Blind Sequence Separation Based on the Eigenstructure of Finite Field Transforms

Juliano B. Lima, Ricardo M. Campello de Souza and Daniel Panario

***Abstract*— A blind sequence separation method based on the eigenstructure of finite field transforms is proposed. In analogy with a multiuser communication system, an additive channel is considered and the information coming from each user is mapped on eigenvectors of a transform matrix. Since orthogonal eigenspaces are related to different users, it is possible to separate such eigenvectors after the channel addition. The recently introduced finite field trigonometric transforms are used. Their eigenstructure is analyzed and applied to the described scenario.**

***Keywords*— Blind separation, multiuser communication, finite field transforms, eigenstructure.**

***Resumo*— Este trabalho propõe um método para separação cega de seqüências baseado em transformadas de corpo finito. Analogamente a um sistema de comunicação multiusuário, considera-se um canal aditivo através do qual as informações são transmitidas como autovetores de uma matriz de transformação. Uma vez que subespaços vetoriais ortogonais estão relacionados a usuários distintos, é possível separar tais autovetores após a adição no canal. As transformadas trigonométricas de corpo finito, recentemente introduzidas, são usadas. Sua auto-estrutura é analisada e aplicada ao cenário descrito.**

***Palavras-Chave*— Separação cega, comunicação multiusuário, transformadas de corpo finito, auto-estrutura.**

I. INTRODUCTION

Multiple access techniques perform an essential role in modern communication systems. The simultaneous use of a channel by different transmitters allows a flexible design of such systems and the reasonable allocation of the available resources [1]. In a code division multiple access system (CDMA), different users share, at the same, time the same frequency band. This is possible due to the spread spectrum technique which uses high rate *signature pulses* to enhance the signal bandwidth far beyond what is necessary for a given data rate. The users can be separated at the receiver by means of their characteristic individual signatures. Commonly, this separation is done without any explicit knowledge concerning the information coming from each user, that is, a *blind* recovery is performed [1]. Nowadays, the most prominent applications of CDMA are mobile communication systems like cdmaOne, UMTS or cdma2000 [2].

In [3], a new multiuser communication technique was proposed. It is based on the eigenstruture of the discrete Fourier transform (DFT) matrix [4]. A noise-free real additive channel is considered and the user signatures are eigenvectors of the DFT matrix; distinct eigenvalues are associated to each user and, after the channel addition, the corresponding eigenvectors are separated by solving a linear system of equations. Since the knowledge of the sequence resulting from the eigenvectors addition is sufficient for performing such a separation, this procedure can be viewed as blind. In this case, the maximum number of simultaneous users is four, because the DFT matrix has at most four distinct eigenvalues: $\{1, -1, j, -j\}$.

Other discrete transforms applicable to the described scenario have been investigated [5]. This paper proposes the use of the recently introduced finite field trigonometric transforms (FFTT), which include finite field cosine and sine transforms [6]. Since FFTT matrices have only integer elements, floating-point and complex arithmetic operations are avoided and a more natural adjustment to the digital systems context is provided. Furthermore, some of the FFTT types have matrices with more than four distinct eigenvalues.

The key-point for developing the reported separation procedure is the knowledge of the eigenstructure of the used transforms. Therefore, a considerable part of this paper is dedicated to the study of the eigenvalues of each FFTT and of the systematic ways for constructing their respective eigenvectors. Under many aspects, this theory is similar to that of the real-valued trigonometric transforms, the eigenstructures of which have been studied with the main purpose of defining fractional transforms [7], [8], [9].

This paper is organized as follows. In Section II, the finite field trigonometric transforms are briefly reviewed. In Sections III and IV, respectively, the eigenstructures of types I and IV FFTT are studied. In Section V, the eigenstructures of types II and III FFTT are investigated. Section VI presents the blind sequence separation procedure based on the eigenstructure of the FFTT and some preliminary discussions of its practical aspects. The paper closes with some concluding remarks in Section VII.

