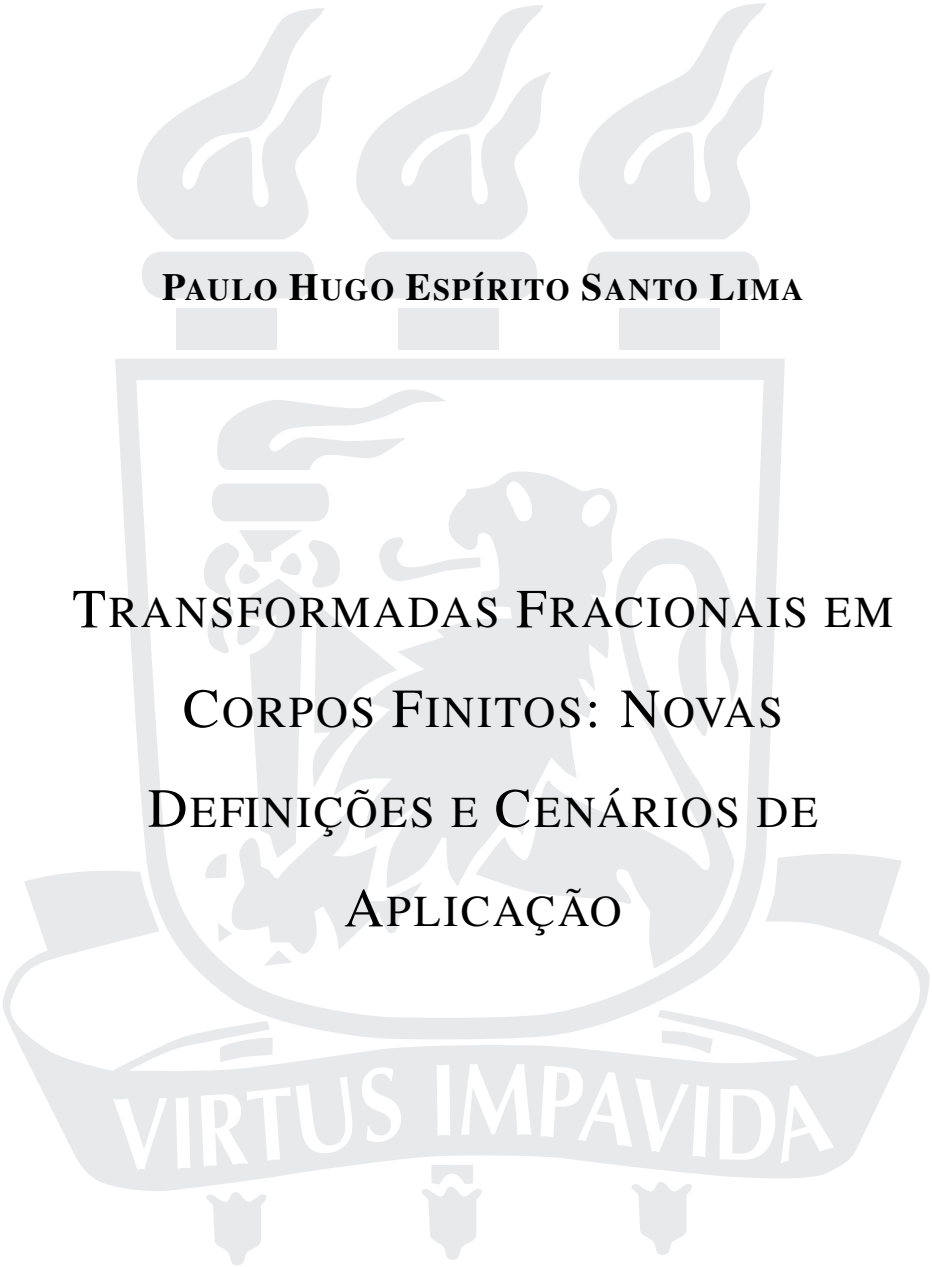
UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE TECNOLOGIA E GEOCIÊNCIAS

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA



PAULO HUGO ESPÍRITO SANTO LIMA

TRANSFORMADAS FRACIONAIS EM CORPOS FINITOS: NOVAS DEFINIÇÕES E CENÁRIOS DE APLICAÇÃO

Recife
2015

PAULO HUGO ESPÍRITO SANTO LIMA

TRANSFORMADAS FRACIONAIS EM CORPOS FINITOS: NOVAS DEFINIÇÕES E CENÁRIOS DE APLICAÇÃO

Tese submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de **Doutor em Engenharia Elétrica**.

Orientador: Prof. Dr. Ricardo Menezes Campello de Souza

Co-orientador: Prof. Dr. Juliano Bandeira Lima

Área de Concentração: Comunicações

Recife
2015

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

L732t Lima. Paulo Hugo Espírito Santo.
Transformadas fracionais em corpos finitos: novas definições e cenários de aplicação/ Paulo Hugo Espírito Santo Lima - Recife: O Autor, 2015.
161folhas, Il.; Abr. e Tab.

Orientador: Prof. Dr. Ricardo Menezes Campello de Souza.
Coorientador: Prof. Dr. Juliano Bandeira Lima.

Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2015.
Inclui Referências e Apêndice.

1. Engenharia Elétrica. 2. Transformadas fracionais. 3. Corpos finitos. I. Souza, Ricardo Menezes Campello de (Orientador). II. Lima, Juliano Bandeira (Coorientador). III. Título.

UFPE

621.3 CDD (22. ed.) BCTG/2016 - 02

Universidade Federal de Pernambuco
Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE TESE DE DOUTORADO DE

PAULO HUGO ESPÍRITO SANTO LIMA

TÍTULO

"TRANSFORMADAS FRACIONAIS EM CORPOS FINITOS: NOVAS DEFINIÇÕES E CENÁRIOS DE APLICAÇÃO"

A comissão examinadora composta pelos professores: JULIANO BANDEIRA LIMA, DES/UFPE; VALDEMAR CARDOSO DA ROCHA JÚNIOR, DES/UFPE; HÉLIO MAGALHÃES DE OLIVEIRA, DE/UFPE; DANIEL CARVALHO DA CUNHA, CIN/UFPE e EMERSON ALEXANDRE DE OLIVEIRA LIMA, POLI/UPE sob a presidência do primeiro, consideram o candidato **PAULO HUGO ESPÍRITO SANTO LIMA APROVADO**.

Recife, 03 de dezembro de 2015.

CECILIO JOSÉ LINS PIMENTEL Coordenador do PPGEE	**JULIANO BANDEIRA LIMA** Coorientador e Membro Titular Interno
HÉLIO MAGALHÃES DE OLIVEIRA Membro Titular Externo	**VALDEMAR CARDOSO DA ROCHA JÚNIOR** Membro Titular Interno
DANIEL CARVALHO DA CUNHA Membro Titular Externo	**EMERSON ALEXANDRE DE OLIVEIRA LIMA** Membro Titular Externo

A Deus, que é Pai, Filho e Espírito Santo.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, porque é n'Ele que tenho a vida, o movimento e o ser (At.17, 28).

A paciência, devoção e compreensão da minha amada esposa Amanda foram indispensáveis para realização deste trabalho. O ambiente de amor e educação em que meus pais, minhas irmãs e todos os meus familiares construíram para mim, permitiu-me ser o que sou e lograr o que logrei. A todos meus mais sinceros e profundos agradecimentos.

Agradeço ao Prof. Ricardo Campello, por sua orientação e principalmente por me mostrar que sou capaz de ir muito mais além do que poderia imaginar. O respeito, a consideração e a dedicação que ele sempre demonstrou, certamente, forjaram o pesquisador, o professor e a pessoa que sou. Em igual medida, agradeço ao Prof. Juliano, por sua confiança, dedicação e presteza na orientação deste trabalho e de minha formação.

Agradeço aos professores, dos quais obtive incentivo, sabedoria e conhecimento. Às Professoras Márcia Mahon e Fernanda Alencar, e aos professores Cecílio Pimentel, Daniel Chaves, Francisco Madeiro, Gilson Jerônimo, Rafael Dueire, Raimundo Correa e Valdemar Cardoso. Em especial, agradeço ao Prof. Hélio Magalhães de Oliveira com o qual tive o imenso prazer de conviver.

Agradeço aos funcionários do DES que sempre me trataram como um profissionalismo e carinho imensos, em especial a Adréa Tenório e a Dona Cristina.

Aos meus estimados amigos que me acolheram tanto no mestrado e quanto no doutorado e com os quais preservo muita admiração e carinho. Cometerei a indelicadeza de não citá-los para não cometer o crime de esquecer-me de alguém.

Por fim, agradeço ao CNPq e a todos que contribuem com o Programa de Pós-Graduação em Engenharia Elétrica da UFPE.

RESUMO

As transformadas fracionais correspondem a uma generalização das transformadas clássicas em que potências não inteiras do operador são admitidas. Em virtude desta generalização, há uma maior flexibilidade na resolução de diversos problemas da Engenharia. Nesse contexto, outros tipos de transformadas são as definidas em corpos finitos, que propiciam vantagens relacionadas à inexistência de erros de truncagem ou arredondamento e baixa complexidade computacional. Aliando esses dois aspectos, foram definidas as transformadas fracionais em corpos finitos baseadas na expansão espectral do operador da transformada. Nesse caso, não é necessária a construção de conjuntos ortogonais de autovetores ou de sequências de Legendre em corpos finitos. Nesta tese, as transformadas fracionais de Fourier, Hartley, seno e cosseno tipos 1 e 4 em corpos finitos são introduzidas, utilizando-se uma abordagem baseada em funções de matrizes sobre corpos finitos. A abordagem proposta é comparada com outras abordagens da literatura, avaliando-se suas limitações, vantagens e desvantagens. Algumas vantagens da abordagem proposta são: há uma expressão fechada para computar as transformadas fracionais em corpos finitos; não há a necessidade de construção de conjuntos ortogonais de autovetores das matrizes de transformação; é possível utilizar os algoritmos rápidos já desenvolvidos para as transformadas clássicas. São apresentadas algumas propriedades da transformada fracional de Fourier em corpos finitos e a relação entre esta e a transformada fracional de Hartley em corpos finitos. Com essas ferramentas, são propostas e avaliadas algumas aplicações em cifragem de imagens, em marcas d'água frágeis usadas em imagens digitais e num sistema de comunicação multiusuário.

Palavras-chaves: Transformadas fracionais. Corpos finitos.

ABSTRACT

Fractional transforms correspond to a generalization of the classical transforms, where non integer powers of the transform operator are allowed. Due to this generalization, there is a greater flexibility in order to solve several problems in Engineering. In this context, other types of transforms used in Engineering are the transforms defined over finite fields, which provide advantages related to error-free computation and low computational complexity. Combining these two aspects, fractional transforms over finite fields were defined, based on the spectral expansion of the transform operator procedure. In this case, it is not necessary to construct orthogonal eigenvectors sets or Legendre sequences over finite fields. In this thesis, the finite field fractional Fourier, Hartley, sine and cosine types 1 and 4 transforms are introduced using a matrix function based procedure. The proposed technique is compared with others in the literature, and its limitations, advantages and disadvantages are evaluated. Some advantages of the proposed approach are: there is a closed form expression to compute finite field fractional transforms; it is not necessary to construct orthogonal eigenvector sets of the transforms matrices; it is possible to use fast algorithms already developed for classical transforms. Some properties of the new finite field fractional Fourier transforms are presented, including the relationship between the finite field fractional Fourier and Hartley transforms. Applications of the new transforms, in the areas of image encryption, digital image fragile watermarks and multiuser communication system, are suggested.

Keywords: Fractional transforms. Finite fields.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

FT	Transformada de Fourier (contínua)
DFT	Transformada discreta de Fourier
DHT	Transformada discreta de Hartley
DCT	Transformada discreta do cosseno
DST	Transformada discreta do seno
GDFT	Transformada discreta de Fourier generalizada
GDHT	Transformada discreta de Hartley generalizada
FFT	*Fast Fourier transform*
FrFT	Transformada fracional de Fourier (contínua)
DFrFT	Transformada fracional de Fourier discreta
DFrHT	Transformada fracional de Hartley discreta
DFrCT	Transformada fracional do cosseno discreta
DFrST	Transformada fracional do seno discreta
FFFT	Transformada de Fourier sobre corpos finitos
FFHT	Transformada de Hartley sobre corpos finitos
FFTT	Transformadas trigonométricas sobre corpos finitos
FFCT	Transformada do cosseno sobre corpos finitos
FFST	Transformada do seno sobre corpos finitos
GFFFT	Transformada de Fourier sobre corpos finitos generalizada
GFFHT	Transformada de Hartley sobre corpos finitos generalizada
FFNT	Tranformada numérica de Fourier-Fermat
HFNT	Tranformada numérica de Hartley-Fermat
FMNT	Tranformada numérica de Fourier-Mersenne
HMNT	Tranformada numérica de Hartley-Mersenne
GFrFT	Transformada fracional de Fourier em corpos finitos
GFrHT	Transformada fracional de Hartley em corpos finitos
GFrCT	Transformada fracional do cosseno em corpos finitos
GFrST	Transformada fracional do seno em corpos finitos
AES	*Advanced encryption standard*
CBC	*Cipher block chaining*
NPCR	*Number of pixels change rate*
UACI	*Unified average changing intensity*
PSNR	*Peak signal-to-noise ratio*
FFAC	*Finite field adder channel*

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

O conceito de transformada fracional se refere à generalização do operador transformada clássica, em que potências fracionais arbitrárias do operador são permitidas. Potências inteiras do operador podem ser vistas como sucessivas aplicações do operador transformada. Em sistemas discretos lineares, o operador de uma transformada é uma matriz de transformação, para a qual se pode definir e computar sua raiz quadrada, isto é, a potência $1/2$ dessa matriz, por exemplo. Considerando um vetor $\mathbf{x}$, uma matriz de transformação $\mathbf{T}$ e o vetor transformado $\mathbf{X} = \mathbf{T}\mathbf{x}$, ao aplicar duas vezes a transformada tem-se que $\mathbf{T}(\mathbf{T}\mathbf{x}) = \mathbf{T}^2\mathbf{x} = \mathbf{T}(\mathbf{X})$, a transformada do vetor $\mathbf{X}$. No entanto, o que representa o vetor obtido a partir da aplicação da raiz quadrada da matriz de transformação $(\mathbf{T}^{\frac{1}{2}}\mathbf{x})$ é uma questão de compreensão não tão direta.

Os primeiros trabalhos que abordaram essa questão surgiram no início do século XX com a proposta de se computar potências fracionais do operador da transformada de Fourier contínua (FT, do inglês *Fourier transform*). Os trabalhos sobre a transformada fracional de Fourier (FrFT, do inglês *fractional Fourier transform*) contínua se estenderam desde então, tornando-a a mais estudada das transformadas fracionais. É apresentada a seguir uma breve evolução cronológica dos estudos desta área:

- A ideia de potências fracionais do operador transformada de Fourier é introduzida, com uma abordagem matemática, em 1929 por Wiener [1];

- Em 1937, Condon [2] mostrou que o operador da FT gera um grupo cíclico de ordem 4, o qual é isomórfico a um grupo de rotações de um plano com ângulo de $\pi/2$ rad. Ele se deteve em encontrar um grupo de transformadas gerado pelo operador Hermitiano, para o qual o grupo

gerado pelo operador da FT fosse um subgrupo;

- Ainda com uma abordagem matemática, Kober [3], em 1939, estudou as transformadas fracionais contínuas, em especial a de Fourier e de Hankel;

- Em 1973, de Bruijn [4] apresentou um tratamento das distribuições de Wigner para análise harmônica e utiliza para tanto a transformada fracional de Fourier;

- A partir de 1980, a área teve maior atenção. Nesta década, Namias [5] retomou o estudo da transformada fracional de Fourier, generalizando o trabalho de Wiener e aplicando-o à mecânica quântica, sendo seguido por outros trabalhos [6];

- Em 1982, Dickinson *et al.* [7] analisaram a autoestrutura da matriz de transformação da transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*) introduzindo um método para se obter conjuntos ortogonais de autovetores. Propuseram também uma forma eficiente de computar potências fracionais da DFT;

- Na década de 1990, Santhanam *et al.* [8] introduziram a transformada fracional de Fourier discreta (DFrFT, do inglês *discrete FrFT*), Ozaktas *et al.* [9] apresentaram um método para computar digitalmente a FrFT, e Deng *et al.* [10] apresentaram um algoritmo para calcular a FrFT numericamente de maneira rápida;

- Ainda na década de 1990, Ozaktas retomou os estudos da transformada fracional de Fourier e o aplicou à óptica [9, 11], sendo seguido por outros trabalhos [12];

- Em 1994, Almeida [13] aplicou a FrFT à área de processamento de sinais e introduziu uma interpretação da FrFT bastante difundida: a FrFT como uma rotação no plano tempo-frequência;

- Em 1998, Pei *et al.* [14] apresentaram uma nova abordagem para definir as transformadas fracionais de Fourier e Hartley discretas com base em autovetores da matriz de transformação da DFT. No entanto, havia algumas ambiguidades na construção dessas matrizes. Com essa abordagem, podem ser construídas matrizes de transformação diferentes e válidas das transformadas fracionais discretas, pois não havia critérios para a ordenação de autovetores e de autovalores;

- Em 1999, a transformada fracional de Fourier discreta bidimensional [15] e a transformada fracional de Hadamard discreta [16] foram introduzidas por Pei *et al.*;

- Em 2000, Candan *et al.* [17] propuseram critérios de ordenação de autovetores e de autovalores, e de suas associações, introduzindo uma abordagem na qual não havia ambiguidades para a construção das matrizes da DFrFT;

- No início dos anos 2000, Pei *et al.* introduziram as transformadas fracionais do cosseno e do seno contínuas [18] e discretas [19];

- Com uma abordagem baseada em sequências de Legendre, Pei *et al.* [20] apresentaram uma nova forma de se obter autovetores da DFT e assim definir a DFrFT;

- Lima e Campello de Souza [21] definiram a transformada fracional de Fourier em corpos finitos usando uma abordagem similar à de Candan [17];

- Ainda com a abordagem baseada em sequências de Legendre, Pei introduziu a transformada numérica fracional de Fourier [22];

- Lima *et al.* [23] [24] definiram as transformadas fracionais do cosseno e do seno em corpos finitos;

- Lima *et al.* introduziram as transformadas fracionais de Fourier [25], de Hartley, do cosseno e do seno [26] em corpos finitos, baseadas em funções de matrizes.

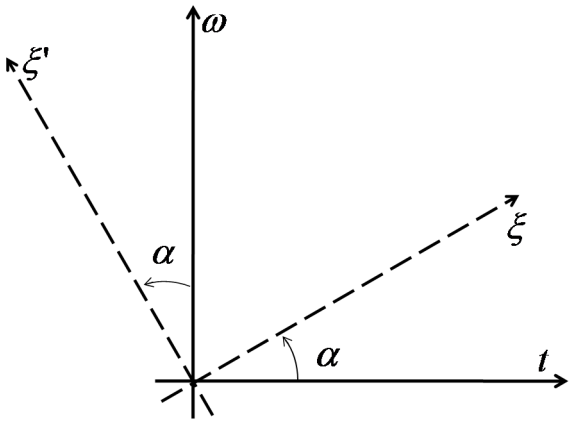
No contexto de processamento de sinais, Almeida mostrou que a aplicação da transformada fracional de Fourier contínua pode ser vista como uma rotação de um sinal no plano tempo-frequência por um ângulo arbitrário [13]. A Figura 1.1 apresenta uma ilustração do plano tempo-frequência. O sinal $x(t)$ no domínio do tempo pode ser rotacionado neste plano por um ângulo α, gerando o sinal $X_\alpha(\xi)$ no domínio fracional ξ. O sinal $X_\alpha(\xi)$ pode ser interpretado como o espectro fracional de $x(t)$. Nesse caso, a rotação pode ser feita pela aplicação da FrFT de ângulo (parâmetro fracional) α. No caso particular, em que $\alpha = \pi/2$, $X_{\pi/2}(\xi) = X(\omega)$ é seu espectro de frequências. Ainda nesse caso, a FrFT é a própria FT.

Definição 1.1

Seja $x(t)$ um sinal no domínio do tempo. A transformada fracional de Fourier de $x(t)$ é o sinal $X_\alpha(\xi)$ dado por [13]

$$X_\alpha(\xi) = \mathfrak{F}^\alpha x(t) := \int_{-\infty}^{\infty} x(t)\kappa_\alpha(t,\xi)dt, \tag{1.1}$$

Figura 1.1: *Plano Tempo-Frequência e um conjunto de coordenadas (ξ,ξ') obtidas pela rotação das coordenadas (t,ω) por um ângulo α.*



Fonte: Próprio Autor.

em que $\mathfrak{F}^{\alpha}$ é o operador da FrFT associado ao parâmetro fracional (ângulo) α, e $\kappa_{\phi}(t,\xi)$ é o núcleo da transformada definido como

$$\kappa_{\alpha}(t,\xi) := \begin{cases} \delta(t-\xi), & \text{se } \alpha = k\pi \\ \delta(t+\xi), & \text{se } \alpha = \pi + k\pi \\ \sqrt{\frac{1-j\cot(\alpha)}{2\pi}}\, e^{j\left(\frac{t^2+\xi^2}{2}\cot(\alpha)\right)} e^{-j\xi t \csc(\alpha)}, & \text{caso contrário,} \end{cases} \quad , \tag{1.2}$$

em que k é um inteiro e $\delta(.)$ representa o delta de Dirac, $\cot(.)$ e $\csc(.)$ representam a cotangente e a cossecante do argumento, respectivamente. □

O operador, $\mathfrak{F}^{\alpha}$, da FrFT apresenta algumas propriedades [11, 27, 28].

Propriedade 1.1

1. *Unitariedade $\left((\mathfrak{F}^{a})^{-1} = (\mathfrak{F}^{a})^{*}\right)$ [28, pp.7], em que $\{.\}^{*}$ representa o conjugado do argumento;*
2. *Aditividade de expoentes $\left(\mathfrak{F}^{a}\mathfrak{F}^{b} = \mathfrak{F}^{a+b}\right)$;*
3. *Redução ao operador identidade se $\alpha = 0$ $\left(\mathfrak{F}^{0}x(t) = x(t)\right)$;*
4. *Redução à transformada de Fourier usual (ordinária) se $\alpha = \pi/2$ $\left(\mathfrak{F}^{\pi/2}x(t) = X(\omega)\right)$;*
5. *Periodicidade $\left(\mathfrak{F}^{4k}x(t) = x(t)\right)$, para k inteiro.* □

Outra importante propriedade é que o núcleo da FrFT admite a seguinte expansão espectral [17]:

$$\kappa_{a}(t,\xi) = \sum_{n=0}^{\infty} \psi_{n}(t) e^{-j(\frac{\pi}{2}na)} \psi_{n}(\xi), \tag{1.3}$$

em que $\psi_n(t)$ denota a n-ésima função Hermite-Gaussiana e $(e^a)^n$ corresponde ao autovalor da FT $\lambda_n = e^{-j\frac{\pi}{2}n}$ elevado ao expoente a. A função Hermite-Gaussiana de n-ésima ordem é definida por

$$\psi_n(t) := \frac{2^{1/4}}{\sqrt{2^n n!}} H_n(\sqrt{2\pi}t) e^{-\pi t^2}, \;\; n = 0, 1, \ldots, \tag{1.4}$$

em que H_n é o n-ésimo polinômio de Hermite [28]. Analisando a Equação (1.3), observa-se que a função Hermite-Gaussiana de n-ésima ordem, $\psi_n(t)$, é uma autofunção da FrFT associada ao autovalor $e^{-j(\frac{\pi}{2}na)}$.

Em aplicações computacionais nas áreas de processamento de sinais de áudio, de imagens e de vídeo, sistemas de comunicações e segurança da informação, por exemplo, é necessária a definição de transformadas discretas, como é o caso da DFT. Para legitimar uma versão discreta da FrFT, assim com a DFT é para a FT, algumas propriedades fundamentais precisam ser satisfeitas [17]:

Propriedade 1.2

1. *Unitariedade;*
2. *Aditividade de expoentes;*
3. *Redução à identidade se $\alpha = 0$, e à DFT se $\alpha = 1$;*
4. *Aproximação numérica da transformada fracional de Fourier contínua.* □

Uma das primeiras propostas para se obter uma versão discreta da FrFT foi feita por Santhanam [8], em que eram tomadas amostras da FrFT. Seguindo esse trabalho, Ozaktas [9] propôs uma maneira de computar por meio digital a FrFT de maneira semelhante à amostragem de Santhanam. Apesar de satisfazerem às propriedades de unitariedade, da redução à DFT e à identidade, e de aproximação numérica com a FrFT, tais propostas falhavam em relação à propriedade de aditividade de expoentes.

Outra proposta para se definir uma versão discreta da FrFT foi tratada sem maiores detalhamentos no trabalho de Dickinson [7], em que o operador discreto é definido por meio de uma combinação linear de potências inteiras da matriz de transformação da DFT. Apesar de satisfazer à propriedade de aditividade de expoentes, ela falha na aproximação com a FrFT.

Como o operador FrFT pode ser escrito por meio da expansão espectral, procurou-se estabelecer a DFrFT utilizando a expansão espectral da DFT, análoga à Equação (1.3). Para tanto, é necessário obter versões discretas das funções Hermite-Gaussianas, de forma a serem empregadas como autovetores da DFT. Algumas abordagens que visam à construção de um conjunto ortogonal de autovetores da DFT e podem ser utilizados para se definir a DFrFT são destacadas a seguir.

- Autovetores da DFT podem ser obtidos por métodos numéricos como o método de eliminação de Gauss [20];

- Autovetores da DFT podem ser obtidos fazendo uma combinação linear entre um vetor e seus sucessivos vetores transformados. Se $\mathbf{s}$ é um vetor de componentes reais, então um autovetor $\mathbf{e}$ da matriz da DFT pode ser escrito como $\mathbf{e} = \mathbf{s} + \lambda^{-1}\mathbf{F}\mathbf{s} + \lambda^{-2}\mathbf{F}^2\mathbf{s} + \lambda^{-3}\mathbf{F}^3\mathbf{s}$, em que $\mathbf{F}$ é a matriz de transformação da DFT. Contudo, os autovetores obtidos por esse método não são necessariamente ortogonais [20];

- Amostragem de expansões periódicas de funções de Hermite [29, 30];

- Em [31], a técnica ZF (*zero forcing*) e a técnica PF (*periodic zero forcing*) são aplicadas a subespaços vetoriais para construir autovetores da DFT;

- Sequências generalizadas de Legendre [20];

- Matrizes que comutam com a matriz da DFT [14, 17, 32].

Com as duas últimas abordagens, as quatro propriedades fundamentais são satisfeitas. Após a proposição de diferentes métodos para se definir a DFrFT, foram introduzidas as transformadas fracionais de Hartley, do cosseno e do seno contínuas [18] e discretas [19]. As transformadas fracionais discretas, em especial a de Fourier e a do cosseno, têm sido usadas em cifragem de imagens [33], esquemas de marca d'água [34], amostragem e filtragem de sinais [35] e multiplexação de sinais [36, 37].

As transformadas definidas em estruturas algébricas finitas (corpos finitos) se apresentam como poderosas ferramentas, pois não necessitam de truncagem ou arredondamento, e possibilitam o uso de algoritmos rápidos que diminuem a complexidade aritmética requerida para calculá-las. Em processamento digital de sinais, transformadas numéricas são empregadas no cálculo de convoluções [38] e em filtragem [39, 40], na área de comunicações são empregadas em codificação e decodificação no domínio da frequência [41, 42] e construção de códigos de bloco lineares baseados em transformadas [43, 44]. Além disso, aplicações em segurança da informação surgem com a proposição de novos sistemas criptográficos [45].

Nos últimos anos, foram desenvolvidos alguns trabalhos com transformadas fracionais em corpos finitos [22, 46]. As abordagens se utilizam da expansão espectral da transformada de Fourier sobre corpos finitos (FFFT, do inglês *finite field Fourier transform*) e se concentram na extensão em corpos

finitos das abordagens de sequências generalizadas de Legendre [20] e de matrizes comutantes [17].

Em ambos os casos, é necessária a construção de um conjunto ortogonal de autovetores para cada transformada. Isso nem sempre é possível para corpos finitos de características específicas e para comprimentos de transformadas específicos.

Esta tese introduz as transformadas fracionais de Fourier, de Hartley, do seno e do cosseno em corpos finitos por meio da abordagem de funções de matrizes. As transformadas fracionais de Fourier, do seno e do cosseno do tipo 1 em corpos finitos baseadas na matriz comutante $\mathbf{S}$ são revisitadas [17], e é introduzida a transformada fracional de Hartley em corpos finitos baseada em matrizes comutantes. São introduzidas também as transformadas fracionais de Fourier e de Hartley generalizadas em corpos finitos, e as transformadas fracionais do seno e do cosseno do tipo 4 em corpos finitos baseadas na matriz comutante $\mathbf{E}$ [47].

Aplicações em que se utilizam as transformadas sobre corpos finitos usuais [48], podem ser projetadas e implementadas, com maior flexibilidade, através da utilização de transformadas fracionais em corpos finitos. Com essa motivação, são apresentadas também algumas aplicações das transformadas fracionais em corpos finitos.

1.1 Contribuições

O objetivo desta tese é a construção de novas transformadas fracionais em corpos finitos. As principais contribuições são as seguintes:

- Definição da transformada fracional de Hartley em corpos finitos por meio da expansão espectral, em que os conjuntos de autovetores são obtidos a partir da matriz comutante $\mathbf{S}$.

- Definição das transformadas fracionais de Fourier e Hartley generalizadas, e transformadas fracionais do seno e cosseno tipo 4 em corpos finitos por meio da expansão espectral, em que os conjuntos de autovetores são obtidos a partir da matriz comutante $\mathbf{E}$.

- Procedimento para se construir matrizes de transformação das transformadas fracionais sem a necessidade de se construir conjuntos ortogonais de autovetores, o que representa uma redução da complexidade computacional das transformadas.

- Definição das transformadas fracionais de Fourier, Hartley, seno e cosseno tipos 1 e 4 em corpos finitos por meio de expressões analíticas baseadas em funções de matrizes.

- Análise da autoestrutura das matrizes de transformação das transformadas fracionais em corpos finitos.

- Propriedades da transformada fracional de Fourier em corpos finitos: linearidade, deslocamento no tempo e reversão no tempo.

- Definição e análise da autoestrutura da matriz $\mathbf{D}$ que relaciona as transformadas de Fourier e Hartley.

- Expressão analítica para computar uma potência fracional da matriz $\mathbf{D}$.

- Relação entre a transformada fracional de Fourier e de Hartley em corpos finitos.

- Análise da limitação do procedimento de matrizes comutantes para construção de conjuntos ortogonais de autovetores.

- Análise da complexidade computacional para computar as transformadas fracionais em corpos finitos.

- Análise de algoritmos rápidos para reduzir a complexidade computacional das transformadas fracionais em corpos finitos.

- Proposta de um esquema de cifragem de imagens digitais que utiliza transformadas fracionais em corpos finitos baseadas em funções de matrizes.

- Proposta de um esquema de marca d'água frágil que utiliza a transformada fracional do cosseno em corpos finitos baseada em funções de matrizes.

- Proposta de um esquema de comunicação multiusuário em corpos finitos que utiliza a transformada fracional de Fourier em corpos finitos baseada na expansão espectral.

1.2 Organização do trabalho

Após o **Capítulo 1**, esta tese está organizada da seguinte forma:

Capítulo 2: Esse capítulo apresenta as ferramentas matemáticas utilizadas nesta tese. São expostos alguns conceitos de trigonometria em corpos finitos, bem como são apresentadas as definições de algumas transformadas em corpos finitos.

Capítulo 3: Esse capítulo aborda os conceitos de transformadas fracionais em corpos finitos, revisando dois procedimentos para construção das matrizes de transformação da transformada fracional de Fourier em corpos finitos. São introduzidas as transformadas fracionais de Fourier e Hartley generalizadas, e as transformadas fracionais do seno e do cosseno do tipo 4 em corpos finitos. São discutidas as limitações de cada procedimento e apresentadas as definições das transformadas do cosseno e do seno em corpos finitos.

Capítulo 4: É apresentado um novo procedimento para construção de matrizes de transformação para transformadas fracionais, baseado em funções de matrizes. Com a nova abordagem são definidas as transformadas fracionais de Fourier, Hartley, seno e cosseno em corpos finitos, sendo apresentadas propriedades e relações entre as transformadas.

Capítulo 5: Esse capítulo apresenta algumas aplicações em criptografia e comunicações das ferramentas desenvolvidas nos capítulos anteriores.

Capítulo 6: Esse capítulo apresenta as conclusões do trabalho e indica sugestões para a continuidade da pesquisa.

Apêndice A: Apresenta uma lista de todas as transformadas citadas e introduzidas nesta tese.

Apêndice B: Apresenta as demonstrações de algumas proposições e lemas introduzidas no **Capítulo 3**.

Apêndice C: Apresenta a demonstração da obtenção dos autovalores da matriz **D** que relaciona as transformadas de Hartley e Fourier.

Apêndice D: É apresentada a lista dos trabalhos publicados e submetidos, decorrentes da pesquisa relatada nesta tese.

CAPÍTULO 2

TRANSFORMADAS SOBRE CORPOS FINITOS

Transformadas definidas sobre estruturas algébricas finitas são atrativas por diversos aspectos: no cálculo das transformadas ou de convoluções, por meio dessas transformadas, há precisão infinita, pois não existem erros de truncagem ou arredondamento; a aritmética inteira (de ponto-fixo) requer menor complexidade computacional em comparação com a aritmética de ponto flutuante; e, é possível a construção de algoritmos rápidos, incluindo algoritmos com complexidade multiplicativa nula. A transformada de Fourier sobre corpos finitos (FFFT) foi inicialmente introduzida por Pollard [49] para computar convoluções cíclicas usando aritmética inteira [50]. A FFFT é utilizada também para outras aplicações nas áreas de processamento digital de sinais [41], códigos corretores de erros [43, 44, 51] e criptografia [52].

Outras importantes transformadas como as de Hartley, do cosseno e do seno, só foram definidas em corpos finitos após a introdução de uma trigonometria em corpos finitos [53]. Neste capítulo são revisadas as ferramentas matemáticas relacionadas à trigonometria em corpos finitos e às definições das transformadas de Fourier, de Hartley, do seno e do cosseno de corpo finito.

2.1 Trigonometria sobre corpos finitos

Definição 2.1

O conjunto de inteiros gaussianos (Gaussian Integers) sobre $\mathrm{GF}(p)$*,* p *ímpar, é o conjunto* $\mathrm{GI}(p) := \{a + jb, a, b \in \mathrm{GF}(p)\}$*, em que* j^2 *não é resíduo quadrático sobre* $\mathrm{GF}(p)$*.* □

Definição 2.2

O conjunto unimodular de $\mathrm{GI}(p)$*,* p *ímpar, é o conjunto de elementos da forma* $(a+jb) \in \mathrm{GI}(p)$*, tais que* $a^2 + b^2 \equiv 1 \pmod{p}$. □

De acordo com a Definição 2.1, um elemento de $\mathrm{GI}(p)$ pode ser visto como um número "complexo", em que a é a parte "real" e b é a parte "imaginária". Se $p \equiv 3 \pmod{4}$, $j^2 = -1$ não é resíduo quadrático sobre $\mathrm{GF}(p)$ [54, p. 177], isto é, $\sqrt{-1} \equiv \sqrt{p-1} \mod(p)$ não pertence a $\mathrm{GF}(p)$. Dessa forma, $j = \sqrt{-1}$ pode ser usado como unidade imaginária, assim como acontece no corpo dos números reais. Se $p \equiv 3 \pmod{8}$ ou $p \equiv 5 \pmod{8}$, o elemento 2 não é resíduo quadrático sobre $\mathrm{GF}(p)$ [54, p. 180], isto é, $\sqrt{2}$ não pertence a $\mathrm{GF}(p)$. Dessa forma, nestes casos, $j = \sqrt{2}$ poderia ser usado como "unidade" imaginária.

A trigonometria sobre corpos finitos foi introduzida por Campello de Souza *et al.* em 1998 [53], com o propósito de se definir a transformada da Hartley sobre corpos finitos. Na proposta, as funções seno e cosseno sobre corpos finitos são definidas em $\mathrm{GI}(p)$, em que $p \neq 2$. Sem perda de generalidade, no que se segue, p é um número primo ímpar e a unidade imaginária usada na construção de $\mathrm{GI}(p)$ é $\sqrt{-1}$, a menos de reconsiderações explícitas no texto.

Definição 2.3

Seja $\zeta \in \mathrm{GI}(p)$ *um elemento de ordem multiplicativa* $\mathrm{ord}(\zeta) = N$*. As funções cosseno e seno sobre* $\mathrm{GI}(p)$ *relacionadas a* ζ *são computadas módulo* p*, respectivamente, por*

$$\cos_\zeta(x) \;:=\; \frac{(\zeta^x + \zeta^{-x})}{2} \tag{2.1}$$

e

$$\sin_\zeta(x) \;:=\; \frac{(\zeta^x - \zeta^{-x})}{2\sqrt{-1}}, \tag{2.2}$$

para $x = 0, 1, \ldots, N-1$. □

Essas funções apresentam propriedades similares (aditividade de arcos, círculo unitário, simetria, etc.) a suas funções trigonométricas análogas definidas no corpo dos reais [53, 55].

2.2 Transformadas em corpos finitos

Nesta tese, a equação matricial $\mathbf{X}_M = \mathbf{M}\mathbf{x}$ expressa a relação entre um vetor $\mathbf{x}$ e seu vetor transformado $\mathbf{X}_M$, em que $\mathbf{M}$ corresponde à matriz de transformação de alguma transformada. O vetor transformado é grafado em letra maiúscula e seu índice está relacionado à transformada empregada.

A fim de evitar ambiguidades em relação aos índices, a i-ésima componente do vetor $\mathbf{x}$ é denotada por $x[i]$ e a k-ésima componente do vetor transformado $\mathbf{X}_M$ é denotada por $X_M[k]$. Para matrizes, na notação $[M]_{i,k}$, i está relacionado às linhas e k está relacionado às colunas de $\mathbf{M}$.

2.2.1 A transformada de Fourier sobre corpos finitos

A transformada de Fourier sobre corpos finitos (FFFT, do inglês *finite field Fourier transform*) foi introduzida por Pollard em 1971 [49].

Definição 2.4

Seja $\zeta \in \mathrm{GF}(p^m)$ *um elemento de ordem multiplicativa* $\mathrm{ord}(\zeta) = N$. *A FFFT do vetor* $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, *de comprimento* N, *é o vetor* $\mathbf{X}_F = (X_F[k])$, $X_F[k] \in \mathrm{GF}(p^m)$, *em que*

$$X_F[k] := \sqrt{N^{-1}} \pmod p \left[\sum_{i=0}^{N-1} x[i]\zeta^{ki} \right], \qquad k = 0, 1, \ldots, N-1. \tag{2.3}$$

□

Para não deixar as equações carregadas de informação, a partir deste ponto, a informação $\sqrt{N^{-1}}(\mathrm{mod} p)$ é substituída por $\sqrt{N^{-1}}$. No entanto, o cálculo de $\sqrt{N^{-1}}$ é feito em $\mathrm{GF}(p)$.

Teorema 2.1

A FFFT inversa do vetor $\mathbf{X}_F = (X_F[k])$, $X_F[k] \in \mathrm{GF}(p^m)$, *de comprimento* N *é o vetor* $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, *em que*

$$x[i] = \sqrt{N^{-1}} \sum_{k=0}^{N-1} X_F[k]\zeta^{-ki}, \qquad i = 0, 1, \ldots, N-1. \qquad \square$$

Na equação matricial da FFFT unitária $\mathbf{X}_F = \mathbf{F}\mathbf{x}$, tem-se que $[F]_{i,k} = \sqrt{N^{-1}}\zeta^{ki}$.

Nesta tese, os corpos finitos em análise tem característica p, em que p é um número primo ímpar, e tem ordem p ou p^2, isto é, a análise se concentra em $\mathrm{GF}(p)$ e $\mathrm{GI}(p)$ que é isomórfico a $\mathrm{GF}(p^2)$. Assim, não se abordará outros corpos de extensão além de $\mathbf{GI}(p)$.

Exemplo 2.1 – FFFT de comprimento 8 em GF(257)

Considerando o elemento $\zeta = 4 \in \mathrm{GI}(257)$, *com ordem multiplicativa* $\mathrm{ord}(4) = 8$, *a FFFT do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255)$ *é o vetor* $\mathbf{X}_F = \mathbf{F}\mathbf{x} = (47, 22, 195, 95, 218, 14, 180, 137)$, *em que*

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

2.2.2 A transformada de Hartley sobre corpos finitos

A transformada de Hartley sobre corpos finitos (FFHT, do inglês *finite field Hartley transform*) foi introduzida por Campello de Souza *et al.* em 1998 [53].

Definição 2.5

Seja $\zeta \in \mathrm{GI}(p)$ *um elemento de ordem multiplicativa* $\mathrm{ord}(\zeta) = N$*. A FFHT unitária do vetor* $\mathbf{x} = (x[i])$*,* $x[i] \in \mathrm{GF}(p)$*, de comprimento* N*, é o vetor* $\mathbf{X}_H = (X_H[k])$*,* $X_H[k] \in \mathrm{GI}(p)$*, em que*

$$X_H[k] := \sqrt{N^{-1}} \sum_{i=0}^{N-1} x[i] \, \mathrm{cas}_\zeta(ki), \;\; k = 0, 1, \ldots, N-1, \tag{2.4}$$

e $\mathrm{cas}_\zeta(x) := \cos_\zeta(x) + \mathrm{sen}_\zeta(x)$. $\square$

Teorema 2.2

A FFHT inversa do vetor $\mathbf{X}_H = (X_H[k])$*,* $X_H[k] \in \mathrm{GI}(p)$*, de comprimento* N*, é o vetor* $\mathbf{x} = (x[i])$*,* $x[i] \in \mathrm{GI}(p)$*, em que*

$$x[i] = \sqrt{N^{-1}} \sum_{k=0}^{N-1} X_H[k] \mathrm{cas}_\zeta(ki), \;\; i = 0, 1, \ldots, N-1. \tag{2.5}$$

$\square$

A prova do Teorema 2.2 pode ser encontrada em [53]. A FFHT inversa é obtida com a mesma expressão da FFHT, ou seja, aplicando duas vezes a transformada de Hartley a um vetor obtém-se o próprio vetor. Diz-se então que a transformada de Hartley é uma involução. Na equação matricial da FFHT $\mathbf{X}_H = \mathbf{H}\mathbf{x}$, tem-se que $[H]_{i,k} = \sqrt{N^{-1}} \, \mathrm{cas}_\zeta(ki)$.

Nota 2. 1 A transformada de Hartley foi proposta como uma transformada que mapeia dos reais para os reais. No entanto, a transformada de Hartley sobre corpos finitos faz um mapeamento

de $\mathrm{GF}(p)$ para um corpo de extensão $\mathrm{GF}(p^m)$. Apesar deste aparente desvio de objetivo, a transformada de Hartley sobre corpos finitos é aplicada em diversas áreas da Engenharia.

Exemplo 2.2 – FFHT de comprimento 8 em GF(31)

Considerando o elemento $\zeta = 4 + 4j \in \mathrm{GI}(31)$*, com ordem multiplicativa* $\mathrm{ord}(4 + 4j) = 8$*, a FFHT do vetor* $\mathbf{x} = (11, 17, 9, 27, 4, 23, 11, 21)$ *é o vetor* $\mathbf{X}_H = \mathbf{H}\mathbf{x} = (29, 7, 5, 21, 18, 13, 6, 15)$*, em que*

$$\mathbf{H} = \begin{bmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 16 & 2 & 0 & 29 & 15 & 29 & 0 \\ 2 & 2 & 29 & 29 & 2 & 2 & 29 & 29 \\ 2 & 0 & 29 & 16 & 29 & 0 & 2 & 15 \\ 2 & 29 & 2 & 29 & 2 & 29 & 2 & 29 \\ 2 & 15 & 2 & 0 & 29 & 16 & 29 & 0 \\ 2 & 29 & 29 & 2 & 2 & 29 & 29 & 2 \\ 2 & 0 & 29 & 15 & 29 & 0 & 2 & 16 \end{bmatrix}. \qquad \square$$

Exemplo 2.3 – FFHT de comprimento 8 em GI(257)

Considerando o elemento $\zeta = 4 \in \mathrm{GF}(257)$*, com ordem multiplicativa* $\mathrm{ord}(4) = 8$*, a FFHT do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255)$ *é o vetor* $\mathbf{X}_H = \mathbf{H}\,\mathbf{x} = (210, 49 + 71j, 198 + 136j, 74 + 169j, 39, 74 + 88j, 198 + 121j, 49 + 186j)$*, em que*

$$\mathbf{H} = \begin{bmatrix} 242 & 242 & 242 & 242 & 242 & 242 & 242 & 242 \\ 242 & 193 + 253j & 240j & 64 + 253j & 15 & 64 + 4j & 17j & 193 + 4j \\ 242 & 240j & 15 & 17j & 242 & 240j & 15 & 17j \\ 242 & 64 + 253j & 17j & 193 + 253j & 15 & 193 + 4j & 240j & 64 + 4j \\ 242 & 15 & 242 & 15 & 242 & 242 & 242 & 15 \\ 242 & 64 + 4j & 240j & 193 + 4j & 15 & 193 + 253j & 17j & 64 + 253j \\ 242 & 17j & 15 & 240j & 242 & 17j & 15 & 240j \\ 242 & 193 + 4j & 17j & 64 + 4j & 15 & 64 + 253j & 240j & 193 + 253j \end{bmatrix}. \qquad \square$$

2.2.3 Transformadas generalizadas em corpos finitos

A transformada discreta de Fourier pode ser generalizada no sentido de permitir deslocamentos em seus índices, sendo assim chamada de transformada discreta de Fourier generalizada (GDFT, do inglês *generalized discrete Fourier transform*). A transformada generalizada pode ser aplicada a vetores que foram submetidos a algum tipo de extensão, para a esquerda e/ou para a direita, segundo algum critério de simetria. O núcleo de transformação da DFT é um caso particular do núcleo da transformada discreta de Fourier generalizada [56, 57]. Um caso especial ocorre quando o núcleo da transformada discreta de Fourier generalizada é $e^{-j\left(\frac{2\pi}{N}(i+0,5)(k+0,5)\right)}$. A partir deste ponto em diante, a transformada discreta de Fourier generalizada se refere apenas a este último caso especial.

Definida dessa maneira, a autoestrutura da GDFT está relacionada com as transformadas trigonométricas do tipo 4, assim como a DFT está relacionada com as transformadas trigonométricas do tipo 1 [58]. O núcleo da transformada discreta de Hartley generalizada [58, 59] (GDHT, do inglês *generalized discrete Hartley transform*) é $\operatorname{cas}\left((i+0,5)(k+0,5)\right)$. Com o propósito de analisar a autoestrutura das transformadas trigonométricas, são definidas as transformadas de Fourier e de Hartley sobre corpos finitos generalizadas.

Definição 2.6

Seja $\zeta \in \mathrm{GF}(p^m)$ um elemento de ordem multiplicativa $\mathrm{ord}(\zeta) = N$. A transformada de Fourier sobre corpos finitos generalizada (GFFFT, do inglês generalized finite field Fourier transform)[60, pp. 72] do vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, de comprimento N, é o vetor $\mathbf{X}_F = (X_F[k])$, $X_F[k] \in \mathrm{GF}(p^m)$, em que

$$X_F[k] := \sqrt{N^{-1}} \sum_{i=0}^{N-1} x[i]\zeta^{(k+1/2)(i+1/2)}, \;\; k = 0, 1, \ldots, N-1. \tag{2.6}$$

□

Teorema 2.3

A GFFFT inversa do vetor $\mathbf{X}_F = (X_F[k])$, $X_F[k] \in \mathrm{GF}(p^m)$, de comprimento N, é o vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, em que

$$x[i] = \sqrt{N^{-1}} \sum_{k=0}^{N-1} X_F[k]\zeta^{-(k+1/2)(i+1/2)}, \;\; i = 0, 1, \ldots, N-1. \qquad \square$$

A prova do Teorema 2.3 é encontrada em [60, pp. 72], e é análoga à prova do Teorema 2.1. Na equação matricial da GFFFT, $\mathbf{X}_F = \mathbf{F_G x}$, tem-se que $[F_G]_{i,k} = \sqrt{N^{-1}}\zeta^{(k+1/2)(i+1/2)}$. Neste caso,

o termo $\zeta^{(k+1/2)(i+1/2)}$ pode ser reescrito como

$$\begin{aligned}\zeta^{(k+1/2)(i+1/2)} &= \zeta^{\frac{4ki+2(k+i)+1}{4}} = \zeta^{ki}\zeta^{\frac{k+i}{2}}\zeta^{\frac{1}{4}} \\ &= \zeta^{ki}(\sqrt{\zeta})^{k+i}(\sqrt[4]{\zeta}). \end{aligned} \tag{2.7}$$

Assim, para que os elementos de $\mathbf{X}_F$ pertençam a $\mathrm{GF}(p)$ é necessário que $\sqrt[4]{\zeta} \in \mathrm{GF}(p)$. Por esta razão, é necessário que o elemento ζ tenha ordem multiplicativa da forma $\mathrm{ord}(\zeta) = 4m$, para m inteiro.

Exemplo 2.4 – GFFFT de comprimento 8 em GF(257)

Considerando o elemento $\zeta = 4 \in \mathrm{GF}(257)$*, com ordem multiplicativa* $\mathrm{ord}(4) = 8$*, a GFFFT do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255)$ *é o vetor* $\mathbf{X}_F = \mathbf{F_G}\ \mathbf{x} = (24, 180, 74, 168, 29, 176, 41, 149)$*, em que*

$$\mathbf{F_G} = \begin{bmatrix} 129 & 1 & 2 & 4 & 8 & 16 & 32 & 64 \\ 1 & 8 & 64 & 255 & 241 & 129 & 4 & 32 \\ 2 & 64 & 249 & 1 & 32 & 253 & 129 & 16 \\ 4 & 255 & 1 & 128 & 193 & 32 & 241 & 8 \\ 8 & 241 & 32 & 193 & 128 & 1 & 255 & 4 \\ 16 & 129 & 253 & 32 & 1 & 249 & 64 & 2 \\ 32 & 4 & 129 & 241 & 255 & 64 & 8 & 1 \\ 64 & 32 & 16 & 8 & 4 & 2 & 1 & 129 \end{bmatrix}. \tag{2.8}$$

□

A transformada generalizada de Hartley sobre corpos finitos é um resultado da pesquisa e se apresenta como contribuição da tese.

Definição 2.7

Seja $\zeta \in \mathrm{GI}(p)$ *um elemento de ordem multiplicativa* $\mathrm{ord}(\zeta) = N$*. A transformada de Hartley sobre corpos finitos generalizada (GFFHT, do inglês generalized finite field Hartley transform) unitária do vetor* $\mathbf{x} = (x[i])$*,* $x[i] \in \mathrm{GF}(p)$*, de comprimento* N*, é o vetor* $\mathbf{X}_H = (X_H[k])$*,* $X_H[k] \in \mathrm{GI}(p)$*, em que*

$$X_H[k] := \sqrt{N^{-1}} \sum_{i=0}^{N-1} x[i]\mathrm{cas}_\zeta\left((k+1/2)(i+1/2)\right),\ \ k = 0, 1, \ldots, N-1. \tag{2.9}$$

□

Teorema 2.4

A GFFHT inversa do vetor $\mathbf{X}_H = (X_H[k])$, $X_H[k] \in \mathrm{GI}(p)$, *de comprimento* N, *é o vetor* $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GI}(p)$, *em que*

$$x[i] = \sqrt{N^{-1}} \sum_{k=0}^{N-1} X_H[k] \mathrm{cas}_\zeta \left((k+1/2)(i+1/2)\right), \;\; i = 0, 1, \ldots, N-1. \tag{2.10}$$

□

Demonstração:

Da Equação 2.9, tem-se que

$$X_H[k] = \sqrt{N^{-1}} \sum_{i=0}^{N-1} x[i] \mathrm{cas}_\zeta \left(k'i'\right),$$

em que $i' = i + 1/2$ e $k' = k + 1/2$, para $k = 0, \ldots, N-1$. Considere o vetor $\mathbf{y} = \mathbf{H}\mathbf{X}_H$, cujas componentes são dadas por

$$y[n] \;\; = \;\; \sqrt{N^{-1}} \sum_{k=0}^{N-1} X_H[k] \mathrm{cas}_\zeta \left(k'n'\right),$$

em que $n' = n + 1/2$, para $n = 0, \ldots, N-1$.

Mostra-se que as funções cas_ζ são otogonais [53], ou seja,

$$\mathrm{cas}_\zeta \left(k'i'\right) \mathrm{cas}_\zeta \left(k'n'\right) = \begin{cases} 0, & \text{se } i' \neq n', \\ N, & \text{se } i' = n'. \end{cases}$$

Assim, para $n = 0, \ldots, N-1$ tem-se que

$$\begin{aligned} y[n] \;\; &= \;\; N^{-1} \sum_{k=0}^{N-1} \sum_{i=0}^{N-1} x[i] \mathrm{cas}_\zeta \left(k'i'\right) \mathrm{cas}_\zeta \left(k'n'\right) \\ &= \;\; \begin{cases} 0, & \text{se } i' \neq n', \\ x[i], & \text{se } i' = n'. \end{cases} \end{aligned}$$

Portanto, $\mathbf{y} = \mathbf{x}$. ■

Na equação matricial da GFFHT, $\mathbf{X}_H = \mathbf{H_G}\mathbf{x}$, tem-se que $[H_G]_{i,k} = \sqrt{N^{-1}} \mathrm{cas}_\zeta \left((k+1/2)(i+1/2)\right)$. Pela mesma razão exposta para a GFFFT, para se obter a matriz de transformação da GFFHT, é necessário que o elemento ζ tenha ordem multiplicativa da forma $\mathrm{ord}(\zeta) = 4m$, para m inteiro.

