THE FINITE FIELD FRACTIONAL FOURIER TRANSFORM

Juliano B. Lima
University of Pernambuco
Recife PE, Brazil
juliano.bandeira@upe.poli.br

Ricardo M. Campello de Souza
Federal University of Pernambuco
Recife PE, Brazil
ricardo@ufpe.br

ABSTRACT
In this paper, a finite field version for the fractional Fourier transform is introduced. We show that, in some aspects, the finite field fractional Fourier transform (4FT) is in perfect analogy with the discrete fractional Fourier transform. On the other hand, we consider some definitions and properties from the finite field context which allow us to discuss particularities of the 4FT.

Index Terms— Fractional Fourier transform, finite fields, eigenstructure.

1. INTRODUCTION
The fractional transforms have stimulated the interest of many researchers in the last years. Particularly in the areas of optics and signal processing, the number of papers dedicated to the theory and application of such tools has increased considerably. Image encryption and sampling rate conversion of band limited signals are specific examples of scenarios where different types of fractional transforms have been used [1], [2].

Following the same track of the ordinary transforms, the continuous fractional Fourier transform (FRT) was the first established fractional transform [3]. Naturally, a discrete version of the FRT was defined later [4], [5]. In this sense, the purpose of the present paper is to go ahead with this sequence of definitions and introduce the finite field fractional Fourier transform (4FT). In order to provide a kind of equivalence with the previous Fourier fractional transforms, the properties listed below have to be respected by the 4FT:

• Unitarity.
• Reduction to the finite field Fourier transform [6] when the order is equal to unity.
• Index additivity.

The discussion of the above cited properties takes into account some particularities of the finite fields. Since all computations are done modulo a prime number $p$, differently from the real-valued fractional transforms, rounding is not necessary. This fact gives advantages related to arithmetic complexity and makes the 4FT a truly digital transform.

2. PRELIMINARIES
In this section, the main concepts related to trigonometry in finite fields are reviewed. The most part of them was introduced by Campello de Souza et al., as a requirement for defining the finite field Hartley transform [7]. We also consider a modified version of the finite field Fourier transform (FFFT) and discuss its eigenstructure. This will play an important role on the definition of the 4FT.

2.1. Trigonometry in finite fields
Definition 1 The set of Gaussian integers over $\text{GF}(p)$ is the set $\text{GI}(p) = \{c + dj, c, d \in \text{GF}(p)\}$, such that $j^2 = -1$ is a quadratic nonresidue over $\text{GF}(p)$, i.e., $p \equiv 3 \pmod{4}$.

The extension field $\text{GF}(p^2)$ is isomorphic to the “complex” structure $\text{GI}(p)$, the elements $\zeta = c + dj$ of which have a “real” part $c \equiv \Re\{\zeta\}$ and an “imaginary” part $d \equiv \Im\{\zeta\}$.

Definition 2 The unimodular set of $\text{GI}(p)$ is the set of elements $\zeta = (c + dj) \in \text{GI}(p)$, such that $c^2 + d^2 \equiv 1 \pmod{p}$.

Definition 3 Let $\zeta \in \text{GI}(p)$ be a nonzero element with multiplicative order denoted by $\text{ord}(\zeta)$. The finite field cosine and sine related to $\zeta$ are computed modulo $p$, respectively, as $\cos_\zeta(x) := 2^{-1}(\zeta^x + \zeta^{-x})$ and $\sin_\zeta(x) := (2j)^{-1}(\zeta^x - \zeta^{-x})$, $x = 0, 1, \ldots, \text{ord}(\zeta) - 1$.

The above defined finite field trigonometric functions hold properties similar to those of the standard real-valued ones [7]. We remark that it is also possible to define $\text{GI}(p)$ and finite field trigonometric functions for $p \equiv 1 \pmod{4}$. In this case, which is not focused here, a quadratic nonresidue $j^2 \neq -1$ over $\text{GF}(p)$ should be used.

Some aspects related to finite fields are reviewed in Section 2. In Section 3, we explain how to obtain the finite field Hermite-Gaussians and define the 4FT. A simple example is presented in Section 4. The paper closes with some concluding remarks in Section 5.
2.2. The finite field Fourier transform

In what follows, a modified version of the unitary form of the FFFT is considered.

