

The Quaternion Fourier Number Transform

Luiz C. da Silva Jr.¹ · Juliano B. Lima¹

Received: 20 December 2017 / Revised: 18 April 2018 / Accepted: 23 April 2018 /
Published online: 4 May 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract In this paper, we introduce the quaternion Fourier number transform (QFNT), which corresponds to a quaternionic version of the well-known number-theoretic transform. We derive several theoretical results necessary to define the QFNT and investigate its main properties. Differently from other quaternion transforms, which are defined over Hamilton's quaternions, the QFNT requires considering a quaternion algebra over a finite field. Thus, its computation involves integer arithmetic only, avoiding truncation and rounding-off errors. We give an illustrative example regarding the application of the QFNT to digital color image processing.

Keywords Number-theoretic transform · Quaternion Fourier transform · Generalized quaternions · Image processing

1 Introduction

Number-theoretic transforms (NTT) have been widely investigated and employed in several application scenarios. In the 1970s, such transforms were presented as an alternative way for efficiently computing error-free convolutions [35,36,39,41]. At that time, this possibility was of fundamental importance, since the available hardware could only work with finite precision arithmetic. In recent years, NTT have been used mainly in scenarios related to information security, which include, for instance, image encryption, watermarking and signal processing in the encrypted domain [6,25,31,40].

✉ Juliano B. Lima
juliano_bandeira@ieee.org

Luiz C. da Silva Jr.
luiz.carlosj@ufrpe.br

¹ Department of Electronics and Systems, Federal University of Pernambuco, Recife, Brazil

Usually, an NTT is defined as a Fourier-like transform, where the complex N th root of unity used as the discrete Fourier transform (DFT) kernel is replaced by an N th root of unity in a finite algebraic structure [4]. However, other types of NTT have been defined; we could mention, for example, cosine, sine, wavelet and Hilbert number transforms, which are, in some sense, analogous to complex- and real-valued discrete transforms with the corresponding nomenclature [11, 17, 24]. Generalizations of NTT have also been proposed; they include, for example, fractional number-theoretic transforms, which are analogous to complex-valued fractional Fourier transforms [42–44] and consist in computing a rational power of the corresponding ordinary NTT matrix operator [22, 26, 33].

In this paper, we introduce a quaternion NTT, which is referred to as quaternion Fourier number transform (QFNT). The definition of the QFNT is motivated by the increasing interest in mathematical tools and applications related to hypercomplex signal processing; in recent works, one has been proposed other new quaternion transforms [12, 38], algorithms concerning quaternion adaptive filters in the frequency domain [30], neural networks with quaternionic neurons [18, 28] and several quaternion-based techniques for color image processing [3, 20, 21, 45], just to mention a few.

The QFNT is a kind of number-theoretic counterpart of the (discrete) quaternion Fourier transform (QFT) [9, 10]. However, in order to obtain a consistent definition, several peculiarities of the algebraic structures where one desires to establish the transform have to be considered. In particular, instead of considering Hamilton quaternions, one has to consider generalized quaternions [19, 34]. We had to develop some new results regarding generalized quaternions over finite fields, such as those related to the multiplicative order of these numbers; these results have direct connection with the existence and the invertibility of the QFNT. At any case, as we demonstrate throughout the paper, some properties of the new transform are, in some sense, equivalent to those of the QFT.

Differently from the QFT, the computation of the QFNT requires modular arithmetic only. This allows to apply this transform to a digital image, for example, without the need of dealing with non-integer numbers and, consequently, avoiding rounding-off. Depending on the field where the QFNT is established, it may still be possible to perform the multiplications necessary to its calculation by means of additions and bit-shift operations [4]; this makes the new transform attractive under the aspect of computational complexity, when compared to the QFT, and suggests that the algebraic structure where it is defined can be used as a surrogate field to perform error-free hypercomplex signal processing. Although this paper is focused on the definition of the QFNT and the investigation of its main properties, we compute, with an illustrative purpose, the QFNT of color images. Preliminary experiments suggest that the QFNT can be used to hide the statistical behavior of an image. This result is interesting from the cryptographic point of view and could not be achieved by using a QFT based on Hamilton quaternions.

This paper is organized as follows. In Sect. 2, we review some important concepts related to quaternions and ordinary number-theoretic transforms; in particular, we give a notion of what the Euler's formula for quaternions over a finite field should be. The quaternion Fourier number transform is defined in Sect. 3, and its properties are given

in Sect. 4. In Sect. 5, we describe some potential applications for the QFNT; we explain how to compute the QFNT of a color image and provide some simulation results. The main concluding remarks of the paper are given in Sect. 6.

2 Generalized Quaternions

In general, given a field \mathbb{F} , whose characteristic is different from 2, and $\alpha, \beta \in \mathbb{F}$, one can define a quaternion algebra denoted by $\mathcal{A} = \left(\frac{\alpha, \beta}{\mathbb{F}}\right)$, where the parameters i and j are generators satisfying

$$i^2 = \alpha, \quad j^2 = \beta, \quad ij = -ji. \tag{1}$$

One also defines $k := ij \in \mathcal{A}$, such that $k^2 = (ij)(ij) = -i^2j^2 = -\alpha\beta \in \mathbb{F}$, and $ik = -ki = \alpha j, kj = -jk = \beta i$. Consequently, the elements i, j, k are anticommutative. If $\mathbb{F} = \mathbb{R}$ and $\alpha = \beta = -1$, the algebra $\left(\frac{-1, -1}{\mathbb{R}}\right)$ corresponds to (usual) Hamilton’s quaternions, which are denoted by \mathcal{H} . An algebra $\left(\frac{\alpha, \beta}{\mathbb{F}}\right)$ over \mathbb{F} is a direct generalization of \mathcal{H} [19,34].

It can be shown that the set $\{1, i, j, k\}$ is a \mathbb{F} -basis for \mathcal{A} and, therefore, $\dim_{\mathbb{F}} \mathcal{A} = 4$. Additionally, if \mathbb{F} is a finite field, differently from \mathcal{H} , which is a division ring, $\left(\frac{\alpha, \beta}{\mathbb{F}}\right)$ is isomorphic to $M_2(\mathbb{F})$, an algebra of 2×2 matrices whose entries lie in \mathbb{F} [19,34]. This is related to the fact that, even if $q \in \left(\frac{\alpha, \beta}{\mathbb{F}}\right)$ and $q \neq 0$, the norm $N(q)$ of q may equal zero. More precisely, if $q = a + bi + cj + d$ and its conjugate is given by $q^* = a - bi - cj - d$, one may define its norm as the map $\mathcal{N} : \left(\frac{\alpha, \beta}{\mathbb{F}}\right) \rightarrow \mathbb{F}$ such that $\mathcal{N}(q) = q^*q$. Since

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

if \mathbb{F} is a finite field, $N(q) = 0$ does not imply $q = 0$. From this point forward, we consider the case in which $\mathbb{F} = \mathbb{F}_p$ is a prime finite field and $\alpha = \beta = -1 \equiv p - 1 \pmod{p}$. The mentioned isomorphism can then be explicated by mapping, for instance, i to

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

and j to

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

Consequently, $k := ij = ji$ is mapped to

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

and $q = a + bi + cj + dk$ is mapped to

$$\mathbf{Q} = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix}. \tag{2}$$

We identify \mathbf{Q} in (2) as the matrix form of the generalized quaternion q . Such a matrix form is considered in several developments made in future sections of this paper. As we will show, this makes easier to demonstrate some theoretical results.