Exemplo 2.5 – GFFHT de comprimento 8 em GI(257)

Considerando o elemento $\zeta = 4 \in \mathrm{GF}(257)$, *com ordem multiplicativa* $\mathrm{ord}(4) = 8$, *a GFFHT do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255)$ *é o vetor* $\mathbf{X}_H = \mathbf{H_G}\,\mathbf{x} = (224, 229, 5, 164, 25, 107, 90, 92)$, *em que*

$$\mathbf{H_G} = \begin{bmatrix} 159 & 106 & 106 & 159 & 163 & 120 & 137 & 94 \\ 106 & 163 & 94 & 151 & 137 & 159 & 159 & 137 \\ 106 & 94 & 94 & 106 & 137 & 98 & 159 & 120 \\ 159 & 151 & 106 & 98 & 163 & 137 & 137 & 163 \\ 163 & 137 & 137 & 163 & 98 & 106 & 151 & 159 \\ 120 & 159 & 98 & 137 & 106 & 94 & 94 & 106 \\ 137 & 159 & 159 & 137 & 151 & 94 & 163 & 106 \\ 94 & 137 & 120 & 163 & 159 & 106 & 106 & 159 \end{bmatrix}. \tag{2.11}$$
□

2.2.4 Transformadas trigonométricas em corpos finitos

A família das transformadas trigonométricas (FFTT, do inglês *finite field trigonometric transforms*) é constituída de oito tipos de transformadas do cosseno (FFCT, do inglês *finite field cosine transform*) e de oito tipos de transformadas do seno (FFST, do inglês *finite field sine transform*) [60, 61]. A construção de cada FFTT é baseada em extensões simétricas de um sequência com elementos em um corpo finito e requer a definição da função de ponderação

$$\beta[r] := \begin{cases} \sqrt{2^{-1}} \pmod p, & r = 0 \text{ ou } N, \\ 1, & r = 1, 2, \ldots, N-1. \end{cases}$$

Nesta tese, são abordadas apenas transformadas trigonométricas tipos 1 e 4 unitárias, em virtude da relação entre essas e as transformadas de Fourier e de Fourier generalizada, respectivamente.

Definição 2.8

Seja $\zeta \in \mathrm{GI}(p)$ um elemento de ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$. A transformada do cosseno sobre corpos finitos tipo 1 (FFCT-1) do vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, de comprimento $N+1$ é o vetor $\mathbf{X}_{C1} = (X_{C1}[k])$, $X_{C1}[k] \in \mathrm{GI}(p)$, em que

$$X_{C1}[k] := \sqrt{2N^{-1}} \sum_{i=0}^{N} \beta[i]\, \beta[k]\, x[i]\, \cos_\zeta(ki), \;\; k = 0, 1, \ldots, N. \tag{2.12}$$
□

Teorema 2.5

A FFCT-1 inversa do vetor $\mathbf{X}_{C1} = (X_{C1}[k])$, $X_{C1}[k] \in \mathrm{GI}(p)$, de comprimento $N+1$, é o vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GI}(p)$, em que

$$x[i] = \sqrt{2N^{-1}} \sum_{k=0}^{N} \beta[k]\, \beta[i]\, X_{C1}[i]\, \cos_\zeta(ki), \;\; i = 0, 1, \ldots, N. \tag{2.13}$$
□

A prova do Teorema 2.5 pode ser encontrada em [61]. Na equação matricial da FFCT-1, $\mathbf{X}_{C1} = \mathbf{C}_1\mathbf{x}$, tem-se que $[C_1]_{i,k} = \beta[i]\ \beta[k]\sqrt{2N^{-1}}\cos_\zeta(ki)$.

Definição 2.9

Seja $\zeta \in \mathrm{GI}(p)$ um elemento de ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$. A transformada do cosseno sobre corpos finitos tipo 4, FFCT-4, do vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, de comprimento N, é o vetor $\mathbf{X}_{C4} = (X_{C4}[k])$, $X_{C4}[k] \in \mathrm{GI}(p)$, em que

$$X_{C4}[k] := \sqrt{2N^{-1}} \sum_{i=0}^{N-1} x[i]\ \cos_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right),\ \ k = 0, 1, \ldots, N-1. \tag{2.14}$$

□

Teorema 2.6

A FFCT-4 inversa do vetor $\mathbf{X}_{C4} = (X_{C4}[k])$, $X_{C4}[k] \in \mathrm{GI}(p)$, de comprimento N, é o vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GI}(p)$, em que

$$x[i] = \sqrt{2N^{-1}} \sum_{k=0}^{N-1} X_{C4}[k]\ \cos_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right),\ \ i = 0, 1, \ldots, N-1. \tag{2.15}$$

□

A prova do Teorema 2.6 pode ser encontrada em [61]. Na equação matricial da FFCT-4, $\mathbf{X}_{C4} = \mathbf{C}_4\mathbf{x}$, tem-se que $[C_4]_{i,k} = \sqrt{2N^{-1}}\cos_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right)$.

Definição 2.10

Seja $\zeta \in \mathrm{GI}(p)$ um elemento de ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$. A transformada do seno sobre corpos finitos tipo 1, FFST-1, do vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, de comprimento $N-1$, é o vetor $\mathbf{X}_{S1} = (X_{S1}[k])$, $X_{S1}[k] \in \mathrm{GI}(p)$, em que

$$X_{S1}[k] := \sqrt{2N^{-1}} \sum_{i=0}^{N-1} x[i]\ \sin_\zeta(ki),\ \ k = 1, 2, \ldots, N-1. \tag{2.16}$$

□

Teorema 2.7

A FFST-1 inversa do vetor $\mathbf{X}_{S1} = (X_{S1}[k])$, $X_{S1}[k] \in \mathrm{GI}(p)$ de comprimento $N-1$, é o vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GI}(p)$, em que

$$x[i] = \sqrt{2N^{-1}} \sum_{k=0}^{N-1} X_{S1}[k]\ \sin_\zeta(ki),\ \ i = 1, 2, \ldots, N-1. \tag{2.17}$$

□

A prova do Teorema 2.7 pode ser encontrada em [61]. Na equação matricial da FFST-1, $\mathbf{X}_{S1} = \mathbf{S}_1\mathbf{x}$, tem-se que $[S_1]_{i,k} = \sqrt{2N^{-1}}\,\mathrm{sin}_\zeta(ki)$.

Definição 2.11

Seja $\zeta \in \mathrm{GI}(p)$ *um elemento de ordem multiplicativa* $\mathrm{ord}(\zeta) = 2N$*. A transformada do seno sobre corpos finitos tipo* 4*, FFST-*4*, do vetor* $\mathbf{x} = (x[i])$*,* $x[i] \in \mathrm{GF}(p)$*, de comprimento* N *é o vetor* $\mathbf{X}_{S4} = (X_{S4}[k])$*,* $X_{S4}[k] \in \mathrm{GI}(p)$*, em que*

$$X_{S4}[k] := \sqrt{2N^{-1}} \sum_{i=0}^{N-1} x[i]\ \mathrm{sin}_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right),\ \ k = 0, 1, \ldots, N-1. \tag{2.18}$$

□

Teorema 2.8

A FFST-4 inversa do vetor $\mathbf{X}_{S4} = (X_{S4}[k])$*,* $X_{S4}[k] \in \mathrm{GI}(p)$*, de comprimento* N*, é o vetor* $\mathbf{x} = (x[i])$*,* $x[i] \in \mathrm{GI}(p)$*, em que*

$$x[i] = \sqrt{2N^{-1}} \sum_{k=0}^{N-1} X_{S4}[k]\ \mathrm{sin}_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right),\ \ i = 0, 1, \ldots, N-1. \tag{2.19}$$

□

A prova do Teorema 2.8 pode ser encontrada em [61]. Na equação matricial da FFST-4, $\mathbf{X}_{S4} = \mathbf{S}_4\mathbf{x}$, tem-se que $[S_4]_{i,k} = \sqrt{2N^{-1}}\,\mathrm{sin}_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right)$.

Exemplo 2.6 – FFCT-1 de comprimento 9 em GF(257)

Considerando o elemento $\zeta = 2 \in \mathrm{GF}(257)$*, com ordem multiplicativa* $\mathrm{ord}(2) = 16$*, a FFCT-1 do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255, 30)$ *é o vetor* $\mathbf{X}_{C1} = \mathbf{C}_1\mathbf{x} = (247, 187, 65, 87, 120, 38, 107, 143, 161)$*, em que*

$$\mathbf{C}_1 = \begin{bmatrix} 64 & 242 & 242 & 242 & 242 & 242 & 242 & 242 & 64 \\ 242 & 160 & 15 & 6 & 0 & 251 & 242 & 97 & 15 \\ 242 & 15 & 0 & 242 & 129 & 242 & 0 & 15 & 242 \\ 242 & 6 & 242 & 97 & 0 & 160 & 15 & 251 & 15 \\ 242 & 0 & 129 & 0 & 128 & 0 & 129 & 0 & 242 \\ 242 & 251 & 242 & 160 & 0 & 97 & 15 & 6 & 15 \\ 242 & 242 & 0 & 15 & 129 & 15 & 0 & 242 & 242 \\ 242 & 97 & 15 & 251 & 0 & 6 & 242 & 160 & 15 \\ 64 & 15 & 242 & 15 & 242 & 15 & 242 & 15 & 64 \end{bmatrix}. \qquad \square$$

Exemplo 2.7 – FFST-1 de comprimento 7 em GF(257)

Considerando o elemento $\zeta = 2 \in \mathrm{GF}(257)$*, com ordem multiplicativa* $\mathrm{ord}(2) = 16$*, a FFST-1 do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117)$ *é o vetor* $\mathbf{X}_{S1} = \mathbf{S}_1\mathbf{x} = (223, 100, 244, 58, 52, 60, 55)$*, em que*

$$\mathbf{S}_1 = \begin{bmatrix} 251 & 242 & 97 & 129 & 97 & 242 & 251 \\ 242 & 129 & 242 & 0 & 15 & 128 & 15 \\ 97 & 242 & 6 & 128 & 6 & 242 & 97 \\ 129 & 0 & 128 & 0 & 129 & 0 & 128 \\ 97 & 15 & 6 & 129 & 6 & 15 & 97 \\ 242 & 128 & 242 & 0 & 15 & 129 & 15 \\ 251 & 15 & 97 & 128 & 97 & 15 & 251 \end{bmatrix}. \qquad \square$$

Exemplo 2.8 – FFCT-4 de comprimento 8 em GF(257)

Considerando o elemento $\zeta = 2 \in \mathrm{GF}(257)$*, com ordem multiplicativa* $\mathrm{ord}(2) = 16$*, a FFCT-4 do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255)$ *é o vetor* $\mathbf{X}_{C4} = \mathbf{C}_4\mathbf{x} = (125, 243, 232, 49, 246, 147, 152, 144)$*, em que*

$$\mathbf{C}_4 = \begin{bmatrix} 228 & 246 & 67 & 130 & 68 & 79 & 103 & 196 \\ 246 & 68 & 196 & 178 & 190 & 29 & 127 & 154 \\ 67 & 196 & 127 & 11 & 154 & 68 & 228 & 79 \\ 130 & 178 & 11 & 196 & 228 & 103 & 190 & 189 \\ 68 & 190 & 154 & 228 & 61 & 11 & 79 & 130 \\ 79 & 29 & 68 & 103 & 11 & 130 & 196 & 190 \\ 103 & 127 & 228 & 190 & 79 & 196 & 189 & 246 \\ 196 & 154 & 79 & 189 & 130 & 190 & 246 & 29 \end{bmatrix}. \qquad \square$$

Exemplo 2.9 – FFST-4 de comprimento 8 em GF(257)

Considerando o elemento $\zeta = 2 \in \mathrm{GF}(257)$*, com ordem multiplicativa* $\mathrm{ord}(2) = 16$*, a FFST-4 do vetor* $\mathbf{x} = (1, 17, 99, 245, 74, 234, 117, 255)$ *é o vetor* $\mathbf{X}_{S4} = \mathbf{S}_4\,\mathbf{x} = (228, 61, 19, 16, 16, 19, 61, 228)$*, em que*

$$\mathbf{S}_4 = \begin{bmatrix} 196 & 103 & 79 & 68 & 130 & 67 & 246 & 228 \\ 103 & 130 & 228 & 67 & 79 & 61 & 189 & 11 \\ 79 & 228 & 68 & 154 & 11 & 127 & 196 & 67 \\ 68 & 67 & 154 & 29 & 61 & 246 & 79 & 127 \\ 130 & 79 & 11 & 61 & 228 & 154 & 190 & 68 \\ 67 & 61 & 127 & 246 & 154 & 189 & 228 & 178 \\ 246 & 189 & 196 & 79 & 190 & 228 & 127 & 103 \\ 228 & 11 & 67 & 127 & 68 & 178 & 103 & 61 \end{bmatrix}. \qquad \square$$

2.3 Autoestrutura das matrizes das transformadas

A determinação da autoestrutura das matrizes das transformadas sobre corpos finitos (relação entre os autovalores e autovetores destas matrizes) tem sido abordada em diferentes trabalhos [7, 58, 61–63] e se mostra de significativa importância, por exemplo, para a concepção de algoritmos rápidos, definição de transformadas fracionais e aplicações em comunicações [41, 42] e criptografia [45].

2.3.1 Autoestrutura das matrizes da FFFT, FFHT e FFTT tipo 1

A matriz de transformação da FFFT, $\mathbf{F}$, tem ciclo 4, isto é, $l = 4$ é o menor inteiro positivo não nulo tal que $\mathbf{F}^l = \mathbf{I}$, sendo $\mathbf{I}$ a matriz identidade. As potências inteiras de $\mathbf{F}$ são tais que

$$\mathbf{F}^1 = \mathbf{F},\ \ \mathbf{F}^2 = \mathbf{P},\ \ \mathbf{F}^3 = \mathbf{PF},\ \ \mathbf{F}^4 = \mathbf{I},$$

em que $\mathbf{P}$ é a matriz de reversão circular (produz uma inversão nos elementos de um vetor), também conhecida como matriz de Schur [63], de dimensão $N \times N$ definida por

$$\mathbf{P} := \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{J} \end{bmatrix}, \tag{2.20}$$

em que $\mathbf{J}$ é a matriz de reversão (produz uma reversão nos elementos de um vetor) de dimensão $(N-1) \times (N-1)$ com elementos 1 em sua antidiagonal [63].

Portanto, a matriz inversa da FFFT é $\mathbf{F}^{-1} = \mathbf{F}^3 = \mathbf{PF}$, em que $[F^3]_{i,k} = \sqrt{N^{-1}}\zeta^{-ki}$. Decorre então o seguinte resultado:

Proposição 2.1

A matriz $\mathbf{F}$ *tem, no máximo, quatro autovalores distintos,* $\left\{\pm 1, \pm\sqrt{-1}\right\}$. $\square$

A prova da Proposição 2.1 pode ser encontrada em [63]. A multiplicidade dos autovalores de $\mathbf{F}$ é encontrada de maneira semelhante à encontrada no estudo da DFT [62]. A multiplicidade dos autovalores da matriz da FFFT depende das dimensões da matriz de transformação, ou seja, depende do comprimento da transformada N. Na Tabela 2.1 é apresentada a multiplicidade dos autovalores da matriz da FFFT de dimensão $N \times N$.

Tabela 2.1: *Multiplicidade dos autovalores da matriz da FFFT de dimensão $N \times N$, para N da forma $4n$, $4n+1$, $4n+3$ e $4n+3$, com n um número inteiro.*

N	Mult. 1	Mult. -1	Mult. $\sqrt{-1}$	Mult. $-\sqrt{-1}$
$4n$	$n+1$	n	$n-1$	n
$4n+1$	$n+1$	n	n	n
$4n+2$	$n+1$	$n+1$	n	n
$4n+3$	$n+1$	$n+1$	n	$n+1$

Fonte: Próprio Autor.

Proposição 2.2

Todo autovetor de $\mathbf{F}$ possui ou simetria par ou simetria ímpar. Os autovetores de simetria par estão associados aos autovalores ± 1, enquanto que os autovetores de simetria ímpar estão associados aos autovalores $\pm\sqrt{-1}$ [63]. □

Os autovalores da matriz da FFHT e suas multiplicidades são iguais aos da transformada discreta da Hartley (DHT, do inglês *discrete Hartley transform*). Da mesma maneira, para encontrá-los, são introduzidas as proposições 2.3 e 2.4, contribuições desta tese. Considere as matrizes $\mathbf{F_R}$ e $\mathbf{F_I}$ definidas, respectivamente, como

$$[F_R]_{i,k} := \sqrt{N^{-1}}\cos_\zeta(ki) \pmod p, \tag{2.21}$$

$$[F_I]_{i,k} := \sqrt{N^{-1}}\sin_\zeta(ki) \pmod p, \tag{2.22}$$

para $i,k = 0,\ldots,N-1$. As matrizes unitárias da FFFT e da FFHT, $\mathbf{H}$, podem ser reescritas, respectivamente, como

$$\mathbf{F} = \mathbf{F_R} - \sqrt{-1}\mathbf{F_I}, \tag{2.23}$$

$$\mathbf{H} = \mathbf{F_R} + \mathbf{F_I}. \tag{2.24}$$

Pelas Equações (2.21) e (2.22), observa-se que $\mathbf{F_R}\mathbf{F_I} = 0$ pois as funções $\cos_\zeta$ e $\sin_\zeta$ são ortogonais.

Proposição 2.3

A matriz $\mathbf{H}$ *tem dois autovalores distintos,* $\{\pm 1\}$.

Demonstração:

Pela Equação (2.24), $\mathbf{H}^2 = \mathbf{F}_\mathbf{r}^2 + \mathbf{F}_\mathbf{i}^2 + 2\mathbf{F}_\mathbf{r}\mathbf{F}_\mathbf{i} = \mathbf{F}_\mathbf{r}^2 + \mathbf{F}_\mathbf{i}^2 = \mathbf{I}$, em virtude de $\cos_\zeta^2(.) + \sin_\zeta^2(.) \equiv 1 \bmod(p)$. Logo, a matriz $\mathbf{H}$ tem ciclo 2 e seus autovalores são as raízes de $\lambda^2 - 1 = 0$. ■

Assim como as transformadas contínuas e discretas de Hartley, a FFHT é uma involução, pois possui o mesmo núcleo para a transformada direta e a inversa.

Lema 2.1

Se $\mathbf{v}$ *é um autovetor de* $\mathbf{F_R}$*, então* $\mathbf{v}$ *não é autovetor de* $\mathbf{F_I}$*, e vice-versa.*

Demonstração:

Se $\mathbf{v}$ é um autovetor de $\mathbf{F_R}$, vale $\mathbf{F_R v} = \lambda \mathbf{v}$ para algum $\lambda \neq 0$. Fazendo $\mathbf{v} = \frac{1}{\lambda}\mathbf{F_R v}$, tem-se

$$\mathbf{F_I v} \;=\; \mathbf{F_I}\left(\frac{1}{\lambda}\mathbf{F_R v}\right) \;=\; \frac{1}{\lambda}\mathbf{F_I F_R v} \;=\; 0.$$

Dessa maneira, como $\mathbf{F_I v} = 0$, $\mathbf{v}$ não é um autovetor de $\mathbf{F_I}$. O resultado inverso pode ser demonstrado da mesma maneira. ■

Proposição 2.4

Se $\mathbf{v}$ *é um autovetor de* $\mathbf{F}$ *associado aos autovalores* $\lambda = \{1, -\sqrt{-1}\}$*, então* $\mathbf{v}$ *é um autovetor de* $\mathbf{H}$ *associado ao autovalor* $\lambda = 1$*. Se* $\mathbf{v}$ *é um autovetor de* $\mathbf{F}$ *associado aos autovalores* $\lambda = \{-1, \sqrt{-1}\}$*, então* $\mathbf{v}$ *é um autovetor de* $\mathbf{H}$ *associado ao autovalor* $\lambda = -1$.

Demonstração:

Se $\mathbf{v}$ é um autovetor de $\mathbf{F}$ associado ao autovalor $\lambda = 1$, então $\mathbf{v}$ é um autovetor de $\mathbf{F_r}$ associado ao autovalor $\lambda = 1$, e

$$\mathbf{Hv} = (\mathbf{F_R} + \mathbf{F_I})\,\mathbf{v} = \mathbf{F_R v} + 0 \;=\; 1\mathbf{v}.$$

Se $\mathbf{v}$ é um autovetor de $\mathbf{F}$ associado ao autovalor $\lambda = -1$, então $\mathbf{v}$ é um autovetor de $\mathbf{F_r}$ associado ao autovalor $\lambda = -1$, e

$$\mathbf{Hv} = (\mathbf{F_R} + \mathbf{F_I})\,\mathbf{v} = \mathbf{F_R v} + 0 \;=\; -1\mathbf{v}.$$

Se $\mathbf{v}$ é um autovetor de $\mathbf{F}$ associado ao autovalor $\lambda = \sqrt{-1}$, então $\mathbf{v}$ é um autovetor de $\mathbf{F_i}$ associado ao autovalor $\lambda = -1$, e

$$\mathbf{Hv} = (\mathbf{F_R} + \mathbf{F_I})\,\mathbf{v} = 0 + \mathbf{F_I v} \;=\; -1\mathbf{v}.$$

Se $\mathbf{v}$ é um autovetor de $\mathbf{F}$ associado ao autovalor $\lambda = -\sqrt{-1}$, então $\mathbf{v}$ é um autovetor de $\mathbf{F_i}$ associado ao autovalor $\lambda = 1$, e

$$\mathbf{Hv} = (\mathbf{F_R} + \mathbf{F_I})\,\mathbf{v} = 0 + \mathbf{F_I v} \quad = \quad 1\mathbf{v}.$$

A partir da multiplicidade dos autovalores de $\mathbf{F}$ e da Proposição 2.4, obtém-se a multiplicidade dos autovalores da matriz da FFHT que é apresentada na Tabela 2.2.

Tabela 2.2: *Multiplicidade dos autovalores da matriz da FFHT de dimensão $N \times N$.*

N	Mult. 1	Mult. -1
$4n$	$2n+1$	$2n-1$
$4n+1$	$2n+1$	$2n$
$4n+2$	$2n+1$	$2n+1$
$4n+3$	$2n+2$	$2n+1$

Fonte: Próprio Autor.

A relação entre as transformadas de Hartley e de Fourier sobre corpos finitos é a mesma relação das transformadas no corpo dos números reais, de forma que [64]

$$\mathbf{H} \quad = \quad \frac{\mathbf{F}+\mathbf{PF}}{2} - \sqrt{-1}\frac{\mathbf{F}-\mathbf{PF}}{2} = \frac{\mathbf{F}+\mathbf{F}^3}{2} - \sqrt{-1}\frac{\mathbf{F}-\mathbf{F}^3}{2}, \tag{2.25}$$

$$\mathbf{F} \quad = \quad \frac{\mathbf{H}+\mathbf{PH}}{2} + \sqrt{-1}\frac{H-\mathbf{PH}}{2}. \tag{2.26}$$

Em relação às transformadas trigonométricas, apenas as matrizes das transformadas dos tipos 1 e 4 têm autoestruturas semelhantes à matriz da transformada de Fourier. As matrizes de transformação dessas transformadas trigonométricas são unitárias e simétricas, portanto, as transformadas têm ciclo 2 [61] e apresentam como autovalores apenas os elementos $\lambda = \pm 1$. Para as matrizes das transformadas trigonométricas tipos 2 e 3, conjectura-se que os autovalores sejam todos distintos [61].

Proposição 2.5

As matrizes $\mathbf{C}_1, \mathbf{C}_4, \mathbf{S}_1$ e $\mathbf{S}_4$ tem, cada uma, no máximo, dois autovalores distintos, $\{\pm 1\}$. A multiplicidade dos autovalores das FFTT tipos 1 e 4 é apresentada na Tabela 2.3[61].

A prova da Proposição 2.5 pode ser encontrada em [60, pp. 70] e em [61]. As autoestruturas das matrizes de transformação das FFTT do tipo 1 estão relacionadas com a autoestrutura da matriz de transformação da FFFT, e dela podem ser derivadas.

Tabela 2.3: *Multiplicidade dos autovalores das matrizes FFTT tipos 1 e 4 de dimensão $N' \times N'$, em que N' pode ser igual a N, $(N-1)$ e $(N+1)$ de acordo com a dimensão de cada matriz.*

N'	Mult. 1	Mult.-1
Ímpar	$\frac{N'+1}{2}$	$\frac{N'-1}{2}$
Par	$\frac{N'}{2}$	$\frac{N'}{2}$

Fonte: Próprio Autor.

Proposição 2.6

i) Se $\mathbf{v} = [v_0, v_1, \ldots, v_{N-1}, v_{N-1}, \ldots, v_1]$ *é um autovetor de simetria par da matriz* $\mathbf{F}$*, com dimensão* $2N \times 2N$*, então*

$$\tilde{\mathbf{v}} = [v_0, \sqrt{2}v_1, \ldots, \sqrt{2}v_{N-2}, v_{N-1}]$$

é um autovetor da matriz $\mathbf{C}_1$ *de dimensão* $(N+1) \times (N+1)$*.*

ii) Se $\mathbf{v} = [0, v_1, \ldots, v_{N-1}, 0, -v_{N-1}, \ldots, -v_1]$ *é um autovetor de simetria ímpar da matriz* $\mathbf{F}$*, com dimensão* $2N \times 2N$*, então*

$$\hat{\mathbf{v}} = \sqrt{2}[v_1, v_2 \ldots, v_{N-1}]$$

é um autovetor da matriz $\mathbf{S}_1$ *de dimensão* $(N-1) \times (N-1)$*.* □

A prova da Proposição 2.6 pode ser encontrada em [60, pp. 70] e em [61].

2.3.2 Autoestrutura das matrizes da GFFFT, GFFHT e FFFT tipo 4

No tocante às transformadas generalizadas, as matrizes unitárias da GFFFT e da GFFHT podem ser reescritas, respectivamente, de acordo com

$$\mathbf{F_G} = \mathbf{F_{Gr}} - \sqrt{-1}\mathbf{F_{Gi}}, \tag{2.27}$$

$$\mathbf{H_G} = \mathbf{F_{Gr}} + \mathbf{F_{Gi}}, \tag{2.28}$$

em que, as componentes das matrizes $\mathbf{F_{Gr}}$ e $\mathbf{F_{Gi}}$ são dadas por

$$[F_{Gr}]_{i,k} := \sqrt{N^{-1}} \cos_\zeta \left((k+1/2)(i+1/2)\right), \tag{2.29}$$

$$[F_{Gi}]_{i,k} := \sqrt{N^{-1}} \sin_\zeta \left((k+1/2)(i+1/2)\right), \tag{2.30}$$

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

As potências inteiras de $\mathbf{F_G}$ são tais que

$$\mathbf{F_G^1} = \mathbf{F_G}, \ \mathbf{F_G^2} = -\mathbf{J}, \ \mathbf{F_G^3} = -\mathbf{J}\mathbf{F_G}, \ \mathbf{F_G^4} = \mathbf{I},$$

em que $\mathbf{J}$ é a matriz de reversão de dimensão $(N) \times (N)$ com elementos 1 em sua antidiagonal [63]. Portanto, a matriz inversa da GFFFT é $\mathbf{F}_{\mathbf{G}}^{-1} = \mathbf{F}_{\mathbf{G}}^{3} = -\mathbf{J}\mathbf{F}_{\mathbf{G}}$. Decorre então o seguinte resultado:

Proposição 2.7

A matriz $\mathbf{F}_{\mathbf{G}}$ possui, no máximo, quatro autovalores distintos ($\pm 1, \pm\sqrt{-1}$), cujas multiplicidades são apresentadas na Tabela 2.4.

Tabela 2.4: *Multiplicidade dos autovalores da matriz da GFFFT de dimensão $N \times N$.*

N	Mult. 1	Mult. -1	Mult. $\sqrt{-1}$	Mult. $-\sqrt{-1}$
$4n$	n	n	n	n
$4n+1$	n	n	n	$n+1$
$4n+2$	$n+1$	n	n	$n+1$
$4n+3$	$n+1$	n	$n+1$	$n+1$

Fonte: Próprio Autor.

A prova da Proposição 2.7 pode ser encontrada em [60, pp. 74].

Proposição 2.8

Os autovalores de $\mathbf{H}_G$ são ± 1, cujas multiplicidades são apresentadas na Tabela 2.5

Tabela 2.5: *Multiplicidade dos autovalores da matriz da GFFHT de dimensão $N \times N$.*

N	Mult. 1	Mult. -1
$4n$	$2n$	$2n$
$4n+1$	$2n+1$	$2n$
$4n+2$	$2n+2$	$2n$
$4n+3$	$2n+2$	$2n+1$

Fonte: Próprio Autor.

A prova é similar à desenvolvida para a FFHT nas Proposições 2.3 e 2.4 e está em consonância com as transformadas discretas [58]. Observando as relações expressas nas Equações (2.27) e (2.28), conclui-se que os autovetores de $\mathbf{F}_{\mathbf{G}}$ associados aos autovalores $\lambda = 1$ e $\lambda = -\sqrt{-1}$ são autovetores de $\mathbf{H}_{\mathbf{G}}$ associados ao autovalor $\lambda = 1$, e que os autovetores de $\mathbf{F}_{\mathbf{G}}$ associados aos autovalores $\lambda = -1$ e $\lambda = \sqrt{-1}$ são autovetores de $\mathbf{H}_{\mathbf{G}}$ associados ao autovalor $\lambda = -1$.

As autoestruturas das matrizes de transformação das FFTT do tipo 4 estão relacionadas com a autoestrutura da matriz de transformação da GFFFT, e dela podem ser derivadas.

Proposição 2.9

i) Se $\mathbf{v} = [v_0, v_1, \ldots, v_{N-1}, v_{N-1}, \ldots, v_0]$ *é um autovetor de simetria par de* $\mathbf{F_G}$ *com dimensão* $2N \times 2N$*, então*

$$\tilde{\mathbf{v}} = [v_1, v_2 \ldots, v_{N-1}]$$

é um autovetor de $\mathbf{S}_4$ *de dimensão* $N \times N$*.*

ii) Se $\mathbf{v} = [v_0, v_1, \ldots, v_{N-1}, -v_{N-1}, \ldots, -v_0]$ *é um autovetor de simetria ímpar de* $\mathbf{F_G}$ *com dimensão* $2N \times 2N$*, então*

$$\hat{\mathbf{v}} = [v_0, \sqrt{2}v_1, \ldots, \sqrt{2}v_{N-2}, v_{N-1}]$$

é um autovetor de $\mathbf{C}_4$ *de dimensão* $N \times N$*.* □

A prova da Proposição 2.9 pode ser encontrada em [60, pp. 76] e em [61].

2.4 Transformadas Numéricas

Transformadas em corpos finitos podem ser vistas como um mapeamento de vetores em $\mathrm{GF}(p)$ para vetores em um corpo de extensão $\mathrm{GF}(p^m)$, m inteiro. Quando $m = 1$, o mapeamento é feito de vetores em $\mathrm{GF}(p)$ para $\mathrm{GF}(p)$, e essas transformadas são chamadas de transformadas numéricas. Nessas condições, emprega-se a aritmética módulo p (as operações de adição e multiplicação são fechadas em $\mathrm{GF}(p)$), a qual tem baixo custo computacional para certos valores de p.

As transformadas de Fourier e trigonométricas sobre corpos finitos são "naturalmente" numéricas se o núcleo de cada transformada, o elemento ζ, pertence a $\mathrm{GF}(p)$, p um número primo. Já o espectro da transformada de Hartley sobre corpos finitos tem elementos em $\mathrm{GI}(p)$, mesmo que $\zeta \in \mathrm{GF}(p)$, como se observa no Exemplo 2.2. Contudo, em alguns casos particulares, a transformada de Hartley pode ser uma transformada numérica. Isto ocorre quando:

- O elemento -1 é resíduo quadrático de $\mathrm{GF}(p)$, isto é, $j = \sqrt{-1} \in \mathrm{GF}(p)$, ocorrendo para $p \equiv 1 \pmod 4$;
- O elemento ζ é um elemento unimodular de $\mathrm{GI}(p)$ [55], como se observa no Exemplo 2.3.

As transformadas numéricas reduzem a complexidade aritmética ao ponto de, em alguns casos, serem livres de multiplicações, havendo somente operações de adição e deslocamentos cíclicos. Contudo, existem algumas restrições quanto ao comprimento da transformada e algumas considerações práticas devem ser observadas para utilizá-las:

- O número primo p deve ser suficientemente grande para evitar *overflow*;
- Se o comprimento da transformada for composto, pode-se utilizar alguns tipos de algoritmos rápidos;
- A multiplicação das potências do núcleo deve ser de baixa complexidade, resultando, se possível, apenas em deslocamentos cíclicos.

Escolhas óbvias para o núcleo das transformadas são as potências de 2, visto que os sistemas digitais são, em geral, baseados em operações binárias. Alguns valores específicos de p originam classes específicas de transformadas numéricas. Assim, quando p é um número primo de Fermat, tem-se as transformadas numéricas de Fermat [65]; quando p é um número primo de Mersenne, tem-se as transformadas numéricas de Mersenne [66].

2.4.1 Transformadas Numéricas de Fermat

Os inteiros da forma $F_s := 2^{2^s} + 1$, para s inteiro, são conhecidos como números de Fermat. Os primeiros números de Fermat, para $s = 0, \ldots, 4$, são os únicos números primos conhecidos que têm essa forma [54, pp. 237].

Quando se utiliza os números primos de Fermat, a transformada numérica de Fourier passa a ser conhecida como transformada numérica de Fourier-Fermat (FFNT, do inglês *Fourier-Fermat number transform*). Para esse caso, $p \equiv 1 \pmod 4$, os elementos não nulos de $\mathrm{GF}(p)$ formam um grupo multiplicativo cuja ordem é um divisor de 2^{2^s}. Assim, os possíveis comprimentos da FFNT são potências de 2, a qual pode ser implementada usando a FFT de Cooley-Tukey base dois.

Para números primos de Fermat, a transformada numérica de Hartley passa a denominada transformada numérica de Hartley-Fermat (HFNT, do inglês *Hartley-Fermat number transform*). Como $p \equiv 1 \pmod 4$, -1 é resíduo quadrático de $\mathrm{GF}(p)$, isto é, $\sqrt{-1} \in \mathrm{GF}(p)$. Assim, os elementos da forma $a + \sqrt{-1}b$ também pertencem a $\mathrm{GF}(p)$. A FFHT é naturalmente uma transformada numérica.

Um importante critério na definição das transformadas numéricas de Fermat é a escolha do núcleo.

- Usando o elemento 2 como núcleo, é possível obter transformadas com comprimento até $2s$. Essa escolha é interessante, pois as multiplicações podem ser realizadas através de deslocamentos cíclicos.
- Usando o elemento $\sqrt{2}$ como núcleo, é possível obter transformadas com comprimento até $4s$. As multiplicações podem ser realizadas com deslocamentos cíclicos e com subtrações [64].

2.4.2 Transformadas Numéricas de Mersenne

Os inteiros da forma $M_s := 2^s - 1$, para s inteiro, são conhecidos como números de Mersenne. Se s for um número primo, então M_s pode ser um número primo [54, pp. 225]. Por exemplo, para $s = 2, 3, 5$, M_s é primo, mas para $s = 11, 23, 29$, M_s não é primo. Nesse cenário, tem-se a transformada numérica de Fourier-Mersenne (FMNT, do inglês *Fourier-Mersenne number transform*) e a transformada numérica de Hartley-Mersenne (HMNT, do inglês *Hartley-Mersenne number transform*).

Para a FMNT os possíveis comprimentos das transformadas são os divisores de $2^s - 2$, que não são potências de 2. Os comprimentos das transformadas dependem do número primo p. Deste modo, não é possível usar a FFT de Cooley-Tukey base dois. Contudo, essa transformada é particularmente interessante, pois todos os seus elementos possuem uma representação binária de s *bits*. Por exemplo, em $\mathrm{GF}(2^{13})$ todos os elementos podem ser representados por treze *bits* e os comprimentos possíveis são fatores de $2^{13} - 2 = 2 \times 5 \times 7 \times 9 \times 13$.

Para números primos de Mersenne tem-se que $p \equiv 3 \pmod 4$, então $\sqrt{-1} \notin \mathrm{GF}(p)$ e o espectro da FFHT é "complexo". Porém, se ζ for um elemento unimodular de $\mathrm{GI}(p)$ a imagem da função $\mathrm{cas}_\zeta = \cos_\zeta + \sin_\zeta$ está contida em $\mathrm{GF}(p)$, e assim a FFHT é a HMNT [55, 64]. Um ponto positivo da HMNT em relação a FMNT é que os comprimentos permitidos para a HMNT são divisores de $p + 1 = 2^s$, isto é, potências de 2. Torna-se possível, então, empregar o algoritmo de Cooley-Tukey base dois para computar a HMNT o que não ocorre para a FMNT [55].

As transformadas numéricas de Hartley-Mersenne permitem uma implementação com complexidade multiplicativa nula, em certos casos, o que é atrativo do ponto de vista prático [64]. Nesses casos, ao se escolher o elemento 2 como núcleo da transformada, e se valer de deslocamentos cíclicos, o comprimento da FMNT é $N = s$, já ao se escolher o elemento -2 o comprimento pode ser $N = 2s$. Para a HMNT, o núcleo da transformação inclui apenas os valores 0, 1 e -1, ou potências não triviais de 2. Nesse último caso, as multiplicações correspondem a deslocamentos cíclicos.

Apesar de não admitir a FFT de Cooley-Tukey base dois, foram desenvolvidos outros algoritmos rápidos para a FMNT. Nibouche *et al.* [67] introduziram a nova transformada numérica de Mersenne e mostrou ser possível usar o algoritmo de Rader-Brenner para reduzir a complexidade aritmética [68, 69]. Em outro trabalho, Boussakta *et al.* [70] introduziram as transformadas numéricas de Mersenne generalizadas e mostraram que é possível utilizar a FFT de Cooley-Tukey base dois e base quatro.

CAPÍTULO 3

TRANSFORMADAS FRACIONAIS EM CORPOS FINITOS

O estudo das transformadas fracionais teve início com a generalização da transformada de Fourier contínua, onde se pretendia calcular potências fracionais do operador da transformada. De forma semelhante, buscou-se definir a transformada fracional de Fourier discreta e em seguida de outras transformadas fracionais a partir das transformadas discretas. Na Tabela A.1 do Apêndice A é apresentada a cronologia do desenvolvimento das transformadas fracionais discretas no corpo dos números reais.

Após a definição da transformada de Fourier sobre corpos finitos feita por Pollard [49], foram concebidas outras transformadas em corpos finitos como as transformadas numéricas [38, 65], a transformada de Hartley [53], as transformadas trigonométricas [71, 72] e a transformada Z [73]. Em sintonia com o desenvolvimento das transformadas no corpo dos números reais, devem ser definidas as transformadas fracionais em corpos finitos. Na Tabela A.2 do Apêndice A é apresentada a cronologia do desenvolvimento das transformadas fracionais em corpos finitos.

As transformadas definidas no **Capítulo 2** são chamadas de transformadas ordinárias ou usuais no decorrer do texto. O termo **ordinária** faz alusão à potência da matriz de transformação que não é fracional, em contraste com as potências fracionais da matriz de transformação das transformadas fracionais. A partir deste capítulo, são apresentadas as transformadas fracionais de Fourier, de Hartley, do cosseno e do seno em corpos finitos.

Os procedimentos para definição das transformadas fracionais no corpo dos números reais auxiliam na definição das transformadas em corpos finitos. Para tanto, esses procedimentos são brevemente e revisados.

Em 1982, Dickinson *et al.* [7] introduziram um procedimento para se computar potências fracionais da matriz da DFT por meio de combinações lineares de potências inteiras da matriz da DFT. A este trabalho, porém, não foi dado destaque porque não se tinha uma boa aproximação com a transformada fracional de Fourier contínua.

Em 1996, Santhanam *et al.* [8, 74] propuseram uma definição para a transformada fracional de Fourier discreta (DFrFT) baseada na amostragem da transformada fracional de Fourier contínua. A essa proposta também não foi dado destaque, visto que não apresentava a propriedade de aditividade de arcos (expoentes).

Outras propostas se basearam na expansão espectral da matriz de transformação da DFT [14, 17]. A transformada discreta de um vetor pode ser expressa por meio de uma equação matricial como o produto de uma matriz de transformação por um vetor. Nesse sentido, para se obter a transformada fracional de um vetor, basta multiplicá-lo pela versão fracional da matriz de transformação, em que potências fracionais são admitidas.

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

$$\mathbf{F} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^{-1}, \tag{3.1}$$

em que $\mathbf{V}$ é uma matriz cujas colunas são autovetores de $\mathbf{F}$ e $\mathbf{\Lambda}$ é uma matriz diagonal de autovalores de $\mathbf{F}$, cujo elemento na k-ésima coluna e k-ésima linha é dado por $(-\sqrt{-1})^k$. O autovetor da k-ésima coluna de $\mathbf{V}$ está associado ao autovalor $(-\sqrt{-1})^k$.

Para se obter a matriz da DFrFT, $\mathbf{F}^a$, é necessário apenas elevar cada autovalor de $\mathbf{\Lambda}$ ao expoente a, real, sem realizar manipulações com a matriz de autovetores $\mathbf{V}$. A DFrFT é então dada por

$$\mathbf{F}^a = \mathbf{V}\mathbf{\Lambda}^a\mathbf{V}^{-1}. \tag{3.2}$$

Um ponto negativo dessa abordagem está na necessidade de construir os autovetores de $\mathbf{F}$ de dimensão $N \times N$ sempre que N muda. Por exemplo, a partir dos autovetores da matriz $\mathbf{F}$ de dimensão 8×8, não há, até o momento, um procedimento para se obter os autovetores da $\mathbf{F}$ de dimensão 9×9. As abordagens que utilizam a Equação (3.2) para definir a DFrFT diferenciam-se no procedimento de construção dos autovetores:

- Um procedimento para se obter autovetores da DFT é baseado em sequências de Legendre generalizadas. Proposto por Pei *et al.* [20], é possível encontrar sequências ortogonais por meio de

expressões fechadas e derivar, por meio de combinações lineares dessas sequências, os autovetores da DFT.

- Outra maneira de obter conjuntos de autovetores ortogonais é por meio de uma matriz que comute com a matriz da DFT, e sobre a qual haja um procedimento sistemático para obter seus autovetores.
- Mais recentemente, Kuznetsov [75] introduziu expressões fechadas para se construir diretamente autovetores da DFT.

Baseados nos procedimentos definidos sobre o corpo dos números reais foram introduzidas a transformada fracional de Fourier em corpos finitos (GFrFT, do inglês *Galois field fractional Fourier transform*), a transformada fracional de Hartley em corpos finitos (GFrHT, do inglês *Galois field fractional Hartley transform*), a transformada fracional do cosseno em corpos finitos (GFrCT, do inglês *Galois field fractional cosine transform*), e a transformada fracional do seno em corpos finitos (GFrST, do inglês *Galois field fractional sine transform*).

3.1 GFrFT obtida a partir das Sequências de Legendre

As sequências de Legendre são sequências periódicas baseadas em resíduos quadráticos e aritmética modular. Para um número primo p, a sequência $\eta(n) = (n/p), n = 0, 1, ..., p-1$, é chamada de sequência de Legendre, em que (n/p) é o símbolo de Legendre [54, p. 175]. Por exemplo, considerando $p = 7$, tem-se $\eta(n) = (0, 1, 1, -1, 1, -1, -1)$.

De maneira similar, as sequências generalizadas de Legendre (GLS, do inglês *generalized Legendre sequence*) podem ser construídas para potências de números primos p^m, de forma que a sequência tenha comprimento p^m. Dentre as propriedades desse tipo de sequência destacam-se duas: *i*) as sequências ou tem simetria par ou simetria ímpar; *ii*) as sequências formam um conjunto ortogonal. Essas são algumas das propriedades desejadas para os autovetores da DFT.

Seja $\phi(n)$ a função de *Euler* que denota o número de inteiros positivos que são relativamente primos a n no intervalo $1, 2, \ldots, n-1$ [54, p. 131]. A partir das GLS de comprimento $N = p^m$ não é possível obter bases para construir o espaço vetorial $\mathbb{C}^N$, pois só existem $\phi(p^m)$ sequências. Isto é um problema, pois, para construir $\mathbb{C}^N$, são necessários N autovetores de comprimento N; porém com as GLS, constrói-se apenas $\phi(p^m)$ vetores de comprimento N [20].

Com a técnica *Zero-Forcing* (ZF) [31] é possível estender uma GLS de comprimento $N_1 = p^{m-1}$ para um comprimento $N = p^m$. Isso é feito adicionando-se zeros em posições específicas da sequência, de forma que as GLS originais e as construídas com a técnica ZF sejam ortogonais.

Dessa maneira, é possível utilizar as GLS de comprimento $p^{m-1}, p^{m-2}, ..., p^0$ estendendo-as com a técnica ZF para que tenham comprimento p^m e, a partir delas, construir o espaço vetorial $\mathbb{C}^N$. As GLS e as sequências construídas com a técnica ZF definem as sequências completas generalizadas de Legendre (CGLS - *Complete GLS*).

Apenas algumas CGLS são autovetores da DFT, mas elas formam um conjunto ortogonal de vetores. Considerando-se uma combinação linear dessas sequências, obtém-se um conjunto completo e ortogonal de autovetores da DFT. Como cada autovetor é combinação linear de sequências de simetria par ou ímpar, os autovetores também têm esses tipos de simetria. Com esse resultado, é possível associar os autovetores aos autovalores da matriz da DFT.

De maneira análoga, Pei *et al.* [22] definiram as CGLS sobre corpos finitos (CGLSF, do inglês *complete generalized Legendre sequence over finite fields*) para que com essas se obtivessem autovetores da matriz da FFFT. Foram feitas algumas adaptações para utilizar o procedimento em corpos finitos: na fórmula para se gerar as CGLS, é utilizada a N-ésima raiz da unidade $\left(e^{\frac{j2\pi a b_n}{N}}\right)$ em que a e b_n são parâmetros do procedimento. Na CGLSF, ao invés de usar a K-ésima raiz da unidade do corpo dos números complexos, emprega-se um elemento γ de ordem multiplicativa $\mathrm{ord}(\gamma) = N$ em $\mathrm{GF}(p)$.

Com essa e outras adaptações, foi proposta uma expressão fechada para se gerar as CGLSF. A partir das CGLSF, adaptou-se o procedimento de construção de um conjunto completo e ortogonal de autovetores da matriz da DFT para a matriz da FFFT. Com o conjunto ortogonal de autovetores, a GFrFT foi definida utilizando-se a expansão espectral.

3.2 GFrFT baseada na expansão espectral - matriz S

O ponto comum e fundamental dos trabalhos que definem a DFrFT por meio da expansão espectral consiste na construção de autovetores da matriz da DFT por meio de matrizes que comutam com a DFT. Neste sentido, o trabalho de Grünbaum [76] se destaca pela introdução de uma classe de matrizes que comutam com a matriz da DFT.

No trabalho sobre os autovetores da matriz da DFT, Dickinson *et al.* [7] introduziram a matriz $\mathbf{S}$ que comuta com a matriz da DFT, para então obter um conjunto de autovetores de $\mathbf{S}$ que por sua vez são autovetores da matriz da DFT. Analisando a Equação (3.2), os autovetores são colunas da matriz $\mathbf{V}$, de forma que permutações nessas colunas geram matrizes diferentes e válidas.

Além disso, segundo a Equação (3.2) a a-ésima potência dos autovalores $\left(-\sqrt{-1}\right)^a$ pode ocupar qualquer posição da diagonal de $\mathbf{\Lambda}^a$, desde que fosse associada a um autovetor correspondente. Isto

é, não foram apresentados critérios de ordenamento de autovetores nem de associação e ordenamento de autovalores, o que resulta em matrizes de transformação diferentes e válidas.

Estas duas ausências foram tratadas pode Pei *et al.* [14] como ambiguidades do procedimento. Pei buscou um procedimento sistemático em que se empregasse a Equação (3.2) para construir uma única matriz de transformação da DFrFT. Ele mostrou que os autovetores de $\mathbf{S}$ são versões discretas das funções Hermite-Gaussianas e propôs um critério para ordenamento de autovalores e um critério para as associações com autovetores. Por fim, Candan *et al.* [17] reescreveu a matriz $\mathbf{S}$ e propôs um critério para ordenamento de autovetores. Com isso, a partir deste último procedimento sistemático, obtém-se uma única matriz da DFrFT que atende à Propriedade 1.2.

O procedimento baseado na expansão espectral em que os autovetores da matriz da FFFT são obtidos por meio de matrizes comutantes foi introduzido em corpos finitos por Lima *et al.* [46]. Assim como no caso da DFrFT, o objetivo é construir um conjunto ortogonal de autovetores para a matriz $\mathbf{F}$ e, usando a Equação (3.2), encontrar $\mathbf{F}^a$, a matriz de transformação da transformada fracional de Fourier em corpos finitos (GFrFT).

Como se observa na Tabela 2.1, a matriz $\mathbf{F}$ tem apenas quatro autovalores distintos, logo esses autovalores são degenerados e o conjunto de autovetores não é único [17]. Pela Proposição 2.2, verifica-se que os autovetores de $\mathbf{F}$ tem simetria par ou ímpar.

Pelo procedimento, os autovetores de $\mathbf{F}$ são obtidos por meio de uma matriz que comuta com $\mathbf{F}$, pois duas matrizes diagonalizáveis e que comutam apresentam um conjunto de autovetores em comum [17]. O procedimento se propõe a orientar a escolha de um **único** conjunto ortogonal de autovetores, de forma a evitar as ambiguidades citadas por Pei *et al.* [14].

Nota 3. 1 Com o procedimento, uma consideração a ser feita é que, sendo $a = a_1/a_2$ racional, as possíveis potências fracionais dos autovalores são dadas por $(-\sqrt{-1})^{\frac{a_1}{a_2}}$. Ora, esses valores dependem da existência da $2a_2$-ésima raiz de -1 em $\mathrm{GI}(p)$ para que o vetor transformado esteja definido em $\mathrm{GI}(p)$ [46] .

3.2.1 A matriz $\mathbf{S}$

Considere a matriz $\mathbf{S}$ de dimensão $N \times N$, cujos elementos não nulos são dados pela regra

$$\begin{cases} [S]_{0,N-1} = [S]_{N-1,0} = 1, & \\ [S]_{i,i+1} = [S]_{i+1,i} = 1, & 0 \leq i \leq N-2, \\ [S]_{i,i} = \sigma_i \pmod p, & 0 \leq i \leq N-1, \end{cases}$$

em que $\sigma_i = 2\,(\cos_\zeta(i) - 2)$, $i = 0, 1, \ldots, N-1$, e ζ é um elemento não nulo de ordem multiplicativa $\mathrm{ord}(\zeta) = N$ em $\mathrm{GI}(p)$. Assim, a matriz $\mathbf{S}$ tem a forma

$$\mathbf{S} = \begin{bmatrix} \sigma_0 & 1 & 0 & \ldots & 1 \\ 1 & \sigma_1 & 1 & \ldots & 0 \\ 0 & 1 & \sigma_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \ldots & \sigma_{N-1} \end{bmatrix} \pmod p. \tag{3.3}$$

Proposição 3.1

As matrizes $\mathbf{F}$ *e* $\mathbf{S}$ *comutam.*

Demonstração: Vide Apêndice B, seção B.1.1. ■

3.2.2 Autovetores da matriz $\mathbf{S}$

No intuito de remover a ambiguidade concernente à associação entre autovetores e autovalores, é necessário que exista um conjunto de autovetores de $\mathbf{S}$ e que este seja único. Uma vez que $\mathbf{S}$ e $\mathbf{F}$ comutam, a **existência** do conjunto de autovetores de $\mathbf{S}$ é garantida.