**Definition 4** The finite field Fourier transform of a vector \( \mathbf{x} = [x[i], i = 0, 1, \ldots, N - 1, x[i] \in \text{GF}(p)] \), is a vector \( \mathbf{X} = X[k], k = 0, 1, \ldots, N - 1, X[k] \in \text{GI}(p) \), computed by

\[
X[k] = \sqrt{N^{-1}} \left( \mod{p} \right) \sum_{i=0}^{N-1} x[i] \zeta^{ki},
\]

where \( \zeta \in \text{GI}(p) \) is unimodular and has multiplicative order \( N \), and \( N^{\frac{p-1}{2}} \equiv 1 \pmod{p} \).

We emphasize that, in the above definition, the choice of \( \zeta \) unimodular provides an analogy with the standard discrete Fourier transform (DFT), which uses \( e^{-\frac{j2\pi}{N}k} \) as the transform kernel. The relationship between \( \mathbf{x} \) and \( \mathbf{X} \) can be written as \( \mathbf{X} = F \mathbf{x} \), where \( F \) is the transform matrix.

2.2.1. Eigenstructure of the FFFT

A vector \( \mathbf{x} \) is said to be an eigenvector of the FFFT, with associated eigenvalue \( \lambda \in \text{GI}(p) \), when it satisfies \( \mathbf{X} = \lambda \mathbf{x} \). The FFFT and the DFT have similar eigenstructures, according to the following propositions [8],[9].

**Proposition 1** The \( F \) matrix has, at most, four distinct eigenvalues, \( \{1, -1, j, -j\} \), computed in \( \text{GI}(p) \), the multiplicities of which are presented in Table 1.

<table>
<thead>
<tr>
<th>( N )</th>
<th>Mult. 1</th>
<th>Mult. -1</th>
<th>Mult. j</th>
<th>Mult. -j</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 \cdot n</td>
<td>( n + 1 )</td>
<td>( n )</td>
<td>( n - 1 )</td>
<td>( n )</td>
</tr>
<tr>
<td>4 \cdot n + 1</td>
<td>( n + 1 )</td>
<td>( n )</td>
<td>( n )</td>
<td>( n )</td>
</tr>
<tr>
<td>4 \cdot n + 2</td>
<td>( n + 1 )</td>
<td>( n + 1 )</td>
<td>( n )</td>
<td>( n )</td>
</tr>
<tr>
<td>4 \cdot n + 3</td>
<td>( n + 1 )</td>
<td>( n + 1 )</td>
<td>( n + 1 )</td>
<td>( n + 1 )</td>
</tr>
</tbody>
</table>

**Proposition 2** Every eigenvector of the \( F \) matrix is even or odd symmetric. Even eigenvectors are related to the eigenvalues \( 1 \) or \(-1\); odd eigenvectors are related to \( j \) or \(-j\).

3. THE FINITE FIELD FRACTIONAL FOURIER TRANSFORM

Similarly to the real discrete case, the finite field fractional Fourier transform is defined through a spectral expansion analogous to that used to define the continuous fractional Fourier transform, i.e., the 4FT matrix has the form

\[
F^a[m, n] = \sum_{k=0}^{N-1} v_k[m](\lambda_k)^a v_k[n],
\]

for \( m, n = 0, \ldots, N - 1 \). In the last equation, where all computations are evaluated in \( \text{GI}(p) \), the vectors \( v_k = v_k[i] \) constitute an arbitrary orthonormal eigenvector set of the \( F \) matrix, with associated eigenvalues \( \lambda_k \). By analogy with the continuous and discrete cases, if we take \( \lambda_k = j^k \), the validation of the properties mentioned in the introduction of this paper is provided; the order \( a = b/c \), where \( b \) and \( c \) are integers, must be a number such that \( j^{ka} = \sqrt{\frac{j^{kb}}{p}} \in \text{GI}(p) \).