It is interesting to note that, although $\left(\frac{\alpha, \beta}{\mathbb{F}_p}\right)$ is isomorphic to $M_2(\mathbb{F}_p)$, if one writes \mathbf{Q} as in (2) and $p \equiv 3 \pmod{4}$, the elements of such a matrix will lie in a structure isomorphic to \mathbb{F}_{p^2} , since i will be a quadratic nonresidue over \mathbb{F}_p [5]. More precisely, the elements of \mathbf{Q} can be viewed as Gaussian integers over \mathbb{F}_p for $i^2 = \alpha \equiv p - 1 \pmod{p}$. The general definition of these numbers is given as follows [7, 24].

Definition 1 The set of Gaussian integers over \mathbb{F}_p is the set $\mathbb{I}_p := \{c + di, c, d \in \mathbb{F}_p\}$, where i^2 is a quadratic nonresidue over \mathbb{F}_p .

The elements $\zeta = c + di$ of the “complex” structure \mathbb{I}_p have a “real” part $c = \Re\{\zeta\}$ and an “imaginary” part $d = \Im\{\zeta\}$. In fact, if $p \equiv 3 \pmod{4}$ and $i^2 = \alpha \equiv p - 1 \pmod{p}$, it is possible to establish some interesting analogies between elements of \mathbb{I}_p and usual complex numbers [7, 24]. On the other hand, if $p \equiv 1 \pmod{4}$, $-1 \equiv p - 1 \pmod{p}$ is a quadratic residue over \mathbb{F}_p and another i has to be selected if one desires elements $c + di$ to remain “complex.” Extending this terminology, a generalized quaternion $q = a + bi + cj + dk$ over \mathbb{F}_p can be viewed as a “hypercomplex” number, whose “real” part is $\Re\{q\} = a$ and “imaginary” part is $\Im\{q\} = bi + cj + dk$. Since the latter has three components, it can also be referred to as the *vector* part of q , while the former can be referred to as its scalar part [9].

Apparently, operations and properties specifically related to quaternions over finite fields have not been clearly addressed in the literature. At any case, some of these operations and properties are mere extensions of what one has for Hamilton’s quaternions. This includes, for example, addition and products among quaternions, which can be carried out in a standard way, but considering the use of the appropriate modular arithmetic when adding, multiplying or taking the additive symmetric of elements lying in \mathbb{F}_p . Naturally, we also have to take into account the fact that α and β do not necessarily equal -1 .

If $a = 0$, so that $q = bi + cj + d$, q is a pure quaternion over \mathbb{F}_p . The modulus of a generalized quaternion is given by $|q| = \sqrt{\mathcal{N}(q)} = \sqrt{q^*q}$. A quaternion q over \mathbb{F}_p is unitary if $|q| = 1$. If $|q| \neq 0$, its inverse exists, being given by

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

and satisfying $qq^{-1} = q^{-1}q = 1$. In the last equation, the term $\frac{1}{|q|^2} = (|q|^2)^{-1}$ is the multiplicative inverse of $|q|^2$ modulo p . The symbol “(mod p)” is omitted in order to simplify the notation. The operations and properties related to quaternions over \mathbb{F}_p can also be carried out and verified by considering the matrix form of q .

The extension of the Euler's formula to the case of quaternions over \mathbb{F}_p should require more creativity, when compared to the analogies mentioned above. Basically, what is expected is to be able to identify a quaternion over \mathbb{F}_p employing its norm and the arc associated with this element or, more specifically, the cosine and sine functions related to this arc. We believe that such functions can be defined borrowing notions of trigonometry over field fields [7, 24]. Thus, fixing a generalized quaternion q and a pure unitary quaternion μ over \mathbb{F}_p , the cosine and the sine of the arc related to q^x would be computed modulo p , respectively, as

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

and

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

where $x = 0, 1, \dots, \text{ord}(q)$ and $\text{ord}(q)$ denotes the multiplicative order of q , i. e., the least positive integer such that $q^{\text{ord}(q)} = 1$; several aspects related to the multiplicative order of a quaternion over \mathbb{F}_p are discussed in the next section. Thus, one would have

$$q^x = \cos_q(x) + \mu \sin_q(x).$$

At this moment, such definitions are only speculations, which may be clarified in a future work. Such a clarification should elucidate, for instance, which criteria have to be used to choose μ and which other properties may come from the restriction of q being unitary. At any case, we suppose that the establishment of cosines and sines associated with generalized quaternions over \mathbb{F}_p gives support to the definition of a whole trigonometry in this scenario, allowing the definition of transforms similar to those introduced in [24].

2.1 The Fourier Number Transform

The ordinary Fourier number transform (FNT) is defined as follows [4].

Definition 2 Let $\omega \in \mathbb{F}_p$ be an element of multiplicative order $\text{ord}(\omega) = N$. The Fourier number transform of the vector $\mathbf{x} = (x(n)) \in \mathbb{F}_p^N$ is the vector $\mathbf{X} = (X(r)) \in \mathbb{F}_p^N$ with components given by

$$X(r) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\omega^{rn}. \quad (3)$$

The invertibility of the FNT is provided by the following lemma.

Lemma 1 An element $\omega \in \mathbb{F}_p$ of multiplicative order $\text{ord}(\omega) = N$ satisfies

$$\sum_{m=0}^{N-1} \omega^{rm} = \begin{cases} N, & \text{if } r \equiv 0 \pmod{N}, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Proof The expression given in Lemma 1 is trivially true when $r \equiv 0 \pmod{N}$ since each term on the summation is unity. Otherwise, we use the relation

$$\left(\sum_{m=0}^{N-1} \omega^{rm} \right) (1 - \omega^r) = 1 - \omega^{Nr} = 0,$$

from which (4) follows since $(1 - \omega^r) \neq 0$. □

Using Lemma 1, it can be shown that the components of a vector \mathbf{x} can be recovered from the components of its FNT as

$$x(n) = \frac{1}{\sqrt{N}} \sum_{r=0}^{N-1} X(r)\omega^{-rn}.$$

3 The Quaternion Fourier Number Transform

3.1 Multiplicative Order of Generalized Quaternions

In this section, we derive some results regarding the multiplicative order of generalized quaternions over \mathbb{F}_p . This plays an important role in the demonstration of the invertibility of the quaternion Fourier number transform. We consider the matrix form \mathbf{Q} in (2) of $q \in \left(\frac{-1, -1}{\mathbb{F}_p} \right)$. The multiplicative order of \mathbf{Q} , which obviously coincides with that of q , is the least positive integer $\text{ord}(\mathbf{Q})$ such that $\mathbf{Q}^{\text{ord}(\mathbf{Q})} = \mathbf{I}$, where \mathbf{I} is the 2×2 identity matrix. We start by computing the characteristic polynomial of \mathbf{Q} as

$$r_{\mathbf{Q}}(\lambda) = \det(\mathbf{Q} - \lambda\mathbf{I}) \tag{5}$$

$$= \lambda^2 - 2a\lambda + a^2 + b^2 + c^2 + d^2. \tag{6}$$

The roots of $r_{\mathbf{Q}}(\lambda)$, which correspond to the eigenvalues of \mathbf{Q} , are then given by

$$\lambda_1 = a + \sqrt{-b^2 - c^2 - d^2} \tag{7}$$

and

$$\lambda_2 = a - \sqrt{-b^2 - c^2 - d^2}. \tag{8}$$

Excluding the cases where at least one eigenvalue is zero (\mathbf{Q} would not be invertible and, therefore, its multiplicative order would not be defined) and assuming that $p \equiv 3 \pmod{4}$, the following cases have to be considered.