II. PRELIMINARIES

A. Finite Field Trigonometry

In this subsection, the main concepts related to the finite field trigonometry are reviewed [10].

Definition 1: The set of Gaussian integers over GF(p) is the set GI(p) $= \{a + jb, a, b \in \text{GF}(p)\}$, where p is a prime such that $j^2 = -1$ is a quadratic nonresidue over GF(p), i.e., $p \equiv 3 (\text{mod } 4)$ [11].

The extension field GF(p^2) is isomorphic to the "complex" structure GI(p), whose elements $\zeta = a + jb$ have a "real" part $a = \Re\{\zeta\}$ and an "imaginary" part $b = \Im\{\zeta\}$ [12].

Juliano B. Lima e Ricardo M. Campello de Souza, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brasil, E-mails: juliano_bandeira@ieee.org, ricardo@ufpe.br.

Daniel Panario, School of Mathematics and Statistics, Carleton University, Ottawa, Canada, E-mail: daniel@math.carleton.ca.

Definition 2: Let ζ be a nonzero element of GI(p) of multiplicative order denoted by $\mathrm{ord}(\zeta)$. The k-trigonometric functions cosine and sine of the "arc" of the element ζ^i are computed modulo p, respectively, as $\cos_\zeta(x) := (\zeta^x + \zeta^{-x})/2$ and $\sin_\zeta(x) := (\zeta^x - \zeta^{-x})/2j$, for $x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$.

For the sake of simplicity, the k-trigonometric functions are denoted by $\cos_k(i)$ and $\sin_k(i)$, while the value of ζ is fixed. The k-cosine and the k-sine hold properties similar to those of the standard real-valued trigonometric functions [10].

Definition 3: The unimodular set of GI(p) is the set of elements $\zeta = (a + jb) \in \mathrm{GI}(p)$, such that $a^2 + b^2 \equiv 1 (\mathrm{mod}\, p)$.

B. Finite Field Trigonometric Transforms

The finite field trigonometric transforms include eight cosine transforms (FFCT) and eight sine transforms (FFST). The first defined FFTT, corresponding to the FFCT-II, was introduced by Mahon *et al.* [13]. Later, new definitions were given and some applications were investigated [6], [14]. In this subsection, the main FFTT types are briefly reviewed.

Any FFTT of a vector $\mathbf{x} = (x_i)$, $x_i \in$ GF(p), can be written as a vector $\mathbf{X} = (X_k)$, $X_k \in$ GI(p), obtained from the equation

$$\mathbf{X} = \mathbf{M} \cdot \mathbf{x}^T, \tag{1}$$

where $\mathbf{M}$ is the respective transform matrix. The transform matrix denoted by $\mathbf{FC}^I_{N+1}$, for instance, is associated to the computation of the FFCT-I of an $N + 1$ length vector; analogously, the matrix $\mathbf{FS}^{III}_N$ is associated to the FFST-III of an N length vector. Such matrices are obtained according to Table I, where the indexes i and k are respectively related to the columns and rows; the weight function β_r is defined as

$$\beta_r = \begin{cases} \sqrt{2^{-1}} \,(\mathrm{mod}\, p), & r = 0 \text{ or } N, \\ 1, & r = 1, 2, \ldots, N-1 \end{cases}$$

Since the matrices are unitary, types I and IV FFTT, the matrices of which are also symmetric, correspond to involutions. Such matrices are elements of order 2 in the general linear group GL(N,GI(p)) [15]. Commonly, an element the order of which is r is said to be a matrix of period r. The inverse FFCT-II matrix, which is not symmetric, corresponds to the forward FFCT-III matrix and vice-versa. This is also valid for FFST-II and FFST-III. Additionally, we remark that, if ζ is unimodular, number theoretic transforms can be obtained [6].

