Operators
and
Matrices
Volume 10, Number 1 (2016), 209–221 doi:10.7153/oam-10-13

ON THE SUMMATION OF FRACTIONAL POWERS OF MATRICES OVER FINITE FIELDS

JULIANO B. LIMA AND RICARDO M. CAMPELLO DE SOUZA

(*Communicated by R. A. Brualdi*)

Abstract. In this paper, we investigate the summation of fractional powers of matrices over finite fields. More specifically, we show how a fractional power of a matrix of a linear transform over a finite field can be obtained from the linear combination of some specific powers of the same matrix. We use the developed theory to construct matrices related to fractional Fourier and cosine transforms over finite fields.

1. Introduction

Fractional transforms have been widely investigated in the last decades. These mathematical tools, which can be viewed as generalizations of the corresponding ordinary transforms, have been successfully applied in several areas, such as signal processing, optics, cryptography and communications [10, 5, 8]. Recently, fractional transforms over finite fields were introduced. In [21], a fractional number-theoretic transform based on complete generalized Legendre sequences over finite fields was proposed. In [7], a finite field fractional Fourier transform based on a matrix commuting with the finite field Fourier transform matrix was introduced.

In this paper, we investigate the summation of fractional powers of matrices over finite fields. More specifically, we establish in the finite field scenario the ideas proposed in [6] and [9], where new methods for computing fractional powers of a matrix with eigenstructure related to that of the discrete Fourier transform matrix are given. Such methods use a linear combination of some specific fractional powers of a matrix to obtain any of its fractional powers. In the case of the fractional Fourier transform, for instance, this makes unnecessary the eigendecomposition-based computation of the new fractional kernel whenever the fractional parameter changes; we only need to compute the coefficients of the linear combination, which can be obtained from an inverse Fourier transform operation.

Here, the validity of the above described principles in the finite field context is demonstrated. With this purpose, we consider the fractional Fourier transform over finite fields defined in [7]. Additionally, we introduce a new theorem, which is specially devoted to matrices with entries in a finite field and whose eigenvalues are all

Mathematics subject classification (2010): 12E20, 15B33, 15A18, 43A32.
Keywords and phrases: Finite field transforms, fractional powers of matrices, periodic matrices.
This research is supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq (Grants 307686/2014-0 and 456744/2014-2).

distinct. We show that fractional powers of matrices with the mentioned property can be computed by a linear combination of its integer powers. This method is applied in the computation of fractional powers of a finite field cosine transform matrix [13].

This paper is organized as follows. In Section 2, we present some concepts related to periodic matrices and review some facts and definitions related to Fourier and cosine transforms over finite fields. We also discuss aspects related to the eigenstructures of the matrices of such transforms. In Section 3, we introduce the main results related to the summation of fractional powers of matrices over finite fields and present some illustrative examples. The paper closes with some concluding remarks in Section 4.

2. Preliminaries

In this section, we present some theoretical concepts related to periodic matrices and transforms over finite fields. Particularly, we review some aspects related to trigonometry in finite fields. Subsequently, we present definitions for Fourier and cosine transforms over finite fields as well as some results concerning the eigenstructures of the corresponding transform matrices.

2.1. Periodic matrices over finite fields

Periodic matrices over finite fields perform an important role in the investigation carried out in this paper. Although the study of the periodicity is more common for matrices whose entries are complex numbers [3, 4], in what follows, we give a suitable finite field extension of the main concepts related to this topic.

DEFINITION 1. A matrix $\mathbf{M}$ with entries in a finite field is periodic if $\mathbf{M}^{r+1} = \mathbf{M}$ for some integer r. If $r = P$ is the least positive integer such that $\mathbf{M}^{P+1} = \mathbf{M}$, then P is called the period of $\mathbf{M}$.

Differently from matrices whose entries are real or complex numbers, all nonsingular matrices over a finite field are periodic. This can be easily concluded using some facts from group theory. Particularly, let us consider the general linear group $\mathrm{GL}(N,q)$[1]. Since $\mathrm{GL}(N,q)$ is finite, its elements have finite multiplicative orders, i. e., periods. In this way, restricting our investigation to nonsingular matrices over finite fields, we can define a P-periodic matrix $\mathbf{M}$ as the one which satisfies $\mathbf{M}^P = \mathbf{I}$, the identity matrix. In the following proposition, a general characterization regarding the eigenvalues of such matrices is given.

PROPOSITION 1. *Let* $\mathbf{M}$ *be a* P*-periodic nonsingular matrix over a finite field and* λ *be an eigenvalue of* $\mathbf{M}$*. Then,* $\lambda \in U = \{\zeta^k, k = 0,1,\ldots,P-1\}$*, where* ζ *has multiplicative order* $\mathrm{ord}(\zeta) = P$.

