UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE TECNOLOGIA E GEOCIÊNCIAS

DEPARTAMENTO DE ELETRÔNICA E SISTEMAS

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

LUIZ CARLOS DA SILVA JÚNIOR

Transformada Numérica de Fourier Quaterniônica: Definições e Cenários de Aplicação

Brasil

2019

LUIZ CARLOS DA SILVA JÚNIOR

Transformada Numérica de Fourier Quaterniônica: Definições e Cenários de Aplicação

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

Área de Concentração: Comunicações.

Orientador: Prof. Dr. Juliano Bandeira Lima

Brasil

2019

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

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

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

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

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

UFPE

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

LUIZ CARLOS DA SILVA JÚNIOR

Transformada Numérica de Fourier Quaterniônica: Definições e Cenários de Aplicação

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

Área de Concentração: Comunicações.

Aprovado em: 31 / 05 / 2019 .

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

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

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

Prof. Dr. Gilson Jerônimo da Silva Jr. (Examinador Externo)
Universidade Federal de Pernambuco

Prof. Dr. Francisco Madeiro Bernardino Jr. (Examinador Externo)
Universidade de Pernambuco

Dedico esse trabalho primeiramente a Deus que me deu forças e à minha família por me compreender e amar.

AGRADECIMENTOS

Primeiramente agradeço a Deus por permitir essa realização e à minha família: Jaqueline (minha amada esposa), Luiz Carlos e Claudeci (meus pais), Luiz Fernando e Keyla (meu irmão e esposa), Geraldo e Isabel(meus sogros), Jhonatas (meu cunhado), aos meus discipuladores Carlsberg e Gilminha, aos meus tios e tias e a comunidade cristã em Jaboatão e Serra Talhada que sirvo com tanto amor.

Aos meus companheiros de ministério que foram tão pacientes com o meu processo, Anderson, Leandro e Daiane, Luciano e Fabiana, Érico e Daise e aos discípulos amados Rodolfo e Edilene, Luiz Henrique e Karine.

A minhas alunas e orientandas que tanto torceram pela minha formação e ao meu amigo e companheiro de trabalho e sua esposa, Mário e Poliana, por terem me apoiado nos momentos em que mais precisei.

Ao meu orientador Prof. Juliano, por ter me aceitado como orientando, mesmo eu sendo de uma área diferente durante toda a minha vida acadêmica; no campo acadêmico: o senhor é o exemplo de pesquisador, professor e orientador que pretendo tentar seguir. O senhor também é um exemplo de pessoa humilde, paciente (muito paciente) e bondoso; vejo que foi plano de Deus ter conhecido o senhor. Foi um grande prazer e honra ter trabalhado e ser orientado pelo senhor.

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

A todos os professores que participaram da minha formação.

A todos os técnicos e funcionaários da UFPE que participaram da minha estadia de mais de quatro anos nesta universidade, principalmente os do DES.

RESUMO

A contribuição central desta tese é a introdução de uma transformada numérica de Fourier quaterniônica (QFNT), isto é, uma transformada definida sobre quaternions cujos coeficientes se encontram num corpo finito primo. O estabelecimeto de tal ferramenta preenche uma importante lacuna existente na literatura de processamento / análise de sinais, uma vez que, até então, apenas transformadas de Fourier sobre quaternions de Hamilton haviam sido investigadas. A definição e a caracterização da QFNT requerem a derivação de diversos resultados referentes aos chamados quaterninos generalizados, como aqueles relacionados às suas ordens multiplicativas e a extensão a esse contexto de proposições associadas à trigonometria sobre corpos finitos; tais resultados, que também são introduzidos nesta tese, apoiam o desenvolvimento de propriedades da QFNT e sugerem cenários em que esta pode ser aplicável. Sobre este último ponto, o presente trabalho se volta especificamente ao processamento de imagens coloridas e demonstra, a partir de uma investigação preliminar, que a QFNT é útil na uniformização de histogramas com vistas à cifragem de tais imagens. Além disso, a QFNT é empregada como base de um esquema de marca d'água frágil e não-cego, em que a marca é inserida de forma "espalhada" em todos os canais de cor da imagem; os resultados obtidos demonstram que, utilizando o referido esquema, é possível localizar regiões da imagem que tenham sofrido manipulações não-autorizadas.

Palavras-chave: Quaternions de Hamilton. Quaternions generalizados. Corpos finitos. Transformada de Fourier quaterniônica. Transformada numérica de Fourier quaterniônica. Processamento digital de imagens. Cifragem de imagens. Marca d'água.

ABSTRACT

This thesis has as its main contribution the introduction of a quaternion Fourier number transform (QFNT), that is, a transform defined over quaternions whose coefficients lie in a prime finite field. The establishment of such a mathematical tool fulfills an important existing gap in the literature of signal processing / analysis, since only Fourier transforms over Hamilton quaternions had been investigated until then. The QFNT definition and characterization require the derivation of several results regarding the so called generalized quaternions, such as those related to their multiplicative orders and the extension to the current context of propositions associated to finite field trigonometry; such results, which are also introduced in this thesis, support the development of QFNT properties and suggest scenarios in which the transform can be applicable. With respect to the latter, this work specifically turns to the processing of color images and, based on a preliminary investigation, demonstrates that the QFNT is useful in uniformizing histograms for encryption of such images. Moreover, the QFNT is employed as the basis of a fragile non-blind watermarking scheme, where the watermark is "spread" across all color channels of an image; the obtained results show that, using the referred scheme, image regions that have been suffered non-authorized manipulation can be located.

Keywords: Hamilton quaternions. Generalized quaternions. Finite fields. Quaternions Fourier transform. Quaternion Fourier number transform. Digital image processing. Image encryption. Watermarking.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

DFT	Discrete Fourier transform
DFrFT	Discrete fractional Fourier transform
FNT	Fourier number transform
QFNT	Quaternion Fourier Number transform

SUMÁRIO

1 INTRODUÇÃO

As transformadas estão entre as ferramentas matemáticas mais úteis em aplicações em Engenharia e, em particular, em processamento de sinais. O seu histórico tem origem na transformada (ordinária) de Fourier, que é aplicável a funções ou sinais de variável contínua, chegando, mais recentemente, às diversas transformadas discretas e suas generalizações (SCHAFER; OPPENHEIM, 1999). Em meio a esta variedade de definições foram introduzidas, na década de 1970, as transformadas de Fourier sobre corpos finitos (POLLARD, 1971), as quais, no campo de processamento digital de sinais, são normalmente consideradas em versões mais específicas conhecidas como transformadas numéricas de Fourier. Mais recentemente, foram propostas transformadas de Fourier quaterniônicas, as quais são aplicáveis a funções ou sinais que assumem valores que podem ser interpretados como quaternions (ELL, 1993; ELL; SANGWINE, 2007).

Neste trabalho, introduz-se, pela primeira vez na literatura, uma transformada numérica de Fourier quaterniônica (QFNT, do inglês *quaternion Fourier number transform*). São apresentados diversos resultados teóricos inéditos, com base nos quais se define a referida transformada e se investiga suas principais propriedades. A partir do conteúdo desenvolvido, são realizados experimentos computacionais que permitem avaliar o desempenho da QFNT em alguns cenários de aplicação relacionados a processamento de imagem.

A seguir, é apresentado um apanhado conciso a respeito das transformadas numéricas e das transformadas quaterniônicas. Além disso, é exposta a motivação para a realização deste trabalho; são listados seus objetivos e contribuições, e descrita a sua estrutura.

1.1 TRANSFORMADAS NUMÉRICAS

Desde a década de 1970, as transformadas numéricas (NTT, do inglês *number-theoretic transforms*) têm sido amplamente investigadas e empregadas em diversos cenários de aplicação. Inicialmente, essas transformadas foram apresentadas como uma forma alternativa para calcular eficientemente convoluções livres de erro de arredondamento (POLLARD, 1971; REED; TRUONG, 1975; SHU; TIANREN, 1988, 1988). Naquele tempo, essa possibilidade, que advém do fato de as referidas transformadas serem definidas sobre corpos finitos, era de fundamental importância, uma vez que o *hardware* disponível trabalhava apenas com aritmética de ponto fixo. Mais recentemente, as NTT têm sido usadas principalmente em cenários relacionados à segurança de informação, os quais incluem, por exemplo, a cifragem de imagens (LIMA; NOVAES, 2014), a ocultação de dados (marca d'água) (LIMA; CAMPELLO DE SOUZA, 2005; CINTRA et al., 2009; CHEDDAD et al., 2010) e o processamento de sinais no domínio cifrado (PEDROUZO-ULLOA; TRONCOSO-PASTORIZA; PÉFEZ-GONZÁLEZ, 2017).

Usualmente, uma NTT é definida como um transformada do tipo da de Fourier, em que

a N-ésima raiz complexa da unidade usada como núcleo da transformada discreta de Fourier[1] (DFT, do inglês *discrete Fourier transform*) é substituída pela N-ésima raiz da unidade numa estrutura algébrica finita (POLLARD, 1971). Entretanto, outros tipos de NTT têm sido definidos; pode-se mencionar, por exemplo, as transformadas numéricas do cosseno (CAMPELLO DE SOUZA et al., 2003; LIMA; BARONE; CAMPELLO DESOUZA, 2016; LIMA; MADEIRO; SALES, 2015; LIMA, 2015), do seno (CAMPELLO DE SOUZA et al., 2005), de Hartley (CAMPELLO DE SOUZA et al.,) e de Hilbert (KAK, 2014), as quais são, em certo sentido, análogas às versões complexas e/ou reais das transformadas discretas com as nomenclaturas correspondentes. Generalizações das NTT também têm sido propostas; essas incluem, por exemplo, as transformadas numéricas fracionárias, as quais consistem em calcular potências racionais do operador matricial associado às NTT ordinárias correspondentes (LIMA; CAMPELLO DE SOUZA, 2016; LIMA; CAMPELLO DE SOUZA, 2013, 2013).

1.2 TRANSFORMADAS QUATERNIÔNICAS

Como a própria terminologia indica, as transformadas quaterniônicas são definidas empregando números denominados *quaternions*[2]. Esses por sua vez, podem ser compreendidos como uma extensão dos números complexos, sendo escritos sob a forma

$$a + bi + cj + dk,$$

em que a, b, c, e d são números reais e i, j e k são operadores complexos (ELL; SANGWINE, 2007). Os quaternions foram inicialmente descritos por William Rowan Hamilton, em 1843, e aplicados à Mecânica em espaços tridimensionais (MUKUNDAN, 2002). Também são encontradas aplicações dos quaternions em computação gráfica tridimensional (MUKUNDAN, 2002), visão computacional (PERVIN; WEBB, 1982) e análise de textura cristalográfica (BACHMANN; HIELSCHER; SCHAEBEN, 2010), por exemplo.

Em trabalhos mais recentes, os quaternions passaram a figurar na lista de ferramentas matemáticas importantes em aplicações relacionadas ao processamento de sinais. Como exemplos de tais aplicações, podem ser mencionados os algoritmos para filtragem quaterniônica adaptativa no domínio da frequência (ORTOLANI et al., 2017), as redes neurais com neurônios quaterniônicos (MINEMOTO et al., 2017) e diversas técnicas para processamento de imagens coloridas (ELL; SANGWINE, 2007; SANGWINE, 1998; SANGWINE; ELL, 2000; SANGWINE, 1996). Nesse contexto, desempenha um papel de destaque a transformada de Fourier quaterniônica (QFT, do inglês *quaternion Fourier transform*) que, tendo por núcleo um quaternion unitário apropriado, é aplicável a funções ou sinais que assumem valores sobre os

[1] Nas próximas seções e no restante desta tese, esta transformada numérica do tipo da de Fourier é identificada pelo acrônimo FNT, do inglês *Fourier number transform*.

[2] Na língua portuguesa, normalmente se usa *quatérnios*, o plural de *quatérnio*, ou *quaterniões*, o plural de *quaternião*. Porém, com o intuito de manter a uniformidade com relação ao termo em inglês, ao longo deste trabalho, usa-se *quaternions*, que corresponde ao plural de *quaternion*.

quaternions (ELL, 1992; ELL, 1993). Uma versão discreta dessa transformada, identificada como transformada discreta de Fourier quaterniônica (DQFT, do inglês *discrete quaternion Fourier transform*) também se encontra disponível, sendo aplicável a estruturas (vetores e matrizes) cujas entradas são quaternions (SANGWINE, 1996; SANGWINE et al., 2000; ELL; SANGWINE, 2007).

A última possibilidade mencionada, em particular, indica como uma imagem digital colorida (com três canais de cor, por exemplo) pode ser interpretada como uma matriz de quaternions: os valores numéricos associados a cada um dos três canais de cor de um pixel numa posição específica da imagem correspondem às componentes b, c, e d de um quaternion, enquanto se faz $a = 0$. Naturalmente, o mapeamento descrito é flexível e dá margem para que outras interpretações sejam empregadas; isso depende da aplicação e de que propriedades dos quaternions e da respectiva transformada de Fourier se pretende explorar.

1.3 MOTIVAÇÃO

As duas principais motivações para o desenvolvimento deste trabalho foram (i) o crescente interesse da comunidade científica especializada, sobretudo da comunidade de processamento de sinais, em ferramentas matemáticas e aplicações relacionadas aos quaternions e (ii) a verificação da existência de diversas lacunas teóricas nesse contexto. O ponto (i) tem reflexo no grande número de trabalhos recentes sobre o tema, que têm sido publicados em veículos importantes; além das referências já citadas nesta introdução, podem ser mencionados como exemplo disso os artigos listados nas referências bibliográficas de (FLETCHER et al., 2017). Com respeito ao ponto (ii), o que chama mais atenção é a escassez de avanços e aplicações em que, em vez dos quaternions usuais (de Hamilton), são considerados os chamados *quaternions generalizados*. Mais especificamente, verifica-se que a transformada discreta de Fourier quaterniônica não encontra uma transformada análoga definida sobre quaternions em que a, b, c e d, em vez de serem números reais, são tomados de um corpo finito; tal transformada seria uma espécie de versão quaterniônica da transformada numérica de Fourier.

1.4 OBJETIVOS

O objetivo geral deste trabalho é definir uma transformada numérica de Fourier quaterniônica; a ideia é que esta transformada esteja para a transformada numérica de Fourier assim como a transformada discreta de Fourier quaterniônica está para a transformada discreta de Fourier. Os objetivos específicos são os seguintes:

1. Reconhecer os conceitos e resultados a respeito de estuturas algébricas finitas mais importantes para o desenvolvimento deste trabalho;

2. Realizar um estudo revisivo a respeito dos quaternions, considerando, a partir dos quaternions de Hamilton, a possibilidade de construir quaternions generalizados sobre corpos

finitos;

3. Identificar propriedades de quaternions definidos sobre corpos finitos, avaliando a possibilidade de enunciar novos resultados nesse contexto;

4. Definir uma transformada numérica de Fourier quaterniônica, identificando suas variantes e estabelecendo suas propriedades;

5. Apresentar ideias preliminares a respeito dos cenários de aplicação da transformada numérica de Fourier quaterniônica, com ênfase no processamento digital de imagens coloridas;

6. Sugerir direções de pesquisa visando à extensão da definição da QFNT para outros tipos de transformadas numéricas quaterniônicas.

1.5 ESTRUTURA DA TESE E CONTRIBUIÇÕES

Esta tese está organizada da seguinte forma:

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

- No Capítulo 2, é apresentada uma revisão acerca da trigonometria sobre corpos finitos; é apresentada, também, a transformada numérica de Fourier (FNT, do inglês *Fourier number transform*), a qual é empregada como uma das referências para definição da transformada numérica de Fourier quaterniônica, e descrita sua autoestutura (autovalores e autovetores do operador matricial associado à FNT).

- No Capítulo 3, um breve histórico dos quaternions é apresentado; os quaternions de Hamilton são caracterizados e os chamados quaternions generalizados são descritos. Algumas propriedades desses últimos são listadas e questões relacionadas ao seu isomorfismo a estruturas algébricas formadas por matrizes são consideradas.

  A partir deste ponto, este trabalho põe o foco em quaternions generalizados sobre corpos finitos (primos), isto é, em quaternions que possuem a forma $a + bi + cj + dk$, em que $a, b, c, d \in \mathbb{F}_p$ e $\mathbb{F}_p$ denota o corpo finito com p elementos (p é um número primo ímpar). Neste cenário, este capítulo apresenta, também, as primeiras contribuições originais desta tese[3]: (i) a derivação de uma série de resultados especificamente ligados a quaternions sobre corpos finitos, que dão suporte à (ii) introdução de uma trigonometria associada a estes números e (iii) a sua caracterização com respeito à ordem multiplicativa.

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

- No Capítulo 4, apresenta-se a contribuição central deste trabalho: (iv) a definição da transformada numérica de Fourier quaterniônica. Para isso, é introduzido um novo lema, o qual é demonstrado a partir do estudo sobre a ordem multiplicativa de quaternions sobre corpos finitos realizado no capítulo anterior. Ainda neste capítulo, (v) são enunciadas algumas propriedades da nova transformada, (vi) é descrita a sua autoestrutura e (vii) são discutidas questões relacionadas ao seu cálculo.

- No Capítulo 5, é realizada uma discussão preliminar a respeito de possíveis aplicações da QFNT. O foco é o campo do processamento digital de imagens coloridas, em que, de modo mais específico, sugere-se o uso da transformada (viii) para uniformização de histogramas visando à cifragem de imagens e (ix) como base de um esquema de marca d'água frágil para imagens multicamadas. São exibidos resultados de simulações e conduzidas reflexões sobre o potencial de uso da QFNT em cenários práticos.

- No Capítulo 6, são apresentadas as considerações conclusivas desta tese, indicadas direções para a realização de pesquisas futuras e listados os artigos científicos resultantes do desenvolvimento deste trabalho.

2 TRIGONOMETRIA SOBRE CORPOS FINITOS E TRANSFORMADA NUMÉRICA DE FOURIER

DENTRE as diversas transformadas discretas estudadas em Engenharia, transformadas definidas sobre corpos finitos desempenham um importante papel em muitas aplicações. Conforme indicado no capítulo introdutório desta tese, tais transformadas são de fundamental importância por não introduzirem erros de arredondamento (SILVA; CAMPELLO DE SOUZA; OLIVEIRA, 2001) e por possuírem propriedades que as tornam adequadas para uso em processamento de imagem, criptografia, codificação de canal etc. (CINTRA et al., 2009; LIMA; LIMA; MADEIRO, 2013; LIMA; NOVAES, 2014). Neste capítulo, é apresentada uma breve revisão acerca da transformada numérica de Fourier (FNT), a transformada sobre corpos finitos mais antiga e mais amplamente estudada. O capítulo é iniciado, na próxima seção, com a apresentação de conceitos relacionados à trigonometria sobre corpos finitos, os quais serão úteis ao longo desta tese e cujo conhecimento é importante para a definição e a caracterização da versão da FNT considerada neste documento.

2.1 TRIGONOMETRIA SOBRE CORPOS FINITOS

Nesta seção, são revisados os principais conceitos relacionados à trigonometria sobre corpos finitos. A ideia de descrever tal trigonometria foi originalmente proposta em (CAMPELLO DE SOUZA et al., 1998), onde ela foi empregada como requisito para definição de uma transformada de Hartley sobre corpos finitos. Em trabalhos subsequentes, a teoria foi expandida, provendo suporte para definição de outras ferramentas matemáticas sobre as referidas estruturas algébricas e para o estudo de suas aplicações (**??**CAMPELLO DE SOUZA et al., 1998; **??**).

Definição 2.1. O conjunto de inteiros Gaussianos sobre $\mathbb{F}_p$ é o conjunto denotado por $\mathbb{I}_p$ cujos elementos possuem a forma $a + bi$, em que $a, b \in \mathbb{F}_p$ e i^2 é um não-resíduo quadrático sobre $\mathbb{F}_p$ (**??**).

Um elemento $\zeta \in \mathbb{I}_p$ pode ser visto como um número "complexo", o qual possui parte real e parte imaginária dadas por $\Re\{\zeta\} = a$ e $\Im\{\zeta\} = b$, respectivamente; $\zeta^* = a - bi$ denota o conjugado em corpo finito de $\zeta = a + bi$. Adicionalmente, observa-se que $\mathbb{I}_p$ é isomórfico a $\mathbb{F}_{p^2}$.

Definição 2.2. O conjunto unimodular de $\mathbb{I}_p$ é o conjunto $\mathrm{G}_{1,p}$ de elementos $a + bi \in \mathbb{I}_p$, tais que $\zeta \cdot \zeta^* = (a + bi) \cdot (a - bi) = a^2 - b^2 i^2 \equiv 1 \pmod{p}$ (**??**).

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

Proposição 2.1. *A estrutura $\langle \mathrm{G}_{1,p}, \cdot \rangle$ é um grupo cíclico de ordem $p + 1$ (**??**).*

A seguir, são definidas as funções trigonométricas sobre corpos finitos.

Definição 2.3. Seja $\zeta \in \mathbb{I}_p$ um elemento com ordem multiplicativa denotada por $\mathrm{ord}(\zeta)$. O cosseno e o seno sobre corpos finitos do ângulo relacionado a ζ^x são calculados módulo p, respectivamente, por

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

e

$$\sin_\zeta(x) = \frac{\zeta^x - \zeta^{-x}}{2i}, \tag{2.2}$$

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

Na Definição 2.3, uma referência explícita ao ângulo relacionado a ζ^x não é relevante; isso permite que se enxergue os cossenos e os senos sobre corpos finitos como funções $(\mathrm{ord}(\zeta))$-periódicas de x, dado um elemento ζ. Tais funções satisfazem algumas propriedades análogas àquelas das funções correspondentes definidas segundo a trigonometria usual (sobre os reais) (**????**). Como exemplo, pode-se considerar a propriedade de círculo unitário, a qual é escrita como

$$\cos^2_\zeta(x) - i^2 \sin^2_\zeta(x) = 1, \tag{2.3}$$

a fórmula de Euler

$$\zeta^x = \cos_\zeta(x) + i \sin_\zeta(x), \tag{2.4}$$

e o seno e o cosseno da soma de dois ângulos:

$$\sin_\zeta(x + y) = \sin_\zeta(x) \cos_\zeta(y) + \sin_\zeta(y) \cos_\zeta(x), \tag{2.5}$$

$$\cos_\zeta(x + y) = \cos_\zeta(x) \cos_\zeta(y) + i^2 \sin_\zeta(x) \sin_\zeta(y). \tag{2.6}$$

Note que, se $p \equiv 3 \pmod 4$ e $i = \sqrt{-1}$, as expressões (2.3) e (2.6) se tornam similares às identidades trigonométricas clássicas correspondentes. Propriedades de simetria das funções cosseno e seno são preservadas no contexto de corpos finitos, isto é, $\cos_\zeta(-x) = \cos_\zeta(x)$ e $\sin_\zeta(-x) = -\sin_\zeta(x)$.

A proposição a seguir estabelece uma particularidade no cálculo das funções cosseno e seno sobre corpos finitos, quando essas são avaliadas com respeito a um elemento pertencente a $\mathrm{G}_{1,p}$.

Proposição 2.2. *Seja $\zeta \in \mathbb{I}_p$ um elemento unimodular. A função cosseno e a função seno sobre corpos finitos do ângulo relacionado a ζ^x, a x-ésima potência de ζ, podem ser calculadas respectivamente como*

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

and

$$\sin_\zeta(x) = \mathfrak{I}\{\zeta^x\},$$

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

Outros diversos resultados da trigonometria sobre corpos finitos são omitidos nesta tese, mas podem ser consultados pelo leitor interessado. Esses incluem, por exemplo, a definição de polinômios de Chebyshev sobre corpos finitos segundo uma abordagem trigonométrica (**??**), a definição e a caracterização de função tangente sobre corpos finitos e de funções trigonométricas inversas sobre corpos finitos (**??**) e a definição dos diversos tipos de transformadas de Hartley, do cosseno e do seno sobre essas estruturas algébricas (**??**).