- Case 1: $b^2 + c^2 + d^2 = 0$. In this case, one has $\lambda_1 = \lambda_2 = a \in \mathbb{F}_p$. The following subcases have to be considered.
 - Subcase 1.1: $b = 0$ or $c = 0$ or $d = 0$. The condition determining the current subcase together with the condition determining case 1 implies $b = c = d = 0$. Thus, \mathbf{Q} reduces to a matrix in the form

$$\mathbf{Q} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \tag{9}$$

and, therefore, one has $\text{ord}(\mathbf{Q}) = \text{ord}(a)$.

- Subcase 1.2: $b \neq 0$ or $c \neq 0$ or $d \neq 0$. The condition determining the current subcase together with the condition determining case 1 implies $b \neq 0, c \neq 0$ and $d \neq 0$. Thus, denoting by $\mathbf{v} = [v(0) \ v(1)]$ an eigenvector of \mathbf{Q} , one may write $\mathbf{Q}\mathbf{v}^T = a\mathbf{v}^T$, which produces the system of equations

$$\begin{cases} biv(0) + (c + di)v(1) = 0 \\ (-c + di)v(0) - biv(1) = 0. \end{cases} \tag{10}$$

From (10), one obtains the relationship

$$v(0) = \frac{bi}{-c + di}v(1), \tag{11}$$

which indicates that the geometric multiplicity of $\lambda_1 = \lambda_2 = a$ is $m_g(a) = 1$. Therefore, \mathbf{Q} is not diagonalizable and admits the Jordan normal form [37]

$$\mathbf{J}_\mathbf{Q} = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}. \tag{12}$$

Computing $\mathbf{J}_\mathbf{Q}^m$, for $m = 2, 3, 4, \dots$, one observes that, in general, one has

$$\mathbf{J}_\mathbf{Q}^m = \begin{bmatrix} a^m & ma^{m-1} \\ 0 & a^m \end{bmatrix}. \tag{13}$$

Therefore, $\mathbf{J}_\mathbf{Q}^m = \mathbf{I}$ only if $a^m \equiv 1 \pmod{p}$, that is, if m is a multiple of $\text{ord}(a)$, and if $ma^{m-1} \equiv 0 \pmod{p}$, that is, if $m \equiv 0 \pmod{p}$. Thus, $\text{ord}(\mathbf{Q}) = \text{ord}(\mathbf{J}_\mathbf{Q}) = \text{lcm}(\text{ord}(a), p)$.

- Case 2: $b^2 + c^2 + d^2 \neq 0$. In this case, \mathbf{Q} has two distinct eigenvalues and admits the diagonal form

$$\Lambda_\mathbf{Q} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}. \tag{14}$$

Thus, $\text{ord}(\mathbf{Q}) = \text{ord}(\Lambda_\mathbf{Q}) = \text{lcm}(\lambda_1, \lambda_2)$.

Cases 1 and 2 just analyzed support the following lemma.

Lemma 2 A generalized quaternion $q = a + bi + cj + dk$ over \mathbb{F}_p , with associated matrix \mathbf{Q} in the form given in (2) and multiplicative order $\text{ord}(q) = \text{ord}(\mathbf{Q}) = N$, satisfies

$$\sum_{m=0}^{N-1} q^{rm} = \begin{cases} N, & N \not\equiv 0 \pmod{p}, \text{ if } r \equiv 0 \pmod{N}, \\ 0, & \text{otherwise,} \end{cases} \tag{15}$$

if, and only if

- (i) $a \neq 0$ and $b = c = d = 0$, or
- (ii) $b^2 + c^2 + d^2 \neq 0$ and $\text{ord}(a \pm \sqrt{-b^2 - c^2 - d^2}) = N$.

Proof Let $S_N(r) = \sum_{m=0}^{N-1} \mathbf{Q}^{rm}$. If condition (i) is met, \mathbf{Q} is of the type analyzed in subcase 1.1 (see the first part of this section), that is, $\text{ord}(\mathbf{Q}) = N = \text{ord}(a)$. Therefore, $N|(p - 1)$; if condition (ii) is met, \mathbf{Q} is of the type analyzed in case 2, with distinct eigenvalues having the same order. Therefore, $N|(p^2 - 1)$. Thus, if \mathbf{Q} satisfies (i) or (ii), one has $\text{ord}(\mathbf{Q}) = N \not\equiv 0 \pmod{p}$, and, therefore,

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

and $\sum_{m=0}^{N-1} q^{rm} = N$. For $r \not\equiv 0 \pmod{N}$, considering Lemma 1, if \mathbf{Q} satisfies (i), one has

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

and, if \mathbf{Q} satisfies (ii), one has

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

which means $\sum_{m=0}^{N-1} q^{rm} = 0$; the eigenvalues of \mathbf{Q} are $\lambda_1 = a + \sqrt{-b^2 - c^2 - d^2}$ and $\lambda_2 = a - \sqrt{-b^2 - c^2 - d^2}$, and \mathbf{V} is a matrix whose columns are the corresponding eigenvectors.

On the other hand, if \mathbf{Q} does not satisfy (i) or (ii), it falls in subcase 1.2 or in case 2, with eigenvalues having distinct multiplicative orders. If \mathbf{Q} is as in subcase 1.2, one has $N = \text{ord}(\mathbf{Q})|p$ and, therefore, $S_N(0) = \mathbf{0}$ and $\sum_{m=0}^{N-1} q^{rm} = 0$; this violates what is established in the first part of (15). If \mathbf{Q} is as in case 2, with $\text{ord}(\lambda_1) \neq \text{ord}(\lambda_2)$, one may assume, without loss of generality, that $\text{ord}(\lambda_1) < \text{ord}(\lambda_2) \leq \text{ord}(\mathbf{Q}) = N$. Thus, one has

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

and $\sum_{m=0}^{N-1} q^{rm} = 0$, which violates what is established in the second part of (15).

If $p \equiv 1 \pmod{4}$, similar conclusions are obtained for cases 1 and 2 analyzed in the first part of this section. Details regarding this possibility are shown in Appendix. At any rate, Lemma 2 remains valid.

3.2 Definition of the QFNT

In what follows, we introduce a definition for the quaternion Fourier number transform and determine the respective inverse transform. The transform corresponds to a finite field counterpart of the discrete quaternion Fourier transform [9,10]. However, the establishment of the QFNT depends on the development carried out in Sect. 3.1; in particular, its invertibility depends on conditions given in Lemma 2, which are completely dissociated from the requirements for inverting the Fourier transform over Hamilton’s quaternions.