[1] The general linear group $\mathrm{GL}(N,q)$ is the set of $N \times N$ invertible matrices with entries from $\mathrm{GF}(q)$, with matrix multiplication as the group operation; $\mathrm{GF}(q)$ denotes the finite field with $q = p^m$ elements (p is a prime and m is a positive integer). Fundamentals of groups and fields can be found in [1] and [2].

Proof. Let λ and $\mathbf{v}$ be an eigenvalue and the corresponding eigenvector of $\mathbf{M}$, respectively. From $\mathbf{M}\mathbf{v} = \lambda\mathbf{v}$, one has $\mathbf{M}^P\mathbf{v} = \lambda^P\mathbf{v}$. Hence, $\mathbf{v} = \lambda^P\mathbf{v}$, which implies $\lambda^P = 1$. The solution set of this equation is the one given in the proposition. □

2.2. Trigonometry over finite fields

The fundamentals of trigonometry over finite fields were introduced in [18], as a requirement for defining the Hartley transform over finite fields. In what follows, we review some important definitions and propositions concerning this theme.

DEFINITION 2. The set of Gaussian integers over $\mathrm{GF}(p)$ is the set $\mathrm{GI}(p) = \{c + dj, c, d \in \mathrm{GF}(p)\}$, where p is a prime such that j^2 is a quadratic nonresidue over $\mathrm{GF}(p)$.

The "complex" structure $\mathrm{GI}(p)$, whose elements $\zeta = c + dj$ have a "real" part $c = \Re\{\zeta\}$ and an "imaginary" part $d = \Im\{\zeta\}$, is isomorphic to the extension field $\mathrm{GF}(p^2)$. Although $\mathrm{GI}(p)$ can be constructed for any prime p, afterward in this paper, we consider $p \equiv 3 \pmod 4$ and use the quadratic nonresidue $j^2 = -1$, which provides an interesting analogy with the usual complex numbers.

DEFINITION 3. The unimodular set of $\mathrm{GI}(p)$, denoted by $\mathrm{G}_{1,p}$, is the set of elements $\zeta = (c + dj) \in \mathrm{GI}(p)$, such that $c^2 + d^2 \equiv 1 \pmod p$.

PROPOSITION 2. *The structure* $\langle \mathrm{G}_{1,p}, \bullet \rangle$ *is a cyclic group of order* $(p+1)$.

The proof of Proposition 2 is given in [7]. Since the structure $\langle \mathrm{G}_{1,p}, \bullet \rangle$ is isomorphic to the group of the $(p+1)$-th complex roots of the unit, we may introduce a graphic representation of unimodular elements over a finite field. This consists in distributing such elements along a unit circle over the corresponding field, according to their multiplicative orders.

EXAMPLE 1. In this illustrative example, we consider the unimodular set of $\mathrm{GI}(31)$.

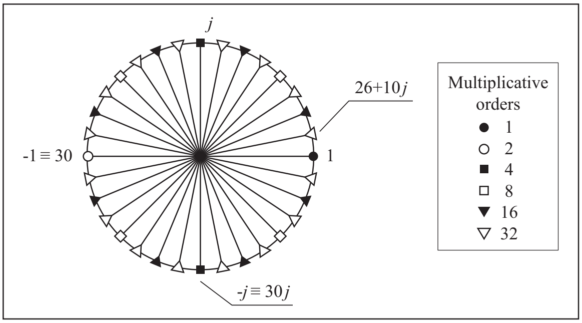

Figure 1: *Representation of the elements of* $\mathrm{G}_{1,31}$ *along the unit circle over* $\mathrm{GI}(31)$.

In Figure 1, we represent the 32 elements of $\mathrm{G}_{1,31}$ along the unit circle over $\mathrm{GI}(31)$. According to this representation, all unimodular elements are cyclically generated by the element $26+10j$, whose multiplicative order is 32. The multiplicative orders of all other unimodular elements are also given.

DEFINITION 4. Let $\zeta \in \mathrm{GI}(p)$ be an element with multiplicative order denoted by $\mathrm{ord}(\zeta)$. The finite field cosine and sine of the arc related to ζ are computed modulo p, respectively, as

$$\cos_\zeta(x) := \frac{\zeta^x + \zeta^{-x}}{2} \tag{1}$$

and

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

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

Trigonometric functions over finite fields hold properties similar to those of the standard real-valued ones, such as symmetry and the addition of arcs, for instance. If such functions are computed with respect to a unimodular element, other interesting properties are verified. If $\zeta \in \mathrm{G}_{1,p}$, for example, one has $\cos_\zeta(x) = \Re\{\zeta^x\}$ and $\sin_\zeta(x) = \Im\{\zeta^x\}$ [18, 7].

2.3. The finite field Fourier transform

In this section, we give a definition for the finite field Fourier transform (FFFT) and present the main results related to the eigenstructure of its matrix [17, 12].