In the finite field case, we also have to deal with the nonuniqueness of the above referred eigenvector set, because the respective eigenvalues are degenerated (see Proposition 1). In order to do this, in the next section, we reproduce in the finite field context the derivation of the discrete counterparts of the Hermite-Gaussian functions [4].

3.1. Finite field Hermite-Gaussians

In the continuous fractional Fourier transform, a commuting operator is used for finding an eigenfunction set of the Fourier transform. Here, analogously to the FRT, the respective commuting operator is

\[
S = \delta^2 + F\delta^2 F^{-1},
\]

which is discrete and, additionally, is taken over the field \( \text{GI}(p) \). In Equation (2), \( \delta^2 \) denotes a second difference operator also computed modulo \( p \), that is \( \delta^2 f_k = f_{k+1} - 2f_k + f_{k-1} \). The indexes of \( \delta^2 \) are cyclic with period \( N \). Therefore, applying the time-shifting property of the FFFT, the operator \( F\delta^2 F^{-1} \) can be expressed as

\[
F\delta^2 F^{-1} = \alpha^k - 2 + \alpha^{-k} = 2[\cos(\zeta(k) - 1)]
\]

where the unimodular element \( \zeta \in \text{GI}(p) \) has multiplicative order \( \text{ord}(\zeta) = N \). From Equations (2) and (3), we write the eigenvalue equation for \( S \), \( Sx_k = \lambda x_k \), which gives

\[
x_{k+1} + 2[\cos(\zeta(k) - 1)]x_k + x_{k-1} = \lambda x_k.
\]

For \( k = 0, 1, \ldots, N - 1 \), from the above equation, we conclude that

\[
S = \begin{bmatrix}
C_0 & 1 & 0 & \ldots & 1 \\
1 & C_1 & 1 & \ldots & 0 \\
0 & 1 & C_2 & \ldots & 0 \\
: & : & : & \ddots & : \\
1 & 0 & 0 & \ldots & C_{N-1}
\end{bmatrix},
\]

where \( C_n = 2[\cos(\zeta(n) - 2)] \). It is simple to demonstrate that the matrices \( S \) and \( F \) commute (we omit such a demonstration here). This fact ensures the existence of a common eigenvector set between them.

In order to show that such a common eigenvector set is unique, the symmetry properties of the eigenvectors of \( F \) are considered. Based on Proposition 2, the nonzero entries of the matrix \( P \), which decomposes an arbitrary vector into its even and odd components, are given by the following rules:
• For $N$ even, $P_{i,i} = 1$, $i = 1, \frac{N}{2}$; $P_{i,i} = \sqrt{2-1}$, $i = 2, \ldots, \frac{N}{2}$; $P_{i,i} = -\sqrt{2-1}$, $i = \frac{N}{2} + 2, \ldots, N$; $P_{N-i,i+2} = \sqrt{2-1}, i = 0, \ldots, N-2, i \neq \frac{N}{2} - 1$.

• For $N$ odd, $P_{1,1} = 1$; $P_{i,i} = \sqrt{2-1}$, $i = 2, \ldots, \lfloor \frac{N}{2} + 1 \rfloor$; $P_{i,i} = -\sqrt{2-1}$, $i = \lfloor \frac{N}{2} + 2 \rfloor, \ldots, N$; $P_{N-i,i+2} = \sqrt{2-1}, i = 0, \ldots, N-2$.

The notation $\lfloor \cdot \rfloor$ represents the greatest integer less than or equal to the argument. In any case, $P$ satisfies $P = P^T = P^{-1}$ and the similarity transformation

$$PSP^{-1} = \begin{bmatrix} \text{Ev} & 0 \\ 0 & \text{Od} \end{bmatrix}$$

produces symmetric tridiagonal matrices $\text{Ev}$ and $\text{Od}$ with dimensions $\lfloor (N/2 + 1) \rfloor$ and $\lfloor (N/2 - 1) \rfloor$ respectively. Basically, this fact depends on the symmetry properties and the positions of the nonzero entries of the matrices $S$ and $P$. Therefore, in the finite field context, the equivalence between the mentioned transformation and the right-hand side of Equation (5) can be demonstrated as a simple extension of the real-valued case [4].