2.2 A TRANSFORMADA NUMÉRICA DE FOURIER

Nesta seção, é brevemente revisada a transformada numérica de Fourier. Num escopo mais geral, esta ferramenta permite que vetores N-dimensionais cujas componentes pertencem a um corpo de extensão $\mathbb{F}_q$, $q = p^m$, m inteiro sejam mapeados em vetores cujas componentes pertencem à mesma estrutura (**??**); esse é o caso em que a referida ferramenta recebe o nome de transformada de Fourier sobre corpos finitos. Por outro lado, podem ser consideradas versões dessas transformadas em que tanto as componentes do vetor original quanto as do vetor transformado correspondente pertençam ao corpo finito primo (corpo base) $\mathbb{F}_p$. Neste último caso, a transformada é normalmente conhecida como transformada numérica de Fourier.

No presente trabalho, considera-se uma transformada que mapeia vetores com componentes sobre $\mathbb{I}_p$ (ou $\mathbb{F}_{p^2}$) em vetores cujas componentes pertencem à mesma estrutura. Conforme o leitor poderá verificar ao longo dos próximos capítulos, tal escolha parece mais adequada ao estabelecimento de paralelos com as outras ferramentas que serão introduzidas e com as aplicações abordadas. Além disso, definir a transformada dessa forma permite analogias interessantes com a transformada discreta de Fourier, que realiza o mapeamento entre vetores com componentes complexas. Nesta tese, a transformada segundo a definição mencionada é chamada de *transformada numérica de Fourier* (embora não seja definida sobre um corpo primo simplesmente) e identificada pelo acrônimo FNT (do inglês *Fourier number transform*). Tal definição é formalizada a seguir.

Definição 2.4. A transformada numérica de Fourier de um vetor $\mathbf{x} = (x(n))$, $x(n) \in \mathbb{I}_p$, $n = 0, 1, \ldots, N-1$, é o vetor $\mathbf{X} = (X(k))$, $X(k) \in \mathbb{I}_p$, $k = 0, 1, \ldots, N-1$, com componentes calculadas por

$$X(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\zeta^{kn}, \tag{2.7}$$

em que $\zeta \in \mathrm{G}_{1,p}$ é um elemento cuja ordem multiplicativa é $\mathrm{ord}(\zeta) = N$.

A invertibilidade da FNT é demonstrada empregando o resultado a seguir.

Lema 2.1. *Um elemento $\zeta \in \mathbb{I}_p$, com ordem $\mathrm{ord}(\zeta) = N$, satisfaz*

$$\sum_{m=0}^{N-1} \zeta^{rm} = \begin{cases} N, & \textit{se } r \equiv 0 \pmod{N}, \\ 0, & \textit{caso contrário}. \end{cases} \tag{2.8}$$

Teorema 2.1. *A transformada numérica de Fourier inversa de um vetor $\mathbf{X} = (X(k))$, $X(k) \in \mathbb{I}_p$, $k = 0, 1, \ldots, N-1$, é o vetor $\mathbf{x} = (x(n))$, $x(n) \in \mathbb{I}_p$, $n = 0, 1, \ldots, N-1$, com componentes calculadas por*

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k)\zeta^{-kn}, \tag{2.9}$$

em que $\zeta \in \mathrm{G}_{1,p}$ é um elemento cuja ordem multiplicativa é $\mathrm{ord}(\zeta) = N$.

Pode-se expressar a cálculo da FNT de $\mathbf{x}$ por meio da equação matricial

$$\mathbf{X} = \mathbf{F}\mathbf{x}, \tag{2.10}$$

em que $\mathbf{F} = (F_{k,n})$, $F_{k,n} = \frac{1}{\sqrt{N}}\zeta^{kn}$, $k, n = 0, 1, \ldots, N-1$, denota a matriz de transformação da FNT.

A FNT possui diversas propriedades, a maior parte das quais está relacionada às propriedades da transformada discreta de Fourier (DFT) (**??**). Na seção a seguir, é revisada a autoestrutura da FNT (**??**), a qual será importante quando do desenvolvimento de resultados sobre a autoestrutura da FNT quaterniônica no Capítulo 4.

2.2.1 Autoestrutura da FNT

A autoestrutura da FNT, isto é, de sua matriz de transformação $\mathbf{F}$, possui certa analogia com a autoestrutura da DFT (**????**); seus autovalores são dados na proposição a seguir.

Proposição 2.3. *Os autovalores da matriz $\mathbf{F}$ da transformada numérica de Fourier com dimensões $N \times N$ pertencem a $\{1, -1, \sqrt{-1}, \sqrt{-1}\}$; as respectivas multiplicidades são mostradas na Tabela 1.*

Além disso, mostra-se que os seguintes resultados relacionados aos autovetores de $\mathbf{F}$ são válidos.

Proposição 2.4. *Todo autovetor de $\mathbf{F}$ possui simetria par, caso em que possui 1 ou -1 como autovalor associado, ou simetria ímpar, caso em que possui $\sqrt{-1}$ ou $-\sqrt{-1}$ como autovalor associado.*

Tabela 1 – Multiplicidades dos autovalores da matriz $\mathbf{F}$ da transformada numérica de Fourier com dimensões $N \times N$.

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

Proposição 2.5. *Seja* $\mathbf{x}$ *um vetor arbitrário, com componentes pertencentes a* $\mathbb{I}_p$ *e comprimento* N*, e* $\mathbf{X}$ *sua FNT. Então,*

1. $\mathbf{u} = \mathcal{E}\{\mathbf{x}\} \pm \mathcal{E}\{\mathbf{X}\}$*, em que* $\mathcal{E}\{\cdot\}$ *extrai a parte par do argumento, é um autovetor de* $\mathbf{F}$ *associado ao autovalor* ± 1*;*

2. $\mathbf{v} = \mathcal{O}\{\mathbf{x}\} \mp i\mathcal{O}\{\mathbf{X}\}$*, em que* $\mathcal{O}\{\cdot\}$ *extrai a parte ímpar do argumento, é um autovetor de* $\mathbf{F}$ *associado ao autovalor* $\pm\sqrt{-1}$*.*

2.2.2 Exemplos

Nesta seção, são apresentados exemplos ilustrativos acerca da definição de uma FNT e da construção de autovetores dessa transformada, associados a autovalores específicos.

Exemplo 2.1. *Seja* $\zeta = 2 + 2i \in \mathrm{G}_{1,p}$*,* $i = \sqrt{-1}$*, um elemento unimodular com ordem multiplicativa* $\mathrm{ord}(\zeta) = 8$ *empregado como núcleo de uma FNT. Então, a respectiva matriz de transformação (direta) é dada por*

$$\mathbf{F} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2+2i & i & 5+2i & 6 & 5+5i & 6i & 2+5i \\ 1 & i & 6 & 6i & 1 & i & 6 & 6i \\ 1 & 5+2i & 6i & 2+2i & 6 & 2+5i & i & 5+5i \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5+5i & i & 2+5i & 6 & 2+2i & 6i & 5+2i \\ 1 & 6i & 6 & i & 1 & 6i & 6 & i \\ 1 & 2+5i & 6i & 5+5i & 6 & 5+2i & i & 2+2i \end{bmatrix}, \tag{2.11}$$

A matriz de transformação inversa é dada por

$$\mathbf{F}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2+5i & 6i & 5+5i & 6 & 5+2i & 1i & 2+2i \\ 1 & 6i & 6 & i & 1 & 6i & 6 & i \\ 1 & 5+5i & i & 2+5i & 6 & 2+2i & 6i & 5+2i \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5+2i & 6i & 2+2i & 6 & 2+5i & i & 5+5i \\ 1 & i & 6 & 6i & 1 & i & 6 & 6i \\ 1 & 2+2i & i & 5+2i & 6 & 5+5i & 6i & 2+5i \end{bmatrix}, \tag{2.12}$$

A FNT do vetor

$$\mathbf{x} = [5+2i \quad 2+2i \quad 5+5i \quad 1 \quad 6i \quad 2+2i] \tag{2.13}$$

seria dada por

$$\mathbf{X} = [5+2i \quad 2+2i \quad 5+5i \quad 5+2i \quad i \quad 1 \quad 6i \quad 2+2i]. \tag{2.14}$$

Exemplo 2.2. *Considere a FNT definida no último exemplo, o vetor com simetria par*

$$\mathbf{x_e} = [1 \quad 3 \quad 5 \quad 6 \quad 2 \quad 6 \quad 5 \quad 3] \tag{2.15}$$

e o vetor com simetria ímpar

$$\mathbf{x_o} = [0 \quad 3 \quad 5 \quad 6 \quad 0 \quad 1 \quad 2 \quad 4], \tag{2.16}$$

bem como suas respectivas transformadas

$$\mathbf{X_e} = [1 \quad 3 \quad 5 \quad 6 \quad 2 \quad 6 \quad 5 \quad 3] \tag{2.17}$$

e

$$\mathbf{X_o} = [0 \quad 3 \quad 5 \quad 6 \quad 0 \quad 1 \quad 2 \quad 4]. \tag{2.18}$$

Então, os vetores

$$\mathbf{x_e} + \mathbf{X_e} = [1 \quad 3 \quad 5 \quad 6 \quad 2 \quad 6 \quad 5 \quad 3], \tag{2.19}$$

$$\mathbf{x_e} - \mathbf{X_e} = [0 \quad 3 \quad 5 \quad 6 \quad 0 \quad 1 \quad 2 \quad 4], \tag{2.20}$$

$$\mathbf{x_o} - i\mathbf{X_o} = [1 \quad 3 \quad 5 \quad 6 \quad 2 \quad 6 \quad 5 \quad 3] \tag{2.21}$$

e

$$\mathbf{x_o} + i\mathbf{X_o} = [0 \quad 3 \quad 5 \quad 6 \quad 0 \quad 1 \quad 2 \quad 4] \tag{2.22}$$

são autovetores da FNT associados aos autovalores 1, -1, $\sqrt{-1} = i$ *e* $-\sqrt{-1} = -i$, *respectivamente.*

3 QUATERNIONS DE HAMILTON E SUA FORMA GENERALIZADA

NESTE capítulo, são abordados os principais conceitos relacionados aos quaternions, números sobre os quais são desenvolvidas as contribuições desta tese. Inicialmente, a título de revisão, apresenta-se um breve histórico, a definição e as propriedades dos quaternions de Hamilton. Em seguida, são apresentados diversos resultados acerca dos chamados quaternions generalizados. Alguns desses resultados já se encontram documentados na literatura ou se tratam de meras extensões ao caso de interesse do presente trabalho: quaternions sobre corpos finitos; outros resultados são contribuições originais desta tese, como, por exemplo, os conceitos e proposições envolvendo trigonometria sobre quaternions generalizados em corpos finitos e o estudo sobre a ordem multiplicativa desses números. Ao longo do capítulo, a fim de situar o leitor, busca-se indicar com clareza o grau de novidade de cada resultado apresentado.

3.1 QUATERNIONS DE HAMILTON

Os números complexos tiveram origem na resolução de equações cúbicas em meados do século XVI (NEVES; GRIMBERG, 2008), problema ao qual se dedicaram nomes como Cardano, Bombelli e Tartaglia . Naquela época, a ideia era que qualquer solução algébrica deveria estar associada a uma representação geométrica; quando da impossibilidade de tais representações, a equação correspondente era considerada de solução inexistente, uma vez que, ainda que houvesse uma metodologia algébrica associada, esta não estaria "legitimada"; as equações cúbicas, por não possuírem uma representação geométrica, eram consideradas assim, sem solução.

René Descartes (1596-1650), em sua grandiosa obra *Discurso do Método*, foi o primeiro que identificou os, até então, chamados *números inexplicáveis* como *números imaginários*, os quais, na ocasião, eram entendidos como *números que poderiam ser imaginados* (e não como os números imaginários que se conhece hoje). Em algumas partes de sua obra, ele cita os números imaginários como uma forma de explicar a impossibilidade de representação geométrica para soluções de algumas equações cúbicas (DESCARTES, 1637). A possibilidade de representar geometricamente os *números imaginários* funcionaria, então, como uma confirmação da existência de tais entidades algébricas, bem como da corretude de sua caracterização; a ausência de tal representação era motivo de cautela para os matemáticos da época de Bombelli, Cardano e Tartaglia, quando da exposição de resultados tidos como novos nesse contexto.

John Wallis (1616-1703), em sua obra intitulada *Tratado de Álgebra* (1685), foi o primeiro a admitir uma construção geométrica para os números ditos até o momento como *números imaginários* (NASCIMENTO, 2016). Entretanto, o matemático que primeiro expôs sua representação como se conhece hoje foi o norueguês Caspar Wessel (1745-1818), em sua obra apresentada à *Royal Danish Academy of Sciences and Letters*, em 1797 (WESSEL, 1797). Em

sua pesquisa, o francês Jean-Robert Argand (1768-1822) obteve a mesma percepção de Wessel; seu trabalho intitulado *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques* pode ser considerado como uma das grandes obras do século XIX, pois, até os dias atuais, ele repercute na forma da "representação de Argand-Gauss" ou "plano de Argand-Gauss" (JÚNIOR, 2009).

O problema que deu origem aos números complexos tinha chegado ao fim com a sua representação geométrica. A interpretação geométrica desses números forneceu métodos analíticos simples para a realização de dois tipos de transformações no plano, as translações, por meio da adição, e as rotações, por meio da multiplicação. A partir desse modelo para o plano, um questionamento a respeito da possibilidade de se obter um modelo analítico similar para o espaço, com as mesmas interpretações geométricas, surgia. Com relação à propriedade aditiva, tanto o plano como o espaço tinham construções similares; tal similaridade, porém, não se confirmava na multiplicação.

Na tentativa de estender para o espaço as descobertas feitas até então, William Rowan Hamilton (1805-1865) criou uma nova classe de números imaginários denominados tripletos e denotados por (x, y, z); era uma tentativa de estender para o espaço as mesmas propriedades da multiplicação dos pares numéricos (x, y). Sua preocupação era definir uma multiplicação para esses novos números que pudesse ser interpretada como uma rotação no espaço. Não tendo obtido sucesso do ponto de vista geométrico, Hamilton passou a utilizar um modelo algébrico para representar os tripletos, escrevendo-os como $x + yi + zj$. Segundo ele, os tripletos também poderiam ser interpretados de maneira geométrica como uma linha orientada no espaço, sendo x, y, z suas "coordenadas retangulares" (HAMILTON, 1837).

Hamilton propôs que a unidade j tivesse a mesma representação de i, ou seja, $\sqrt{-1}$. Além disso, as operações entre os tripletos deveriam ser análogas àquelas definidas para os números imaginários do tipo (x, y), o que lhes asseguraria propriedades de comutatividade, associatividade, existência de elemento identidade e de elementos simétricos; isso permitiria identificar os tripletos como um corpo (HAMILTON, 1837). Todavia, conforme mencionado anteriormente, o estabelecimento da referida analogia encontrou obstáculo na operação de multiplicação. De modo mais específico, realizando o produto

$$(x_1 + y_1 i + z_1 j) \cdot (x_2 + y_2 i + z_2 j),$$

ter-se-ia como resultado

$$(x_1 x_2 - y_1 y_2 - z_1 z_2) + (x_1 y_2 + y_1 x_2)i + (x_1 z_2 + z_1 x_2)j + (y_1 z_2 + y_2 z_1)ij.$$

Embora várias tentativas tenham sido feitas, não se pôde explicar o termo ij na última equação à luz da teoria dos tripletos; a conjectura estabelecida por Hamilton, de que o produto entre dois tripletos deveria resultar em um tripleto, tinha aparentemente falhado. Diante disso, Hamilton propôs que se tivesse $ij = -ji = k$, o que resultou no surgimento de uma nova dimensão e, por

conseguinte, na descoberta de um nova classe de números imaginários denominados quaternions. Um quaternion seria, então, expresso por

$$x_1 + y_1 i + z_1 j + w_1 k.$$

Em uma carta direcionada ao filho Archibaldi, ele narra a descoberta que realizou:

"Mas no dia 16 do mesmo mês (outubro de l843) - que era uma segunda-feira e dia de reunião do Conselho da Real Sociedade da Irlanda - eu ia andando para participar e presidir, e tua mãe andava comigo, ao longo do Royal Canal. Embora ela falasse comigo ocasionalmente, uma corrente subjacente de pensamento estava acontecendo na minha mente, que finalmente teve um resultado, cuja importância senti imediatamente. Pareceu como se um circuito elétrico tivesse se fechado; e saltou uma faísca, o arauto de muitos anos vindouros de pensamento e trabalho dirigidos, por mim, se poupado, e de qualquer forma por parte de outros, se eu vivesse o suficiente para comunicar minha descoberta. Nesse instante eu peguei um caderneta de anotações que ainda existe e fiz um registro naquela hora. Não pude resistir ao impulso - tão não filosófico quanto possa ser - de gravar com um canivete numa pedra da ponte de Brougham, quando a cruzamos, a fórmula fundamental dos símbolos i, j, k,

$$i^2 = j^2 = k^2 = ijk = -1,$$

que contém a solução do problema."

Assim, surgiram os quaternions, os quais se conhece hoje como quaternions de Hamilton (HAMILTON, 2000; ELL; SANGWINE, 2007; SANGWINE; ELL, 2000; SANGWINE; ELL, 1999):

$$q = a + bi + cj + dk, \tag{3.1}$$

em que a, b, c e d são números reais e i, j e k são operadores complexos, que obedecem as seguintes regras:

$$ijk = i^2 = j^2 = k^2 = -1, \tag{3.2}$$

e

$$jk = -kj = i, \;\; ki = -ik = j, \;\; ij = -ji = k. \tag{3.3}$$

A adição entre dois quaternions $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ e $q_2 = a_2 + b_2 i + c_2 j + d_2 k$ segue a regra:

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k. \tag{3.4}$$

O produto entre os quaternions q_1 e q_2 é dado por:

$$\begin{aligned} q_1 q_2 = {} & (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i \\ & + (a_1 c_2 + c_1 a_2 + d_1 b_2 - b_1 d_2)j + (a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2)k. \end{aligned} \tag{3.5}$$

Um quaternion pode ser divido em duas partes, uma parte real (ou escalar) representada por $S(q) = a$ e uma parte imaginária (ou vetorial), que possui três componentes, representada por $V(q) = bi + cj + dk$. Pode-se, dessa forma, reescrever (3.1) como

$$q = S(q) + V(q). \tag{3.6}$$

Um quaternion com a parte escalar nula, ou seja, $S(q) = 0$ é chamado de quaternion puro.

O produto escalar e o produto vetorial entre as partes vetoriais dos quaternions q_1 e q_2, são calculados, respectivamente, por

$$q_1 \bullet q_2 := b_1b_2 + c_1c_2 + d_1d_2 \tag{3.7}$$

e

$$q_1 \times q_2 = \begin{bmatrix} i & j & k \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{bmatrix} := (c_1d_2 - c_2d_1)i + (d_1b_2 - b_1d_2)j + (b_1c_2 - c_1b_2)i, \tag{3.8}$$

em que o símbolo $:=$ indica *igual por definição*. Com isso, pode-se expressar o produto entre dois quaternions como

$$q_1q_2 = S(q_1)S(q_2) - V(q_1) \bullet V(q_2) + S(q_1)V(q_2) + V(q_1)S(q_2) + V(q_1) \times V(q_2). \tag{3.9}$$

O complexo conjugado do quaternion $q_1 = a_1 + b_1i + c_1j + d_1k$ é denotado por q_1^*, sendo dado por

$$q_1^* = S(q) - V(q) = a_1 - b_1i - c_1j - d_1k. \tag{3.10}$$

Mostra-se que $(q_1q_2)^* = q_2^*q_1^*$.

A módulo de um quaternion q_1 é dada por $|q_1| = \sqrt{q_1^*q_1} = \sqrt{a_1^2 + b_1^2 + c_1^2 + d_1^2}$ e sua norma é $||q|| = |q|^2$. Um quaternion com norma unitária é chamado de quaternion unitário.

O inverso de um quaternion é dado por

$$q^{-1} = \frac{q^*}{|q|^2}, \tag{3.11}$$

de maneira que $q^{-1}q = qq^{-1} = 1$.

A fórmula de Euler na forma hipercomplexa é

$$e^{\mu\Phi} = \cos\Phi + \mu\sin\Phi, \tag{3.12}$$

em que μ é um quaternion puro unitário. Um quaternion pode ser representado na forma polar como

$$q = |q|e^{\mu\Phi}. \tag{3.13}$$

Pode-se, ainda, representar um quaternion como uma combinação de dois números complexos. Essa forma é conhecida como forma de Cayley-Dickson (ELL; SANGWINE, 2007):

$$q = A + Bj, \tag{3.14}$$

em que $A = a + bi$ e $B = c + di$, de modo que se tem

$$q = (a + bi) + (c + di)j = a + bi + cj + dk. \tag{3.15}$$

A representação na forma de Cayley-Dickson pode ser generalizada empregando quaternions puros unitários μ, tal que $\mu^2 = -1$ (os operadores i, j e k são casos especiais de μ). Escolhendo dois quaternions μ_1 e μ_2 com as referidas propriedades e, ainda, que satisfaçam $\mu_1 \perp \mu_2$, pode-se representar um quaternion arbitrário como

$$q = A' + B'\mu_2, \tag{3.16}$$

em que $A' = a' + b'\mu_1$ e $B' = c' + d'\mu_1$, de modo que

$$q = (a' + b'\mu_1) + (c' + d'\mu_1)\mu_2. \tag{3.17}$$

A representação (3.16) é denominada forma simplética; A' e B' são denominadas, respectivamente, parte simplex e parte perplex do quaternion. Expandindo (3.17), obtém-se

$$q = a' + b'\mu_1 + c'\mu_2 + d'\mu_3,$$

em que $\mu_3 = \mu_1\mu_2$ e, além disso, $\mu_3 \perp \mu_1$ e $\mu_3 \perp \mu_2$. Dessa forma, o sistema baseado nos operadores μ_1, μ_2 e μ_3 é isomórfico àquele baseado em i, j e k. Consequentemente, a relação entre as quádruplas (a, b, c, d) e (a', b', c', d') equivale a uma mudança de base de (i, j, k) para (μ_1, μ_2, μ_3).

3.2 QUATERNIONS GENERALIZADOS

A álgebra usual de quaternions, estabelecida sobre os números reais $\mathbb{R}$, pode ser estabelecida sobre um corpo arbitrário $\mathbb{F}$ com característica diferente de 2. Mais especificamente, dados $\alpha, \beta \in \mathbb{F}$, em que α e β são não-nulos, pode-se definir uma álgebra de quaternions denotada por $A = \left(\frac{\alpha,\beta}{\mathbb{F}}\right)$, onde A é um espaço com quatro dimensões, podendo ser denominado também como um $\mathbb{F}$-espaço com base $1, i, j, k$, em que os parâmetros i e j são geradores que satisfazem às seguintes relações (LAM, 2005):

$$i^2 = \alpha, \;\; j^2 = \beta, \;\; ij = -ji. \tag{3.18}$$

Define-se, ainda, $k := ij \in A$ e tem-se $k^2 = (ij)(ij) = -i^2j^2 = -\alpha\beta \in \mathbb{F}$, e $ik = -ki = \alpha j$, $kj = -jk = \beta i$, de modo que os elementos i, j, k são anticomutativos. É importante notar que, para o caso em que $\mathbb{F} = \mathbb{R}$ e $\alpha = \beta = -1$, $\left(\frac{-1,-1}{\mathbb{R}}\right)$ é o anel de divisão usual dos quaternions sobre os reais, isto é, os quaternions de Hamilton que são descritos na última seção e que podem ser denotados por $\mathcal{H}$. A estrutura denotada por $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$, estabelecida sobre $\mathbb{F}$, corresponde a uma generalização direta de $\mathcal{H}$.

Teorema 3.1. *O conjunto* $\{1, i, j, k\}$ *forma uma* $\mathbb{F}$*-base para* A*, de modo que* $\dim_{\mathbb{F}} A = 4$.