Definition 3 Let q be a generalized quaternion over \mathbb{F}_p , which has multiplicative order $\text{ord}(q) = N$ and satisfies conditions (15). The (right) quaternion Fourier number transform of a vector $\mathbf{x} = (x(n))$, $n = 0, 1, \dots, N - 1$, whose components are generalized quaternions over \mathbb{F}_p , is the vector $\mathbf{X}^R = (X^R(r))$, $r = 0, 1, \dots, N - 1$, with components lying in the same structure and given by

$$X^R(r) = \sum_{n=0}^{N-1} x(n)q^{rn}. \tag{16}$$

Theorem 1 Let q be a generalized quaternion over \mathbb{F}_p , which has multiplicative order $\text{ord}(q) = N$ and satisfies conditions (15). The inverse (right) quaternion Fourier number transform of a vector $\mathbf{X}^R = (X^R(r))$, $r = 0, 1, \dots, N - 1$, whose components are generalized quaternions over \mathbb{F}_p , is the vector $\mathbf{x} = (x(n))$, $n = 0, 1, \dots, N - 1$, with components lying in the same structure and given by

$$x(n) = \frac{1}{N} \sum_{r=0}^{N-1} X^R(r)q^{-rn}. \tag{17}$$

Proof In (17), we replace $X^R(r)$ by (16) with n changed to m and obtain

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

According to Lemma 1, if $m \neq n$ in the first summation of the last equation, the second summation in the same equation gives zero; on the other hand, if $m = n$, the second summation gives N . Therefore, the last equation reduces to

$$x(n) = \frac{1}{N} x(n) N = x(n).$$

A right QFNT pair is denoted by

$$\mathbf{x} \overset{\text{QFNT}^R}{\longleftrightarrow} \mathbf{X}^R.$$

A left QFNT can also be defined, if the positions of the transform kernel and the vector component are permuted in (16) and (17). In this case, the QFNT vector would be denoted by $\mathbf{X}^L = (X^L(r)), r = 0, 1, \dots, N - 1$ and the QFNT pair would be denoted by

$$\mathbf{x} \overset{\text{QFNT}^L}{\longleftrightarrow} \mathbf{X}^L.$$

4 Properties of the QFNT

In this section, we develop some properties of the quaternion Fourier number transform. Similarly to what happens with the ordinary Fourier number transform with respect to the discrete Fourier transform, such properties hold some analogy with those of the quaternion discrete Fourier transform. In this sense, we highlight the cyclic convolution property, which allows us to suppose that, also in the quaternionic context, it is possible to perform filtering in the transform domain employing modular arithmetic operations only, conveniently adapted to generalized quaternions over finite fields.

4.1 Linearity

If

$$\mathbf{x}_1 \overset{\text{QFNT}^R}{\longleftrightarrow} \mathbf{X}_1$$

and

$$\mathbf{x}_2 \overset{\text{QFNT}^R}{\longleftrightarrow} \mathbf{X}_2,$$

then

$$c_1 \mathbf{x}_1 + c_2 \overset{\text{QFNT}^R}{\longleftrightarrow} c_1 \mathbf{X}_1 + c_2 \mathbf{X}_2,$$

$c_1, c_2 \in \mathbb{F}_p$. The demonstration of this result is trivial, being omitted in this work.

4.2 Cyclic Convolution

With the purpose of developing the QFNT cyclic convolution property, one considers the right definition of this transform. Additionally, in what follows, the indices of all vector components are taken modulo N . The result of the N -point cyclic convolution between $\mathbf{x} = (x(n))$ and $\mathbf{h} = (h(n))$ is denoted by $\mathbf{y} = \mathbf{x} \circ_N \mathbf{h}$, $\mathbf{y} = (y(n))$, $n = 0, 1, \dots, N - 1$, and given by

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

We remark that, due to the noncommutativity of the product between the components of \mathbf{x} and \mathbf{h} , the last equation corresponds to a kind of right convolution; a left convolution could also be considered. The cyclic convolution property is given in the following theorem.

Theorem 2 *Let $\mathbf{x} = (x(n))$ and $\mathbf{h} = (h(n))$, $n = 0, 1, \dots, N - 1$, be vectors whose components are generalized quaternions over \mathbb{F}_p . The QFNT of the N -point cyclic convolution \mathbf{y} between \mathbf{x} and \mathbf{h} is given by*

$$Y^R(k) = H^R(r)X_a^R(r) + iH^R(r)X_b^R(r) + jH^R(r)X_c^R(r) + kH^R(r)X_d^R(r). \quad (18)$$

Proof Using the QFNT definition, one may write

$$Y^R(r) = \sum_{n=0}^{N-1} [x \circ_N h(n)] q^{rn} = \sum_{n=0}^{N-1} \left[\sum_{m=0}^{N-1} x(n - m)h(m) \right] q^{rn}. \quad (19)$$

In the last equation, using the substitution $n' = n - m$, one obtains

$$Y^R(r) = \sum_{n'=0}^{N-1} \left[\sum_{m=0}^{N-1} x(n')h(m) \right] q^{r(n'+m)} \quad (20)$$

$$= \sum_{n'=0}^{N-1} x(n') \left[\sum_{m=0}^{N-1} h(m)q^{rm} \right] q^{rn'} \quad (21)$$

$$= \sum_{n'=0}^{N-1} x(n')H^R(r)q^{rn'}. \quad (22)$$

Writing $x(n') = x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k$, the last equation becomes

$$Y^R(r) = \sum_{n'=0}^{N-1} [x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k] H^R(r) q^{rn'} \tag{23}$$

$$= H^R(r) \sum_{n'=0}^{N-1} x_a(n') q^{rn'} + i H^R(r) \sum_{n'=0}^{N-1} x_b(n') q^{rn'} \tag{24}$$

$$+ j H^R(r) \sum_{n'=0}^{N-1} x_c(n') q^{rn'} + k H^R(r) \sum_{n'=0}^{N-1} x_d(n') q^{rn'} \tag{25}$$

$$= H^R(r) X_a^R(r) + i H^R(r) X_b^R(r) + j H^R(r) X_c^R(r) + k H^R(r) X_d^R(r). \tag{26}$$

If (26) has “imaginary” part equal to zero, it reduces to

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

which coincides with the result of the cyclic convolution theorem for the ordinary FNT. Similar relations are obtained if the left QFNT is considered.

4.3 Cyclic Shift in the Original Domain

The QFNT of the cyclically shifted sequence $x'(n) = x(n + n_0)$ is given by

$$X'^R(r) = \sum_{n=0}^{N-1} x'(n) q^{rn} = \sum_{n=0}^{N-1} x(n + n_0) q^{rn}. \tag{27}$$

Using the substitution $n + n_0 = n'$ in the last equation, one obtains

$$X'^R(r) = \sum_{n'=0}^{N-1} x(n') q^{r(n'-n_0)} = \sum_{n'=0}^{N-1} x(n') q^{rn'} q^{-rn_0}. \tag{28}$$

Writing $x(n') = x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k$, the last equation becomes

$$X'^R(r) = \sum_{n'=0}^{N-1} [x_a(n') + x_b(n')i + x_c(n')j + x_d(n')k] q^{rn'} q^{-rn_0} \tag{29}$$

$$= q^{-rn_0} X_a^R(r) + i q^{-rn_0} X_b^R(r) + j q^{-rn_0} X_c^R(r) + k q^{-rn_0} X_d^R(r). \tag{30}$$

Again, if X'^R has “imaginary” part equal to zero, the obtained result coincides with that obtained in the cyclic shift property of the ordinary FNT.