DEFINITION 5. The finite field Fourier transform of a vector $\mathbf{x} = (x_i)$, $x_i \in \mathrm{GI}(p)$, $i = 0, 1, \ldots, N-1$, is a vector $\mathbf{X} = (X_k)$, $X_k \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, the components of which are

$$X_k := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} x_i \zeta^{-ki},$$

where $\zeta \in \mathrm{GI}(p)$ has multiplicative order N. The inverse transform is given by

$$x_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_k \zeta^{ki}.$$

The relationship between $\mathbf{x}$ and $\mathbf{X}$ can be expressed by the matrix equation

$$\mathbf{X} = \mathbf{F} \cdot \mathbf{x}, \tag{3}$$

where $\mathbf{F}$ is the transform matrix, whose element in the $(k+1)$-th row and the $(i+1)$-th column is given by $F_{k,i} = \frac{1}{\sqrt{N}} \zeta^{-ki}$.

PROPOSITION 3. *The period of* $\mathbf{F}$ *is* 4.

PROPOSITION 4. *The* $\mathbf{F}$ *matrix has, at most, four distinct eigenvalues, namely* $\{1, -1, \sqrt{-1}, -\sqrt{-1}\}$, *whose multiplicities are given in Table 1.*

Table 1: *Multiplicities of the eigenvalues of an $N \times N$ finite field Fourier transform matrix* [17].

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

2.4. The finite field cosine transform

In [13], the familiy of finite field trigonometric transforms was introduced. This family includes eight types of cosine (FFCT) and eight types of sine (FFST) transforms over finite fields. Several theoretical aspects of these transforms have been investigated and applications for them have been proposed [20, 14]. FFCT and FFST of types 1 and 4 are closely related to the FFFT. On the other hand, FFCT and FFST of types 2 and 3 have some remarkable peculiarities, specially regarding the eigenstructure of the respective transform matrices [12]. In what follows, we present the definition of the FFCT of type 2 and discuss some of its properties.

DEFINITION 6. The finite field cosine transform of a vector $\mathbf{x} = (x_i)$, $x_i \in \mathrm{GI}(p)$, $i = 0, 1, \ldots, N-1$, is a vector $\mathbf{X} = (X_k)$, $X_k \in \mathrm{GI}(p)$, $k = 0, 1, \ldots, N-1$, the components of which are

$$X_k := \sqrt{\frac{2}{N}} \sum_{i=0}^{N-1} \beta_k x_i \cos_\zeta \left(k \left(i + \frac{1}{2} \right) \right), \tag{4}$$

where $\zeta \in \mathrm{GI}(p)$ has multiplicative order $2N$, and

$$\beta_k = \begin{cases} \frac{1}{\sqrt{2}} \pmod{p}, & k = 0, \\ 1, & k = 1, 2, \ldots, N-1. \end{cases}$$

The inverse transform is given by

$$x_i = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} \beta_k X_k \cos_\zeta \left(k \left(i + \frac{1}{2} \right) \right).$$

Analogously to the FFFT, the computation of an FFCT can be expressed as

$$\mathbf{X} = \mathbf{C} \cdot \mathbf{x},$$

where $\mathbf{C}$ is the FFCT matrix, whose components are computed from Equation (4). We observe that $\mathbf{C}^{-1} = \mathbf{C}^T$, where $\{\cdot\}^T$ denotes the transposition of the argument.

PROPOSITION 5. *Let $\mathbf{C}$ be a diagonalizable FFCT matrix. The period of $\mathbf{C}$ is the least common multiple (*lcm*) of the multiplicative orders of its eigenvalues.*

Proof. Let $\mathbf{C}$ be the $N \times N$ FFCT matrix and $\lambda_1, \lambda_2, \ldots, \lambda_N$ its eigenvalues. Using the fact that $\mathbf{C}$ is diagonalizable, one has

$$\mathbf{C} = \mathbf{V}\mathbf{\Lambda}_{\mathbf{C}}\mathbf{V}^{-1}, \tag{5}$$

where $\mathbf{V}$ is a matrix whose columns are N linearly independent eigenvectors of $\mathbf{C}$ and $\mathbf{\Lambda}_{\mathbf{C}}$ is a diagonal matrix whose entries are $\lambda_1, \lambda_2, \ldots, \lambda_N$. Since

$$\mathbf{C}^r = \mathbf{V}\mathbf{\Lambda}_{\mathbf{C}}^r\mathbf{V}^{-1}, \tag{6}$$

where r is an integer, the period P, such that $\mathbf{C}^P = \mathbf{I}$, is the least positive integer satisfying $\mathbf{\Lambda}_{\mathbf{C}}^P = \mathbf{I}$. Such a condition is achieved if the P-th power of all eigenvalues of $\mathbf{C}$ equals 1. Therefore, $P = \mathrm{lcm}(\lambda_1, \lambda_2, \ldots, \lambda_N)$. □

Some aspects regarding the eigenstructure of the FFCT of type 2 were investigated in [12], leading to a conjecture, which follows a line analogous to that developed for the real-valued discrete cosine transform of type 2 [19]: all eigenvalues of the FFCT matrix of type 2 are distinct. If we take this conjecture into account, every $\mathbf{C}$ matrix is diagonalizable and, therefore, its period can be evaluated from the spectral expansion given in Equation (6).