The even-odd orthogonal eigenvector set of $S$ is unique because tridiagonal matrices, also in a finite field, have distinct eigenvalues [10]. Specifically, the even eigenvectors of $S$ are obtained as

$$u_{2k} = P \begin{bmatrix} e_k^T & 0 \ldots & 0 \end{bmatrix}^T, k = 0, \ldots, [N/2],$$

(6)

where $e_k$ is an eigenvector of $\text{Ev}$; the odd eigenvectors of $S$ are obtained as

$$u_{2k+1} = P \begin{bmatrix} 0 \ldots & 0 & o_k^T \end{bmatrix}^T, k = 0, \ldots, [N/2 - 2],$$

(7)

where $o_k$ is an eigenvector of $\text{Od}$. If $N$ is even, the vector $u_{N-1}$ is null.

Similarly to the discrete fractional Fourier transform, the eigenvectors $u_k, k = 0, \ldots, 2[N/2]$, must be conveniently ordered. Obviously, in the present context, such a procedure cannot be based on the number of zero-crossings [4]; it is not possible to perform any numerical comparison between the eigenvectors of $S$ and the Hermite-Gaussian functions. Indeed, the unique important fact to be considered is that such eigenvectors (the finite field Hermite-Gaussians) correspond to the $F$ matrix eigenvector set we are looking for. In this sense, ordering the eigenvectors $u_k$ only requires the correspondence, in Equation (1), between the eigenvalue to which a given eigenvector is associated and the number $\lambda_k = j^k$. Since the sequence $j^k$, where $k$ is integer, has period equal to 4, different orderings may be possible.

In order to clarify the above idea, let us denote the ordered eigenvector set by $v_k, k = 0, \ldots, 2[N/2]$. As an example, if the eigenvector $u_2$ is related to the eigenvalue $\lambda_{u_2} = 1$, any association with the form $v_{4k+3} = u_2, 4k + 3 \leq 2[N/2]$, is valid; if the eigenvector $u_3$ is related to the eigenvalue $\lambda_{u_3} = -j$, any association with the form $v_{4k+3} = u_3, 4k + 3 \leq 2[N/2]$, is valid, and so on.

Moreover, it is important to remark that the matrix $F^a$ has to be unitary. This means that the eigenvectors $v_k$ should be normalized, before being used in Equation (1). However, in the present framework, the normalization of a vector has a particularity. If we define the norm of the vector $v_k = v_k[i]$, $i = 0, \ldots, N-1, v_k[i] \in \mathbb{GF}(p)$, as

$$\|v_k\| = \sqrt{v_k[0]^2 + v_k[1]^2 + \ldots + v_k[N-1]^2} \mod p,$$

$\|v_k\|$ will be “complex”, in case the argument of the square root is a quadratic nonresidue. Thus, the “normalized” version of $v_k$, i.e., $\|v_k\|^{-1}v_k \mod p$, could have norm 1 or $p-1$. Due to this possibility, we have chosen to include the scaling factor $\|v_k\|^{-2} \mod p$ in Equation (1), instead of normalizing each eigenvector before using them in the referred equation. This modification is shown in the next section.

3.2. Finite field fractional Fourier transform

After including in Equation (1) the above described adjustments, the finite field fractional Fourier transform over $\mathbb{GF}(p)$ can be given in terms of its transform matrix as

$$F^a[m,n] = \sum_{k=0}^{2[N/2]} \|v_k\|^{-2}v_k[m]j^{kn}v_k[n],$$

(8)

for $m, n = 0, \ldots, N-1; v_k, \|v_k\| \neq 0$, is an eigenvector of $S$ related to the eigenvalue $j^k$.