4.4 Parseval Theorem

Theorem 3 Let \mathbf{x} be a N -point vector of generalized quaternions over \mathbb{F}_p , such that $\mathbf{x} \xleftrightarrow{QFNT^R} \mathbf{X}^R$ and $|q| = 1$. Thus, the relationship

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

holds.

Proof

$$\sum_{n=0}^{N-1} |x(n)|^2 = \sum_{n=0}^{N-1} x(n)x^*(n) = \frac{1}{N} \sum_{n=0}^{N-1} \left[\sum_{r=0}^{N-1} X^R(r)q^{-rn} \right] x^*(n) \tag{31}$$

$$= \frac{1}{N} \sum_{r=0}^{N-1} X^R(r) \sum_{n=0}^{N-1} [q^{rn}]^* x^*(n) = \frac{1}{N} \sum_{r=0}^{N-1} X^R(r) \sum_{n=0}^{N-1} [x(n)q^{rn}]^* \tag{32}$$

$$= \frac{1}{N} \sum_{r=0}^{N-1} X^R(r) [X^R(r)]^* = \frac{1}{N} \sum_{r=0}^{N-1} |X^R(r)|^2. \tag{33}$$

□

5 Color Image Processing Using the QFNT

In this section, we perform a preliminary discussion regarding potential applications of the QFNT. We focus on the field of digital image processing, where the QFNT allows the joint manipulation of up to four channels related to a color space. This idea, which has been exploited in several recent investigations, runs counter to most techniques devoted to digital image processing, which are applied to monochromatic images (grayscale images, for example); when one desires to process color images, normally, such techniques are independently applied to each color channel [13].

Employing quaternions, one maps in the coordinates of a quaternion the numerical values related to each color channel of a pixel in a specific position of the image. If an RGB (*red, green, blue*) image is considered, it is possible, for instance, to map the numerical values of the red, the green and the blue layers of a pixel in the i, j and k coefficients of the same quaternion, respectively. If a PNG (*portable network graphics*) image is considered, besides the three RGB color channels, an additional transparency layer can be applied; such a layer could be mapped in the “real” part of the quaternions, which had be set to zero in the case of RGB images without an extra transparency channel. More specifically, the pixel in the l th row and the c th column of a PNG image can be represented as the quaternion

$$T(l, c) + R(l, c)i + G(l, c)j + B(l, c)k,$$

where $T(l, c)$, $R(l, c)$, $G(l, c)$ and $B(l, c)$ denote, respectively, the values related to transparency, red, blue and green layers of the referred pixel. Using such strategy, the whole color image can be represented by a quaternion matrix, whose QFNT can be computed.

Naturally, the application of a QFNT to an image requires a two-dimensional version of such a transform. In fact, 2D-QFT has been extensively studied and applied in scenarios related to image processing [1, 2, 9, 14]. Most properties of such transforms come from simple extensions of QFT properties to two dimensions. The expectation is that a similar behavior be observed, considering the one- and the two-dimensional versions of the QFNT. At this time, it is enough to observe that a 2D-QFNT of a squared color image \mathbf{y} with dimensions $N \times N$ pixels can be computed multiplying the 1D-QFNT matrix and the corresponding row–column transposed matrix on the left and on the right by \mathbf{y}_q , the quaternionic representation of \mathbf{y} . In this manner, the 2D-QFNT is computed as

$$\mathbf{Y}_q = \mathbf{M}_Q \mathbf{y}_q \mathbf{M}_Q^T, \quad (34)$$

where $\mathbf{M}_Q = (M_Q(r, n)) = q^{rn}$, $r, n = 0, 1, \dots, N - 1$, is the 1D-QFNT matrix. From the quaternionic matrix \mathbf{Y}_q , one obtains the transformed (color) image \mathbf{Y} . The inverse 2D-QFNT is computed replacing \mathbf{M}_Q by \mathbf{M}_Q^{-1} .

As a consequence of the possibility of computing the QFNT of color images, some more specific applications can be glimpsed. The following examples can be mentioned:

- Filtering of color images using filters whose coefficients are generalized quaternions over a finite field. It is reasonable to expect that such a kind of filtering be processed in the 2D-QFNT domain using the cyclic convolution theorem adapted to this transform (see Sect. 4.2) [15, 29, 30, 32];
- Insertion / extraction of fragile watermarks. There are papers where watermarking schemes based on number-theoretic transforms are proposed [6, 40]. It may be possible to use the QFNT to create similar schemes directly applicable to color images;
- Encryption of color images. Recently, techniques for image encryption based on NTT and, in particular, in fractional versions of such transforms have been proposed [23, 25, 27]. This is made possible by the use of the fractional order as a secret parameter that changes to each image block being processed. By introducing some kind of parametrization in the definition of the QFNT, a similar idea may be proposed. Even if there is no parametrization, it is possible that the application of the QFNT contributes to the robustness of image encryption schemes against statistical attacks. This is illustrated in the following section.

5.1 An Illustrative Example

In this section, we present some illustrative results regarding the application of the QFNT to color images. One defines a 2D-QFNT from an 1D-QFNT whose kernel

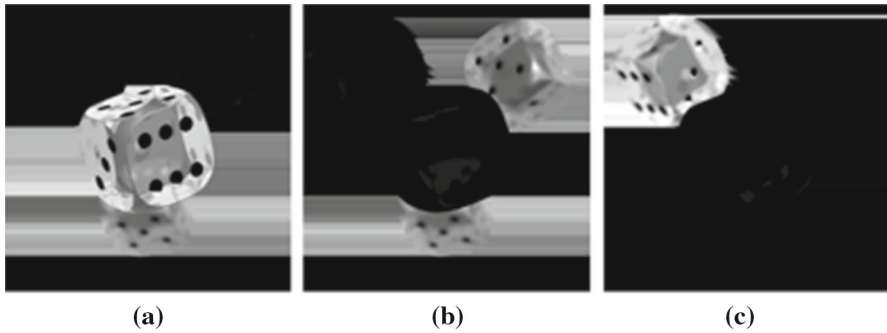


Fig. 1 Original image: **a** red, **b** green and **c** blue layers

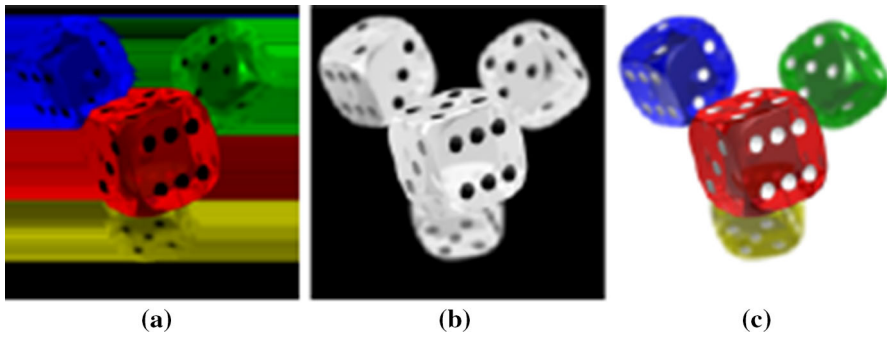


Fig. 2 Original image: **a** three color layers (without transparency layer), **b** transparency layer and **c** three color layers (with transparency layer) (Color figure online)

is the quaternion $q = 7 + 8i + 4j + 8k$ over \mathbb{F}_{257} . The multiplicative order of q is $\text{ord}(q) = 128$ and, therefore, a transform with $N = 128$ points is obtained. This transform is then applied, according to our previous description, to the quaternionic representation of a PNG image with dimensions 128×128 , formed by three color channels and one transparency layer.