2.5. Fractional Fourier and cosine transforms over finite fields

Using the procedure introduced in [7], the $N \times N$ matrix of the fractional Fourier transform over a finite field (GFrFT) can be computed from the spectral expansion

$$\mathbf{F}^a = \mathbf{V}\mathbf{\Lambda}_{\mathbf{F}}^a\mathbf{V}^T. \tag{7}$$

In Equation (7), a represents the fractional parameter, which is actually a rational number; the matrix $\mathbf{V}$ has in its columns N orthonormal eigenvectors $\mathbf{v}$ of $\mathbf{F}$. In this case, such eigenvectors are Hermite-Gaussian vectors over finite fields derived from a commuting matrix based approach [7, 16]; $\mathbf{\Lambda}_{\mathbf{F}}^a$ is a diagonal matrix whose entries are $(-j)^{ka}$, $k = 0, 1, \ldots, 2\left\lfloor \frac{N}{2} \right\rfloor$ ($k \neq N-1$, if N is even). The GFrFT of a vector $\mathbf{x}$ is then computed as

$$\mathbf{X}_a = \mathbf{F}^a\mathbf{x}.$$

Fractional cosine and sine transform matrices of types 1 and 4 over finite fields can be obtained using spectral expansions closely related to that given in Equation (7) [11].

The matrix of the fractional FFCT considered in this paper can be obtained from the spectral expansion given in Equation (6), replacing the integer r by the fractional parameter a. However, according to our previous discussion and differently from the matrix $\mathbf{F}$, the eigenstructure of $\mathbf{C}$ does not follow any *systematic* behavior. This makes the computation of its eigenvalues and the subsequent construction of the eigenvector set to be used in its spectral expansion a laborious work. The eigenvalues of $\mathbf{C}$, for instance, can lie in larger extension fields; besides having components also in extension fields, the corresponding eigenvectors do not have any symmetry[2]. As we will show in Section 3, the method proposed in this paper allows the computation of fractional powers of $\mathbf{C}$, avoiding the mentioned constraints.

[2] The eigenvectors of $\mathbf{F}$ have even or odd symmetry. This makes its construction simpler.

3. Summation of fractional powers of matrices over finite fields

3.1. GFrFT computation by linear combination of GFrFTs

In [6], a procedure for computing a discrete fractional Fourier transform from a linear combination of some discrete fractional Fourier transforms with specific fractional parameters is given. In Propositions 6 and 7, we establish such a procedure for finite fields.

PROPOSITION 6. *Let* $\mathbf{x} = (x_i)$, $x_i \in \mathrm{GI}(p)$, $i = 0, 1, \ldots, N-1$, *be a vector with odd length* N. *The GFrFT of* $\mathbf{x}$, *with fractional parameter* a, *can be computed as*

$$\mathbf{X}_a = \sum_{i=0}^{N-1} B_{i,a} X_{ib},$$

where the coefficients $B_{i,a}$ *are*

$$B_{i,a} = \mathbf{F}^{-1}\left(\frac{1}{\sqrt{N}} j^{-ka}\right)_{k=0,\ldots,N-1} = \frac{1}{N}\frac{1-j^{N(ib-a)}}{1-j^{ib-a}}, \quad i = 0, \ldots, N-1,$$

and $b = 4/N$.

Proof. Computing the FFFT of $B_{i,a}$, we obtain

$$j^{-ka} = \sum_{i=0}^{N-1} B_{i,a} \zeta^{-ik},$$

where $\mathrm{ord}(\zeta) = N$. Expanding Equation (7) and replacing $(-j)^{ka} = j^{-ka}$ by the above expression, one computes the GFrFT of $\mathbf{x}$ as

$$\begin{aligned}\mathbf{X}_a &= \sum_{k=0}^{N-1}\left(\sum_{i=0}^{N-1} B_{i,a}\zeta^{-ik}\right)\mathbf{v}_k\mathbf{v}_k^T\mathbf{x}\\ &= \sum_{i=0}^{N-1} B_{i,a}\left(\sum_{k=0}^{N-1}\zeta^{-ik}\mathbf{v}_k\mathbf{v}_k^T\mathbf{x}\right).\end{aligned}$$

Since $\zeta^N = j^4 = 1$, ζ can be taken as $\zeta = j^b$, where $b = \frac{4}{N}$. Therefore, the last equation becomes

$$\mathbf{X}_a = \sum_{i=0}^{N-1} B_{i,a}\left(\sum_{k=0}^{N-1} j^{-kib}\mathbf{v}_k\mathbf{v}_k^T\mathbf{x}\right) = \sum_{i=0}^{N-1} B_{i,a}X_{ib}. \quad \square$$