Demonstração. Sejam γ e δ pertencentes ao fecho algébrico[1] $\mathbb{E}$ de $\mathbb{F}$ tais que $\gamma^2 = -\alpha$ e $\delta^2 = \beta$; considere as matrizes

$$i_0 = \begin{bmatrix} 0 & \gamma \\ -\gamma & 0 \end{bmatrix}$$

e

$$j_0 = \begin{bmatrix} 0 & \delta \\ \delta & 0 \end{bmatrix}$$

em $M_2(\mathbb{E})$ (a álgebra das matrizes 2×2 sobre $\mathbb{E}$). Cálculos diretos mostram que $i_0^2 = \alpha\mathbf{I}$ e $j_0^2 = \beta\mathbf{I}$, em que $\mathbf{I}$ denota a matriz identidade 2×2 e

$$i_0 j_0 = \begin{bmatrix} \gamma\delta & 0 \\ 0 & -\gamma\delta \end{bmatrix} = -j_0 i_0.$$

Assim, existe um homomorfismo $\varphi : \left(\frac{\alpha,\beta}{\mathbb{F}}\right) \to M_2(\mathbb{E})$, com $\varphi(i) = i_0$ e $\varphi(j) = j_0$. Uma vez que o conjunto $\{\mathbf{I}, i_0, j_0, i_0 j_0\}$ é claramente linearmente independente sobre $\mathbb{E}$, o conjunto $\{1, i, j, ij\}$ é linearmente independente sobre $\mathbb{F}$. □

Conforme indicado anteriormente, $\mathcal{H}$ é uma álgebra de divisão, isto é, cada elemento não-nulo de $\mathcal{H}$ é inversível. Em geral, $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$ não precisa ser uma álgebra de divisão; isso depende da escolha de $\mathbb{F}$, α e β. De fato, há apenas duas possibilidades:

1. $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$ é uma álgebra de divisão;
2. $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$ é isomórfico a $M_2(\mathbb{F})$, a álgebra de matrizes 2×2 com entradas pertencentes a $\mathbb{F}$.

A forma mais rápida de enxergar as duas possibilidades enumeradas é notar que $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$ é uma álgebra simples central, ou seja, ela tem $\mathbb{F}$ como centro e é simples por não possuir ideais bilaterais não-triviais, e, então, empregar um famoso teorema estabelecido por J. H. M. Wedderburn em 1907. Este teorema afirma que qualquer álgebra simples central, com dimensão finita sobre seu centro, é isomórfica a uma álgebra $M_n(\mathbb{D})$ para algum inteiro n e alguma álgebra de divisão $\mathbb{D}$ sobre $\mathbb{F}$. Considerando que $\dim_{\mathbb{F}} \left(\frac{\alpha,\beta}{\mathbb{F}}\right) = 4$ e $\dim_{\mathbb{F}} M_n(\mathbb{D}) = n^2 \dim_{\mathbb{F}} \mathbb{D}$, as únicas possibilidades são $n = 1$, $\left(\frac{\alpha,\beta}{\mathbb{F}}\right) = \mathbb{D}$ ou $n = 2$, $\mathbb{D} = \mathbb{F}$.

A identificação do caso em que determinada álgebra de quaternions se enquadra depende de propriedades da respectiva *norma*. Para clarificar tal questão, considere $q \in \left(\frac{\alpha,\beta}{\mathbb{F}}\right)$, $q = a + bi + cj + dk$, e seu conjugado $q^* = a - bi - cj - dk$; considere também o mapeamento $N : \left(\frac{\alpha,\beta}{\mathbb{F}}\right) \to \mathbb{F}$, tal que $N(q) = q^* q$ para cada $q \in \left(\frac{\alpha,\beta}{\mathbb{F}}\right)$. Como

$$N(q) = q^* q = q q^* = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2,$$

[1] Uma extensão $\mathbb{E}$ de um corpo $\mathbb{F}$ é um fecho algébrico de $\mathbb{F}$ quando $\mathbb{E}$ é uma extensão algébrica que é algebricamente fechada, isto é, contém todas as raízes de polinômios com coeficientes em $\mathbb{F}$. Levando em conta a possibilidade de isomorfismo, cada corpo $\mathbb{F}$ tem apenas um fecho algébrico.

N pode ser visto como uma forma quadrática em quatro variáveis, a, b, c e d, a qual é conhecida como *forma de norma* da álgebra de quaternions. Na notação padrão da teoria de formas quadráticas, essa forma é denotada por $\langle 1, -\alpha, -\beta, \alpha\beta \rangle$, o que corresponde a representar a forma quadrática por uma matriz diagonal com 1, $-\alpha$, $-\beta$ e $\alpha\beta$ como entradas.

Sempre que $N(q) \neq 0$, o elemento q é inversível; seu inverso é dado por $\left(\frac{1}{N(q)}\right) q^*$. De fato, q é inversível, se e somente se $N(q) \neq 0$, uma vez que $N(q) = 0$ implica que q é um divisor de 0. Com isso, tem-se o seguinte:

Teorema 3.2. *A álgebra de quaternions* $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$ *é uma álgebra de divisão se e somente se sua forma de norma não representa zero não-trivialmente, isto é,* $N(q) = 0 \Rightarrow q = 0$.

Na linguagem da teoria de formas quadráticas, uma forma que satisfaz à condição enunciada no Teorema 3.2 é dita ser anisotrópica. Empregando tal terminologia, pode-se afirmar, por exemplo, que a forma de norma de qualquer álgebra de quaternions $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$, em que $\mathbb{F}$ é um corpo finito, é isotrópica; consequentemente, $\left(\frac{\alpha,\beta}{\mathbb{F}}\right)$ é isomórfico a $M_2(\mathbb{F})$. Esse isomorfismo pode ser explicitado mapeando-se, por exemplo, i em

$$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

e j em

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Com isso, tem-se $k := ij = -ji$ mapeado em

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Dessa forma, $q = a + bi + cj + dk$ é mapeado na matriz

$$\mathbf{Q} = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix},$$

como visto em (LEWIS, 2006; VOIGHT, 2014; CIGLIOLA,).

De fato, ao longo deste trabalho, são considerados predominantemente quaternions generalizados em que $\mathbb{F} = \mathbb{F}_p$ é um corpo finito primo (com característica ímpar p); isso porque é sobre esses quaternions que se pretende definir uma transformada análoga à de Fourier. O estudo de operações e de propriedades envolvendo especificamente esses quaternions, aparentemente, não se encontra disponível na literatura. De qualquer forma, algumas dessas operações e propriedades são meras extensões do que se tem para os quaternions de Hamilton. A adição e os produtos, por exemplo, são efetuados conforme as regras anteriormente expostas neste capítulo, porém, considerando o uso da aritmética modular apropriada ao se somar, multiplicar ou tomar o

simétrico aditivo de elementos pertencentes a $\mathbb{F}_p$, e levando em conta o fato de que α e β não são necessariamente iguais a -1.

O complexo conjugado de um quaternion generalizado sobre $\mathbb{F}_p$ também é dado como em (3.10), tomando-se os simétricos aditivos módulo p de b_1, c_1 e d_1, naturalmente. De modo semelhante, define-se a norma de um quaternion generalizado sobre $\mathbb{F}_p$ bem como o seu inverso. Conforme anteriormente discutido, um desses quaternions generalizados, ainda que não seja nulo, pode ter norma nula, o que, obviamente, implica em sua não invertibilidade. Um quaternion sobre $\mathbb{F}_p$ unitário é aquele que tem norma igual a 1. As operações e propriedades mencionadas podem ser, respectivamente, efetuadas e verificadas considerando a representação matricial dos quaternions em questão.

Um quaternion generalizado $q = a + bi + cj + dk$ pode ser escrito em termos de suas partes escalar e vetorial como

$$q = S(q) + V(q),$$

em que $S(q) = a$ e $V(q) = bi + cj + dk$. Isso permite que se obtenha o seguinte desenvolvimento a respeito do produto entre dois quaternions generalizados $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ e $q_2 = a_2 + b_2 i + c_2 j + d_2 k$:

$$\begin{aligned} q_1 q_2 &= (S(q_1) + V(q_1))(S(q_1) + V(q_1)) \\ &= S(q_1)S(q_2) + S(q_1)V(q_1) + S(q_2)V(q_1) + V(q_1)V(q_2) \\ &= S(q_1)S(q_2) + S(q_1)V(q_2) + V(q_1)S(q_2) + V(q_1) \bullet V(q_2) + V(q_1) \times V(q_2). \end{aligned} \tag{3.19}$$

Na última equação, $\bullet$ e $\times$ denotam respectivamente o produto escalar e o vetorial entre os operandos; no caso generalizado, tais produtos são calculados de acordo com

$$V(q_1) \bullet V(q_2) := b_1 b_2 i^2 + c_1 c_2 j^2 + d_1 d_2 k^2 \tag{3.20}$$

e

$$V(q_1) \times V(q_2) = \begin{bmatrix} i & j & k \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{bmatrix} := (c_1 d_2 - c_2 d_1)i + (d_1 b_2 - b_1 d_2)j + (b_1 c_2 - c_1 b_2)k. \tag{3.21}$$

A proposição a seguir, que constitui uma contribuição original desta tese, é útil na caracterização de potências de um quaternion generalizado sobre corpos finitos.

Proposição 3.1. *Seja $q = S(q) + V(q)$ um quaternion sobre $\mathbb{F}_p$. Qualquer potência de q possui como sua parte vetorial $V(q^x)$, $x \in \mathbb{Z}$, um múltiplo escalar de $V(q)$, isto é, $V(q^x) = \rho V(q)$, $\rho \in \mathbb{F}_p$.*

Demonstração. Usando (3.19), q^2 pode ser escrito como

$$q^2 = S(q)S(q) - V(q) \bullet V(q) + S(q)V(q) + V(q)S(q) + V(q) \times V(q).$$

O último termo da última equação é nulo, de modo que se tem

$$q^2 = S(q^2) + V(q^2),$$

em que $S(q^2) = S(q)S(q) - V(q) \bullet V(q)$ e $V(q^2) = 2S(q)V(q)$. Considerando o fato de que o produto vetorial entre dois vetores que possuem a mesma direção é nulo, uma conclusão similar pode ser obtida para q^x, $x = 3, 4, \ldots$, de onde o resultado segue. □

A seguir, caracteriza-se o conjunto unimodular relacionado a quaternions generalizados sobre $\mathbb{F}_p$.

Definição 3.1. O conjunto unimodular de $\left(\frac{\alpha,\beta}{\mathbb{F}_p}\right)$ é o conjunto $\mathrm{Q}_{1,p}$ formado pelos elementos $q = a+bi+cj+dk$, tais que $qq^* = (a+bi+cj+dk)(a-bi-cj-dk) = a^2-b^2i^2-c^2j^2-d^2k^2 \equiv 1 \pmod{p}$, isto é, $|q| = 1$.

Na proposição a seguir, caracteriza-se o conjunto $\mathrm{Q}_{1,p}$ com respeito ao seu fechamento sob a operação de multiplicação.

Proposição 3.2. *O conjunto $\mathrm{Q}_{1,p}$ é fechado com respeito à operação de multiplicação.*

Demonstração. Seja $q_3 = q_1q_2$ um quaternion generalizado sobre $\mathbb{F}_p$ e $q_1, q_2 \in \mathrm{Q}_{1,p}$. Claramente, tem-se $q_3^{-1} = q_2^{-1}q_1^{-1} = q_2^*q_1^*$. Se se escrever $q_1 = a_1+b_1i+c_1j+d_1k$ e $q_2 = a_2+b_2i+c_2j+d_2k$, pode-se demonstrar diretamente que $q_3^* = (q_1q_2)^* = q_2^*q_1^* = q_3^{-1}$, de onde segue o resultado. □

As representações na forma de Cayley-Dickson e na simplética também são admissíveis para os quaternions generalizados considerados. Observe que, nesta última representação, o que basicamente se tem é a escrita de um quaternion numa base (μ_1, μ_2, μ_3) formada por quaternions puros. Assim, diferentemente do que normalmente se estabelece no caso de quaternions de Hamilton, não é necessário que μ_1, μ_2 e μ_3, vistos como vetores num espaço tridimensional, formem um conjunto ortonormal, isto é, sejam ortogonais e de norma unitária; é suficiente que eles formem um conjunto linearmente independente para que a referida representação seja factível.

3.2.1 Trigonometria sobre Quaternions Generalizados em Corpos Finitos

Nesta seção, que é toda constituída de contribuições originais desta tese, são introduzidos conceitos relacionados à trigonometria sobre quaternions cujas componentes pertencem a um corpo finito $\mathbb{F}_p$. Isso permitirá estender a fórmula de Euler ao cenário em questão e obter diversos outros resultados interessantes. Primeiramente, são definidas as funções cosseno e seno relacionadas ao ângulo de um quaternion $q \in \left(\frac{\alpha,\beta}{\mathbb{F}_p}\right)$.

Definição 3.2. Seja $q \in \left(\frac{\alpha,\beta}{\mathbb{F}_p}\right)$ um quaternion generalizado com ordem multiplicativa[2] denotada por $\mathrm{ord}(q)$ e μ um quaternion puro pertencente à mesma estrutura. O cosseno e o seno quaterniônicos do ângulo relacionado a q^x, a x-ésima potência de q, são definidos respectivamente como

$$\cos_q(x) = \frac{q^x + q^{-x}}{2} \tag{3.22}$$

e

$$\sin_q(x) = \frac{q^x - q^{-x}}{2\mu}, \tag{3.23}$$

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

Usando a Definição 3.2, estabelece-se a seguinte generalização para a fórmula de Euler:

$$q^x = \cos_q(x) + \mu \sin_q(x). \tag{3.24}$$

Propriedades relacionadas às funções $\cos_q(x)$ e $\sin_q(x)$ também podem ser derivadas. De forma bem direta, verifica-se que tais funções possuem, respectivamente, simetria par e ímpar, isto é, $\cos_q(x) = \cos_q(-x)$ e $\sin_q(x) = -\sin_q(-x)$. Os argumentos do cosseno e do seno quaterniônicos são sempre calculados $(\mathrm{mod}\ \mathrm{ord}(q))$; a ordem $\mathrm{ord}(q)$ também corresponde ao período de tais funções. Se cossenos e senos quaterniônicos forem calculados com respeito a um quaternion generalizado unimodular, a seguinte proposição pode ser estabelecida.

Proposição 3.3. *Sejam $q \in \mathrm{Q}_{1,p}$ um quaternion generalizado unimodular com ordem multiplicativa denotada por $\mathrm{ord}(q)$ e $\mu = V(\mu)$ um quaternion puro que satisfaz $\mu = \nu V(q)$, $\nu \in \mathbb{F}_p$ e $\nu \neq 0$. Então, o cosseno e o seno quaterniônicos do ângulo relacionado a q^x, $x = 0, 1, \ldots, \mathrm{ord}(q) - 1$, pertencem a $\mathbb{F}_p$. Mais especificamente, o referido cosseno é dado por*

$$\cos_q(x) = S(q^x). \tag{3.25}$$

Demonstração. Uma vez que $\mathrm{Q}_{1,p}$ é fechado com respeito à multiplicação (Proposição 3.2), se q é unimodular, então q^x também é unimodular. Dessa forma, se q^x for escrito como $q^x = a + bi + cj + dk$, tem-se $q^{-x} = (q^x)^* = a - bi - cj - dk$ e, portanto, (3.22) pode ser expressa como

$$\cos_q(x) = \frac{a + bi + cj + dk + a - bi - cj - dk}{2} = a = S(q^x).$$

De modo similar, (3.23) pode ser expressa como

$$\sin_q(x) = \frac{a + bi + cj + dk - a + bi + cj + dk}{2\mu} = \frac{(bi + cj + dk)}{\mu} = \frac{V(q^x)}{\mu}.$$

[2] Detalhes relacionados à ordem multiplicativa de quaternions generalizados sobre $\mathbb{F}_p$ são discutidos na próxima seção; por enquanto, assume-se simplesmente que os quaternions em questão possuem tal ordem.

Devido à Proposição 3.1, sabe-se que existe um elemento $\rho \in \mathbb{F}_p$, tal que $V(q^x) = \rho V(q)$. Portanto, a última equação pode ser reescrita como

$$\operatorname{sin}_q(x) = \frac{\rho V(q)}{\nu V(q)} = \rho \nu^{-1}.$$

□

A seguinte proposição indica que é possível escolher um quaternion generalizado unimodular q e um inteiro Gaussiano unimodular ζ sobre $\mathbb{F}_p$, de modo que se obtenha coincidência, para cada argumento inteiro x, entre os senos e cossenos calculados com respeito aos referidos elementos, isto é, $\operatorname{cos}_q(x) = \operatorname{cos}_\zeta(x)$ e $\operatorname{sin}_q(x) = \operatorname{sin}_\zeta(x)$.

Proposição 3.4. *Se $q = a + bi + cj + dk \in \mathrm{Q}_{1,p}$ é um quaternion generalizado unimodular sobre $\mathbb{F}_p$ e $\zeta = a_1 + b_1 i \in \mathrm{G}_{1,p}$ é um inteiro Gaussiano unimodular sobre $\mathbb{F}_p$, tais que $a_1 = a = S(q)$ e $(b_1 i)^2 = V(q) \bullet V(q) = b^2 i^2 + c^2 j^2 + d^2 k^2$, e $\mu = V(\mu)$ é um quaternion puro que satisfaz $\mu = b_1^{-1} V(q)$, $b \in \mathbb{F}_p$ e $b \neq 0$, então $\operatorname{cos}_q(x) = \operatorname{cos}_\zeta(x)$ e $\operatorname{sin}_q(x) = \operatorname{sin}_\zeta(x)$, para todo $x \in \mathbb{Z}$.*

Demonstração. Usando o Teorema Binomial, a seguinte expansão pode ser realizada:

$$q^x = (S(q) + V(q))^x = \sum_{k=0}^{x} \binom{x}{k} [S(q)]^{x-k} [V(q)]^k.$$

Uma vez que $[V(q)]^2 = V(q) \bullet V(q) + V(q) \times V(q) = V(q) \bullet V(q)$ (veja a prova da Proposição 3.1), sabe-se que $[V(q)]^k = [V(q) \bullet V(q)]^{\frac{k}{2}}$, se k for par, e $[V(q)]^k = [V(q) \bullet V(q)]^{\frac{k-1}{2}} V(q)$, se k for ímpar. Isso permite reescrever a última equação como

$$q^x = \sum_{k \text{ par}} \binom{x}{k} [S(q)]^{x-k} [V(q) \bullet V(q)]^{\frac{k}{2}} + \sum_{k \text{ ímpar}} \binom{x}{k} [S(q)]^{x-k} [V(q) \bullet V(q)]^{\frac{k-1}{2}} V(q),$$

a qual, juntamente com a Proposição 3.3, permite que se conclua que

$$\operatorname{cos}_q(x) = \sum_{k \text{ par}} \binom{x}{k} [S(q)]^{x-k} [V(q) \bullet V(q)]^{\frac{k}{2}} \tag{3.26}$$

e

$$\operatorname{sin}_q(x) = \frac{\sum_{k \text{ ímpar}} \binom{x}{k} [S(q)]^{x-k} [V(q) \bullet V(q)]^{\frac{k-1}{2}} V(q)}{\mu} \tag{3.27}$$

$$= \sum_{k \text{ ímpar}} \binom{x}{k} [S(q)]^{x-k} [V(q) \bullet V(q)]^{\frac{k-1}{2}} b_1. \tag{3.28}$$

De modo similar, obtém-se

$$\zeta^x = (a_1 + b_1 i)^x = \sum_{k=0}^{x} \binom{x}{k} a_1^{x-k} (b_1 i)^k \tag{3.29}$$

$$= \sum_{k \text{ par}} \binom{x}{k} a_1^{x-k} [(b_1 i)^2]^{\frac{k}{2}} + \sum_{k \text{ ímpar}} \binom{x}{k} a_1^{x-k} [(b_1 i)^2]^{\frac{k-1}{2}} b_1 i \tag{3.30}$$

e, usando a Proposição 2.2, conclui-se que

$$\cos_\zeta(x) = \sum_{k \text{ par}} \binom{x}{k} a_1^{x-k} [(b_1 i)^2]^{\frac{k}{2}} \tag{3.31}$$

e

$$\sin_\zeta(x) = \sum_{k \text{ ímpar}} \binom{x}{k} a_1^{x-k} [(b_1 i)^2]^{\frac{k-1}{2}} b_1. \tag{3.32}$$

Verifica-se que (3.26) corresponde a (3.31) depois que a_1 e $(b_1 i)^2$ são substituídos por $S(q)$ e $V(q) \bullet V(q)$, respectivamente. Adicionalmente, (3.28) corresponde a (3.32) depois que a mesma substituição é realizada. □

3.2.2 Exemplos

Exemplo 3.1. *Neste exemplo, são ilustrados alguns conceitos relacionados a quaternions generalizados sobre corpos finitos. É considerada a álgebra* $A = \left(\frac{6,6}{\mathbb{F}_7}\right)$*, o que significa que se tem* $i^2 = j^2 = \alpha = \beta = 6$*. No que se segue, todas as operações entre escalares são efetuadas utilizando aritmética módulo* 7 *(o símbolo "*$(\text{mod } 7)$*" é omitido, exceto em pontos do texto em que seu uso seja útil para evitar interpretações errôneas por parte do leitor). É considerado o quaternion*

$$q_1 = 1 + 3i + 4j + 2k,$$

o qual pode ser mapeado na matriz

$$\begin{bmatrix} 1+3i & 4+2i \\ 3+2i & 1+4i \end{bmatrix}.$$

A parte real e a imaginária de q_1 *são* $S(q_1) = 1$ *e* $V(q_1) = 3i + 4j + 2k$*, respectivamente. O produto entre* q_1 *e um quaternion* $q_2 = 3 + 3i + j + 6k$ *é dado por*

$$q_1 q_2 = 6 + 6i + j + 3k.$$

O complexo conjugado de q_1 *é* $q_1^* = S(q_1) - V(q_1) = 1 + 4i + 3j + 5k$*. A norma de* q_1 *é calculada por*

$$|q_1| = \sqrt{1^2 + 3^2 + 4^2 + 2^2} = \sqrt{2} = \pm 4 \ (\text{mod } 7).$$

Observe que, diferentemente do que acontece com os quaternions de Hamilton, em que se toma o valor positivo da raiz quadrada da qual se calcula a norma de um quaternion, quando quaternions generalizados sobre corpos finitos são considerados, parece não haver um critério claro para escolher entre os dois possíveis valores de tal raiz. Assim, em princípio, tal escolha seria arbitrária e, no exemplo, poder-se-ia deliberadamente considerar $|q_1| = 4$ *ou* $|q_1| = 3$*. Essa questão não influencia no cálculo do inverso de* q_1*, que é naturalmente único e dado por*

$$q_1^{-1} = \frac{q_1^*}{|q_1|^2} = 4 + 2i + 5j + 6k.$$

Na forma de Cayley-Dickson, q_1 é escrito como

$$q = (1 + 3i) + (4 + 2i)j.$$

Para expressar q_1 numa forma simplética, pode-se considerar, por exemplo, os quaternions puros unitários

$$\mu_1 = 3i + 2j + 4k$$

e

$$\mu_2 = 4i + 4j + 2k,$$

para os quais se tem

$$\mu_1 \bullet \mu_2 = 3 \cdot 4 + 2 \cdot 4 + 4 \cdot 2 \equiv 0 \pmod 7$$

e, portanto, $\mu_1 \perp \mu_2$. Obtém-se $\mu_3 = \mu_1\mu_2 = 2i + 3j + 4k$, o qual é também unitário e satisfaz $\mu_3 \perp \mu_1$ e $\mu_3 \perp \mu_2$ e, daí, a representação simplética de q_1, que é dada por

$$q_1 = (1 + 4\mu_1) + (4 + 5\mu_1)\mu_2;$$

na última expressão, $A' = 1 + 4\mu_1$ e $B' = 4 + 5\mu_1$ são, respectivamente, a parte simplex e a perplex do quaternion. Expandindo a última equação, tem-se, naturalmente,

$$q_1 = 1 + 4\mu_1 + 4\mu_2 + 5\mu_3,$$

cuja correspondência com a representação original de q_1, isto é, na base (i, j, k), pode ser verificada. A ordem multiplicativa de q_1 é $\mathrm{ord}(q_1) = 24$.