In our computer experiments, we have considered the image whose color layers are presented in Fig. 1. In Fig. 2a, we show the corresponding color image, without the transparency layer, which is shown in Fig. 2b. In such a transparency layer, which acts as a window “aligned” to the color layers, the closer to white a region is, more visible the colors behind such a region will be; the closer to black a region is, less visible the colors behind such a region will be. The final image, considering the action of the transparency layer, is shown in Fig. 2c.

In Figs. 3 and 4, we present layers and images corresponding to those presented in Figs. 1 and 2, but considering the transformed version of the original image. What draws attention in the last figures is the noisy visual aspect, which suggests a degradation in the content of the original layers and images. This aspect is reflected in the histogram of each referred layer, as shown in Fig. 5. While the histograms of the color and the transparency layers of the original image have arbitrary shapes, the same histograms have predominantly uniform shapes in the transformed image. The appar-

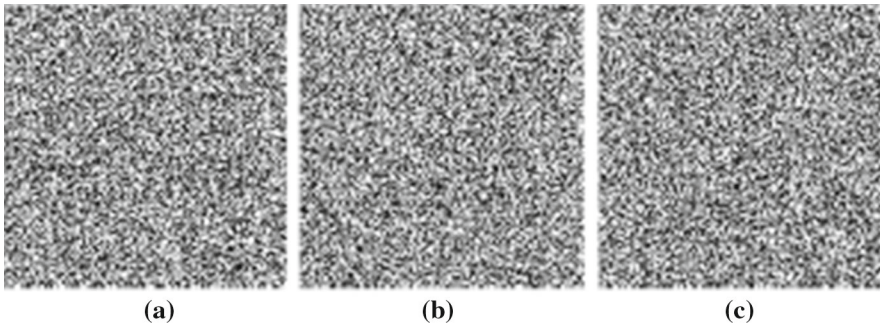


Fig. 3 Transformed image: **a** red, **b** green and **c** blue layers

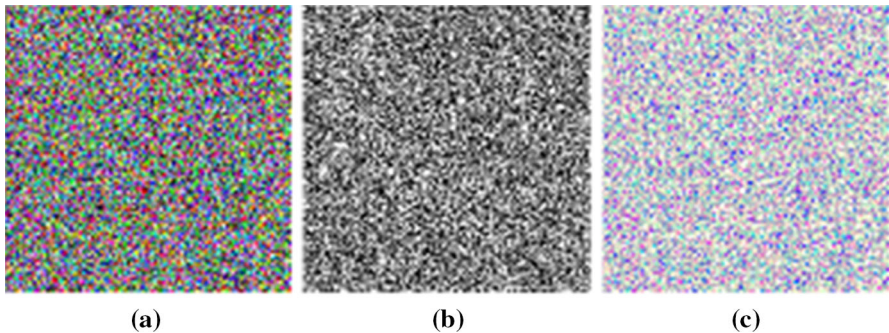


Fig. 4 Transformed image: **a** three color layers (without transparency layer), **b** transparency layer and **c** three color layers (with transparency layer) (Color figure online)

ent hiding of the original distribution of the pixel values of the image, caused by the application of the QFNT, is a desirable phenomenon from the cryptographic point of view.

Another interesting observation can be made by the computation of correlation coefficients for layers of original and transformed images. This coefficient measures the correlation among adjacent pixels of an image (the adjacency can be vertical, horizontal or diagonal) and should be close to one for images that have not been manipulated or artificially constructed; this is confirmed by the values exhibited in the first part of Table 1. On the other hand, after transforming the image using the QFNT, the obtained correlation coefficients have absolute values less than 0.05 always, which indicates low dependency among the values assumed by adjacent pixels. Such a behavior is also desirable from the cryptographic point of view. Other metrics such as, for example, the normalized entropy could be computed in order to complement the evaluation of the effects of the application of the QFNT on the statistical properties of an image [25].

As we mentioned before, the simple application of the QFNT to an image does not constitute a cryptographic scheme. It would be necessary the inclusion of some key-dependent mechanism as well as steps to ensure the satisfaction of basic premises in this scenario. At any case, considering the results presented in this section, the

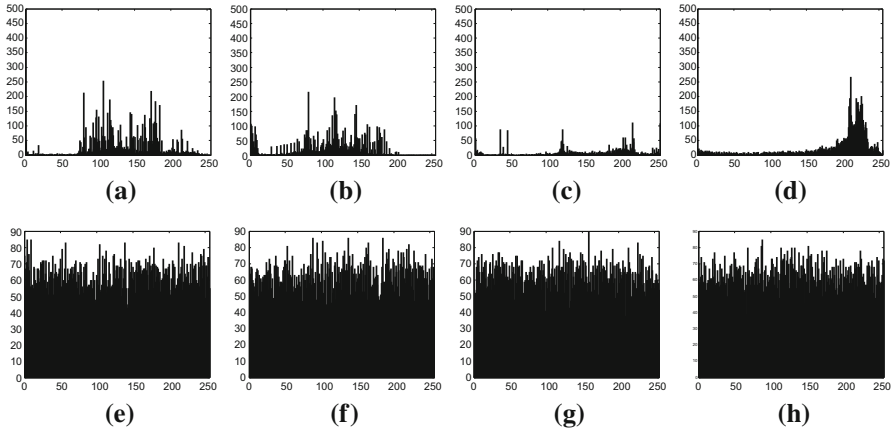


Fig. 5 Histograms: **a** red, **b** green, **c** blue and **d** transparency layers of original image; **e** red, **f** green, **g** blue and **h** transparency layers of transformed image

QFNT can be viewed as a potential candidate to be part of image encryption schemes, bringing the inherent possibility of processing in an aggregate way all layers of a color image. If a non-quaternionic number transform is used (see, for example [25] and [23]), this is not possible, that is, the layers of a color image must be separately encrypted, as if they were independent monochromatic images. This may have impact on the security of the scheme (a longer secret key may be required to ensure a certain robustness against brute-force attacks, for example).

The possibilities discussed in this section may also be potentially exploited by applying the QFNT to 3D objects, such as point clouds [16] and 3D medical data [8]. In this case, we should consider a three-dimensional QFNT, which can be defined by extending the one-dimensional QFNT to three dimensions analogously to what was previously done in this section for defining the 2D-QFNT; if one desires to transform a 3D object with dimensions $N_1 \times N_2 \times N_3$, for example, we have to choose three quaternions with multiplicative orders N_1 , N_2 and N_3 in a given finite field and use them as kernels of the QFNT applied in each direction. In another way, we can divide the referred 3D object into $N \times N \times N$ cubes in order to apply a 3D-QFNT defined by employing a single quaternion of order N as kernel (this would be similar to perform a block-based 2D image transformation). If the elements of the processed object are characterized by up to four components or *layers* (an RGB color can be associated with a point in a cloud, for instance), they can be represented by generalized quaternions in a manner analogous to that employed to represent the pixels of a 2D color image. In this way, in the 3D-QFNT domain, we can expect to obtain results similar to those achieved in the 2D case. This suggests that the use of the QFNT to encrypt 3D objects may also be feasible.