PROPOSITION 7. *Let* $\mathbf{x} = (x_i)$, $x_i \in \mathrm{GI}(p)$, $i = 0, 1, \ldots, N-1$, *be a vector with even length* N. *The GFrFT of* $\mathbf{x}$, *with fractional parameter* a, *can be computed as*

$$\mathbf{X}_a = \frac{1}{N+1}\sum_{i=0}^{N} B_{i,a} X_{ib},$$

where the coefficients $B_{i,a}$ *are*

$$B_{i,a} = \mathbf{F}^{-1}\left(\frac{1}{\sqrt{N+1}}j^{-ka}\right)_{k=0,\ldots,N-1} = \frac{1}{N+1}\frac{1-j^{(N+1)(ib-a)}}{1-j^{ib-a}}, \quad i=0,\ldots,N,$$

and $b = 4/(N+1)$.

The proof of Proposition 7 is analogous to that of Proposition 6.

3.2. Linear combination of fractional powers of matrices

In [9], the procedure proposed in [6] was refined. A method for computing fractional powers of matrices whose periods are different from 4 and whose eigestructure is related to that of the FFFT was proposed. In the following theorem, this method is extended to the finite field scenario.

THEOREM 1. *Let* $\mathbf{L}$ *be an* $N \times N$ *matrix,* N *odd, with period* P *and whose spectral expansion is written as* $\mathbf{L} = \mathbf{V\Lambda V}^{-1}$. *Let* $b = P/N$ *and* $\mathbf{K} = \mathbf{L}^b = \mathbf{L}^{P/N} = \mathbf{V\Lambda}^{P/N}\mathbf{V}^{-1}$. *Then, we compute*

$$\mathbf{L}^a = \mathbf{K}^{a/b} = \sum_{i=0}^{N-1} C_{i,a/b}\mathbf{K}^i, \tag{8}$$

where

$$C_{i,a} = \mathbf{F}^{-1}\left(\frac{1}{\sqrt{N}}\zeta^{-ka}\right)_{k=0,\ldots,N-1} = \frac{1}{N}\frac{1-1^{i-a}}{1-\zeta^{i-a}} \tag{9}$$

and $\operatorname{ord}(\zeta) = N$. *Particularly, when* $P = N$, *one has*

$$\mathbf{L}^a = \sum_{i=0}^{N-1} C_{i,a}\mathbf{K}^i.$$

Proof. The spectral expansion of $\mathbf{K}$ is written as

$$\mathbf{K} = \mathbf{V\Lambda}^{P/N}\mathbf{V}^T = \sum_{k=0}^{N-1}\alpha^{-\frac{P}{N}k}\mathbf{v}_k\mathbf{v}_k^T$$

and, therefore, one has

$$\mathbf{K}^{a/b} = \sum_{k=0}^{N-1}\alpha^{-\frac{P}{N}k\frac{a}{b}}\mathbf{v}_k\mathbf{v}_k^T.$$

Let us define

$$\widehat{\mathbf{K}}^{a/b} := \sum_{i=0}^{N-1} C_{i,a/b}\mathbf{K}^i,$$

which can be rewritten as

$$\begin{aligned}\widehat{\mathbf{K}}^{a/b} &= \sum_{i=0}^{N-1} C_{i,a/b} \sum_{k=0}^{N-1} \alpha^{-\frac{P}{N}ki}\mathbf{v}_k\mathbf{v}_k^T \\ &= \sum_{k=0}^{N-1}\left(\sum_{i=0}^{N-1} C_{i,a/b}\alpha^{-\frac{P}{N}ki}\right)\mathbf{v}_k\mathbf{v}_k^T \\ &= \sum_{k=0}^{N-1}\left(\sum_{i=0}^{N-1} C_{i,a/b}\zeta^{-ki}\right)\mathbf{v}_k\mathbf{v}_k^T.\end{aligned}$$

The expression in parenthesis in the last equation corresponds to $\mathbf{F}\left(C_{i,a/b}\right)_{i=0,\dots,N-1} = \zeta^{-k\frac{a}{b}}$. Then,

$$\widehat{\mathbf{K}}^{a/b} = \sum_{k=0}^{N-1} \zeta^{-k\frac{a}{b}}\mathbf{v}_k\mathbf{v}_k^T = \mathbf{K}^{a/b} = \mathbf{L}^a. \quad \square$$

We remark that, in Equation (9), if the fractional parameter is written as $a = a_1/a_2$, one has

$$1^{i-a} = 1^{1-\frac{a_1}{a_2}} = \left(1^{\frac{1}{a_2}}\right)^{a_2-a_1};$$

we first compute $(1^{1/a_2})$ as the a_2-th root of largest multiplicative order of 1 and then we calculate its $(a_2 - a_1)$-th power. In $\mathrm{GI}(31)$, for example, it would be $(1^{1/32}) = 26 + 10j$ (see Example 1). The same procedure is applied to the computation of fractional powers of ζ. If N is even, we just have to replace N by $N+1$ in the statement of Theorem 1. The proof is also analogous to that developed above. In what follows, we present an illustrative example of the application of Theorem 1.