3.3 ORDEM MULTIPLICATIVA DE QUATERNIONS GENERALIZADOS SOBRE $\mathbb{F}_p$

Nesta seção, que é preenchida apenas por contribuições originais desta tese, são abordados alguns aspectos importantes relativos à ordem multiplicativa de quaternions generalizados sobre $\mathbb{F}_p$. Deste ponto em diante, considera-se especificamente que $\alpha = \beta = -1 \equiv (p-1) \pmod p$, ou seja, considera-se a álgebra $\left(\frac{-1,-1}{\mathbb{F}_p}\right)$, embora se possa atribuir outros valores a α e β. Inicialmente, considera-se o caso em que $p \equiv 3 \pmod 4$. São considerados quaternions

$$q = a + bi + cj + dk, \tag{3.33}$$

em que $a, b, c, d \in \mathbb{F}_p$, que, na forma matricial, são escritos como

$$\mathbf{Q} = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix}, \tag{3.34}$$

em que $i^2 \equiv (p - 1) \pmod p$.

Calculando-se o polinômio característico de $\mathbf{Q}$ por $r(\lambda) = \det(\mathbf{Q} - \lambda\mathbf{I})$, obtém-se

$$r(\lambda) = \lambda^2 - 2a\lambda + a^2 + b^2 + c^2 + d^2. \tag{3.35}$$

As raízes de $r(\lambda)$, que correspondem aos autovalores de $\mathbf{Q}$, são então dadas por

$$\lambda = a \pm \sqrt{-b^2 - c^2 - d^2}. \tag{3.36}$$

Excluindo os casos em que pelo menos um autovalor é nulo ($\mathbf{Q}$ não possuiria inversa e, portanto, também não possuiria ordem multiplicativa definida), são considerados os casos a seguir.

- Caso 1: $b^2 + c^2 + d^2 \equiv 0 \ (mod\ p)$. Neste caso, tem-se $\lambda = a \in \mathbb{F}_p$, isto é, $\mathbf{Q}$ possui dois autovalores iguais. Os dois subcasos a seguir são considerados.

  - Subcaso 1.1: $b = 0$ ou $c = 0$ ou $d = 0$. A condição que determina o presente subcaso, unida à condição que determina o caso 1, implica que $b = c = d = 0$. Assim, $\mathbf{Q}$ se reduz a uma matriz da forma

    $$\mathbf{Q} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \tag{3.37}$$

    e, portanto, tem-se $\mathrm{ord}(\mathbf{Q}) = \mathrm{ord}(a)$.

  - Subcaso 1.2: $b \neq 0$ ou $c \neq 0$ ou $d \neq 0$. A condição que determina o presente subcaso, unida à condição que determina o caso 1, implica que $b \neq 0$, $c \neq 0$ e $d \neq 0$. Assim, denotando por $\mathbf{v} = [v(0)\ \ v(1)]$ um autovetor de $\mathbf{Q}$, pode-se escrever $\mathbf{Q}\mathbf{v}^T = a\mathbf{v}^T$, o que produz o sistema de equações

    $$\begin{cases} biv(0) + (c + di)v(1) = 0 \\ (-c + di)v(0) - biv(1) = 0. \end{cases} \tag{3.38}$$

    Do sistema acima, obtém-se a relação

    $$v(0) = \frac{bi}{-c + di} v(1), \tag{3.39}$$

    o que indica que a multiplicidade geométrica de $\lambda = a$ é igual a $m_g(a) = 1$. Assim, $\mathbf{Q}$ é não-diagonalizável e admite forma normal de Jordan

    $$\mathbf{J_Q} = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}. \tag{3.40}$$

    Calculando ${\mathbf{J_Q}}^m$, para $m = 2, 3, 4, \ldots$, observa-se que, em geral, tem-se

    $${\mathbf{J_Q}}^m = \begin{bmatrix} a^m & ma^{m-1} \\ 0 & a^m \end{bmatrix}. \tag{3.41}$$

    Portanto, ${\mathbf{J_Q}}^m = \mathbf{I}$ apenas quando $a^m \equiv 1 \pmod{p}$, isto é, quando m for um múltiplo de $\mathrm{ord}(a)$, e quando $ma^{m-1} \equiv 0 \pmod{p}$, isto é, quando $m \equiv 0 \pmod{p}$. Assim, $\mathrm{ord}(\mathbf{Q}) = \mathrm{ord}(\mathbf{J_Q}) = \mathrm{mmc}(\mathrm{ord}(a), p) = \mathrm{ord}(a) \times p$, em que mmc significa o mínimo múltiplo comum.

- Caso 2: $b^2 + c^2 + d^2 \neq 0$. Neste caso, $\mathbf{Q}$ possui dois autovalores distintos e admite a forma diagonal

$$\mathbf{\Lambda_Q} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}, \tag{3.42}$$

em que $\lambda_1 = a + \sqrt{-b^2 - c^2 - d^2}$ e $\lambda_2 = a - \sqrt{-b^2 - c^2 - d^2}$. Assim, $\mathrm{ord}(\mathbf{Q}) = \mathrm{ord}(\mathbf{\Lambda_Q}) = \mathrm{mmc}(\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2))$.

É necessário considerar, também, o caso em que $p \equiv 1 \pmod 4$, quando, fazendo-se $i^2 \equiv (p-1) \pmod p$, tem-se $i = \sqrt{-1} \in \mathbb{F}_p$. A ordem multiplicativa de $\mathbf{Q}$ pode ser determinada de acordo com os seguintes casos.

- Caso 1: $b^2 + c^2 + d^2 = 0$. Neste caso, tem-se $\lambda_1 = \lambda_2 = a \in \mathbb{F}_p$. Os seguintes subcasos precisam ser considerados.

  - Subcaso 1.1: $b = c = d = 0$. A condição que determina este subcaso é idêntica àquela considerada no subcaso 1.1 para $p \equiv 3 \pmod 4$ e, portanto, leva ao mesmo resultado.
  - Subcaso 1.2: $b = 0$ e $c \neq 0$ e $d \neq 0$. Neste caso, tem-se $c^2 = -d^2 \Rightarrow c = \pm di$. Assumindo que $c = di$, $\mathbf{Q}$ se reduz a uma matriz na forma

$$\mathbf{Q} = \begin{bmatrix} a & 2di \\ 0 & a \end{bmatrix}. \tag{3.43}$$

Denotando por $\mathbf{v} = [v(0)\ v(1)]$ um autovetor de $\mathbf{Q}$, pode-se escrever $\mathbf{Q}\mathbf{v}^T = a\mathbf{v}^T$, o que produz o sistema de equações

$$\begin{cases} av(0) + 2div(1) = av(0) \\ av(1) = av(1). \end{cases} \tag{3.44}$$

A solução de (3.44) é simplesmente $v(1) = 0$, a qual indica que a multiplicidade geométrica de $\lambda_1 = \lambda_2 = a$ é $m_g(a) = 1$. Portanto, $\mathbf{Q}$ é não-diagonalizável e admite a forma normal de Jordan

$$\mathbf{J_Q} = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}. \tag{3.45}$$

Analogamente ao subcaso 1.2 para $p \equiv 3 \pmod 4$, conclui-se que $\mathrm{ord}(\mathbf{Q}) = \mathrm{ord}(\mathbf{J_Q}) = \mathrm{mmc}(\mathrm{ord}(a), p)$. Obtém-se o mesmo resultado se $c = -di$ ou $c = 0$ e $b \neq 0$ e $d \neq 0$ ou $d = 0$ e $b \neq 0$ e $c \neq 0$.

  - Subcaso 1.3: $b \neq 0$ e $c \neq 0$ e $d \neq 0$. Neste caso, pode-se escrever $b^2 = -(c^2 + d^2) \Rightarrow b = \pm i\sqrt{c^2 + d^2}$, com $i \in \mathbb{F}_p$. Assumindo que $b = i\sqrt{c^2 + d^2}$, $\mathbf{Q}$ se reduz a uma matriz na forma

$$\mathbf{Q} = \begin{bmatrix} a - \sqrt{c^2 + d^2} & c + di \\ -c + di & a + \sqrt{c^2 + d^2} \end{bmatrix}. \tag{3.46}$$

Denotando por $\mathbf{v} = [v(0)\ v(1)]$ um autovetor de $\mathbf{Q}$, pode-se escrever $\mathbf{Q}\mathbf{v}^T = a\mathbf{v}^T$, o que produz o sistema de equações

$$\begin{cases} -\sqrt{c^2+d^2}v(0) + (c+di)v(1) = 0 \\ (-c+di)v(0) + \sqrt{c^2+d^2}v(1) = 0 \end{cases} \tag{3.47}$$

De (3.47), obtém-se a relação

$$v(0) = -\frac{\sqrt{c^2+d^2}}{-c+di}v(1),$$

a qual indica que a multiplicidade geométrica de $\lambda_1 = \lambda_2 = a$ é $m_g(a) = 1$. Portanto, $\mathbf{Q}$ é não-diagonalizável e admite a forma normal de Jordan (3.45). Analogamente ao subcaso 1.2 para $p \equiv 3 \pmod 4$, conclui-se que $\mathrm{ord}(\mathbf{Q}) = \mathrm{ord}(\mathbf{J_Q}) = \mathrm{mmc}(\mathrm{ord}(a), p) = \mathrm{ord}(a) \times p$. Obtém-se o mesmo resultado se $b = -i\sqrt{c^2+d^2}$. Um desenvolvimento similar é obtido se se realizar, inicialmente, uma substituição conforme $c = \pm i\sqrt{b^2+d^2}$ ou $d = \pm i\sqrt{b^2+c^2}$.

- Caso 2: $b^2 + c^2 + d^2 \neq 0$. Neste caso, $\mathbf{Q}$ possui dois autovalores distintos e admite forma diagonal

$$\mathbf{\Lambda_Q} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}. \tag{3.48}$$

Assim, $\mathrm{ord}(\mathbf{Q}) = \mathrm{ord}(\mathbf{\Lambda_Q}) = \mathrm{mmc}(\mathrm{ord}((\lambda_1)), \mathrm{ord}(\lambda_2))$.

3.3.1 Exemplos

A seguir, são dados alguns exemplos de quaternions generalizados sobre corpos finitos; para cada exemplo, indica-se em qual dos casos anteriormente analisados o quaternion considerado se encaixa e fornece-se a sua ordem multiplicativa.

Exemplo 3.2. *Considere o quaternion generalizado sobre* $\mathbb{F}_{11}$*,*

$$q = 2 + 0i + 0j + 0k, \tag{3.49}$$

em que $i = j = \sqrt{10} \pmod{11}$*. Na forma matricial,* q *é escrito como*

$$\mathbf{Q} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}. \tag{3.50}$$

Este quaternion, que se encaixa no Subcaso 1.1 para $p \equiv 3 \pmod 4$*, possui ordem multiplicativa coincidente com a ordem multiplicativa de* 2 *no grupo cíclico de* $\mathbb{F}_{11}$*, isto é,* $\mathrm{ord}(q) = \mathrm{ord}(2) = 10$.

Exemplo 3.3. *Considere o quaternion generalizado sobre* $\mathbb{F}_{11}$*,*

$$q = 2 + 2i + 3j + 8k, \tag{3.51}$$

em que $i = j = \sqrt{10} \pmod{11}$*. Na forma matricial,* q *é escrito como*

$$\mathbf{Q} = \begin{bmatrix} 2+2i & 3+8i \\ -3+8i & 2-2i \end{bmatrix}. \tag{3.52}$$

Este quaternion se encaixa no Subcaso 1.2 para $p \equiv 3 \pmod{4}$*, uma vez que* $2^2 + 3^2 + 8^2 \equiv 0 \pmod{11}$*. Sua ordem multiplicativa é, portanto, dada por* $\mathrm{ord}(q) = \mathrm{mmc}(\mathrm{ord}(a), p) = \mathrm{mmc}(\mathrm{ord}(2), 11) = \mathrm{ord}(2) \times p = 110$*.*

Exemplo 3.4. *Considere o quaternion generalizado sobre* $\mathbb{F}_{11}$*,*

$$q = 1 + 2i + 3j + 4k, \tag{3.53}$$

em que $i = j = \sqrt{10} \pmod{11}$*. Na forma matricial,* q *é escrito como*

$$\mathbf{Q} = \begin{bmatrix} 1+2i & 3+4i \\ -3+4i & 1-2i \end{bmatrix}. \tag{3.54}$$

Este quaternion se encaixa no Caso 2 para $p \equiv 3 \pmod{4}$*, uma vez que* $\mathbf{Q}$ *possui dois autovalores distintos* $\lambda_1 = 3$ *e* $\lambda_2 = 10$*; esses autovalores possuem ordens multiplicativas dadas, respectivamente, por* $\mathrm{ord}(3) = 10$ *e* $\mathrm{ord}(10) = 2$*. Assim, a ordem multiplicativa de* q *é dada por* $\mathrm{ord}(q) = \mathrm{mmc}(\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2)) = \mathrm{mmc}(10, 2) = 10$*.*

Exemplo 3.5. *Considere o quaternion generalizado sobre* $\mathbb{F}_{11}$*,*

$$q = 0 + 2i + 3j + 4k, \tag{3.55}$$

em que $i = j = \sqrt{10} \pmod{11}$*. Na forma matricial,* q *é escrito como*

$$\mathbf{Q} = \begin{bmatrix} 2i & 3+4i \\ -3+4i & 2i \end{bmatrix}. \tag{3.56}$$

Este quaternion se encaixa no Caso 2 para $p \equiv 3 \pmod{4}$*, uma vez que* $\mathbf{Q}$ *possui dois autovalores distintos* $\lambda_1 = 2$ *e* $\lambda_2 = 9$*; esses autovalores possuem a mesma ordem multiplicativa* $\mathrm{ord}(2) = \mathrm{ord}(9) = 10$*. Assim, a ordem multiplicativa de* q *é dada por* $\mathrm{ord}(q) = \mathrm{ord}(\lambda_1) = \mathrm{ord}(\lambda_2) = 10$*.*

Como os casos analisados para $p \equiv 1(\mathrm{mod}4)$ são similares àqueles em que $p \equiv 3(\mathrm{mod}4)$, a seguir, apresenta-se apenas um exemplo de ordem multiplicativa de um quaternion generalizado sobre um corpo finito $\mathbb{F}_p$ em que $p \equiv 1 \pmod{4}$. O quaternion em questão será usado na definição de uma transformada que pode ser aplicada ao processamento de imagens coloridas.

Exemplo 3.6. *Considere o quaternion generalizado sobre* $\mathbb{F}_{257}$*,*

$$q = 7 + 8i + 4j + 8k, \tag{3.57}$$

em que $i = j = \sqrt{256} \pmod{257} \equiv 16 \pmod{257}$*. Na forma matricial,* q *é escrito como*

$$\mathbf{Q} = \begin{bmatrix} 7+8i & 4+8i \\ 253+8i & 7+249i \end{bmatrix}. \tag{3.58}$$

Este quaternion se encaixa no Caso 2 para $p \equiv 1 (\mathrm{mod}\, 4)$*, uma vez que* $\mathbf{Q}$ *possui dois autovalores distintos* $\lambda_1 = 72$ *e* $\lambda_2 = 199$*; esses autovalores possuem a mesma ordem multiplicativa* $\mathrm{ord}(72) = \mathrm{ord}(199) = 128$*. Assim, a ordem multiplicativa de* q *é dada por* $\mathrm{ord}(q) = \mathrm{ord}(\lambda_1) = \mathrm{ord}(\lambda_2) = 128$*.*

Os casos analisados, tanto para $p \equiv 3 \pmod{4}$ quanto para $p \equiv 1 \pmod{4}$, dão suporte ao lema a seguir.

Lema 3.1. *Um quaternion generalizado* q *sobre* $\mathbb{F}_p$*, com matriz associada* $\mathbf{Q}$ *e que possui ordem multiplicativa* $\mathrm{ord}(q) = \mathrm{ord}(\mathbf{Q}) = N$*, satisfaz*

$$\sum_{m=0}^{N-1} \mathbf{Q}^{km} = \begin{cases} \begin{bmatrix} N & 0 \\ 0 & N \end{bmatrix},\ N \not\equiv 0 \pmod{p}, & \text{se } k = 0, \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{0}, & \text{se } k = 1, 2, \ldots, N-1, \end{cases} \tag{3.59}$$

se, e somente se

$$\mathbf{Q} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \tag{3.60}$$

ou se $\mathbf{Q}$ *possuir dois autovalores distintos com ordens multiplicativas coincidentes.*

Demonstração. Seja $S_N(k) = \sum_{m=0}^{N-1} \mathbf{Q}^{km}$. Se $\mathbf{Q}$ for do tipo analisado nos subcasos 1.1 (vide parte inicial desta seção), então $\mathrm{ord}(\mathbf{Q}) = N = \mathrm{ord}(a)$ e, assim, $N|(p-1)$; se $\mathbf{Q}$ for do tipo analisado nos casos 2, com os autovalores λ_1 e λ_2 tendo ordens multiplicativas coincidentes, então $\mathrm{ord}(\mathbf{Q}) = N = \mathrm{ord}(\lambda_1) = \mathrm{ord}(\lambda_2)$ e, assim, $N|(p^2-1)$. Logo, se $\mathbf{Q}$ for de um dos dois tipos indicados no enunciado do lema, tem-se $\mathrm{ord}(\mathbf{Q}) = N \not\equiv 0 \pmod{p}$, e, portanto,

$$S_N(0) = \sum_{m=0}^{N-1} \left(\mathbf{Q}^0\right)^m = \sum_{m=0}^{N-1} \mathbf{I}^m = \sum_{m=0}^{N-1} \mathbf{I} = \begin{bmatrix} N & 0 \\ 0 & N \end{bmatrix}.$$

Para $k = 1, 2, \ldots, N-1$, considerando o Lema 2.1, tem-se, se $\mathbf{Q}$ for do tipo analisado nos subcasos 1.1,

$$S_N(k) = \begin{bmatrix} \sum_{m=0}^{N-1} a^{km} & 0 \\ 0 & \sum_{m=0}^{N-1} a^{km} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix};$$

se $\mathbf{Q}$ for do tipo analisado nos casos 2, com os autovalores tendo ordens multiplicativas coincidentes, tem-se

$$S_N(k) = \mathbf{V} \begin{bmatrix} \sum_{m=0}^{N-1} \lambda_1^{km} & 0 \\ 0 & \sum_{m=0}^{N-1} \lambda_2^{km} \end{bmatrix} \mathbf{V}^{-1} = \mathbf{V} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \mathbf{V}^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

em que $\mathbf{V}$ é uma matriz cujas colunas são autovetores de $\mathbf{Q}$ associados aos autovalores λ_1 e λ_2.

Por outro lado, se $\mathbf{Q}$ não for de um dos tipos indicados no enunciado do lema, essa matriz se enquadra nos subcasos 1.2, no subcaso 1.3 ($p \equiv 1 \pmod 4$) ou nos casos 2, com os autovalores λ_1 e λ_2 tendo ordens multiplicativas distintas. Se $\mathbf{Q}$ for do tipo analisado nos subcasos 1.2 ou 1.3, tem-se $N = \mathrm{ord}(\mathbf{Q})|p$ e, assim, $S_N(0) = \mathbf{0}$; isso viola o que se estabelece na primeira parte de (3.59). Se $\mathbf{Q}$ for do tipo analisado nos casos 2, com $\mathrm{ord}(\lambda_1) \neq \mathrm{ord}(\lambda_2)$, pode-se assumir, sem perda de generalidade, que $\mathrm{ord}(\lambda_1) < \mathrm{ord}(\lambda_2) \leq \mathrm{ord}(\mathbf{Q}) = N$. Assim, tem-se

$$S_N(\mathrm{ord}(\lambda_1)) = \mathbf{V} \begin{bmatrix} \sum_{m=0}^{N-1} \lambda_1^{\mathrm{ord}(\lambda_1)m} & 0 \\ 0 & \sum_{m=0}^{N-1} \lambda_2^{\mathrm{ord}(\lambda_1)m} \end{bmatrix} \mathbf{V}^{-1} = \mathbf{V} \begin{bmatrix} N & 0 \\ 0 & 0 \end{bmatrix} \mathbf{V}^{-1} \neq \mathbf{0},$$

o que viola o que se estabelece na segunda parte de (3.59). □

4 A TRANSFORMADA NUMÉRICA DE FOURIER QUATERNIÔNICA

NESTE capítulo, é introduzida uma transformada numérica de Fourier quaterniônica, a qual constitui a principal contribuição desta tese. A transformada é identificada pelo acrônimo QFNT, do inglês *quaternion Fourier number transform*. Os resultados derivados na Seção 3.3, sobre a ordem multiplicativa de quaternions generalizados sobre corpos finitos, são essenciais para a definição da QFNT, a qual é apresentada na Seção 4.1. Na Seção 4.2, são discutidas as principais propriedades da QFNT; na Seção 4.3, são apresentadas proposições relacionadas aos autovalores e autovetores da matriz da QFNT; por fim, na Seção 4.4, são discutidas de forma preliminar algumas questões relacionadas ao cálculo da QFNT.

4.1 A TRANSFORMADA NUMÉRICA DE FOURIER QUATERNIÔNICA

A seguir, é introduzida uma definição para a transformada numérica de Fourier quaterniônica e determinada a respectiva transformada inversa. A transformada corresponde, de alguma forma, a uma versão sobre corpos finitos da versão discreta da transformada de Fourier quaterniônica, conforme apresentado em (ELL; SANGWINE, 2007), por exemplo. De qualquer maneira, o estabelecimento da QFNT depende de todo o desenvolvimento realizado na Seção 3.3; sua invertibilidade depende, em particular, das condições dadas no Lema 3.1, as quais são completamente dissociadas do que se considera no cenário usual de definição da transformada, isto é, sobre quaternions de Hamilton.

Definição 4.1. Seja q um quaternion generalizado sobre $\mathbb{F}_p$, com ordem multiplicativa dada por $\mathrm{ord}(q) = N$ e que satisfaz as condições dadas no Lema 3.1. A transformada numérica de Fourier quaterniônica (à direita) de um vetor $\mathbf{x} = (x(n))$, $x(n) \in \left(\frac{-1,-1}{\mathbb{F}_p}\right)$, $n = 0, 1, \ldots, N-1$, é o vetor $\mathbf{X}^R = (X^R(k))$, $X^R(k) \in \left(\frac{-1,-1}{\mathbb{F}_p}\right)$, $k = 0, 1, \ldots, N-1$, cujas componentes são dadas por

$$X^R(k) = \sum_{n=0}^{N-1} x(n) q^{kn}. \tag{4.1}$$

Teorema 4.1. *Seja q um quaternion generalizado sobre $\mathbb{F}_p$, com ordem multiplicativa dada por $\mathrm{ord}(q) = N$ e que satisfaz as condições dadas no Lema 3.1. A transformada numérica de Fourier quaterniônica (à direita) inversa de um vetor $\mathbf{X}^R = (X^R(k))$, $X^R(k) \in \left(\frac{-1,-1}{\mathbb{F}_p}\right)$, $k = 0, 1, \ldots, N-1$, é o vetor $\mathbf{x} = (x(n))$, $x(n) \in \left(\frac{-1,-1}{\mathbb{F}_p}\right)$, $n = 0, 1, \ldots, N-1$, cujas componentes são dadas por*

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X^R(k) q^{-kn}. \tag{4.2}$$

Demonstração. Substituindo, em (4.2), $X^R(k)$ pela expressão (4.1) com n substituído por m, obtém-se

$$\begin{aligned} x(n) &= \frac{1}{N}\sum_{k=0}^{N-1}\left(\sum_{m=0}^{N-1} x(m)q^{km}\right)q^{-kn} \\ &= \frac{1}{N}\sum_{m=0}^{N-1} x(m)\left(\sum_{k=0}^{N-1} q^{k(m-n)}\right). \end{aligned}$$

Se as componentes do vetor $\mathbf{x}$ e o quaternion q forem tratados em seus respectivos formatos matriciais, de acordo com o Lema 3.1, sempre que $m \neq n$ no primeiro somatório da última equação, o segundo somatório da mesma equação resulta numa matriz 2×2 nula; por outro lado, se $m = n$, o segundo somatório fornece a matriz $N \cdot \mathbf{I}_2$, em que $\mathbf{I}_2$ é a matriz identidade 2×2. Assim, a última equação se resume a

$$x(n) = \frac{1}{N}x(n)\begin{bmatrix} N & 0 \\ 0 & N \end{bmatrix} = x(n).$$

□

O cálculo de uma QFNT pode ser expresso como um produto matricial entre o vetor $\mathbf{x}$ e uma matriz de transformação $\mathbf{F}_q$ cuja componente na n-ésima linha e na k-ésima coluna é dada por

$$F_q(n,k) = q^{kn}, \tag{4.3}$$

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

$$\mathbf{X}^R = \mathbf{x}\mathbf{F}_q.$$

Consequentemente, o cálculo de uma QFNT inversa pode ser expresso como

$$\mathbf{x} = \mathbf{X}^R\mathbf{F}_q^{-1},$$

em que

$$F_q^{-1}(k,n) = \frac{1}{N}q^{-kn}.$$

A QFNT também pode ser definida à esquerda, bastando que, em (4.1) e (4.2), sejam permutadas as posições do núcleo da transformada e da componente do vetor que o está ponderando. Neste caso, o vetor da QFNT seria denotado por $\mathbf{X}^L = (X^L(k))$, $k = 0, 1, \ldots, N-1$. Deste ponto em diante, sempre que se omitir o tipo da QFNT considerada, o leitor deve assumir que se está considerando a QFNT à direita. Ainda com relação à transformada definida, é relevante observar que a opção por representar os quaternions generalizados envolvidos (componentes

dos vetores e núcleo da transformada) como em (3.33) ou matricialmente, como em (3.34), é um aspecto puramente computacional, não influenciando nos resultados que têm sido obtidos. Para manter a coerência com relação a isso, na escrita das equações, sempre que se optar pela representação matricial $\mathbf{Q}$ do núcleo q da transformada, assume-se que as componentes dos vetores também são representadas matricialmente, ainda que não se indique tal opção por meio de uma notação específica.