Para verificar a unicidade do conjunto, considere a matriz $\mathbf{L} = [L]_{i,k}$, de dimensão $N \times N$, que decompõe um vetor em partes par e ímpar. Considere que $\lfloor . \rfloor$ representa a parte inteira do argumento. A matriz $\mathbf{L}$ é dada pela seguinte regra:

- Para N ímpar, os elementos não nulos de $\mathbf{L}$ são dados por

$$[L]_{i,k} := \begin{cases} 1, & \text{se } \; i = k = 0, \\ \sqrt{2^{-1}} \pmod p, & \text{se } i = k = 2, \ldots, \lfloor N/2 + 1 \rfloor, \\ -\sqrt{2^{-1}} \pmod p, & \text{se } i = k = \lfloor N/2 + 2 \rfloor, \ldots, N, \\ \sqrt{2^{-1}} \pmod p, & \text{se } i = N - n + 2, \; k = 2, \ldots, N. \end{cases} \tag{3.4}$$

A matriz $\mathbf{L}$ tem a forma

$$\mathbf{L} \;=\; \sqrt{2^{-1}} \begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & \mathbf{I}_{\frac{N-1}{2}} & \mathbf{J}_{\frac{N-1}{2}} \\ 0 & \mathbf{J}_{\frac{N-1}{2}} & -\mathbf{I}_{\frac{N-1}{2}} \end{bmatrix}$$

$$= \sqrt{2^{-1}} \begin{bmatrix} \sqrt{2} & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & -1 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 & -1 \end{bmatrix}.$$

- Para N par, os elementos não nulos de $\mathbf{L}$ são dados por

$$[L]_{i,k} := \begin{cases} 1, & \text{se } i = k = \{0, N/2+1\}, \\ \sqrt{2^{-1}} \pmod p, & \text{se } i = k = 1, \dots, N/2, \\ -\sqrt{2^{-1}} \pmod p, & \text{se } i = k = N/2+2, \dots, N, \\ \sqrt{2^{-1}} \pmod p, & \text{se } i = N-k+2,\ k = 2, \dots, N,\ k \neq N/2+1. \end{cases} \tag{3.5}$$

A matriz $\mathbf{L}$ tem a forma

$$\mathbf{L} = \sqrt{2^{-1}} \begin{bmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & \mathbf{I}_{\frac{N}{2}-1} & 0 & \mathbf{J}_{\frac{N}{2}-1} \\ 0 & 0 & \sqrt{2} & 0 \\ 0 & \mathbf{J}_{\frac{N}{2}-1} & 0 & -\mathbf{I}_{\frac{N}{2}-1} \end{bmatrix}$$

$$= \sqrt{2^{-1}} \begin{bmatrix} \sqrt{2} & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & \sqrt{2} & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & -1 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & -1 \end{bmatrix}.$$

Por meio do Lema B.2 (Vide Apêndice B), mostra-se que a transformação de similaridade

$$\mathbf{LSL}^{-1} = \begin{bmatrix} \mathbf{Ev} & \mathbf{0} \\ \mathbf{0} & \mathbf{Od} \end{bmatrix} \tag{3.6}$$

produz as matrizes tridiagonais simétricas $\mathbf{Ev}$ e $\mathbf{Od}$, com dimensões $\lfloor N/2+1 \rfloor$ e $\lfloor N/2-1 \rfloor$, respectivamente.

Os autovalores das matrizes tridiagonais $\mathbf{Ev}$ e $\mathbf{Od}$ são todos distintos, logo existe um único conjunto de autovetores para $\mathbf{Ev}$ e um único conjunto de autovetores para $\mathbf{Od}$ [46] [77, p. 299]. Analisando o Lema B.3, os autovetores de $\mathbf{S}$ podem ser obtidos por meio de extensões simétricas dos autovetores de $\mathbf{Ev}$ e de $\mathbf{Od}$, portanto, existe um **único** conjunto de autovetores para $\mathbf{S}$.

Dessa maneira os autovetores de $\mathbf{F}$ com simetria par podem ser obtidos por meio dos autovetores de $\mathbf{Ev}$, $\mathbf{e}_k$, fazendo

$$\mathbf{u}_{2k} = \mathbf{L}[\mathbf{e}_k^t | 0 \ldots 0]^t, \;\; k = 0, \ldots, \left\lfloor \frac{N}{2} \right\rfloor, \tag{3.7}$$

e os autovetores de $\mathbf{F}$ com simetria ímpar podem ser obtidos por meio dos autovetores de $\mathbf{Od}$, $\mathbf{o}_k$, fazendo

$$\mathbf{u}_{2k+1} = \mathbf{L}[0 \ldots 0 | \mathbf{o}_k^t]^t, \;\; k = 0, \ldots, \left\lfloor \frac{N-3}{2} \right\rfloor, \tag{3.8}$$

em que $\{.\}^t$ representa a transposta do argumento.

Nota 3. 2 Analisando as Equações (3.4) e (3.5), a condição $\sqrt{2} \in \mathrm{GF}(p)$ deve ser satisfeita para que a transformação de similaridade resulte numa matriz com elementos em $\mathrm{GF}(p)$.

3.2.3 Ordenação dos autovetores da matriz $\mathbf{S}$

A segunda ambiguidade apontada por Pei era o ordenamento de autovetores. É preciso ordenar os autovetores de maneira a associar corretamente cada autovetor ao seu respectivo autovalor em relação a $\mathbf{F}$. No procedimento sobre o corpo dos reais, Candan *et al.* [17] fizeram o ordenamento segundo o número de cruzamentos pelo zero dos vetores. O número de cruzamentos pelo zero está relacionado ao número de zeros de cada uma das funções Hermite-Gaussianas.

Em corpos finitos, não é possível estabelecer, de maneira direta, um critério similar a esse, visto que não faz sentido falar em elementos positivos e negativos. No entanto, a Equação (3.2) permanece válida desde que haja uma associação correta entre os autovetores e autovalores de $\mathbf{F}$. O autovetor da $(i+1)$-ésima coluna de $\mathbf{V}$ é associado ao autovalor $\left((-\sqrt{-1})^a\right)^i$, em que a é um número racional. Com esse critério, é possível gerar matrizes distintas para $\mathbf{F}^a$. Permutando-se dois vetores

que são associados ao mesmo autovalor, gera-se matrizes distintas. Em [46], é feita uma análise mais detalhada sobre o número de matrizes distintas para $\mathbf{F}^a$.

3.2.4 Normalização dos autovetores da matriz $\mathbf{F}$

Como a matriz $\mathbf{F}$ é unitária, os autovetores $\mathbf{u}_k$ devem ser normalizados antes de serem utilizados como colunas de $\mathbf{V}$ na Equação (3.2).

Definição 3.1

A norma quadrática de um vetor $\mathbf{u} = (u[i])$*,* $i = 0, \ldots, N-1$*,* $u[i] \in \mathrm{GI}(p)$ *é dada por*

$$||\mathbf{u}||^2 := \sum_{i=0}^{N-1} u[i]u^*[i] \pmod p, \tag{3.9}$$

em que $\{.\}^*$ *representa o conjugado do argumento sobre* $\mathrm{GI}(p)$. □

Se as componentes de $\mathbf{u}$ estão em $\mathrm{GF}(p)$, então $||\mathbf{u}||^2 = \sum_{i=0}^{N-1} u^2[i] \pmod p$.

Analisando a Definição 3.1, conclui-se que se $||\mathbf{u}||^2$ não for resíduo quadrático em $\mathrm{GF}(p)$, então a norma de $\mathbf{u}$, $||\mathbf{u}||$, é um elemento de $\mathrm{GI}(p)$. Dessa maneira, mesmo que os elementos de $\mathbf{V}$ e $\mathbf{\Lambda}^a$ estejam em $\mathrm{GF}(p)$, a matriz $\mathbf{F}^a$ tem elementos em $\mathrm{GI}(p)$.

Para evitar operações em $\mathrm{GI}(p)$, ao invés de normalizar cada autovetor $\mathbf{u}_k$ obtido nas Equações 3.7 e 3.8, a expressão da Equação (3.2) é calculada e em seguida tem a k-ésima coluna multiplicada por $||\mathbf{u}_k||^2$.

Após essas considerações, é possível encontrar um conjunto único ortonormal de autovetores de $\mathbf{F}$, como era o objetivo. Reescrevendo a Equação (3.2) de acordo com a normalização dos autovetores, tem-se

$$\mathbf{F}^a[m,n] = \sum_{\substack{k=0 \\ (||\mathbf{u}_k|| \neq 0)}}^{2\lfloor N/2 \rfloor} ||\mathbf{u}_k||^{-2} u_k[m](-\sqrt{-1})^a u_k[n]. \tag{3.10}$$

A Tabela 3.1 resume o procedimento para a obtenção de $\mathbf{F}^a$ de acordo com a expansão espectral de $\mathbf{F}$ e utilizando a matriz $\mathbf{S}$.

A transformada inversa da GFrFT com parâmetro fracional $a = (a_1/a_2)$ é obtida escolhendo o parâmetro fracional $a' = (4 - a)$. A matriz de transformação da GFrFT inversa, $\mathbf{F}^{-a}$, é tal que

$$\mathbf{F}^{-a}[m,n] = \sum_{\substack{k=0 \\ (||\mathbf{u}_k|| \neq 0)}}^{2\lfloor N/2 \rfloor} ||\mathbf{u}_k||^{-2} u_k[m](-\sqrt{-1})^{-a} u_k[n]. \tag{3.11}$$

Tabela 3.1: *Síntese do procedimento para construção da matriz da GFrFT com dimensões $N \times N$ a partir da matriz comutante* $\mathbf{S}$.

Passo 1.	Escolha um elemento $\zeta \in \mathrm{GI}(p)$, de ordem multiplicativa $\mathrm{ord}(\zeta) = N$;
Passo 2.	Construa a matriz $\mathbf{S}$ a partir da Equação (3.3);
Passo 3.	Construa a matriz $\mathbf{L}$ a partir da Equação (3.4) ou Equação (3.5) de acordo com N ímpar ou par, respectivamente;
Passo 4.	Obtenha as matrizes $\mathbf{Ev}$ e $\mathbf{Od}$ a partir da transformação de similaridade da Equação (3.6) e calcule os autovalores e autovetores de cada matriz;
Passo 5.	Calcule os autovetores de $\mathbf{S}$ com a Equação (3.7) para os autovetores de $\mathbf{Ev}$ e com a Equação (3.8) para os autovetores de $\mathbf{Od}$;
Passo 6.	Construa a matriz $\mathbf{V}$ ordenando os autovetores obtidos no Passo 5 segundo os autovalores correspondentes de $\mathbf{\Lambda}$;
Passo 7.	De acordo com o parâmetro $a = a_1/a_2$, calcule a a-ésima potência dos autovalores de $\mathbf{F}$;
Passo 8.	Com a Equação (3.10) calcule a matriz de transformação de $\mathbf{F}^a$ usando os autovetores normalizados segundo a Equação (3.9).

Fonte: Próprio Autor.

Exemplo 3.1

Considere o elemento unimodular $\zeta = 24 + 6j \in \mathrm{GI}(47)$ *com ordem multiplicativa* $N = 6$*. As matrizes* $\mathbf{F}$*,* $\mathbf{S}$ *e* $\mathbf{L}$*, calculadas de acordo com as Equações (2.3), (3.3) e (3.5), respectivamente, são*

$$\mathbf{F} = \begin{bmatrix} 14 & 14 & 14 & 14 & 14 & 14 \\ 14 & 7+10j & 40+10j & 33 & 40+37j & 7+37j \\ 14 & 40+10j & 40+37j & 14 & 40+10j & 40+37j \\ 14 & 33 & 14 & 33 & 14 & 33 \\ 14 & 40+37j & 40+10j & 14 & 40+37j & 40+10j \\ 14 & 7+37j & 40+37j & 33 & 40+10j & 7+10j \end{bmatrix},$$

$$\mathbf{S} = \begin{bmatrix} 45 & 1 & 0 & 0 & 0 & 1 \\ 1 & 44 & 1 & 0 & 0 & 0 \\ 0 & 1 & 42 & 1 & 0 & 0 \\ 0 & 0 & 1 & 41 & 1 & 0 \\ 0 & 0 & 0 & 1 & 42 & 1 \\ 1 & 0 & 0 & 0 & 1 & 44 \end{bmatrix} \text{ e } \mathbf{L} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 27 & 0 & 0 & 0 & 27 \\ 0 & 0 & 27 & 0 & 27 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 27 & 0 & 20 & 0 \\ 0 & 27 & 0 & 0 & 0 & 20 \end{bmatrix}.$$

Aplicando a transformação de similaridade $\mathbf{LSL}^{-1}$*, gera-se a matriz*

$$\mathbf{LSL}^{-1} = \begin{bmatrix} 45 & 7 & 0 & 0 & 0 & 0 \\ 7 & 44 & 1 & 0 & 0 & 0 \\ 0 & 1 & 42 & 7 & 0 & 0 \\ 0 & 0 & 7 & 41 & 0 & 0 \\ 0 & 0 & 0 & 0 & 42 & 1 \\ 0 & 0 & 0 & 0 & 1 & 44 \end{bmatrix}.$$

A matriz tridiagonal $\mathbf{Ev}$ *tem dimensão* 4×4*. Observe que, para* $N = 6$*,* $(\lfloor 6/2 + 1 \rfloor) = 4$*. A matriz tridiagonal* $\mathbf{Od}$ *tem dimensão* 2×2*. Observe que, para* $N = 6$*,* $(\lfloor 6/2 - 1 \rfloor) = 2$*. As matrizes* $\mathbf{Ev}$ *e* $\mathbf{Od}$ *são, respectivamente,*

$$\mathbf{Ev} = \begin{bmatrix} 45 & 7 & 0 & 0 \\ 7 & 44 & 1 & 0 \\ 0 & 1 & 42 & 7 \\ 0 & 0 & 7 & 41 \end{bmatrix} \text{ e } \mathbf{Od} = \begin{bmatrix} 42 & 1 \\ 1 & 44 \end{bmatrix}.$$

Encontrando o polinômio característico da matriz $\mathbf{Ev}$ *e calculando suas raízes, mostra-se que* $\{2, 12, 27, 37\}$ *são seus autovalores. De forma semelhante, mostra-se que* $\{3, 36\}$ *são autovalores de* $\mathbf{Od}$*. Escalonando essas matrizes, foram obtidos os autovetores* $\mathbf{e}_k$ *de* $\mathbf{Ev}$ *e os autovetores* $\mathbf{o}_k$ *de* $\mathbf{Od}$*, que são apresentados na Tabela 3.2.*

Tabela 3.2: *Autovetores de* $\mathbf{Ev}$ *e* $\mathbf{Od}$ *para* $p = 47, \zeta = 24 + 6j, N = 6$*.*

k	$\mathbf{e}_k$	$\mathbf{o}_k$
0	1 14 16 14	1 8
1	1 2 23 2	1 41
2	1 31 30 32	–
3	1 19 1 10	–

Fonte: Próprio Autor.

Os autovetores de simetria par de $\mathbf{F}$ *são construídos por* $\mathbf{u}_{2k} = \mathbf{L}[\mathbf{e}_k^t, |0, 0]^t$*,* $k = 0, 1, 2, 3$*, e os autovetores de simetria ímpar de* $\mathbf{F}$ *são construídos por* $\mathbf{u}_{2k+1} = \mathbf{L}[0, 0, 0, 0, |\mathbf{o}_k^t]^t$*,* $k = 0, 1$*. Os autovetores de* $\mathbf{F}$ *são apresentados na Tabela 3.3 associados aos seus respectivos autovalores em relação a* $\mathbf{F}$*.*

Tabela 3.3: *Conjunto ortogonal de autovetores de* $\mathbf{F}$*, para* $p = 47, \zeta = 24 + 6j, N = 6$.

k	$\mathbf{u}_k$						λ_{u_k}
0	1	2	9	14	9	2	1
1	0	28	27	0	20	19	$-\sqrt{-1}$
2	1	7	10	22	10	7	-1
3	0	26	27	0	20	21	$\sqrt{-1}$
4	1	38	11	32	11	38	1
5	0	0	0	0	0	0	$-$
6	1	43	27	10	27	43	-1

Fonte: Próprio Autor.

Após a normalização dos autovetores e considerando o parâmetro $a = 3/8$*, pela Equação (3.10), a matriz da GFrFT é (considere que* $j = \sqrt{-1} \pmod p$*)*

$$\mathbf{F}^{\frac{3}{8}} = \begin{bmatrix} 19+2j & 23+13j & 23+13j & 23+13j & 23+13j & 23+13j \\ 23+13j & 38+29j & 17+17j & 24+34j & 7+17j & 28+20j \\ 23+13j & 17+17j & 5+16j & 23+13j & 15+7j & 7+17j \\ 23+13j & 24+34j & 23+13j & 20+23j & 23+13j & 24+34j \\ 23+13j & 7+17j & 15+7j & 23+13j & 5+16j & 17+17j \\ 23+13j & 28+20j & 7+17j & 24+34j & 17+17j & 38+29j \end{bmatrix}. \qquad \square$$

3.3 GFrCT e GFrST tipo 1 baseadas na expansão espectral - matriz S

A transformada fracional do cosseno em corpos finitos (GFrCT) tipo 1 e a transformada fracional do seno em corpos finitos (GFrST) tipo 1 podem ser obtidas a partir dos autovetores de $\mathbf{F}$. Para se construir um conjunto ortogonal de autovetores das matrizes de dimensão $(N+1) \times (N+1)$ da FFCT do tipo 1 e de dimensão $(N-1) \times (N-1)$ da FFST do tipo 1, é preciso construir uma matriz $\mathbf{F}$ de dimensão $2N \times 2N$.

Proposição 3.2

As matrizes $\mathbf{C}_1$*, obtida pela Equação (2.12), e* $\mathbf{Ev}$*, obtida pela Equação (3.6), comutam. As matrizes* $\mathbf{S}_1$*, obtida pela Equação (2.16), e* $\mathbf{Od}$*, obtida pela Equação (3.6), comutam.*

Demonstração: Vide Apêndice B, seção B.1.2. ■

De acordo com as Proposições 2.6 e 3.2, os $(N+1)$ autovetores de $\mathbf{Ev}$ são os $(N+1)$ autovetores de $\mathbf{C}_1$, enquanto que os $(N-1)$ autovetores de $\mathbf{Od}$ são os $(N-1)$ autovetores de $\mathbf{S}_1$. Após um processo de normalização dos autovetores, tem-se que a matriz de transformação da GFrCT é

$$\mathbf{C}_1^a = \hat{\mathbf{V}}\hat{\mathbf{\Lambda}}^a\hat{\mathbf{V}}^t \tag{3.12}$$

e a matriz de transformação da GFrST é

$$\mathbf{S}_1^a = \tilde{\mathbf{V}}\tilde{\mathbf{\Lambda}}^a\tilde{\mathbf{V}}^t, \tag{3.13}$$

em que $\hat{\mathbf{V}}$ e $\tilde{\mathbf{V}}$ são matrizes cujas colunas são autovetores ortonormais de $\mathbf{C}_1$ e $\mathbf{S}_1$, respectivamente. $\hat{\mathbf{\Lambda}}$ e $\tilde{\mathbf{\Lambda}}$ são matrizes diagonais cujo elemento na k-ésima linha e k- ésima coluna é dado por $(-1)^k$.

As transformadas inversas da GFrCT e da GFrST associadas ao parâmetro fracional a são obtidas escolhendo o parâmetro fracional $a' = (2-a)$. Note que nem a GFrCT nem a GFrST são involuções.

A Tabela 3.4 resume o procedimento para a obtenção de $\mathbf{C}_1^a$ e a Tabela 3.5 resume o procedimento para a obtenção de $\mathbf{S}_1^a$, de acordo com suas respectivas expansões espectrais.

Tabela 3.4: *Síntese do procedimento para construção da matriz da GFrCT tipo 1, com dimensões* $(N+1)\times(N+1)$*, a partir da matriz comutante* $\mathbf{S}$.

Passo 1.	Escolha um elemento $\zeta \in \mathrm{GI}(p)$, de ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$;
Passo 2.	Construa a matriz $\mathbf{S}$ a partir da Equação (3.3);
Passo 3.	Construa a matriz $\mathbf{L}$ a partir da Equação (3.4) ou Equação (3.5), de acordo com N ímpar ou par, respectivamente;
Passo 4.	Obtenha a matriz $\mathbf{Ev}$ a partir da transformação de similaridade da Equação (3.6) e calcule seus autovalores e autovetores;
Passo 5.	Use os autovetores de $\mathbf{Ev}$ como autovetores de $\mathbf{C}_1$ associando-os aos correspondentes autovalores de $\mathbf{C}_1$;
Passo 6.	De acordo com o parâmetro $a = a_1/a_2$, calcule a a-ésima potência dos autovalores de $\mathbf{C}_1$;
Passo 7.	Com a Equação (3.12) calcule a matriz de transformação de $\mathbf{C}_1^a$.

Fonte: Próprio Autor.

Exemplo 3.2

Considere o elemento unimodular $\zeta = 24+6j \in \mathrm{GI}(47)$ *com ordem multiplicativa* $N = 6$*. Os autovetores de* $\mathbf{C}_1$ *são os mesmos de* $\mathbf{Ev}$*, reapresentados na segunda coluna da Tabela 3.6 e associados aos seus respectivos autovalores, terceira coluna da Tabela 3.6.*

Tabela 3.5: *Síntese do procedimento para construção da matriz da GFrST tipo 1, com dimensões* $(N-1)\times(N-1)$*, a partir da matriz comutante* $\mathbf{S}$*.*

Passo 1.	Escolha um elemento $\zeta \in \mathrm{GI}(p)$, de ordem multiplicativa $\mathrm{ord}(\zeta) = 2N+2$;
Passo 2.	Construa a matriz $\mathbf{S}$ a partir da Equação (3.3);
Passo 3.	Construa a matriz $\mathbf{L}$ a partir da Equação (3.4) ou Equação (3.5), de acordo com N ímpar ou par, respectivamente;
Passo 4.	Obtenha a matriz $\mathbf{Od}$ a partir da transformação de similaridade da Equação (3.6) e calcule seus autovalores e autovetores;
Passo 5.	Use os autovetores de $\mathbf{Od}$ como autovetores de $\mathbf{S}_1$ associando-os aos correspondentes autovalores de $\mathbf{S}_1$;
Passo 6.	De acordo com o parâmetro $a = a_1/a_2$, calcule a a-ésima potência dos autovalores de $\mathbf{S}_1$;
Passo 7.	Com a Equação (3.13) calcule a matriz de transformação de $\mathbf{S}_1^a$.

Fonte: Próprio Autor.

Tabela 3.6: *Autovetores de* $\mathbf{C}_1$ *associados aos respectivos autovalores, para* $p = 47, \zeta = 24+6j, N = 6$*.*

k	$\mathbf{e}_k$	λ_k
0	1 14 16 14	-1
1	1 2 23 2	1
2	1 31 30 32	-1
3	1 19 1 10	1

Fonte: Próprio Autor.

Após a normalização dos autovetores, usando a Equação (3.9), e considerando o parâmetro $a = 3/8$*, a matriz da GFrCT tipo 1 é*

$$\mathbf{C}_1^{\frac{3}{8}} = \begin{bmatrix} 20+23j & 27+3j & 27+3j & 24+34j \\ 27+3j & 20+23j & 27+13j & 20+44j \\ 27+3j & 23+13j & 19+2j & 27+3j \\ 24+34j & 20+44j & 27+3j & 19+2j \end{bmatrix}. \qquad \square$$

Nota 3. 3 Esses procedimentos estão condicionados à existência de autovalores e autovetores de $\mathbf{S}$ em $\mathrm{GF}(p)$ ou $\mathrm{GI}(p)$. Por exemplo, para $p = 47$, alguns autovalores estão em corpos de extensão. A Tabela 3.7 relaciona os autovalores das matrizes $\mathbf{Ev}$ e $\mathbf{Od}$ que pertencem a $\mathrm{GI}(47)$ com os elementos unimodulares de ordem $N = 16$ em $\mathrm{GI}(47)$.

Tabela 3.7: *Autovalores de* $\mathbf{Ev}$ *e* $\mathbf{Od}$ *que pertencem a* $\mathrm{GI}(47)$*, associados a diferentes elementos* ζ *de ordem* $N = 16$ *em* $\mathrm{GI}(47)$*. Com esses parâmetros há autovalores de* $\mathbf{Ev}$ *e* $\mathbf{Od}$ *que não pertencem a* $\mathrm{GI}(p)$*. Por serem tridiagonais, as matrizes* $\mathbf{Ev}$ *e* $\mathbf{Od}$ *de dimensão* 9×9 *e* 7×7*, respectivamente, devem ter nove e sete autovalores distintos, respectivamente. Para* $\mathbf{Ev}$*, há nove autovalores em* $\mathrm{GI}(47)$ *considerando* $\zeta = 25 + 9j$*, mas há apenas um autovalor em* $\mathrm{GI}(47)$ *considerando* $\zeta = 22 + 9j$*. Para* $\mathbf{Od}$*, há sete autovalores em* $\mathrm{GI}(47)$ *considerando* $\zeta = 22 + 9j$*, mas há apenas três autovalores em* $\mathrm{GI}(47)$ *considerando* $\zeta = 38 + 22j$*.*

ζ	Autovalores de $\mathbf{Ev}$	Autovalores de $\mathbf{Od}$
$9 + 22j$	$41,\ 43,\ 43 + 20j,\ 43 + 27j,\ 45$	$39,\ 43,\ 43 + 8j,\ 43 + 9j,\ 43 + 38j,\ 43 + 39j$
$9 + 25j$	$41,\ 43,\ 43 + 20j,\ 43 + 27j,\ 45$	$39,\ 43,\ 43 + 8j,\ 43 + 9j,\ 43 + 38j,\ 43 + 39j$
$22 + 9j$	43	$2,\ 7,\ 32,\ 37,\ 43,\ 43 + 2j,\ 43 + 45j$
$22 + 38j$	43	$2,\ 7,\ 32,\ 37,\ 43,\ 43 + 2j,\ 43 + 45j$
$25 + 9j$	$19,\ 20,\ 43,\ 12 + 13j,\ 12 + 34j,\ 27 + 13j,$ $27 + 34j,\ 43 + 5j,\ 43 + 42j$	$43,\ 43 + 13j,\ 43 + 34j$
$25 + 38j$	$19,\ 20,\ 43,\ 12 + 13j,\ 12 + 34j,\ 27 + 13j,$ $27 + 34j,\ 43 + 5j,\ 43 + 42j$	$43,\ 43 + 13j,\ 43 + 34j$
$38 + 22j$	$43,\ 43 + 19j,\ 43 + 21j,\ 43 + 26j,\ 43 + 28j$	$1,\ 38,\ 43$
$38 + 25j$	$43,\ 43 + 19j,\ 43 + 21j,\ 43 + 26j,\ 43 + 28j$	$1,\ 38,\ 43$

Fonte: Próprio Autor.

3.4 GFrHT baseada na expansão espectral - matriz S

A transformada fracional de Hartley em corpos finitos baseada na matriz $\mathbf{S}$ é um resultado da pesquisa e se apresenta como contribuição da tese.

O procedimento desenvolvido para encontrar a GFrFT usando matrizes comutantes pode ser replicado para se encontrar a transformada fracional de Hartley em corpos finitos (GFrHT). As considerações feitas para a matriz $\mathbf{F}$ também são válidas para a matriz $\mathbf{H}$. Inicialmente, mostra-se que as matrizes $\mathbf{S}$ e $\mathbf{H}$ comutam.

Proposição 3.3

As matrizes $\mathbf{H}$*, obtida da Equação (2.4) e* $\mathbf{S}$*, definida na Equação (3.3), comutam.*

Demonstração: Vide Apêndice B, seção B.1.3. ■

Com isso, o procedimento para se obter os autovetores de $\mathbf{H}$ a partir de $\mathbf{S}$ é análogo ao procedimento desenvolvido para se obter os autovetores da matriz $\mathbf{F}$. Há, no entanto, uma diferença no que se refere à associação de autovetores e autovalores no processo de ordenação de autovetores. Como visto na Proposição 2.4, os autovetores de $\mathbf{H}$ associados ao autovalor 1 são autovetores de $\mathbf{F}$ associados aos autovalores 1 e $-\sqrt{-1}$, enquanto que os autovetores de $\mathbf{H}$ associados ao autovalor -1

são autovetores de $\mathbf{F}$ associados aos autovalores -1 e $\sqrt{-1}$. Essas relações devem ser respeitadas quando da ordenação dos autovetores. Pelas mesmas considerações expostas na Seção 3.2.4, os autovetores de $\mathbf{H}$ devem ser normalizados utilizando-se a Equação (3.9). Reescrevendo a Equação (3.2) de acordo com a normalização dos autovetores, tem-se

$$\mathbf{H}^a[m,n] = \sum_{\substack{k=0 \\ (||\mathbf{u}_k|| \neq 0)}}^{2\lfloor N/2 \rfloor} ||\mathbf{u}_k||^{-2} u_k[m](-\sqrt{-1})^a u_n. \tag{3.14}$$

A transformada inversa da GFrHT associada ao parâmetro fracional a é obtida escolhendo o parâmetro fracional $a' = (2-a)$. Note que a GFrHT não é uma involução.

A Tabela 3.8 resume o procedimento para a obtenção de $\mathbf{H}^a$ de acordo com a expansão espectral de $\mathbf{H}$ e utilizando a matriz $\mathbf{S}$.

Tabela 3.8: *Síntese do procedimento para construção da matriz da GFrHT com dimensões $N \times N$ a partir da matriz comutante* $\mathbf{S}$.

Passo 1.	Escolha um elemento $\zeta \in \mathrm{GI}(p)$, de ordem multiplicativa $\mathrm{ord}(\zeta) = N$;
Passo 2.	Construa a matriz $\mathbf{S}$ a partir da Equação (3.3);
Passo 3.	Construa a matriz $\mathbf{L}$ a partir da Equação (3.4) ou Equação (3.5) de acordo com N ímpar ou par, respectivamente;
Passo 4.	Obtenha as matrizes $\mathbf{Ev}$ e $\mathbf{Od}$ a partir da transformação de similaridade da Equação (3.6) e calcule os autovalores e autovetores de cada matriz;
Passo 5.	Calcule os autovetores de $\mathbf{S}$ com a Equação (3.7) para os autovetores de $\mathbf{Ev}$ e com a Equação (3.8) para os autovetores de $\mathbf{Od}$;
Passo 6.	Construa a matriz $\mathbf{V}$ ordenando os autovetores obtidos no Passo 5 segundo os autovalores correspondentes de $\mathbf{\Lambda}$, atentando-se à Proposição 2.4;
Passo 7.	De acordo com o parâmetro $a = a_1/a_2$, calcule a a-ésima potência dos autovalores de $\mathbf{H}$;
Passo 8.	Com a Equação (3.14) calcule a matriz de transformação de $\mathbf{H}^a$, usando os autovetores normalizados segundo a Equação (3.9).

Fonte: Próprio Autor.

Exemplo 3.3

Considere o elemento unimodular $\zeta = 24 + 6j \in \mathrm{GI}(47)$ com ordem multiplicativa $N = 6$. Os autovetores de $\mathbf{H}$ são os mesmos de $\mathbf{F}$ e são reapresentados na Tabela 3.9, mas associados aos autovalores de $\mathbf{H}$.

Após a normalização dos autovetores e considerando o parâmetro $a = 3/8$, a matriz da GFrHT é

$$\mathbf{H}^{\frac{3}{8}} = \begin{bmatrix} 19+2j & 23+13j & 23+13j & 23+13j & 23+13j & 23+13j \\ 23+13j & 34+35j & 15+33j & 24+34j & 9+1j & 32+14j \\ 23+13j & 15+33j & 5+37j & 23+13j & 15+33j & 9+1j \\ 23+13j & 24+34j & 23+13j & 20+23j & 23+13j & 24+34j \\ 23+13j & 9+1j & 15+33j & 23+13j & 5+37j & 15+33j \\ 23+13j & 32+14j & 9+1j & 24+34j & 15+33j & 34+35j \end{bmatrix}. \quad \square$$

Tabela 3.9: *Conjunto ortogonal de autovetores de* $\mathbf{H}$*, para* $p = 47, \zeta = 24 + 6j, N = 6$.

k	$\mathbf{u}_k$						λ_{u_k}
0	1	2	9	14	9	2	1
1	0	28	27	0	20	19	1
2	1	7	10	22	10	7	-1
3	0	26	27	0	20	21	-1
4	1	38	11	32	11	8	1
5	0	0	0	0	0	0	$-$
6	1	43	27	10	27	43	-1

Fonte: Próprio Autor.

3.5 GFrFT e GFrHT generalizadas baseadas na expansão espectral - matriz E

A definição das transformadas fracionais de Fourier e Hartley generalizadas e das transformadas fracionais do seno e do cosseno tipo 4 é resultado da pesquisa e se apresenta como contribuição da tese.

3.5.1 A matriz E

Pei *et al.* [47] propuseram uma matriz definida sobre o corpo dos números reais que comuta com a matriz de transformação da transformada discreta de Fourier generalizada. Mostrou-se também que o procedimento para se obter autovetores ortogonais a partir da matriz **S** pode ser utilizado com matriz **E**, observando algumas modificações. Baseado nesse trabalho, nesta Seção é definida a matriz **E** em corpos finitos e é verificado que o procedimento para se obter autovetores ortogonais da matriz **S** em corpos finitos é válido também para a matriz **E** em corpos finitos.

Considere a matriz $\mathbf{E}$ de dimensão $N \times N$, cujos elementos não nulos são dados pela regra

$$\begin{cases} [E]_{0,N-1} = [E]_{N-1,0} = p-1, & \\ [E]_{i,i+1} = [E]_{i+1,i} = 1, & 0 \leq i \leq N-2, \\ [E]_{i,i} = \varepsilon_i \pmod p, & 0 \leq i \leq N-1, \end{cases} \tag{3.15}$$

em que $\varepsilon_i = 2\cos_\zeta(i+1/2)$, $i = 0, 1, \ldots$, e ζ é um elemento não nulo de ordem multiplicativa $\mathrm{ord}(\zeta) = N$ em $\mathrm{GI}(p)$. Assim a matriz $\mathbf{E}$ tem a forma

$$\mathbf{E} = \begin{bmatrix} \varepsilon_0 & 1 & 0 & \ldots & -1 \\ 1 & \varepsilon_1 & 1 & \ldots & 0 \\ 0 & 1 & \varepsilon_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \ldots & \varepsilon_{N-1} \end{bmatrix} \pmod p. \tag{3.16}$$

Proposição 3.4

As matrizes $\mathbf{F_G}$, obtida pela Equação (2.6), e $\mathbf{E}$, obtida pela Equação (3.15), comutam. As matrizes $\mathbf{H_G}$, obtida pela Equação (2.9), e $\mathbf{E}$, obtida pela Equação (3.15), comutam.

Demonstração: Vide Apêndice B, seção B.2.1. ■

3.5.2 Autovetores da matriz $\mathbf{E}$

De forma semelhante ao desenvolvido com a matriz $\mathbf{S}$, a unicidade dos autovetores da matriz $\mathbf{E}$ é verificada por meio de um procedimento que usa uma transformação de similaridade. Considere a matriz $\mathbf{L} = [L]_{i,k}$, de dimensão $N \times N$, dada pela seguinte regra:

- Para N ímpar, os elementos não nulos de $\mathbf{L}$ são dados por

$$[L]_{i,k} := \begin{cases} 1, & \text{se } i = k = 1, \ldots, (N-1)/2, \\ -1, & \text{se } i = k = (N+1)/2+1, \ldots, N, \\ \sqrt{2^{-1}} \pmod p, & \text{se } i = k = (N+1)/2, \\ 1, & \text{se } i = (N+1)/2+1, \ldots, N, \ k = 1, \ldots, (N-1)/2, \\ 1, & \text{se } i = 1, \ldots, (N-1)/2, \ k = (N+1)/2+1, \ldots, N. \end{cases} \tag{3.17}$$

A matriz $\mathbf{L}$ tem a forma

$$\mathbf{L} = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{I}_{\frac{N-1}{2}} & 0 & \mathbf{J}_{\frac{N-1}{2}} \\ 0 & \sqrt{2} & 0 \\ \mathbf{J}_{\frac{N-1}{2}} & 0 & -\mathbf{I}_{\frac{N-1}{2}} \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \sqrt{2} & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & \dots & -1 & 0 \\ 1 & 0 & \dots & 0 & \dots & 0 & -1 \end{bmatrix}.$$

- Para N par, os elementos não nulos de $\mathbf{L}$ são dados por

$$[L]_{i,k} = \begin{cases} 1, & \text{se } i = k = 1, \dots, N/2, \\ -1, & \text{se } i = k = N/2+1, \dots, N, \\ 1, & \text{se } i = N/2+1, \dots, N, \ k = 1, \dots, N/2, \\ 1, & \text{se } i = 1, \dots, N/2, \ k = N/2+1, \dots, N. \end{cases} \tag{3.18}$$

A matriz $\mathbf{L}$ tem a forma

$$\mathbf{L} = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{I}_{\frac{N}{2}} & \mathbf{J}_{\frac{N}{2}} \\ \mathbf{J}_{\frac{N}{2}} & -\mathbf{I}_{\frac{N}{2}} \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & \dots & -1 & 0 \\ 1 & 0 & \dots & 0 & \dots & 0 & -1 \end{bmatrix}.$$

Por meio do Lema B.5 (Vide Apêndice B), mostra-se que a transformação de similaridade

$$\mathbf{L}\mathbf{E}\mathbf{L}^{-1} = \begin{bmatrix} \mathbf{Ev} & \mathbf{0} \\ \mathbf{0} & \mathbf{Od} \end{bmatrix} \tag{3.19}$$

produz as matrizes tridiagonais simétricas $\mathbf{Ev}$ e $\mathbf{Od}$, com dimensões $\lfloor (N+1)/2 \rfloor$ e $\lfloor (N-1)/2 \rfloor$, respectivamente [47]. De maneira similar ao analisado com a matriz $\mathbf{S}$, conclui-se que os autovetores dessas matrizes são únicos, e por meio de extensões simétricas são obtidos os autovetores de $\mathbf{E}$.

A partir da Proposição 2.9, os autovetores de $\mathbf{F_G}$ com simetria par podem ser obtidos por meio dos autovetores de $\mathbf{Ev}$, $\mathbf{e}_k$, fazendo

$$\mathbf{u}_{2k} = \mathbf{L}[\mathbf{e}_k^t | 0 \dots 0]^t, \;\; k = 0, \dots, \left\lfloor \frac{N+1}{2} \right\rfloor, \tag{3.20}$$

e os autovetores de $\mathbf{F_G}$ com simetria ímpar podem ser obtidos por meio dos autovetores de $\mathbf{Od}$, $\mathbf{o}_k$, fazendo

$$\mathbf{u}_{2k+1} = \mathbf{L}[0 \dots 0 | \mathbf{o}_k^t]^t, \;\; k = 0, \dots, \left\lfloor \frac{N-1}{2} \right\rfloor. \tag{3.21}$$

Como os autovetores de $\mathbf{F_G}$ são autovetores de $\mathbf{H_G}$, o procedimento pode ser usado desde que seja respeitado a associação entre autovetores e autovalores para esta matriz.

Da mesma forma que para a matriz $\mathbf{S}$, não há um critério para ordenamento de autovetores de $\mathbf{E}$ de forma a se obter uma matriz única. O processo de normalização deve também ser feito, como o utilizado com a matriz $\mathbf{E}$, para se construir matrizes unitárias.

O procedimento descrito na Tabela 3.1 pode ser usado para a construção da GFrFT generalizada com algumas modificações: troca-se a matriz $\mathbf{S}$ pela matriz $\mathbf{E}$, e no Passo 3, a matriz $\mathbf{L}$ é construída de acordo com a Equação 3.17 ou com a Equação 3.18. O mesmo pode ser dito para a construção da GFrHT generalizada, em que no procedimento descrito na Tabela 3.8 pode ser usado trocando-se a matriz $\mathbf{S}$ pela matriz $\mathbf{E}$ e construindo a matriz $\mathbf{L}$ de acordo com a Equação 3.17 ou com a Equação 3.18.

Exemplo 3.4

Considere o elemento unimodular $\zeta = 4 \in \mathrm{GI}(257)$ com ordem multiplicativa $N = 8$. As matrizes $\mathbf{S}$ e $\mathbf{L}$, calculadas de acordo com a Equações (3.15) e (3.18), respectivamente, são

$$\mathbf{E} = \begin{bmatrix} 131 & 1 & 0 & 0 & 0 & 0 & 0 & 256 \\ 1 & 233 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 24 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 126 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 126 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 24 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 223 & 1 \\ 256 & 0 & 0 & 0 & 0 & 0 & 1 & 131 \end{bmatrix}$$

e

$$\mathbf{L} = \begin{bmatrix} 30 & 0 & 0 & 0 & 0 & 0 & 0 & 30 \\ 0 & 30 & 0 & 0 & 0 & 0 & 30 & 0 \\ 0 & 0 & 30 & 0 & 0 & 30 & 0 & 0 \\ 0 & 0 & 0 & 30 & 30 & 0 & 0 & 0 \\ 0 & 0 & 0 & 30 & 227 & 0 & 0 & 0 \\ 0 & 0 & 30 & 0 & 0 & 227 & 0 & 0 \\ 0 & 30 & 0 & 0 & 0 & 0 & 227 & 0 \\ 30 & 0 & 0 & 0 & 0 & 0 & 0 & 227 \end{bmatrix}.$$

Aplicando a transformação de similaridade $\mathbf{LSL}^{-1}$*, gera-se a matriz*

$$\mathbf{LEL}^{-1} = \begin{bmatrix} 130 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 233 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 24 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 127 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 125 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 24 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 233 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 132 \end{bmatrix}.$$

A matriz tridiagonal $\mathbf{Ev}$ *tem dimensão* $4 \times 4\,(8/2)$*, e a matriz tridiagonal* $\mathbf{Od}$ *tem dimensão* $2 \times 2\,(8/2)$*, em que*

$$\mathbf{Ev} = \begin{bmatrix} 132 & 1 & 0 & 0 \\ 1 & 233 & 1 & 0 \\ 0 & 1 & 24 & 1 \\ 0 & 0 & 1 & 125 \end{bmatrix} \text{ e } \mathbf{Od} = \begin{bmatrix} 130 & 1 & 0 & 0 \\ 1 & 233 & 1 & 0 \\ 0 & 1 & 24 & 1 \\ 0 & 0 & 1 & 127 \end{bmatrix}.$$

Encontrando o polinômio característico da matriz $\mathbf{Ev}$ *e calculando suas raízes, mostra-se que* $\{52, 81, 176, 205\}$ *são seus autovalores. De forma semelhante, mostra-se que* $\{56, 112, 145, 201\}$ *são autovalores de* $\mathbf{Od}$*. Escalonando essas matrizes, foram obtidos os autovetores* $\mathbf{e}_k$ *de* $\mathbf{Ev}$ *e os autovetores* $\mathbf{o}_k$ *de* $\mathbf{Od}$*, que são apresentrados na Tabela 3.10.*

Tabela 3.10: *Autovetores de* $\mathbf{Ev}$ *e* $\mathbf{Od}$ *para* $p = 257, \zeta = 4, N = 8$.

k	$\mathbf{e}_k$				$\mathbf{o}_k$			
0	1	183	247	11	1	177	87	203
1	1	239	121	129	1	44	61	233
2	1	15	221	255	1	206	41	75
3	1	71	40	70	1	73	11	119

Fonte: Próprio Autor.

Os autovetores de simetria par de $\mathbf{F}$ *são construídos por* $\mathbf{u}_{2k} = \mathbf{L}[\mathbf{e}_k^t, |0, 0]^t$, $k = 0, 1, 2, 3$, *e os autovetores de simetria ímpar de* $\mathbf{F}$ *são construídos por* $\mathbf{u}_{2k+1} = \mathbf{L}[0, 0, 0, 0, |\mathbf{o}_k^t]^t$, $k = 0, 1$. *Os autovetores de* $\mathbf{F}$ *são apresentados na Tabela 3.11 associados aos seus respectivos autovalores em relação a* $\mathbf{F}$.

Tabela 3.11: *Conjunto ortogonal de autovetores de* $\mathbf{F_G}$, *para* $p = 257, \zeta = 4, N = 8$.

k	$\mathbf{u}_k$								λ_{u_k}
0	1	183	247	11	11	247	183	1	$\sqrt{-1}$
1	1	239	121	129	129	121	239	1	$-\sqrt{-1}$
2	1	15	221	255	255	221	15	1	$\sqrt{-1}$
3	1	71	40	70	70	40	71	1	$-\sqrt{-1}$
4	1	177	87	203	54	170	80	256	1
5	1	44	61	233	24	196	213	256	-1
6	1	206	41	75	182	216	51	256	1
7	1	73	11	119	138	246	184	256	-1

Fonte: Próprio Autor.

Após a normalização dos autovetores e considerando o parâmetro $a = 3/8$, *pela Equação (3.10), a matriz da GFrFT generalizada é*

$$\mathbf{F}_{\mathbf{G}}^{\frac{3}{8}} = \begin{bmatrix} 10 & 8 & 46 & 107 & 93 & 254 & 28 & 233 \\ 8 & 129 & 73 & 211 & 3 & 231 & 10 & 28 \\ 46 & 73 & 200 & 8 & 28 & 53 & 231 & 254 \\ 107 & 211 & 8 & 62 & 87 & 28 & 3 & 93 \\ 93 & 3 & 28 & 87 & 62 & 8 & 211 & 107 \\ 254 & 231 & 53 & 28 & 8 & 200 & 73 & 46 \\ 28 & 10 & 231 & 3 & 211 & 73 & 129 & 8 \\ 233 & 28 & 254 & 93 & 107 & 46 & 8 & 10 \end{bmatrix}.$$

Os autovetores de $\mathbf{H_G}$ são os mesmos de $\mathbf{F_G}$ e são reapresentados na Tabela 3.12, mas associados aos autovalores de $\mathbf{H_G}$.

Tabela 3.12: *Conjunto ortogonal de autovetores de $\mathbf{H_G}$, para $p = 257, \zeta = 4, N = 8$.*

k	$\mathbf{u}_k$								λ_{u_k}
0	1	183	247	11	11	247	183	1	1
1	1	239	121	129	129	121	239	1	-1
2	1	15	221	255	255	221	15	1	1
3	1	71	40	70	70	40	71	1	-1
4	1	177	87	203	54	170	80	256	1
5	1	44	61	233	24	196	213	256	-1
6	1	206	41	75	182	216	51	256	1
7	1	73	11	119	138	246	184	256	-1

Fonte: Próprio Autor.

Após a normalização dos autovetores e considerando o parâmetro $a = 3/8$, pela Equação (3.14), a matriz da GFrHT generalizada é

$$\mathbf{H}_{\mathbf{G}}^{\frac{3}{8}} = \begin{bmatrix} 219 & 143 & 143 & 86 & 72 & 94 & 163 & 185 \\ 143 & 205 & 185 & 114 & 163 & 86 & 86 & 163 \\ 143 & 185 & 61 & 143 & 163 & 171 & 86 & 94 \\ 86 & 114 & 143 & 47 & 72 & 163 & 163 & 72 \\ 72 & 163 & 163 & 72 & 47 & 143 & 114 & 86 \\ 94 & 86 & 171 & 163 & 143 & 61 & 185 & 143 \\ 163 & 86 & 86 & 163 & 114 & 185 & 205 & 143 \\ 185 & 163 & 94 & 72 & 86 & 143 & 143 & 219 \end{bmatrix}. \qquad \square$$

3.6 GFrCT e GFrST tipo 4 baseadas na expansão espectral - matriz E

A transformada fracional do cosseno em corpos finitos (GFrCT) tipo 4 e a transformada fracional do seno em corpos finitos (GFrST) tipo 4 podem ser obtidas a partir dos autovetores de $\mathbf{F_G}$. Para se construir um conjunto ortogonal de autovetores das matrizes de dimensão $(N) \times (N)$ da FFCT do tipo 4 e da FFST do tipo 4, é preciso construir a matriz $\mathbf{F_G}$ de dimensão $2N \times 2N$.

Proposição 3.5

As matrizes $\mathbf{C}_4$ *e* $\mathbf{Od}$*, definida em 3.19, comutam. As matrizes* $\mathbf{S}_4$ *e* $\mathbf{Ev}$*, definida em 3.19, comutam.*

Demonstração: Vide Apêndice B, seção B.2.2. ■

De acordo com as Proposições 2.9 e 3.5, os N autovetores de $\mathbf{Od}$ são os N autovetores de $\mathbf{C}_4$, enquanto que os N autovetores de $\mathbf{Ev}$ são os N autovetores de $\mathbf{S}_4$. Tem-se então que

$$\mathbf{C}_4^a = \hat{\mathbf{V}}\hat{\mathbf{\Lambda}}^a\hat{\mathbf{V}}^t \tag{3.22}$$

e

$$\mathbf{S}_4^a = \tilde{\mathbf{V}}\tilde{\mathbf{\Lambda}}^a\tilde{\mathbf{V}}^t, \tag{3.23}$$

em que $\hat{\mathbf{V}}$ e $\tilde{\mathbf{V}}$ são matrizes cujas colunas são autovetores ortonormais de $\mathbf{C}_4$ e $\mathbf{S}_4$, respectivamente. $\hat{\mathbf{\Lambda}}$ e $\tilde{\mathbf{\Lambda}}$ são matrizes diagonais cujo elemento na k-ésima linha e k- ésima coluna é dado por $(-1)^k$.

Exemplo 3.5

Considere o elemento unimodular $\zeta = 4 \in \mathrm{GI}(257)$ *com ordem multiplicativa* $N = 8$*. Os autovetores de* $\mathbf{S}_4$ *são os mesmos de* $\mathbf{Ev}$*, reapresentados na segunda coluna da Tabela 3.13 e associados aos seus respectivos autovalores, terceira coluna da Tabela 3.13.*

Os autovetores de $\mathbf{C}_4$ *são os mesmos de* $\mathbf{Od}$*, reapresentados na segunda coluna da Tabela 3.14 e associados aos seus respectivos autovalores, terceira coluna da Tabela 3.14.*

Após a normalização dos autovetores, usando a Equação (3.9), e considerando o parâmetro $a = 3/8$*, a matriz da GFrST tipo 4 é*

$$\mathbf{S}_4^{\frac{3}{8}} = \begin{bmatrix} 147 & 49 & 237 & 158 \\ 49 & 34 & 14 & 20 \\ 237 & 14 & 232 & 49 \\ 158 & 20 & 49 & 119 \end{bmatrix}$$

e a matriz da GFrCT tipo 4 é

$$\mathbf{C}_4^{\frac{3}{8}} = \begin{bmatrix} 34 & 237 & 49 & 14 \\ 237 & 119 & 99 & 208 \\ 49 & 99 & 147 & 237 \\ 14 & 208 & 237 & 232 \end{bmatrix}. \qquad \square$$

Tabela 3.13: *Autovetores de* $\mathbf{S}_4$ *associados aos respectivos autovalores, para* $p = 257, \zeta = 4, N = 8$.

k	$\mathbf{e}_k$	λ_k
0	1 183 247 11	1
1	1 239 121 129	-1
2	1 15 221 255	1
3	1 71 40 70	-1

Fonte: Próprio Autor.

Tabela 3.14: *Autovetores de* $\mathbf{C}_4$ *associados aos respectivos autovalores, para* $p = 257, \zeta = 4, N = 8$.

k	$\mathbf{o}_k$	λ_k
0	1 177 87 203	1
1	1 44 61 233	-1
2	1 206 41 75	1
3	1 73 11 119	-1

Fonte: Próprio Autor.

3.7 Autoestrutura da GFrFT baseada na expansão espectral

Na Equação (3.10) da matriz da GFrFT, derivada da expansão espectral da Equação (3.2), observa-se que $\mathbf{F}^a$ é diagonalizável. Se $\mathbf{V}$ é um conjunto completo e ortonormal de autovetores de $\mathbf{F}$, ele também o é para $\mathbf{F}^a$. Contudo, os autovalores de $\mathbf{F}^a$ não são os mesmos de $\mathbf{F}$. Seguindo os critérios de ordenamento dos autovetores, Seção 3.2.3, o k-ésimo autovalor, λ'_k, associado ao autovetor $\mathbf{u}_k$ é dado por

$$\lambda'_k = \left(-\sqrt{-1}^{\,a}\right)^k, \;\; k = 0, 1, \ldots, 2\lfloor N/2 \rfloor. \tag{3.24}$$

Observe que, de acordo com a multiplicidade dos autovalores de $\mathbf{F}$, alguns autovalores de $\mathbf{F}^a$ podem ser iguais. Se N é um número ímpar, tem-se que $k = 0, 1, \ldots, N-1$, mas se N é par, tem-se que $k = 0, 1, \ldots, N-2, N$. Ou seja, para N par, $\left(-\sqrt{-1}^{\,(N-1)a}\right)$ não é autovalor de $\mathbf{F}^a$. Isso ocorre porque há $(N/2+1)$ autovetores de simetria par e $(N/2-1)$ autovetores de simetria ímpar. Como $N-1$ é ímpar, $\left(-\sqrt{-1}^{\,(N-1)a}\right)$ deve ser descartado e o último autovalor é $\left(-\sqrt{-1}^{\,(N)a}\right)$. Em [17], Candan verifica que esse fenômeno ocorre para a transformada discreta fracional de Fourier e o justifica pela ausência de autovetores com $N-1$ cruzamentos pelo zero.

CAPÍTULO 4

TRANSFORMADAS BASEADAS EM FUNÇÕES DE MATRIZES

Neste capítulo, é introduzida a teoria de funções de matrizes [78] em corpos finitos, sobre a qual é desenvolvido um novo procedimento para se definir e computar transformadas fracionais em corpos finitos. Todo material deste capítulo é resultado da pesquisa e se apresenta como contribuição da tese.

Com o procedimento de funções de matrizes sobre corpos finitos, são estabelecidas expressões fechadas para se computar potências fracionais de matrizes. A partir das potências fracionais das matrizes de transformação, são definidas a transformada fracional de Fourier em corpos finitos (GFrFT), a transformada fracional de Hartley em corpos finitos (GFrHT), a transformada fracional do cosseno em corpos finitos (GFrCT) e a transformada fracional do seno em corpos finitos (GFrST) [25, 26]. Uma significativa diferença entre a abordagem baseada em funções de matrizes e as abordagens apresentadas no **Capítulo 3**, reside no fato de que não é necessária a construção de um conjunto ortogonal de autovetores.