EXAMPLE 2. Let us consider an FFFT over $\mathrm{GI}(31)$ with length $N = 5$. We use the element $\zeta = 2$, whose multiplicative order is $\mathrm{ord}(\zeta) = 5$. The transform matrix is

$$\mathbf{F} = \begin{bmatrix} 26 & 26 & 26 & 26 & 26 \\ 26 & 13 & 22 & 11 & 21 \\ 26 & 22 & 21 & 13 & 11 \\ 26 & 11 & 13 & 21 & 22 \\ 26 & 21 & 11 & 22 & 13 \end{bmatrix}.$$

In order to compute fractional powers of $\mathbf{F}$, according to Theorem 1, we must construct the matrix $\mathbf{K} = \mathbf{F}^{4/5}$. Using the procedure given in [7], we obtain

$$\mathbf{K} = \mathbf{F}^{4/5} = \begin{bmatrix} 2 & 21 & 26 & 26 & 21 \\ 21 & 1+7j & 14+2j & 14+29j & 22+24j \\ 26 & 14+2j & 29+24j & 19+7j & 14+29j \\ 26 & 14+29j & 19+7j & 29+24j & 14+2j \\ 21 & 22+24j & 14+29j & 14+2j & 1+7j \end{bmatrix}.$$

If we want to compute $\mathbf{F}^{1/2}$, for instance, we have $a/b = 5/8$ and Equation (9) becomes

$$C_{i,5/8} = \frac{1}{5}\frac{1-1^{i-5/8}}{1-\zeta^{i-5/8}}.$$

The 8-th root of 1 is $27+27j$. Additionally, since $\zeta = 2$, its 8-th root is $16+16j$. Therefore, using $1/5 \equiv 25 \pmod{31}$, the last equation can be rewritten as

$$C_{i,5/8} = 25\frac{1-(27+4j)^{8i-5}}{1-(16+16j)^{8i-5}}.$$

Finally, using Equation (8), we obtain

$$\mathbf{F}^{1/2} = \begin{bmatrix} 7+28j & 6+13j & 27+13j & 27+13j & 6+13j \\ 6+13j & 3+3j & 12+25j & 12+7j & 3+29j \\ 27+13j & 12+25j & 9+2j & 9+30j & 12+7j \\ 27+13j & 12+7j & 9+30j & 9+2j & 12+25j \\ 6+13j & 3+29j & 12+7j & 12+25j & 3+3j \end{bmatrix}.$$

It is important to remark that, using the additivity of the fractional parameter a, Equation (8) can be rewritten as

$$\begin{aligned} \mathbf{L}^a &= \sum_{i=0}^{N-1} C_{i,a/b}\mathbf{K}^i \\ &= C_{N-1,a/b}\mathbf{K}^{N-1} + C_{N-2,a/b}\mathbf{K}^{N-2} + \ldots + C_{1,a/b}\mathbf{K} + C_{0,a/b}\mathbf{I} \\ &= \mathbf{K}(\ldots(\mathbf{K}(\mathbf{K}(C_{N-1,a/b}\mathbf{K} + C_{N-2,a/b}\mathbf{I}) + C_{N-3,a/b}\mathbf{I}) + C_{N-4,a/b}\mathbf{I}) + \ldots) + C_{0,a/b}\mathbf{I}. \end{aligned}$$

The last equation indicates that $\mathbf{L}^a$ can be computed, according to Theorem 1, from the matrix $\mathbf{K} = \mathbf{L}^b$ uniquely. This means that Equation (8) can be efficiently evaluated and implemented using regular architectures.

Although Theorem 1 also works for $P > N$, in practical applications, one usually has the length of the signal greater than the period of the matrix ($N > P$) [9]. In fact, this is the case when the Fourier ($P = 4$) and the sine and cosine of types 1 and 4 ($P = 2$) transform matrices over finite fields are considered. However, for the finite field cosine transform considered in this paper (type 2), this is not true. Such a behavior is explained by the eigenstructure of the $\mathbf{C}$ matrix, whose main aspects were discussed earlier. Since the eigenvalues of $\mathbf{C}$ are also not related to those of $\mathbf{F}$, Theorem 1 can not be used to compute $\mathbf{C}^a$. These particularities have inspired Theorem 2, which can be applied to the computation of fractional powers of any periodic matrix whose eigenvalues are all distinct; this is done by combining integer powers of the original matrix and does not require the precomputation of one of its fractional powers.