Table 1 Correlation coefficients of adjacent pixels in the layers of the original image (r) and the transformed image (\tilde{r}). The subscripts v , h and d are related to vertical, horizontal and diagonal adjacency, respectively

	Red	Green	Blue	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

6 Concluding Remarks

In this paper, we conducted an investigation related to generalized quaternions over finite fields, identifying existing properties and deriving some new results in this context. Such results were used to define the quaternion Fourier number transform, which corresponds to a finite field version of the discrete quaternion Fourier transform. We developed some QFNT properties and performed a preliminary evaluation regarding the application of a 2D-QFNT to digital image processing. In particular, the QFNT seems to be suitable for applications in the scenario of image encryption; this is partially due to the fact that the QFNT is highly sensitive to changes in the data one desires to process, which is not true for the QFT defined over Hamilton quaternions.

We are currently investigating several ideas related to the content presented in this paper. In particular, we believe that the QFNT can be useful to perform efficient and error-free hypercomplex signal filtering, replacing the QFT in the same sense that the NTT replaces the DFT in the fast computation of a convolution. At any case, our current investigations can be summarized in (i) introduction of new properties of generalized quaternions over finite fields, (ii) establishment of other properties of the QFNT, (iii) investigation of details related to the extension of the transform to two- and three-dimensional cases, (iv) definition of other types of quaternion number-theoretic transforms, such as cosine-, sine- and Hartley-type transforms and (v) investigation of specific QFNT applications.

Acknowledgements Juliano B. Lima is partially supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico—CNPq—under Grants 307686/2014-0 and 456744/2014-2.

Appendix

If $p \equiv 1 \pmod{4}$, one has $i = \sqrt{-1} \in \mathbb{F}_p$ [5]. The multiplicative order of \mathbf{Q} can be determined according to the following cases.

- **Case 1:** $b^2 + c^2 + d^2 = 0$. In this case, one has $\lambda_1 = \lambda_2 = a \in \mathbb{F}_p$. The following subcases have to be considered.
 - **Subcase 1.1:** $b = c = d = 0$. The condition determining the current subcase is identical to that considered in subcase 1.1 for $p \equiv 3 \pmod{4}$ and, therefore, leads to the same result.

- Subcase 1.2: $b = 0$ and $c \neq 0$ and $d \neq 0$. In this case, one has $c^2 = -d^2 \Rightarrow c = \pm di$. Assuming that $c = di$, \mathbf{Q} reduces to a matrix in the form

$$\mathbf{Q} = \begin{bmatrix} a & 2di \\ 0 & a \end{bmatrix}. \quad (35)$$

Denoting by $\mathbf{v} = [v(0) \ v(1)]$ an eigenvector of \mathbf{Q} , one may write $\mathbf{Q}\mathbf{v}^T = a\mathbf{v}^T$, which produces the system of equations

$$\begin{cases} av(0) + 2div(1) = av(0) \\ av(1) = av(1). \end{cases} \quad (36)$$

The solution for (36) is simply $v(1) = 0$, which indicates that the geometric multiplicity of $\lambda_1 = \lambda_2 = a$ is $m_g(a) = 1$. Therefore, \mathbf{Q} is not diagonalizable and admits the Jordan normal form

$$\mathbf{J}_\mathbf{Q} = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}. \quad (37)$$

Analogously to subcase 1.2 for $p \equiv 3 \pmod{4}$, one concludes that $\text{ord}(\mathbf{Q}) = \text{ord}(\mathbf{J}_\mathbf{Q}) = \text{lcm}(\text{ord}(a), p)$. One obtains the same result if $c = -di$ or $c = 0$ and $b \neq 0$ and $d \neq 0$ or $d = 0$ and $b \neq 0$ and $c \neq 0$.

- Subcase 1.3: $b \neq 0$ and $c \neq 0$ and $d \neq 0$. In this case, one may write $b^2 = -(c^2 + d^2) \Rightarrow b = \pm i\sqrt{c^2 + d^2}$. Assuming that $b = i\sqrt{c^2 + d^2}$, \mathbf{Q} reduces to a matrix in the form

$$\mathbf{Q} = \begin{bmatrix} a - \sqrt{c^2 + d^2} & c + di \\ -c + di & a + \sqrt{c^2 + d^2} \end{bmatrix}. \quad (38)$$

Denoting by $\mathbf{v} = [v(0) \ v(1)]$ an eigenvector of \mathbf{Q} , one may write $\mathbf{Q}\mathbf{v}^T = a\mathbf{v}^T$, which produces the system of equations

$$\begin{cases} -\sqrt{c^2 + d^2}v(0) + (c + di)v(1) = 0 \\ (-c + di)v(0) + \sqrt{c^2 + d^2}v(1) = 0 \end{cases}. \quad (39)$$

From (39), one obtains the relationship

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

which indicates that the geometric multiplicity of $\lambda_1 = \lambda_2 = a$ is $m_g(a) = 1$. Therefore, \mathbf{Q} is not diagonalizable and admits the Jordan normal form (37). Analogously to subcase 1.2 for $p \equiv 3 \pmod{4}$, one concludes that $\text{ord}(\mathbf{Q}) = \text{ord}(\mathbf{J}_\mathbf{Q}) = \text{lcm}(\text{ord}(a), p)$. One obtains the same result if $b = -i\sqrt{c^2 + d^2}$. A similar development can be carried out if we use $c = \pm i\sqrt{b^2 + d^2}$ or $d = \pm i\sqrt{b^2 + c^2}$.

- Case 2: $b^2 + c^2 + d^2 \neq 0$. In this case, \mathbf{Q} has two distinct eigenvalues and admits the diagonal form

$$\Lambda_{\mathbf{Q}} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}. \quad (40)$$

Thus, $\text{ord}(\mathbf{Q}) = \text{ord}(\Lambda_{\mathbf{Q}}) = \text{lcm}(\lambda_1, \lambda_2)$.