Dickinson [7] apresentou um método para computar uma potência fracional da matriz de transformação da DFT. O método consiste em escrever uma potência fracional da matriz da DFT como combinação linear de potências inteiras dessa matriz, computando potências fracionais apenas dos coeficientes da combinação. Esse método é uma aplicação da teoria de funções de matrizes [78, 79].

Com essa teoria, aplicar uma função $f(.)$ a uma matriz $\mathbf{A} = [A]_{i,j}$ não significa aplicar isoladamente a função a cada elemento da matriz $f(A_{i,j})$, mas sim usar $\mathbf{A}$ como argumento da função. Em linhas gerais, funções definidas para escalares são reescritas conforme suas expansões em séries de

potência e, sobre essa nova expressão, a função é aplicada a matrizes (tem-se potenciação, multiplicação e adição de matrizes).

Definição 4.1

O polinômio mínimo da matriz $\mathbf{A}$ *é o polinômio mônico* ψ *de menor grau tal que* $\psi(\mathbf{A}) = 0$. □

Definição 4.2

O conjunto $\{\lambda_1, \lambda_2, \ldots, \lambda_s\}$ *de autovalores distintos de* $\mathbf{A}$*, com multiplicidades* $m_1, m_2, \ldots, m_s$*, respectivamente, é denominado espectro de* $\mathbf{A}$ *[79, pp. 150].* □

Se $\mathbf{A}$ é diagonalizável, então o polinômio mínimo ψ, de grau m, de $\mathbf{A}$ é

$$\psi(t) = (t - \lambda_1)^{m_1}(t - \lambda_2)^{m_2}...(t - \lambda_s)^{m_s},$$

em que $m = m_1 + m_2 + \ldots + m_s$ [79, p. 155].

Definição 4.3

Denote por $f^{(j)}$ *a derivada de ordem* j *da função* $f(t)$*. A função* $f(t)$ *é dita ser definida no espectro de* $\mathbf{A}$ *se os valores*

$$f(\lambda_k), f^1(\lambda_k), \ldots, f^{(m_k-1)}(\lambda_k), \quad k = 1, 2, \ldots, s, \tag{4.1}$$

denominados valores de f *no espectro de* $\mathbf{A}$*, existem [78, p. 3].* □

Teorema 4.1

Sejam r_1 *e* r_2 *polinômios e* $\mathbf{A}$ *uma matriz definida em* $\mathrm{GF}(q)$*. Então* $r_1(\mathbf{A}) = r_2(\mathbf{A})$ *se, e somente se,* r_1 *e* r_2 *têm os mesmos valores no espectro de* $\mathbf{A}$ *[78, pp. 5].* □

Assim, considera-se que todas as funções que são definidas e assumem os mesmos valores no espectro de $\mathbf{A}$ devem gerar a mesma matriz que $f(\mathbf{A})$. Generalizando a propriedade do Teorema 4.1, para qualquer $f(t)$ definida no espectro de $\mathbf{A}$ é possível escrever $f(\mathbf{A}) = r(\mathbf{A})$, em que $r(t)$ é um polinômio com os mesmos valores de $f(t)$ no espectro de $\mathbf{A}$ [78, pp. 3].

Definição 4.4

O polinômio $r(t)$ *é denominado polinômio interpolador de Hermite [78, pp. 5] se satisfaz a seguinte condição. Considere* $f(t)$ *uma função definida no espectro de uma matriz* $\mathbf{A}$ *e seja* ψ *o polinômio mínimo de* $\mathbf{A}$*. Então,* $f(\mathbf{A}) = r(\mathbf{A})$*, em que* $r(t)$ *é o polinômio de grau menor que o grau de* ψ *e que satisfaz a condição de interpolação*

$$r^{(j)}(\lambda_k) = f^{(j)}(\lambda_k), \quad j = 0, 1, \ldots, m_k - 1,\ k = 1, 2, \ldots, s. \tag{4.2}$$

□

Definição 4.5

O polinômio de interpolação de Hermite, $r(t)$, é dado explicitamente pela fórmula de Lagrange-Hermite

$$r(t) = \sum_{k=1}^{s} \left[\left(\sum_{j=0}^{m_k - 1} \frac{1}{j!} \varphi_k^{(j)}(\lambda_k)(t - \lambda_k)^j \right) \prod_{j \neq k} (t - \lambda_j)^{m_j} \right], \tag{4.3}$$

em que

$$\varphi_k(t) = \frac{f(t)}{\prod_{j \neq k}(t - \lambda_j)^{m_j}}.$$ □

Se $\mathbf{A}$ é uma matriz diagonalizável com autovalores distintos ($m_k = 1$, para $k = 1, \ldots, s$), o polinômio r corresponde ao polinômio de interpolação de Lagrange [78, pp. 6],

$$r(t) = \sum_{k=1}^{s} f(\lambda_k) l_k(t), \tag{4.4}$$

em que

$$l_k(t) = \prod_{\substack{j=1 \\ j \neq k}}^{s} \frac{t - \lambda_j}{\lambda_k - \lambda_j}. \tag{4.5}$$

O ponto chave do procedimento é computar uma potência fracional de uma matriz $\mathbf{A}$ usando o polinômio de interpolação de Lagrange, empregando a Definição 4.4. Nesse sentido, define-se $r(t) = t^a = t^{\frac{a_1}{a_2}}$, em que $a = a_1/a_2$, $a_2 \neq 0$, é uma razão entre dois inteiros. Isto é feito substituindo a variável t por uma matriz $\mathbf{A}$ no polinômio r.

4.1 GFrFT baseada em funções de matrizes

A transformada fracional de Fourier em corpos finitos de um vetor $\mathbf{x}$ de comprimento N é computada por meio de $\mathbf{X}_a = \mathbf{F}^a\mathbf{x}$. De acordo com a Proposição 2.1, existem quatro autovalores distintos para $\mathbf{F}$, $\lambda = \{\pm 1, \pm\sqrt{-1}\}$. Para este caso, as funções $l_k(t)$ definidas na Equação (4.5) são

$$\begin{aligned} l_1(t) &= \frac{t^3+t^2+t+1}{4}, \\ l_2(t) &= \frac{-t^3+t^2-t+1}{4}, \\ l_3(t) &= \frac{\sqrt{-1}\,t^3-t^2-\sqrt{-1}\,t+1}{4}, \\ l_4(t) &= \frac{-\sqrt{-1}\,t^3-t^2+\sqrt{-1}\,t+1}{4}. \end{aligned} \tag{4.6}$$

Da Equação (4.4), $r(t) = l_1(t) + (-1)^{\,a} l_2(t) + (\sqrt{-1})^{\,a} l_3(t) + (-\sqrt{-1})^{a} l_4(t)$. Agrupando os coeficientes das potências de t e considerando $\alpha_i(a) := \alpha_i(a_1, a_2) \in \mathrm{GI}(p)$ como o coeficiente da i-ésima potência de t, tem-se

$$r(t) = \sum_{i=0}^{3} \alpha_i(a_1, a_2) t^i,$$

em que

$$\begin{aligned}
\alpha_0(a_1,a_2) &= \frac{1 + (\sqrt[2a_2]{-1})^{a_1} + (-1)^{a} + (-\sqrt[2a_2]{-1})^{a_1}}{4} \\
&= \frac{1}{4}\left[(\sqrt[2a_2]{-1})^{a_1}\left(1 + (\sqrt[2a_2]{-1})^{a_1}\right) + (\sqrt[2a_2]{-1})^{-a_1}\left(1 + (\sqrt[2a_2]{-1})^{a_1}\right)\right] \\
&= \frac{1 + (\sqrt[2a_2]{-1})^{a_1}}{2} \cos_{\sqrt[2a_2]{-1}}(a_1), \\
\alpha_1(a_1,a_2) &= \frac{1 - \sqrt{-1}(\sqrt[2a_2]{-1})^{a_1}}{2} \sin_{\sqrt[2a_2]{-1}}(a_1), \\
\alpha_2(a_1,a_2) &= \frac{-1 + (\sqrt[2a_2]{-1})^{a_1}}{2} \cos_{\sqrt[2a_2]{-1}}(a_1), \\
\alpha_3(a_1,a_2) &= \frac{-1 - \sqrt{-1}(\sqrt[2a_2]{-1})^{a_1}}{2} \sin_{\sqrt[2a_2]{-1}}(a_1).
\end{aligned} \tag{4.7}$$

Finalmente, a matriz de transformação da GFrFT com parâmetro fracional $a = (a_1/a_2)$ é

$$\mathbf{F}^a = \mathbf{F}^{\frac{a_1}{a_2}} = r(\mathbf{F}) = \sum_{i=0}^{3} \alpha_i(a_1, a_2)\mathbf{F}^i. \tag{4.8}$$

A GFrFT inversa com parâmetro fracional $a = (a_1/a_2)$ é a GFrFT com parâmetro fracional $a' = (4 - (a_1/a_2))$. A matriz de transformação da GFrFT inversa, $\mathbf{F}^{a'}$, é tal que

$$\mathbf{F}^{a'} = \sum_{i=0}^{3} \alpha_i(4 - a)\mathbf{F}^i. \tag{4.9}$$

Uma vez que $\cos_\zeta(a) = \cos_\zeta(a')$, $\sin_\zeta(a) = -\sin_\zeta(a')$ e $\left(\sqrt{-1}\right)^{a'} = \left(-\sqrt{-1}\right)^{a}$, as expressões de $\alpha_i(a')$, $i = 0, \ldots, 3$, são

$$\begin{aligned}
\alpha_0(-a) &= \frac{1 + \left(\sqrt[a_2]{-\sqrt{-1}}\right)^{a_1}}{2} \cos_{\sqrt[2a_2]{-1}}(a_1), \\
\alpha_1(-a) &= \frac{-1 + \sqrt{-1}\left(\sqrt[a_2]{-\sqrt{-1}}\right)^{a_1}}{2} \sin_{\sqrt[2a_2]{-1}}(a_1), \\
\alpha_2(-a) &= \frac{-1 + \left(\sqrt[a_2]{-\sqrt{-1}}\right)^{a_1}}{2} \cos_{\sqrt[2a_2]{-1}}(a_1), \\
\alpha_3(-a) &= \frac{1 + \sqrt{-1}\left(\sqrt[a_2]{-\sqrt{-1}}\right)^{a_1}}{2} \sin_{\sqrt[2a_2]{-1}}(a_1).
\end{aligned} \tag{4.10}$$

O mesmo procedimento pode ser aplicado na construção da matriz de transformação da GFrFT generalizada. Como a matriz $\mathbf{F_G}$ tem os mesmos autovalores que $\mathbf{F}$, o polinômio interpolador é o mesmo. Dessa maneira,

$$\mathbf{F}_{\mathbf{G}}^{a} = \sum_{i=0}^{3} \alpha_i(a_1, a_2)\mathbf{F}_{\mathbf{G}}^{i}. \tag{4.11}$$

Nota 4. 1 Baseado neste procedimento, potências fracionais das matrizes são obtidas sem a necessidade de construção de conjuntos ortogonais de autovetores.

Nota 4. 2 Para definir a GFrFT e a GFrFT generalizada, é necessário que $\sqrt[2a_2]{-1} \in \mathrm{GI}(p)$.

Exemplo 4.1 – Construção da GFrFT de comprimento 8 em GF(257).

Considere o elemento $\zeta = 4 \in \mathrm{GI}(257)$*, com ordem multiplicativa* $\mathrm{ord}(4) = 8$*. A matriz da FFFT de comprimento* 8 *com* $\zeta = 4$ *é dada por* $[F]_{i,k} = \sqrt{8^{-1}}4^{ki}$*, conforme Exemplo 2.1, e* $\mathbf{F}^{3/8}$ *é a matriz da GFrFT de parâmetro* $a = 3/8$*. Para escrever* $\mathbf{F}^{3/8}$ *de acordo com a Equação (4.8), é necessário computar os valores de* $\alpha_i(3, 8)$ *em* $\mathrm{GI}(257)$*. Portanto, tem-se que*

$$\sqrt{-1}^{\frac{3}{8}} \equiv \sqrt[16]{256}^{3} \equiv 60^3 \equiv 120 \pmod{257},$$
$$\cos_{\sqrt{-1}}(3/8) = \cos_{60}(3) = \tfrac{1}{2}(60^3 + 60^{-3}) = 129(120 + 36) \equiv 196 \pmod{257},$$
$$\sin_{\sqrt{-1}}(3/8) = \sin_{60}(3) = \tfrac{1}{2\sqrt{-1}}(60^3 - 60^{-3}) = 249(120 - 36) \equiv 188 \pmod{257},$$

e os coeficientes da combinação são

$$\begin{aligned}
\alpha_0(3,8) &= \tfrac{1+120}{2}(196) &&\equiv 221 \pmod{257},\\
\alpha_1(3,8) &= \tfrac{1-16(120)}{2}(188) &&\equiv 229 \pmod{257},\\
\alpha_2(3,8) &= \tfrac{-1+120}{2}(196) &&\equiv 120 \pmod{257},\\
\alpha_3(3,8) &= \tfrac{-1-16(120)}{2}(188) &&\equiv 120 \pmod{257}.
\end{aligned}$$

Dessa forma, $\mathbf{F}^{\frac{3}{8}} = 221\mathbf{F}^0 + 229\mathbf{F}^1 + 120\mathbf{F}^2 + 120\mathbf{F}^3$*,*

$$\mathbf{F}^{\frac{3}{8}} = \begin{bmatrix}
200 & 76 & 76 & 76 & 76 & 76 & 76 & 76\\
76 & 16 & 145 & 243 & 181 & 205 & 112 & 174\\
76 & 145 & 145 & 112 & 76 & 145 & 84 & 112\\
76 & 243 & 112 & 16 & 181 & 174 & 145 & 205\\
76 & 181 & 76 & 181 & 200 & 181 & 76 & 181\\
76 & 205 & 145 & 174 & 181 & 16 & 112 & 243\\
76 & 112 & 84 & 145 & 76 & 112 & 145 & 145\\
76 & 174 & 145 & 205 & 181 & 243 & 145 & 16
\end{bmatrix}.$$

A matriz da transformada fracional de Fourier em corpos finitos é obtida a partir da combinação linear de potências inteiras de $\mathbf{F}$*, e neste caso tem elementos em* $\mathrm{GF}(257)$. □

4.2 GFrHT, GFrCT e GFrST baseadas em funções de matrizes

Para se obter as matrizes de transformação das transformadas fracionais de Hartley (GFrHT), do cosseno (GFrCT) tipos 1 e 4, e do seno (GFrST) tipos 1 e 4 em corpos finitos, é necessário computar $\mathbf{H}^a$, $\mathbf{C}_1^a$, $\mathbf{C}_4^a$, $\mathbf{S}_1^a$ e $\mathbf{S}_4^a$, respectivamente.

De acordo com as Proposições 2.3 e 2.5, essas matrizes têm dois autovalores distintos $\lambda = \{\pm 1\}$. Para esses casos, as funções $l_k(t)$ definidas na Equação (4.5) são

$$l_1(t) = \frac{1+t}{2} \quad \text{e} \quad l_2(t) = \frac{1-t}{2}.$$

Da Equação (4.4),

$$r(t) = \left(\frac{1+t}{2}\right) + (-1)^a \left(\frac{1-t}{2}\right). \tag{4.12}$$

Agrupando os coeficientes das potências de t, tem-se

$$r(t) = \frac{1+(-1)^a}{2} + \frac{1-(-1)^a}{2} t. \tag{4.13}$$

Finalmente, para um parâmetro fracional $a = (a_1/a_2)$, a matriz de transformação $\mathbf{M}^a$ é

$$\mathbf{M}^a = \frac{1}{2}(\mathbf{I} + \mathbf{M}) + \frac{(\sqrt[a_2]{-1})^{a_1}}{2}(\mathbf{I} - \mathbf{M}). \tag{4.14}$$

Deve-se substituir $\mathbf{M}$ por cada matriz de transformação a fim de se obter a correspondente transformada fracional.

O mesmo procedimento pode ser aplicado na construção da matriz de transformação da GFrHT generalizada. Como a matriz $\mathbf{H_G}$ tem os mesmos autovalores que $\mathbf{H}$, o polinômio interpolador é o mesmo. Dessa maneira,

$$\mathbf{H}_\mathbf{G}^a = \frac{1}{2}(\mathbf{I} + \mathbf{H_G}) + \frac{(\sqrt[a_2]{-1})^{a_1}}{2}(\mathbf{I} - \mathbf{H_G}). \tag{4.15}$$

Nota 4. 3 Para a definição das transformadas introduzidas nesta seção, é necessário apenas que $\sqrt[a]{-1} \in \mathrm{GI}(p)$.

Exemplo 4.2 – Construção da GFrHT de comprimento 8 em GF(257)

Considere o elemento $\zeta = 4 \in \mathrm{GI}(257)$*, com ordem multiplicativa* $\mathrm{ord}(4) = 8$*. A matriz da FFHT de dimensão* 8×8 *com* $\zeta = 4$ *é dada por* $[H]_{i,k} = \sqrt{8^{-1}}\mathrm{cas}_4(ki)$*, conforme Exemplo 2.3, e* $\mathbf{H}^{3/8}$ *é a matriz da GFrHT de parâmetro* $a = 3/8$*. Para escrever* $\mathbf{H}^{3/8}$ *de acordo com a Equação (4.14) é necessário computar os valores*

$$\frac{1+(-1)^{\frac{3}{8}}}{2} \equiv \frac{1+8}{2} \equiv 133 \pmod{257}$$
$$\frac{1-(-1)^{\frac{3}{8}}}{2} \equiv \frac{1-8}{2} \equiv 125 \pmod{257}$$

Dessa forma, $\mathbf{H}^{\frac{3}{8}} = 133\mathbf{H}^0 + 125\mathbf{H}^1$,

$$\mathbf{H}^{\frac{3}{8}} = \begin{bmatrix} 1 & 125 & 125 & 125 & 125 & 125 & 125 & 125 \\ 125 & 238+118j & 56j & 152+119j & 132 & 152+138j & 201j & 105+138j \\ 125 & 56j & 8 & 201j & 125 & 56j & 132 & 201j \\ 125 & 152+119j & 201j & 238+119j & 132 & 105+138j & 56j & 152+138j \\ 125 & 132 & 125 & 132 & 1 & 132 & 125 & 132 \\ 125 & 152+138j & 56j & 105+138j & 132 & 238+119j & 201j & 152+119j \\ 125 & 201j & 132 & 56j & 125 & 201j & 8 & 56j \\ 125 & 105+138j & 201j & 152+138j & 132 & 152+119j & 56j & 238+119j \end{bmatrix}.$$

□

Exemplo 4.3

Construção da GFrCT de comprimento 8 em GF(*257****).*** *Para construir a matriz da GFrCT de dimensão* 8×8 *é necessário tomar um elemento de ordem multiplicativa* 16 *em* $\mathrm{GI}(257)$*. Por exemplo,* $\zeta = 2$ *tem ordem multiplicativa* 16 *em* $\mathrm{GI}(257)$*. A matriz da FFCT-4 é construída com a Equação (2.14),*

$$\boldsymbol{C}_4 = \begin{bmatrix} 29 & 11 & 190 & 127 & 189 & 178 & 154 & 61 \\ 11 & 189 & 61 & 79 & 67 & 228 & 130 & 103 \\ 190 & 61 & 130 & 246 & 103 & 189 & 29 & 178 \\ 127 & 79 & 246 & 61 & 29 & 154 & 67 & 68 \\ 189 & 67 & 103 & 29 & 196 & 246 & 178 & 127 \\ 178 & 228 & 189 & 154 & 246 & 127 & 61 & 67 \\ 154 & 130 & 29 & 67 & 178 & 61 & 68 & 11 \\ 61 & 103 & 178 & 68 & 127 & 67 & 11 & 228 \end{bmatrix}. \tag{4.16}$$

A transformada do cosseno tipo 4 *tem o mesmo polinômio de interpolação que a transformada de Hartley. Para uma potência racional* $a = 3/8$, $\mathbf{C}_4^{\frac{3}{8}} = 133\mathbf{C}_4^0 + 125\mathbf{C}_4^1$,

$$\mathbf{C}_4^{\frac{3}{8}} = \begin{bmatrix} 160 & 90 & 106 & 198 & 238 & 148 & 232 & 172 \\ 90 & 114 & 172 & 109 & 151 & 230 & 59 & 25 \\ 106 & 172 & 192 & 167 & 25 & 238 & 27 & 148 \\ 198 & 109 & 167 & 48 & 27 & 232 & 151 & 19 \\ 238 & 151 & 25 & 27 & 218 & 167 & 148 & 198 \\ 148 & 230 & 238 & 232 & 167 & 74 & 172 & 151 \\ 232 & 59 & 27 & 151 & 148 & 172 & 152 & 90 \\ 172 & 25 & 148 & 19 & 198 & 151 & 90 & 106 \end{bmatrix}. \qquad \square$$

4.3 Propriedades

Com o objetivo de manipular e avaliar as transformadas fracionais, é importante investigar suas propriedades. A seguir, são apresentadas algumas propriedades da GFrFT. É apresentada também a relação entre a GFrFT e a GFrHT.

4.3.1 Linearidade

Considere dois vetores $\mathbf{x}$ e $\mathbf{y}$ com componentes em $\mathrm{GF}\,(p)$, cujas GFrFT são os vetores $\mathbf{X}^a = \mathbf{F}^a\mathbf{x}$ e $\mathbf{Y}_a = \mathbf{F}^a\mathbf{y}$ com componentes em $\mathrm{GI}\,(p)$, respectivamente. A GFrFT da combinação de $\mathbf{x}$ e $\mathbf{y}$,

$$\mathbf{z} = k_1\mathbf{x} + k_2\mathbf{y},$$

em que $k_1, k_2 \in$ GI (p), é

$$\mathbf{Z}^a = \mathbf{F}^a\mathbf{z} = k_1\mathbf{X}^a + k_2\mathbf{Y}^a.$$

A demonstração desta propriedade é análoga à demonstração da propriedade de linearidade para a FFFT e para a DFT, uma vez que a GFrFT de um vetor é dada como uma combinação linear da FFFT do próprio vetor.

4.3.2 Deslocamento no tempo

Se $\hat{\mathbf{x}} = (x[i - i_0])$, para i_0 um número inteiro, então a GFrFT de $\hat{\mathbf{x}}$ é o vetor $\hat{\mathbf{X}}^a$, cuja k-ésima componente é $\hat{X}^a[k] = \zeta^{ki_0}X^a[k]$.

Demonstração:

Se $\mathbf{X}$ é a FFFT do vetor $\mathbf{x}$, pela propriedade de deslocamento no tempo para a FFFT, $\hat{\mathbf{X}} = \zeta^{i_0}\mathbf{X}$.

A k-ésima componente de $\hat{\mathbf{X}}^a$ é dada por

$$\begin{aligned}
\hat{X}^a[k] &= \left(\alpha_0(a)\mathbf{I} + \alpha_1(a)\mathbf{F} + \alpha_2(a)\mathbf{F}^2 + \alpha_3(a)\mathbf{F}^3\right) x[i - i_0] \\
&= \alpha_0(a)\mathbf{F}^4x[i - i_0] + \alpha_1(a)\mathbf{F}x[i - i_0] \\
&\quad +\alpha_2(a)\mathbf{F}^2x[i - i_0] + \alpha_3(a)\mathbf{F}^3x[i - i_0] \\
&= \zeta^{ki_0}\left(\alpha_0(a)\mathbf{F}^3 + \alpha_1(a)\mathbf{I} + \alpha_2(a)\mathbf{F} + \alpha_3(a)\mathbf{F}^2\right) X[k] \\
&= \zeta^{ki_0}\mathbf{F}\mathbf{F}^{-1}\left(\alpha_0(a)\mathbf{F}^3 + \alpha_1(a)\mathbf{I} + \alpha_2(a)\mathbf{F} + \alpha_3(a)\mathbf{F}^2\right) X[k] \\
&= \zeta^{ki_0}\left(\alpha_0(a)\mathbf{F}^4 + \alpha_1(a)\mathbf{F} + \alpha_2(a)\mathbf{F}^2 + \alpha_3(a)\mathbf{F}^3\right)\mathbf{F}^{-1}X[k] \\
&= \zeta^{ki_0}\mathbf{F}^a x[i] = \zeta^{ki_0}X^a[k]. \qquad (4.17)
\end{aligned}$$

4.3.3 Reversão no tempo

Considere o vetor $\mathbf{x}$ com componentes em GI(p) e o vetor $\hat{\mathbf{x}} = (x[-i \pmod N])$, isto é, $\hat{\mathbf{x}}$ é $\mathbf{x}$ revertido no tempo. Se $\mathbf{X}^a$ é a GFrFT de $\mathbf{x}$, então a GFrFT de $\hat{\mathbf{x}}$ é o vetor $\hat{\mathbf{X}}^a$, em que $\hat{\mathbf{X}}^a = \mathbf{F}^2\mathbf{X}^a$. Assim, a reversão de um vetor no domínio do tempo implica na reversão do vetor transformado no domínio da transformada fracional.

Demonstração:

Se $\mathbf{x}$ é revertido no tempo, então vale $\hat{\mathbf{x}} = \mathbf{F}^2x$. Assim, o vetor $\hat{\mathbf{X}}^a$ é dado por

$$\begin{aligned}
\hat{\mathbf{X}}^a &= \left(\alpha_0(a)\mathbf{I} + \alpha_1(a)\mathbf{F} + \alpha_2(a)\mathbf{F}^2 + \alpha_3(a)\mathbf{F}^3\right)\mathbf{F}^2\mathbf{x} \\
&= \mathbf{F}^2\left(\alpha_0(a)\mathbf{I} + \alpha_1(a)\mathbf{F} + \alpha_2(a)\mathbf{F}^2 + \alpha_3(a)\mathbf{F}^3\right)\mathbf{x} = \mathbf{F}^2\mathbf{X}^a. \qquad (4.18)
\end{aligned}$$

4.3.4 Relação entre a GFrHT e a GFrFT - A matriz D

A partir da matriz de transformação da FFHT pode-se obter a matriz de transformação da FFFT e vice-versa. A relação entre as matrizes da GFrFT, $\mathbf{F}^a$, e da GFrHT, $\mathbf{H}^a$, é uma generalização da relação entre as matrizes da FFFT, $\mathbf{F}$, e da FFHT, $\mathbf{H}$, dada por

$$\mathbf{F} = \frac{1}{2}(\mathbf{I}+\mathbf{P})\mathbf{H} + \frac{\sqrt{-1}}{2}(\mathbf{I}-\mathbf{P})\mathbf{H}, \tag{4.19}$$

ou

$$\mathbf{H} = \left(\frac{1}{2}(1-\sqrt{-1})\mathbf{I} + \frac{1}{2}(1+\sqrt{-1})\mathbf{P}\right)\mathbf{F}, \tag{4.20}$$

em que $\mathbf{P} = \mathbf{F}^2$, a matriz de Schur [63].

A Equação (4.20) pode ser reescrita como $\mathbf{H} = \mathbf{DF}$ e $\mathbf{F} = \mathbf{D}^{-1}\mathbf{H}$, em que a matriz $\mathbf{D}$ é definida como $\mathbf{D} := \frac{1}{2}(1-\sqrt{-1})\mathbf{I} + \frac{1}{2}(1+\sqrt{-1})\mathbf{P}$. Para determinar a relação entre a GFrFT e a GFrHT a partir da Equação (4.20), deve-se fazer $\mathbf{H}^a = (\mathbf{DF})^a$.

Teorema 4.2

As matrizes $\mathbf{D}$ *e* $\mathbf{F}$ *comutam.*

Demonstração:

Como $\mathbf{F}^2 = \mathbf{P}$, tem-se que

$$\begin{aligned}
\mathbf{DF} &= \left(\frac{(1-\sqrt{-1})}{2}\mathbf{I} + \frac{(1+\sqrt{-1})}{2}\mathbf{F}^2\right)\mathbf{F} \\
&= \left(\frac{(1-\sqrt{-1})}{2}\mathbf{F} + \frac{(1+\sqrt{-1})}{2}\mathbf{F}^3\right) \\
&= \mathbf{F}\left(\frac{(1-\sqrt{-1})}{2}\mathbf{I} + \frac{(1+\sqrt{-1})}{2}\mathbf{F}^2\right) = \mathbf{FD}.
\end{aligned}$$

Sendo $\mathbf{H}^a = \mathbf{D}^a\mathbf{F}^a$, é necessário computar uma potência fracional de $\mathbf{D}$ para se encontrar a relação. Conhecendo a autoestrutura de $\mathbf{D}$, é possível utilizar o procedimento baseado na interpolação de Lagrange para encontrar uma expressão fechada de $\mathbf{D}^a$. A Tabela 4.1 mostra a multiplicidade dos autovalores da matriz $\mathbf{D}$ segundo suas dimensões, conforme obtido no Apêndice C.

Como a matriz $\mathbf{D}$ tem dois autovalores distintos, utilizando a Definição 4.4, tem-se que as funções $l_k(t)$ são

$$\begin{aligned}
l_1(t) &= \frac{t+\sqrt{-1}}{1+\sqrt{-1}} = \frac{1-\sqrt{-1}}{2}\left(\sqrt{-1}+t\right), \\
l_2(t) &= \frac{t-1}{-\sqrt{-1}-1} = \frac{1-\sqrt{-1}}{2}\left(1-t\right),
\end{aligned} \tag{4.21}$$

Tabela 4.1: *Multiplicidade dos autovalores da matriz* $\mathbf{D}$.

$\mathbf{N}$	Multiplicidade dos Autovalores de $\mathbf{D}$			
	$\lambda = 1$	$\lambda = -1$	$\lambda = \sqrt{-1}$	$\lambda = -\sqrt{-1}$
$2k$	$k+1$	0	0	$k-1$
$2k+1$	$k+1$	0	0	k

Fonte: Próprio Autor.

enquanto o polinômio de interpolação $r(t)$ é dado por

$$r(t) \;=\; (1)^a \frac{1-\sqrt{-1}}{2}\left(\sqrt{-1}+t\right) + (-\sqrt{-1})^a \frac{1-\sqrt{-1}}{2}\left(1-t\right).$$

Substituindo a variável t por $\mathbf{D}$ e fazendo $\mathbf{D} = \frac{1-\sqrt{-1}}{2}\mathbf{I} + \frac{1+\sqrt{-1}}{2}\mathbf{F}^2$, tem-se

$$r(\mathbf{D}) \;=\; \frac{1-\sqrt{-1}}{2}\left(\sqrt{-1}\mathbf{I}+\mathbf{D}\right) + (-\sqrt{-1})^a \frac{1-\sqrt{-1}}{2}\left(\mathbf{I}-\mathbf{D}\right),$$

e a expressão para se computar uma potência fracional da matriz $\mathbf{D}$ é

$$\mathbf{D}^a = \frac{1}{2}(\mathbf{I}+\mathbf{P}) + \frac{(-\sqrt{-1})^a}{2}(\mathbf{I}-\mathbf{P}). \tag{4.22}$$

Finalmente, a relação entre as matrizes da GFrHT e da GFrFT é dada por

$$\mathbf{H}^a = \frac{1}{2}(\mathbf{I}+\mathbf{P})\mathbf{F}^a + \frac{(-\sqrt{-1})^a}{2}(\mathbf{I}-\mathbf{P})\mathbf{F}^a. \tag{4.23}$$

Analogamente, obtém-se a matriz da GFrFT a partir da matriz da GFrHT por meio de

$$\mathbf{F}^a = \frac{1}{2}(\mathbf{I}+\mathbf{P})\mathbf{H}^a + \frac{(\sqrt{-1})^a}{2}(\mathbf{I}-\mathbf{P})\mathbf{H}^a. \tag{4.24}$$

4.3.5 Autoestrutura da GFrFT baseada em funções de matrizes

Pela Equação (3.1), vê-se que $\mathbf{F}$ é diagonalizável. Da relação $\mathbf{P} = \mathbf{F}^2$, tem-se que

$$\mathbf{P} = (\mathbf{V}\mathbf{\Lambda}\mathbf{V}^{-1})(\mathbf{V}\mathbf{\Lambda}\mathbf{V}^{-1}) = \mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^{-1},$$

ou seja, $\mathbf{P}$ é diagonalizável. Os autovetores associados aos autovalores de $\mathbf{F}$, $\lambda = \pm 1$, são associados ao autovalor $\lambda = 1$ de $\mathbf{P}$, enquanto que os autovetores associados aos autovalores de $\mathbf{F}$, $\lambda = \pm\sqrt{-1}$, são associados ao autovalor $\lambda = -1$ de $\mathbf{P}$.

De maneira similar, $\mathbf{F}^3$ também é diagonalizável, de forma que

$$\mathbf{F}^3 = \mathbf{V}\mathbf{\Lambda}^3\mathbf{V}^{-1}.$$

Os autovetores associados aos autovalores de $\mathbf{F}$, $\lambda = \pm\sqrt{-1}$, são associados ao autovalor $\lambda' = \lambda^3$ de $\mathbf{F}^3$.

Combinando as equações (3.1) e (4.8), tem-se que

$$\begin{aligned}\mathbf{F}^a &= \alpha_0(a)\mathbf{V}\mathbf{I}\mathbf{V}^{-1} + \alpha_1(a)\mathbf{V}\mathbf{\Lambda}\mathbf{V}^{-1} + \alpha_2(a)\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^{-1} + \alpha_3(a)\mathbf{V}\mathbf{\Lambda}^3\mathbf{V}^{-1} \\ &= \mathbf{V}\left(\alpha_0(a)\mathbf{I} + \alpha_1(a)\mathbf{\Lambda} + \alpha_2(a)\mathbf{\Lambda}^2 + \alpha_3(a)\mathbf{\Lambda}^3\right)\mathbf{V}^{-1} \\ &= \mathbf{V}\mathbf{\Lambda}'\mathbf{V}^{-1}.\end{aligned}$$

Como $\mathbf{\Lambda}'$ é uma matriz diagonal, $\mathbf{F}^a$ é diagonalizável. Se $\mathbf{F}^a$ tem dimensão $N \times N$, então são admitidos no máximo N autovalores distintos. Adicionalmente, os autovetores de $\mathbf{F}$ são autovetores de $\mathbf{F}^a$.

Considere que λ_k, $k = 0, 1, \ldots, N-1$, seja o k-ésimo autovalor de $\mathbf{F}$ (o k-ésimo elemento da diagonal de $\mathbf{\Lambda}$). O k-ésimo autovalor de $\mathbf{F}^a$, λ'_k, é tal que

$$\lambda'_k = \alpha_0(a) + \alpha_1(a)\lambda_k + \alpha_2(a)(\lambda_k)^2 + \alpha_3(a)(\lambda_k)^3. \tag{4.25}$$

Se $\mathbf{v}$ é um autovetor associado ao autovalor $\lambda = 1$ de $\mathbf{F}$, então $\mathbf{v}$ é um autovetor associado ao autovalor

$$\lambda' = \alpha_0(a) + \alpha_1(a) + \alpha_2(a) + \alpha_3(a) = 1$$

de $\mathbf{F}^a$.

Se $\mathbf{v}$ é um autovetor associado ao autovalor $\lambda = -1$ de $\mathbf{F}$, então $\mathbf{v}$ é um autovetor associado ao autovalor

$$\lambda' = \alpha_0(a) - \alpha_1(a) + \alpha_2(a) - \alpha_3(a) = (-1)^a$$

de $\mathbf{F}^a$.

Se $\mathbf{v}$ é um autovetor associado ao autovalor $\lambda = \sqrt{-1}$ de $\mathbf{F}$, então $\mathbf{v}$ é um autovetor associado ao autovalor

$$\begin{aligned}\lambda' &= \alpha_0(a) - \alpha_2(a) + \sqrt{-1}(\alpha_1(a) - \alpha_3(a)) \\ &= \frac{\sqrt{-1}^a + \sqrt{-1}^{-a}}{2} + \frac{\sqrt{-1}}{\sqrt{-1}}\frac{\sqrt{-1}^a + \sqrt{-1}^{-a}}{2} = (\sqrt{-1})^a\end{aligned}$$

de $\mathbf{F}^a$.

Se $\mathbf{v}$ é um autovetor associado ao autovalor $\lambda = -\sqrt{-1}$ de $\mathbf{F}$, então $\mathbf{v}$ é um autovetor associado ao autovalor

$$\begin{aligned}\lambda' &= \alpha_0(a) - \alpha_2(a) - \sqrt{-1}(\alpha_1(a) - \alpha_3(a)) \\ &= \frac{\sqrt{-1}^a + \sqrt{-1}^{-a}}{2} - \frac{\sqrt{-1}}{\sqrt{-1}}\frac{\sqrt{-1}^a + \sqrt{-1}^{-a}}{2} = (\sqrt{-1})^{-a} = (-\sqrt{-1})^a\end{aligned}$$

de $\mathbf{F}^a$. Conclui-se que λ em $\mathbf{F}$ associa λ^a em $\mathbf{F}^a$.

4.4 Algoritmos rápidos para as transformadas fracionais em corpos finitos

O uso das transformadas discretas em diversas áreas da Engenharia tornou-se mais frequente devido à existência de algoritmos rápidos, isto é, algoritmos que reduzem a complexidade aritmética (número de adições e multiplicações) para computar as transformadas [44, 80–83]. A importância desses algoritmos fica evidente quando se trabalha com vetores de grande comprimento. Para o cálculo da FFFT de um vetor de comprimento N usando a Definição 2.4, são necessárias N^2 multiplicações e $N(N-1)$ adições, o que pode limitar certas aplicações em virtude do alto custo computacional [84]. Por exemplo, se $N = 1024$, são necessárias $1.048.576$ multiplicações e $1.047.552$ adições.

Verificou-se que é possível computar uma DFT unidimensional, cujo comprimento é um número composto, por meio de uma DFT bidimensional. Algoritmos que se baseiam nesta abordagem requerem menor complexidade aritmética, em relação à abordagem associada à Definição 2.4, sendo exemplos de transformadas rápidas de Fourier (FFT, do inglês *fast Fourier transform*) [44, p. 68].

Diversos trabalhos foram apresentados visando a redução da complexidade aritmética para se computar transformadas discretas. Heideman [85, 86] apresentou uma fórmula para determinar o número mínimo de multiplicações necessárias para computar a DFT, que se constituiu em limite teórico para a redução. Em se tratando de transformadas discretas, existem diferentes algoritmos que se propõem a reduzir a complexidade aritmética até os limites teóricos [44, 87], dentre os quais se destacam os algoritmos de:

- **Cooley-Tukey**, cuja ideia é converter uma transformada unidimensional em uma transformada bidimensional [84];

- **Good-Thomas**, também chamado de algoritmo do fator primo (PFA, do inglês *prime factor algorithm*), é baseado na fatoração do comprimento do vetor em fatores primos e no uso do teorema chinês do resto [88–90];

- **Rader**, é usado quando o comprimento do vetor é uma potência de um número primo [38] e requer apenas operações de indexação e convoluções cíclicas. Em algumas propostas, utiliza-se o algoritmo de Winograd para realizar as convoluções [91, 92].

Há outros algoritmos para calcular de maneira otimizada as transformadas discretas como as propostas apresentadas em [93–95].

A Tabela 4.2 apresenta o número de adições e multiplicações requeridas no cálculo de uma FFFT com os algoritmos de Cooley-Tukey, de Cooley-Tukey base dois e de Good-Thomas. Considere que $M(N)$ e $A(N)$ representam o número de multiplicações e adições, respectivamente, requeridas para computar uma FFFT de comprimento N. O algoritmo de Cooley-Tukey (CT), em geral, é aplicado quando N é o produto de dois números compostos N_1 e N_2. No caso particular em que N é uma potência de dois, $N = 2^m$, o algoritmo é conhecido como Cooley-Tukey de base dois (CT-2). O algoritmo de Good-Thomas (GT), em geral, é aplicado quando N é o produto de duas potências de números primos $p_1^{m_1}$ e $p_2^{m_2}$. Nesse algoritmo, pode-se reduzir ainda mais a complexidade aritmética utilizando o produto de Kronecker para o cálculo da transformada bidimensional [44, pp. 40] .

O algoritmo de Rader é aplicado quando N é um número primo. Na verdade, Rader propôs se utilizar de uma convolução cíclica de comprimento $N - 1$ para computar a DFT. Para tanto, pode-se computar a convolução em corpos finitos através da transformada numérica de Mersenne ou utilizando algoritmos específicos para convolução. Dessa forma, não há uma expressão fechada para a complexidade aritmética para esse tipo de FFT.

Tabela 4.2: *Complexidade multiplicativa e aditiva dos algoritmos rápidos para cálculo da FFFT de comprimento N, segundo o algoritmo de Cooley-Tukey (CT), Cooley-Tukey base dois (CT-2) e Good-Thomas (GT).*

Algoritmo	N	$M(N)$	$A(N)$
CT	N_1N_2	$N_1M(N_2) + N_2M(N_1) + N$	$N_1M(N_2) + N_2M(N_1)$
CT-2	2^m	$Nm/2$	Nm
GT	N_1N_2 com MDC$(N_1, N_2) = 1$	$p_1M(p_2) + p_2M(p_1)$	$p_1M(p_2) + p_2M(p_1)$

Fonte: Próprio Autor.

A complexidade aritmética associada às transformadas fracionais baseadas em funções de matrizes é um pouco superior à complexidade associada às transformadas usuais (ordinárias). Analisando a Equação (4.8), para se obter a matriz de transformação da GFrFT são empregadas as matrizes $\mathbf{I}$ (matriz identidade), $\mathbf{P}$ (matriz de reversão circular, conforme Equação (2.20)), $\mathbf{F}$ (matriz da FFFT) e $\mathbf{PF}$ (matriz da FFFT com colunas permutadas).

Na combinação de matrizes da Equação (4.8), há $4N$ multiplicações referentes aos coeficientes da combinação e $3N$ adições referentes à adição das matrizes. Desconsiderando o custo computacional associado às permutações de colunas, a maior parcela da complexidade aritmética está na multiplicação de um vetor pela matriz $\mathbf{F}$.

Considerando que $M(N)$ e $A(N)$ denotam o número de multiplicações e adições em $\mathrm{GI}(p)$,

respectivamente, requeridas para calcular a FFFT de comprimento N, e $M'(N)$ e $A'(N)$ denotam o número de multiplicações e adições, respectivamente, requeridas para calcular a GFrFT, tem-se que $M'(N) = M(N) + 4N$ e $A'(N) = A(N) + 3N$.

O mesmo pode ser observado para as matrizes de transformação obtidas pela Equação (4.14). O número de multiplicações e adições, respectivamente, requeridas para calcular as transformadas fracionais obtidas pela Equação (4.14) é $M'(N) = M(N) + 2N$ e $A'(N) = A(N) + N$, em que $M(N)$ e $A(N)$ é o número de multiplicações e adições, respectivamente, associados a cada transformada usual.

Em comparação com as transformadas usuais, o aumento da complexidade aritmética é linear. Em razão disso, algoritmos rápidos desenvolvidos para as transformadas clássicas também podem ser empregados para reduzir a complexidade aritmética das transformadas fracionais.

No caso da transformada de Hartley, há algoritmos específicos para reduzir sua complexidade aritmética [96–98], mas também é possível obtê-la a partir de sua relação com a transformada de Fourier. No que se refere às transformadas trigonométricas, é possível utilizar as relações entre a FFFT, a FFCT-1 e a FFST-1, como também a relação entre a GFFFT, a FFCT-4 e a FFST-4, para se reduzir a complexidade aritmética. Além disso, como a matriz de transformação de uma FFTT específica apresenta exatamente o mesmo tipo de simetria de sua versão equivalente sobre o corpo dos números reais, é viável o uso dos mesmos algoritmos rápidos propostos para as transformadas trigonométricas sobre o corpo dos números reais. A Tabela 4.3 apresenta a complexidade aritmética de transformadas trigonométricas em corpos finitos de comprimento N [99].

Tabela 4.3: *Complexidade aritmética das FFTT de comprimento N, em que $M(N)$ e $A(N)$ denotam os números de multiplicações e adições.*

Transformada	$M(N)$	$A(N)$
FFCT/FFST II e III	$(N/2)\log_2(N)$	$(3N/2)\log_2(N) - N + 1$
FFCT/FFST IV	$(N/2)\log_2(N) + N$	$(3N/2)\log_2(N)$
FFCT I	$(N/2)\log_2(N) - N + 1$	$(5N/2)\log_2(N) - 2N + 4$
FFST I	$(N/2)\log_2(N) - N$	$(N/2)\log_2(N) - 2N + 2$

Fonte: Próprio Autor.

CAPÍTULO 5

APLICAÇÕES

Este capítulo apresenta algumas aplicações da transformada fracional sobre corpos finitos na Engenharia.São propostos: (i) um sistema de cifragem de imagens digitais em que parâmetros fracionais da transformada são utilizados como chave; (ii) um sistema que insere uma marca d'água frágil em imagens no domínio fracional; e, (iii) um sistema de comunicação multiusuário que explora a ortogonalidade dos autovetores da GFrFT.

Nos sistemas de cifragem e de marca d'água, é necessário calcular uma transformada de uma imagem. Essa operação pode ser realizada pela equação matricial

$$\mathbf{A}' = \mathbf{M}\mathbf{A}\mathbf{M}^t,$$

em que $\mathbf{A}'$ é o espectro fracional da matriz (imagem) $\mathbf{A}$, $\mathbf{M}$ é uma matriz de transformação e $\mathbf{M}^t$ é sua transposta. Com o propósito de não especificar a transformada fracional a ser empregada, emprega-se o acrônimo GFrMT para representar genericamente uma transformada fracional, cuja matriz de transformação é $\mathbf{M}$.

5.1 Cifragem de imagens no domínio fracional

O sistema de cifragem apresentado nesta seção é um cifrador de bloco, simétrico, aplicado a imagens. O esquema de cifragem combina a arquitetura de substituição-permutação do sistema AES (do inglês, *Advanced Encryption Standard*) [100, pp. 147] com a transformada fracional de Fourier sobre corpos finitos para transformar cada bloco da imagem de maneira similar ao esquema proposto por Lima *et al.* [45]. Nos esquemas propostos em [45] e em [101], a não linearidade das operações é

obtida fazendo-se sobreposições dos blocos da imagem e cifrando duas vezes cada bloco da imagem. Já no esquema de cifragem proposto nesta tese, a arquitetura de substituição-permutação provê a não linearidade, evitando sobreposições e repetições, o que contribui para a redução do custo computacional da implementação do esquema.

Na proposta de Lima *et al.* [45], antes da cifragem, pares de *pixels* são convertidos em vetores de duas posições, constituindo uma estrutura semelhante aos números complexos, e suas operações e transformadas são definidas sobre $\mathrm{GI}(p)$. Na proposta de Lima *et al.* [101], são usadas as transformadas do cosseno em corpos finitos do tipo 2 para a transformação de cada bloco. Potências inteiras das matrizes de transformação são aplicadas a cada bloco, e o valor de cada expoente é um parâmetro da chave secreta. Conjectura-se que as matrizes dessas transformadas tenham ciclo infinito, assim seria inviável recuperar o bloco transformado com sucessivas aplicações da transformada.

Dois princípios de criptossistemas de chave secreta empregados para dificultar análises estatísticas são a difusão e a confusão [100, pp. 72]. A difusão está relacionada à redução da redundância da informação em grandes quantidades de dados. A confusão objetiva tornar mais complexa a relação entre o texto cifrado e a chave, de forma que cada elemento do texto cifrado dependa de vários elementos da chave. A arquitetura de substituição-permutação provê confusão e difusão ao sistema, enquanto que a aplicação da transformada provê difusão.

Apesar de empregar a arquitetura de substituição-permutação, o esquema de cifragem proposto é realizado em apenas uma rodada, ou seja, cada bloco percorre uma única vez cada estágio da cifragem. A difusão associada ao uso da transformada possibilita essa redução do número de rodadas sem prejudicar a segurança do processo da cifragem.

Em linhas gerais, a cifragem consiste do seguinte processo: inicialmente, a imagem original, $\mathbf{I}$, é embaralhada e dividida em blocos de dimensão 8×8; cada bloco é combinado com elementos da chave e ao bloco resultante é aplicada uma GFrMT de parâmetro fracional a; esse parâmetro varia a cada bloco processado, sendo definido por alguns elementos da chave; há uma realimentação no sistema, de forma que um bloco cifrado dependa de outros blocos anteriormente cifrados.

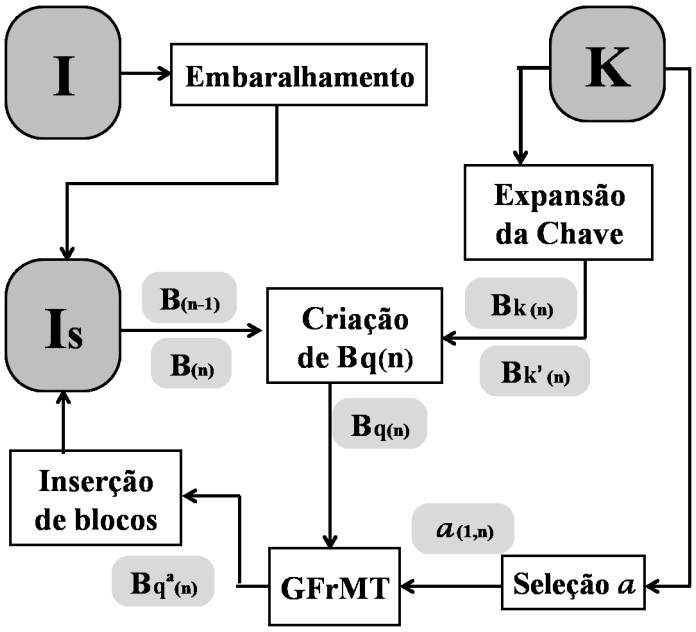
Um ponto a ser destacado na presente proposta reside na possibilidade de se empregar qualquer uma das transformadas fracionais sobre corpos finitos baseadas em funções de matrizes introduzidas nesta tese. No entanto, é preferível que os elementos da matriz de transformação estejam em $\mathrm{GF}(p)$ para que os elementos da imagem cifrada sejam representados por números inteiros e não por números complexos (elementos de $\mathrm{GI}(p)$).

5.1.1 Esquema de cifragem

O diagrama em blocos da Figura 5.1 apresenta a proposta do esquema de cifragem de imagens desta tese. Para melhor compreender a descrição dos esquemas de cifragem e de decifragem, denote por $\mathbf{Is}$, a imagem $\mathbf{I}$ embaralhada, por $\mathbf{B}_{(n)}$, o n-ésimo bloco de $\mathbf{Is}$ e por $\mathbf{Bq}_{(n)}$ o n-ésimo bloco ao qual é efetivamente aplicada uma GFrMT. O esquema é dividido em quatro estágios: (I) embaralhamento, (II) formação do bloco $\mathbf{Bq}$, (III) expansão da chave e (IV) aplicação da GFrMT.

Provê-se a difusão nos estágios de embaralhamento, de formação do bloco $\mathbf{Bq}$ e de aplicação da GFrMT. Provê-se a confusão no estágio de formação de $\mathbf{Bq}$.

Figura 5.1: *Diagrama em blocos do esquema de cifragem de imagens usando uma GFrMT.*

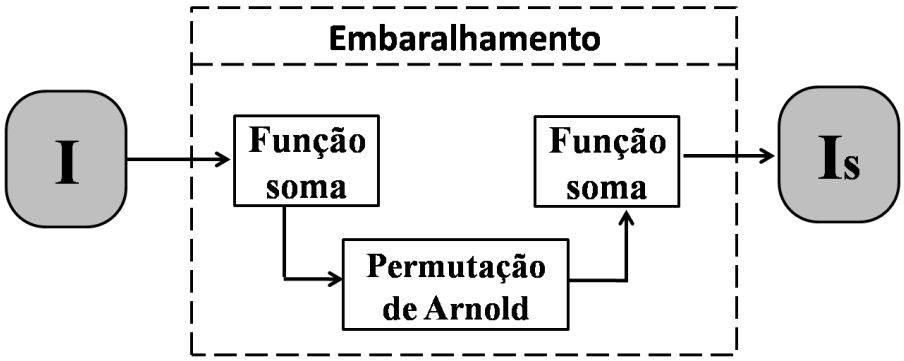


A imagem $\mathbf{I}$ *é embaralhada, resultando na imagem* $\mathbf{Is}$*. De* $\mathbf{Is}$ *são extraídos os blocos* $\mathbf{B}_{(n)}$ *e* $\mathbf{B}_{(n-1)}$*, e da chave* $\mathbf{K}$ *pela processo de expansão da chave são formados os blocos* $\mathbf{Bk}'_{(n)}$ *e* $\mathbf{Bk}_{(n)}$*. Com estes quatro blocos é formado o bloco* $\mathbf{Bq}_{(n)}$ *ao qual é aplicada uma GFrMT de parâmetro fracional* a_n*, resultando no bloco* $\mathbf{Bq}^a_{(n)}$*. O parâmetro* $a_{(n)}$ *é construído a partir de elementos da chave secreta. O bloco* $\mathbf{Bq}^a_{(n)}$ *substitui* $\mathbf{B}_{(n)}$ *em* $\mathbf{Is}$ *e o processo é repetido até que a todos os blocos de* $\mathbf{Is}$ *seja aplicada uma GFrMT.* Fonte: Próprio Autor.