TABLE I
FINITE FIELD TRIGONOMETRIC TRANSFORMS

Transform matrix elements	Matrix dimensions
$\mathbf{FC}^I_{N+1} = \sqrt{2/N}\,\beta_i\beta_k \cos_k(i)$	$k, i = 0, 1, \ldots, N$
$\mathbf{FC}^{II}_N = \sqrt{2/N}\,\beta_k \cos_k\left(i + \frac{1}{2}\right)$	$k, i = 0, 1, \ldots, N-1$
$\mathbf{FC}^{III}_N = \sqrt{2/N}\,\beta_i \cos_{k+\frac{1}{2}}(i)$	$k, i = 0, 1, \ldots, N-1$
$\mathbf{FC}^{IV}_N = \sqrt{2/N}\,\cos_{k+\frac{1}{2}}\left(i + \frac{1}{2}\right)$	$k, i = 0, 1, \ldots, N-1$
$\mathbf{FS}^I_{N-1} = \sqrt{2/N}\,\sin_k(i)$	$k, i = 1, 2, \ldots, N-1$
$\mathbf{FS}^{II}_N = \sqrt{2/N}\,\beta_k \sin_k\left(i + \frac{1}{2}\right)$	$k = 1, 2, \ldots, N$ $i = 0, 1, \ldots, N-1$
$\mathbf{FS}^{III}_N = \sqrt{2/N}\,\beta_i \sin_{k+\frac{1}{2}}(i)$	$k = 0, 1, \ldots, N-1$ $i = 1, 2, \ldots, N$
$\mathbf{FS}^{IV}_N = \sqrt{2/N}\,\sin_{k+\frac{1}{2}}\left(i + \frac{1}{2}\right)$	$k, i = 0, 1, \ldots, N-1$

III. EIGENSTRUCTURE OF TYPE I FFTT

Similarly to the real case, the FFCT-I and the FFST-I eigenstructure is strongly connected to the finite field Fourier transform (FFFT) [16], [8], [17]. The FFFT of a vector $\mathbf{x} = (x_i)$, $i = 0, \ldots, N-1$, $x_i \in$ GF(p), is a vector $\mathbf{X} = (X_k)$, $X_k \in$ GF(p^m), $k = 0, \ldots, N-1$, computed by Equation (1), with the transform matrix $\mathbf{M}$ substituted by

$$\mathbf{FF}_N = \sqrt{N^{-1}} \cdot \alpha^{i \cdot k}, \tag{2}$$

where $\alpha \in$ GF(p^m) and ord(α) $= N$.

Proposition 1: The FFFT transform matrix has, at most, four distinct eigenvalues, $\{1, -1, j, -j\}$, whose multiplicities are presented in Table II [17].

TABLE II
MULTIPLICITIES OF THE EIGENVALUES OF AN $N \times N$ FINITE FIELD FOURIER TRANSFORM MATRIX.

N	Mult. of 1	Mult. of -1	Mult. of j	Mult. of $-j$
$4 \cdot n$	$n+1$	n	n	$n-1$
$4 \cdot n+1$	$n+1$	n	n	n
$4 \cdot n+2$	$n+1$	n	$n+1$	n
$4 \cdot n+3$	$n+1$	$n+1$	$n+1$	n

Proposition 2: Every eigenvector associated to the FFFT has even or odd symmetry. Even eigenvectors are related to the eigenvalues 1 or -1 and odd eigenvectors are related to the eigenvalues j or $-j$ [17].

In this work, procedures for constructing FFFT eigenvectors are not discussed. However, we remark that, in this case, an even symmetric vector $\mathbf{x}_e = (x_{e,i})$ holds the condition $x_{e,i} = x_{e,-i}$; similarly, an odd symmetric vector $\mathbf{x}_o = (x_{o,i})$ holds $x_{o,i} = -x_{o,-i}$ [17]. Based on Propositions 1 and 2, the following propositions related to the FFCT-I and the FFST-I eigenstructure are presented.

Proposition 3: The FFCT-I and FFST-I eigenvectors are constructed from the FFFT eigenvectors according to the following relations.

