvectors of a novel nearly tridiagonal commuting matrix. **IET Signal Processing**, v. 5, n. 2, p. 150–156, Apr 2011. ISSN 1751-9675. Citado 2 vezes nas páginas 56 e 57.

WEIMANN, S. et al. Implementation of quantum and classical discrete fractional Fourier transforms. **Nature Communications**, v. 7, p. 1–8, Mar 2016. Citado 3 vezes nas páginas 24, 56 e 117.

WU, H. Z. et al. Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 27, n. 8, p. 1620–1631, Aug 2017. Citado na página 94.

WU, Y.; NOONAN, J. P.; AGAIAN, S. NPCR and UACI randomness tests for image encryption. **Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT),**, p. 31–38, Apr 2011. Citado 5 vezes nas páginas 95, 104, 105, 107 e 108.

XU, X.; WANG, Y.; CHEN, S. Medical image fusion using discrete fractional wavelet transform. **Biomedical Signal Processing and Control**, v. 27, p. 103 – 111, 2016. ISSN 1746-8094. Citado na página 19.

ZHANG, W. et al. Decomposing joint distortion for adaptive steganography. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 27, n. 10, p. 2274–2280, Oct 2017. Citado na página 94.

ZHAO, B. et al. A novel NTT-based authentication scheme for 10-GHz quantum key distribution systems. **IEEE Trans. Ind. Electron.**, v. 63, n. 8, p. 5101–5108, Aug 2016. Citado na página 76.

ZHAO, T. et al. Security of image encryption scheme based on multi-parameter fractional Fourier transform. **Optics Communications**, v. 376, n. Supplement C, p. 47 – 51, Oct 2016. ISSN 0030-4018. Citado 4 vezes nas páginas 94, 95, 104 e 105.

ZHAO, Y. et al. Parameter estimation of wideband underwater acoustic multipath channels based on fractional Fourier transform. **IEEE Transaction on Signal Processing**, v. 64, n. 20, p. 5396–5408, Oct 2016. Citado 3 vezes nas páginas 24, 56 e 117.

ZHENG, L.; SHI, D. Maximum amplitude method for estimating compact fractional Fourier domain. **IEEE Signal Processing Letters**, v. 17, n. 3, p. 293–296, Mar 2010. Citado na página 72.

APÊNDICE A – PROVAS DAS PROPOSIÇÕES 2.2 E 2.3

PROVA DA PROPOSIÇÃO 2.2

Seja $\mathbf{P}$ a matriz

$$\mathbf{P} = \sqrt{2^{-1}} \left[\begin{array}{c|ccc|ccc} \sqrt{2} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & & & & & 1 \\ \vdots & & \ddots & & & \iddots & \\ 0 & & & 1 & 1 & & \\ \hline 0 & & & 1 & -1 & & \\ \vdots & & \iddots & & & \ddots & \\ 0 & 1 & & & & & -1 \end{array}\right],$$

que satisfaz $\mathbf{P} = \mathbf{P}^T = \mathbf{P}^{-1}$. A transformação de similaridade $\mathbf{P}\mathbf{S}_{\overline{\mathbf{T}}}\mathbf{P}^{-1}$ produz a matriz (A.1), em que $S_n = \text{sen}\left(n\frac{2\pi}{N}\right)$. O determinante de $\mathbf{P}\mathbf{S}_{\overline{\mathbf{T}}}\mathbf{P}^{-1}$, que é dado pelo produto dos elementos das suas antidiagonais, é $\det(\mathbf{P}\mathbf{S}_{\overline{\mathbf{T}}}\mathbf{P}^{-1}) = 0$. Desde que $\det(\mathbf{P}) = \det(\mathbf{P}^{-1}) = 1$, necessariamente tem-se $\det\left(\mathbf{S}_{\overline{\mathbf{T}}}\right) = 0$.