Estágio (I): Embaralhamento

Em imagens digitais, os *pixels* de certas regiões apresentam alta correlação. Com o intuito de inserir difusão ao sistema, inicialmente é realizado um embaralhamento nos *pixels* da imagem. O embaralhamento é realizado em duas etapas: a *soma* e a *permutação de pixels*. A Figura 5.2 ilustra este processo.

Figura 5.2: *Diagrama em blocos do processo de embaralhamento de pixels.*



Na etapa de soma*, cada pixel é substituído pela soma do pixel atual com o anterior. Em seguida, na etapa da permutação, os pixels são permutados de posição. Novamente a imagem é submetida à etapa de* soma. Fonte: Próprio Autor.

Na etapa de *soma*, cada *pixel* da imagem é somado com o *pixel* anterior; a soma é módulo 256 para que o valor de cada *pixel* esteja no intervalo de 0 a 255. Esta etapa se repete duas vezes conforme se observa na Figura 5.2.

Na etapa de permutação de *pixels*, é usado o algoritmo de Arnold [102]. Esse algoritmo foi desenvolvido na área de teoria ergódica de mecânica quântica, sendo também conhecido como *cat face transform*. Para uma imagem quadrada de dimensão $W \times W$, o *pixel* da i-ésima linha e j-ésima coluna, posição (i, j) da imagem original $\mathbf{I}$, é mapeado para a posição (i', j') da imagem embaralhada, $\mathbf{Is}$, de acordo com

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^b \begin{bmatrix} i \\ j \end{bmatrix} \pmod{W}, \tag{5.1}$$

em que b, número de vezes em que a permutação é realizada, depende da chave secreta. Se a chave $\mathbf{K} = \{k_0, k_1, \ldots, k_{L-1}\}$ é formada por L inteiros, o número de vezes em que a permutação é realizada é $b = \sum_{l=1}^{L} k_l \pmod{10}$. O processo é realizado para inviabilizar um ataque diferencial (vide Seção 5.1.4), de forma que uma pequena alteração na imagem original ou na chave secreta gere uma imagem cifrada consideravelmente diferente da imagem cifrada sem alteração.

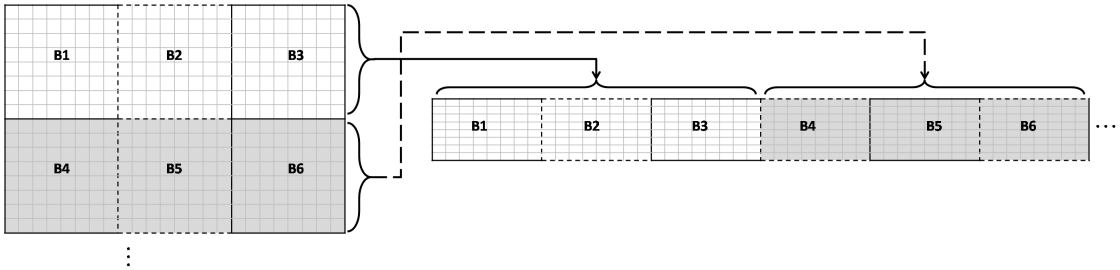
Estágio (II): Formação de Bq

Após o embaralhamento dos *pixels*, a imagem embaralhada $\mathbf{Is}$ é dividida em blocos de dimensão 8×8. Se a imagem tem dimensões $W \times W$, com $W = 8c$, para c um número inteiro, são formados c^2 blocos com a imagem.

O processo de obtenção dos blocos da imagem pode ser feito por meio de um arranjo dos *pixels*.

Para facilitar a implementação, os blocos podem ser organizados em um arranjo simples, dispondo-os em sequência. A Figura 5.3 ilustra o processo de arranjo dos blocos da imagem.

Figura 5.3: *Esquema de arranjo de blocos* 8×8 *sem sobreposição.*

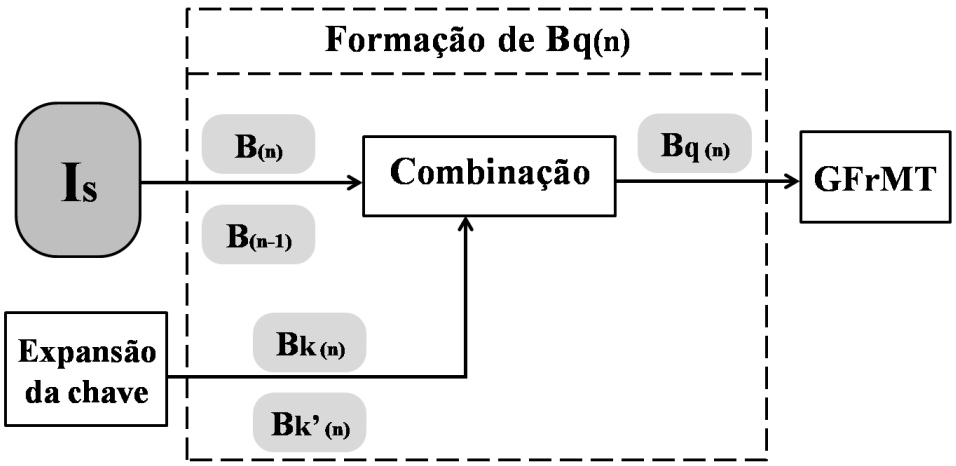


Os blocos são ordenados em ordem crescente da esquerda para direita e de cima para baixo. Na figura, são selecionados os blocos de uma mesma linha (B1, B2, B3), depois são selecionados os blocos da linha seguinte (B4, B5, B6) e assim sucessivamente. Fonte: Próprio Autor.

Outra maneira de organizar é formar cada bloco com sobreposições conforme a proposta apresentada em [101]. Isso provê mais difusão ao sistema, contudo eleva a complexidade computacional, uma vez que uma maior quantidade de blocos é processada.

Na Figura 5.4 é apresentado o esquema de formação de $\mathbf{Bq}_{(n)}$, o n-ésimo bloco ao qual é efetivamente aplicada uma GFrMT. Na formação de $\mathbf{Bq}_{(n)}$, considere que $\mathbf{B}_{(n)}$ é o n-ésimo bloco de $\mathbf{Is}$ e $\mathbf{Bk}_{(n)}$ é o n-ésimo bloco formado no processo de expansão da chave, estágio (III).

Figura 5.4: *Esquema de formação do* n*-ésimo bloco* $\mathbf{Bq}$.



São selecionados os blocos $\mathbf{B}_{(n)}$ *e* $\mathbf{B}_{(n-1)}$ *de* $\mathbf{Is}$*, e o bloco* $\mathbf{Bk}_{(n)}$ *da chave. O bloco* $\mathbf{Bq}_{(n)}$ *é o resultado da combinação desses blocos de acordo com as equações (5.2) e (5.3).* Fonte: Próprio Autor.

As Equações (5.2) e (5.3) descrevem a combinação feita entre os blocos selecionados:

$$\mathbf{Bq}'_{(n)} = (\mathbf{B}_{(n)} \oplus \mathbf{B}_{(n-1)}) + \mathbf{Bk}'_{(n)} \pmod{256}, \tag{5.2}$$

$$\mathbf{Bq}_{(n)} = (\mathbf{Bq}'_{(n)} \oplus \mathbf{B}_{(n-1)}) + \mathbf{Bk}_{(n)} \pmod{256}. \tag{5.3}$$

Na Equação (5.2), são selecionados os blocos $\mathbf{B}_{(n)}$ e $\mathbf{B}_{(n-1)}$ de $\mathbf{Is}$. É obtido também o bloco $\mathbf{Bk}'_{(n)}$ do processo de expansão da chave. É feita uma operação ou-exclusivo binária (XOR, do inglês *exclusive or*) entre os *bits* de $\mathbf{B}_{(n)}$ e de $\mathbf{B}_{(n-1)}$, e deste resultado é feita uma soma módulo 256 com os elementos do bloco $\mathbf{Bk}_{(n)}$. Ao final destas operações, tem-se o bloco auxiliar $\mathbf{Bq}'_{(n)}$.

Na Equação (5.3), são usados o bloco $\mathbf{B}_{(n-1)}$ de $\mathbf{Is}$ e o bloco $\mathbf{Bq}'_{(n)}$, resultado da Equação (5.2). A chave é deslocada ciclicamente em um *bit* e dela é obtido um novo bloco $\mathbf{Bk}_{(n)}$ do processo de expansão da chave. É feita uma operação XOR entre os *bits* de $\mathbf{Bq}'_{(n)}$ e de $\mathbf{B}_{(n-1)}$, e deste resultado é feita uma soma módulo 256 com os elementos do bloco $\mathbf{Bk}_{(n)}$. Ao final destas operações, tem-se o bloco $\mathbf{Bq}_{(n)}$.

O bloco $\mathbf{Bq}_n$ depende do bloco $\mathbf{B}_{(n-1)}$, que é um bloco cujos elementos já foram cifrados, e depende da chave. Note que há dois blocos diferentes construídos com elementos da chave: $\mathbf{Bk}'_{(n)}$ e $\mathbf{Bk}_{(n)}$. Uma análise da influência da chave no processo de cifragem e decifragem é feita na Seção 5.1.4.

Quando $\mathbf{B}_{(n)}$ é o primeiro bloco da imagem, $\mathbf{B}_{(n-1)}$ é formado por um bloco padrão. O bloco padrão é construído com todos os elementos da chave. Os *bits* da chave são agrupados em *bytes* e cada *byte* representa um elemento do bloco padrão. Como o número de *bytes* é menor que a quantidade de elementos do bloco, a chave é deslocada em um *bit* e novamente os *bits* são agrupados em *bytes*. Isso é repetido sucessivas vezes até que se obtenham os 64 elementos do bloco padrão.

Estágio (III): Expansão da Chave

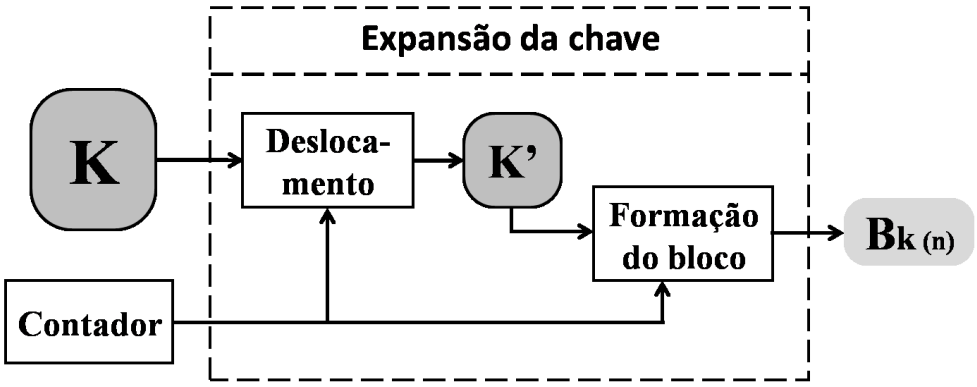
A formação dos blocos $\mathbf{Bk}'$ e $\mathbf{Bk}$ é feita no estágio de expansão da chave. A Figura 5.5 apresenta um diagrama em blocos do processo de expansão da chave.

Com os 256 *bits* da chave secreta são formados 32 *bytes*: $k_{(1)}, k_{(2)}, \ldots, k_{(32)}$. A partir desses 32 *bytes*, são construídos os vetores $\mathbf{v}_1$, com os *bytes* $k_{(1)}, \ldots, k_{(8)}$, e $\mathbf{v}_2$, com os *bytes* $k_{(17)}, \ldots, k_{(24)}$. É formada também a constante E_0, que é a soma módulo 256 de todos os 32 *bytes* da chave. Se a soma for igual zero, seu valor é trocado para 1.

Com o vetor $\mathbf{v}_1$ e os *bytes* $k_{(9)}, \ldots, k_{(16)}$, é formado o bloco $\mathbf{C}$, de dimensão 8×8, num processo ilustrado pela Figura 5.6. A m-ésima coluna de $\mathbf{C}$, $\mathbf{c}_m$, é dada por

$$c_m = \mathbf{v}_1 \oplus E_0 \oplus \mathbf{k}_{(8+m)}, \quad m = 1, \ldots, 8. \tag{5.4}$$

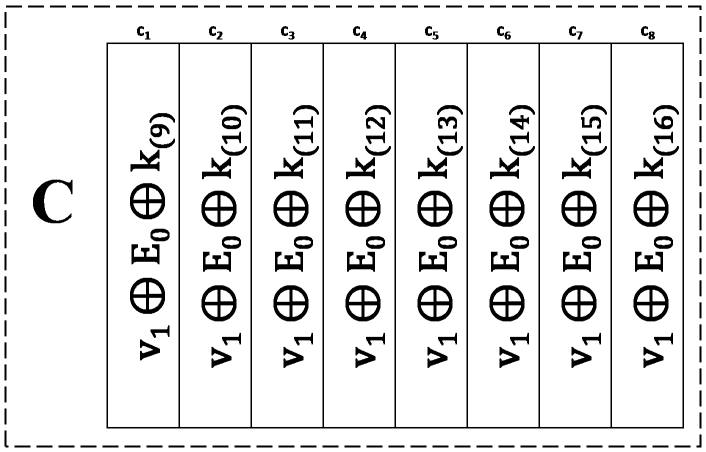
Figura 5.5: *Esquema de formação do n-ésimo bloco $\mathbf{Bk}'$.*



A chave $\mathbf{K}$ é deslocada em 1 bit *a direita. De forma similar, o bloco $\mathbf{Bk}_{(n)}$ é construído deslocando a chave $\mathbf{K}$ em* 1 bit *e repetindo as demais etapas do processo.* Fonte: Próprio Autor.

Por exemplo, a primeira coluna do bloco $\mathbf{C}$ (coluna $\mathbf{c}_1$) é dada por $\mathbf{c}_1 = \mathbf{v}_1 \oplus E_0 \oplus \mathbf{k}_{(9)}$.

Figura 5.6: *Construção do bloco auxiliar $\mathbf{C}$ usado na construção do n-ésimo bloco $\mathbf{Bk}'$.*



A m-ésima coluna de $\mathbf{C}$, $\mathbf{c}_m$, é dada por uma operação XOR entre o vetor $\mathbf{v}_1$, a constante E_0 e o byte $k_{(8+m)}$. Fonte: Próprio Autor.

Com o vetor $\mathbf{v}_2$ e os *bytes* $k_{(25)}, \ldots, k_{(32)}$, é formado o bloco $\mathbf{D}$, de dimensão 8×8, num processo ilustrado pela Figura 5.7. A m-ésima coluna de $\mathbf{D}$, $\mathbf{d}_m$, é dada por

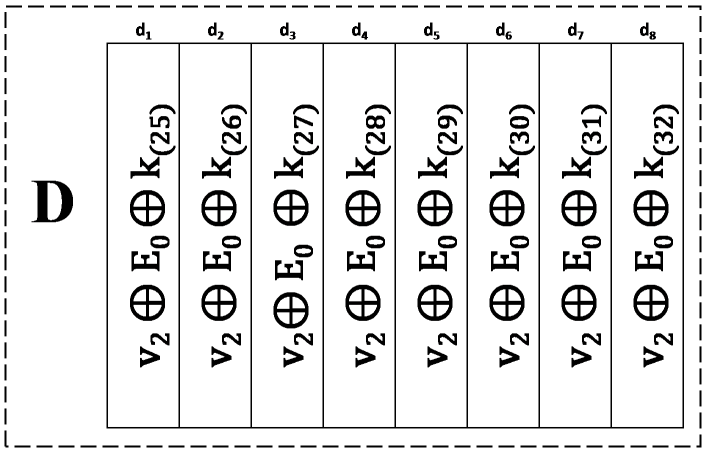
$$d_m = \mathbf{v}_2 \oplus E_0 \oplus \mathbf{k}_{(24+m)}, \quad m = 1, \ldots, 8. \tag{5.5}$$

O bloco $\mathbf{Bk}'_{(n)}$ é construído com $\mathbf{C}$ e $\mathbf{D}$ por meio de

$$\mathbf{Bk}'_{(n)} = \mathbf{C} + (E_0 + n) \times \mathbf{D} \pmod{256}, \tag{5.6}$$

em que n representa o n-ésimo bloco $\mathbf{Bk}$ construído. A chave é deslocada ciclicamente a direita em um *bit* e o bloco $\mathbf{Bk}_{(n)}$ é construído pelo mesmo processo.

Figura 5.7: *Construção do bloco auxiliar* $\mathbf{D}$ *usado na construção do* n*-ésimo bloco* $\mathbf{Bk}'$.



A m*-ésima coluna de* $\mathbf{D}$*,* $\mathbf{d}_m$*, é dada por uma operação XOR entre o vetor* $\mathbf{v}_2$*, a constante* E_0 *e o* byte $k_{(24+m)}$. Fonte: Próprio Autor.

Estágio (IV): Aplicação da transformada

O espectro fracional dos blocos da imagem é obtido através de uma GFrMT com parâmetro fracional a, o qual é especificado por uma sequência de 6 *bits* da chave secreta $\mathbf{K}$. A matriz de transformação a ser aplicada ao bloco $\mathbf{Bq}_n$ tem parâmetro fracional dado por $a_n = \left(\frac{a_{1,n}}{a_2}\right)$. O termo a_2 é constante e especifica o número de *bits* L. Já o termo $a_{1,n}$ é um número inteiro formado pelos 6 primeiros *bits* da chave. A cada escolha de a_1, a chave é deslocada ciclicamente a direita em um *bits*. O bloco $\mathbf{B}_n^{a_n}$ representa o espectro fracional do bloco $\mathbf{Bq}_n$ e é dado por

$$\mathbf{B}_n^{a_n} = (\mathbf{M}^{a_{1,n}})\ \mathbf{Bq}_n\ (\mathbf{M}^{a_{1,n}})^t. \tag{5.7}$$

A Equação (5.7) é aplicada recursivamente até que os elementos de $\mathbf{B}_n^{a_n}$ estejam no intervalo de 0 a 255. Isso ocorre porque a transformada é definida em $\mathrm{GF}(257)$, então os *pixels* dos blocos podem assumir valores entre 0 e 256.

Em seguida, o bloco $\mathbf{B}_n^{a_n}$ é inserido na imagem, substituindo o bloco $\mathbf{B}_n$. Esse processo ocorre com todos os blocos da imagem em uma única rodada. No final, a imagem $\mathbf{Is}$ contém apenas blocos cifrados e passa a ser chamada de $\mathbf{Ic}$.

Nota 5. 1 O máximo valor do parâmetro a_2 é dado pela ordem do elemento ζ com o qual se constrói a matriz $\mathbf{M}$. É considerado sempre o maior valor de a_2.

Nota 5. 2 Fixando o valor de a_2, os possíveis valores de a_1 devem estar no intervalo $1 \leq a_1 \leq a_2 - 1$.

Nota 5. 3 O comprimento da chave é arbitrário, desde que seja maior que 192 *bits* e menor que o número de blocos a serem cifrados.

5.1.2 Esquema de decifragem

O processo de decifragem é exatamente o inverso do processo de cifragem. É necessário saber a quantidade de blocos cifrados para se deslocar a chave de maneira coerente com o número de deslocamentos feito na cifragem. O último bloco cifrado da imagem deve ser o primeiro bloco a ser decifrado.

Na cifragem, se a foi o parâmetro fracional, deve-se usar, na decifragem, o parâmetro fracional $a' = (4-a)$. Ao bloco $\mathbf{B}_n^{a_n}$ é aplicada a matriz da GFrMT associada ao parâmetro a' correspondente. A aplicação da GFrMT associada a a também é realizada de maneira recursiva até que os elementos de $\mathbf{B}_n$ estejam no intervalo de 0 a 255. De maneira similar, deve-se atentar ao caso em que se deve usar o bloco padrão. Após esses estágios, é desfeito o embaralhamento, e obtém-se a imagem decifrada.

5.1.3 Exemplo do esquema de cifragem

Neste exemplo, é mostrado o progresso do processo de cifragem de uma imagem de dimensões 16×16 codificada a 8 *bpp*. A Tabela 5.1 mostra os valores dos *pixels* da imagem de teste. Apesar de não ter sido dividida em blocos, para efeito de ilustração, as linhas da tabela delimitam os blocos 8×8.

Tabela 5.1: *Valores dos* pixels *das colunas* 1 *a* 16 *e linhas* 1 *a* 16 *de uma imagem sem embaralhamento,* $\mathbf{I}_0$. *A partir desses elementos são formados* 4 *blocos de* 8×8 pixels. *Fonte: Próprio Autor.*

100	89	66	46	28	36	62	53	57	38	77	139	172	171	173	174
70	56	42	37	28	43	31	51	59	73	140	181	175	168	164	168
46	53	33	42	41	27	28	36	69	116	168	175	163	163	161	171
24	37	45	38	61	22	16	61	101	155	172	155	157	152	162	182
24	26	35	48	62	24	63	133	145	156	172	149	141	147	172	185
36	24	28	42	41	64	119	162	159	159	160	137	138	155	176	185
33	26	35	35	36	109	149	156	180	133	111	128	155	157	168	180
30	21	44	30	93	156	166	165	137	96	86	67	98	143	155	173
44	29	17	62	145	182	172	90	36	37	50	41	75	107	141	182
23	30	27	113	168	191	109	22	31	32	138	76	71	93	140	183
20	11	73	150	183	122	88	85	74	94	162	131	81	87	147	172
18	38	123	183	115	78	113	123	115	109	120	133	101	88	136	193
25	86	169	126	55	90	116	137	148	149	151	134	109	90	123	197
45	137	160	33	67	91	109	130	151	157	151	131	112	93	115	194
81	174	65	22	67	91	103	121	137	147	142	121	99	86	105	190
125	113	8	40	64	89	97	114	123	132	133	109	90	91	98	183

Fonte: Próprio Autor.

O primeiro bloco é formado por elementos das linhas 1 a 8 e das colunas 1 a 8. O segundo bloco

é formado por elementos das linhas 1 a 8 e das colunas 9 a 16. O terceiro bloco é formado por elementos das linhas 9 a 16 e das colunas 1 a 8. O quarto bloco é formado por elementos das linhas 9 a 16 e das colunas 9 a 16.

Embaralhamento

O primeiro estágio do processo de cifragem é o embaralhamento, que é realizado com todos os elementos da imagem original. Como visto na Figura 5.2, o embaralhamento é realizado em duas etapas. Inicialmente, a imagem original é submetida à etapa de *soma*, Tabela 5.2.

Tabela 5.2: *Imagem* $\mathbf{I}_1$ *obtida após a primeira etapa de* soma*. O primeiro* pixel *da imagem* $\mathbf{I}_1$*, de valor* 100*, é dado pela soma do primeiro* pixel *da imagem* $\mathbf{I}_1$*,* 100*, com zero. O segundo* pixel *da imagem* $\mathbf{I}_1$*, de valor* 189*, é dado pela soma do segundo* pixel *da imagem* $\mathbf{I}_0$*,* 89*, com o primeiro* pixel *da imagem* $\mathbf{I}_1$*,* 100*. O terceiro* pixel *da imagem* $\mathbf{I}_1$*, de valor* 255*, é dado pela soma do terceiro* pixel *da imagem* $\mathbf{I}_0$*,* 66*, com o segundo* pixel *da imagem* $\mathbf{I}_1$*,* 189*. O* pixel *da segunda linha da imagem* $\mathbf{I}_1$*, de valor* 15*, é dado pela soma do primeiro* pixel *da segunda linha da imagem* $\mathbf{I}_0$*,* 70*, com o último* pixel *da segunda linha da imagem* $\mathbf{I}_1$*,* 201*. Observe que a soma é módulo* 256 *para que os* pixels *sejam codificados com* 8 bits*.*

100	189	255	45	73	109	171	224	25	63	140	23	195	110	27	201
15	71	113	150	178	221	252	47	106	179	63	244	163	75	239	151
197	250	27	69	110	137	165	201	14	130	42	217	124	31	192	107
131	168	213	251	56	78	94	155	0	155	71	226	127	23	185	111
135	161	196	244	50	74	137	14	159	59	231	124	9	156	72	1
37	61	89	131	172	236	99	5	164	67	227	108	246	145	65	250
27	53	88	123	159	12	161	61	241	118	229	101	0	157	69	249
23	44	88	118	211	111	21	186	67	163	249	60	158	45	200	117
161	190	207	13	158	84	0	90	126	163	213	254	73	180	65	247
14	44	71	184	96	31	140	162	193	225	107	183	254	91	231	158
178	189	6	156	83	205	37	122	196	34	196	71	152	239	130	46
64	102	225	152	11	89	202	69	184	37	157	34	135	223	103	40
65	151	64	190	245	79	195	76	224	117	12	146	255	89	212	153
198	79	239	16	83	174	27	157	52	209	104	235	91	184	43	237
62	236	45	67	134	225	72	193	74	221	107	228	71	157	6	196
65	178	186	226	34	123	220	78	201	77	210	63	153	244	86	13

Fonte: Próprio Autor.

Em seguida, ocorre o processo de permutação de elementos segundo o algoritmo de Arnold, Tabela 5.3. A chave original é $\mathbf{K} = (129, 130, 63, 224, 12, 30, 73, 48, 29, 32, 163, 24, 112, 103, 173, 148, 5, 3, 4, 233, 8, 35, 67, 28, 1, 2, 44, 64, 28, 11, 27, 44)$, assim o número de vezes em que o algoritmo é usado é $2122 \equiv 2 \pmod{10}$. Observe que o elemento da primeira linha e primeira coluna da Tabela 5.2, destacado em negrito, é deslocado para a quinta linha e oitava coluna da Tabela 5.3.

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^2 \begin{bmatrix} 1 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 8 \end{bmatrix} \pmod{16}.$$

Tabela 5.3: *Imagem* $\mathbf{I}_2$ *obtida após permutação de linhas e colunas da imagem* $\mathbf{I}_1$ *usando o algoritmo de Arnold. O algoritmo foi aplicado* 2 *vezes. Observe que o elemento da primeira linha e coluna da imagem* $\mathbf{I}_1$*, após a permutação é o elemento da quinta linha e oitava coluna da imagem* $\mathbf{I}_2$*.*

239	62	225	158	99	14	210	255	231	27	213	73	27	196	249	9
101	23	201	79	156	111	14	179	228	223	247	61	69	123	76	225
184	213	246	192	65	64	96	161	0	140	91	130	23	196	178	72
109	157	34	60	156	151	236	152	84	5	130	63	89	158	53	251
89	110	220	224	107	0	185	**100**	239	83	21	159	63	71	103	161
46	44	244	221	193	37	254	145	107	178	190	31	61	155	23	184
153	212	14	88	56	171	52	196	158	72	15	45	11	0	164	42
59	244	157	40	190	131	137	78	117	183	157	111	189	16	205	186
140	241	71	195	43	178	88	50	252	74	157	73	65	197	186	245
67	89	90	67	217	244	153	44	123	78	224	209	71	45	1	71
131	255	83	37	67	231	163	6	64	207	172	165	201	12	254	69
180	250	250	226	79	162	118	226	110	237	189	118	74	47	221	34
104	152	200	135	113	134	202	126	227	124	86	65	71	159	94	25
201	77	146	91	249	168	45	174	122	163	124	75	196	102	13	236
211	137	106	107	135	65	37	27	34	195	193	229	127	27	198	6
151	184	12	155	63	235	239	117	161	150	225	69	163	108	31	13

Fonte: Próprio Autor.

Novamente a imagem é submetida à etapa de Soma, Tabela 5.4.

Tabela 5.4: *Imagem* $\mathbf{I}_3$ *obtida após a segunda etapa de Soma. É feito o mesmo processo de soma que o mostrado na Tabela 5.2. Novamente, o primeiro* pixel *é somado com zero.*

239	45	14	172	15	29	239	238	213	240	197	14	41	237	230	239
84	107	52	131	31	142	156	79	51	18	9	70	139	6	82	51
235	192	182	118	183	247	87	248	248	132	223	97	120	60	238	54
163	64	98	158	58	209	189	85	169	174	48	111	200	102	155	150
239	93	57	25	132	132	61	161	144	227	248	151	214	29	132	37
83	127	115	80	17	54	52	197	48	226	160	191	252	151	174	102
255	211	225	57	113	28	80	20	178	250	9	54	65	65	229	15
74	62	219	3	193	68	205	27	144	71	228	83	16	32	237	167
51	36	107	46	89	11	99	149	145	219	120	193	2	199	129	118
185	18	108	175	136	124	21	65	188	10	234	187	2	47	48	119
250	249	76	113	180	155	62	68	132	83	255	164	109	121	119	188
112	106	100	70	149	55	173	143	253	234	167	29	103	150	115	149
253	149	93	228	85	219	165	35	6	130	216	25	96	255	93	118
63	140	30	121	114	26	71	245	111	18	142	217	157	3	16	252
207	88	194	45	180	245	26	53	87	26	219	192	63	90	32	38
189	117	129	28	91	70	53	170	75	225	194	7	170	22	53	66

Fonte: Próprio Autor.

Expansão da chave

O terceiro estágio é a expansão da chave, em que são construídos blocos de dimensão 8×8 codificados a 8 *bpp*. Esses blocos são usados no estágio (II) para a formação dos blocos $\mathbf{Bq}$. São construídos apenas os dois primeiros blocos: o primeiro bloco com a chave original; o segundo com a chave deslocada ciclicamente em um *bit*. Para cada chave, são construídos 32 *bytes*, $k_{(1)}$ a $k_{(32)}$.

A chave original é $\mathbf{K}_0 = (129, 130, 63, 224, 12, 30, 73, 48, 29, 32, 163, 24, 112, 103, 173, 148, 5, 3, 4, 233, 8, 35, 67, 28, 1, 2, 44, 64, 28, 11, 27, 44)$, a qual é a sequência dos primeiros 32 *bytes*. As Tabelas 5.5 e 5.6 mostram, respectivamente, os dois primeiros blocos auxiliares $\mathbf{C}$ e $\mathbf{D}$, que são combinados segundo a Equação (5.6) para gerar o bloco $\mathbf{Bk}'_{(1)}$, que é apresentado na Tabela 5.7. Para esses dois blocos, a constante E_0 é 74 $(2122 \equiv 74 \pmod{256})$.

Tabela 5.5: *Processo de expansão da chave e formação do primeiro bloco auxiliar,* $\mathbf{C}$*, do bloco da chave* $\mathbf{Bk}'_{(1)}$*. A coluna* c_0 *da tabela é formada por* $\mathbf{v}_1 \oplus E_0$ $((129, 130, 63, 224, 12, 30, 73, 48) \oplus 39)$*. Os elementos da coluna* c_1 *de* $\mathbf{C}$ *são dados por um XOR entre* $\mathbf{v}_1 \oplus E_0$ *e* $k_{(9)} = 29$*. Os elementos da coluna* c_2 *de* $\mathbf{C}$ *são dados por um XOR entre* $\mathbf{v}_1 \oplus E_0$ *e* $k_{(10)} = 32$*, e assim sucessivamente.*

c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
	$\mathbf{v}_1 \oplus E_0 \oplus k_{(.)}$							
$\mathbf{v}_1 \oplus E_0$	$k_{(9)}$	$k_{(10)}$	$k_{(11)}$	$k_{(12)}$	$k_{(13)}$	$k_{(14)}$	$k_{(15)}$	$k_{(16)}$
203	214	213	104	183	91	73	30	103
200	213	214	107	180	88	74	29	100
117	104	107	214	9	229	247	160	217
170	211	208	109	178	94	76	27	98
70	187	184	5	218	54	36	115	10
84	73	74	247	40	196	214	129	248
3	102	101	216	7	235	249	174	215
122	95	92	225	62	210	192	151	238

Fonte: Próprio Autor.

A chave $\mathbf{K}_0$ é deslocada ciclicamente a direita em um *bit* gerando a chave $\mathbf{K}_1 = (64, 193, 31, 240, 6, 15, 36, 152, 14, 144, 81, 140, 56, 51, 214, 202, 2, 129, 130, 116, 132, 17, 161, 142, 0, 129, 22, 32, 14, 5, 141, 150)$. As Tabelas 5.8 e 5.9 mostram, respectivamente, os dois primeiros blocos auxiliares $\mathbf{C}$ e $\mathbf{D}$, que são combinados segundo a Equação 5.6 para gerar o bloco $\mathbf{Bk}_{(1)}$, que é apresentado na Tabela 5.10. Para esses dois blocos, a constante E_0 é 30 $(2846 \equiv 30 \pmod{256})$.

Tabela 5.6: *Processo de expansão da chave e formação do primeiro bloco auxiliar,* $\mathbf{D}$*, do bloco da chave* $\mathbf{Bk}'_{(1)}$*. A coluna* d_0 *da tabela é formada por* $\mathbf{v}_2 \oplus E_0$*,* $((5, 3, 4, 233, 8, 35, 67, 28) \oplus 39)$*. Os elementos da coluna* d_1 *de* $\mathbf{D}$ *são dados por um XOR entre* $\mathbf{v}_2 \oplus E_0$ *e* $k_{(25)} = 1$*. Os elementos da coluna* d_2 *de* $\mathbf{D}$ *são dados por um XOR entre* $\mathbf{v}_2 \oplus E_0$ *e* $k_{(26)} = 2$*, e assim sucessivamente.*

d_0	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8
	$\mathbf{v}_2 \oplus E_0 \oplus k_{(.)}$							
$\mathbf{v}_2 \oplus E_0$	$k_{(25)}$	$k_{(26)}$	$k_{(27)}$	$k_{(28)}$	$k_{(29)}$	$k_{(30)}$	$k_{(31)}$	$k_{(32)}$
79	78	72	79	162	67	104	8	87
73	77	75	76	161	64	107	11	84
78	99	101	98	143	110	69	37	122
163	15	9	14	227	2	41	73	22
66	83	85	82	191	94	117	21	74
105	68	66	69	168	73	98	2	93
9	84	82	85	184	89	114	18	77
86	99	101	98	143	110	69	37	122

Fonte: Próprio Autor.

Tabela 5.7: *Processo de expansão da chave e formação do primeiro bloco da chave* $\mathbf{Bk}'_{(1)}$*. Os blocos* $\mathbf{C}$ *e* $\mathbf{D}$ *mostrados nas Tabelas 5.5 e 5.6, respectivamente, são combinados de acordo com a Equação (5.6) para gerar o bloco* $\mathbf{Bk}'_{(1)}$*.*

176	237	14	14	5 25	2 193	118	228
100	207	175	223	24	163	86	0
105	2	140	238	31	46	119	151
56	115	135	51	244	79	126	212
12	159	11	207	192	107	154	184
53	160	46	96	39	140	23	55
2	107	191	239	254	95	244	102
96	243	151	35	12	247	110	172

Fonte: Próprio Autor.

Formação de $\mathbf{Bq}$

No segundo estágio do processo de cifragem são construídos os blocos $\mathbf{Bq}$, aos quais são efetivamente aplicadas as transformadas fracionais. Na formação do bloco $\mathbf{Bq}_{(1)}$ é selecionado o bloco $\mathbf{B}_{(1)}$ da imagem e construído o bloco $\mathbf{B}_{(0)}$ da chave, o qual é chamado de bloco padrão. Na Tabela 5.11 é mostrado o bloco padrão. Na Tabela 5.12 é mostrada a formação do bloco $\mathbf{Bq}_{(1)}$, com a chave $\mathbf{K}_0$ e os blocos $\mathbf{Bk}'_{(1)}$ e $\mathbf{Bk}_{(1)}$ mostrados nas Tabelas 5.7 e 5.10, respectivamente.

Tabela 5.8: *Processo de expansão da chave e formação do primeiro bloco auxiliar,* $\mathbf{C}$*, do bloco da chave* $\mathbf{Bk}_{(1)}$*. A coluna* c_0 *da tabela por* $\mathbf{v}_1 \oplus E_0$ $((64, 193, 31, 240, 6, 15, 36, 152) \oplus 141)$*. Os elementos da coluna* c_1 *de* $\mathbf{C}$ *são dados por um XOR entre* $\mathbf{v}_1 \oplus E_0$ *e* $k_{(9)} = 14$*. Os elementos da coluna* c_2 *de* $\mathbf{C}$ *são dados por um XOR entre* $\mathbf{v}_1 \oplus E_0$ *e* $k_{(10)} = 144$*, e assim sucessivamente.*

c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
	$\mathbf{v}_1 \oplus E_0 \oplus k_{(.)}$							
$\mathbf{v}_1 \oplus E_0$	$k_{(9)}$	$k_{(10)}$	$k_{(11)}$	$k_{(12)}$	$k_{(13)}$	$k_{(14)}$	$k_{(15)}$	$k_{(16)}$
94	80	209	15	224	22	31	52	136
223	209	80	142	97	151	158	181	9
1	15	142	80	191	73	64	107	215
238	210	83	141	98	148	157	182	10
24	102	231	57	214	32	41	2	190
17	31	158	64	175	89	80	123	199
58	8	137	87	184	78	71	108	208
134	148	21	203	36	210	219	240	76

Fonte: Próprio Autor.

Tabela 5.9: *Processo de expansão da chave e formação do primeiro bloco auxiliar,* $\mathbf{D}$*, do bloco da chave* $\mathbf{Bk}_{(1)}$*. A coluna* d_0 *da tabela por* $\mathbf{v}_2 \oplus E_0$ $((2, 129, 130, 116, 132, 17, 161, 142) \oplus 141)$*. Os elementos da coluna* d_1 *de* $\mathbf{D}$ *são dados por um XOR entre* $\mathbf{v}_2 \oplus E_0$ *e* $k_{(25)} = 0$*. Os elementos da coluna* d_2 *de* $\mathbf{D}$ *são dados por um XOR entre* $\mathbf{v}_2 \oplus E_0$ *e* $k_{(26)} = 129$*, e assim sucessivamente.*

d_0	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8
	$\mathbf{v}_2 \oplus E_0 \oplus k_{(.)}$							
$\mathbf{v}_2 \oplus E_0$	$k_{(25)}$	$k_{(26)}$	$k_{(27)}$	$k_{(28)}$	$k_{(29)}$	$k_{(30)}$	$k_{(31)}$	$k_{(32)}$
28	28	159	156	106	154	15	191	144
159	157	30	29	235	27	142	62	17
156	10	137	138	124	140	25	169	134
106	60	191	188	74	186	47	159	176
154	18	145	146	100	148	1	177	158
15	25	154	153	111	159	10	186	149
191	145	18	17	231	23	130	50	29
144	138	9	10	252	12	153	41	6

Fonte: Próprio Autor.

Tabela 5.10: *Processo de expansão da chave e formação do primeiro bloco da chave* $\mathbf{Bk}_{(1)}$. *Os blocos* $\mathbf{C}$ *e* $\mathbf{D}$ *mostrados nas Tabelas 5.8 e 5.9, respectivamente, são combinados de acordo com a Equação (5.6) para gerar o bloco* $\mathbf{Bk}_{(1)}$.

180	18	243	182	188	240	85	248
212	242	17	214	220	208	55	24
69	37	6	195	61	71	226	17
22	116	81	88	26	78	247	90
148	118	231	242	12	72	113	224
38	68	199	32	154	134	1	210
151	183	102	177	23	5	122	83
74	44	1	168	70	98	231	6

Fonte: Próprio Autor.

Tabela 5.11: *Bloco padrão,* $\mathbf{B}_{(0)}$, *construído com elementos da chave. Com uma chave de* 256 bits *são construídos* 32 bytes. *Em seguida, a chave é deslocada ciclicamente a direita em um* bit *e são construídos os* 32 bytes *restantes.*

129	130	63	224	12	30	73	48
29	30	163	24	112	130	173	148
5	3	4	233	8	35	67	28
1	2	44	64	28	11	27	44
64	193	31	240	6	15	36	152
14	143	81	140	56	65	86	202
2	129	130	116	132	17	161	142
0	129	22	32	14	5	141	150

Fonte: Próprio Autor.

Aplicação da GFrFT

Para cada bloco, a chave é deslocada em um *bit* e são selecionados seus seis *bits* iniciais para formar o parâmetro a usado na construção da matriz de transformação. Os valores de a são $a(1) = \frac{32}{64}$, $a(2) = \frac{16}{64}$, $a(3) = \frac{8}{64}$ e $a(4) = \frac{36}{64}$. Na Tabela 5.13 é mostrado o progresso do processo de cifragem.

Tabela 5.12: *Formação do bloco* $\mathbf{Bq}_1$. *As linhas de cada bloco são apresentadas como uma sequência de dois dígitos em hexadecimal. Em sequência são apresentados:* $\mathbf{B}_{(0)}$, *o bloco padrão;* $\mathbf{B}_{(1)}$, *o* 1^o *bloco da imagem* $\mathbf{Is}$*;* $\mathbf{C}(\mathbf{Bk}'_1)$ *e* $\mathbf{D}(\mathbf{Bk}'_1)$, *blocos auxiliares na formação de* $\mathbf{Bk}'_{(1)}$*;* $\mathbf{Bk}'_{(1)}$, *o* 1^o *bloco da chave;* $\mathbf{C}(\mathbf{Bk}_1)$ *e* $\mathbf{D}(\mathbf{Bk}_1)$, *blocos auxiliares na formação de* $\mathbf{Bk}_{(1)}$*;* $\mathbf{Bk}_{(1)}$, *o* 2^o *bloco da chave; e,* $\mathbf{Bq}_{(1)}$, *o bloco obtido após as Equações (5.2) e (5.3).*

$\mathbf{B}_0$	$\mathbf{B}_1$	$\mathbf{C}(\mathbf{Bk}'_1)$	$\mathbf{D}(\mathbf{Bk}'_1)$	$\mathbf{Bk}'_1$
81 82 3*F* *E*0 0*C* 1*E* 49 30	*EF* 2*D* 0*E* *AC* 0*F* 1*D* *EF* *EE*	*D*6 *D*5 68 *B*7 5*B* 49 1*E* 67	4*E* 48 4*F* *A*2 43 68 08 57	*B*0 *ED* 8*D* 2*D* *FC* *C*1 76 *E*4
1*D* 1*E* *A*3 18 70 82 *AD* 94	54 6*B* 34 83 1*F* 8*E* 9*C* 4*F*	*D*5 *D*6 6*B* *B*4 58 4*A* 1*D* 64	4*D* 4*B* 4*C* *A*1 40 6*B* 0*B* 54	64 *CF* *AF* *DF* 18 *A*3 56 00
05 03 04 *E*9 08 23 43 1*C*	*EB* *C*0 *B*6 76 *B*7 *F*7 57 *F*8	68 6*B* *D*6 09 *E*5 *F*7 *A*0 *D*9	63 65 62 8*F* 6*E* 45 25 7*A*	69 02 8*C* *EE* 1*F* 2*E* 77 97
01 02 2*C* 40 1*C* 0*B* 1*B* 2*C*	*A*3 40 62 9*E* 3*A* *D*1 *BD* 55	*D*3 *D*0 6*D* *B*2 5*E* 4*C* 1*B* 62	0*F* 09 0*E* *E*3 02 29 49 16	38 73 87 33 *F*4 4*F* 7*E* *D*4
40 *C*1 1*F* *F*0 06 0*F* 24 98	*EF* 5*D* 39 19 84 84 3*D* *A*1	*BB* *B*8 05 *DA* 36 24 73 0*A*	53 55 52 *BF* 5*E* 75 15 4*A*	0*C* 9*F* 0*B* *CF* *C*0 6*B* 9*A* *B*8
0*E* 8*F* 51 8*C* 38 41 56 *CA*	53 7*F* 73 50 11 36 34 *C*5	49 4*A* *F*7 28 *C*4 *D*6 81 *F*8	44 42 45 *A*8 49 62 02 5*D*	35 *A*0 2*E* 60 27 8*C* 17 37
02 81 82 74 84 11 *A*1 8*E*	*FF* *D*3 *E*1 39 71 1*C* 50 14	66 65 *D*8 07 *EB* *F*9 *AE* *D*7	54 52 55 *B*8 59 72 12 4*D*	02 6*B* *BF* *EF* *FE* 5*F* *F*4 66
00 81 16 20 0*E* 05 8*D* 96	4*A* 3*E* *DB* 03 *C*1 44 *CD* 1*B*	5*F* 5*C* *E*1 3*E* *D*2 *C*0 97 *EE*	63 65 62 8*F* 6*E* 45 25 7*A*	60 *F*3 97 23 0*C* *F*7 6*E* *AC*

$\mathbf{Bq}'_1$	$\mathbf{C}(\mathbf{Bk}_1)$	$\mathbf{D}(\mathbf{Bk}_1)$	$\mathbf{Bk}_1$	$\mathbf{Bq}_1$
1*E* 9*C* *BE* 79 *FF* *C*4 1*C* *C*2	50 *D*1 0*F* *E*0 16 1*F* 34 88	1*C* 9*F* 9*C* 6*A* 9*A* 0*F* *BF* 90	*B*4 12 *F*3 *B*6 *BC* *F*0 55 *F*8	53 30 74 4*F* *AF* *CA* *AA* *EA*
AD 44 46 7*A* 87 *AF* 87 *DB*	*D*1 50 8*E* 61 97 9*E* *B*5 09	9*D* 1*E* 1*D* *EB* 1*B* 8*E* 3*E* 11	*D*4 *F*2 11 *D*6 *DC* *D*0 37 18	84 4*C* *F*6 38 *D*3 *FD* 61 67
57 *C*5 3*E* 8*D* *DE* 02 8*B* 7*B*	0*F* 8*E* 50 *BF* 49 40 6*B* *D*7	0*A* 89 8*A* 7*C* 8*C* 19 *A*9 86	45 25 06 *C*3 3*D* 47 *E*2 11	97 *EB* 40 27 13 68 *AA* 78
DA *B*5 *D*5 11 1*A* 29 24 4*D*	*D*2 53 8*D* 62 94 9*D* *B*6 0*A*	3*C* *BF* *BC* 4*A* *BA* 2*F* 9*F* *B*0	16 74 51 58 1*A* 4*E* *F*7 5*A*	*F*1 2*B* 4*A* *A*9 20 70 36 *BB*
BB 3*B* 31 *B*8 42 *F*6 *B*3 *F*1	66 *E*7 39 *D*6 20 29 02 *BE*	12 91 92 64 94 01 *B*1 9*E*	94 76 *E*7 *F*2 0*C* 48 71 *E*0	8*F* 70 15 3*A* 50 41 08 49
92 90 50 3*C* 50 03 79 46	1*F* 9*E* 40 *AF* 59 50 7*B* *C*7	19 9*A* 99 6*F* 9*F* 0*A* *BA* 95	26 44 *C*7 20 9*A* 86 01 *D*2	*C*2 63 *C*8 *D*0 02 *C*8 30 5*E*
FF *BD* 22 3*C* *F*3 6*C* *E*5 00	08 89 57 *B*8 4*E* 47 6*C* *D*0	91 12 11 *E*7 17 82 32 1*D*	97 *B*7 66 *B*1 17 05 7*A* 53	94 *F*3 06 *F*9 8*E* 82 *BE* *E*1
AA *B*2 64 46 *DB* 38 *AE* 39	94 15 *CB* 24 *D*2 *DB* *F*0 4*C*	8*A* 09 0*A* *FC* 0*C* 99 29 06	4*A* 2*C* 01 *A*8 46 62 *E*7 06	*F*4 5*F* 73 0*E* 1*B* 9*F* 0*A* *B*5

Fonte: Próprio Autor.

Tabela 5.13: *Progresso da cifragem, estágios (II) a (IV), dos quatro blocos. As linhas de cada bloco são apresentadas como uma sequência de dois dígitos em hexadecimal. Em sequência são apresentados:* $\mathbf{B}_{(n-1)}$*, o bloco anterior;* $\mathbf{B}_{(n)}$*, o bloco da imagem a ser cifrado;* $\mathbf{Bk}'_{(n)}$ *e* $\mathbf{Bk}_{(n)}$*, os blocos construídos com a expansão da chave;* $\mathbf{Bq}_{(n)}$*, o bloco obtido após as Equações (5.2) e (5.3); e,* $\mathbf{Bq}^{a}_{(n)}$*, bloco ao qual foi aplicada uma GFrFT de parâmetro fracional* a*.*

$B_{(0)}$	$B_{(1)}$	$Bk'_{(1)}$	$Bk_{(1)}$	$Bq_{(1)}$	$Bq^{32/64}_{(1)}$
81 82 3F E0 0C 1E 49 30	EF2D0EAC0F1DEFEE	B0 ED 8D 2D FC C1 76 E4	B4 12 F3 B6 BC F0 55 F8	53 30 74 4F AF CA AA EA	BA 3E C9 14 02 21 FA 38
1D 1E A3 18 70 82 AD 94	54 6B 34 83 1F 8E 9C 4F	64 CF AF DF 18 A3 56 00	D4 F2 11 D6 DC D0 37 18	84 4C F6 38 D3 FD 61 67	2A 57 04 E1 97 FD FC 38
05 03 04 E9 08 23 43 1C	EB C0 B6 76 B7 F7 57 F8	69 02 8C EE 1F 2E 77 97	45 25 06 C3 3D 47 E2 11	97 EB 40 27 13 68 AA 78	1D 53 F4 96 BE 82 D6 9C
01 02 2C 40 1C 0B 1B 2C	A3 40 62 9E 3A D1 BD 55	38 73 87 33 F4 4F 7E D4	16 74 51 58 1A 4E F7 5A	F1 2B 4A A9 20 70 36 BB	D3 37 01 13 E3 C1 40 46
40 C1 1F F0 06 0F 24 98	EF 5D 39 19 84 84 3D A1	0C 9F 0B CF C0 6B 9A B8	94 76 E7 F2 0C 48 71 E0	8F 70 15 3A 50 41 08 49	BD BA 5D 0F A6 52 D0 E9
0E 8F 51 8C 38 41 56 CA	53 7F 73 50 11 36 34 C5	35 A0 2E 60 27 8C 17 37	26 44 C7 20 9A 86 01 D2	C2 63 C8 D0 02 C8 30 5E	CB 40 AB EE 27 F4 03 E2
02 81 82 74 84 11 A1 8E	FF D3 E1 39 71 1C 50 14	02 6B BF EF FE 5F F4 66	97 B7 66 B1 17 05 7A 53	94 F3 06 F9 8E 82 BE E1	14 34 28 78 06 A2 5F 31
00 81 16 20 0E 05 8D 96	4A 3E DB 03 C1 44 CD 1B	60 F3 97 23 0C F7 6E AC	4A 2C 01 A8 46 62 E7 06	F4 5F 73 0E 1B 9F 0A B5	FD 09 0B 85 CD 08 2A CE
$B_{(1)}$	$B_{(2)}$	$Bk'_{(2)}$	$Bk_{(2)}$	$Bq_{(2)}$	$Bq^{16/64}_{(2)}$
BA 3E C9 14 02 21 FA 38	D5 F0 C5 0E 29 ED E6 EF	86 11 19 A7 C6 94 6F 1C	2D 8D FA 81 FC 3E 74 5B	7C 6E E6 56 EF 7F E5 26	AB B2 89 95 BF 35 2A CC
2A 57 04 E1 97 FD FC 38	33 12 09 46 8B 06 52 33	86 11 99 27 46 94 EF 1C	8D 2D 5A 21 5C 9E D4 FB	42 2E FC 50 51 10 35 1A	08 D2 44 9C C9 35 A8 A5
1D 53 F4 96 BE 82 D6 9C	F8 84 DF 61 78 3C EE 36	A2 17 8F 41 E2 94 B9 64	3A 9A 6D 96 6B 29 E3 CC	D4 57 BB 44 81 F9 0A 5E	CD A3 F4 08 74 A3 43 5A
D3 37 01 13 E3 C1 40 46	A9 AE 30 6F C8 66 9B 96	F7 02 88 38 35 03 80 0D	4D ED 9A 61 1C 5E 14 BB	EF 99 52 08 9F C9 2F 56	05 64 A8 B1 57 6F 94 2F
BD BA 5D 0F A6 52 D0 E9	90 E3 F8 97 D6 1D 84 25	5A CF FF 29 5A 54 11 7C	E0 40 B7 CC 31 F3 39 96	1A D2 B0 9A 9D E4 EE 37	B2 E2 63 7B F8 B2 92 81
CB 40 AB EE 27 F4 03 E2	30 E2 A0 BF FC 97 AE 66	77 02 54 6C CD CF A4 29	7E DE 29 52 AF 6D A7 08	37 C2 1D A5 3E 33 F9 57	8A 8A 95 03 6D 49 BB D0
14 34 28 78 06 A2 5F 31	B2 FA 09 36 41 41 E5 0F	5C 67 C7 61 30 B2 05 46	3B 9B 6C 97 6A 28 E2 CD	51 9C 2C 6E DB 5F C2 82	A0 0F 29 9B 2B F0 D9 F9
FD 09 0B 85 CD 08 2A CE	90 47 E4 53 10 20 ED A7	2D A2 84 3C EF 19 C4 D7	DC 7C 8B F0 0D CF 05 AA	43 75 03 87 0E 18 A6 38	24 86 A7 0B 49 B0 84 87
$B_{(2)}$	$B_{(3)}$	$Bk'_{(3)}$	$Bk_{(3)}$	$Bq_{(3)}$	$Bq^{8/64}_{(3)}$
AB B2 89 95 BF 35 2A CC	33 24 6B 2E 59 0B 63 95	34 C4 AB 72 4C 79 00 E1	58 C8 85 C2 A4 45 50 BD	BF B0 89 7A 31 C7 B3 B3	0D 28 8A 6D 60 A7 BC 8D
08 D2 44 9C C9 35 A8 A5	B9 12 6C AF 88 7C 15 41	44 B4 7B A2 1C 89 50 D1	A8 38 C5 02 64 D5 D0 6D	A5 DE AC 4B F8 BC 75 7D	56 22 8F 69 DA B3 AB 9B
CD A3 F4 08 74 A3 43 5A	FA F9 4C 71 B4 9B 3E 44	17 27 60 81 BF D2 33 D6	86 B6 E9 BC CA 99 F6 C1	09 D8 D5 AE D5 42 E9 6F	A9 98 E4 5B 98 06 91 AC
05 64 A8 B1 57 6F 94 2F	70 6A 64 46 95 37 AD 8F	DC 8C 13 CA F4 21 38 A9	5E BE 6B BC AA 4B 5A B3	B2 BC E2 2C 8B 61 3F 19	D5 AF C0 05 93 30 5E 5C
B2 E2 63 7B F8 B2 92 81	FD 95 5D E4 55 DB A5 23	14 A4 8F 5E 2C 59 E8 F9	77 67 E2 E3 83 A4 33 9A	48 60 90 69 A4 14 C0 B4	35 F6 BA 78 A2 31 09 61
8A 8A 95 03 6D 49 BB D0	3F 8C 1E 79 72 1A 47 F5	2D BD B2 6B 55 80 09 E8	5C CC 81 C6 A0 41 4C B9	C4 15 29 AC B9 DB 0A 96	A7 52 DB 8F 20 61 8F B6
A0 0F 29 9B 2B F0 D9 F9	CF 58 C2 2D B4 F5 1A 35	51 21 5A 53 B9 A4 AD 04	65 45 78 AD D9 0A 45 D0	C5 BC E4 3F 4C 63 EE F9	B0 7F 3A 04 E0 5F 12 E6
24 86 A7 0B 49 B0 84 87	BD 75 81 1C 5B 46 35 AA	48 B8 0F 0E 30 05 E4 65	05 95 FA 4D 39 98 05 A2	CA C2 8C 7B 44 E3 16 B7	E4 53 A9 98 BA 45 A6 DE
$B_{(3)}$	$B_{(4)}$	$Bk'_{(4)}$	$Bk_{(4)}$	$Bq_{(4)}$	$Bq^{36/64}_{(4)}$
0D 28 8A 6D 60 A7 BC 8D	91 DB 78 C1 02 C7 81 76	08 2C FA FB D2 2A CD DE	25 BF 38 A3 FC 64 00 AE	CE F6 9E 6D 50 91 B6 02	36 99 0A 46 EE 70 E3 54
56 22 8F 69 DA B3 AB 9B	BC 0A EA BB 02 2F 30 77	4C 28 2E 47 86 2E 61 5A	BF 25 A2 39 E6 7E 9A 34	1F 97 BE A9 6A F7 F1 11	0D 06 D7 94 B7 5F 33 0E
A9 98 E4 5B 98 06 91 AC	84 53 FF A4 6D 79 77 BC	42 06 40 45 68 20 73 54	F8 E2 65 7E A1 B9 5D F3	BE 2B 24 9D 66 52 25 BB	B0 76 77 B4 5A 0E 28 03
D5 AF C0 05 93 30 5E 5C	FD EA A7 1D 67 96 73 95	7E AA 80 85 48 A0 4F 5C	03 99 1E C5 DA 42 26 88	76 D9 45 5D 89 B8 48 01	93 52 0D 77 E4 6D EE 49
35 F6 BA 78 A2 31 09 61	06 82 D8 19 60 FF 5D 76	49 2D 3B 3A 93 2B 4C 5F	75 6F E8 F3 2C 34 D0 7E	BE C6 0F D6 23 FC 79 95	A7 64 4C 79 03 EF 2E D9
A7 52 DB 8F 20 61 8F B6	6F 12 8E D9 9D 03 10 FC	0A 2E F8 FD D0 28 CB DC	A4 3E B9 22 7D E5 81 2F	19 7A 4F FE 2A D0 66 BF	28 C0 A1 03 48 E3 EE E0
B0 7F 3A 04 E0 5F 12 E6	57 1A DB C0 3F 5A 20 26	8A BE F8 0D A0 E8 4B CC	00 9A 1D C6 59 C1 25 8B	C1 F6 00 9B F8 73 94 F5	95 E3 15 5A C9 8D 27 24
E4 53 A9 98 BA 45 A6 DE	4B E1 C2 07 AA 16 35 42	BE 9A BC 39 74 1C 6F E8	DE C4 43 98 07 1F 7B D5	67 E3 D1 D8 45 49 1F 2F	59 29 A0 81 12 C7 00 92

Fonte: Próprio Autor.