- If $\mathbf{x} = [x_0, x_1, \ldots, x_{N-2}, x_{N-1}, x_{N-2}, \ldots, x_1]$ is an even eigenvector of the matrix $\mathbf{FF}_{2N-2}$, then

$$\mathbf{x}_{\mathbf{FC}_I} = \left[x_0, \sqrt{2}x_1, \ldots, \sqrt{2}x_{N-2}, x_{N-1}\right] \tag{3}$$

  is an eigenvector of the matrix $\mathbf{FC}^I_N$.
- If $\mathbf{x} = [0, x_1, x_2, \ldots, x_N, 0, -x_N, -x_{N-1}, \ldots, -x_1]$ is an odd eigenvector of the matrix $\mathbf{FF}_{2N+2}$, then

$$\mathbf{x}_{\mathbf{FS}_I} = \sqrt{2}\,[x_1, x_2, \ldots, x_N] \tag{4}$$

  is an eigenvector of the matrix $\mathbf{FS}^I_N$ with associated eigenvalue $j\lambda$.

  Proof: It is similar to the proof of Proposition 3 in [8]. ■

TABLE III
MULTIPLICITIES OF THE EIGENVALUES OF A TYPE I $N \times N$ FINITE FIELD COSINE OR SINE TRANSFORM MATRIX.

N	Mult. of 1	Mult. of -1
odd	$\frac{N+1}{2}$	$\frac{N-1}{2}$
even	$\frac{N}{2}$	$\frac{N}{2}$

Proposition 4: The FFCT-I and the FFST-I matrices have only the eigenvalues 1 and -1. Their multiplicities are presented in Table III.

Proof: As we previously remarked, the FFCT-I is involutive, i.e., $(\mathbf{FC}_N^I)^2 = \mathbf{I}_N$, where $\mathbf{I}_N$ is the $N \times N$ identity matrix. Hence, the eigenvalues of $\mathbf{FC}_N^I$ are the solutions of $\lambda^2 = 1$, i.e., $\{-1, 1\}$. The same argument is valid for $\mathbf{FS}_N^I$. The multiplicities of the eigenvalues can be determined using a proof similar to that presented for the Proposition 4 in [8]. ■

IV. EIGENSTRUCTURE OF TYPE IV FFTT

In this section, the FFCT-IV and the FFST-IV eigenstructure is discussed. In this case, there is also a connection with the eigenvalues and the eigenvectors of the finite field Fourier transform. Therefore, a generalized finite field Fourier transform (GFFFT) is defined. Initially, the eigenstructure of the GFFFT is analyzed and, hence, propositions concerning the FFCT-IV and the FFST-IV eigenstructure are derived.

A. The Generalized Finite Field Fourier Transform

The GFFFT of a vector $\mathbf{x} = (x_i)$, $x_i \in$ GF(p), is a vector $\mathbf{X} = (X_k)$, $X_k \in$ GF(p^m), computed by Equation (1), with the matrix $\mathbf{M}$ substituted by

$$\mathbf{FF}_N^G = \sqrt{N^{-1}} \cdot \alpha^{\left(i+\frac{1}{2}\right)\cdot\left(k+\frac{1}{2}\right)}, \tag{5}$$

where $\alpha \in$ GF(p^m) and ord(α) $= N$. The inverse of $\mathbf{FF}_N^G$ is

$$\left(\mathbf{FF}_N^G\right)^{-1} = \sqrt{N^{-1}} \cdot \alpha^{-\left(i+\frac{1}{2}\right)\cdot\left(k+\frac{1}{2}\right)}. \tag{6}$$

In the following, some properties used for studying the $\mathbf{FF}_N^G$ eigenstructure are presented.

Property 1: Let $\mathbf{J}$ be an $N \times N$ anti-diagonal matrix, where every nonzero element equals 1. Then, $(\mathbf{FF}_N^G)^2 = -\mathbf{J}$.