PROVA DA PROPOSIÇÃO 2.3

Relembremos as seguintes propriedades do traço de uma matriz:

Propriedade A.1. *Sejam* $\mathbf{A}$ *e* $\mathbf{B}$ *matrizes* $N \times N$*, os índices* $i, j = 1, 2, \ldots, N$ *os elementos na* i*-ésima linha e na* j*-ésima coluna, e* β *uma constante (HAZEWINKEL, 2001), tem-se:*

$$\mathbf{P}\mathbf{S}_{\overline{\mathbf{T}}}\mathbf{P}^{-1} = \left[\begin{array}{ccccccccccc} & & & & & & & & & & -\frac{\sqrt{2}}{2} \\ & & & & & & & & & -\frac{1}{2} & S_1 \\ & & & & & & & & -\frac{1}{2} & S_2 & \frac{1}{2} \\ & & & & & & & \iddots & \iddots & \iddots & \\ & & & & & & -\frac{1}{2} & S_{\frac{N-3}{2}} & \frac{1}{2} & & \\ & & & & & 0 & S_{\frac{N-1}{2}} + \frac{1}{2} & \frac{1}{2} & & & \\ & & & & \frac{1}{2} & S_{\frac{N-1}{2}} - \frac{1}{2} & 0 & & & & \\ & & & \frac{1}{2} & S_{\frac{N-3}{2}} & -\frac{1}{2} & & & & & \\ & & \iddots & \iddots & \iddots & & & & & & \\ & \frac{1}{2} & S_2 & -\frac{1}{2} & & & & & & & \\ \frac{\sqrt{2}}{2} & S_1 & -\frac{1}{2} & & & & & & & & \end{array}\right] \quad \text{(A.1)}$$

i $\operatorname{tr}(\mathbf{AB}) = \operatorname{tr}(\mathbf{BA})$;

ii $\operatorname{tr}(\mathbf{A}+\mathbf{B}) = \operatorname{tr}(\mathbf{A}) + \operatorname{tr}(\mathbf{B})$;

iii $\operatorname{tr}(\beta\mathbf{A}) = \beta \operatorname{tr}(\mathbf{A})$

iv $\operatorname{tr}(\mathbf{AB}^T) = \sum_{i,j}(\mathbf{A} \circ \mathbf{B})_{i,j}$, *em que* $\circ$ *denota multiplicação elemento a elemento.*

Em geral, o Teorema Binomial pode ser usado para expandir potências da soma de duas matrizes apenas se estas matrizes comutarem; o que não é o caso das matrizes $-i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F}$ e $\overline{\mathbf{T}}$. Contudo, desde que não se esteja interessado em calcular ${\mathbf{S}_{\overline{\mathbf{T}}}}^m$, e sim $\operatorname{tr}\left({\mathbf{S}_{\overline{\mathbf{T}}}}^m\right)$, devido à propriedade A.1(i), pode-se escrever

$$\begin{aligned}\operatorname{tr}\left({\mathbf{S}_{\overline{\mathbf{T}}}}^m\right) &= \operatorname{tr}\left[\left(-i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F} + \overline{\mathbf{T}}\right)^m\right] \\ &= \operatorname{tr}\left[\sum_{k=0}^{m}\binom{m}{k}\left(-i\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F}\right)^{m-k}\overline{\mathbf{T}}^k\right]. \end{aligned} \tag{A.2}$$

Devido à propriedade A.1(ii), $\operatorname{tr}\left({\mathbf{S}_{\overline{\mathbf{T}}}}^m\right)$ pode ser avaliado considerando o traço de cada termo do somatório na última equação. São então analisados os seguintes casos:

i. m é ímpar

   a) k é ímpar: usando as propriedades A.1(iii) e A.1(iv), e observando que

   $$\left(\mathbf{F}^{-1}\overline{\mathbf{T}}\mathbf{F}\right)^{m-k} = \mathbf{F}^{-1}\overline{\mathbf{T}}^{m-k}\mathbf{F}$$

   e $\overline{\mathbf{T}}^T = \overline{\mathbf{T}}$, o traço tr_k do k-ésimo termo do somatório em (A.2) é dado por

   $$\operatorname{tr}_k = \binom{m}{k}(-i)^{m-k}\sum_{i,j}\left[\left(\mathbf{F}^{-1}\overline{\mathbf{T}}^{m-k}\mathbf{F}\right)\circ\left(\overline{\mathbf{T}}^k\right)\right].$$