5.1.4 Resultados e Análises

Com o propósito de avaliar a segurança do esquema de cifragem de imagens, foram realizados diversos testes, comparando os resultados com os obtidos com o algoritmo AES (*Advanced Encryption Standard*). O modo de operação usado como referência é o CBC (do inglês, *Cipher Block Chaining*), o qual foi projetado de forma que blocos de texto claro repetidos não produzam blocos de texto cifrado idênticos [100, pp. 201]. Apesar da semelhança entre o esquema de cifragem introduzido e o proposto por Lima *et al.* [45], não foi possível realizar uma comparação direta com os resultados apresentados no trabalho [45] com os obtidos com o esquema de cifragem presente, em virtude dos ambientes de simulação serem diferentes. Por exemplo, os *pixels* são codificados como inteiros entre 0 e 255 na presente proposta, enquanto que na proposta de Lima *et al.* [45], os *pixels* são codificados como números complexos.

Os testes foram implementados no ambiente *Matlab*® com imagens em escala de cinza codificadas a 8 *bits por pixels*, e com dimensões 512×512 *pixels*. Foi utilizada uma implementação do AES elaborada por Stepan Matejka e disponível em [103]. No AES, a imagem foi convertida num vetor de comprimento 512^2, para então ser cifrada. As imagens empregadas nos testes são mostradas nas Figuras 5.9(a) a 5.9(d) e podem ser obtidas em [104]. Utilizou-se a GFrFT desenvolvida no Exemplo 4.1, com $a_2 = 64$ e o parâmetro a_1 obtido da seguinte chave secreta de comprimento 256 *bits*,

$$\mathbf{K} = (129\,130\,63\,224\,12\,30\,73\,48\,29\,30\,163\,24\,112\,130\,173\,148\,5\,3\,4\,233\,8\,35\,67\,28\,1\,2\,44\,64\,28\,1\,2\,44).$$

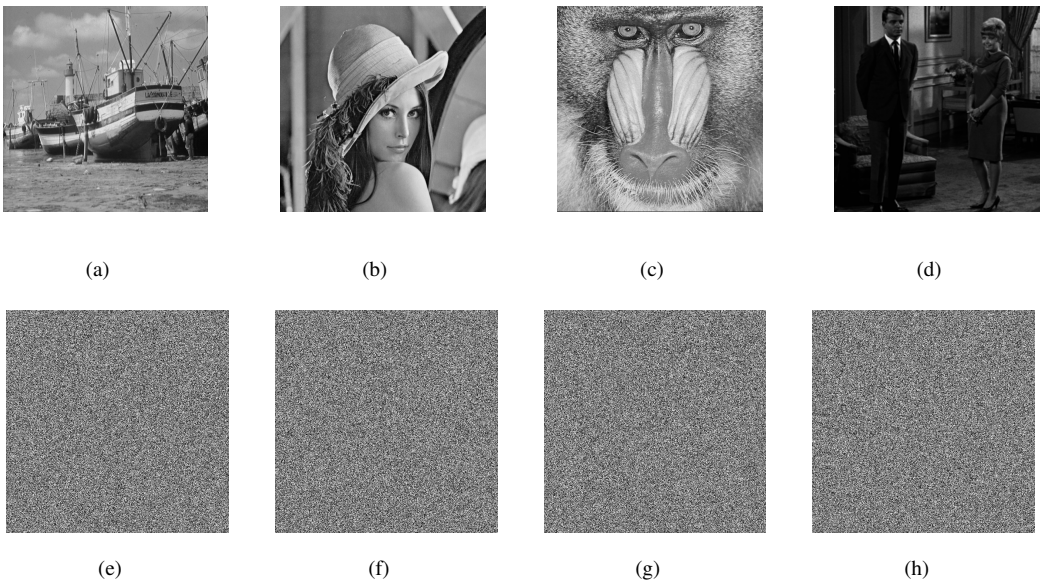
Análise estatística

Nas Figuras 5.9(e) a 5.9(h) são mostradas as imagens cifradas com a chave $\mathbf{K}$. Observa-se que o aspecto visual dessas imagens é completamente ruidoso.

Para que não se extraia informações da imagem original, é desejável que os histogramas das imagens cifradas tenham distribuição uniforme. Na Figura 5.9, os histogramas das imagens originais são mostrados na parte superior (Figuras 5.10(a) a 5.10(d)) e os histogramas das imagens cifradas são mostrados na parte inferior (Figuras 5.10(e) a 5.10(h)). A aplicação da GFrFT leva a uma uniformização dos histogramas, sugerindo que ataques estatísticos podem não ser viáveis.

Uma característica intrínseca de uma imagem digital é a alta correlação entre *pixels* de uma certa vizinhança. Um ataque pode ser desenvolvido explorando essa característica. Para evitá-lo, o esquema de cifragem deve remover tal correlação entre *pixels* adjacentes [105]. Selecionando-se arbitrariamente M *pixels* de uma imagem, o coeficiente de correlação é calculado por [106]

Figura 5.8: *Imagens originais e cifradas, respectivamente, utilizadas nos testes.*



Figuras 5.9(a) e 5.9(e) da ima-gem Boat; figuras 5.9(b) e 5.9(f) da imagem Lenna; figuras 5.9(c) e 5.9(g) da imagem Mandril; figuras 5.9(d) e 5.9(h) da imagem Couple. Fonte: Próprio Autor.

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}, \tag{5.8}$$

em que

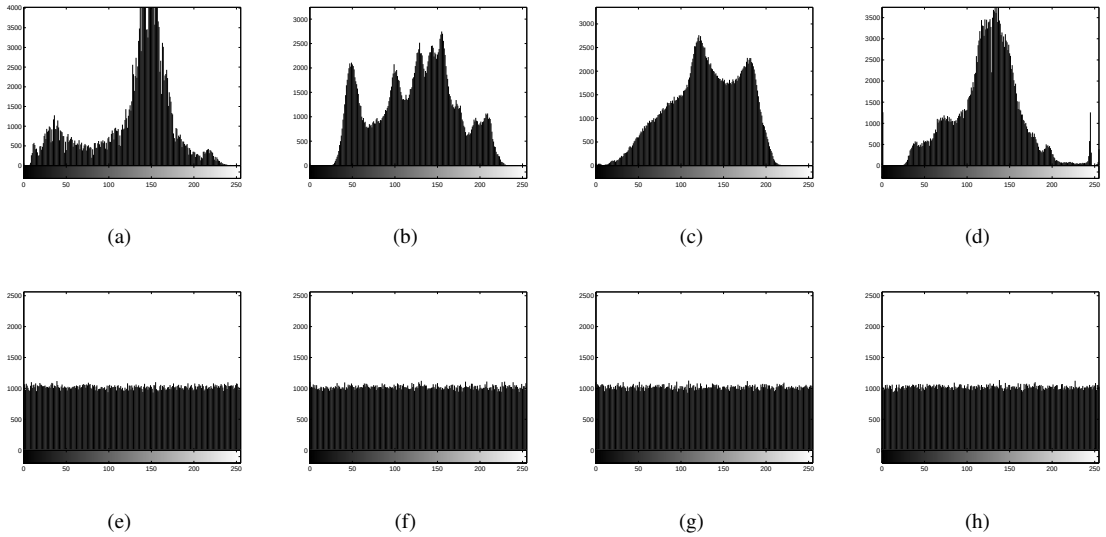
$$\begin{aligned} \mathrm{cov}(x,y) &= \frac{1}{M}\sum_{m=1}^{M}\left[\left(x_m - E(x)\right)\left(y_m - E(y)\right)\right], \\ D(x) &:= \frac{1}{M}\sum_{m=1}^{M}\left(x_m - E(x)\right)^2, \end{aligned}$$

e

$$E(x) := \frac{1}{M}\sum_{n=1}^{M} x_m.$$

Na Tabela 5.14, são apresentados os coeficientes de correlação, r, para as imagens originais e para suas correspondentes imagens cifradas, $\tilde{r}$, com o esquema proposto e, $\hat{r}$, com o AES. Selecionado um *pixel*, é calculado o coeficiente de correlação com *pixels* adjacentes na vertical (r_v), na horizontal (r_h) e em diagonal (r_d). Observa-se que as imagens originais têm altos coeficientes de correlação, próximos a 1, enquanto que os coeficientes de correlação para as imagens cifradas são próximos a 0.

Figura 5.9: *Histogramas das imagens originais e cifradas, respectivamente, obtidos nos testes.*



Figuras 5.10(a) e 5.10(e) da imagem Boat; figuras 5.10(b) e 5.10(f) da imagem Lenna; figuras 5.10(c) e 5.10(g) da imagem Mandril; figuras 5.10(d) e 5.10(h) da imagem Couple. No eixo horizontal estão os possíveis valores dos pixels e no eixo vertical está a quantidade de pixels que assumem determinado valor. Fonte: Próprio Autor.

Análise da entropia da informação

A entropia $H(s)$ de uma fonte de informação s pode ser medida por

$$H(s) \quad := \quad \sum_{i=0}^{M-1} p(s_i) \log_2 \frac{1}{p(s_i)}, \tag{5.9}$$

em que M é o número total de símbolos da fonte, e s_i e $p(s_i)$ representam o i-ésimo símbolo da fonte e sua probabilidade, respectivamente [106]. Para os parâmetros do teste, deseja-se que os valores de entropia estejam próximos a 8 *bits* (máximo teórico), que representa uma fonte com emissão equiprovável de 256 símbolos independentes. A Tabela 5.15 apresenta os resultados de entropia das imagens originais, $\mathbf{I}$, e de suas correspondentes imagens cifradas, $\mathbf{Ic}$, com o esquema proposto e, $\mathbf{Ic}_{AES}$, com o AES. Ela revela que os valores de entropia para as imagens cifradas são mais próximas de 8 *bpp* que os valores de entropia das imagens originais. Isso significa que o presente esquema e o AES são seguros contra ataques de entropia [105].

Resistência ao ataque de texto claro escolhido

No ataque por texto claro escolhido, conhecendo-se a estrutura do sistema e o texto cifrado correspondente, pode-se tentar obter informações sobre a chave [100, pp. 197]. O bloco $\mathbf{B}_n^{a_n}$ é um bloco do texto cifrado, ao qual o atacante tem acesso. Da Equação (5.7), tem-se que

Tabela 5.14: *Coeficientes de correlação, r, para as imagens originais e para suas correspondentes imagens cifradas, $\tilde{r}$, com o esquema proposto e, $\hat{r}$, com o AES. Os índices v, h e d estão relacionados à correlação entre pixels na vertical, na horizontal e na diagonal, respectivamente. Para cada imagem, os coeficientes de correlação são calculados usando 2^{15} pares de pixels aleatoriamente selecionados.*

Imagem	r_h	$\tilde{r}_h$	$\hat{r}_h$	r_v	$\tilde{r}_v$	$\hat{r}_v$	r_d	$\tilde{r}_d$	$\hat{r}_d$
Boat	0,9702	0,0011	0,0012	0,9356	-0,0043	-0,0024	0,9202	0,0040	0,0030
Lenna	0,9844	0,0064	0,0078	0,9692	0,0024	0,0039	0,9567	-0,0026	-0,0047
Mandril	0,7537	0,0053	0,0045	0,8654	0,0023	-0,0049	0,7199	-0,0036	0,0045
Couple	0,8932	0,0090	0,0008	0,9388	0,0087	0,0001	0,8534	0,0082	0,0064

Fonte: Próprio Autor.

Tabela 5.15: *Entropia das imagens originais,* $\mathbf{I}$*, e de suas correspondentes imagens cifradas* $\mathbf{Ic}$*, com o esquema proposto e,* $\mathbf{Ic}_{AES}$*, com o AES. As imagens cifradas apresentam valores de entropia mais próximas do limite teórico de* 8 bpp*, indicando que o esquema de cifragem é seguro contra ataques de entropia.*

Imagem	$\mathbf{I}$	$\mathbf{Ic}$	$\mathbf{Ic}_{AES}$
Boat	7,1914	7,9993	7,9993
Lenna	7,4473	7,9994	7,9994
Mandril	7,3579	7,9992	7,9994
Couple	7,2010	7,9993	7,9993

Fonte: Próprio Autor.

$$\mathbf{Bq}_{(n)} = \mathbf{F}^{a'_{1,n}}\, \mathbf{B}_{(n)}^{a'_{1,n}}\, \mathbf{F}^{a'_{1,n}}. \tag{5.10}$$

Como a' tem 6 *bits*, o atacante tem que testar 64 combinações para encontrar este parâmetro.

O atacante também tem acesso ao bloco cifrado $\mathbf{B}_{(n-1)}$ e ao bloco original $\mathbf{B}_{(n)}$. No estágio de formação de cada bloco $\mathbf{Bq}$, a partir das Equações (5.2) e (5.3) tem-se que

$$\mathbf{Bq}_{(n)} = \Big((\mathbf{B}_{(n)} \oplus \mathbf{B}_{(n-1)}) + \mathbf{Bk}'_{(n)}) \oplus \mathbf{B}_{(n-1)}\Big) + \mathbf{Bk}_{(n)} \pmod{256} \tag{5.11}$$

$$\mathbf{B}_{(n)} = \Big[\Big((\mathbf{Bq}_{(n)} - \mathbf{Bk}_{(n)}) \oplus \mathbf{B}_{(n-1)}\Big) - \mathbf{Bk}'_{(n)}\Big] \oplus \mathbf{B}_{(n-1)}. \tag{5.12}$$

Dessa maneira, o atacante precisa descobrir os blocos $\mathbf{Bk}'_{(n)}$ e $\mathbf{Bk}_{(n)}$ para obter a igualdade. Como cada um desses blocos é formado por 256 *bits* da chave, tem-se 2^{256} possibilidades. No total, tem-se 2^{518} ($2^6 \times 2^{256} \times 2^{256}$) possibilidades, o que inviabiliza este tipo de ataque para descobrir a chave.

Análise do espaço de chaves

Se M é o número de *bits* de uma chave, a cardinalidade do espaço de chaves é 2^M. Embora não se garanta a impossibilidade de um ataque por força bruta, é necessário que um esquema de cifragem tenha um espaço de chaves maior que 2^{100}, pelos padrões de segurança descritos em [105, 107]. Por exemplo, o sistema AES tem comprimento de chave mínimo 128 *bits* e é resistente a ataques de força bruta [100, p. 150].

Como visto, a cada bloco há 2^{518} combinações possíveis para descobrir o bloco $\mathbf{Bq}$, e assim descobrir a chave secreta. Portanto, a cardinalidade do espaço de chaves é 2^{518}, o qual satisfaz aos requisitos gerais para um espaço de chaves "desejável", de forma que, com os atuais recursos computacionais, seja impraticável o ataque por força bruta [108]. O esquema de cifragem AES, por exemplo, é especificado com chaves de comprimentos 128, 192 ou 256 *bits*.

Resistência ao ataque diferencial

Se a diferença entre textos cifrados é constante ou se a diferença entre o texto claro e o texto cifrado apresenta algum padrão, é possível promover um ataque explorando essas características. Em cifras de bloco, por exemplo, pode-se descobrir a chave secreta comparando textos cifrados por meio da criptoanálise diferencial. A eficácia deste tipo de criptoanálise é comprometida quando não se obtém padrões estatísticos entre pares de blocos de textos cifrados diferentemente [100, pp. 90].

No contexto de imagens, pode-se realizar a criptoanálise diferencial cifrando uma imagem e uma versão modificada desta, por exemplo, alterando apenas um *pixel*. A diferença entre essas imagens pode ser mensurada por meio da razão do número de *pixels* modificados (NPCR, do inglês *number of pixels change rate*) [105] e da média unificada da intensidade de modificação (UACI, do inglês *unified average changing intensity*) [106], respectivamente definidas por

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W_1 \times W_2} \times 100\% \tag{5.13}$$

e

$$UACI = \frac{1}{W_1 \times W_2} \left[\sum_{i=0}^{W_1-1} \sum_{j=0}^{W_2-1} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\%, \tag{5.14}$$

em que W_1 e W_2 correspondem ao número de colunas e linhas da imagem cifrada, respectivamente; $C_1(i,j)$ e $C_2(i,j)$ correspondem aos *pixels* da i-ésima linha e j-ésima coluna das imagens cifradas C_1 e C_2, obtidas das imagens original e modificada, respectivamente; enquanto que a matriz $D(i,j)$

é definida por

$$D(i,j) := \begin{cases} 1, & C_1(i,j) = C_2(i,j), \\ 0, & \text{caso contrário}, \end{cases} \tag{5.15}$$

Um valor de NPCR próximo a 100% indica uma grande quantidade de *pixels* modificados, ou seja, indica uma grande diferença entre as imagens C_1 e C_2. Já o valor desejável para a UACI é próximo a $1/3$ [106].

Nos testes, a imagem C_2 foi obtida invertendo-se o *bit* menos significativo de um único *pixel* da imagem original escolhido aleatoriamente. Foram criadas 100 versões modificadas para cada imagem original e computados os valores de NPCR e de UACI de cada imagem gerada. A Tabela 5.16 apresenta os valores médio, máximo e mínimo para as imagens apresentadas nas Figuras 5.9(a) a 5.9(d).

Tabela 5.16: *Valores médio, máximo e mínimo de NPCR e UACI obtidos de um conjunto de 100 imagens. Foram feitas simulações para as imagens apresentadas nas Figuras 5.9(a) a 5.9(d).*

Imagem	Métrica	Proposto			AES		
		Max(%)	Min(%)	Med(%)	Max(%)	Min(%)	Med(%)
Boat	NPCR	99,65	99,58	99,61	99,19	5,91	50,44
	UACI	33,58	33,33	33,46	15,95	1,01	8,47
Lenna	NPCR	99,64	99,57	99,61	98,06	2,00	45,44
	UACI	33,54	30,33	33,44	16,36	0,35	7,61
Mandril	NPCR	99,64	99,58	99,61	96,40	0,16	51,18
	UACI	33,61	33,36	33,45	16,23	0,03	8,62
Couple	NPCR	99,64	99,58	99,61	99,40	5,91	51,58
	UACI	33,52	33,34	33,44	16,47	1,01	8,67

Fonte: Próprio Autor.

Com os resultados, é possível observar a resistência do esquema a um ataque diferencial. Uma pequena modificação na imagem original resulta numa grande mudança na imagem cifrada. Observe que os valores de NPCR estão próximos a 100%, sendo o menor valor obtido $99,57\%$. Já os valores de UACI estão próximos a $33,33\%$. Os resultados obtidos com o AES, baixos valores de NPCR e UACI, mostram que há vulnerabilidades em relação a este tipo de ataque diferencial.

Sensibilidade da Chave

Outra maneira de se avaliar a confusão inserida pelo esquema é analisar quão uma pequena variação da chave influencia na imagem cifrada, ou seja, é avaliar a sensibilidade da chave. Tanto na cifragem quanto na decifragem, uma mudança na chave provoca uma alteração desde o início

do processo. Isso ocorre porque o bloco padrão com o qual se inicia tanto a cifragem quanto a decifragem depende da chave. Dessa maneira, espera-se que o esquema seja "sensível" a mudanças na chave.

Nos testes, tenta-se obter as imagens originais decifrando-se imagens cifradas com chaves "minimamente" diferentes das corretas. Para tanto, seja $\hat{\mathbf{K}}$ uma chave incorreta que difere da chave correta somente em um *bit*. A chave incorreta, que difere da original apenas no *bit* menos significativo, é

$\hat{\mathbf{K}} = (129\,130\,63\,224\,12\,30\,73\,48\,29\,30\,163\,24\,112\,130\,173\,148\,5\,3\,4\,233\,8\,35\,67\,28\,1\,2\,44\,64\,28\,1\,2\,\underline{43})$.

Observe que o valor na posição destacada é 43, enquanto que na chave correta é 44. As imagens cifradas com a chave $\mathbf{K}$, mostradas nas Figuras 5.9(e) a 5.9(h), foram decifradas com cinco chaves incorretas $\hat{\mathbf{K}}$ e os resultados da NPCR e UACI entre a imagem original e cada uma das cinco imagens decifradas foram obtidos. A Tabela 5.17 apresenta os valores médio, máximo e mínimo para as imagens decifradas com 6 chaves modificadas, que diferem da original em 1 *bit* em posições aleatoriamente selecionadas.

Tabela 5.17: *Valores médio, máximo e mínimo de NPCR e UACI obtidos de um conjunto de 6 imagens decifradas com chaves diferentes da chave de cifragem. A diferença consiste na alteração de 1* bit*, selecionado aleatoriamente, em cada chave. Foram feitas simulações para as imagens apresentadas nas Figuras 5.9(a) a 5.9(d).*

Imagem	Métrica	Proposto			AES		
		Max(%)	Min(%)	Med(%)	Max(%)	Min(%)	Med(%)
Boat	NPCR	99,62	99,59	99,60	99,63	99,59	99,61
	UACI	28,49	27,78	28,12	28,46	27,82	28,15
Lenna	NPCR	99,63	99,59	99,61	98,62	99,59	99,61
	UACI	28,68	28,57	28,64	28,66	28,57	28,62
Mandril	NPCR	99,62	99,59	99,61	96,63	99,60	99,61
	UACI	27,87	27,78	27,82	27,89	27,77	27,83
Couple	NPCR	99,62	99,59	99,60	99,63	99,59	99,61
	UACI	27,59	27,56	27,58	27,64	27,56	27,61

Fonte: Próprio Autor.

Esses resultados indicam que o esquema proposto e o AES são sensíveis a mínimas variações da chave, o que inviabiliza ataques diferenciais sobre a chave.

Complexidade computacional

Não foi possível efetuar uma comparação de tempo requerido para cifragem e decifragem das imagens com o esquema proposto e o AES. A implementação do AES foi obtida de terceiros [103].

Dessa maneira, não pode ser considerada que esta implementação seja a que requer menor custo computacional.

A complexidade aritmética das transformadas representa a parte mais importante no custo computacional do sistema proposto. As imagens de teste têm dimensão 512×512 e seus blocos têm dimensão 8×8, formando 4096 blocos. Como cada GFrFT é aplicada recursivamente no correspondente bloco até que o valor máximo de qualquer de seus *pixels* seja menor ou igual a 255, não há uma expressão fechada para se computar a complexidade aritmética dada uma imagem arbitrária.

Nesse cenário, é importante computar o número de vezes que a GFrFT é aplicada recursivamente aos blocos de forma a manter os valores de *pixels* entre 0 e 255. O número máximo de GFrFT aplicadas recursivamente ocorreu para a imagem apresentada na Figura 5.9(b), exatamente 5316 vezes, em que a GFrFT foi aplicada 6 vezes em três blocos, 5 vezes em seis blocos, 4 vezes em trinta e oito blocos, 3 vezes em 171 blocos, 2 vezes em 725 blocos.

Para analisar a redução da complexidade computacional, foi implementado um esquema de cifragem com sobreposição de blocos, similar ao introduzido em [101] mas que utiliza a FFCT ao invés da matriz da GFrFT. Considerando a superposição de uma coluna e uma linha, para uma imagem de 512×512 *pixels* o número total de blocos a serem processados é 10752. Avaliando a complexidade aritmética associada à imagem apresentada na Figura 5.9(b), verificou-se que o número de vezes em que a GFrFT foi aplicada foi de 13821 vezes. Comparando com o esquema proposto na tese com o esquema com sobreposição, há uma redução de aproximadamente 62% do número de multiplicações matriciais.

Um aspecto importante no uso dessas transformadas é a existência de algoritmos rápidos e cálculos em aritmética inteira, que contribuem para a diminuição do custo computacional do esquema. Como visto na Seção 4.4, para computar uma GFrFT são necessárias $M'(N) = N\log_2(N)/2 + 4N$ multiplicações e $A'(N) = N\log_2(N) + 3N$ adições. Assim, como cada bloco requer 44 multiplicações e 48 adições, são necessárias 233.904 multiplicações e 255.168 adições para a cifragem da imagem apresentada na Figura 5.9(b). É possível reduzir esta complexidade usando-se a GFrHT, GFrST ou a GFrCT no lugar da GFrFT.

5.2 Marca d'água no domínio fracional

Desde o início do século XXI, a distribuição, o compartilhamento e comercialização de imagens digitais crescem aliados ao desenvolvimento de novas tecnologias de produção e comunicação. Um ponto negativo é que ações ilegais se valem dessas tecnologias para alterar imagens, colocando em

risco a integridade e autenticidade das mesmas. Apoiado no crescimento da rede mundial de computadores (*Internet*), a distribuição e comercialização de cópias ilegais de conteúdo protegidas por direitos autorais é um elemento de forte tensão na sociedade. A técnica de marca d'água digital emergiu para proteção de conteúdo. Assinaturas ou logomarcas visivelmente inseridas constituem um exemplo de marca d'água, contudo a conjunção desta com a esteganografia permite a inserção de informações sem alterar visivelmente a imagem [109].

Aspectos desejáveis às técnicas de marca d'água são a robustez (resistência a ataques que se propõem a destruí-la), transparência (não degradação visual da imagem original), detecção de alteração e segurança. Em relação à robustez, as técnicas de marca d'água podem ser classificadas como: robusta, frágil e semi-frágil.

Sistemas robustos devem ser capazes de sobreviver a uma vasta gama de manipulações e são aplicados para garantir a autoria, enquanto que sistemas frágeis tem por objetivo garantir a integridade de conteúdo, identificando adulterações da imagem. Por serem sensíveis a mínimas manipulações, sistemas frágeis podem ser usados para autenticação [110]. Sistemas semi-frágeis mesclam características de sistemas robustos e frágeis, sendo usados para identificação de alteração em certos locais da imagem [111].

O domínio em que as imagens são processadas é outro critério para classificar as técnicas de marca d'água: o domínio espacial e da frequência. Uma parte significativa dos sistemas que trabalham no domínio espacial insere a marca no *bit* menos significativo (LSB, do inglês *least significant bit*) de cada *pixel* da imagem.

No domínio da frequência, a marcação é feita nos coeficientes da transformada. No uso das transformadas discretas como a DFT [112], a DCT [113] e a DWT (*Discrete Wavelet Transform*) [114, 115] deve ser levado em consideração o custo computacional e a precisão para calcular tais transformadas em aritmética de ponto flutuante. Abordagens que usam as transformadas digitais como a FFFT e a FFCT se valem da aritmética inteira para reduzir tais problemas. Aoki *et al.* [116] propuseram um sistema de marca d'água frágil no domínio da frequência usando a FFFT para autenticação com capacidade de detecção de adulteração local.

Baseado nessa proposta, Cintra *et al.* [117] introduziram um sistema aplicado à autenticação e detecção de adulteração de imagens no domínio da frequência usando a FFHT e a FFCT tipo 2. Como este esquema utiliza um ferramental definido numa estrutura algébrica finita (cálculos são realizados com aritmética inteira), a inserção e a extração da marca d'água são precisas e, tanto a imagem original quanto a marca, são exatamente recuperadas. Outra proposta também baseada em

aritmética inteira foi feita por Lima *et al.* [118].

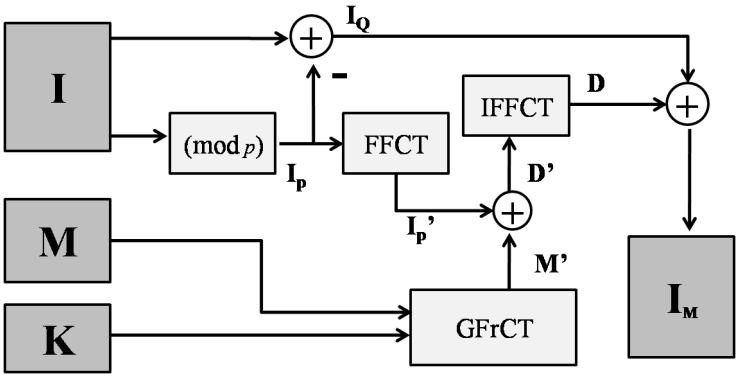
A seguir, é apresentado um sistema de marca d'água frágil baseado na transformada fracional do cosseno de corpo finito. Após a apresentação dos esquemas de inserção e extração da marca o desempenho do sistema é avaliado a partir dos resultados de testes realizados.

5.2.1 Esquema de inserção da marca

O esquema foi projetado para imagens em escala de cinza, codificadas a 8 *bpp*, contudo pode ser estendido a imagens coloridas. Uma imagem colorida pode ser representada pela concatenação de três imagens em escala de cinza, em que cada imagem representa a intensidade de cada cor fundamental da representação. A marca é uma imagem binária, isto é, cada *pixel* só assume os valores 0 ou 1.

Denote por $\mathbf{I}$ a imagem original a ser marcada, por $\mathbf{I}_p$ uma imagem de resíduos obtida pela redução módulo p do valor de cada *pixel* de $\mathbf{I}$, e por $\mathbf{I}_Q$ uma imagem em que o valor de cada *pixel* é múltiplo de p, de forma que $\mathbf{I} = \mathbf{I}_p + \mathbf{I}_Q$. Denote por $\mathbf{M}$ a marca, imagem a ser inserida em $\mathbf{I}$. O diagrama em blocos da Figura 5.10 resume o esquema de inserção da marca $\mathbf{M}$ numa imagem $\mathbf{I}$.

Figura 5.10: *Diagrama em blocos do esquema de inserção da marca d'água no domínio fracional usando a GFrCT.*



São obtidas as imagens $\mathbf{I}_Q$ e $\mathbf{I}_p$ a partir da imagem $\mathbf{I}$. À imagem $\mathbf{I}_p$ é aplicada a FFCT bidimensional, resultando em $\mathbf{I}'_p$. A marca $\mathbf{M}$ e a chave $\mathbf{K}$ são combinadas usando-se uma GFrCT, resultando em $\mathbf{M}'$. As imagens $\mathbf{M}'$ e $\mathbf{I}'_p$ são somadas, e é aplicada a FFCT inversa resultando em $\mathbf{D}$. As imagens $\mathbf{D}$ e $\mathbf{I}_Q$ são somadas resultando na imagem com a marca, $\mathbf{I}_M$.
Fonte: Próprio Autor.

Inicialmente, devem ser obtidas as imagens $\mathbf{I}_p$ e $\mathbf{I}_Q$. Para que a inserção da marca não degrade a imagem marcada, uma "boa escolha" de p é fundamental. Espera-se que a marca d'água seja transparente, portanto o intervalo de valores de $\mathbf{I}_Q$ não deve ser grande, uma vez que $\mathbf{I}_Q$ é alterada pela marca d'água. De acordo com a Figura 5.11, que apresenta imagens marcadas para diferentes valores de p,

quanto maiores forem os valores de p, maior é a distorção na imagem marcada. A alteração de *bits* menos significativos refletem numa pequena alteração visual da imagem. Por exemplo, para $p = 7$, no máximo os três últimos *bits* dos *pixels* da imagem marcada podem diferir da imagem original. Já para, para $p = 79$, os cinco últimos *bits* dos *pixels* da imagem marcada podem diferir da imagem original.

Figura 5.11: *Imagens marcadas usando uma FFCT com diferentes valores de p, em que as operações são realizadas em* $\mathrm{GF}(p)$.

(a) Imagem original. (b) Imagem marcada em GF(7). (c) Imagem marcada em GF(11).

(d) Imagem marcada em GF(13). (e) Imagem marcada em GF(23). (f) Imagem marcada em GF(31).

(g) Imagem marcada em GF(47). (h) Imagem marcada em GF(53). (i) Imagem marcada em GF(79).

A degradação visual da imagem aumenta com o aumento do valor de p utilizado. Fonte: Próprio Autor.

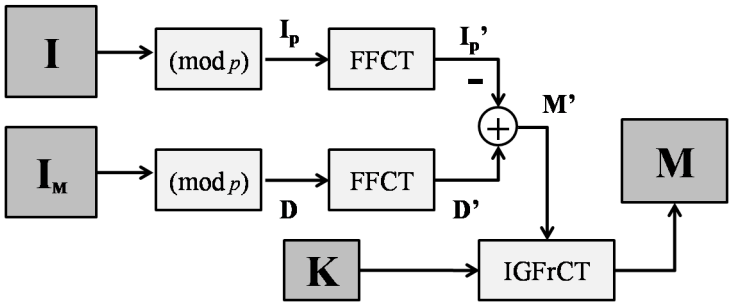
Para se obter o espectro da imagem, é necessário dividir cada imagem em blocos $N \times N$. Os espectros da imagem $\mathbf{I}_p$ e da imagem $\mathbf{M}$, denotados por $\mathbf{I}'_p$ e $\mathbf{M}'$, respectivamente, são obtidos através da aplicação de uma FFCT e de uma GFrCT bidimensionais, respectivamente, em cada bloco da imagem. Cada bloco de $\mathbf{M}'$ é obtido por uma GFrCT cujo parâmetro fracional é um elemento

específico da chave $\mathbf{K}$. Logo em seguida, os espectros $\mathbf{I}'_p$ e $\mathbf{M}'$ são somados, formando-se uma imagem $\mathbf{D}'$. Os elementos de $\mathbf{D}'$ pertencem a $\mathrm{GI}(p)$, em virtude dos elementos de $\mathbf{M}'$. Assim, $\mathbf{I}'_p$ pode ser obtida usando uma FFCT de elementos em $\mathrm{GI}(p)$. Na sequência, a imagem $\mathbf{D}'$ é submetida a uma FFCT bidimensional inversa gerando a imagem $\mathbf{D}$. Por fim, a imagem marcada $\mathbf{I}_M$ é obtida pela soma das imagens $\mathbf{D}$ e $\mathbf{I}_Q$.

5.2.2 Esquema de extração da marca

Para a extração da marca, é necessário possuir a chave $\mathbf{K}$ e a imagem original $\mathbf{I}$. O diagrama em blocos da Figura 5.12 resume o esquema de extração da marca $\mathbf{M}$ de uma imagem marcada $\mathbf{I}_M$.

Figura 5.12: *Diagrama em blocos do esquema de extração da marca d'água no domínio fracional usando uma GFrCT.*



Conhecidas as imagens original e marcada, a marca $\mathbf{M}$ *é obtida a partir do processo inverso ao apresentado na Figura 5.10.* Fonte: Próprio Autor.

As imagens $\mathbf{D}$ e $\mathbf{I}_p$ são obtidas pela redução módulo p das imagens $\mathbf{I}_M$ e $\mathbf{I}$, respectivamente. Em seguida, são calculados os espectros de $\mathbf{D}$ e $\mathbf{I}_p$ por meio de uma FFCT bidimensional, denotados por $\mathbf{D}'$ e $\mathbf{I}'_p$, respectivamente. Da subtração de $\mathbf{D}'$ por $\mathbf{I}'_p$ obtem-se $\mathbf{M}'$, o espectro fracional da marca $\mathbf{M}$. Ao se usar a GFrCT inversa, é necessário ter conhecimento da chave, pois cada elemento da chave é um parâmetro fracional com o qual se constrói as matrizes de transformação para cada bloco de $\mathbf{M}'$.

5.2.3 Resultados e Análises

Os testes foram realizados em *Matlab*® para uma imagem de dimensão 256×256 e uma imagem binária de dimensões 64×64 foi usada como marca. Na Figura 5.13 são mostradas a imagem original (Figura 5.13(a)), a marca d'água (Figura 5.13(b)) e a imagem marcada (Figura 5.13(c)) com o esquema proposto. Diferenças visuais entre as imagens da Figura 5.13(a) e da Figura 5.13(b) não são verificadas.

Figura 5.13: *Comparação entre a imagem original e a imagem com marca d'água.*

(a) (b) (c)

Figura 5.13(a) imagem original, 256×256 *pixels; Figura 5.13(b) marca d'água ampliada,* 64×64 *pixels; Figura 5.13(c) imagem marcada,* 256×256 *pixels. Por uma inspeção visual, não se verifica diferenças visuais significativas entre as imagens.* Fonte: Próprio Autor.

A PSNR, medida em dB, entre as duas imagens, $\mathbf{I}_1$ e $\mathbf{I}_2$, é

$$\begin{aligned} PSNR &= 10\log_{10}\left(\frac{255^2}{MSE^2}\right), \\ MSE &= \frac{1}{W_1 \times W_2}\sum_{i=0}^{W_1-1}\sum_{j=0}^{W_2-1}[I_1(i,j) - I_2(i,j)]^2, \end{aligned} \tag{5.16}$$

em que W_1 e W_2 correspondem ao número de colunas e linhas das imagens, respectivamente.

Considerando que as imagens têm dimensões $N_1 \times N_2$, é analisada a relação sinal-ruído de pico (PSNR, do inglês *peak signal-to-noise ratio*) entre as imagens originais $\mathbf{I}$ e marcada $\mathbf{I}_M$. Com a PSNR tem-se uma métrica objetiva para avaliar distorções introduzidas em imagens digitais.

Neste caso, quanto maior for o valor da PSNR menor é diferença entre as imagens. A PSNR obtida com as imagens da Figura 5.13 foi $41,30$ dB, indicando que mesmo com a inserção da marca as imagens são semelhantes. Para efeito de comparação, compactando essa imagem com o padrão JPG, a PSNR obtida é de $37,40$ dB.

Apesar de ser um sistema com marca d'água frágil, deseja-se que o sistema seja robusto a alguns tipos de manipulações. Em outras palavras, é desejável que a marca d'água possa ser recuperada mesmo havendo algumas degradações na imagem marcada. A imagem marcada foi alterada de três maneiras diferentes para avaliar a robustez do esquema. Novamente, a PSNR é usada para avaliar a diferença entre a marca original e a extraída. Além do sistema proposto, foram avaliados também o sistema introduzidos por Cintra *et al.* [117] e por Lima *et al.* [118].

Na primeira bateria de testes, os *pixels* da imagem marcada foram alterados aleatoriamente com probabilidade 10^{-3}, Figura 5.14(a). A alteração consistiu em incrementar em uma unidade o valor do *pixel*.] A PSNR obtida foi $50,30$ dB para o sistema de Cintra, Figura 5.14(c), e $65,05$ dB para

Tabela 5.18: *Valores da PSNR (dB) entre a marca d'água original e a marca d'água extraída segundo o esquema proposto, o esquema de Cintra* et al. *[117] e o esquema de Lima* et al. *[118]. Na* 1^a *bateria de testes, os* pixels *da imagem marcada foram incrementados em uma unidade aleatoriamente com probabilidade* 10^{-3}*, e a marca foi extraída desta imagem modificada. A marca extraída é igual à original com o esquema proposto, pois o valor da PSNR é* ∞*. Os valores da PSNR para os outros esquemas indicam que as marcas extraídas são semelhantes à original. Na* 2^a *bateria de testes, uma região da imagem marcada teve os valores de seus* pixels *zerados, e a marca foi extraída desta imagem modificada. A marca extraída é igual à original com o esquema proposto, pois o valor da PSNR é* ∞*. Os valores da PSNR para os outros esquemas indicam que as marcas extraídas são semelhantes à original. Na* 3^a *bateria de testes, todos os* pixels *da imagem marcada tiveram seus valores incrementados em uma unidade, exceto para valores iguais a* 255*, e a marca foi extraída desta imagem modificada. Os valores da PSNR para os três esquemas indicam que as marcas extraídas são semelhantes à original.*

Teste	Proposto	Cintra	Lima
1^a bateria	∞	$50,30$ dB	$65,05$ dB
2^a bateria	∞	$46,29$ dB	$62,17$ dB
3^a bateria	$61,91$ dB	$53,54$ dB	$66,23$ dB

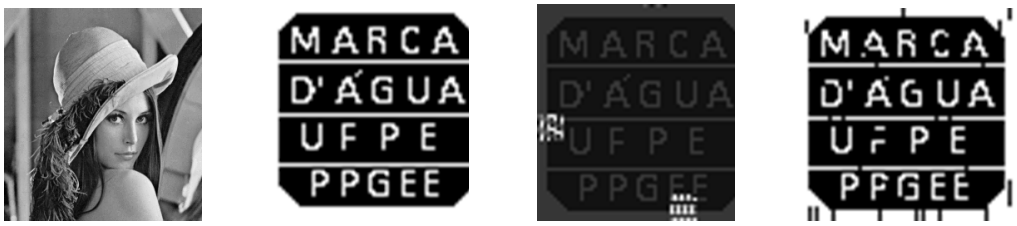
Fonte: Próprio Autor.

o sistema de Lima, Figura 5.14(d). Para o sistema proposto o valor da PSNR foi infinito, indicando que as imagens são exatamente iguais, Figura 5.14(b).

Na segunda bateria de testes, uma região da imagem marcada teve os valores de seus *pixels* zerados, Figura 5.15(a). A PSNR obtida foi $46,29$ dB para o sistema de Cintra, Figura 5.15(c), e $62,17$ dB para o sistema de Lima, Figura 5.15(d). Para o sistema proposto o valor da PSNR foi infinito, indicando que as imagens são exatamente iguais, Figura 5.15(b).

Na terceira bateria de testes, todos os *pixels* da imagem marcada tiveram seus valores incrementados em 1 unidade, exceto para valores iguais a 255, Figura 5.16(a). A PSNR obtida foi de $53,54$ dB para o sistema proposto, Figura 5.16(b), $66,23$ dB para o sistema de Cintra, Figura 5.16(c), e 61.91 dB para o sistema de Lima, Figura 5.16(d). Uma inspeção visual indica que a imagem da marca d'água recuperada com o sistema proposto foi degradada, conforme se observa na Figura 5.16(b).

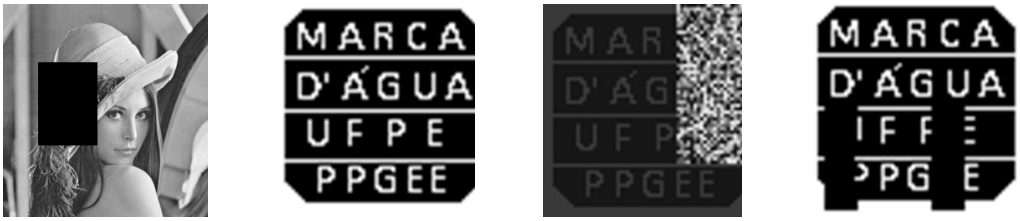
Figura 5.14: *Marca d'água extraída de uma imagem marcada alterada, Figura 5.14(a), de acordo com a primeira bateria de testes.*



(a) (b) (c) (d)

Na Figura 5.14(b) está a marca d'água extraída segundo o sistema proposto, na Figura 5.14(c) segundo o sistema de Cintra, e na Figura 5.14(d) segundo o sistema de Lima. Fonte: Próprio Autor.

Figura 5.15: *Marca d'água extraída de uma imagem marcada alterada, Figura 5.15(a), de acordo com a segunda bateria de testes.*



(a) (b) (c) (d)

Na Figura 5.15(b) está a marca d'água extraída segundo o sistema proposto, na Figura 5.15(c) segundo o sistema de Cintra, e na Figura 5.15(d) segundo o sistema de Lima. Fonte: Próprio Autor.

Figura 5.16: *Marca d'água extraída de uma imagem marcada alterada, Figura 5.16(a), de acordo com a terceira bateria de testes.*

(a) (b) (c) (d)

Na Figura 5.16(b) está a marca d'água extraída segundo o sistema proposto, na Figura 5.16(c) segundo o sistema de Cintra, e na Figura 5.16(d) segundo o sistema de Lima. Uma inspeção visual indica que a imagem da marca d'água recuperada com o sistema proposto foi significativamente degradada, conforme se observa na Figura 5.16(b). Fonte: Próprio Autor.

O sistema de marca d'água frágil apresentado mostrou um desempenho superior às propostas de Cintra e Lima. Alguns tipos de manipulações na imagem que diminuíam a eficiência dos demais sistemas não alteraram a eficiência do sistema proposto, como é o caso de introdução de ruído e alteração em certos locais da imagem. Com o emprego das transformadas fracionais em corpos finitos é possível se obter um sistema de baixa complexidade computacional. É possível também associar uma chave secreta para a extração da marca. Neste caso, mesmo em posse da imagem original, a marca só é extraída por pessoas autorizadas.

5.3 Comunicação Multiusuário

Sistemas de comunicação multiusuário têm por objetivo o aumentar a eficiência dos recursos dos sistemas de comunicações, isto é, o aumento das taxas de transmissão de dados dos usuários [119–122] para as faixas de frequências disponíveis para comunicação. O compartilhamento de recursos, especialmente da largura de banda, pode ser feito por meio de sistemas de acesso múltiplo. A banda total disponível para um sistema pode ser dividida em canais, e a cada usuário deste sistema pode ser atribuído um canal individual. No sistema de acesso múltiplo por divisão de frequência (FDMA, do inglês *frequency division multiple access*), há um compartilhamento do meio de comunicação por meio da divisão em canais. Enquanto o canal estiver alocado para um usuário, nenhum outro usuário pode usar esta faixa de frequências. Ao invés de dividir a banda total em canais, pode-se aumentar o número de usuários, por exemplo, com o sistema de acesso múltiplo por divisão de tempo (TDMA, do inglês *time division multiple access*) ou com o sistema de acesso múltiplo por divisão de código (CDMA, do inglês *code division multiple access*).

No sistema CDMA, os usuários enviam mensagens ao mesmo tempo e nas mesmas faixas de frequência. As mensagens dos usuários são sequências ortogonais, isto é, o produto escalar com sequências de outros usuários é zero. A partir de uma sequência de referência para cada usuário, é possível separar e recuperar todas as mensagens transmitidas de cada usuário.

De maneira similar ao sistema CDMA, foram desenvolvidos sistemas de comunicação em que as mensagens dos usuários são construídas a partir de autovetores de transformadas discretas. Para estes sistemas, cada autovetor pertence a um único autoespaço, isto é, está associado a um único autovalor. O número de autovalores distintos das matrizes de transformação dessas transformadas, portanto, é o limite do número de usuários distintos do sistema.

Em um sistema proposto por Campello de Souza *et al.* [41], os autovetores da DFT são utilizados como mensagens de usuários transmitidas através de um canal real aditivo (RAC, do inglês *Real*

Adder Channel). Nesse esquema, como um autovetor pertence a somente um autoespaço, no receptor as mensagens dos usuários podem ser separadas através de sucessivas aplicações da DFT. Esse sistema suporta até quatro usuários, pois a DFT tem apenas quatro autovalores distintos. Por se tratar de um esquema multiusuário, com essa proposta, é possível aumentar a taxa de transmissão, além de tornar mais eficiente o uso do espectro eletromagnético [123].

Para conceber um sistema com mais de quatro usuários, é necessário utilizar outras transformadas discretas. As transformadas discretas do cosseno tipos 2 e 3 emergem como alternativas, pois o número de seus autovalores distintos depende das dimensões das matrizes de transformação [124]. Apesar de haver um procedimento sistemático para obtenção dos autovetores e autovalores das matrizes de transformação dessas transformadas, não há uma fórmula fechada para determinar o número de autovalores e, com isso, construir os autovetores ortogonais para um comprimento arbitrário.

Em [42], Lima *et al.* propuseram a utilização da transformada discreta fracional de Fourier (DFrFT) num esquema de comunicação para oito usuários. A matriz de transformação de uma DFrFT de comprimento N pode ter até N autovalores distintos, o que indica a flexibilidade desta transformada nesse tipo de aplicação. Para a DFrFT, há inúmeras propostas de determinação de autovalores e construção de conjuntos de autovetores [125]. Contudo, para este esquema de oito usuários, é necessário usar matrizes de transformação de dimensão 9×9, ou seja, as sequências devem ter comprimento nove.

A complexidade computacional para se calcular as transformadas discretas é um fator importante que pode limitar suas aplicações. Outro aspecto está relacionado à precisão nos cálculos, que fica comprometida devido à necessidade de arredondamentos e ao uso de aritmética de ponto flutuante. Esses problemas estão associados à estrutura algébrica na qual os cálculos são realizados.

Como já pontuado no decorrer desta tese, em corpos finitos a precisão é garantida e os cálculos podem ser realizados com menor custo computacional. Nesta Seção, é proposto um esquema multiusuário baseado nas transformadas fracionais em corpos finitos.

Inicialmente, é formado um dicionário de mensagens para cada usuário, e cada mensagem está associada a uma constante. Uma sequência de um usuário é construída pelo produto do autovetor associado a este usuário com a constante selecionada. Na recepção, a constante é recuperada a partir do autovetor, sequência padrão do usuário, e analisando o dicionário é obtida a mensagem. O número de mensagens distintas de um usuário é dado pelo número de constantes distintas. As sequências dos usuários são transmitidas por meio de um canal somador em corpos finitos (FFAC, do inglês *Finite Field Adder Channel*), resultando num vetor soma. Na recepção, as mensagens são separadas,

valendo-se da propriedade de ortogonalidade.

Diferentemente dos sistemas "criptográficos" propostos anteriormente, o sistema de comunicação multiusuário proposto emprega transformadas fracionais em corpos finitos baseadas na expansão espectral da matriz de transformação. A abordagem com funções de matrizes não é utilizada, pois não é possível se gerar mais autoespaços do que os já gerados pelas transformadas usuais. Como visto na Seção 4.3.5, a matriz da GFrFT baseada em funções de matrizes só apresenta quatro autovalores distintos. Assim, ela não será considerada para esse tipo de aplicação, pois não seria possível gerar mais de quatro autoespaços, o que representa uma severa limitação em relação ao número de usuários do sistema.