Theorem 2. *Let* $\mathbf{L}$ *be an* $N \times N$ *matrix, with period* P *and whose eigenvalues* $\lambda \in U = \{\zeta^k, k = 0, 1, \ldots, P-1\}$, *where* ζ *has multiplicative order* $\operatorname{ord}(\zeta) = P$, *are all distinct. Then, we compute*

$$\mathbf{L}^a = \sum_{i=0}^{P-1} C_{i,a}\mathbf{L}^i. \tag{10}$$

Proof. Let us denote by $\{\lambda_{(0)}, \lambda_{(1)}, \ldots, \lambda_{(N-1)}\}$ the eigenvalues of $\mathbf{L}$. We construct the matrix

$$\widetilde{\mathbf{L}} = \left[\begin{array}{c|ccc} \mathbf{L} & & & \\ \hline & \lambda_{(N)} & & \\ & & \ddots & \\ & & & \lambda_{(P-1)} \end{array}\right],$$

such that $\{\lambda_0, \lambda_1, \ldots, \lambda_{(P-1)}\} = U$. From Theorem 1, one has

$$\widetilde{\mathbf{L}}^a = \sum_{i=0}^{P-1} C_{i,a} \widetilde{\mathbf{L}}^i. \tag{11}$$

Since the a-th power of $\widetilde{\mathbf{L}}$ is given by

$$\widetilde{\mathbf{L}}^a = \left[\begin{array}{c|ccc} \mathbf{L}^a & & & \\ \hline & \lambda_{(N)}^a & & \\ & & \ddots & \\ & & & \lambda_{(P-1)}^a \end{array}\right],$$

directly from Equation (11) we derive Equation (10). □

In what follows, we show an illustrative example where a fractional power of the $\mathbf{C}$ matrix is computed from a linear combination of its integer powers.

EXAMPLE 3. Let us consider an FFCT over $\mathrm{GI}(31)$ with length $N = 4$. We use the unimodular element $\zeta = 4 + 27j$, whose multiplicative order is $\mathrm{ord}(\zeta) = 8$. The transform matrix is

$$\mathbf{C} = \begin{bmatrix} 16 & 16 & 16 & 16 \\ 28 & 10 & 21 & 3 \\ 16 & 15 & 15 & 16 \\ 10 & 3 & 28 & 21 \end{bmatrix}$$

and its eigenvalues are $\lambda_{(0)} = 7 + 13j$, $\lambda_{(1)} = 7 + 18j$, $\lambda_{(2)} = 24 + 13j$ and $\lambda_{(3)} = 24 + 18j$. The period of $\mathbf{C}$ is $P = 16$. Therefore, in order to compute $\mathbf{C}^{1/2}$ from Theorem 2, we choose $\gamma = 7 + 13j$, such that $\mathrm{ord}(\gamma) = 16$, and use Equation (9) to evaluate

$$C_{i,1/2} = \frac{1}{16} \frac{1 - 1^{i-1/2}}{1 - \gamma^{i-1/2}}.$$

Using $1/16 \equiv 2 \pmod{31}$, $1^{1/2} = -1$ and $\gamma^{1/2} = 2 + 11j$, we rewrite the last equation as

$$C_{i,1/2} = 2 \frac{1 - (-1)^{2i-1}}{1 - (2 + 11j)^{2i-1}}.$$

Finally, using Equation (10), we obtain

$$\mathbf{C}^{1/2} = \begin{bmatrix} 5j & 1j & 22j & 24j \\ 29j & 15j & 24j & 23j \\ 28j & 9j & 17j & 26j \\ 5j & 29j & 4j & 7j \end{bmatrix}.$$

4. Concluding remarks

In this paper, we have investigated the computation of fractional powers of a matrix over a finite field from a linear combination of some of its powers. The main results, which are presented in Section 3, are focused on the computation of fractional Fourier and trigonometric transforms over finite fields. In this sense, two cases can be distinguished. In the first one, which is summarized by Theorem 1, we establish in the finite field scenario a method for computing fractional powers of matrices whose eigenstructure is related to that of the $\mathbf{F}$ matrix. In the second one, which is represented by Theorem 2, we give a method for computing fractional powers of matrices whose eigenvalues are all distinct.

The methods we have mentioned allow the computation of a finite field fractional transform with a *new* fractional parameter a without the need of recurrent evaluations of spectral expansions such as that given by Equation (7). This provides some computational advantages, which become relevant specially in applications involving multiple-parameter fractional transforms. This is the case of some encryption schemes, such as that proposed in [5], where discrete fractional transforms are employed. In [15], an image encryption scheme based on the same premise, but using the GFrFT, is proposed. This scheme can be implemented using the method given in Theorem 1.

Regarding Theorem 2, it is clear that it may become unpractical as P increases. However, once it can be applied to any periodic matrix whose eigenvalues are all distinct, there may be other specific classes of matrices (different from those related to the cosine transform of type 2) whose fractional powers can be efficiently computed using the referred method. This includes matrices whose entries are complex numbers, to which the theorem can be applied after some slight adjustments. In fact, there are several areas to which the study of periodic matrices is relevant [3, 4]. Currently, we have carried out further investigations related to this topic.

REFERENCES

[1] D. S. DUMMIT AND R. M. FOOTE, *Abstract Algebra*, Wiley, 2003.