   Desde que $m-k$ é par, todos os elementos da diagonal principal de $\mathbf{F}^{-1}\overline{\mathbf{T}}^{m-k}\mathbf{F}$ são uma constante não nula denotada por γ. Portanto, a última equação pode ser escrita como

   $$\operatorname{tr}_k = \binom{m}{k}(-i)^{m-k}\gamma\sum_{j}\overline{\mathbf{T}}^k_{j,j}.$$

   Os elementos ao longo da diagonal principal de $\overline{\mathbf{T}}^k$ formam uma sequência com simetria ímpar. Portanto, tem-se $\sum_j \overline{\mathbf{T}}^k_{j,j} = 0$ e $\operatorname{tr}_k = 0$.

   b) k é par: pode-se proceder de forma análoga ao caso anterior. Contudo, sendo $m-k$ agora ímpar, $\mathbf{F}^{-1}\overline{\mathbf{T}}^{m-k}\mathbf{F}$ é uma matriz cujos elementos na diagonal principal são todos nulos. Então o produto elemento a elemento $(\mathbf{F}^{-1}\overline{\mathbf{T}}^{m-k}\mathbf{F}) \circ (\overline{\mathbf{T}}^k)$ dá a matriz nula e, portanto, $\operatorname{tr}_k = 0$.

ii. $m \equiv 2 \pmod 4$

a) k é ímpar: sendo $m-k$ ímpar, é possível demonstrar que $\mathrm{tr}_k = 0$ de uma maneira análoga à aplicada no caso ii.b).

b) k é par: assumindo que $k = 4r$ e escrevendo $m = 4s+2$, tem-se $(-i)^{m-k} = (-i)^{4(s-r)+2} = -1$ e

$$\mathrm{tr}_k = \binom{m}{k}(-1)\mathrm{tr}\left[\left(\mathbf{F}^{-1}\overline{\mathbf{T}}^{4(s-r)+2}\mathbf{F}\right)\overline{\mathbf{T}}^{4r}\right].$$

Observa-se que tr_k é cancelado por tr_{m-k}, o $(m-k)$-ésimo termo do somatório em (A.2), que é obtido se for assumido que $k = 4r+2$. Mais especificamente, tem-se $(-i)^{m-(m-k)} = (-i)^{4r} = 1$ e

$$\mathrm{tr}_{m-k} = \binom{m}{k}\mathrm{tr}\left[\left(\mathbf{F}^{-1}\overline{\mathbf{T}}^{4r}\mathbf{F}\right)\overline{\mathbf{T}}^{4(s-r)+2}\right].$$

Desde que $\mathbf{F}^{-1}\overline{\mathbf{T}}^{4r}\mathbf{F} = \mathbf{F}\overline{\mathbf{T}}^{4r}\mathbf{F}^{-1}$, a última equação torna-se

$$\mathrm{tr}_{m-k} = \binom{m}{k}\mathrm{tr}\left[\left(\mathbf{F}^{-1}\overline{\mathbf{T}}^{4(s-r)+2}\mathbf{F}\right)\overline{\mathbf{T}}^{4r}\right] = -\mathrm{tr}_k.$$

Isso fornece $\mathrm{tr}(\mathbf{S}^m_{\overline{\mathbf{T}}}) = 0$.

iii. $m \equiv 0 \pmod 4$

a) k é ímpar: este caso é análogo ao caso ii.a) e fornece $\mathrm{tr}_k = 0$.

b) k é par: assumindo que $k = 4r$ e escrevendo $m = 4s$, tem-se no k-ésimo termo do somatório em (A.2), tem-se $(-i)^{m-k} = (-i)^{4(s-r)} = 1$. Por outro lado, no $(m-k)$-ésimo termo do somatório em (A.2), tem-se $(-i)^{m-(m-k)} = (-i)^{4r} = 1$. Então, diferentemente do caso ii.b), em vez tr_k e tr_{m-k} serem cancelados, eles são somados, de modo que $\mathrm{tr}(\mathbf{S}^m_{\overline{\mathbf{T}}}) \neq 0$. Similarmente, assumindo que $k = 4r+2$, no k-ésimo termo do somatório em (A.2), tem-se $(-i)^{m-k} = (-i)^{4(s-r)-2} = -1$ e, no $(m-k)$-ésimo termo, tem-se $(-i)^{m-(m-k)} = (-i)^{4r+2} = -1$. Isso leva à mesma conclusão do caso em que $k = 4r$.