5.3.1 Definição do esquema de comunicação multiusuário

No esquema de comunicação multiusuário proposto, cada usuário é alocado em um autoespaço relacionado a um autovalor específico de uma matriz de transformação. Como o número de usuários depende do número de autovalores distintos, a matriz da GFrFT pode ser empregada, visto que seus autovalores dependem do parâmetro fracional a. A matriz da GFrFT de dimensão $N \times N$, baseada na expansão espectral, tem ao menos $N - 1$ autovalores distintos [17].

Em linhas gerais, as mensagens transmitidas por um usuário correspondem a autovetores multiplicados por diferentes constantes. As mensagens de um usuário, portanto, pertencem a um único autoespaço. Com o produto do autovetor por diferentes constantes, é possível criar um dicionário para o usuário.

Para construir um sistema para M usuários, é necessário que a matriz da GFrFT tenha M autovalores distintos. Considere que $\mathbf{v}_m$, $m = 1, \ldots, M$, seja um autovetor da matriz $\mathbf{F}^a$ associado ao autovalor λ_m. O dicionário com K mensagens distintas do m-ésimo usuário é construído a partir de mensagens s_m. As mensagens do m-ésimo usuário podem ser obtidas fazendo-se $s_m = \alpha_k v_m$, $k = 1, \ldots, K$, em que $\alpha_k \in \mathrm{GI}(p)$.

As mensagens criada pelos M usuários são inseridas num *FFAC*, cuja saída, a sequência $\mathbf{y}$, é a soma das mensagens de todos os usuários, ou seja $\mathbf{y} = \sum_{m=1}^{M} v_m$. Não é do escopo deste trabalho o comportamento do sistema na presença de ruído. A influência deste último foi avaliada em [123].

No receptor, recebida a sequência $\mathbf{y}$, a GFrFT é aplicada M vezes, obtendo-se diferentes sequências transformadas, $\mathbf{Y}_m$, em que $m = 0, 1, \ldots, M$. Note que $\mathbf{Y}_0 = \mathbf{y}$, $\mathbf{Y}_1 = \mathbf{F}^a\mathbf{y}$, *etc*. As sequências recuperadas relacionadas ao m-ésimo usuário, $\hat{s}_m$, são obtidas através de

$$\hat{s}_m = \frac{1}{M} \sum_{k=0}^{M-1} (\lambda_k)^{k(m-1)} \left(\mathbf{F}^{4/M}\right)^k \mathbf{y}, \tag{5.17}$$

para $m = 1, 2, \ldots, M$.

Para determinar a mensagem que o usuário enviou, basta comparar a sequência $\hat{s}_m$ com o autovetor v_m. Obtida a constante α_k e com auxílio do dicionário, a mensagem é recuperada.

A recuperação das mensagens de cada usuário também pode ser feita por um cálculo da correlação [123]. Este cálculo é feito a partir do produto interno entre as sequências recebidas e cada autovetor da matriz $\mathbf{F}^a$ associado a um usuário. Devido às características de ortogonalidade entre os autovetores, a sequência de dados de um usuário específico pode ser recuperada. Contudo, essa abordagem não será considerada na tese.

Sistema com dois usuários

Para um sistema com dois usuários são necessários dois autovalores distintos, que no caso da FFFT são $\lambda = \pm 1$. Sejam $s_1 = \alpha_k v_1$ e $s_2 = \alpha_k v_2$ sequências (mensagens) dos usuários 1 e 2, associados aos autovalores 1 e -1, respectivamente. Na saída do canal (*FFAC*) tem-se a sequência $\mathbf{y} = s_1 + s_2$. Aplicando a FFFT a $\mathbf{y}$, são obtidas as sequências $\mathbf{Y}_0 = \mathbf{F}^0 y = y$ e $\mathbf{Y}_1 = \mathbf{F}^2 y$. Usando a Equação (5.17), as sequências $\hat{s}_1$ e $\hat{s}_2$, associadas aos usuários 1 e 2, respectivamente, são

$$\begin{aligned}
\hat{s}_1 &= \tfrac{1}{2}\left((1)^{0(1-1)}\left(\mathbf{F}^{4/2}\right)^0 \mathbf{y} + (-1)^{1(1-1)}\left(\mathbf{F}^{4/2}\right)^1 \mathbf{y}\right) \\
&= \tfrac{1}{2}\left(\mathbf{y} + \mathbf{Y}_1\right) = \tfrac{1}{2}\left((s_1 + s_2) + (s_1 - s_2)\right) = s_1, \\
\hat{s}_2 &= \tfrac{1}{2}\left((1)^{0(2-1)}\left(\mathbf{F}^{4/2}\right)^0 \mathbf{y} + (-1)^{1(2-1)}\left(\mathbf{F}^{4/2}\right)^1 \mathbf{y}\right) \\
&= \tfrac{1}{2}\left(\mathbf{y} - \mathbf{Y}_1\right) = \tfrac{1}{2}\left((s_1 + s_2) - (s_1 - s_2)\right) = s_2.
\end{aligned}$$

Esquema com quatro usuários

Para um sistema com quatro usuários são necessários quatro autovalores distintos que, no caso da FFFT, são $\lambda = \{\pm 1, \pm\sqrt{-1}\}$. Sejam $s_1 = \alpha_k v_1$, $s_2 = \alpha_k v_2$, $s_3 = \alpha_k v_3$ e $s_4 = \alpha_k v_4$ sequências dos usuários $1, 2, 3$ e 4, associadas aos autovalores $1, -1, \sqrt{-1}$ e $-\sqrt{-1}$, respectivamente. Se a sequência de saída do *FFAC* é $\mathbf{y} = s_1 + s_2 + s_3 + s_4$, as sequências transformadas são $\mathbf{Y}_0 = y$,

$\mathbf{Y}_1 = \mathbf{F}y$, $\mathbf{Y}_2 = \mathbf{F}^2y$ e $\mathbf{Y}_3 = \mathbf{F}^3y$. Usando a Equação (5.17), as sequências recuperadas $\hat{s}_m$ são

$$\begin{aligned}
\hat{s}_1 &= \frac{1}{4}\sum_{k=0}^{3}(\lambda_k)^{k(1-1)}\left(\mathbf{F}^{4/4}\right)^k\mathbf{y} = \frac{1}{4}\sum_{k=0}^{3}(\lambda_k)^0(\mathbf{F})^k\mathbf{y} \\
&= \frac{1}{4}\left((1)^0(\mathbf{F})^0 + (\sqrt{-1})^0(\mathbf{F})^1 + (-1)^0(\mathbf{F})^2 + (-\sqrt{-1})^0(\mathbf{F})^3\right)\mathbf{y} \\
&= \frac{1}{4}\big((s_1+s_2+s_3+s_4) + (s_1+\sqrt{-1}s_2 - s_3 - \sqrt{-1}s_4) \\
&\quad +(s_1-s_2+s_3-s_4) + (s_1-\sqrt{-1}s_2-s_3+\sqrt{-1}s_4)\big) \;=\; s_1, \\
\hat{s}_2 &= \frac{1}{4}\left((1)^0(\mathbf{F})^0 + \left(\sqrt{-1}\right)^1(\mathbf{F})^1 + (-1)^2(\mathbf{F})^2 + \left(-\sqrt{-1}\right)^3(\mathbf{F})^3\right)\mathbf{y} \\
&= \frac{1}{4}\left(\mathbf{I} + \sqrt{-1}\;\mathbf{F} + \mathbf{F}^2 + \sqrt{-1}\;\mathbf{F}^3\right)\mathbf{y} \;=\; s_2, \\
\hat{s}_3 &= \frac{1}{4}\left((1)^0(\mathbf{F})^0 + \left(\sqrt{-1}\right)^2(\mathbf{F})^1 + (-1)^4(\mathbf{F})^2 + \left(-\sqrt{-1}\right)^6(\mathbf{F})^3\right)\mathbf{y} \\
&= \frac{1}{4}\left(\mathbf{I} - \mathbf{F} + \mathbf{F}^2 - \mathbf{F}^3\right)\mathbf{y} = s_3, \\
\hat{s}_4 &= \frac{1}{4}\left((1)^0(\mathbf{F})^0 + \left(\sqrt{-1}\right)^3(\mathbf{F})^1 + (-1)^6(\mathbf{F})^2 + \left(-\sqrt{-1}\right)^9(\mathbf{F})^3\right)\mathbf{y} \\
&= \frac{1}{4}\left(\mathbf{I} - \sqrt{-1}\;\mathbf{F} + \mathbf{F}^2 - \sqrt{-1}\;\mathbf{F}^3\right)\mathbf{y} = s_4,
\end{aligned}$$

em que $\mathbf{I}$ é a matriz identidade.

Esquema com oito usuários

Para um sistema de oito usuários, são necessários oito autovalores distintos. Usando uma GFrFT com parâmetro fracional $a = 1/2$, obtem-se os autovalores $\lambda = (\sqrt{[4]-1})^k$, para $k = 0, 1, \ldots, 6, 8$. Neste caso, há o autovalor $1 = (\sqrt[4]{-1})^0 = (\sqrt[4]{-1})^8$ com multiplicidade dois, como visto na Seção 4.3.5. Isso significa que só há sete autoespaços distintos.

Para resolver este problema, pode ser usada a matriz de uma GFrFT com nove autovalores distintos. Em corpos finitos, para construir essa matriz é necessário um elemento de ordem multiplicativa igual a nove. Assim, as sequências dos usuários devem ter nove componentes.

Uma alternativa para que as sequências permaneçam com oito componentes, é usar uma GFrFT com parâmetro fracional $a = 1/4$, pois $(\sqrt[4]{-1})^0 = 1$ e $(\sqrt[4]{-1})^4 = -1$. Se a sequência de saída do *FFAC* é $\mathbf{y} = \sum_{m=1}^{8} s_m$, as sequências transformadas são $\mathbf{Y}_k = \mathbf{F}^k y$, para $k = 0, 1, \ldots, 7$. Fazendo $i(k) = 0, 1, \ldots, 6, 8$, para $k = 0, 1, \ldots, 7$, os autovalores da GFrFT são dados por $\lambda = (\sqrt{-1})^{i(k)/2}$. Usando a Equação (5.17), as sequências recuperadas $\hat{s}_m$ são

$$
\begin{aligned}
\hat{s}_1 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{k(1-1)}\left(\mathbf{F}^{\frac{4}{8}}\right)^k\mathbf{y} = \frac{1}{8}\sum_{k=0}^{7}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\left(\mathbf{I}+\mathbf{F}^{\frac{1}{2}}+\mathbf{F}+\mathbf{F}^{\frac{3}{2}}+\mathbf{F}^2+\mathbf{F}^{\frac{5}{2}}+\mathbf{F}^3+\mathbf{F}^{\frac{7}{2}}\right)\mathbf{y} = s_1, \\
\hat{s}_2 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})^{\frac{1}{2}}\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})\mathbf{F}+(-\sqrt{-1})^{\frac{3}{2}}\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^2\left(\mathbf{F}^2\right) \\
&\quad +(-\sqrt{-1})^{\frac{5}{2}}\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^3\left(\mathbf{F}^3\right)+(-\sqrt{-1})^4\left(\mathbf{F}^{\frac{7}{2}}\right)\Big)\mathbf{y} = s_2, \\
\hat{s}_3 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{2k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})^2\mathbf{F}+(-\sqrt{-1})^3\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^4\left(\mathbf{F}^2\right) \\
&\quad +(-\sqrt{-1})^5\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^6\left(\mathbf{F}^3\right)+(-\sqrt{-1})^8\left(\mathbf{F}^{\frac{7}{2}}\right)\Big)\mathbf{y} = s_3, \\
\hat{s}_4 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{3k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})^{\frac{3}{2}}\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})^3\mathbf{F}+(-\sqrt{-1})^{\frac{9}{2}}\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^6\left(\mathbf{F}^2\right) \\
&\quad +(-\sqrt{-1})^{\frac{15}{2}}\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^9\left(\mathbf{F}^3\right)+(-\sqrt{-1})^{12}\left(\mathbf{F}^{\frac{7}{2}}\right)\Big)\mathbf{y} = s_4, \\
\hat{s}_5 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{4k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})^2\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})^4\mathbf{F}+(-\sqrt{-1})^6\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^8\left(\mathbf{F}^2\right) \\
&\quad +(-\sqrt{-1})^{10}\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^{12}\left(\mathbf{F}^3\right)+(-\sqrt{-1})^{16}\left(\mathbf{F}^{\frac{7}{2}}\right)\Big)\mathbf{y} = s_5, \\
\hat{s}_6 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{5k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})^{\frac{5}{2}}\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})^5\mathbf{F}+(-\sqrt{-1})^{\frac{15}{2}}\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^{10}\left(\mathbf{F}^2\right) \\
&\quad +(-\sqrt{-1})^{\frac{25}{2}}\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^{15}\left(\mathbf{F}^3\right)+(-\sqrt{-1})^4\left(\mathbf{F}^{\frac{35}{2}}\right)\Big)\mathbf{y} = s_6, \\
\hat{s}_7 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{6k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})^3\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})^6\mathbf{F}+(-\sqrt{-1})^9\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^{12}\left(\mathbf{F}^2\right) \\
&\quad +(-\sqrt{-1})^{15}\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^{18}\left(\mathbf{F}^3\right)+(-\sqrt{-1})^{24}\left(\mathbf{F}^{\frac{7}{2}}\right)\Big)\mathbf{y} = s_7,
\end{aligned}
$$

$$
\begin{aligned}
\hat{s}_8 &= \frac{1}{8}\sum_{k=0}^{7}(\lambda_k)^{7k}\left(\mathbf{F}^{\frac{1}{2}}\right)^k\mathbf{y} \\
&= \frac{1}{8}\Big(\ \mathbf{I}+(-\sqrt{-1})^{\frac{7}{2}}\left(\mathbf{F}^{\frac{1}{2}}\right)+(-\sqrt{-1})^{7}\mathbf{F}+(-\sqrt{-1})^{\frac{21}{2}}\left(\mathbf{F}^{\frac{3}{2}}\right)+(-\sqrt{-1})^{14}\left(\mathbf{F}^{2}\right) \\
&\qquad +(-\sqrt{-1})^{\frac{35}{2}}\left(\mathbf{F}^{\frac{5}{2}}\right)+(-\sqrt{-1})^{21}\left(\mathbf{F}^{3}\right)+(-\sqrt{-1})^{4}\left(\mathbf{F}^{\frac{49}{2}}\right)\Big)\mathbf{y}=s_8.
\end{aligned}
$$

Neste último caso, usando uma GFrFT com parâmetro fracional $a = 1/4$, o sistema poderia comportar até 15 usuários. Sistemas com mais usuários podem ser projetados respeitando três aspectos:

1. Para construir sequências de N componentes, deve existir um elemento ζ de ordem multiplicativa $\mathrm{ord}(\zeta) = N$ em $\mathrm{GI}(p)$.
2. O elemento $(\sqrt{-1})^{4/N}$ deve pertencer a $\mathrm{GI}(p)$.
3. A distribuição dos autovalores associados aos autovetores da FFFT deve ser respeitada, estando em consonância com a Tabela 2.1

Exemplo 5.1 – Sistema de comunicação com oito usuários.

Considere o elemento $\zeta = 8 + 8j \in \mathrm{GI}(127)$*, com ordem multiplicativa* $\mathrm{ord}(8 + 8j) = 8$*. A matriz da FFFT construída sobre esses termos é*

$$
\mathbf{F} = \begin{bmatrix}
4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\
4 & 32+95j & 123j & 95+95j & 123 & 95+32j & 4j & 32+32j \\
4 & 123j & 123 & 4j & 4 & 123j & 123 & 4j \\
4 & 95+95j & 4j & 32+95j & 123 & 32+32j & 123j & 95+32j \\
4 & 123 & 4 & 123 & 4 & 123 & 4 & 123 \\
4 & 95+32j & 123j & 32+32j & 123 & 32+95j & 4j & 95+95j \\
4 & 4j & 123 & 123j & 4 & 4j & 123 & 123j \\
4 & 32+32j & 4j & 95+32j & 123 & 95+95j & 123j & 32+95j
\end{bmatrix}.
$$

A matriz da GFrFT com parâmetro fracional $a = 1/4$*, construída de acordo com o procedimento descrito na Tabela 3.1, é*

$$\mathbf{F}^{\frac{1}{4}} = \begin{bmatrix} 72+29j & 73+120j & 72+11j & 54+18j & 93+99j & 54+18j & 72+11j & 73+120j \\ 73+120j & 107+111j & 64+13j & 68+44j & 122+74j & 14+123j & 46+103j & 43+85j \\ 72+11j & 64+13j & 95+63j & 115+58j & 79+6j & 47+33j & 11+73j & 46+103j \\ 54+18j & 68+44j & 115+58j & 44+113j & 9+5j & 86+63j & 47+33j & 14+123j \\ 93+99j & 122+74j & 79+6j & 9+5j & 50+113j & 9+5j & 79+6j & 122+74j \\ 54+18j & 14+123j & 47+33j & 86+63j & 9+5j & 44+113j & 115+58j & 68+44j \\ 72+11j & 46+103j & 11+73j & 47+33j & 79+6j & 115+58j & 95+63j & 64+13j \\ 73+120j & 43+85j & 46+103j & 14+123j & 122+74j & 68+44j & 64+13j & 107+111j \end{bmatrix}.$$

□

As matrizes $\mathbf{F}$ *e* $\mathbf{F}^{\frac{1}{4}}$ *têm os mesmos autovetores, os quais são apresentados na segunda coluna da Tabela 5.19. Os autovalores das matrizes* $\mathbf{F}$ *e* $\mathbf{F}^{\frac{1}{4}}$ *são apresentados nas terceira e quarta colunas da Tabela 5.19, respectivamente, associados aos respectivos autovetores, segunda coluna da Tabela 5.19.*

Tabela 5.19: *Conjunto ortogonal de autovetores de* $\mathbf{F}$ *e de* $\mathbf{F}^{\frac{1}{4}}$ *para* $p = 127, \zeta = 8 + 8j, N = 8$*, segunda coluna. Os autovalores de* $\mathbf{F}$ *são apresentados na terceira coluna, e os autovalores de* $\mathbf{F}^a$ *são apresentados na quarta coluna, associados aos seus respectivos autovetores.*

k	$\mathbf{v}_k$	$\lambda(\mathbf{F})$	$\lambda(\mathbf{F}^{1/4})$
1	1, 126, 15, 1, 1, 1, 15, 126	1	1
2	0, 22, 112, 8, 0, 119, 15, 105	$126j$	$106 + 24j$
3	1, 81, 49, 81, 53, 81, 49, 81	126	$119 + 8j$
4	0, 119, 1, 8, 0, 119, 126, 8	j	$103 + 21j$
5	$1,\ 126 + 25j,\ 35 + 58j,\ 22 + 74j,\ 46 + 67j,\ 22 + 74j,\ 35 + 58j,\ 126 + 25j$	1	$126j$
6	0, 26, 17, 8, 0, 119, 110, 101	$126j$	$24 + 21j$
7	1, 44, 80, 44, 12, 44, 80, 44	126	$8 + 8j$
8	$1,\ 126 + 102j,\ 35 + 69j,\ 22 + 53j,\ 46 + 60j,\ 22 + 53j,\ 35 + 69j,\ 126 + 102j$	1	126

Fonte: Próprio Autor.

Considere que as mensagens dos usuários são dadas por: $s_1 = 12v_1$*,* $s_2 = 7v_2$*,* $s_3 = 5v_3$*,* $s_4 = 3v_4$*,* $s_5 = 9v_5$*,* $s_6 = 11v_6$*,* $s_7 = 33v_7$ *e* $s_8 = 46v_8$*. A mensagem de saída enviada ao* FFAC *é dada por* $Y_0 = \sum_{m=1}^{8} s_m$ *e é apresentada na primeira coluna da Tabela 5.20.*

A existência de ruído em canais aditivos provoca erros entre as mensagens transmitidas e recebidas. Sobre certas situações, as quais não são tratadas nesta tese, com o uso de códigos corretores de erro as mensagens podem ser corrigidas. Considerando esse cenário, as sequências s_m*,* $m = 1, \ldots, 8$*, são recuperadas de acordo com a Equação (5.17). Nas colunas 2 a 8 da Tabela 5.20 são apresentadas as sequências* $\mathbf{Y}_k$*,* $k = 1, \ldots, 7$*, as quais são as sequências*

transformadas de $\mathbf{Y}_0$, respectivamente. Usando a Equação (5.17), a mensagem recuperada do primeiro usuário é

$$s_1 = \frac{1}{8}\sum_{k=0}^{7} Y_k = 12\,(1,\ 126,\ 15,\ 1,\ 1,\ 1,\ 15,\ 126)\,.$$

Tabela 5.20: *Sequências de saída do* FFAC *e suas transformadas. A n-ésima coluna representa a n-ésima autosequência da transformada fracional de Fourier sobre corpos finitos associada ao parâmetro $(n)/4$. Na primeira coluna está a sequência recebida Y_0. Na segunda coluna está a sequência Y_1, que representa a GFrFT de parâmetro $a = 1/4$ de Y_0, e assim por diante.*

Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7
$105+0j$	$63+41j$	$49+28j$	$123+59j$	$29+0j$	$123+68j$	$49+99j$	$63+86j$
$47+91j$	$14+67j$	$53+75j$	$23+116j$	$108+8j$	$57+13j$	$103+13j$	$42+55j$
$122+13j$	$108+106j$	$25+68j$	$23+121j$	$109+61j$	$72+67j$	$4+104j$	$46+42j$
$72+56j$	$20+41j$	$4+88j$	$97+55j$	$0+63j$	$74+46j$	$124+26j$	$0+62j$
$28+61j$	$55+82j$	$63+2j$	$55+21j$	$103+61j$	$118+47j$	$63+121j$	$119+113j$
$117+56j$	$62+15j$	$124+89j$	$12+31j$	$0+49j$	$32+22j$	$4+27j$	$85+36j$
$79+13j$	$74+87j$	$4+120j$	$44+62j$	$109+92j$	$51+8j$	$25+29j$	$80+23j$
$104+91j$	$111+86j$	$103+31j$	$115+1j$	$108+47j$	$92+25j$	$53+96j$	$72+74j$

Fonte: Próprio Autor.

CAPÍTULO 6

CONCLUSÕES

As transformadas em corpos finitos continuam a ser objeto de investigação e fornecem várias possibilidades para novos estudos, como é o caso das transformadas fracionais em corpos finitos. A importância dessas ferramentas é percebida pelas aplicações em diversas áreas da Engenharia, e por dois aspectos de significativa e crescente necessidade: simplicidade nas operações aritméticas e a ausência de erros de arredondamento.

Acompanhando a evolução das transformadas no corpo dos números reais, onde se tem definidas transformadas fracionais contínuas e discretas, esta tese introduz transformadas fracionais em estruturas algébricas finitas.

Além disso, ferramentas desenvolvidas no corpo dos números reais, como a teoria de funções de matrizes, também se mostram válidas em corpos finitos e foram empregadas para as definições das transformadas fracionais de Fourier, de Hartley, do seno e do cosseno tipos 1 e 4 em corpos finitos.

6.1 Contribuições

No Capítulo 2 é introduzida a transformada de Hartley sobre corpos finitos generalizada. As autoestruturas dessa matriz e da matriz da transformada de Fourier em corpos finitos generalizada são investigadas para se obter ferramentas destinadas à definição das transformadas fracionais do cosseno e do seno sobre corpos finitos tipo 4 baseadas na expansão espectral. No Capítulo 3, é introduzida a transformada fracional de Hartley sobre corpos finitos baseada na expansão espectral que utiliza autovetores construídos a partir da matriz $\mathbf{S}$. São introduzidas também as transformadas fracionais de Fourier e de Hartley sobre corpos finitos generalizadas e as transformadas fracionais do

cosseno e do seno sobre corpos finitos tipo 4 baseadas na expansão espectral que utilizam autovetores construídos a partir da matriz $\mathbf{E}$.

No Capítulo 4, é desenvolvida a teoria de funções de matrizes em corpos finitos com o propósito de se obter potências fracionais das matrizes das transformadas clássicas sobre corpos finitos. A capital importância desta teoria reside no fato de que não é necessário se construir conjuntos ortogonais de autovetores para se definir as transformadas fracionais em corpos finitos. É desenvolvida uma expressão analítica para se obter as matrizes de transformação.

Ainda no Capítulo 4, foram definidas as transformadas fracionais em corpos finitos e obtidas algumas propriedades das mesmas. O material deste capítulo foi publicado em anais de simpósios internacionais [25, 26]. Nas Seções 3.7 e 4.3.5, foi analisada a autoestrutura da transformada fracional de Fourier sobre corpos finitos, que serve de fundamentação teórica para aplicações em comunicação multiusuário, como visto na Seção 5.3.

Na Seção 4.4, foram encontradas expressões analíticas para determinar o número de multiplicações e adições requiridas no cálculo das transformadas fracionais. Com a proposta baseada em funções de matrizes, não há um aumento significativo na complexidade computacional associada às transformadas fracionais em corpos finitos quando comparadas com as correspondentes transformadas clássicas em corpos finitos. Em comparação com procedimentos baseados na expansão espectral [22, 24, 46], a complexidade computacional é menor. Isso ocorre, pois é possível utilizar os algoritmos rápidos desenvolvidos para as transformadas clássicas para qualquer comprimento de transformada.

Mostrou-se que os algoritmos rápidos usados em transformadas ordinárias podem ser usados também em transformadas fracionais. A nova abordagem contribui para o uso das transformadas fracionais em aplicações em que o custo computacional é essencial, como em criptografia, por exemplo. Nas Seções 5.1 e 5.2, foram apresentadas propostas de sistemas criptográficos para cifragem de imagem e para marca d'água, respectivamente.

No Capítulo 5, algumas aplicações em criptografia e em comunicações foram desenvolvidas e avaliadas, mostrando a flexibilidade e a aplicabilidade das ferramentas matemáticas e transformadas introduzidas nesta tese.

6.2 Trabalhos Futuros

A seguir, são apresentados alguns tópicos para continuidade da tese em trabalhos futuros.

- Em relação ao procedimento baseado na expansão espectral, em que se emprega matrizes comu-

tantes para se obter um conjunto ortogonal de autovetores, pode ser avaliada a utilização de outras matrizes que comutem com a matriz $\mathbf{F}$, como a matriz $\mathbf{T}$ [32]. Isso é relevante, porque em alguns casos a matriz $\mathbf{S}$ não tem autovalores em $\mathrm{GF}(p)$ ou em $\mathrm{GI}(p)$, mas sim em corpos de extensão mais alta. Com isso, fica inviável a construção de conjutos ortogonais de autovetores, necessários para aplicações como em comunicação multiusuário.

- Pode-se investigar para quais números primos existem elementos unimodulares com autovetores e autovalores em $\mathrm{GI}(p)$. A razão é a mesma que no item anterior, pois assim é possível saber quando se obtém conjuntos ortogonais de autovetores.
- Podem ser investigadas as propriedades de deslocamento, convolução, multiplicação nos domínios fracionais e do "tempo". Com essas propriedades será possível fundamentar teoricamente processos de filtragem no domínio fracional em corpos finitos.
- Podem ser investigadas as relações entre números positivos e negativos no corpo dos números reais com os elementos que são resíduos quadráticos e com os que não são resíduos quadráticos em corpos finitos. Dessa maneira, uma fundamentação teórica é obtida para se realizar operações entre números reais em corpos finitos, como na proposta de Rader [38]. Isso permite que aplicações como filtragem de sinais de radar, biométrico, dentre outras, possam ser realizadas em corpos finitos e depois "retornem" ao corpo dos números reais.
- A teoria desenvolvida para as transformadas fracionais sobre corpso finitos é foi feita considerando números primos ímpares. Contudo, para corpos de característica dois, $\mathrm{GF}(2^m)$, ainda não foram definidas as funções do seno e do cosseno. Nesse sentido, podem ser investigados corpos de característica dois, e em seguida definidas as transformadas clássicas e fracionais.
- Pode ser investigada a relação entre a GFrCT e a GFrFT, com o propósito de se obter mais facilmente uma transformada a partir da outra. Isso é importante, pois em alguns casos uma das transformadas pode ser livre de operações de multiplicação, como é o caso das transformadas numéricas.
- Podem ser investigados sistemas de cifragem de imagens baseados em transformadas fracionais em corpos finitos, realizando comparações com outros sistemas de cifragem, avaliando, especialmente, a complexidade computacional.

REFERÊNCIAS

[1] N. Wiener, "Hermitian polynomials and Fourier analysis," *Journal of Mathematics and Physics*, vol. 8, no. 1, pp. 70–73, 1929.

[2] E. Condon, "Immersion of the Fourier transform in a continuous group of functional transformations," in *Proceedings of National Academy of Sciences of the United States of America*, vol. 23, no. 3, 1937, pp. 158–164.

[3] H. Kober, "Wurzeln aus der hankel- und Fourier und anderen stetigen transformationen," *The Quarterly Journal of Mathematics*, no. 10, pp. 45–49, 1939.

[4] N. D. Bruijn, "A theory of generalized functions, with applications to Wigner distribution and Weyl correspondence," *Nieuw Archief voor Wiskunde*, no. 3, pp. 205–280, 1973.

[5] V. Namias, "The fractional order Fourier transform and its application in quantum mechanics," *IMA Journal of Applied Mathematics*, vol. 25, pp. 241–265, 1980.

[6] A. C. McBride and F. H. Kerr, "On Namias's fractional Fourier transforms," *IMA Journal of Applied Mathematics*, vol. 39, pp. 159–175, 1987.

[7] B. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 30, no. 1, pp. 25–31, 1982.

[8] B. Santhanam and J. H. McClellan, "The DRFT- A rotation in time-frequency space," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, vol. 2, 1995, pp. 921–924.

[9] H. Ozaktas, M. Kutay, and G. Bozdağı, "Digital computation of the fractional Fourier transform," *IEEE Transaction on Signal Processing*, vol. 25, no. 3, pp. 241–265, 1996.

[10] X. Deng, Y. Li, D. Fan, and Y. Qiu, "A fast algorithm for fractional Fourier transforms," *Optics Communications*, vol. 138, pp. 270–274, 1997.

[11] H. Ozaktas and D. Mendlovic, "Fractional Fourier transforms and their optical implementation," *Journal of Optical Society of America*, vol. 10, no. 12, pp. 2522–2531, 1993.

[12] T. Alieva, V. Lopez, F. Agullo-Lopez, and L. Almeida, "The fractional Fourier transform in optical propagation problems," *Journal of Modern Optics*, vol. 41, pp. 1037–1044, 1994.

[13] L. Almeida, "The fractional Fourier transform and time-frequency representations," *IEEE Transactions on Signal Processing*, vol. 42, no. 11, pp. 3084–3091, 1994.

[14] S.-C. Pei, C. Tseng, M. Yeh, and J. Shyu, "Discrete fractional Hartley and Fourier transforms," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 45, no. 6, pp. 665–675, 1998.

[15] S.-C. Pei and M. Yeh, "Two dimensional discrete fractional Fourier transform," *Signal Processing*, vol. 67, no. 1, pp. 99 – 108, 1998.

[16] ——, "Discrete fractional Hadamard transform," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, vol. 3, 1999, pp. 179–182.

[17] C. Candan, M. Kutay, and H. Ozaktas, "The discrete fractional Fourier transform," *IEEE Transactions on Signal Processing*, vol. 48, no. 5, pp. 1329–1337, 2000.

[18] S.-C. Pei and J. Ding, "Fractional cosine, sine and Hartley transforms," *IEEE Transactions on Signal Processing*, vol. 50, no. 7, pp. 1661–1680, 2002.

[19] S.-C. Pei and M. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Transactions on Signal Processing*, vol. 49, no. 6, pp. 1198–1207, 2001.

[20] S.-C. Pei, C.-C. Wen, and J.-J. Ding, "Closed-form orthogonal DFT eigenvectors generated by complete generalized Legendre sequence," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 55, no. 11, pp. 3469–3479, 2008.

[21] J. B. Lima and R. M. Campello de Souza, "The finite field fractional Fourier transform," in *Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, 2010, pp. 3670–3673.

[22] S.-C. Pei, C.-C. Wen, and J.-J. Ding, "Closed-form orthogonal number theoretic transform eigenvectors and the fast fractional NTT," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2124–2135, 2011.

[23] J. B. Lima, R. M. Campello de Souza, and P. H. E. S. Lima, "Transformada fracional do cosseno em corpos finitos," in *Anais do Simpósio Brasileiro de Telecomunicações (SBrT)*, 2012.

[24] J. B. Lima and R. M. Campello de Souza, "Fractional cosine and sine transforms over finite fields," *Linear Algebra and its Applications*, vol. 438, no. 8, pp. 3217–3230, 2013.

[25] J. B. Lima, R. M. Campello de Souza, and P. H. E. S. Lima, "Fractional number-theoretic transform based on matrix functions," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 24, no. 7, Florence, Italy, 2014, pp. 587–597.

[26] P. H. E. S. Lima, J. B. Lima, and R. M. Campello de Souza, "Hartley, cosine and sine fractional transforms over finite fields," in *Proceedings of the International Telecommunications Symposium (ITS)*, São Paulo, Brazil, 2014, pp. 1–5.

[27] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The fractional Fourier transform*, 2nd ed. John Wiley, 2001.

[28] A. Bultheel and H. Martínez, "A shattered survey of the fractional fourier transform," Report TW337, 2002, Department of Computer Science, K. U. Leuven, Belgium.

[29] M. L. Mehta, "Eigenvalues and eigenvectors of the finite Fourier transform," *Journal of Mathematical Physics*, vol. 28, no. 4, pp. 781–785, 1987.

[30] N. M. Atakishiyev, L. E. Vicent, and K. B. Wolf, "Continuous versus discrete fractional Fourier transforms," *Journal of Computation and Applied Mathematics*, vol. 107, no. 1, pp. 73–95, 1999.

[31] T. Erseghe and G. Cariolaro, "An orthonormal class of exact and simple DFT eigenvectors with a high degree of symmetry," *IEEE Transactions on Signal Processing,*, vol. 51, no. 10, pp. 2527–2539, 2003.

[32] S.-C. Pei, W. Hsue, and J.-J. Ding, "Discrete fractional Fourier transform based on new nearly tridiagonal commuting matrices," *IEEE Transactions on Signal Processing*, vol. 54, no. 10, pp. 3815–3828, 2006.

[33] R. Tao, X.-Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Transactions on Information Security and Forensics*, vol. 5, no. 4, pp. 734–738, 2010.

[34] M. Fan and H. Wang, "Chaos-based discrete fractional sine transform domain audio watermarking scheme," *Computers and Electrical Engineering*, vol. 35, no. 3, pp. 506–516, 2009.

[35] J. G. Vargas-Rubio and B. Santhanam, "An improved spectrogram using the multiangle centered discrete fractional Fourier transform," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 4, 2005, pp. 505–508.

[36] R. Tao, X.-Y. Meng, and Y. Wang, "Transform order division multiplexing," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 598–609, 2011.

[37] C. C. Yang, "Modified Legendre sequence for optical-CDMA based passive optical networks," *IEEE Communications Letters*, vol. 10, no. 5, pp. 393–395, 2006.

[38] C. Rader, "Discrete Fourier transforms when the number of data samples is prime," *Proceedings of the IEEE*, vol. 56, pp. 1107 – 1108, 1968.

[39] ——, "On the application of the number theoretic methods of high-speed convolution to two dimensional filtering," *IEEE Transactions on Circuits and Systems*, vol. 22, pp. 575 – 1108, 1975.

[40] T. Toivonen and J. Heikkilä, "Video filtering with Fermat number theoretic transforms using residue number system," *IEEE Transactions on Circuits and Systems Video Technology*, vol. 16, no. 1, pp. 92–101, 2006.

[41] R. M. Campello de Souza, M. M. Campello de Souza, and H. M. de Oliveira, "Eigensequences for multiuser communication over the real adder channel," in *Proceedings of the International Telecommunications Symposium (ITS)*, Fortaleza, Brazil, 2006, pp. 989–994.

[42] J. B. Lima, R. M. Campello de Souza, and D. C. Cunha, "Multiuser communication based on the discrete fractional Fourier transform," in *Proceedings of the IEEE International Conference on Communications*, Ottawa, Canada, 2012, pp. 3618–3622.

[43] R. M. Campello de Souza, E. S. V. Freire, and H. M. de Oliveira, "Fourier codes," in *Proceedings of the International Symposium on Communication Theory and Applications (ICSTA)*, vol. 1, Ambleside, United Kingdom, 2009, pp. 370–375.

[44] R. E. Blahut, *Fast Algorithms for Signal Processing*, 2nd ed. Cambridge University Press, 2010.

[45] J. B. Lima and L. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," *Signal Processing*, vol. 94, pp. 521–530, 2013.

[46] J. B. Lima and R. M. Campello de Souza, "The fractional Fourier transform over finite fields," *Signal Processing*, vol. 92, no. 2, pp. 465–476, 2012.

[47] S.-C. Pei and W.-L. Hsue, "Tridiagonal commuting matrices and fractionalizations of DCT and DST matrices of types I, IV, V, and VIII," *IEEE Transactions on Signal Processing*, vol. 56, no. 6, pp. 2357–2369, 2008.

[48] S. Güdvangen, "Practical applications of number theoretic transforms," 2006. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.1921

[49] J. M. Pollard, "The fast Fourier transform in a finite field," *Mathematics of Computation*, vol. 25, no. 114, pp. 365– 374, 1971.

[50] I. S. Reed and T. K. Truong, "The use of finite fields to compute convolutions," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 208 – 213, 1975.

[51] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[52] J. L. Massey, "The discrete Fourier transform in coding and cryptography," *IEEE Information Theory Workshop*, pp. 9 – 11, 1998.

[53] R. M. Campello de Souza, H. M. de Oliveira, A. N. Kauffman, and A. J. A. Paschoal, "Trigonometry in finite fields and a new Hartley transform," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, vol. 1, Cambridge, USA, 1998, p. 293.

[54] D. M. Burton, *Elementary number theory*, 7th ed. McGraw-Hill, 2010.

[55] R. M. Campello de Souza, M. M. Campello de Souza, H. M. de Oliveira, and L. B. E. Palma, "Hartley number theoretic transforms," in *Proceedings of the International Symposium on Information Theory (ISIT)*, vol. 1, Washington, USA, 2001, p. 210.

[56] G. Bongiovanni, P. Corsini, and G. Frosini, "One-dimensional and two-dimensional generalised discrete Fourier transforms," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 24, no. 1, pp. 97–99, 1976.

[57] P. Corsini and G. Frosini, "Properties of the multidimensional generalized discrete Fourier transform," *IEEE Transactions on Computers*, vol. C-28, no. 11, pp. 819–830, 1979.

[58] C. Tseng, "Eigenvalues and eigenvectors of generalized DFT, generalized DHT, DCT-IV and DST-IV matrices," *IEEE Transactions on Signal Processing*, vol. 50, no. 4, pp. 866–877, 2002.

[59] C. Moraga, "Generalized discrete Hartley transforms," in *Proceedings of the International Symposium on Multiple-Valued Logic (ISMVL)*, 2009, pp. 185–190.

[60] J. B. Lima, "Trigonometria sobre corpos finitos: Novas definições e cenários de aplicação," Programa de Pós-graduação em Engenharia Elétrica, UFPE, Recife,PE, Tese, Setembro 2008.

[61] J. B. Lima, R. M. Campello de Souza, and D. Panario, "The eigenstructure of finite field trigonometric transforms," *Linear Algebra and its Applications*, no. 435, pp. 1956–1971, 2011.

[62] J. H. McClellan and T. W. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Transactions on Audio and Electroacoustics*, vol. 20, no. 1, pp. 66–74, 1972.

[63] D. T. Birtwistle, "The eigenstructure of the number theoretic transforms," *Signal Processing*, vol. 4, no. 4, pp. 287–294, 1982.

[64] R. M. Campello de Souza, M. M. Campello de Souza, H. M. de Oliveira, and L. B. E. Palma, "Transformadas numéricas de Hartley," in *Anais do Simpósio Brasileiro de Telecomunicações (SBrT)*, vol. 1, Gramado, RS, 2000, pp. 1–5.

[65] R. C. Agarwal and C. S. Burrus, "Fast convolution using Fermat number transforms with applications to digital filtering," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 22, no. 2, pp. 87–97, 1974.

[66] C. M. Rader, "Discrete convolutions via Mersenne transform," *IEEE Transactions on Computers*, vol. C-21, pp. 1269 – 1273, 1971.

[67] M. T. Hamood and S. Boussakta, "Efficient algorithms for computing the new Mersenne number transform," *Digital Signal Processing*, vol. 25, pp. 280–288, 2014.

[68] O. Nibouche, S. Boussakta, and M. Darnell, "Pipeline architectures for radix-2 new Mersenne number transform," *IEEE Transactions on Circuits and Systems-I: Regular papers*, vol. 56, no. 8, pp. 1668–1680, 2009.

[69] S. Boussakta and M. T. Hamood, "Rader–Brenner algorithm for computing new Mersenne number transform," *IEEE Transactions on Circuits and Systems-II: Express briefs*, vol. 58, no. 8, pp. 532–536, 2011.

[70] S. Boussakta, M. T. Hamood, and N. Rutter, "Generalized new Mersenne number transforms," *IEEE Transactions on Signal Processing*, vol. 60, no. 5, pp. 2640–2647, 2012.

[71] R. M. Campello de Souza, H. M. de Oliveira, M. M. Campello de Souza, and M. M. Vasconcelos, "A transformada discreta do seno em um corpo finito," in *Anais do Congresso Nacional de Matemática Aplicada e Computacional (CNMAC)*, Rio de Janeiro, Brasil, 2005.

[72] M. M. Campello de Souza, H. M. de Oliveira, R. M. Campello de Souza, and M. M. Vasconcelos, "The discrete cosine transform over finite prime fields," in *Proceedings of the International Telecommunications Symposium (ITS)*, 2004.

[73] R. M. Campello de Souza, H. M. de Oliveira, and D. Silva, "The Z transform over finite fields," in *Proceedings of the International Telecommunications Symposium (ITS)*, vol. 1, Natal, Brazil, 2002, pp. 1–5.

[74] B. Santhanam and J. McClellan, "The discrete rotational Fourier transform," *IEEE Transactions on Signal Processing*, vol. 44, no. 4, pp. 994 – 998, 1996.

[75] A. Kuznetsov, "Explicit Hermite-type eigenvectors of the discrete Fourier transform," 2015. [Online]. Available: http://arxiv.org/pdf/1501.07646v1.pdf

[76] F. A. Grübaum, "The eigenvectors of the discrete Fourier transform: A version of the Hermite functions," *Journal of Mathematical Analysis and Applications*, vol. 88, no. 2, pp. 355 –363, 1982.

[77] J. H. Wilkinson, *The Algebraic Eigenvalue Problem*. Oxford University Press, 1998.

[78] N. J. Higham, *Functions of Matrices: Theory and Computation*. Society for Industrial and Applied Mathematics, 2008.

[79] P. Lancaster and M. Tismenestsky, *The Theory of Matrices: With Applications*, 2nd ed. Academic Press, 1985.

[80] G. Bergland, "Fast Fourier transform hardware implementations - an overview," *IEEE Transactions on Audio and Electroacoustics*, vol. 17, no. 2, pp. 104–108, 1969.

[81] A. M. Despain, "Very fast Fourier transform algorithms hardware for implementation," *IEEE Transactions on Computers*, vol. C-28, no. 5, pp. 333–341, 1979.

[82] W. T. Cochran, J. W. Cooley, D. L. Favin, H. D. Helms, R. A. Kaenel, W. W. Lang, G. C. Maling, D. E. Nelson, C. M. Rader, and P. D. Welch, "What is the fast Fourier transform?" *Proceedings of the IEEE*, vol. 55, pp. 1664–1674, 1967.

[83] H. M. de Oliveira and R. M. Campello de Souza, "A fast algorithm for computing the Hartley/Fourier spectrum," in *Anais da Academia Brasileira de Ciências*, vol. 73, no. 9, 2001, pp. 468 – 468.

[84] J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series," *Mathematics of Computation*, vol. 19, no. 90, pp. 297–301, 1965.

[85] M. Heideman, C. Burrus, and H. Johnson, "Prime factor FFT algorithms for real-valued series," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 9, pp. 492 – 495, 1984.

[86] M. T. Heideman, *Multiplicative complexity, convolution, and the DFT*. Springer-Verlag, Inc., 1988.

[87] G. J. da Silva Jr and R. M. Campello de Souza, "Minimum multiplicative complexity algorithm for computing a single component of the discrete Fourier transform," *Digital Signal Processing*, vol. 23, pp. 1040 – 1043, 2013.

[88] I. J. Good, "The interaction algorithm and practical Fourier analysis," *Journal of the Royal Statistical Society*, vol. B20, pp. 361 – 372, 1958.

[89] L. H. Thomas, "Using a computer to solve problems in physics," *Applications of Digital Computers*, pp. 44 – 45, 1963.

[90] I. J. Good, "The relationship between two fast Fourier transforms," *IEEE Transactions on Computers*, vol. C-20, pp. 310 – 317, 1971.

[91] S. Winograd, "On computing the discrete Fourier transform," *Proc. Nat. Acad. Sci. Mathematics*, vol. 73, pp. 1005–1006, 1976.

[92] ——, "On computing the discrete Fourier transform," *Mathematics of Computation*, vol. 32, pp. 175 – 199, 1978.

[93] G. J. da Silva Jr and R. M. Campello de Souza, "Cyclotomic basis for computing the discrete fourier transform," in *Proceedings of the International Telecommunications Symposium (ITS)*, vol. 7, Manaus, Brazil, 2010, pp. 1–5.

[94] R. C. de Oliveira, R. M. Campello de Souza, and H. M. de Oliveira, "Matrix expansions for computing the discrete Hartley transform," in *Proceedings of the International Telecommunications Symposium (ITS)*, vol. 1, Manaus, Brazil, 2010.

[95] R. J. Cintra and V. S. Dimitrov, "The arithmetic cosine transform: Exact and approximate algorithms," *IEEE Transactions on Signal Processing*, vol. 58, pp. 3076–3085, 2010.

[96] R. C. de Oliveira, R. M. Campello de Souza, and H. M. de Oliveira, "Matrix expansions for computing the discrete Hartley transform for blocklength $n \equiv 0 \pmod 4$," in *Proceedings of the IEEE Latin-America Conference on Communications (LATINCOM)*, Cuenca, Ecuador, 2012, pp. 1–6.

[97] R. C. de Oliveira, H. de Oliveira, R. Campello de Souza, and E. Santos, "A flexible implementation of a matrix Laurent series-based 16-point fast Fourier and Hartley transforms," in *Proceedings of the Southern Programmable Logic Conference (SPL)*, 2010, pp. 175–178.

[98] H. M. de Oliveira, V. L. Sousa, H. A. N. Silva, and R. M. Campello de Souza , "Radix-2 fast Hartley transform revisited," *Congresso de Informática da Amazônia*, vol. 1, pp. 285–292, 2001.

[99] S. C. Chan and K. L. Ho, "Direct methods for computing discrete sinusoidal transforms," in *Proceedings of the IEE Radar and Signal Processing*, vol. 137, no. 6, 1990, pp. 433–442.

[100] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2011.

[101] J. B. Lima, E. Lima, and F. Madeiro, "Image encryption based on the finite field cosine transform," *Signal Processing: Image Communication*, vol. 28, pp. 1537–1547, 2013.

[102] Q. Guo, Z. Liu, and S. Liu, "Color image encryption by using Arnold and discrete fractional random transforms in IHS space," *Optics and Lasers in Engineering*, vol. 48, no. 12, pp. 1174 – 1181, 2010.

[103] S. Matejka, "Implementação do algoritmo aes em matlab," 2014, software. [Online]. Available: https://www.mathworks.com/matlabcentral/linkexchange/links/3025.html

[104] Signal and I. P. I. University of Southern California, "The USC-SIPI Image Database," 2015, base de imagens. [Online]. Available: http://www.sipi.usc.edu/services/database/Database.html

[105] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, 2010.

[106] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, pp. 514–522, 2011.

[107] S. K. Chhotaray, A. Chhotaray, and G. S. Rath, "A new method of generating public key matrix and using it for image encryption," in *Proceedings of the International Conference on Signal Processing and Integrated Networks (SPIN)*, 2015, pp. 453–458.

[108] N. Smart, "ECRYPT II yearly report on algorithms and keysizes (2010-2011)," European Network of Excellence in Cryptology II, Relatório Técnico, 2011.

[109] S. Keshari and S. G. Modani, "Dual watermarking based on multiple parameter fractional Fourier transform and LSB technique," in *Proceedings of the IEEE International Conference on Image Information Processing (ICIIP)*, Nov 2011, pp. 1–5.

[110] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1167–1180, Jul 1999.

[111] C.-Y. Lin and S.-F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," in *Proceedings of the International Conference on Security and Watermarking of Multimedia Contents*, 2000, pp. 140–151.

[112] J. Ruanaidh, W. Dowling, and F. Boland, "Watermarking digital images for copyright protection," *IEE Transactions on Vision, Image and Signal Processing*, vol. 143, no. 4, pp. 250–256, Aug 1996.

[113] M. Suhail and M. Obaidat, "Digital watermarking-based DCT and JPEG model," *IEEE Transactions on Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640–1647, Oct 2003.

[114] H. Liu, J. Liu, J. Huang, D. Huang, and Y. Shi, "A robust DWT-based blind data hiding algorithm," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, vol. 2, 2002, pp. II–672–II–675 vol.2.

[115] H. Inoue, A. Miyazaki, and T. Katsura, "Wavelet-based watermarking for tamper proofing of still images," in *Proceedings of the International Conference on Image Processing (ICIP)*, vol. 2, 2000, pp. 88–91.

[116] H. Tamori, N. Aoki, and T. Yamamoto, "Fragile digital watermarking technique by number theoretic transform," *IEICE Transactions on Fundamentals*, vol. E85-A, no. 8, p. 1902–1904, 2002.

[117] R. Cintra, V. Dimitrov, R. M. Campello de Souza, and H. M. de Oliveira, "Fragile watermarking using finite field trigonometric transforms," *Signal Processing: Image Communication*, vol. 24, no. 7, pp. 587–597, 2009.

[118] J. B. Lima and R. M. Campello de Souza, "Uma marca d'água digital baseada na transformada do cosseno sobre corpos finitos," in *Anais do Simpósio Brasileiro de Telecomunicações (SBrT)*, Campinas, Brasil, 2005, pp. 1–5.

[119] R. Merched, "On OFDM and single-carrier frequency-domain systems based on trigonometric transforms," *IEEE Signal Processing Letters*, vol. 13, pp. 472–476, August 2006.

[120] G. D. Mandyam, "Sinusoidal transforms in OFDM systems," *IEEE Transaction on Broadcasting*, vol. 50, no. 2, pp. 172–184, June 2004.

[121] N. Al-Dahir and H. Minn, "A new multicarrier transceiver based on the discrete cosine transform," in *Proceedings of the Wireless Communications Networking Conference*, vol. 1, 2005, pp. 45–50.

[122] X. Zhang, M. Li, H. Hu, H. Wang, B. Zhou, and X. You, "DFT spread generalized multicarrier scheme for broadband mobile communications," in *Proceedings of the International Symposium on Personal, Indoor and Mobile Radio Communications,*, vol. 1, 2006, pp. 1–5.

[123] A. A. Assunção and J. B. Lima, "Recuperação de sequências em esquemas de comunicação multiusuário baseados na transformada fracional de Fourier," in *Anais do Simpósio Brasileiro de Telecomunicações (SBrT)*, Fortaleza, Brasil, 2013.

[124] J. B. Lima and R. M. Campello de Souza, "A multiple access technique based on the eigenstructure of the trigonometric transforms," in *Anais do Simpósio Brasileiro de Telecomunicações (SBrT)*, 2007.

[125] E. Sejdić, I. Djurović, and L. Stanković, "Fractional Fourier transform as a signal processing tool: overview of recent developments," *Signal Processing*, vol. 91, no. 6, pp. 1351–1369, 2011.

[126] C. F. Gauss, "Nachlass: Theoria interpolationis methodo nova tractata," *Carl Friedrich Gauss, Werke, Band 3: Königliche Gesellschaft der Wissenschaften, Göttingem*, pp. 265–330, 1866.

[127] C. Runge, "Über die zerlegung empirisch gegebener funktion in sinuswellen," *Z. Math. Phys.*, vol. 48, pp. 443–456, 1905.

[128] R. N. Bracewell, "Discrete Hartley transform," *Journal of the Optical Society of America*, vol. 73, no. 12, pp. 1832–1835, 1983.

[129] N. Ahmed, T. Natarajan, and K. Rao, "Discrete cosine transform," *IEEE Transactions on Computers*, vol. C-23, no. 1, pp. 90–93, Jan 1974.

[130] S. A. Martucci, "Symmetric convolution and the discrete sine and cosine transforms," *IEEE Transactions on Signal Processing*, vol. 42, pp. 1038–1051, 1994.

[131] A. K. Jain, "A sinusoidal family of unitary transforms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. PAMI-1, no. 4, pp. 356–365, Oct 1979.