[2] J. E. HUMPHREYS, *Linear Algebraic Groups*, Graduate Texts in Mathematics, Springer, 1998.

[3] L. LEBTAHI, O. ROMERO AND N. THOME, *Characterizations of {K,s+1}-potent matrices and applications*, Linear Algebra and its Applications **2**, vol. 436, 293–306, 2012.

[4] Y. WU AND D. F. LINDER, *On the Eigenstructures of Functional K-Potent Matrices and Their Integral Forms*, WSEAS Transactions on Mathematics **1**, vol. 9, 244–253, 2010.

[5] F. ZHANG, Y. HU, R. TAO AND Y. WANG, *New fractional matrix with its applications in image encryption*, Optics & Lasers Technology, vol. 64, 82–93, 2014.

[6] M.-H. YEH AND S.-C. PEI, *A method for the discrete fractional Fourier transform computation*, IEEE Transactions on Signal Processing **3**, vol. 51, 889–891, 2003.

[7] J. B. LIMA AND R. M. CAMPELLO DE SOUZA, *The fractional Fourier transform over finite fields*, Signal Processing **2**, vol. 92, 465–476, 2012.

[8] X. SHA, X. QIU AND L. MEI, *Hybrid carrier CDMA communication system based on weighted-type fractional Fourier transform*, IEEE Communications Letters **4**, vol. 16, 432–435, 2012.

[9] R. TAO, F. ZHANG AND Y. WANG, *Linear summation of fractional-order matrices*, IEEE Transactions on Signal Processing **7**, vol. 58, 3912–3916, 2010.

[10] E. SEJDIĆ, I. DJUROVIĆ AND L. STANKOVIĆ, *Fractional Fourier transform as a signal processing tool: An overview of recent developments*, Signal Processing **6**, vol. 91, 1351–1369, 2011.

[11] J. B. LIMA AND R. M. CAMPELLO DE SOUZA, *Fractional cosine and sine transforms over finite fields*, Linear Algebra and its Applications, **8**, vol. 438, 3217–3230, 2013.

[12] J. B. LIMA, R. M. CAMPELLO DE SOUZA AND D. PANARIO, *The Eigenstructure of finite field trigonometric transforms*, Linear Algebra and its Applications, **8**, vol. 435, 1956–1971, 2011.

[13] J. B. LIMA AND R. M. CAMPELLO DE SOUZA, *Finite field trigonometric transforms*, Applicable Algebra in Engineering, Communication and Computing, **5–6**, vol. 22, 393–411, 2011.

[14] J. B. LIMA, E. A. O. LIMA AND F. MADEIRO, *Image encryption based on the finite field cosine transform*, Signal Processing: Image Communication **10**, vol. 28, 1537–1547, 2013.

[15] J. B. LIMA AND L. F. G. NOVAES, *Image encryption based on the fractional Fourier transform over finite fields*, Signal Processing, vol. 94, 521–530, 2014.

[16] C. CANDAN, M. ALPER KUTAY AND H. M. OZAKTAS, *The discrete fractional Fourier transform*, IEEE Trans. Signal Process. **5**, vol. 48, 1329–1337, 2000.

[17] D. T. BIRTWISTLE, *The Eigenstructure of the Number Theoretic Transforms*, Signal Processing **4**, vol. 4, 287–294, 1982.

[18] R. M. CAMPELLO DE SOUZA, H. M. DE OLIVEIRA, A. N. KAUFFMAN AND A. J. A. PASCHOAL, *Trigonometry in Finite Fields and a New Hartley Transform*, Proc. IEEE Int. Symp. Information Theory (ISIT'98), 293, 1998.

[19] CARIOLARO, G. AND ERSEGHE, T. AND KRANIAUSKAS, P., *The fractional discrete cosine transform*, IEEE Transactions on Signal Processing **4**, vol. 50, 902–911, 2002.

[20] R. J. CINTRA, V. S. DIMITROV, R. M. CAMPELLO DE SOUZA AND H. M. DE OLIVEIRA, *Fragile watermarking using finite field trigonometrical transforms*, Signal Processing, Image Communication, vol. 24, 587–597, 2009.

[21] S.-C. PEI, C.-C. WEN AND J. J. DING, *Closed form orthogonal number theoretic transform eigenvectors and the fast fractional NTT*, IEEE Trans. on Signal Processing **5**, vol. 59, 2124–2135, 2011.

(Received March 20, 2015)

Juliano B. Lima
Department of Electronics and Systems
Federal University of Pernambuco
Av. da Arquitetura, S/N, 4^o andar
Cidade Universitária, Recife, PE Brazil – 50740-550
e-mail: juliano_bandeira@ieee.org

Ricardo M. Campello de Souza
Department of Electronics and Systems
Federal University of Pernambuco
Av. da Arquitetura, S/N, 4^o andar
Cidade Universitária, Recife, PE Brazil – 50740-550
e-mail: ricardo@ufpe.br