References

1. D.S. Alexiadis, G.D. Sergiadis, Estimation of motions in color image sequences using hypercomplex Fourier transforms. *IEEE Trans. Image Process.* **18**(1), 168–187 (2009)
2. D. Assefa, L. Mansinha, K.F. Tiampo, H. Rasmussen, K. Abdella, Local quaternion Fourier transform and color image texture analysis. *Signal Process.* **90**(6), 1825–1835 (2010)
3. B. Augereau, P. Carré, Hypercomplex polynomial wavelet-filter bank transform for color image. *Signal Process.* **136**(7), 16–28 (2017)
4. R.E. Blahut, *Fast Algorithms for Signal Processing* (Cambridge University Press, Cambridge, 2010)
5. D.M. Burton, *Elementary Number Theory*, 7th edn. (McGraw-Hill Education, New York, 2010)
6. R.J. Cintra, V.S. Dimitrov, H.M. de Oliveira, R.M. Campello de Souza, Fragile watermarking using finite field trigonometrical transforms. *Signal Process. Image Commun.* **24**(7), 587–597 (2009)
7. R.M.C. de Souza, H.M. de Oliveira, A.N. Kauffman, A.J.A. Paschoal, in *Information Theory, 1998. Proceedings. 1998 IEEE International Symposium*. Trigonometry in finite fields and a new hartley transform (IEEE, 1998), p. 293
8. A. del Rey, J.L. Hernández Pastora, G. Rodríguez Sánchez, 3D medical data security protection. *Expert Syst. Appl.* **54**, 379–386 (2016)
9. T.A. Ell, S.J. Sangwine, Hypercomplex Fourier transforms of color images. *IEEE Trans. Image Process.* **16**(1), 22–35 (2007)
10. T.A. Ell, N. Le Bihan, S.J. Sangwine, *Quaternion Fourier Transforms for Signal and Image Processing* (Wiley, New York, 2014)
11. F. Fekri, S.W. McLaughlin, R.M. Mersereau, R.W. Schafer, Block error correcting codes using finite-field wavelet transforms. *IEEE Trans. Signal Process.* **54**(3), 991–1004 (2006)
12. P. Fletcher, S.J. Sangwine, The development of the quaternion wavelet transform. *Signal Process.* **136**(7), 2–15 (2017)
13. R.C. Gonzalez, R.E. Woods, *Digital Image Processing*, 4th edn. (Pearson, London, 2017)
14. A.M. Grigoryan, J. Jenkinson, S.S. Agaian, Quaternion fourier transform based alpha-rooting method for color image measurement and enhancement. *Signal Process.* **109**, 269–289 (2015)
15. M. Jiang, W. Liu, Y. Li, Z. Zhang, in *TENCON 2013-2013 IEEE Region 10 Conference (31194)*. Frequency-domain quaternion-valued adaptive filtering and its application to wind profile prediction (IEEE, 2013), pp. 1–5
16. A. Jolfaei, X.W. Wu, V. Muthukkumarasamy, A 3D object encryption scheme which maintains dimensional and spatial stability. *IEEE Trans. Inf. Forensics Secur.* **10**(2), 409–422 (2015)
17. S. Kak, The number theoretic Hilbert transform. *Circuits Syst. Signal Process.* **33**(8), 2539–2548 (2014)
18. M. Kobayashi, Fixed points of split quaternionic hopfield neural networks. *Signal Process.* **136**(7), 38–42 (2017)
19. T.Y. Lam, *Introduction to Quadratic Forms Over Fields. Graduate Studies in Mathematics*, vol. 67 (American Mathematical Society, New York, 2004)
20. R. Lan, Y. Zhou, Quaternion-Michelson descriptor for color image classification. *IEEE Trans. Image Process.* **25**(11), 5281–5292 (2016)
21. Y.N. Li, Quaternion polar harmonic transforms for color images. *IEEE Signal Process. Lett.* **20**(8), 803–806 (2013)
22. J.B. Lima, R.M. Campello de Souza, Closed-form Hermite–Gaussian-like number-theoretic transform eigenvectors. *Signal Process.* **128**, 409–416 (2016)
23. J.B. Lima, L.F.G. Novaes, Image encryption based on the fractional fourier transform over finite fields. *Signal Process.* **94**, 521–530 (2014)
24. J.B. Lima, R.M.C. Souza, Finite field trigonometric transforms. *Appl. Algebra Eng. Commun. Comput.* **22**(5–6), 393–411 (2011)

25. J.B. Lima, F. Madeiro, F.J.R. Sales, Encryption of medical images based on the cosine number transform. *Signal Process. Image Commun.* **35**, 1–8 (2015)
26. P.H.E.S. Lima, J.B. Lima, R.M. Campello de Souza, Fractional Fourier, Hartley, cosine and sine number-theoretic transforms based on matrix functions. *Circuits Syst. Signal Process.* **36**(7), 2893–2916 (2016)
27. M. Mikhail, Y. Abouelseoud, G. ElKobrosy, Two-phase image encryption scheme based on FFCT and fractals. *Security and Communication Networks* **2017**, 1–13 (2017)
28. T. Minemoto, T. Isokawa, H. Nishimura, N. Matsui, Feed forward neural network with random quaternionic neurons. *Signal Process.* **136**(7), 59–68 (2017)
29. T. Ogunfunmi, Adaptive filtering using complex data and quaternions. *Proc. Comput. Sci.* **61**, 334–340 (2015)
30. F. Ortolani, D. Commiello, M. Scarpiniti, A. Uncini, Frequency domain quaternion adaptive filters: algorithms and convergence performance. *Signal Process.* **136**(7), 69–80 (2017)
31. A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, F. Pérez-González, Number theoretic transforms for secure signal processing. *IEEE Trans. Inf. Forensics Secur.* **12**(5), 1125–1140 (2017)
32. S.C. Pei, Y.Z. Hsiao, *Circuits and Systems (ISCAS), 2013 IEEE International Symposium*. Demosaicking of color filter array patterns using quaternion Fourier transform and low pass filter. (IEEE, 2013), pp. 2800–2803
33. S.C. Pei, C.C. Wen, J.J. Ding, Closed form orthogonal number theoretic transform eigenvectors and the fast fractional NTT. *IEEE Trans. Signal Process.* **59**(5), 2124–2135 (2011)
34. R.S. Pierce, *Associative Algebras. Graduate Texts in Mathematics*, vol. 88 (Springer, New York, 1982)
35. J.M. Pollard, The fast Fourier transform in a finite field. *Math. Comput.* **25**(114), 365–374 (1971)
36. I.S. Reed, T.K. Truong, The use of finite fields to compute convolutions. *IEEE Trans. Inf. Theory* **21**(2), 208–213 (1975)
37. S. Roman, *Advanced Linear Algebra. Graduate Texts in Mathematics*, vol. 135, 3rd edn. (Springer, New York, 2007)
38. R. Roopkumar, Quaternionic one-dimensional fractional Fourier transform. *Opt. Int. J. Light Electron Opt.* **127**(24), 11657–11661 (2016)
39. W. Shu, Y. Tianren, Algorithm for linear convolution using number theoretic transforms. *Electron. Lett.* **24**(5), 249–250 (1988)
40. H. Tamori, T. Yamamoto, Asymmetric fragile watermarking scheme using a number-theoretic transform. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E92.A**(3), 836–838 (2009)
41. T. Toivonen, J. Heikkilä, Video filtering with Fermat number theoretic transforms using residue number system. *IEEE Trans. Circuits Syst. Video Technol.* **16**(1), 92–101 (2006)
42. D. Wei, Image super-resolution reconstruction using the high-order derivative interpolation associated with fractional filter functions. *IET Signal Process.* **10**(9), 1052–1061 (2016)
43. D. Wei, Y. Li, Different forms of Plancherel theorem for fractional quaternion Fourier transform. *Opt. Int. J. Light Electron Opt.* **124**(24), 6999–7002 (2013)
44. D. Wei, Y.M. Li, Generalized sampling expansions with multiple sampling rates for lowpass and bandpass signals in the fractional Fourier transform domain. *IEEE Trans. Signal Process.* **64**(18), 4861–4874 (2016)
45. Y. Xu, L. Yu, H. Xu, H. Zhang, T. Nguyen, Vector sparse representation of color image using quaternion matrix analysis. *IEEE Trans. Image Process.* **24**(4), 1315–1329 (2015)