Exemplo 4.1. *Neste exemplo ilustrativo, é considerada a álgebra* $A = \left(\frac{6,6}{\mathbb{F}_7}\right)$*, de modo que se possa definir uma QFNT cujos quaternions generalizados têm seus coeficientes sobre* $\mathbb{F}_7$*. Como núcleo da transformada, emprega-se* $q = 3 + 3i + j + 6k$*, que possui ordem multiplicativa* $\mathrm{ord}(q) = 16$ *e cuja forma matricial é*

$$\mathbf{Q} = \begin{bmatrix} 3+3i & 6+i \\ 1+i & 3+4i \end{bmatrix}.$$

Assim, uma QFNT com comprimento $N = 16$ *pode ser obtida. Empregando a Definição 4.1, calcula-se a QFNT à direita* $\mathbf{X}^R = (X^R(k))$*,* $k = 0, 1, \ldots, 15$*, do vetor produzido aleatoriamente*

$$\mathbf{x} = \begin{bmatrix} 5+6i+0j+6k \\ 4+0i+1j+3k \\ 6+6i+1j+6k \\ 6+3i+5j+0k \\ 2+6i+5j+6k \\ 4+0i+5j+6k \\ 4+5i+5j+2k \\ 4+1i+4j+0k \\ 1+0i+0j+5k \\ 4+2i+6j+0k \\ 3+2i+5j+5k \\ 1+3i+3j+4k \\ 4+5i+1j+4k \\ 4+1i+0j+3k \\ 6+2i+4j+1k \\ 5+1i+3j+4k \end{bmatrix}.$$

Obtém-se

$$\mathbf{X} = \begin{bmatrix} 0+1i+6j+6k \\ 2+0i+6j+1k \\ 3+2i+0j+2k \\ 1+6i+1j+0k \\ 3+6i+5j+5k \\ 4+3i+5j+6k \\ 5+3i+0j+3k \\ 5+2i+3j+3k \\ 6+0i+1j+1k \\ 1+0i+2j+5k \\ 3+3i+6j+3k \\ 4+6i+5j+2k \\ 4+5i+5j+2k \\ 5+3i+5j+3k \\ 3+0i+5j+3k \\ 3+0i+1j+2k \end{bmatrix}.$$

4.2 PROPRIEDADES DA QFNT

Nesta seção, são desenvolvidas algumas propriedades da transformada numérica de Fourier quaterniônica. De modo análogo ao que acontece com a transformada numérica de Fourier ordinária em relação à transformada discreta de Fourier, essas propriedades guardam certa analogia com as propriedades da transformada discreta de Fourier quaterniônica. O destaque fica por conta da propriedade de convolução cíclica, a qual se imagina que, também no contexto quaterniônico, possa ser empregada para realizar filtragem empregando apenas operações de aritmética modular convenientemente adaptadas aos quaternions generalizados definidos sobre corpos finitos.

Propriedade 4.1 (Linearidade)**.** *Se as QFNT dos vetores* $\mathbf{x}_1 = (x_1(n))$ *e* $\mathbf{x}_2 = (x_2(n))$, $n = 0, 1, \ldots, N-1$, *cujas componentes são quaternions sobre* $\mathbb{F}_p$, *forem, respectivamente,* $\mathbf{X}_1 = (X_1(k))$ *e* $\mathbf{X}_2 = (X_2(k))$, $k = 0, 1, \ldots, N-1$, *então, a transformada de* $\mathbf{x} = c_1\mathbf{x}_1 + c_2\mathbf{x}_2$, $c_1, c_2 \in \left(\frac{-1,-1}{\mathbb{F}_p}\right)$, *será* $\mathbf{X} = c_1\mathbf{X}_1 + c_2\mathbf{X}_2$.

Demonstração. A prova dessa propriedade decorre diretamente da Definição 4.1, sendo omitida neste trabalho. □

Propriedade 4.2 (Deslocamento)**.** *Seja* $\mathbf{x} = \mathbf{x}_a + \mathbf{x}_b i + \mathbf{x}_c j + \mathbf{x}_d k = (x(n))$, $n = 0, 1, \ldots, N-1$, *um vetor de quaternions, cujas componentes (vetoriais)* $\mathbf{x}_a$, $\mathbf{x}_b$, $\mathbf{x}_c$ *e* $\mathbf{x}_d$ *possuem QFNT identificadas respectivamente por* $\mathbf{X}_a^R$, $\mathbf{X}_b^R$, $\mathbf{X}_c^R$ *e* $\mathbf{X}_d^R$. *Então, a QFNT do vetor* $\mathbf{x}' = (x'(n)) =$

$(x(n+n_0))$, *em que* n_0 *é um inteiro, possui componentes dadas por*

$$X'^R(k) = q^{-kn_0}X_a^R(k) + iq^{-kn_0}X_b^R(k) + jq^{-kn_0}X_c^R(k) + kq^{-kn_0}X_d^R(k),$$

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

Demonstração. Fazendo $x'(n) = x(n+n_0)$, tem-se

$$X'^R(k) = \sum_{n=0}^{N-1} x'(n)q^{kn} = \sum_{n=0}^{N-1} x(n+n_0)q^{kn}. \tag{4.4}$$

Substituindo, na última equação, $n + n_0 = n'$, obtém-se

$$X'^R(k) = \sum_{n'=0}^{N-1} x(n')q^{k(n'-n_0)} = \sum_{n'=0}^{N-1} x(n')q^{kn'}q^{-kn_0}. \tag{4.5}$$

Escrevendo $x(n') = x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k$, a última equação se torna

$$X'^R(k) = \sum_{n'=0}^{N-1} \left[x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k\right] q^{kn'}q^{-kn_0} \tag{4.6}$$

$$= q^{-kn_0}X_a^R(k) + iq^{-kn_0}X_b^R(k) + jq^{-kn_0}X_c^R(k) + kq^{-kn_0}X_d^R(k). \tag{4.7}$$

Se $\mathbf{x}$ for uma sequência real, o resultado encontrado coincide com aquele obtido para a propriedade de deslocamento da FNT (naturalmente, com o quaternion q no lugar do elemento que seria usado como núcleo da FNT). □

Propriedade 4.3 (QFNT do impulso)**.** *A QFNT do vetor* $\delta = [1\,0\,0\,\cdots\,0]$ *é o vetor* $\mathbf{X} = (X(k))$, $X(k) = 1$, $k = 0, 1, \ldots, N-1$.

Demonstração. A prova segue diretamente da Definição 4.1, visto que, em (4.1), para cada $k = 0, 1, \ldots, N-1$, o único termo não nulo no somatório é igual a $X(k) = x(0)q^{k\cdot 0} = 1$. □

Propriedade 4.4 (QFNT de uma linha da matriz de transformação)**.** *A QFNT do vetor* $\mathbf{x} = [q^{0m}q^{1m}q^{2m}\cdots q^{(N-1)m}]$*, correspondente à* m*-ésima linha da matriz da respectiva transformada, é o vetor* $\mathbf{X} = N\delta_m = (N\delta(-n-m))$.

Demonstração. O produto matricial correspondente ao cálculo da QFNT pode ser visto como o cálculo de somas de produtos ponto a ponto entre o vetor a ser transformado e cada coluna da matriz de transformação $\mathbf{F}_q$. Considerando a composição dessa matriz (vide (4.3)), sabe-se que sua n-ésima linha corresponde ao conjugado de sua $(N-m)$-ésima coluna. Assim, como as referidas somas de produtos podem ser vistas como produtos internos e as colunas de $\mathbf{F}_q$ constituem uma base ortogonal para o espaço formado por vetores N-dimensionais cujos componentes são quaternions (na qual o vetor a ser transformado será expresso), a única dessas somas de produtos a ser não-nula, quando o vetor de entrada é a m-ésima linha de $\mathbf{F}_q$, é aquela calculada com relação à $(N-m)$-ésima coluna da mesma matriz. O fator N aparece multiplicando o impulso deslocado δ_m pois a referida base não é ortonormal (vide Lema 3.1). □

Propriedade 4.5 (QFNT de um vetor constante)**.** *A QFNT do vetor constante* $\mathbf{x} = [1\ 1\ 1\ \cdots\ 1]$ *é o vetor* $N\delta = [N\ 0\ 0\ \cdots\ 0]$.

Demonstração. A prova segue diretamente do Lema 3.1. □

Em seguida, desenvolve-se a propriedade de convolução cíclica para a QFNT. Para isso, considera-se a definição à direita dessa transformada; o resultado da convolução cíclica de comprimento N entre $\mathbf{x} = (x(n))$ e $\mathbf{h} = (h(n))$ é denotado por $\mathbf{y} = \mathbf{x} \circ_N \mathbf{h}$, $\mathbf{y} = (y(n))$, $n = 0, 1, \ldots, N-1$, e dado por

$$y(n) = x \circ_N h(n) = \sum_{m=0}^{N-1} x(n-m)h(m).$$

Observe que, em função da não-comutatividade entre as componentes de $\mathbf{x}$ e $\mathbf{h}$, a última equação corresponde a uma espécie de convolução à direita; uma convolução à esquerda também poderia ser considerada.

Propriedade 4.6 (Convolução cíclica)**.** *Sejam* $\mathbf{x} = (x(n)) = (x_a(n)+x_b(n)i+x_c(n)j+x_d(n)k)$ *e* $\mathbf{h} = (h(n))$, $n = 0, 1, \ldots, N-1$*, vetores cujas componentes são quaternions generalizados sobre* $\mathbb{F}_p$*. A QFNT da convolução cíclica* $\mathbf{y}$ *de comprimento* N *entre* $\mathbf{x}$ *e* $\mathbf{h}$ *é dada por*

$$Y^R(k) = H^R(k)X_a^R(k) + iH^R(k)X_b^R(k) + jH^R(k)X_c^R(k) + kH^R(k)X_d^R(k). \tag{4.8}$$

Demonstração. Da definição da QFNT, pode-se escrever

$$Y^R(k) = \sum_{n=0}^{N-1} \left[x \circ_N h(n)\right] q^{kn} = \sum_{n=0}^{N-1} \left[\sum_{m=0}^{N-1} x(n-m)h(m)\right] q^{kn}. \tag{4.9}$$

Na última equação, usando a substituição $n' = n - m$, obtém-se

$$Y^R(k) = \sum_{n'=0}^{N-1} \left[\sum_{m=0}^{N-1} x(n')h(m)\right] q^{k(n'+m)} \tag{4.10}$$

$$= \sum_{n'=0}^{N-1} x(n') \left[\sum_{m=0}^{N-1} h(m)q^{km}\right] q^{kn'} \tag{4.11}$$

$$= \sum_{n'=0}^{N-1} x(n')H^R(k)q^{kn'}. \tag{4.12}$$

Escrevendo $x(n') = x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k$, a última equação se torna

$$Y^R(k) = \sum_{n'=0}^{N-1} \left[x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k\right] H^R(k) q^{kn'} \tag{4.13}$$

$$= H^R(k) \sum_{n'=0}^{N-1} x_a(n') q^{kn'} + iH^R(k) \sum_{n'=0}^{N-1} x_b(n') q^{kn'} \tag{4.14}$$

$$+ jH^R(k) \sum_{n'=0}^{N-1} x_c(n') q^{kn'} + kH^R(k) \sum_{n'=0}^{N-1} x_d(n') q^{kn'} \tag{4.15}$$

$$= H^R(k) X_a^R(k) + iH^R(k) X_b^R(k) + jH^R(k) X_c^R(k) + kH^R(k) X_d^R(k). \tag{4.16}$$

□

Se a QFNT de $\mathbf{x}$ for uma sequência real $\mathbf{X}^R = \mathbf{X}_a^R$, a última equação assume a forma

$$Y^R(k) = H^R(k) X^R(k),$$

a qual coincide com o resultado do Teorema da convolução cíclica para a FNT. Relações semelhantes são obtidas se se considerar a QFNT à esquerda.

Propriedade 4.7 (Teorema de Parseval)**.** *Seja* $\mathbf{x}$ *um vetor cujas componentes são quaternions generalizados sobre* $\mathbb{F}_p$ *e* $\mathbf{X}^R$ *sua QFNT à direita, cujo núcleo é um quaternion unitário* q*. Então, a relação*

$$\sum_{n=0}^{N-1} |x(n)|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |X^R(k)|^2$$

é satisfeita.

Demonstração.

$$\sum_{n=0}^{N-1} |x(n)|^2 = \sum_{n=0}^{N-1} x(n) x^*(n) = \frac{1}{N} \sum_{n=0}^{N-1} \left[\sum_{k=0}^{N-1} X^R(k) q^{-kn}\right] x^*(n) \tag{4.17}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} X^R(k) \sum_{n=0}^{N-1} \left[q^{kn}\right]^* x^*(n) \tag{4.18}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} X^R(k) \sum_{n=0}^{N-1} \left[x(n) q^{kn}\right]^* \tag{4.19}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} X^R(k) \left[X^R(k)\right]^* = \frac{1}{N} \sum_{k=0}^{N-1} |X^R(k)|^2. \tag{4.20}$$

□

4.3 AUTOESTRUTURA DA QFNT

Nesta seção, são desenvolvidos resultados relacionados à autoestrutura da QFNT. O que se faz, basicamente, é demonstrar que qualquer autovetor da transformada numérica de Fourier é também um autovetor da QFNT; além disso, são identificados os autovalores aos quais esses autovetores estão relacionados, bem como suas multiplicidades. No que segue, considera-se uma versão unitária da QFNT, que consiste, basicamente, em incluir o fator de escala $1/\sqrt{N}$ em (4.1) e trocar o fator de escala $1/N$ por $1/\sqrt{N}$ em (4.2).

Proposição 4.1. *Seja* $\mathbf{v} = (v(n))$, $n = 0, 1, \ldots, N-1$, *um autovetor associado ao autovalor* λ *de uma FNT definida com núcleo* $\zeta = a_1 + b_1 i \in \mathrm{G}_{1,p}$, *tal que* $\mathrm{ord}(\zeta) = N$; *seja QFNT uma transformada definida com núcleo* $q = a + bi + cj + dk \in \mathrm{Q}_{1,p}$, *tal que* $\mathrm{ord}(q) = N$, $a_1 = a$ *e* $(b_1 i)^2 = b^2 i^2 + c^2 j^2 + d^2 k^2$.

(a) Se $\mathbf{v}$ *tem simetria par (caso em que* $\lambda = \pm 1$*), então ele também é um autovetor com autovalor* λ *da QFNT indicada no enunciado da proposição.*

(b) Se $\mathbf{v}$ *tem simetria ímpar (caso em que* $\lambda = \pm\sqrt{-1}$*), então ele é um autovetor com autovalor* $i^{-1}\lambda\mu$, *em que* $\mu = b_1^{-1} V(q)$, *da QFNT indicada no enunciado da proposição.*

Demonstração. (a) Se $\mathbf{v}$ tem simetria par, i. e. $v(n) = v(N-n)$, $n = 1, \ldots, N-1$, então

$$\sum_{n=0}^{N-1} v(n) \sin_q(kn) = 0. \tag{4.21}$$

Portanto, empregando (3.24), pode-se escrever

$$\begin{aligned} V^R(k) &= \frac{1}{\sqrt{N}} \sum_{n=1}^{N-1} v(n) q^{kn} = \frac{1}{\sqrt{N}} \left[\sum_{n=1}^{N-1} v(n) \cos_q(kn) + \underbrace{\mu \sum_{n=1}^{N-1} v(n) \sin_q(kn)}_{=0} \right] \\ &= \frac{1}{\sqrt{N}} \sum_{n=1}^{N-1} v(n) \cos_q(kn). \end{aligned} \tag{4.22}$$

Da Proposição 3.4, tem-se que $\cos_\zeta(x) = \cos_q(x)$ e $\sin_\zeta(x) = \sin_q(x)$, $x = 0, 1, \ldots, N-1$. Então, (4.22) pode ser reescrita como

$$\begin{aligned} V^R(k) &= \frac{1}{\sqrt{N}} \left[\sum_{n=1}^{N-1} v(n) \cos_\zeta(kn) + \underbrace{i \sum_{n=1}^{N-1} v(n) \sin_\zeta(kn)}_{=0} \right] \\ &= \frac{1}{\sqrt{N}} \sum_{n=1}^{N-1} v(n) \zeta^{kn} = \lambda v(k). \end{aligned}$$

(b) De modo análogo, se **v** tem simetria ímpar, i. e. $v(n) = -v(N-n)$, $n = 1, \ldots, N-1$ e $v(0) = 0$, então

$$\sum_{n=0}^{N-1} v(n) \cos_q(kn) = 0. \tag{4.23}$$

Portanto, pode-se escrever

$$\begin{aligned} V^R(k) &= \frac{1}{\sqrt{N}} \sum_{n=1}^{N-1} v(n) q^{kn} = \frac{1}{\sqrt{N}} \left[\underbrace{\sum_{n=1}^{N-1} v(n) \cos_q(kn)}_{=0} + \mu \sum_{n=1}^{N-1} v(n) \sin_q(kn) \right] \\ &= \frac{\mu}{\sqrt{N}} \sum_{n=1}^{N-1} v(n) \sin_q(kn). \end{aligned} \tag{4.24}$$

Mas, por hipótese,

$$V(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} v(n) \zeta^{kn} = \frac{i}{\sqrt{N}} \sum_{n=0}^{N-1} v(n) \sin_\zeta(kn) = \lambda v(k), \tag{4.25}$$

e, então,

$$\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} v(n) \sin_\zeta(kn) = i^{-1} \lambda v(k). \tag{4.26}$$

Utilizando a última equação, (4.24) pode ser reescrita como

$$V^R(k) = \mu i^{-1} \lambda v(k). \tag{4.27}$$

□

Na Tabela 2, são indicados os autovalores da QFNT e suas multiplicidades para diferentes comprimentos N; naturalmente, essas multiplicidades são determinadas com base na correspondência entre os referidos autovalores e os autovalores da FNT (vide Proposição 4.1). Autovetores associados a autovalores específicos da QFNT podem, então, ser construídos empregando as diferentes técnicas para construção de autovetores da FNT. Essas técnicas incluem o uso de matrizes geradoras, de fórmulas fechadas, de matrizes comutantes etc. (**??**). A seguir, um exemplo ilustrativo dos conceitos abordados nesta seção é provido.

Exemplo 4.2. *Neste exemplo, ilustra-se a construção de autovetores de uma QFNT de comprimento* $N = 8$ *sobre* $\mathbb{F}_7$.

Tabela 2 – Multipicidades dos autovalores da matriz $\mathbf{F}_q$ da transformada numérica de Fourier quaterniônica com dimensões $N \times N$.

	$\#\{1\}$	$\#\{-\mu i^{-1}\sqrt{-1}\}$	$\#\{-1\}$	$\#\{\mu i^{-1}\sqrt{-1}\}$
$4L$	$L+1$	L	L	$L-1$
$4L+1$	$L+1$	L	L	L
$4L+2$	$L+1$	L	$L+1$	L
$4L+3$	$L+1$	$L+1$	$L+1$	L

4.4 CÁLCULO DA QFNT

Nesta seção, realiza-se uma discussão preliminar sobre formas de calcular a QFNT. O primeiro método apresentado é uma extensão, considerando a definição da transformada sobre quaternions generalizados em $\mathbb{F}_p$, de uma ideia que originalmente considera a QFT e demonstra que esta pode ser calculada por meio de duas DFT (**??**). No presente contexto, o cálculo é feito empregando duas FNT, as quais, por sua vez, podem ser calculadas empregando algoritmos rápidos conhecidos e que demandam números reduzidos de operações aritméticas de adição e multiplicação, quando comparados com a complexidade de $\mathcal{O}(N^2)$ exigida pelo cálculo direto da transformada. A restrição deste método é que o núcleo da QFNT a ser calculada precisa ser um quaternion puro.

Considere um vetor $\mathbf{x} = (x(n))$, $n = 0, 1, \ldots, N-1$, cuja transformada quaterniônica $\mathbf{X} = (X(k))$, $k = 0, 1, \ldots, N-1$, deseja-se calcular. Segundo a Definição 4.1, assumindo que o núcleo da transformada é um quaternion puro q tal que $\mathrm{ord}(q) = N$, as componentes $X(k)$ são calculadas por

$$X(k) = \sum_{n=0}^{N-1} x(n) q^{kn}. \tag{4.28}$$

Se se fizer $\mu_1 = q$ e se encontrar um outro quaternion puro μ_2 tal que $\mu_1 \perp \mu_2$, determina-se um terceiro quaternion puro μ_3 e compõe-se a base ortogonal (μ_1, μ_2, μ_3)[1]. Assim, é possível expressar as componentes $x(n)$ na forma simplética associada à referida base como

$$x(n) = (a'(n) + b'(n)\mu_1) + (c'(n) + d'(n)\mu_1)\mu_2$$

e reescrever (4.28) como

$$\begin{aligned} X(k) &= \sum_{n=0}^{N-1} [(a'(n) + b'(n)\mu_1) + (c'(n) + d'(n)\mu_1)\mu_2]\mu_1^{kn} \\ &= \sum_{n=0}^{N-1} (a'(n) + b'(n)\mu_1)\mu_1^{kn} + \sum_{n=0}^{N-1} (c'(n) + d'(n)\mu_1)\mu_2\mu_1^{kn}. \end{aligned} \tag{4.29}$$

[1] Lembre que, na verdade, a condição $\mu_1 \perp \mu_2$ não precisa ser satisfeita; neste caso, a base (μ_1, μ_2, μ_3) não seria ortogonal, mas nada do que se considera no desenvolvimento que se apresenta em seguida, com respeito à representação simplética de quaternions generalizados, seria alterado.