Proof: It is similar to the proof of Fact 1 in [7]. ■

Based on Property 1 and denoting by $x_i \overset{G}{\longleftrightarrow} X_k$ the relation between $\mathbf{x}$ and its generalized finite field Fourier transform $\mathbf{X}$, the relation $X_i \overset{G}{\longleftrightarrow} -x_{-k-1}$ is valid.

In order to analyze the GFFFT of symmetric vectors, differently from the FFFT, we consider even symmetric vectors $\mathbf{x}_e$ holding the condition $x_{e,i} = x_{e,-i-1}$. They can be constructed from any vector $\mathbf{x}$ by $x_{e,i} = \mathcal{E}\{x_i\} = 2^{-1} \cdot (x_i + x_{-i-1})$; symmetric odd vectors hold $x_{o,i} = -x_{o,-i-1}$ and they can be obtained by $x_{o,i} = \mathcal{O}\{x_i\} = 2^{-1} \cdot (x_i - x_{-i-1})$.

Property 2: If $x_i \overset{G}{\longleftrightarrow} X_k$, then, the relations $\mathcal{E}\{x_i\} \overset{G}{\longleftrightarrow} \mathcal{E}\{X_k\}$ and $\mathcal{O}\{x_i\} \overset{G}{\longleftrightarrow} \mathcal{O}\{X_k\}$ are valid.

Proof: This property can be demonstrated using Equation (5) and the established symmetry conditions. ■

Proposition 5: The GFFFT matrix has, at most, four distinct eigenvalues, $\{1, -1, j, -j\}$, the multiplicities of which are presented in Table IV.

TABLE IV
MULTIPLICITIES OF THE EIGENVALUES OF AN $N \times N$ GENERALIZED FINITE FIELD FOURIER TRANSFORM MATRIX.

N	Mult. of 1	Mult. of -1	Mult. of j	Mult. of $-j$
$4 \cdot n$	n	n	n	n
$4 \cdot n + 1$	n	n	n	$n+1$
$4 \cdot n + 2$	$n+1$	n	n	$n+1$
$4 \cdot n + 3$	$n+1$	n	$n+1$	$n+1$

Proof: Using Property 1, we know that $(\mathbf{FF}_N^G)^4 = \mathbf{I}_N$. Consequently, the eigenvalues of $\mathbf{FF}_N^G$ correspond to the solutions of $\lambda^4 = 1$, i.e., $\{1, -1, j, -j\}$. Their multiplicities are determined using a proof similar to that presented for Fact 3 in [7]. ■

Proposition 6: The eigenvectors of the GFFFT matrix are constructed according to the following rules. If $x_i \overset{G}{\longleftrightarrow} X_k$, then:

- the even symmetric vector $\mathbf{x}_G = \mathcal{E}\{x_i\} \mp j \cdot \mathcal{E}\{X_i\}$ is an eigenvector of the matrix $\mathbf{FF}_N^G$ associated to the eigenvalue $\lambda = \pm j$.
- the odd symmetric vector $\mathbf{x}_G = \mathcal{O}\{x_i\} \pm \mathcal{O}\{X_i\}$ is an eingenvector of the matrix $\mathbf{FF}_N^G$ associated to the eigenvalue $\lambda = \pm 1$.

Proof: The proof is based on Properties 1 and 2. It is similar to those presented for Propositions 3 and 4 in [3]. ■

B. Eigenvalues and Eigenvectors of Type IV FFTT

Based on the GFFFT eigenstructure, the following propositions related to the FFCT-IV and the FFST-IV eigenstructure are presented.

Proposition 7: The FFCT-IV and the FFST-IV eigenvectors are constructed from the GFFFT eigenvectors according to the following relations.