4. AN EXAMPLE

In order to illustrate the procedure we have described through the present paper, in this section, we develop a simple example for the finite field fractional Fourier transform. Initially, the prime number $p = 47$ is considered and the unimodular element $\zeta = 24 + 6j$ with multiplicative order $N = 6$ in $\mathbb{GF}(47)$ is chosen. According to Equation (4), we get

$$S = \begin{bmatrix} 45 & 1 & 0 & 0 & 0 & 1 \\ 1 & 44 & 1 & 0 & 0 & 0 \\ 0 & 1 & 42 & 1 & 0 & 0 \\ 0 & 0 & 1 & 41 & 1 & 0 \\ 0 & 0 & 0 & 1 & 42 & 1 \\ 1 & 0 & 0 & 0 & 1 & 44 \end{bmatrix}.$$  

Following the presented rules, the matrix

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 27 & 0 & 0 & 0 & 27 \\ 0 & 0 & 27 & 0 & 27 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 27 & 0 & 20 & 0 \\ 0 & 27 & 0 & 0 & 0 & 20 \end{bmatrix}$$
is constructed and, from the similarity transformation $PSP^{-1}$, the matrices
\[
\mathbf{Ev} = \begin{bmatrix}
4 & 5 & 7 & 0 & 0 \\
7 & 44 & 1 & 0 \\
0 & 1 & 42 & 7 \\
0 & 0 & 7 & 41
\end{bmatrix}
\text{ and } \mathbf{Od} = \begin{bmatrix}
42 & 1 \\
1 & 44
\end{bmatrix}
\]
are obtained. The eigenvalues of $\mathbf{Ev}$ are $\{2, 12, 27, 37\}$ and the eigenvalues of $\mathbf{Od}$ are $\{3, 36\}$. The eigenvectors of such matrices are shown in Table 2.

**Table 2.** Eigenvectors of the tridiagonal matrices $\mathbf{Ev}$ and $\mathbf{Od}$ ($p = 47, \zeta = 24 + 6j, N = 6$).

<table>
<thead>
<tr>
<th>$k$</th>
<th>$e_k$</th>
<th>$\alpha_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>[1 14 16 14]</td>
<td>[1 8]</td>
</tr>
<tr>
<td>1</td>
<td>[1 2 23 2]</td>
<td>[1 41]</td>
</tr>
<tr>
<td>2</td>
<td>[1 31 30 32]</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>[1 19 1 10]</td>
<td>-</td>
</tr>
</tbody>
</table>

Using Equations (6) and (7), the eigenvectors $u_k$, $k = 0, \ldots, 6$, which constitutes the even-odd orthogonal eigenvector set of the matrix $\mathbf{S}$, are obtained. Such eigenvectors and their associated eigenvalues are shown in Table 3. In this example, by observing the third column of the table, we form the ordered eigenvector set $v_k$, $k = 0, \ldots, 6$, according to $v_{2k} = u_{2k}$, $k = 0, \ldots, 3$, $v_1 = u_3$ and $v_3 = u_1$. At this point, we have all information required to obtain the 4FT matrix using Equation (8), for a given value of $a$.

**Table 3.** Even-odd orthogonal eigenvector set of the matrix $\mathbf{S}$ and associated eigenvalues ($p = 47, \zeta = 24 + 6j, N = 6$).

<table>
<thead>
<tr>
<th>$k$</th>
<th>$u_k$</th>
<th>$\lambda_{u_k}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>[1 2 9 14 9 2]</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>[0 28 27 0 20 19]</td>
<td>$-j$</td>
</tr>
<tr>
<td>2</td>
<td>[1 7 10 22 10 7]</td>
<td>$-1$</td>
</tr>
<tr>
<td>3</td>
<td>[0 26 27 0 20 21]</td>
<td>$j$</td>
</tr>
<tr>
<td>4</td>
<td>[1 38 11 32 11 38]</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>[0 0 0 0 0 0]</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>[1 43 27 10 27 43]</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

**5. CONCLUDING REMARKS**

In this paper, we have introduced a finite field version for the fractional Fourier transform. Several concepts required to define the 4FT were developed in analogy with the usual fractional Fourier transforms. Additionally, other aspects exclusively related to the finite field scenario were discussed and incorporated to the mentioned definition.

We believe that the finite field fractional Fourier transform is a promising mathematical tool and can be used in manifold applications in Engineering. With this purpose, further investigations concerning the 4FT should include, among other topics, a more detailed study of its properties, the development of algorithms for its fast computation and the elucidation of the meaning of varying the order $a$ in the finite field framework. Also in this context, other fractional transforms such as the cosine and sine transforms should be studied.

**6. REFERENCES**