Neste ponto, convém avaliar o comportamento de potências de μ_1 e, para isso, a representação matricial deste quaternion, que é denotada por $[\mu_1]$, é considerada. Assumindo que $\mu_1 = b_{\mu_1} i + c_{\mu_1} j + d_{\mu_1} k$, tem-se

$$[\mu_1] = \begin{bmatrix} b_{\mu_1} i & c_{\mu_1} + d_{\mu_1} i \\ -c_{\mu_1} + d_{\mu_1} i & -b_{\mu_1} i \end{bmatrix}, \tag{4.30}$$

a qual pode ser expandida como

$$[\mu_1] = \mathbf{V} \begin{bmatrix} \lambda & 0 \\ 0 & -\lambda \end{bmatrix} \mathbf{V}^{-1}. \tag{4.31}$$

Na última equação, $\mathbf{V}$ é uma matriz cujas colunas são autovetores de $[\mu_1]$ associados aos autovalores λ e $-\lambda$, em que, segundo (3.36), $\lambda = \sqrt{-b_{\mu_1}^2 - c_{\mu_1}^2 - d_{\mu_1}^2}$. Sabe-se que $\lambda \neq 0$, pois, caso contrário, q não seria inversível e a QFNT em questão não poderia ser definida. Vê-se, então, que dois casos precisam ser considerados, ao se elevar μ_1 a um expoente m. Se m for par, tem-se

$$[\mu_1]^m = \mathbf{V} \begin{bmatrix} \lambda^m & 0 \\ 0 & \lambda^m \end{bmatrix} \mathbf{V}^{-1} = \begin{bmatrix} \lambda^m & 0 \\ 0 & \lambda^m \end{bmatrix} \tag{4.32}$$

ou, equivalentemente, $\mu_1^m = \lambda^m$. Neste caso, tem-se que $\mu_1^m = \lambda^m \in \mathbb{F}_p$. Se m for ímpar, tem-se

$$[\mu_1]^m = \mathbf{V} \begin{bmatrix} \lambda^{m-1}\lambda & 0 \\ 0 & \lambda^{m-1}(-\lambda) \end{bmatrix} \mathbf{V}^{-1} = \begin{bmatrix} \lambda^{m-1} & 0 \\ 0 & \lambda^{m-1} \end{bmatrix} [\mu_1] \tag{4.33}$$

ou, equivalentemente, $\mu_1^m = \lambda^{m-1}\mu_1$, em que $\lambda^{m-1} \in \mathbb{F}_p$.

Voltando a (4.29), observa-se que a expressão no primeiro somatório tem a mesma forma que a do cálculo de uma FNT definida com núcleo μ_1 e cujas componentes do vetor cuja transformada se deseja calcular são expressas na base $(1, \mu_1)$ de um espaço bidimensional sobre $\mathbb{F}_p$. Noutras palavras, identifica-se um isomorfismo entre o cálculo neste primeiro somatório e aquele realizado após a substituição de μ_1 por um imaginário puro $\alpha \in \mathbb{I}_p$. De modo mais específico, se se fizer

$$A' + B'\mu_1 = \sum_{n=0}^{N-1} (a'(n) + b'(n)\mu_1)\mu_1^{kn},$$

pode-se obter A' e B' escolhendo um elemento α tal que $\mathrm{ord}(\alpha) = N$ e $\alpha^m = \mu_1^m = \lambda^m$, para m par, isto é, $\alpha = \pm\lambda$, e calculando a FNT

$$A' + B'\alpha = \sum_{n=0}^{N-1} (a'(n) + b'(n)\alpha)\alpha^{kn}.$$

Algo semelhante pode ser obtido do segundo somatório de (4.29). Neste caso, é preciso mover μ_2 para fora do somatório (à direita). Isso pode ser feito considerando o fato de que, devido à não-comutatividade entre μ_1 e μ_2, se kn for par, tem-se

$$\mu_2\mu_1^{kn} = \mu_1^{kn}\mu_2,$$

e, se kn for ímpar, tem-se

$$\mu_2\mu_1^{kn} = -\mu_1^{kn}\mu_2.$$

Assim,

$$\begin{aligned}\sum_{n=0}^{N-1}(c'(n)+d'(n)\mu_1)\mu_2\mu_1^{kn} &= \left[\sum_{n=0}^{N-1}(c'(n)+d'(n)\mu_1)(-1)^{kn}\mu_1^{kn}\right]\mu_2 \\ &= \left[\sum_{n=0}^{N-1}(c'(n)+d'(n)\mu_1)(-\mu_1)^{kn}\right]\mu_2\end{aligned}$$

e, se se fizer,

$$C'+D'\mu_1 = \sum_{n=0}^{N-1}(c'(n)+d'(n)\mu_1)(-\mu_1)^{kn},$$

pode-se obter C' e D' usando o mesmo elemento $\alpha = \lambda$ anteriormente caracterizado e calculando a FNT

$$C'+D'\alpha = \sum_{n=0}^{N-1}(c'(n)+d'(n)\alpha)(-\alpha)^{kn}.$$

Como resultado, obtém-se a QFNT de $\mathbf{x}$ em sua forma simplética

$$\mathbf{X} = (A'+B'\mu_1)+(C'+D'\mu_1)\mu_2.$$

Do ponto de vista de complexidade aritmética associada ao cálculo propriamente dito da QFNT, o procedimento desenvolvido requer o cálculo de duas transformadas numéricas de Fourier de comprimento N sobre $\mathbb{I}_p$. Conforme mencionado anteriormente, este cálculo pode ser feito empregando algoritmos rápidos disponíveis na literatura (**??**). Além disso, independentemente do algoritmo que se utilize para computar tais transformadas, deve-se observar que, como α é puramente imaginário, os elementos das respectivas matrizes de transformação são também puramente imaginários ou pertencentes a $\mathbb{F}_p$; assim, todos os produtos efetuados envolvem 2 multiplicações em $\mathbb{F}_p$ (e não 3 ou 4, que seria o número necessário caso os operandos fossem elementos de $\mathbb{I}_p$, com partes reais e imaginárias possivelmente não nulas).

Os passos do procedimento apresentado para o cálculo de $\mathbf{X}$, a QFNT de comprimento N com núcleo dado por um quaternion puro $\mu_1 = b_{\mu_1}i + c_{\mu_1}j + d_{\mu_1}k$ de um vetor $\mathbf{x}$, são sumarizados a seguir:

1. Encontre um quaternion puro μ_2, tal que $\mu_1 \perp \mu_2$, e obtenha a representação simplética

   $$\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2\mu_2;$$

   as componentes de $\mathbf{x}_1$ e $\mathbf{x}_2$ pertencem ao plano $(1, \mu_1)$.

2. Expanda as componentes simpléticas

   $$\mathbf{x}_1 = a' + b'\mu_1$$

e

$$\mathbf{x}_2 = c' + d'\mu_1;$$

as componentes a', b', c' e d' são escalares.

3. Faça $\alpha = \pm\lambda = \sqrt{-b_{\mu_1}^2 - c_{\mu_1}^2 - d_{\mu_1}^2}$ e construa os vetores complexos

$$\mathbf{x}_1' = a' + b'\alpha$$

e

$$\mathbf{x}_2' = c' + d'\alpha.$$

4. Calcule as FNT com núcleos dados por α e $-\alpha$ de $\mathbf{x}_1'$ e $\mathbf{x}_2'$, respectivamente. Essas FNT são expressas como

$$\mathbf{X}_1' = A' + B'\alpha$$

e

$$\mathbf{X}_2' = C' + D'\alpha.$$

5. Obtenha as componentes da representação simplética de $\mathbf{X}$

$$\mathbf{X}_1 = A' + B'\mu_1$$

e

$$\mathbf{X}_2 = C' + D'\mu_1.$$

6. Obtenha $\mathbf{X}$ em sua forma simplética por

$$\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2\mu_2.$$

Exemplo 4.3. *A fim de ilustrar a aplicação do procedimento descrito, considera-se a QFNT de comprimento* $N = 12$ *do vetor de quaternions generalizados sobre* $\mathbb{F}_7$

$$\mathbf{x} = \begin{bmatrix} 5+6i+0j+1k \\ 4+0i+6j+4k \\ 6+6i+6j+1k \\ 6+3i+2j+0k \\ 2+6i+2j+1k \\ 4+0i+2j+1k \\ 4+5i+2j+5k \\ 4+1i+3j+0k \\ 1+0i+0j+2k \\ 4+2i+1j+0k \\ 3+2i+2j+2k \\ 1+3i+4j+3k \end{bmatrix}.$$

O quaternion puro usado para definir a transformada é $q = 6i + 4j + 1k$*, o qual possui ordem multiplicativa* $\mathrm{ord}(q) = 12$*. Diretamente da definição, obtém-se a QFNT de* $\mathbf{x}$*:*

$$\mathbf{X} = \begin{bmatrix} 2+6i+2j+6k \\ 4+4i+2j+2k \\ 1+4i+3j+0k \\ 4+6i+4j+2k \\ 4+0i+4j+6k \\ 3+6i+5j+6k \\ 5+2i+1j+4k \\ 5+6i+5j+0k \\ 2+0i+2j+6k \\ 0+6i+1j+4k \\ 5+5i+0j+0k \\ 4+6i+6j+4k \end{bmatrix}.$$

Para aplicar o procedimento descrito e verificar que, como resultado, obtém-se o mesmo vetor transformado $\mathbf{X}$ *dado na última expressão, (1) faz-se, inicialmente,* $\mu_1 = q$ *e, escolhendo* $\mu_2 = 4i + 4j + 2k$*, obtém-se a representação simplética de* $\mathbf{x}$*, a qual é dada por*

$$\mathbf{x} = \begin{bmatrix} (5+4\mu_1)+(5+1\mu_1)\mu_2 \\ (4+0\mu_1)+(4+3\mu_1)\mu_2 \\ (6+3\mu_1)+(1+3\mu_1)\mu_2 \\ (6+3\mu_1)+(6+6\mu_1)\mu_2 \\ (2+6\mu_1)+(6+4\mu_1)\mu_2 \\ (4+4\mu_1)+(3+5\mu_1)\mu_2 \\ (4+2\mu_1)+(3+4\mu_1)\mu_2 \\ (4+1\mu_1)+(2+2\mu_1)\mu_2 \\ (1+4\mu_1)+(4+4\mu_1)\mu_2 \\ (4+4\mu_1)+(5+0\mu_1)\mu_2 \\ (3+2\mu_1)+(6+2\mu_1)\mu_2 \\ (1+4\mu_1)+(6+1\mu_1)\mu_2 \end{bmatrix}.$$

(2) As componentes simplex e perplex de $\mathbf{x}$ *são dadas respectivamente por*

$$\mathbf{x}_1 = \begin{bmatrix} 5+4\mu_1 \\ 4+0\mu_1 \\ 6+3\mu_1 \\ 6+3\mu_1 \\ 2+6\mu_1 \\ 4+4\mu_1 \\ 4+2\mu_1 \\ 4+1\mu_1 \\ 1+4\mu_1 \\ 4+4\mu_1 \\ 3+2\mu_1 \\ 1+4\mu_1 \end{bmatrix} \quad e \quad \mathbf{x}_2 = \begin{bmatrix} 5+1\mu_1 \\ 4+3\mu_1 \\ 1+3\mu_1 \\ 6+6\mu_1 \\ 6+4\mu_1 \\ 3+5\mu_1 \\ 3+4\mu_1 \\ 2+2\mu_1 \\ 4+4\mu_1 \\ 5+0\mu_1 \\ 6+2\mu_1 \\ 6+1\mu_1 \end{bmatrix}.$$

(3) Faça $\alpha = \sqrt{-6^2 - 4^2 - 1^2} = \sqrt{-4} = 2i$ *e construa os vetores*

$$\mathbf{x}_1' = \begin{bmatrix} 5+4(2i) \\ 4+0(2i) \\ 6+3(2i) \\ 6+3(2i) \\ 2+6(2i) \\ 4+4(2i) \\ 4+2(2i) \\ 4+1(2i) \\ 1+4(2i) \\ 4+4(2i) \\ 3+2(2i) \\ 1+4(2i) \end{bmatrix} = \begin{bmatrix} 5+1i \\ 4+0i \\ 6+6i \\ 6+6i \\ 2+5i \\ 4+1i \\ 4+4i \\ 4+2i \\ 1+1i \\ 4+1i \\ 3+4i \\ 1+1i \end{bmatrix} \quad e \quad \mathbf{x}_2' = \begin{bmatrix} 5+1(2i) \\ 4+3(2i) \\ 1+3(2i) \\ 6+6(2i) \\ 6+4(2i) \\ 3+5(2i) \\ 3+4(2i) \\ 2+2(2i) \\ 4+4(2i) \\ 5+0(2i) \\ 6+2(2i) \\ 6+1(2i) \end{bmatrix} = \begin{bmatrix} 5+2i \\ 4+6i \\ 1+6i \\ 6+5i \\ 6+1i \\ 3+3i \\ 3+1i \\ 2+4i \\ 4+1i \\ 5+0i \\ 6+4i \\ 6+2i \end{bmatrix}.$$

(4) Empregando a Definição 2.4[2]*, obtém-se a matriz da FNT com núcleo* $\alpha = 2i$ *a ser aplicada*

[2] Observe que, na Definição 2.4, embora se tenha imposto a restrição de que o núcleo da FNT predominantemente considerada neste trabalho seja unimodular, isto é, pertença ao conjunto $\mathrm{G}_{1,p}$, nada impede que tal núcleo seja um elemento arbitrário pertencente a $\mathbb{I}_p$, como se faz nesta seção e, em particular, neste exemplo.

a $\mathbf{x}'_1$*:*

$$\mathbf{F}_{(2i)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2i & 3 & 6i & 2 & 4i & 6 & 5i & 4 & 1i & 5 & 3i \\ 1 & 3 & 2 & 6 & 4 & 5 & 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 6i & 6 & 1i & 1 & 6i & 6 & 1i & 1 & 6i & 6 & 1i \\ 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 4i & 5 & 6i & 4 & 2i & 6 & 3i & 2 & 1i & 3 & 5i \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5i & 3 & 1i & 2 & 3i & 6 & 2i & 4 & 6i & 5 & 4i \\ 1 & 4 & 2 & 1 & 4 & 2 & 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 1i & 6 & 6i & 1 & 1i & 6 & 6i & 1 & 1i & 6 & 6i \\ 1 & 5 & 4 & 6 & 2 & 3 & 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 3i & 5 & 1i & 4 & 5i & 6 & 4i & 2 & 6i & 3 & 2i \end{bmatrix};$$

analogamente, obtém-se a matriz da FNT com núcleo $\alpha = -2i$ *a ser aplicada a* $\mathbf{x}'_2$*:*

$$\mathbf{F}_{(-2i)} = \begin{bmatrix} 1 & 5i & 3 & 1i & 2 & 3i & 6 & 2i & 4 & 6i & 5 & 4i \\ 1 & 3 & 2 & 6 & 4 & 5 & 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 1i & 6 & 6i & 1 & 1i & 6 & 6i & 1 & 1i & 6 & 6i \\ 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 3i & 5 & 1i & 4 & 5i & 6 & 4i & 2 & 6i & 3 & 2i \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2i & 3 & 6i & 2 & 4i & 6 & 5i & 4 & 1i & 5 & 3i \\ 1 & 4 & 2 & 1 & 4 & 2 & 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6i & 6 & 1i & 1 & 6i & 6 & 1i & 1 & 6i & 6 & 1i \\ 1 & 5 & 4 & 6 & 2 & 3 & 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4i & 5 & 6i & 4 & 2i & 6 & 3i & 2 & 1i & 3 & 5i \end{bmatrix};$$

daí, obtém-se

$$\mathbf{X}'_1 = \mathbf{F}_{(2i)}\mathbf{x}'_1 = \begin{bmatrix} 2+2i \\ 2+5(2i) \\ 5+4(2i) \\ 2+3(2i) \\ 2+0(2i) \\ 0+1(2i) \\ 5+5(2i) \\ 5+2(2i) \\ 4+2(2i) \\ 2+4(2i) \\ 1+2(2i) \\ 2+4(2i) \end{bmatrix} \quad e \quad \mathbf{X}'_2 = \mathbf{F}_{(-2i)}\mathbf{x}'_2 = \begin{bmatrix} 2+0(2i) \\ 3+6(2i) \\ 6+5(2i) \\ 0+6(2i) \\ 6+1(2i) \\ 6+3(2i) \\ 6+1(2i) \\ 4+4(2i) \\ 0+4(2i) \\ 3+1(2i) \\ 0+5(2i) \\ 3+4(2i) \end{bmatrix}.$$

(5), (6) Assim, $\mathbf{X}$ *é dado em sua forma simplética por*

$$\mathbf{X} = \begin{bmatrix} (2+2\mu_1)+(2+0\mu_1)\mu_2 \\ (2+5\mu_1)+(3+6\mu_1)\mu_2 \\ (5+4\mu_1)+(6+5\mu_1)\mu_2 \\ (2+3\mu_1)+(0+6\mu_1)\mu_2 \\ (2+0\mu_1)+(6+1\mu_1)\mu_2 \\ (0+1\mu_1)+(6+3\mu_1)\mu_2 \\ (5+5\mu_1)+(6+1\mu_1)\mu_2 \\ (5+2\mu_1)+(4+4\mu_1)\mu_2 \\ (4+2\mu_1)+(0+4\mu_1)\mu_2 \\ (2+4\mu_1)+(3+1\mu_1)\mu_2 \\ (1+2\mu_1)+(0+5\mu_1)\mu_2 \\ (2+4\mu_1)+(3+4\mu_1)\mu_2 \end{bmatrix},$$

a qual, se convertida para a base canônica (i, j, k)*, coincide com a representação de* $\mathbf{X}$ *dada no início do exemplo.*

O segundo método para implementação da QFNT é baseado nas ideias clássicas de dizimação no tempo e na frequência. A aplicação de tais ideias ao presente cenário é bastante direta, uma vez que o núcleo da transformada, assim como no caso da DFT e no da FNT, é uma raiz $\omega_N = q$ de ordem N da unidade na estrutura algébrica considerada, a qual pode ser usada para expressar, por exemplo, uma raiz $\gamma_{N'}$ de ordem $N' = N/2$ da unidade como $\gamma_{N'} = \omega_N^2$. Neste caso, agrupando as componentes de índice par e as de índice ímpar do vetor $\mathbf{x}$ cuja transformada se deseja obter, a expressão para o cálculo das componentes da QFNT pode ser reescrita como

$$\begin{aligned} X(k) &= \sum_{n=0}^{N'-1} x(2n)\omega_N^{k(2n)} + \sum_{n=0}^{N'-1} x(2n+1)\omega_N^{k(2n+1)} \\ &= \sum_{n=0}^{N'-1} x_e(n)\gamma_{N'}^{kn} + \omega_N^k \sum_{n=0}^{N'-1} x_o(n)\gamma_{N'}^{kn}, \end{aligned} \tag{4.34}$$

$k = 0, 1, \ldots, N-1$, em que $x_e(n) = x(2n)$ e $x_o(n) = x(2n+1)$, $n = 0, 1, \ldots, N'-1$. Em (4.34), vê-se que o cálculo de uma QFNT de comprimento par N pode ser realizado por meio do cálculo de duas QFNT de comprimento $N' = N/2$; produtos entre ω_N^k e o segundo somatório da referida expressão precisam ser contabilizados. Essa ideia pode ser generalizada para valores de N com diferentes fatorações. Em particular, quando N é uma potência de 2, algoritmos com complexidade de $\mathcal{O}(N \log_2 N)$ operações entre quaternions podem ser obtidos.

Em todo caso, se o objetivo for mensurar a complexidade aritmética deste segundo método de implementação da QFNT em termos de operações sobre o corpo base, é preciso considerar estratégias para calcular sobretudo produtos entre quaternions de modo mais eficiente

que o direto, o qual emprega 16 multiplicações em $\mathbb{F}_p$ (vide (3.5)). Embora essa questão não seja abordada com profundidade no presente trabalho, é válido citar algumas referências que podem ser úteis ao leitor interessado. O problema de determinar a complexidade de um produto entre quaternions é um caso especial do problema de determinar a complexidade de um conjunto de formas bilineares (**??**). Outros casos especiais aparecem na literatura, como, por exemplo, o do cálculo do produto entre matrizes 2×2, que, segundo (**??**), pode ser efetuado com 7 multiplicações. Em (**??**) e (**??**), mostra-se que o referido número é também necessário, tanto no caso geral (os elementos das matrizes podem pertencer a aneis comutativos ou não-comutativos) quanto no caso comutativo. Em (**??**), o autor menciona que 10 multiplicações são suficientes para o produto quaterniônico e, em (**??**), demonstra-se que 10 é o número necessário e suficiente de mutiplicações para calcular simultaneamente os produtos q_1q_2 e q_2q_1 entre dois quaternions q_1 e q_2. Finalmente, em (**??**), mostra-se que 8 é o número necessário e suficiente para realizar um produto quaterniônico no caso geral e que pelo menos 7 multiplicações são necessárias no caso comutativo. Em trabalhos futuros, pretende-se considerar as referências citadas e avaliar, inclusive, se o fato de, no cálculo de uma QFNT, estar-se realizando produtos basicamente por potências de um elemento q fixo empregado como núcleo, permite que o número global de operações no corpo base $\mathbb{F}_p$ requeridos pela transformada seja reduzido ainda mais.

5 APLICAÇÕES DA QFNT EM PROCESSAMENTO DE IMAGENS

NESTE capítulo, são discutidas de forma preliminar algumas possíveis aplicações da transformada introduzida no Capítulo 4. O foco é no campo de processamento digital de imagens, em que a QFNT permite a manipulação simultânea de até quatro canais associados a algum espaço de cores. Essa ideia, que tem sido explorada em diversos trabalhos arquivados na literatura, faz contraponto à maioria das técnicas voltadas ao processamento digital de imagem, que são aplicáveis a imagens monocromáticas (imagens em escala de cinza, por exemplo); quando se trata de processar imagens coloridas, o que normalmente se faz é aplicar essas técnicas de forma independente a cada canal de cor.

Recorrendo aos quaternions, o que se faz é mapear nas coordenadas de um quaternion os valores numéricos associados a cada canal de cor de um pixel em determinada posição da imagem. No caso de uma imagem RGB (*red*,*green*,*blue*), pode-se, por exemplo, atribuir o valor zero à parte real do respectivo quaternion, e atribuir os valores numéricos associados às camadas vermelha, verde e azul de um pixel aos coeficientes de i, j e k do mesmo quaternion, respectivamente. No caso de uma imagem PNG (*portable network graphics*), além dos três canais de cor RGB, pode-se ter uma camada adicional de transparência que é aplicada às primeiras; essa camada de transparência seria associada à parte real dos quaternions, que tinha sido anulada no caso de images RGB sem canal extra de transparência. Utilizando estratégias como essas, uma imagem colorida pode ser representada por uma matriz de quaternions, cuja QFNT pode ser calculada. Observe que, se os quaternions nessa matriz forem também representados matricialmente, ter-se-á a imagem representada como uma *matriz de matrizes* 2×2, cujos números de linhas e de colunas são o dobro dos números de linhas e colunas da imagem correspondente.

Naturalmente, a aplicação de uma QFNT a uma imagem requer uma versão bidimensional dessa ferramenta. De fato, versões 2D da QFT discreta têm sido extensivamente estudadas e aplicadas em cenários envolvendo processamento de imagem. A maior parte das propriedades dessas transformadas decorre de extensões relativamente simples a duas dimensões das respectivas propriedades da QFT unidimensional. A expectativa é que algo semelhante seja observado, considerando as versões em uma e em duas dimensões da QFNT; tal hipótese deve ser investigada até a conclusão desta tese. Por ora, é suficiente observar que uma QFT bidimensional de uma imagem $\mathbf{y}$ quadrada com dimensões $N \times N$ pode ser calculada multiplicando a matriz de transformação da QFNT unidimensional e a sua versão transposta respectivamente à direita e à esquerda por $\mathbf{y}_q$, representação quaterniônica de $\mathbf{y}$. Dessa forma, a 2D-QFNT é calculada por

$$\mathbf{Y}_q = \mathbf{M_Q} \mathbf{y}_q \mathbf{M_Q}^T, \tag{5.1}$$

em que $\mathbf{M_Q} = (M_\mathbf{Q}(m,n)) = \mathbf{Q}^{mn}$, $m, n = 0, 1, \ldots, N-1$, é a matriz da QFNT unidimensional. Da matriz quaterniônica $\mathbf{Y}_q$, obtém-se a imagem (colorida) transformada $\mathbf{Y}$. A 2D-QFNT

inversa é calculada trocando-se $\mathbf{M_Q}$ por $\mathbf{M_Q}^{-1}$.