APÊNDICE A

LISTA DE TRANSFORMADAS

Neste apêndice é resumida a nomenclatura, siglas, operadores e dada uma breve descrição das transformadas mencionadas e utilizadas nesta tese. A Tabela A.1 apresenta as transformadas discretas no corpo dos números reais e, fora da ordem cronológica, mostra a evolução das transformadas desde suas versões ordinárias e versões generalizadas até as versões fracionais.

A Tabela A.2 apresenta as transformadas em corpos finitos. Da mesma maneira, a disposição das transformadas busca mostrar a evolução desde suas versões ordinárias e versões generalizadas até as versões fracionais. As transformadas das últimas cinco linhas desta tabela são contribuições desta tese.

Tabela A.1: *Relação de transformadas discretas no corpo dos números reais.*

Transformada	Sigla	Operador	Ano/Ref.	Descrição
Fourier	DFT	$[\mathbf{F}]_{i,k}$	(1805) [126] (1905) [127]	Surgida, provavelmente, antes da transformada de Fourier contínua. Sem ser formalmente denominada de DFT, foi desenvolvida para o cálculo dos coeficientes de séries finitas de Fourier para análise harmônica. Na Tese também é chamada de DFT ordinária .
Hartley	DHT	$[\mathbf{H}]_{i,k}$	(1983) [128]	Transformada discreta de Hartley para funções discretas. Na Tese também é chamada de DHT ordinária.
Cosseno	DCT	$[\mathbf{C}]_{i,k}$	(1974) [129] (1994) [130]	Há 8 tipos de transformadas (DCT tipos 1,2,3 ou 4, e par ou ímpar), as quais são baseadas em extensões simétricas de uma sequência. Na Tese também é chamada de DCT ordinária.
Seno	DST	$[\mathbf{S}]_{i,k}$	(1979) [131] (1994) [130]	Há 8 tipos de transformadas (DST tipos 1,2,3 ou 4, e par ou ímpar), as quais são baseadas em extensões simétricas de uma sequência. Na Tese também é chamada de DST ordinária.
Fourier generalizada	GDFT	$[\mathbf{Fg}]_{i,k}$	(1976) [56]	Generalização da DFT para sequências estendidas com um tipo específico de simetria. Os elementos de sua matriz de transformação são dados por.
Hartley generalizada	GDHT	$[\mathbf{Hg}]_{i,k}$	(2009) [59]	Generalização da DHT para sequências estendidas com um tipo específico de simetria. Os elementos de sua matriz de transformação são dados por .
Fracional de Fourier	DFrFT	$[\mathbf{F}^a]_{i,k}$	(1972) [62] (2000) [17]	Generalização da DFT para potências fracionais do operador. Há diferentes abordagens para defini-la. Na Tese também é chamada de DFT fracional.
Fracional de Hartley	DFrHT	$[\mathbf{H}^a]_{i,k}$	(1998) [14]	Generalização da DHT para potências fracionais do operador. Há diferentes abordagens para defini-la. Na Tese também é chamada de DHT fracional.
Fracional do cosseno	DFrCT	$[\mathbf{C}^a]_{i,k}$	(2001) [19]	Generalização da DCT para potências fracionais do operador. Apenas para as DCT tipo 1 e 4. Na Tese também é chamada de DCT fracional.
Fracional do seno	DFrST	$[\mathbf{S}^a]_{i,k}$	(2001) [19]	Generalização da DST para potências fracionais do operador. Apenas para as DST tipo 1 e 4. Na Tese também é chamada de DST fracional.

Fonte: Próprio Autor.

Tabela A.2: *Relação das transformadas em corpos finitos.*

Transformada	Sigla	Operador	Ano/Ref.	Descrição
Fourier	FFFT	$[\mathbf{F}]_{i,k}$ Eq. (2.3)	(1971) [49]	DFT em corpos finitos. Na Tese também é chamada de transformada de Fourier sobre corpos finitos ordinária.
Numérica de Fourier-Mersenne	FMNT	$[\mathbf{F}]_{i,k}$ Eq. (2.3)	(1971) [66]	Transformada numérica, em que as componentes do vetor transformado estão em $\mathrm{GF}(p)$ e p é um número primo de Mersenne.
Numérica de Fourier-Fermat	FFNT	$[\mathbf{F}]_{i,k}$ Eq. (2.3)	(1974) [65]	Transformada numérica, em que as componentes do vetor transformado estão em $\mathrm{GF}(p)$ e p é um número primo de Fermat.
Hartley	FFHT	$[\mathbf{H}]_{i,k}$ Eq. (2.4)	(1998) [53]	DHT em corpos finitos. Na Tese também é chamada de transformada de Hartley sobre corpos finitos ordinária.
Numérica de Hartley-Mersenne	HMNT	$[\mathbf{H}]_{i,k}$ Eq. (2.4)	(2001) [64]	Transformada numérica, em que as componentes do vetor transformado estão em $\mathrm{GF}(p)$ e p é um número primo de Mersenne.
Numérica de Hartley-Fermat	HFNT	$[\mathbf{H}]_{i,k}$ Eq. (2.4)	(2001) [64]	Transformada numérica, em que as componentes do vetor transformado estão em $\mathrm{GF}(p)$ e p é um número primo de Fermat.
Z	FFZT	$[\mathbf{Z}]_{i,k}$	(2002) [73]	Transformada Z em corpos finitos. Tem-se as mesmas considerações sobre convergência em sequências de comprimento infinito.
Cosseno	FFCT	$[\mathbf{C}]_{i,k}$ Eq. (2.12) a (2.14)	(2003) [72]	DCT em corpos finitos. Há oito tipos de FFCT que dependem da extensão simétrica das sequências. Na Tese também é chamada de FFCT ordinária.
Seno	FFST	$[\mathbf{S}]_{i,k}$ Eq. (2.16) a (2.18)	(2005) [71]	DST em corpos finitos. Há oito tipos de FFST que dependem da extensão simétrica das sequências. Na Tese também é chamada de FFST ordinária.
Fourier generalizada	GFFFT	$[\mathbf{F_G}]_{i,k}$ Eq. (2.6)	(2011) [61]	Generalização da FFFT para sequências estendidas com um tipo específico de simetria. Tem-se que $[\mathbf{F_G}]_{i,k} = \sqrt{N^{-1}}\zeta^{(k+1/2)(i+1/2)}$.
Hartley generalizada	GFFHT	$[\mathbf{H_G}]_{i,k}$ Eq. (2.9)	Não publicada	Generalização da FFHT para sequências estendidas com um tipo específico de simetria. Tem-se que $[\mathbf{H_G}]_{i,k} = \sqrt{N^{-1}}\mathrm{cas}((k+1/2)(i+1/2))$.

Fonte: Próprio Autor.

Continuação da Tabela A.2.

Transformada	Sigla	Operador	Ano/Ref.	Descrição
Fracional de Fourier	GFrFT	$[\mathbf{F}^a]_{i,k}$	(2010) [21] (2014) [25]	Generalização da FFFT para potências fracionais do operador. Na Tese também é chamada de transformada fracional de Fourier em corpos finitos.
Fracional de Hartley	GFrHT	$[\mathbf{H}^a]_{i,k}$	(2014) [26]	Generalização da FFHT para potências fracionais do operador. Na Tese é chamada de transformada fracional de Hartley em corpos finitos.
Fracional do cosseno	GFrCT	$[\mathbf{C}^a]_{i,k}$	(2010) [24] (2014) [26]	Generalização da FFCT tipos 1 e 4 para potências fracionais do operador. No texto é chamada de transformada fracional do cosseno em corpos finitos.
Fracional do seno	GFrST	$[\mathbf{S}^a]_{i,k}$	(2010) [24] (2014) [26]	Generalização da FFST tipos 1 e 4 para potências fracionais do operador. Na Tese é chamada de transformada fracional do seno em corpos finitos.
Fracional de Fourier generalizada	GFrFT	$[\mathbf{F}_{\mathbf{F}}^a]_{i,k}$	Não publicada	Generalização da GFFFT para potências fracionais do operador. Na Tese é chamada de transformada fracional de Fourier em corpos finitos generalizada.
Fracional de Hartley generalizada	GFrHT	$[\mathbf{H}_{\mathbf{F}}^a]_{i,k}$	Não publicada	Generalização da GFFHT para potências fracionais do operador. Na Tese é chamada de transformada fracional de Hartley em corpos finitos generalizada.

Fonte: Próprio Autor.

APÊNDICE B

DEMONSTRAÇÕES

Neste apêndice são apresentadas as provas de algumas proposições introduzidas no Capítulo 3, necessárias para a caracterização das transformadas fracionais em corpos finitos baseadas na expansão espectral da matriz de transformação e em matrizes comutantes.

B.1 Proposições relacionadas à matriz S

Considere a matriz diagonal $\mathbf{T}$ de dimensão $N \times N$, cujos elementos não nulos sãos dados por $[T]_{n,n} = 2\cos_\zeta(n)$. A matriz $\mathbf{T}$ tem a forma

$$\mathbf{T} = \begin{bmatrix} 2\cos_\zeta(0) & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 2\cos_\zeta(1) & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 2\cos_\zeta(2) & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 2\cos_\zeta(N-1) \end{bmatrix} \pmod p. \tag{B.1}$$

Considere a matriz $\mathbf{U}$ de dimensão $N \times N$, cujas colunas são os vetores $\mathbf{u}_m$, $m = 0, \dots, N-1$, isto é, $\mathbf{U} := [\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_{N-1}]$. As componentes do vetor $\mathbf{u}_m$ são dadas por

$$u_m[n] := \begin{cases} 1, & \text{se } n = m-1 \text{ ou } n = m+1 \\ 0, & \text{c.c.} \end{cases}$$

para $n = 0, \ldots, N-1$. A matriz $\mathbf{U}$ tem a forma

$$\mathbf{S} = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & \ldots & 1 & 0 \end{bmatrix} \pmod{p}. \tag{B.2}$$

Lema B.1

Se $\mathbf{f}_m$ é a m-ésima coluna da matriz $\mathbf{F}$, matriz de transformação da FFFT definida na Equação (2.3), então

$$\mathbf{F}\mathbf{u}_m = \mathbf{T}\mathbf{f}_m,$$

para $m = 0, \ldots, N-1$.

Demonstração:

Considere que $[T]_{r,m}$ seja o elemento na r-ésima linha e m-ésima coluna da matriz $\mathbf{T}$, em que $r, m = 0, 1, \ldots, N-1$. Considere que $f_m[r]$ seja o r-ésimo elemento do vetor $\mathbf{f}_m$. Em virtude dos elementos não nulos estarem apenas na diagonal de $\mathbf{T}$, a multiplicação de $\mathbf{T}$ por $\mathbf{f}_m$ resulta em

$$[T]_{r,m} f_m[r] = (2\cos_\zeta(r) - 4)\,\zeta^{rm},$$

para $r, m = 0, 1, \ldots, N-1$.

Como a matriz $\mathbf{F}$ é simétrica, tem-se que $[F]_{r,m+1} = [F]_{r+1,m}$, ou seja, $\zeta^{r(m+1)} = \zeta^{m(r+1)}$. Assim,

$$\begin{aligned} \mathbf{F}\mathbf{u}_m &= [F]_{r,m+1} + [F]_{r,m-1} - 4[F]_{r,m} \\ &= \zeta^{r(m+1)} + \zeta^{r(m-1)} + \zeta^{r(m-1)} \\ &= \zeta^{rm} 2\cos_\zeta(r) - 4\zeta^{rm} = \zeta^{rm}\left(2\cos_\zeta(r) - 4\right). \end{aligned}$$

Logo, $\mathbf{T}\mathbf{f}_m = \mathbf{F}\mathbf{u}_m$. ■

B.1.1 Demonstração da Proposição 3.1

Proposição 3.1

As matrizes $\mathbf{F}$ e $\mathbf{S}$ comutam.

Demonstração:

Como a matriz $\mathbf{U}$ tem como colunas os vetores $\mathbf{u}_m$, $m = 0, 1, \ldots, N-1$, a partir do Lema B.1 conclui-se que $\mathbf{TF} = \mathbf{FU}$, e que

$$\begin{aligned} (\mathbf{TF})^t &= (\mathbf{FU})^t \\ \mathbf{UF} &= \mathbf{FT}, \end{aligned}$$

em que $\{.\}^t$ denota a transposta do argumento. Como a matriz $\mathbf{S}$, definida na Equação (3.3), pode ser escrita como $\mathbf{S} = \mathbf{U} + \mathbf{T}$, e as matrizes $\mathbf{F}$, $\mathbf{T}$ e $\mathbf{U}$ são simétricas, então

$$\begin{aligned} \mathbf{FS} &= \mathbf{F}(\mathbf{U} + \mathbf{T}) &= \mathbf{FU} + \mathbf{FT} \\ &= \mathbf{TF} + \mathbf{UF} &= \mathbf{SF}. \end{aligned}$$

Lema B.2

Considere as matrizes $\mathbf{S}$ *e* $\mathbf{L}$ *de dimensão* $2N \times 2N$*, definidas nas Equações (3.3) e (3.5), respectivamente. A transformação de similaridade* $\mathbf{LSL}^{-1}$ *separa em partes par (*$\mathbf{Ev}$*) e ímpar (*$\mathbf{Od}$*) a matriz* $\mathbf{S}$*, em que* $\mathbf{Ev}$ *é uma matriz de dimensão* $(N+1) \times (N+1)$ *e* $\mathbf{Od}$ *é uma matriz de dimensão* $(N-1) \times (N-1)$*.*

Demonstração:

Como $\mathbf{L}$ é simétrica, então $\mathbf{L}^{-1} = \mathbf{L}^T = \mathbf{L}$. Mostra-se que

- Se $\mathbf{v} = [v[0], v[1], \ldots, v[N-1], v[N], v[N-1], \ldots, v[1]]$ é um vetor de simetria par e comprimento $2N$, então o produto $\mathbf{vL}$ resulta no vetor $\hat{\mathbf{v}} = \sqrt{2}\left[\frac{1}{\sqrt{2}}\, v[0], v[1], \ldots, v[N-1], \frac{1}{\sqrt{2}}\, v_[N], 0, \ldots, 0\right]$.
- Se $\mathbf{v} = [0, v[1], \ldots, v[N-1], 0, -v[N-1], \ldots, -v[1]]$ é um vetor de simetria ímpar e comprimento $2N$, então o produto $\mathbf{vL}$ resulta no vetor $\tilde{\mathbf{v}} = \sqrt{2}\,[0, \ldots, 0, v[N-1], \ldots, v[1]]$.

Considere que $\mathbf{s}_n$ é a n-ésima coluna de $\mathbf{S}$, escrevendo $\mathbf{S} = [\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{2N-1}]$, o produto $\mathbf{LS} := [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{N-2}, \mathbf{r}_{N-1}]$ resulta em

$$\begin{aligned} \mathbf{LS} = \frac{1}{\sqrt{2}} \Big[& \sqrt{2}\mathbf{s}_0, \mathbf{s}_1 + \mathbf{s}_{2N-1}, \ldots, \mathbf{s}_{N-1} + \mathbf{s}_{N+1}, \sqrt{2}\mathbf{s}_N, \mathbf{s}_{N-1} - \mathbf{s}_{N+1}, \\ & \ldots, \mathbf{s}_1 - \mathbf{s}_{2N-1} \Big]^t . \end{aligned} \tag{B.3}$$

Assim, as $(N+1)$ primeiras linhas de $\mathbf{LS}$, $\mathbf{r}_0, \ldots, \mathbf{r}_N$, são vetores de simetria par, enquanto que as $(N-1)$ últimas linhas de $\mathbf{LS}$, $\mathbf{r}_{N+1}, \ldots, \mathbf{r}_{2N-1}$, são vetores de simetria ímpar.

Já o produto $\mathbf{LSL} = \left[\mathbf{r}'_0, \mathbf{r}'_1, \mathbf{r}'_2, \ldots, \mathbf{r}'_{2N-1}\right]$ resulta em

$$\begin{aligned}\mathbf{LSL} &= [\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{2N-1}]\,\mathbf{L} \\ &= [\mathbf{r}_0, \mathbf{r}_1 + \mathbf{r}_{2N-1}, \ldots, \mathbf{r}_{N-1} + \mathbf{r}_{N+1}, \mathbf{r}_N, \mathbf{r}_{N-1} - \mathbf{r}_{N+1}, \\ &\quad \ldots, \mathbf{r}_1 - \mathbf{r}_{N-1}]. \end{aligned} \tag{B.4}$$

Observe que os vetores $\mathbf{r}_0$ a $\mathbf{r}_N$ tem simetria par. Dessa maneira, $\mathbf{r}'_m = \sqrt{2}\left[\frac{1}{\sqrt{2}} r_m[0], r_m[1], \ldots, r_m[N-1], \frac{1}{\sqrt{2}} r_m[N], 0, \ldots, 0\right]$, para $m = 0, \ldots, N$.

Observe também que os vetores $\mathbf{r}_{N+1}$ a $\mathbf{r}_{2N-1}$ tem simetria ímpar. Dessa maneira, $\mathbf{r}'_m = \sqrt{2}\,[0, \ldots, 0, r_m[N-1], \ldots, r_m[1]]$, para $m = N+1, \ldots, 2N-1$.

Com isso, $\mathbf{LSL}^{-1}$ é a soma direta das matrizes $\mathbf{Ev}$ e $\mathbf{Od}$,

$$\mathbf{LSL}^{-1} = \begin{bmatrix} \mathbf{Ev} & \mathbf{0} \\ \mathbf{0} & \mathbf{Od} \end{bmatrix}.$$

Pelo fato de $\mathbf{S}$ ser uma matriz tridiagonal, as matrizes $\mathbf{Ev}$ e $\mathbf{Od}$ também são tridiagonais. De maneira similar, pode-se verificar o caso em que $\mathbf{L}$ tem dimensão $(2N+1) \times (2N+1)$, ímpar. Para este caso, $\mathbf{Ev}$ é uma matriz de dimensão $(N+2) \times (N+2)$ e $\mathbf{Od}$ é uma matriz de dimensão $(N-1) \times (N-1)$. ■

Lema B.3

Os autovetores de simetria par de $\mathbf{S}$ *são extensões simétricas dos autovetores de* $\mathbf{Ev}$. *Os autovetores de simetria ímpar de* $\mathbf{S}$ *são extensões simétricas dos autovetores de* $\mathbf{Od}$.

Demonstração:

Se $\mathbf{e}_k$ é um autovetor de $\mathbf{Ev}$, então o vetor $\mathbf{e} = [\mathbf{e}_k^t | 0 \ldots 0]^t$, para $k = 0, \ldots, \lfloor N/2 \rfloor$, é um autovetor de simetria par de $\mathbf{LSL}^{-1}$, uma vez que

$$\mathbf{LSL}^{-1}\mathbf{e} = \lambda\mathbf{e} \Longrightarrow \mathbf{S}\left(\mathbf{L}^{-1}\mathbf{e}\right) = \lambda\left(\mathbf{L}^{-1}\mathbf{e}\right).$$

De maneira análoga, se $\mathbf{o}_k$ é um autovetor de $\mathbf{Od}$, então $\mathbf{o} = [0 \ldots 0 | \mathbf{o}_k^t]^t$, para $k = 0, \ldots, \lfloor N/2 - 2 \rfloor$, é um autovetor de simetria ímpar de $\mathbf{LSL}^{-1}$, uma vez que

$$\mathbf{LSL}^{-1}\mathbf{o} = \lambda\mathbf{o} \Longrightarrow \mathbf{S}\left(\mathbf{L}^{-1}\mathbf{o}\right) = \lambda\left(\mathbf{L}^{-1}\mathbf{o}\right).$$

Como $\mathbf{L}^{-1} = \mathbf{L}$, é possível encontrar autovetores de $\mathbf{S}$ com simetria par, a partir de $\mathbf{Ev}$, ou com simetria ímpar, a partir de $\mathbf{Od}$, fazendo

$$\mathbf{u}_{2k} = \mathbf{L}[\mathbf{e}_k^t | 0 \ldots 0]^t, \;\; k = 0, \ldots, \left\lfloor \frac{N}{2} \right\rfloor, \tag{B.5}$$

e

$$\mathbf{u}_{2k+1} = \mathbf{L}[0 \ldots 0 | \mathbf{o}_k^t]^t, \;\; k = 0, \ldots, \left\lfloor \frac{N-3}{2} \right\rfloor, \tag{B.6}$$

respectivamente. ■

B.1.2 Demonstração da Proposição 3.2

Proposição 3.2

As matrizes $\mathbf{C}_1$, obtida pela Equação (2.12), e $\mathbf{Ev}$, obtida pela Equação (3.6), comutam. As matrizes $\mathbf{S}_1$, obtida pela Equação (2.16), e $\mathbf{Od}$, obtida pela Equação (3.6), comutam.

Demonstração:

Pela Proposição 2.6, se $\mathbf{v}$ é um autovetor de comprimento $2N$ e simetria par de $\mathbf{S}$, e portanto de $\mathbf{F}$, então $\hat{\mathbf{v}}$ é um autovetor de comprimento $(N+1)$ de $\mathbf{C}_1$.

Analisando o Lema B.2, se $\hat{\mathbf{v}}$ é um autovetor de $\mathbf{Ev}$, então $\hat{\mathbf{v}}$ é um autovetor de $\mathbf{C}_1$. Por ser tridigonal $\mathbf{Ev}$ tem um único conjunto de autovetores, $\hat{\mathbf{V}}$. Assim,

$$\begin{aligned} \mathbf{Ev}\mathbf{C}_1 &= \hat{\mathbf{V}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}^{-1}\mathbf{C}_1 = \mathbf{C}_1\hat{\mathbf{V}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}^{-1} \\ &= \mathbf{C}_1\mathbf{Ev} \end{aligned}$$

Considere que as matrizes $\mathbf{F}$, $\mathbf{S}$ e $\mathbf{L}$ tenham dimensão $2N \times 2N$. A matriz $\overline{\mathbf{F}}$, obtida pela transformação de similaridade $\mathbf{LFL}$, é tal que

$$\overline{\mathbf{F}} = \mathbf{LFL} = \begin{bmatrix} \mathbf{C}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{S}_1 \end{bmatrix},$$

em que $\mathbf{C}_1$ tem dimensão $(N+1) \times (N+1)$ e $\mathbf{S}_1$ tem dimensão $(N-1) \times (N-1)$.

A matriz $\overline{\mathbf{S}}$, obtida pela transformação de similaridade $\mathbf{LSL}$, é tal que

$$\overline{\mathbf{S}} = \mathbf{LSL} = \begin{bmatrix} \mathbf{Ev} & \mathbf{0} \\ \mathbf{0} & \mathbf{Od} \end{bmatrix},$$

em que $\mathbf{Ev}$ tem dimensão $(N+1) \times (N+1)$ e $\mathbf{Od}$ tem dimensão $(N-1) \times (N-1)$. ■

B.1.3 Demonstração da Proposição 3.3

Proposição 3.3

As matrizes $\mathbf{H}$, obtida da Equação (2.4) e $\mathbf{S}$, definida na Equação (3.3), comutam.

Demonstração:

Uma vez que $\mathbf{F}$ pode ser escrito de acordo com a Equação (2.23) e como $\mathbf{F}$ e $\mathbf{S}$ comutam,

$$(\mathbf{F_r} - \sqrt{-1}\mathbf{F_i})\mathbf{S} = \mathbf{S}(\mathbf{F_r} - \sqrt{-1}\mathbf{F_i}).$$

Como os elementos da matriz $\mathbf{S}$ pertencem a $\mathrm{GF}(p)$, as matrizes $\mathbf{F_r}$ e $\mathbf{F_i}$ comutam com $\mathbf{S}$. Dessa maneira,

$$\mathbf{HS} = (\mathbf{F_r} + \mathbf{F_i})\mathbf{S} = \mathbf{S}(\mathbf{F_r} + \mathbf{F_i}) = \mathbf{SH}.$$

B.2 Proposições relacionadas à matriz E

Considere a matriz diagonal $\mathbf{T}$ de dimensão $N \times N$, cujos elementos não nulos sãos dados por $[T]_{n,n} = 2\cos_\zeta(n + 1/2)$. A matriz $\mathbf{T}$ tem a forma

$$\mathbf{T} = \begin{bmatrix} 2\cos_\zeta\left(\frac{1}{2}\right) & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 2\cos_\zeta\left(\frac{3}{2}\right) & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 2\cos_\zeta\left(\frac{5}{2}\right) & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 2\cos_\zeta\left(\frac{N+1}{2}\right) \end{bmatrix} \pmod p. \tag{B.7}$$

Considere a matriz $\mathbf{U}$ de dimensão $N \times N$, cujas colunas são os vetores $\mathbf{u}_m$, $l = 0, \dots, N-1$, isto é, $\mathbf{U} := [\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_{N-1}]$. Os vetores $\mathbf{u}_m$ são definidos como:

- $\mathbf{u}_0 := [0, 1, \dots, -1]^t \pmod p$
- Para $m = 1, \dots, N-2$, e $n = 0, \dots, N-1$, $\mathbf{u}_m$ tem suas componentes dadas por:

$$u_m[n] := \begin{cases} 1, & \text{se } n = m-1 \text{ ou } n = m+1 \\ 0, & \text{c.c.} \end{cases}.$$

- $\mathbf{u}_{N-1} := [-1, \dots, 1, 0]^t \pmod p$

Lema B.4

Se $\mathbf{f}_m$ é a m-ésima coluna da matriz $\mathbf{F_G}$, então

$$\mathbf{F_G}\mathbf{u}_m = \mathbf{T}\mathbf{f}_m,$$

para $m = 0, \dots, N-1$.

Demonstração:

Para $m = 1, \ldots, N-2$, o resultado segue a demonstração do Lema B.1. Para $m = 0$, tem-se $\mathbf{u}_0$, $\mathbf{F_G u}_0 = \mathbf{f}_1 - \mathbf{f}_{N-1}$. Para $m = N-1$, tem-se $\mathbf{F_G u}_{N-1} = \mathbf{f}_{N-2} - \mathbf{f}_0$.

Fazendo $\overline{\mathbf{f}}_0 = \mathbf{T}\mathbf{f}_0$, a n-ésima componente do vetor $\overline{\mathbf{f}}_0$ é dada por

$$\begin{aligned} \overline{f}_0[n] &= \left(\zeta^{(n+1/2)} + \zeta^{-(n+1/2)}\right)\zeta^{1/2(n+1/2)} \\ &= \zeta^{\frac{3}{2}(n+1/2)} + \zeta^{-\frac{1}{2}(n+1/2)}. \end{aligned}$$

A n-ésima componente do vetor $\mathbf{f}_{N-1}$ é obtida por

$$f_{N-1}[n] = \zeta^{(N-1+1/2)(n+1/2)} = \zeta^{Nn}\zeta^{Nn/2}\zeta^{-1/2(n+1/2)} = -1\zeta^{-1/2(n+1/2)}.$$

Assim, $\mathbf{f}_1 = \zeta^{\frac{3}{2}(n+1/2)}$ e $\mathbf{f}_{N-1} = -\zeta^{(N-1/2)(n+1/2)}$, de forma que $\mathbf{F_G u}_0 = \mathbf{T}\mathbf{f}_0$. Fazendo $\overline{\mathbf{f}}_{N-1} = \mathbf{T}\mathbf{f}_{N-1}$, a n-ésima componente do vetor $\overline{\mathbf{f}}_{N-1}$ é dada por

$$\begin{aligned} \overline{f}_{N-1}[n] &= \left(\zeta^{(n+1/2)} + \zeta^{-(n+1/2)}\right)\zeta^{(N-1/2)(n+1/2)} \\ &= -1\left(\zeta^{n/2+1/4} + \zeta^{-3n/2-1/4}\right) \\ &= -1\left(\zeta^{1/2(n+1/2)} + \zeta^{-3/2(n+1/2)}\right). \end{aligned}$$

Assim, $\mathbf{f}_0 = \zeta^{\frac{1}{2}(n+1/2)}$ e $\mathbf{f}_{N-2} = -\zeta^{-3/2(n+1/2)}$, de forma que $\mathbf{F_G u}_{N-1} = \mathbf{T}\mathbf{f}_{N-1}$. ■

B.2.1 Demonstração da Proposição 3.4

Proposição 3.4

As matrizes $\mathbf{F_G}$, obtida pela Equação (2.6), e $\mathbf{E}$, obtida pela Equação (3.15), comutam. As matrizes $\mathbf{H_G}$, obtida pela Equação (2.9), e $\mathbf{E}$, obtida pela Equação (3.15), comutam.

Demonstração:

Analisando o Lema B.4, conclui-se que $\mathbf{TF_G} = \mathbf{F_G U}$, e que

$$\begin{aligned} (\mathbf{TF_G})^t &= (\mathbf{F_G U})^t \\ \mathbf{UF_G} &= \mathbf{F_G T}. \end{aligned}$$

Como a matriz $\mathbf{E}$ pode ser escrita como $\mathbf{E} = \mathbf{U} + \mathbf{T}$, e as matrizes $\mathbf{F_G}$, $\mathbf{T}$ e $\mathbf{U}$ são simétricas, então

$$\begin{aligned} \mathbf{F_G E} &= \mathbf{F_G}(\mathbf{U} + \mathbf{T}) &&= \mathbf{F_G U} + \mathbf{F_G T} \\ &= \mathbf{TF_G} + \mathbf{UF_G} &&= \mathbf{SF_G}. \end{aligned}$$

Uma vez que $\mathbf{F_G}$ pode ser escrito de acordo com a Equação (2.27) e como $\mathbf{F_G}$ e $\mathbf{E}$ comutam,

$$(\mathbf{F_{Gr}} - \sqrt{-1}\mathbf{F_{Gi}})\mathbf{E} = \mathbf{E}(\mathbf{F_{Gr}} - \sqrt{-1}\mathbf{F_{Gi}}).$$

Como os elementos da matriz $\mathbf{E}$ pertencem a $\mathrm{GF}(p)$, as matrizes $\mathbf{F_{Gr}}$ e $\mathbf{F_{Gi}}$ comutam com $\mathbf{S}$. Dessa maneira,

$$\mathbf{H_G E} = (\mathbf{F_{Gr}} + \mathbf{F_{Gi}})\mathbf{E} = \mathbf{E}(\mathbf{F_{Gr}} + \mathbf{F_{Gi}}) = \mathbf{EH}.$$

Lema B.5

Considere as matrizes $\mathbf{E}$ *e* $\mathbf{L}$ *de dimensão* $2N \times 2N$*, definidas nas Equações (3.15) e (3.5), respectivamente. A transformação de similaridade* $\mathbf{LEL}^{-1}$ *separa em partes par (*$\mathbf{Ev}$*) e ímpar (*$\mathbf{Od}$*) a matriz* $\mathbf{E}$*, em que* $\mathbf{Ev}$ *é uma matriz de dimensão* $N \times N$ *e* $\mathbf{Od}$ *é uma matriz de dimensão* $N \times N$*.*

Demonstração:

Como $\mathbf{L}$ é simétrica, então $\mathbf{L}^{-1} = \mathbf{L}^T = \mathbf{L}$. Mostra-se que

- Se $\mathbf{v} = [v[0], v[1], \ldots, v[N-1], v[N-1], \ldots, v_1, v_0]$ é um vetor de simetria par de comprimento $2N$, então o produto $\mathbf{vL}$ resulta no vetor $\hat{\mathbf{v}} = \sqrt{2}\,[v[0], v[1], \ldots, v[N-1], 0, \ldots, 0]$.
- Se $\mathbf{v} = [v[0], v[1], \ldots, v[N-1], -v[N-1], \ldots, -v[1], -v[0]]$ é um vetor simetria ímpar de comprimento $2N$, então o produto $\mathbf{vL}$ resulta no vetor $\tilde{\mathbf{v}} = \sqrt{2}\,[0, \ldots, 0, v[N-1], \ldots, v[1], v[0]]$.

Considere que $\mathbf{e}_n$ é a n-ésima coluna de $\mathbf{E}$, e escrevendo $\mathbf{E} = [\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{2N-1}]$, o produto $\mathbf{LE} := [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{N-2}, \mathbf{r}_{N-1}]$ resulta em

$$\mathbf{LE} = \frac{1}{\sqrt{2}} \quad [\mathbf{e}_0 + \mathbf{e}_{2N-1}, \ldots, \mathbf{e}_{N-1} + \mathbf{e}_{N+1}, \mathbf{e}_{N-1} - \mathbf{e}_{N+1}, \ldots, \mathbf{e}_0 - \mathbf{e}_{2N-1}]^t \quad \text{(B.8)}$$

Assim, as N primeiras linhas de $\mathbf{LE}$, $\mathbf{r}_0, \ldots, \mathbf{r}_{N-1}$, são vetores centro-simétricos pares, enquanto que as N últimas linhas de $\mathbf{LE}$, $\mathbf{r}_N, \ldots, \mathbf{r}_{2N-1}$, são vetores centro-simétricos ímpares. Já o produto $\mathbf{LEL} = \left[\mathbf{r}'_0, \mathbf{r}'_1, \mathbf{r}'_2, \ldots, \mathbf{r}'_{2N-1}\right]$ resulta em

$$\begin{aligned} \mathbf{LEL} &= [\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{2N-1}]\,\mathbf{L} \\ &= [\mathbf{r}_0 + \mathbf{r}_{2N-1}, \ldots, \mathbf{r}_{N-1} + \mathbf{r}_{N+1}, \mathbf{r}_{N-1} - \mathbf{r}_{N+1}, \ldots, \mathbf{r}_0 - \mathbf{r}_{2N-1}]. \quad \text{(B.9)} \end{aligned}$$

Observe que $\mathbf{r}_0$ a $\mathbf{r}_N$ são vetores centro-simétricos pares. Dessa maneira, $\mathbf{r}'_m = \sqrt{2}\,[r_m[0], \ldots, r_m[N-1], 0, \ldots, 0]$, para $m = 0, \ldots, N-1$.

Observe também que $\mathbf{r}_{N+1}$ a $\mathbf{r}_{2N-1}$ são vetores centro-simétricos ímpares. Dessa maneira, $\mathbf{r}'_m = \sqrt{2}\,[0,\ldots,0,r_m[N-1],\ldots,r_m[0]]$, para $m = N,\ldots,2N-1$.

Com isso, $\mathbf{LEL}^{-1}$ é a soma direta das matrizes $\mathbf{Ev}$ e $\mathbf{Od}$,

$$\mathbf{LEL}^{-1} = \begin{bmatrix} \mathbf{Ev} & \mathbf{0} \\ \mathbf{0} & \mathbf{Od} \end{bmatrix}.$$

Pelo fato de $\mathbf{S}$ ser uma matriz tridiagonal, as matrizes $\mathbf{Ev}$ e $\mathbf{Od}$ também são tridiagonais. De maneira similar, pode-se verificar o caso em que $\mathbf{L}$ tem dimensão $(2N+1)\times(2N+1)$, ímpar. Para este caso, $\mathbf{Ev}$ é uma matriz de dimensão $(N+1)\times(N+1)$ e $\mathbf{Od}$ é uma matriz de dimensão $N \times N$. ■

Lema B.6

Os autovetores centro-simétricos pares $\mathbf{E}$ *são extensões simétricas dos autovetores de* $\mathbf{Ev}$. *Os autovetores centro-simétricos ímpares* $\mathbf{E}$ *são extensões simétricas dos autovetores de* $\mathbf{Od}$.

Demonstração:

Se $\mathbf{e}_k$ é um autovetor de $\mathbf{Ev}$, então o vetor $\mathbf{e} = [\mathbf{e}_k^t|0\ldots0]^t$, para $k = 0,\ldots,\lfloor(N+1)/2\rfloor$, é um autovetor centro-simétrico par de $\mathbf{LEL}^{-1}$, uma vez que

$$\mathbf{LEL}^{-1}\mathbf{e} = \lambda\mathbf{e} \Longrightarrow \mathbf{E}\left(\mathbf{L}^{-1}\mathbf{e}\right) = \lambda\left(\mathbf{L}^{-1}\mathbf{e}\right).$$

De maneira análoga, se $\mathbf{o}_k$ é um autovetor de $\mathbf{Od}$, então $\mathbf{o} = [0\ldots0|\mathbf{o}_k^t]^t$, para $k = 0,\ldots,\lfloor N/2-2\rfloor$, é um autovetor centro-simétrico ímpar de $\mathbf{LEL}^{-1}$, uma vez que

$$\mathbf{LEL}^{-1}\mathbf{o} = \lambda\mathbf{o} \Longrightarrow \mathbf{E}\left(\mathbf{L}^{-1}\mathbf{o}\right) = \lambda\left(\mathbf{L}^{-1}\mathbf{o}\right).$$

Como $\mathbf{L}^{-1} = \mathbf{L}$, é possível encontrar autovetores centro-simétricos pares de $\mathbf{E}$ a partir de $\mathbf{Ev}$, ou autovetores centro-simétricos ímpares a partir de $\mathbf{Od}$, fazendo

$$\mathbf{u}_{2k} = \mathbf{L}[\mathbf{e}_k^T|0\ldots0]^T,\ \ k = 0,\ldots,\left\lfloor\frac{N+1}{2}\right\rfloor, \tag{B.10}$$

e

$$\mathbf{u}_{2k+1} = \mathbf{L}[0\ldots0|\mathbf{o}_k^T]^T,\ \ k = 0,\ldots,\left\lfloor\frac{N}{2}\right\rfloor, \tag{B.11}$$

respectivamente. ■

B.2.2 Demonstração da Proposição 3.5

Proposição 3.5

As matrizes $\mathbf{C}_4$ e $\mathbf{Od}$, definida em 3.19, comutam. As matrizes $\mathbf{S}_4$ e $\mathbf{Ev}$, definida em 3.19, comutam.

Demonstração:

Pela Proposição 2.9, se $\mathbf{v}$ é um autovetor centro-simétrico par de comprimento N de $\mathbf{E}$, e portanto de $\mathbf{F_G}$, então $\hat{\mathbf{v}}$ é um autovetor de comprimento $\lfloor \frac{N+1}{2} \rfloor$ de $\mathbf{S}_4$.

Analisando o Lema B.5, se $\hat{\mathbf{v}}$ é um autovetor de $\mathbf{Ev}$, então $\hat{\mathbf{v}}$ é um autovetor de $\mathbf{S}_4$. Por ser tridiagonal $\mathbf{Ev}$ tem um único conjunto de autovetores, $\hat{\mathbf{V}}$. Assim,

$$\begin{aligned} \mathbf{EvS}_1 &= \hat{\mathbf{V}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}^{-1}\mathbf{S}_4 = \mathbf{S}_4\hat{\mathbf{V}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}^{-1} \\ &= \mathbf{S}_4\mathbf{Ev}. \end{aligned}$$

Considere que as matrizes $\mathbf{F}$, $\mathbf{E}$ e $\mathbf{L}$ tenham dimensão $N \times 2$. A matriz $\overline{\mathbf{F}}$, obtida pela transformação de similaridade $\mathbf{LFL}$, é tal que

$$\overline{\mathbf{F}} = \mathbf{LFL} = \begin{bmatrix} \mathbf{S}_4 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_4 \end{bmatrix},$$

em que $\mathbf{S}_4$ tem dimensão $\lfloor \frac{N+1}{2} \rfloor \times \lfloor \frac{N+1}{2} \rfloor$ e $\mathbf{C}_4$ tem dimensão $\lfloor \frac{N}{2} \rfloor \times \lfloor \frac{N}{2} \rfloor$.

A matriz $\overline{\mathbf{E}}$, obtida pela transformação de similaridade $\mathbf{LEL}$, é tal que

$$\overline{\mathbf{E}} = \mathbf{LEL} = \begin{bmatrix} \mathbf{Ev} & \mathbf{0} \\ \mathbf{0} & \mathbf{Od} \end{bmatrix},$$

em que $\mathbf{Ev}$ tem dimensão $\lfloor \frac{N+1}{2} \rfloor \times \lfloor \frac{N+1}{2} \rfloor$ e $\mathbf{Od}$ tem dimensão $\lfloor \frac{N}{2} \rfloor \times \lfloor \frac{N}{2} \rfloor$. ■

APÊNDICE C

AUTOVALORES DA MATRIZ D

Neste apêndice é determinada a multiplicidade dos autovalores da matriz $\mathbf{D}$, apresentada na Tabela 4.1.

Proposição C.1

A matriz $\mathbf{D}$ *tem, no máximo, quatro autovalores distintos.*

Demonstração:

A matriz $\mathbf{D}$ tem ciclo 4 e suas potências inteiras são

$$\begin{aligned}
&\mathbf{D} = (\tfrac{1}{2}(1-j)\mathbf{I} + \tfrac{1}{2}(1+j)\\
&\mathbf{D}^2 = \left(\tfrac{1}{2}(1-j)\mathbf{I} + \tfrac{1}{2}(1+j)\mathbf{P}\right)^2 = \mathbf{P},\\
&\mathbf{D}^3 = \mathbf{PD},\\
&\mathbf{D}^4 = \mathbf{PD}^2 = \mathbf{I}
\end{aligned}$$

e o resultado segue. ■

Proposição C.2

A matriz inversa de $\mathbf{D}$ *é* $\mathbf{D}^{-1} = \frac{1}{2}(1+j)\mathbf{I} + \frac{1}{2}(1-j)\mathbf{P}$.

Demonstração:

Como $\mathbf{D}$ tem ciclo 4, então $\mathbf{D}^{-1} = \mathbf{D}^3$. Assim,

$$\begin{aligned}\mathbf{D}^{-1} &= \mathbf{D}^3 = \mathbf{PD} \\ &= \mathbf{P}\left(\frac{1}{2}(1-j)\mathbf{I} + \frac{1}{2}(1+j)\mathbf{P}\right) \\ &= \frac{1}{2}(1+j)\mathbf{I} + \frac{1}{2}(1-j)\mathbf{P}.\end{aligned}$$

Os possíveis autovalores (λ) de $\mathbf{D}$ são as 4 raízes da unidade ($\lambda^4 = 1$, $\lambda \in \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$). Isso não implica que todos estes sejam de fato autovalores de $\mathbf{D}$. Uma maneira de determinar os autovalores de $\mathbf{D}$ e suas multiplicidades é através de seu polinômio característico $P_{\mathbf{D}}(\lambda) = |\lambda\mathbf{I} - \mathbf{D}|$.

O Lema C.1 auxilia na obtenção do polinômio característico de $\mathbf{D}$.

Lema C.1

Para N par, a matriz de dimensão $N \times N$,

$$\mathbf{M} = \begin{bmatrix} b & 0 & \dots & 0 & 0 & \dots & 0 & c \\ 0 & b & \dots & 0 & 0 & \dots & c & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & b & c & \dots & 0 & 0 \\ 0 & 0 & \dots & c & b & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & c & \dots & 0 & 0 & \dots & b & 0 \\ c & 0 & \dots & 0 & 0 & \dots & 0 & b \end{bmatrix} \tag{C.1}$$

tem determinante dado por $\left(b^2 - c^2\right)^{\frac{N}{2}}$.

Demonstração:

Permutando a segunda e a última linhas de $\mathbf{M}$, obtém-se a matriz $\mathbf{M}'$,

$$\mathbf{M}' = \begin{bmatrix} b & 0 & \dots & 0 & 0 & \dots & 0 & c \\ c & 0 & \dots & 0 & 0 & \dots & 0 & b \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & b & c & \dots & 0 & 0 \\ 0 & 0 & \dots & c & b & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & c & \dots & 0 & 0 & \dots & b & 0 \\ 0 & b & \dots & 0 & 0 & \dots & c & 0 \end{bmatrix}. \tag{C.2}$$

Essa matriz tem em suas primeira e segunda linhas elementos nulos nas mesmas posições. Rearranjando as linhas de $\mathbf{M}$ de maneira que duas linhas consecutivas (1° linha e 2° linha,

3° linha e 4° linha, *etc*.) tenham elementos nulos nas mesmas posições, a matriz $\mathbf{M}'$ tem a seguinte estrutura

$$\mathbf{M}' = \begin{bmatrix} b & 0 & \dots & 0 & 0 & \dots & 0 & c \\ c & 0 & \dots & 0 & 0 & \dots & 0 & b \\ 0 & b & \dots & 0 & 0 & \dots & c & 0 \\ 0 & c & \dots & 0 & 0 & \dots & b & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & b & c & \dots & 0 & 0 \\ 0 & 0 & \dots & c & b & \dots & 0 & 0 \end{bmatrix}. \tag{C.3}$$

Obtém-se a matriz $\mathbf{M}'$ com um número par de permutações, então $|\mathbf{M}| = |\mathbf{M}'|$. O determinante de $\mathbf{M}'$ é dado por $|\mathbf{M}'| = \left(b^2 - c^2\right)|\mathbf{M}'_s|$, em que $\mathbf{M}'_s$ é obtida pela exclusão da primeira e segunda linhas de $\mathbf{M}'$. Tem-se ainda que $|\mathbf{M}'| = \left(b^2 - c^2\right)^2 |\mathbf{M}'_{s-1}|$, em que $\mathbf{M}'_{s-1}$ é obtida pela exclusão da primeira e segunda linhas de $\mathbf{M}'_{s-1}$. Em geral, observa-se que $|\mathbf{M}'| = \left(b^2 - c^2\right)^{s_0} |\mathbf{M}'_{s-s_0+1}|$, para $s_0 = 1, \dots, N/2$, de forma que $|\mathbf{M}| = |\mathbf{M}'| = \left(b^2 - c^2\right)^{\frac{N}{2}}$. ■

Considere $\mathbf{D}$ uma matriz de dimensão $N \times N$. Quando N é ímpar, $\mathbf{D}$ tem a estrutura

$$\mathbf{D} = \frac{1}{2}\begin{bmatrix} 2 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1-j & \dots & 0 & 0 & \dots & 1+j \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1-j & 1+j & \dots & 0 \\ 0 & 0 & \dots & 1+j & 1-j & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1+j & \dots & 0 & 0 & \dots & 1-j \end{bmatrix}. \tag{C.4}$$

Teorema C.1

Para N ímpar, o polinômio característico de $\mathbf{D}$ é

$$P_{\mathbf{D}}(\lambda) = (\lambda - 1)\left((2\lambda - 1 + j)^2 - (1+j)^2\right)^{\frac{N-1}{2}}. \tag{C.5}$$

Demonstração:

Fazendo $a = (\lambda - 1)$, $b = (2\lambda - 1 + j)$ e $c = (1 + j)$ na Equação (C.4), o polinômio

característico $P_{\mathbf{D}}(\lambda)$ torna-se

$$P_{\mathbf{D}}(\lambda) = \begin{vmatrix} a & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & b & \dots & 0 & 0 & \dots & c \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b & c & \dots & 0 \\ 0 & 0 & \dots & c & b & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & c & \dots & 0 & 0 & \dots & b \end{vmatrix} = (a) \begin{vmatrix} 0 & b & \dots & 0 & 0 & \dots & c \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b & c & \dots & 0 \\ 0 & 0 & \dots & c & b & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & c & \dots & 0 & 0 & \dots & b \end{vmatrix}.$$

A submatriz obtida excluindo-se a primeira linha tem a mesma estrutura que a matriz $\mathbf{M}$ do Lema C.1 e sua dimensão é um número par. Assim, $P_{\mathbf{D}}(\lambda) = a\left(b^2 - c^2\right)^{\frac{N-1}{2}}$, ou seja,

$$P_{\mathbf{D}}(\lambda) = (\lambda - 1)\left((2\lambda - 1 + j)^2 - (1 + j)^2\right)^{\frac{N-1}{2}}.$$

Teorema C.2

Para N ímpar, os autovalores de $\mathbf{D}$ são $\lambda = 1$, com multiplicidade $\frac{N+1}{2}$, e $\lambda = -j$, com multiplicidade $\frac{N-1}{2}$.

Demonstração:

Os autovalores de $\mathbf{D}$ são as raízes do polinômio $P_{\mathbf{D}}(\lambda)$, ou seja, as soluções de

$$(\lambda - 1)\left((2\lambda - 1 + j)^2 - (1 + j)^2\right)^{\frac{N-1}{2}} = 0.$$

Do termo $(2\lambda - 1 + j)^2 - (1 + j)^2)^{\frac{N-1}{2}} = 0$, tem-se que as raízes são $\lambda = 1$ e $\lambda = -j$ que ocorrem $\frac{N-1}{2}$ vezes. A raiz $\lambda = 1$ ocorre mais uma vez devido ao termo $\lambda - 1 = 0$. ■

Quando N é par, $\mathbf{D}$ tem a estrutura

$$\mathbf{D} = \frac{1}{2}\begin{bmatrix} 2 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 1-j & \dots & 0 & 0 & 0 & \dots & 1+j \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1-j & 0 & 1+j & \dots & 0 \\ 0 & 0 & \dots & 0 & 2 & 0 & \dots & 0 \\ 0 & 0 & \dots & 1+j & 0 & 1-j & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1+j & \dots & 0 & 0 & 0 & \dots & 1-j \end{bmatrix}. \tag{C.6}$$

Teorema C.3

Para N par, o polinômio característico de $\mathbf{D}$ é

$$P_{\mathbf{D}}(\lambda) = (\lambda - 1)^2 \left((2\lambda - 1 + j)^2 - (1 + j)^2\right)^{\frac{N-2}{2}}. \tag{C.7}$$

Demonstração:

Fazendo $a = (\lambda - 1)$, $b = (2\lambda - 1 + j)$ e $c = (1 + j)$ na Equação (C.6), o polinômio característico $P_{\mathbf{D}}(\lambda)$ torna-se

$$P_{\mathbf{D}}(\lambda) = \begin{vmatrix} a & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & b & 0 & \dots & 0 & 0 & 0 & \dots & 0 & c \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & 0 & \dots & b & 0 & c & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & a & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & c & 0 & b & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & c & 0 & \dots & 0 & 0 & 0 & \dots & 0 & b \end{vmatrix}. \tag{C.8}$$

Pode-se rearranjar as linhas de C.8 de forma que a $(N/2 + 1)-$ésima linha passe a ser a segunda linha, ou seja,

$$P'_{\mathbf{D}}(\lambda) = \begin{vmatrix} a & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & a & 0 & \dots & 0 & 0 \\ 0 & b & 0 & \dots & 0 & 0 & 0 & \dots & 0 & c \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & 0 & \dots & b & 0 & c & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & c & 0 & b & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & c & 0 & \dots & 0 & 0 & 0 & \dots & 0 & b \end{vmatrix}. \tag{C.9}$$

Este rearranjo é feito com um número par de permutações, logo $P_{\mathbf{D}}(\lambda) = P'_{\mathbf{D}}(\lambda)$. De maneira análoga à demonstração do Teorema C.1, o polinômio característico $P_{\mathbf{D}}(\lambda)$ é

$$P_{\mathbf{D}}(\lambda) \;=\; (a)^2 \begin{vmatrix} 0 & b & \dots & 0 & 0 & \dots & c \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b & c & \dots & 0 \\ 0 & 0 & \dots & c & b & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & c & \dots & 0 & 0 & \dots & b \end{vmatrix}.$$

Assim, $P_{\mathbf{D}}(\lambda) = a^2\left(b^2 - c^2\right)^{\frac{N-2}{2}} = (\lambda-1)^2\left((2\lambda - 1 + j)^2 - (1+j)^2\right)^{\frac{N-2}{2}}$. ■

Teorema C.4

Para N par, os autovalores de $\mathbf{D}$ são $\lambda = 1$, com multiplicidade $\frac{N+2}{2}$, e $\lambda = -j$, com multiplicidade $\frac{N-2}{2}$.

Demonstração:

Os autovalores de $\mathbf{D}$ são as raízes do polinômio $P_{\mathbf{D}}(\lambda)$, ou seja, as soluções de

$$(\lambda-1)^2\left((2\lambda - 1 + j)^2 - (1+j)^2\right)^{\frac{N-2}{2}} = 0.$$

Do termo $(2\lambda - 1 + j)^2 - (1+j)^2)^{\frac{N-1}{2}} = 0$, tem-se que as raízes são $\lambda = 1$ e $\lambda = -j$ que ocorrem $\frac{N-2}{2}$ vezes. A raiz $\lambda = 1$ ocorre mais duas vezes devido ao termo $(\lambda-1)^2 = 0$. ■

APÊNDICE D

ARTIGOS

D.1 Artigos publicados

NESTE apêndice são enumerados os artigos publicados até o presente com os resultados desta Tese, bem como os artigos submetidos.

1. J. B. Lima, R. M. Campello de Souza e P. H. E. S. Lima. "Transformada Fracional do Cosseno em Corpos Finitos". Anais do Simpósio Brasileiro de Telecomunicações (SBrT), 2012.
2. J. B. Lima, R. M. Campello de Souza and P. H. E. S. Lima. "Fractional number-theoretic transform based on matrix functions". Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), vol 24, no. 7, pp. 2614-2618, Florence, Italy, 2014.
3. P. H. E. S. Lima, J. B. Lima and R. M. Campello de Souza. "Hartley, Cosine and Sine Fractional Transforms over Finite Fields." Proceedings of the International Telecommunications Symposium (ITS), pp. 1-5, São Paulo, Brazil, 2014.
4. P. H. E. S. Lima, J. B. Lima e R. M. Campello de Souza. "Cifragem de Imagens Baseada na Transformada Fracional de Fourier sobre Corpos Finitos". Anais do XXXIII Simpósio Brasileiro de Telecomunicações (SBrT), 2015.

D.2 Artigos submetidos

1. P. H. E. S. Lima, J. B. Lima e R. M. Campello de Souza . "Fractional Fourier, Hartley, Cosine and Sine Number-Theoretic Transforms Based on Matrix Functions". Circuits, Systems and Signal Processing - Springer, 2015. (**Submetido**)