Como consequência da possibilidade de se calcular a QFNT de imagens coloridas, algumas aplicações mais específicas podem ser vislumbradas. Dentre elas, podem ser mencionadas:

- A filtragem de imagens coloridas usando filtros cujos coeficientes sejam quaternions generalizados sobre um corpo finito. É razoável esperar que uma filtragem desse tipo possa ser processada no domínio da 2D-QFNT, empregando alguma versão do Teorema da Convolução adaptado para essa transformada;
- A inserção / extração de marcas d'água frágeis. Há artigos em que são documentados esquemas de marca d'água baseados em transformadas numéricas. Usando a QFNT, talvez seja possível criar esquemas semelhantes diretamente aplicáveis a imagens coloridas;
- A cifragem de imagens coloridas. Recentemente, têm sido propostas técnicas para cifragem de imagens empregando transformadas numéricas e, em particular, versões fracionárias dessas transformadas. Isso é possível, basicamente, empregando a ordem fracionária como um parâmetro secreto, que muda a cada bloco de imagem processado. Introduzindo alguma espécie de parametrização na definição da QFNT, algo similar pode ser proposto. Ainda que não haja parametrização, é possível que uma etapa de aplicação da QFNT possa contribuir para a robustez de esquemas de cifragem de imagem contra ataques baseados em medidas estatísticas. Isso é ilustrado na seção a seguir.

5.1 FORMATAÇÃO DE HISTOGRAMAS PARA CIFRAGEM DE IMAGENS

Nesta seção, são apresentados alguns resultados ilustrativos da aplicação da QFNT a imagens coloridas. Define-se uma 2D-QFNT a partir de uma QFNT unidimensional cujo núcleo é o quaternion $q = 7 + 8i + 4j + 8k$ sobre $\mathbb{F}_{257}$. A ordem multiplicativa de q é $\mathrm{ord}(q) = 128$ e, portanto, uma transformada com comprimento $N = 128$ é obtida. Essa transformada é, então, aplicada à representação quaterniônica de uma imagem PNG com dimensões 128×128 e com camada de transparência, conforme descrito anteriormente.

Nos experimentos computacionais realizados, considerou-se a imagem cujas camadas de cor são apresentadas na Figura 1. Na Figura 2a, é apresentada a respectiva imagem colorida, sem a inclusão da camada de transparência, que é mostrada isoladamente na Figura 2b. Nesta camada de transparência, que, alinhada com as camadas de cor, funciona como uma espécie de "janela", quanto mais próxima do branco for determinada região, mais se verá das cores que estão "por trás" dessa região; quanto mais próxima do preto for determinada região, menos se verá das cores que estão "por trás" dessa região, a qual, na imagem final, é substituída por uma região com tom igualmente próximo do branco. A referida imagem final, considerando a ação da camada de transparência, é apresentada na Figura 2c.

(a) (b) (c)

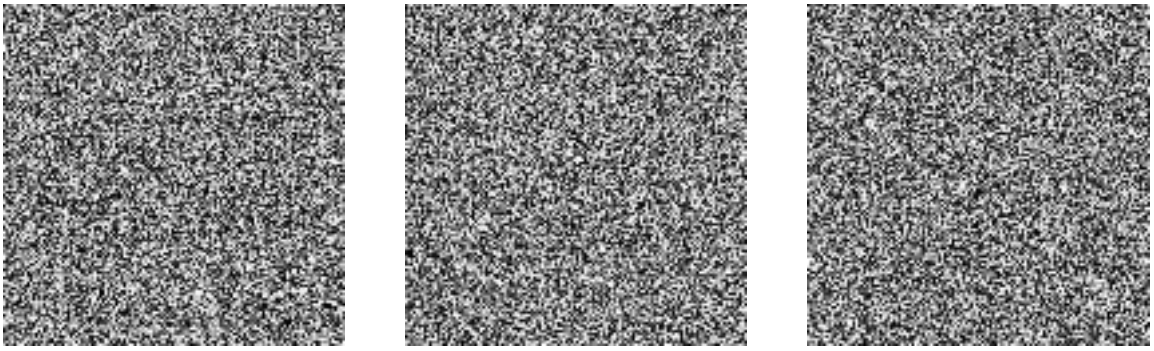
Figura 1 – Imagem original: camadas (a) vermelha, (b) verde e (c) azul.

(a) (b) (c)

Figura 2 – Imagem original: (a) três camadas de cor (sem camada de transparência), (b) camada de transparência e (c) três camadas de cor (com camada de transparência).

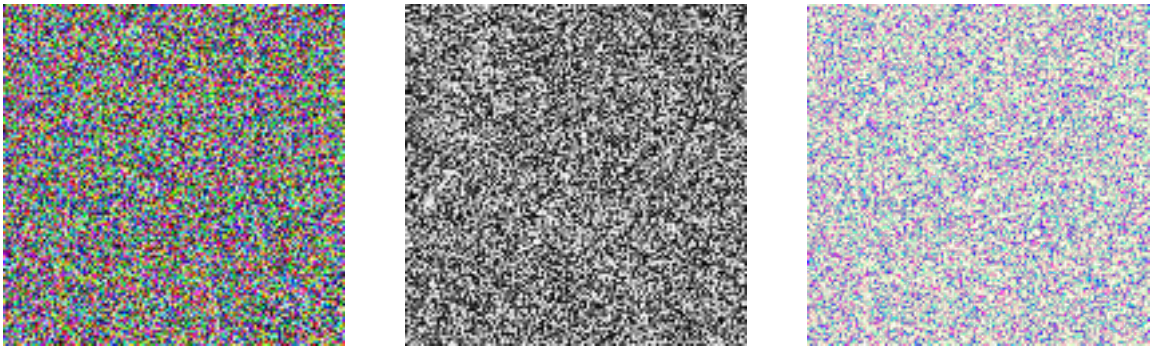
Nas Figuras 3 e 4, são apresentadas camadas e imagens correspondentes àquelas apresentadas nas Figuras 1 e 2, porém, considerando a versão transformada da imagem original. O que mais chama atenção nas últimas figuras é o aspecto visual ruidoso, que sugere uma degradação do conteúdo das camadas e imagens originais. Tal aspecto tem reflexo no histograma de cada uma das referidas camadas, conforme mostrado na Figura 5. Enquanto os histogramas das camadas de cor e de transparência da imagem original têm formatos arbitrários, os mesmos histogramas têm formato predominantemente uniforme na imagem transformada. A aparente ocultação, proporcionada pela aplicação da QFNT, da distribuição original dos valores dos pixels da imagem é um fenômeno positivo do ponto de vista criptográfico.

Outra observação interessante pode ser feita ao se calcular os coeficientes de correlação para as camadas da imagem original e da imagem transformada. Este coeficiente mede a correlação entre pixels vizinhos de uma imagem (a vizinhança pode ser vertical, horizontal ou diagonal) e deve ser elevado (próximo de 1) em imagens que não tenham sido manipuladas



(a) (b) (c)

Figura 3 – Imagem transformada: camadas (a) vermelha, (b) verde e (c) azul.

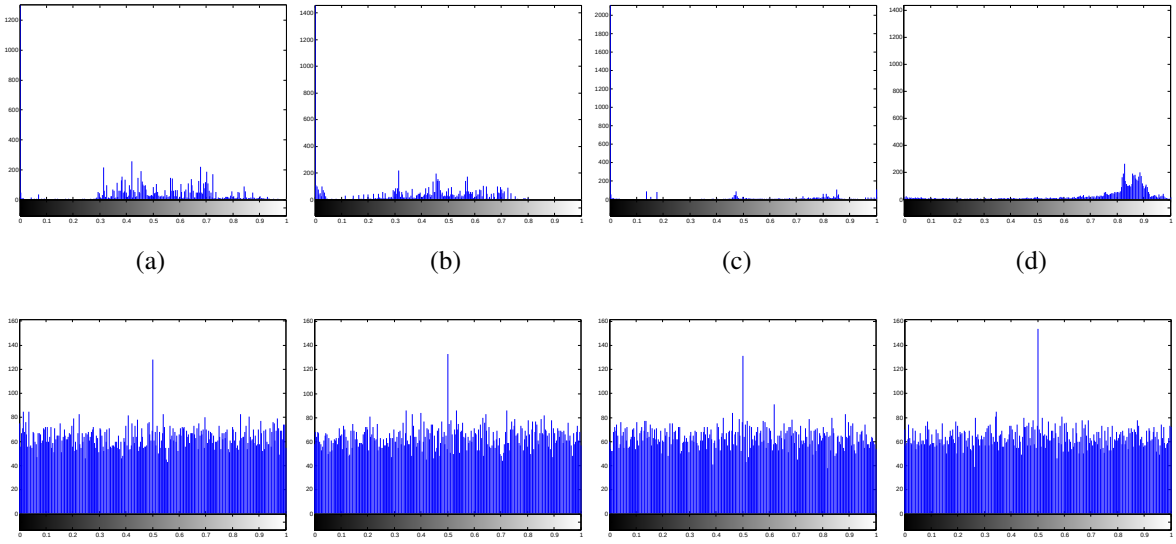


(a) (b) (c)

Figura 4 – Imagem transformada: (a) três camadas de cor (sem camada de transparência), (b) camada de transparência e (c) três camadas de cor (com camada de transparência).

ou construídas artificialmente; isso é confirmado pelos valores obtidos e exibidos na primeira parte da Tabela 3. Por outro lado, ao se transformar a imagem com a QFNT, os coeficientes de correlação obtidos têm valor absoluto sempre menor que 0.05, o que indica pouca dependência entre os valores assumidos por pixels vizinhos. Tal comportamento também é desejável do ponto de vista criptográfico. Outras métricas como, por exemplo, a entropia normalizada, poderiam ser calculadas para complementar a avaliação dos efeitos da aplicação da QFNT sobre o comportamento estatístico de uma imagem.

Conforme exposto anteriormente, a simples aplicação da QFNT a uma imagem não constitui um esquema criptográfico. Seria necessária a inclusão de algum mecanismo dependente de uma chave secreta e de etapas que garantissem a satisfação de premissas básicas neste cenário. De qualquer forma, considerando os resultados apresentados nesta seção, pode-se observar indícios de que a QFNT é uma candidata em potencial a fazer parte de sistemas para cifragem de imagens, trazendo, inerentemente, a possibilidade de se processar de forma agregada todas as



(a) (b) (c) (d)

(e) (f) (g) (h)

Figura 5 – Histogramas: camadas (a) vermelha, (b) verde, (c) azul e (d) de transparência da imagem original; camadas (d) vermelha, (e) verde, (f) azul e (g) de transparência da imagem transformada.

camadas de uma imagem colorida.

Tabela 3 – Coeficientes de correlação entre pixels vizinhos nas camadas da imagem original (r) e nas da imagem transformada ($\tilde{r}$). As letras v, h e d estão associadas às vizinhanças vertical, horizontal e diagonal, respectivamente.

	vermelha	verde	azul	transp.
r_v	0.9837	0.9937	0.9855	0.9700
r_h	0.9576	0.9620	0.9394	0.9723
r_d	0.9515	0.9589	0.9268	0.9487
$\tilde{r}_v$	0.0061	-0.0056	-0.0238	-0.0233
$\tilde{r}_h$	0.0052	0.0325	0.0401	-0.0048
$\tilde{r}_d$	0.0086	0.0117	-0.0244	0.0216

5.2 MARCA D'ÁGUA DIGITAL NO DOMÍNIO DA QFNT

Neste século de muito avanço tecnológico, computadores ultra velozes, câmeras de alta resolução, internet de altíssima velocidade todas essas ferramentas facilitaram a distribuição gratúita de mídias, porém essa distribuição não possue limites, ter fotos e vídeos vazados na rede mundial de comunicação não é mais um problema de grandes marcas do cinema ou de pessoas com um alto grau de fama, o avanço tecnológico tem tornado a privacidade uma questão de justiça. Se para pessoas comuns isso tem se tornado um pesadelo, supõe-se que para a grande indústria cinematográfica e para os grandes fotográfos e artistas em geral é uma verdadeira guerra provar que tais arquivos (fotos, desenhos, músicas, videos, entre outros)

verdadeiramente é sua propriedade. Uma necessidade adivinda dos problemas de divulgação irregular de mídias (pirataria digital) é a proteção e verificação da autenticidade da mesma, priorizando os processos relacionados a imagens uma ferramenta muito útel e bastante eficaz no combate a pirataria é imprimir secretamente na imagem uma maneira de identificação da mesma, esse processo de imprimir secretamente denomina-se marca d'água digital, ou seja, a marca d'água deve ser detectada facilmente por quem a usou, resistente aos processos que uma imagem pode sofrer (compressão, filtragem e etc.), estatisticamente invisível, impercepitível não alterando visualmente o objeto marcado e ao mesmo tempo deve ser resistente a ataques por parte de terceiros com a intenção de destruir sua existência (LUO; HEILEMAN; PIZANO, 2004; NIKOLAIDIS; PITAS, 1998; VERMA; JHA; OJHA, 2015). Existem dois métodos de inserir uma marca d'água em uma imagem, o primeiro é a inserção da marca no domínio espacial e o segundo é a inserção no domínio da frequência. Para o método de aplicação da marca no domínio espacial sua atuação é a nível do pixel a informação é inserida no bit menos significativo de maneira que não provoque alteração a percepção humana (LUO; HEILEMAN; PIZANO, 2004; NIKOLAIDIS; PITAS, 1998; VERMA; JHA; OJHA, 2015). O segundo método que é a marcação no domínio da frequência, a informação é inserida em coeficientes selecionados, após a aplicação de um método como: Transformada Discreta do Cosseno (DCT), Transformada Discreta de Fourier (DFT), A Transformada Numérica de Fourier Quaterniônica (QFNT), Transformada de Hartley de Corpo Finito (THCF) (LUO; HEILEMAN; PIZANO, 2004; NIKOLAIDIS; PITAS, 1998; VERMA; JHA; OJHA, 2015). O método de inserção de marca d'água em uma imagem pode ser ainda dividida em duas classes distintas baseadas na necessidade de possuir ou não a imagem original para detecção da marca inserida.

5.2.1 A marca d'água proposta

Marca d'água em imagens coloridas que não fazem uso dos quaternions de uma forma geral, operam dividindo a imagem em suas respectivas camadas de cores e inserem a marca em uma ou mais dessas camadas, uma forma similar é alterar apenas a luminância de uma imagem colorida, tal método pode ser facilmente implementado, porém o mesmo não utiliza o vínculo que existe entre as camadas de cores, e também pode diminuir a capacidade da informação inserida (MA et al., 2008; RZADKOWSKI WOJCIECHAND SNOPEK, 2015). Nos últimos anos tem surgido diversos métodos que utilizam quaternions como uma ferramenta que permite a inserção de uma marca d'água em todas as camadas de cores de uma imagem (MA et al., 2008; RZADKOWSKI WOJCIECHAND SNOPEK, 2015). O método proposto neste trabalho para marcação de uma imagem, está baseado na marcação no domínio da frequência e utiliza para essa finalidade os coeficientes da transformada numérica quaterniônica de Fourier para inserir a informação desejada.

5.2.1.1 Inserção da marca-padrão binário

Esse método foi baseado no artigo de Cintra et. al. (CINTRA et al., 2009) onde é exposto de forma detalhada o processo de inserção da marca. Os números quaterniônicos foram utilizados como ferramenta para o processamento da imagem, a imagem hospedeira que é uma imagem colorida PNG possuindo uma quarta camada adicional denominada de transparência, foi transformada em uma imagem na forma de quaternion utilizando a seguinte estratégia, cada pixel dessa imagem possui quatro componentes, por exemplo um pixel de coordenadas (n, m) pode ser representado na forma quaterniônica como: $f(n, m) = t(n, m) + r(n, m)i + g(n, m)j + b(n, m)k$, onde $t(n, m)$ é a componente de transparência, $r(n, m)$, $g(n, m)$ e $b(n, m)$ são as componentes vermelha, verde e azul do pixel. O primeiro passo do processo é escrever a imagem colorida original (I) com a camada adicional de transparência na forma quaterniônica (Iq). Essa imagem na forma de quaternion (Iq) é dividida em dois componentes podendo ser escrita como:

$$Iq = Iq_R + Iq_M, \tag{5.2}$$

onde $Iq_R \equiv Iq\ (mod\ p)$, o Iq_R é denominado resíduo módulo p e Iq_M é uma imagem contendo elementos que são múltiplos de p. O método consiste na inserção de uma imagem de marca d'água (M) no espectro da NTT do resíduo de Iq. Tem-se que $\hat{I}q_R$ é a NTT bidimensional de Iq_R, consequentemente temos a marca sendo inserida

$$\hat{I}'q_R = \hat{I}q_R + Mq\ (mod\ p) \tag{5.3}$$

onde $\hat{I}'q_R$ é o conteúdo espectral de Iq_R contendo a marca e Mq é a marca na forma quaterniônica. Aplicando a NTT bidimensional inversa em $\hat{I}'q_R$ resulta em uma imagem $I'q_R$ quaterniônica no domínio espacial e marcada, associada ao resíduo da imagem hospedeira. Para se obter a imagem quaterniônica final e marcada $(I'q)$ precisa-se adicionar Iq_M, como segue:

$$I'q = I'q_R + Iq_M \tag{5.4}$$

por último precisa-se transformar a imagem queterniônica marcada $I'q$ na imagem marcada I'.

5.2.1.2 Extração da marca-padrão binário

A extração da marca d'água da imagem marcada, ocorre de maneira análoga, primeiro transformamos as imagens para suas respectivas formas quaterniônicas e depois calculamos o

resíduo Iq_R da imagem original e da imagem marcada $I'q_R$,

$$Iq_R = Iq \ (mod \ p), \tag{5.5}$$

$$I'q_R = I'q \ (mod \ p). \tag{5.6}$$

Após esse processo aplica-se a NTT a ambos, tanto ao resíduo da imagem quaterniônica original, quanto ao resíduo da imagem quaterniônica marcada, e a marca Mq pode ser obtida após a diferença entre os espectros obtidos após a aplicação da NTT:

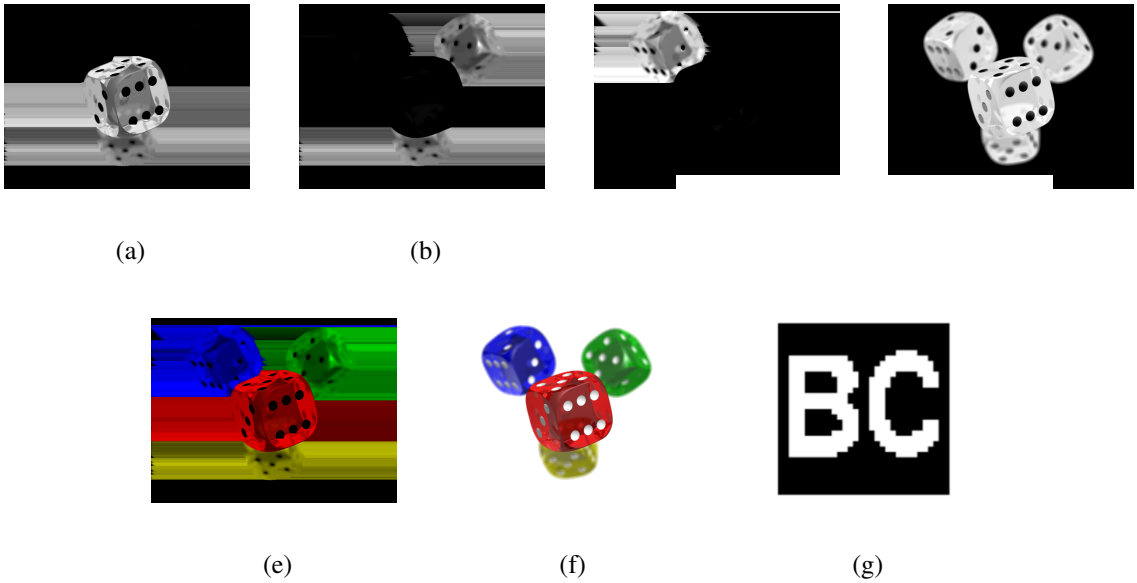
$$Mq = \hat{I}'q_R + \hat{I}q_R \tag{5.7}$$

onde $\hat{I}'q_R$ e $\hat{I}q_R$ são as transfomadas numéricas de $I'q_R$ e Iq_R respectivamente. Porém a marca extraída Mq ainda encontra-se na forma de um quaternion sendo necessário transforma-la para o seu formato original M.

5.2.1.3 Simulações e resultados para marca-padrão binária

Considerou-se uma imagem colorida com uma camada adicional denominada transparência, de tamanho 600×800 pixels com extensão $.png$, a imagem inicialmente não possuia nenhuma marca d'água. O próximo passo foi inserir uma marca no formato de uma imagem binária, de tamanho 32×32 pixels e de extensão $.bmp$.

Na Figura 6a, 6b e 6c são apresentadas as camadas de cores correspondentes a imagem colorida,

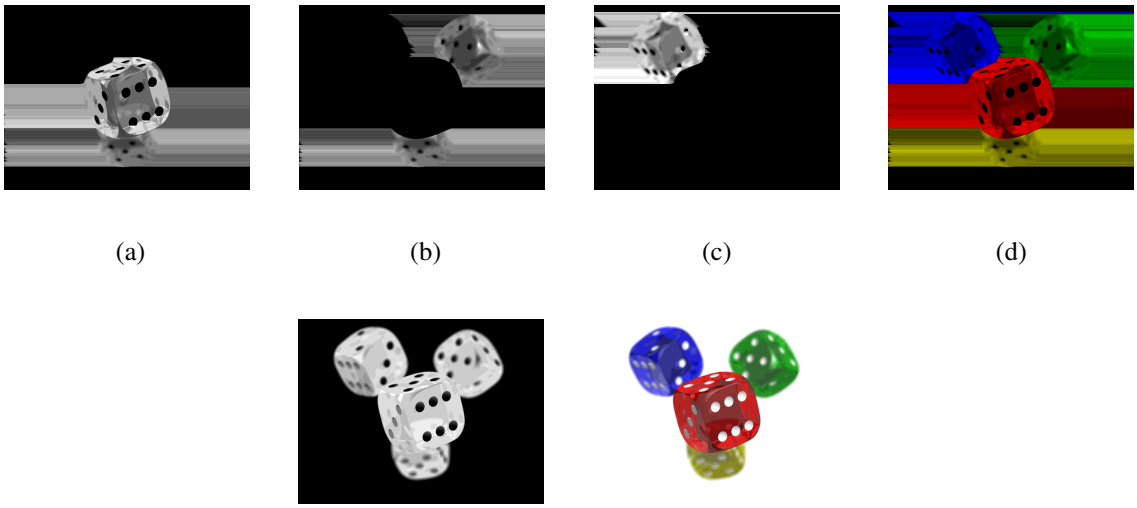


(a) (b)

(e) (f) (g)

Figura 6 – Imagens: (a) camada vermelha, (b) camada verde, (c) camada azul, (d) camadas RGB juntas, (e) camada de transparência (f) camada RGB juntamente com a transparência e (g) marca a ser inserida

na Figura 6d a camada de transparência, na figura 6e as camadas RGB juntas e na Figura 6f a imagem com a camada de transparência e na Figura 6g a marca a ser inserida na imagem hospedeira. O quaternion utilizado como núcleo da transformada envolvido no processo de marcação foi, $q = 4 + 3i + 3j + 10k$ com ordem multiplicativa igual a 16 e fixou-se $p = 17$. O processamento da imagem ocorreu dividindo-a em blocos de 32×32 pixels.

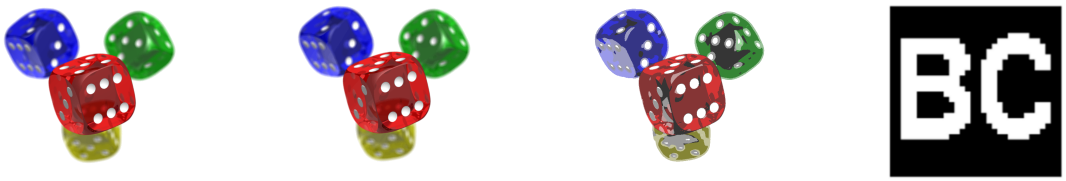


(a) (b) (c) (d)

(e) (f)

Figura 7 – Imagens: camadas da figura marcada (a) camada vermelha com $PSNR = 32.01dB$, (b) camada verde com $PSNR = 32.75dB$, (c) camada azul com $PSNR = 36.85dB$, (d) camada RGB com $PSNR = 33.41dB$, (e) camada de transparência com $PSNR = 33.95dB$ e (f) camada RGB com a camada adicional de transparência com $PSNR = 33.54dB$

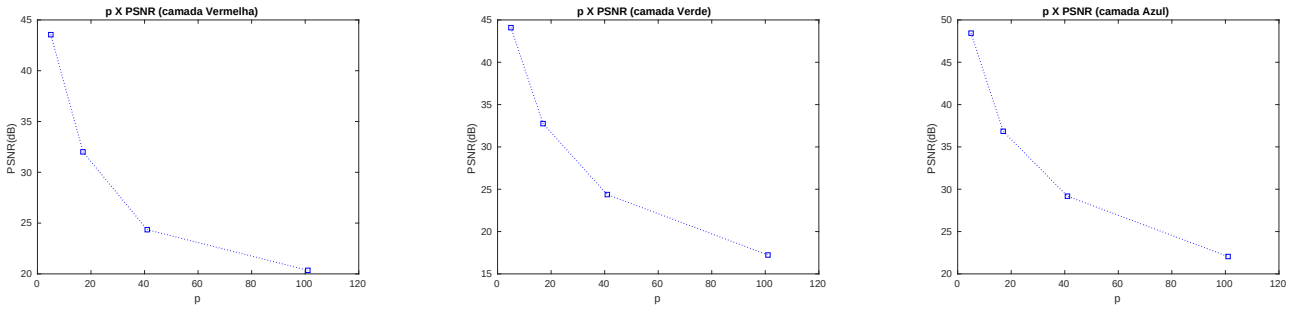
Na Figura 7, são apresentadas as camadas de cores correspondentes a imagem colorida, a camada de transparência e a figura RGB com a camada de transparência inserida, todas as figuras estão marcadas e foi calculado para cada camada de cor, camada RGB e camada de transparência o sinal-ruído de pico (PSNR) que quantifica o quanto a inserção da marca modifica a imagem original.



(a) (b) (c) (d)

Figura 8 – Imagens: (a) imagem original (600 $\times$ 800), (b) imagem marcada em $GF(5)$ (600 $\times$ 800), (c) imagem marcada em $GF(101)$ (600 $\times$ 800), e (d) marca d'água inserida (32 $\times$ 32).

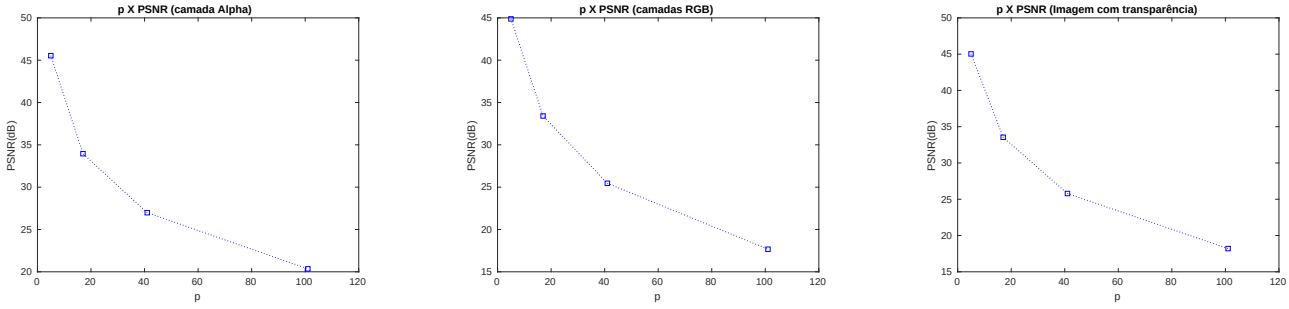
Na Figura 8 a imagem 8b foi marcada utilizando a $QFNT$ com $GF(5)$ o quaternion utilizado como núcleo foi $q = 1i+4j+3k$, a imagem 8c foi marcada com $GF(101)$ o quaternion utilizado como núcleo foi $q = 7 + 1i + 2j + 2k$, pode-se perceber visualmente que o aumento do p característico acarreta em distorções significativas da imagem marcada.



(a) (b) (c)

Figura 9 – Imagem original: camadas (a) vermelha, (b) verde e (c) azul.

Nas Figuras 9 e 10 temos os comportamentos do PSNR em relação ao p característico, para quatro escolhas de p, ou seja, $GF(5)$ cujo quaternion utilizado como núcleo da transformada foi $q = 1i + 4j + 3k$, $GF(17)$ cujo quaternion utilizado como núcleo da transformada foi $q = 1i+5j+3k$, $GF(41)$ cujo quaternion utilizado como núcleo da transformada foi $q = 9+4i+4k$ e $GF(101)$ cujo quaternion utilizado como núcleo da transformada foi $q = 7 + 1i + 2j + 2k$, todos os quaternions utilizados como núcleo da transformada obedecem as regras vistas no capítulo 4 desta tese, pode-se perceber com os gráficos das Figuras 9 e 10 que o PSNR dimunui com o aumento da característica p do corpo, limitando a aplicação desta transformada para produção de marca d'água frágeis para pequenos valores de p.



(a) (b) (c)

Figura 10 – Imagem original: camadas (a) vermelha, (b) verde e (c) azul.

5.2.1.4 Sistema de assinatura

A partir do modelo de marcação de imagens, esse modelo pode ser interpretado também como no artigo de Cintra et. al. (CINTRA et al., 2009) como um sistema de geração de assinatura, nesse contexto a assinatura é a imagem marcada e a extração da marca dessa imagem é a confirmação se houve ou não modificação na imagem original.

(a) (b)

Figura 11 – Imagens: (a) imagem (600 × 800) marcada com pixel de posição (100,100) alterado, (b) marca d'água extraida com o pixel da imagem marcada alterada na posição (100,100).

Para o caso apresentado na Figura 11 foi utilzado para o núcleo da transformada o quaternion $q = 1i + 4j + 3k$ que gera uma matriz de transformação de comprimento igual a 8, pode-se perceber que a alteração do pixel $(100, 100)$ não provocou alterações visuais na imagem marcada, porém foi possível identificar que a imagem sofreu alteração e em qual pixel a alteração foi realizada por meio da extração da marca d'água.

5.2.1.5 Inserção da marca-colorida-4bits

Da mesma maneira que a inserção da marca padrão-binária os números quaternionicos foram utilizados como ferramenta para o processamento da imagem, a imagem hospedeira foi a mesma utilizada para a marca binária, seguindo os primeiros passos descritos para iserção da marca binária a distinção entre a inserção da marca binária e a marca colorida de quatro bits utilizada nessa seção encontra-se na inserção da marca colorida no conteúdo espectral da imagem hospedeira, pois como a marca colorida possui quatro bits, cada bit dessa marca foi inserido em um coeficiente da matriz de quaternion da imagem hospedeira,

$$\hat{I}'q_R = \hat{I}q_R + Mcolor_q \ (mod\ p) \tag{5.8}$$

,

onde $\hat{I}'q_R$ é o conteúdo espectral de Iq_R que é o resíduo da imagem hospedeira na forma quaterniônica contendo $Mcolor_q$ que é a marca colorida na forma quaterniônica onde

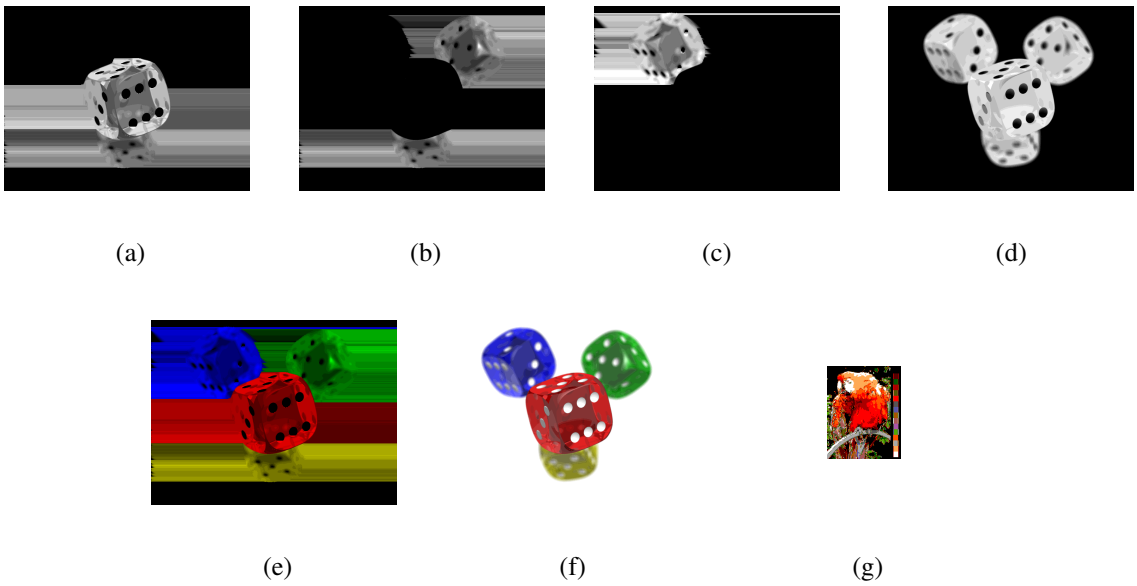
cada coeficiente dessa matriz de quaternion representa um bit da marca colorida original. Os procedimentos após essa fase segue identicos aos mencionados para marca padrão binária

5.2.1.6 Extração da marca-colorida-4bits

O processo de extração da marca colorida é idêntico ao da marca padrão binária, ressaltando o cuidado na reorganização dos bits da imagem colorida.

5.2.1.7 Simulações e resultados para marca colorida

Considerou-se a mesma imagem hospedeira utilizada para marca padrão binária, ou seja, de dimensões 600×800 pixels com extensão $.png$, e inicialmente a imagem não possuia nenhuma marca d'água. O passo seguinte foi inserir uma marca colorida de dimensões 200×160 pixels e de extensão $.png$, onde cada pixel é composto quatro bits.



(a) (b) (c) (d)

(e) (f) (g)

Figura 12 – Imagens: (a) camada vermelha, (b) camada verde, (c) camada azul, (d) camadas RGB juntas, (e) camada de transparência (f) camada RGB juntamente com a transparência e (g) marca a ser inserida

Na Figura 12a, 12b e 12c são apresentadas as camadas de cores correspondentes a imagem colorida com seu respectivo $PSNR$, camada vermelha com $PSNR = 32.01$, camada verde com $PSNR = 32.75$, camada azul com $PSNR = 36.85$ na Figura 12d a camada de transparência com $PSNR = 33.95$, na figura 12e as camadas RGB juntas com $PSNR = 33.41$ e na Figura 12f a imagem com a camada de transparência com $PSNR = 33.54$ e na Figura 12g a marca inserida na imagem hospedeira. O quaternion utilizado como núcleo da transformada envolvido no processo de marcação foi, $q = 4 + 3i + 3j + 10k$ com ordem multiplicativa igual a 16 e fixou-se $p = 17$. O processamento da imagem ocorreu dividindo-a em blocos de 32×32 pixels.

6 CONCLUSÕES E TRABALHOS FUTUROS

NESTE capítulo, são listadas de forma concisa as principais conclusões do trabalho que foi realizado até o momento e colocados pontos que se pretende investigar até a finalização da tese. Com relação às primeiras, podem ser declaradas de forma destacada as seguintes:

1. Condução de uma investigação relacionada aos quaternions generalizados, sobretudo, àqueles definidos sobre corpos finitos, identificando as propriedades existentes e estabelecendo alguns conceitos novos nesse contexto;
2. Definição, pela primeira vez na literatura, de uma transformada numérica de Fourier quaterniônica, a qual consiste, de alguma forma, numa versão definida sobre corpos finitos da QFT discreta;
3. Avaliação preliminar da aplicação de uma versão bidimensional da QFNT ao processamento digital de imagem e, em particular, ao cenário de cifragem de imagens.

Com relação aos trabalhos que se pretende desenvolver até a finalização da tese, podem ser destacados os seguintes:

1. Introdução de novas propriedades dos quaternions generalizados sobre corpos finitos;
2. Estabelecimento de outras propriedades da transformada numérica de Fourier quaterniônica e investigação mais detalhada das propriedades introduzidas;
3. Extensão mais criteriosa da QFNT ao caso bidimensional;
4. Definição de outros tipos de transformadas numéricas quaterniônicas, como a do cosseno, a do seno e a de Hartley;
5. Estudo com mais detalhes de aplicações para a QFNT, tanto no campo do processamento de imagem quanto no de processamento de sinais de modo geral.

O desenvolvimento dos pontos mencionados deve ser pautado pelo estudo do vasto material que já se tem à disposição (artigos em revista, artigos em eventos e livros) e pela continuidade da busca por temas preferencialmente recentes e com lacunas a serem preenchidas. Atualmente, encontra-se em elaboração um artigo que se pretende submeter a uma revista internacional. O trabalho consiste, essencialmente, num resumo do material apresentado no presente documento, tendo como focos a distinção entre os quaternions generalizados e os de Hamilton, que são bem mais conhecidos da comunidade científica interessante no tema, as proposições necessários à definição da QFNT, a definição propriamente dita dessa transformada,

o estabelecimento de suas principais propriedades e a sugestão de aplicações. Espera-se que o artigo possa estar pronto para submissão até o final do mês de Setembro do ano corrente.

REFERÊNCIAS

BACHMANN, F.; HIELSCHER, R.; SCHAEBEN, H. Texture analysis with mtex–free and open source software toolbox. In: TRANS TECH PUBL. **Solid State Phenomena**. [S.l.], 2010. v. 160, p. 63–68. Citado na página 14.

CAMPELLO DE SOUZA, R. M. et al. A transformada discreta do seno em um corpo finito. In: **Anais do XXVIII Congresso Nacional de Matemática Aplicada e Computacional**. [S.l.: s.n.], 2005. São Paulo, Brasil. Citado na página 14.

CAMPELLO DE SOUZA, R. M. et al. A transformada complexa de hartley em um corpo finito. Citado na página 14.

CAMPELLO DE SOUZA, R. M. et al. Trigonometry in finite fields and a new Hartley transform. In: **Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on**. [S.l.: s.n.], 1998. p. 293. Citado na página 18.

CAMPELLO DE SOUZA, R. M. et al. A transformada discreta do cosseno em um corpo finito. **Anais do XX Simpósio Brasileiro de Telecomunicaçoes, Rio de Janeiro, RJ**, 2003. Citado na página 14.

CHEDDAD, A. et al. Digital image steganography: Survey and analysis of current methods. **Signal processing**, Elsevier, v. 90, n. 3, p. 727–752, 2010. Citado na página 13.

CIGLIOLA, A. Split quaternions, generalized quaternions and integer-valued polynomials. Citado na página 30.

CINTRA, R. J. et al. Fragile watermarking using finite field trigonometrical transforms. **Signal Processing: Image Communication**, v. 24, p. 587–597, Aug 2009. Citado 4 vezes nas páginas 13, 18, 67 e 71.

DESCARTES, R. **Discours de la méthode pour bien conduire la raison, et chercher la verité dans les sciences**. [S.l.]: Leiden, Holanda, 1637. Citado na página 24.

ELL, T. A. Hypercomplex spectral transformations. University of Minnesota, 1992. Citado na página 15.

ELL, T. A. Quaternion-fourier transforms for analysis of two-dimensional linear time-invariant partial differential systems. In: IEEE. **Decision and Control, 1993., Proceedings of the 32nd IEEE Conference on**. [S.l.], 1993. p. 1830–1841. Citado 2 vezes nas páginas 13 e 15.

ELL, T. A.; SANGWINE, S. J. Hypercomplex fourier transforms of color images. **IEEE Transactions on image processing**, IEEE, v. 16, n. 1, p. 22–35, 2007. Citado 6 vezes nas páginas 13, 14, 15, 26, 28 e 43.

FLETCHER, P. et al. Hypercomplex signal processing. In: **Signal processing**. [S.l.]: Elsevier, 2017. v. 136, p. 1–106. Citado na página 15.

HAMILTON, W. R. Theory of conjugate functions, or algebraic couples; with a preliminary and elementary essay on algebra as the science of pure time. **Transactions of the Royal Irish Academy**, v. 17, n. part 1, p. 293–422, 1837. Citado na página 25.

HAMILTON, W. R. **The Mathematical Papers of Sir William Rowan Hamilton**. [S.l.]: CUP Archive, 2000. Citado na página 26.

JÚNIOR, U. P. A história dos números complexos: das quantidades sofisticadas de cardano às linhas orientadas de argand. 2009. Citado na página 25.

KAK, S. The number theoretic hilbert transform. **Circuits, Systems, and Signal Processing**, Springer, v. 33, n. 8, p. 2539–2548, 2014. Citado na página 14.

LAM, T.-Y. **Introduction to quadratic forms over fields**. [S.l.]: American Mathematical Soc., 2005. v. 67. Citado na página 28.

LEWIS, D. W. Quaternion algebras and the algebraic legacy of hamilton's quaternions. **Irish Math. Soc. Bull**, v. 57, p. 41–64, 2006. Citado na página 30.

LIMA, J. B. Fast algorithm for computing cosine number transform. **Electronics Letters**, v. 51, n. 20, p. 1570–1572, Oct 2015. ISSN 0013-5194. Citado na página 14.

LIMA, J. B.; BARONE, M.; CAMPELLO DESOUZA, R. M. Cosine transforms over fields of characteristic 2. **Finite Fields and Their Applications**, Elsevier, v. 37, p. 265–284, 2016. Citado na página 14.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Uma marca d'água digital baseada na transformada do cosseno sobre corpos finitos. **Anais do XXII Simpósio Brasileiro de Telecomunicações**, 2005. Citado na página 13.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Fractional cosine and sine transforms over finite fields. **Linear Algebra and its Applications**, v. 438, n. 8, p. 3217 – 3230, 2013. ISSN 0024-3795. Citado na página 14.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. On the summation of fractional powers of matrices over finite fields. **OPERATORS AND MATRICES**, ELEMENT R AUSTRIJE 11, 10000 ZAGREB, CROATIA, v. 10, n. 1, p. 209–221, 2016. Citado na página 14.

LIMA, J. B.; LIMA, E.; MADEIRO, F. Image encryption based on the finite field cosine transform. **Signal Processing: Image Communication**, Elsevier, v. 28, n. 10, p. 1537–1547, 2013. Citado na página 18.

LIMA, J. B.; MADEIRO, F.; SALES, F. J. R. Encryption of medical images based on the cosine number transform. **Signal Processing: Image Communication**, Elsevier BV, v. 35, p. 1–8, Jul 2015. Citado na página 14.

LIMA, J. B.; NOVAES, L. Image encryption based on the fractional fourier transform over finite fields. **Signal Processing**, Elsevier, v. 94, p. 521–530, 2014. Citado 2 vezes nas páginas 13 e 18.

LUO, W.; HEILEMAN, G. L.; PIZANO, C. E. A fast and robust watermarking method for jpeg images. **Computer modeling & new Technologies**, p. 39–47, 2004. Citado na página 66.

MA, X. et al. Color image watermarking using local quaternion fourier spectral analysis. In: IEEE. **2008 IEEE International Conference on Multimedia and Expo (ICME)**. [S.l.], 2008. p. 233–236. Citado na página 66.

MINEMOTO, T. et al. Feed forward neural network with random quaternionic neurons. **Signal Processing**, Elsevier, v. 136, p. 59–68, 2017. Citado na página 14.

MUKUNDAN, R. Quaternions: From classical mechanics to computer graphics, and beyond. In: **Proceedings of the 7th Asian Technology conference in Mathematics**. [S.l.: s.n.], 2002. p. 97–105. Citado na página 14.

NASCIMENTO, M. L. F. Amigo imaginário: a raiz quadrada de-1 tem uma história que pode ser dita complexa. Instituto Ciência Hoje, 2016. Citado na página 24.

NEVES, R. C.; GRIMBERG, G. E. **Os quatérnios de Hamilton e o Espaço**. Tese (Doutorado) — Dissertação de Mestrado, 2008. Citado na página 24.

NIKOLAIDIS, N.; PITAS, I. Robust image watermarking in the spatial domain. **Signal processing**, Elsevier, v. 66, n. 3, p. 385–403, 1998. Citado na página 66.

ORTOLANI, F. et al. Frequency domain quaternion adaptive filters: Algorithms and convergence performance. **Signal Processing**, Elsevier, v. 136, p. 69–80, 2017. Citado na página 14.

PEDROUZO-ULLOA, A.; TRONCOSO-PASTORIZA, J. R.; PÉFEZ-GONZÁLEZ, F. Number theoretic transforms for secure signal processing. **IEEE Transactions on Information Forensics and Security**, v. 12, n. 5, p. 1125–1140, May 2017. ISSN 1556-6013. Citado na página 13.

PERVIN, E.; WEBB, J. A. Quaternions in computer vision and robotics. 1982. Citado na página 14.

POLLARD, J. M. The fast Fourier transform in a finite field. **Mathematics of Computation**, American Mathematical Society (AMS), v. 25, n. 114, p. 365–365, May 1971. Citado 2 vezes nas páginas 13 e 14.

REED, I.; TRUONG, T.-K. The use of finite fields to compute convolutions. **IEEE Transactions on Information Theory**, IEEE, v. 21, n. 2, p. 208–213, 1975. Citado na página 13.

RZADKOWSKI WOJCIECHAND SNOPEK, K. A new quaternion color image watermarking algorithm. In: IEEE. **Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on**. [S.l.], 2015. v. 1, p. 245–250. Citado na página 66.

SANGWINE, S. J. Fourier transforms of colour images using quaternion or hypercomplex, numbers. **Electronics letters**, IET, v. 32, n. 21, p. 1979–1980, 1996. Citado 2 vezes nas páginas 14 e 15.

SANGWINE, S. J. Colour image edge detector based on quaternion convolution. **Electronics Letters**, IET, v. 34, n. 10, p. 969–971, 1998. Citado na página 14.

SANGWINE, S. J.; ELL, T. Hypercomplex auto-and cross-correlation of color images. In: IEEE. **Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on**. [S.l.], 1999. v. 4, p. 319–322. Citado na página 26.

SANGWINE, S. J.; ELL, T. A. Colour image filters based on hypercomplex convolution. **IEE Proceedings-Vision, Image and Signal Processing**, IET, v. 147, n. 2, p. 89–93, 2000. Citado 2 vezes nas páginas 14 e 26.

SANGWINE, S. J. et al. The discrete fourier transform of a colour image. **Image Processing II Mathematical Methods, Algorithms and Applications**, Chichester, UK, p. 430–441, 2000. Citado na página 15.

SCHAFER, A. V. .; OPPENHEIM, R. W. **Discrete-time Signal Processing, 3rd**. [S.l.]: Prentice Hall, 1999. ISBN 8131704920. Citado na página 13.

SHU, W.; TIANREN, Y. Algorithm for linear convolution using number theoretic transforms. **Electronics Letters**, IET, v. 24, n. 5, p. 249–250, 1988. Citado na página 13.

SILVA, D.; CAMPELLO DE SOUZA, R. M.; OLIVEIRA, H. M. D. Transformadas em corpos finitos e grupos de inteiros gaussianos. In: **XIX Simpó sio Brasileiro de Telecomunicac-oes (Brazilian Symposium on Telecommunications), Fortaleza, Brazil**. [S.l.: s.n.], 2001. Citado na página 18.

VERMA, V. S.; JHA, R. K.; OJHA, A. Digital watermark extraction using support vector machine with principal component analysis based feature reduction. **Journal of Visual Communication and Image Representation**, Elsevier, v. 31, p. 75–85, 2015. Citado na página 66.

VOIGHT, J. The arithmetic of quaternion algebras. **preprint**, 2014. Citado na página 30.

WESSEL, C. **Essai sur la représentation analytique de la direction**. [S.l.]: Bianco Luno (F. Dreyer), imprimeur, 1797. Citado na página 24.