- If $\mathbf{x} = [x_0, \ldots, x_{N-1}, -x_{N-1}, \ldots, -x_0]$ is an odd eigenvector of the matrix $\mathbf{FF}_{2N}^G$, then

$$\mathbf{x}_{\mathbf{FC}_{IV}} = [x_0, \ldots, x_{N-1}] \tag{7}$$

  is an eigenvector of the matrix $\mathbf{FC}_N^{IV}$.
- If $\mathbf{x} = [x_0, \ldots, x_{N-1}, x_{N-1}, \ldots, x_0]$ is an even eigenvector of the matrix $\mathbf{FF}_{2N}^G$, then

$$\mathbf{x}_{\mathbf{FS}_{IV}} = [x_0, \ldots, x_{N-1}] \tag{8}$$

  is an eigenvector of the matrix $\mathbf{FS}_N^{IV}$.

Proof: It is based on the same principles applied to demonstrate Proposition 3. ■

Proposition 8: The FFCT-IV and the FFST-IV transform matrices have only the eigenvalues 1 and -1. Their multiplicities are presented in Table V.

Proof: It is similar to the proof of Proposition 4. ■

TABLE V
MULTIPLICITIES OF THE EIGENVALUES OF AN $N \times N$ TYPE IV FINITE FIELD COSINE OR SINE TRANSFORM MATRIX.

N	Mult. of 1	Mult. of -1
odd	$\frac{N+1}{2}$	$\frac{N-1}{2}$
even	$\frac{N}{2}$	$\frac{N}{2}$

V. TYPES II AND III FFTT EIGENSTRUCTURE

Since types II and III FFTT matrices are not symmetric, in order to analyze their eigenstructures, it is not possible to use arguments similar to those applied to types I and IV FFTT. In fact, the eigenstructure of the real-valued types II and III trigonometric transforms remains unclear, being restricted to some conjectures supported by numerical simulations [9]. In this section, we also discuss a conjecture and investigate some aspects concerning the eigenstructure of the mentioned transforms in the finite field case.

The conventional procedure for obtaining the eigenvalues of a matrix consists in evaluating the roots of its characteristic polynomial. Since the FFTT matrices are orthogonal, the following theorem is valid.

Theorem 1: The characteristic polynomial of an orthogonal matrix modulo p is a reciprocal polynomial $f(\lambda)$.

Proof: It is similar to the proof of Theorem 1 in [5], all computations being modulo p. ■

The polynomial $f(\lambda)$ is also called palindromic, if $f(\lambda) = \lambda^N f(1/\lambda)$, or anti-palindromic, if $f(\lambda) = -\lambda^N f(1/\lambda)$. The computation of the roots of such polynomials is simplified by the use of a variable substitution method reducing its degree by half [18]. Therefore, it is possible to use closed formulas to evaluate the roots of palindromic polynomials with degrees up to 10. In this extreme case, after excluding roots $\pm 1 (\text{mod } p)$, the degree is reduced to 4. For $f(\lambda)$ with degree greater than 10, factorization techniques are used [19].

It has been conjectured, after computing the roots of the characteristic polynomial of the matrix $\mathbf{FC}_N^{II}$ for different values of N, that all eigenvalues of the FFCT-II transform matrix are distinct. This conjecture has also been proposed for the FFCT-III, FFST-II and FFST-III transforms. Moreover, although the considered matrices have all elements in GF(p), their eigenvalues can be located in extension fields [20].

The period of the matrices $\mathbf{FC}_N^{II}$, $\mathbf{FC}_N^{III}$, $\mathbf{FS}_N^{II}$ and $\mathbf{FS}_N^{III}$ can be investigated by writing them in diagonal form. Let us consider again the FFCT-II transform matrix and write it as $\mathbf{FC}_N^{II} = \mathbf{U}\Lambda\mathbf{U}^*$ ($\mathbf{U}$ is a unitary matrix, the columns of which are eigenvectors of $\mathbf{FC}_N^{II}$, and $\mathbf{U}^*$ is its conjugate transpose; Λ is a diagonal matrix whose elements are the eigenvalues of $\mathbf{FC}_N^{II}$). Since $\mathbf{U}^*\mathbf{U} = \mathbf{I}$, powers of $\mathbf{FC}_N^{II}$ can be computed from powers of Λ, which are computed taking the respective power of each element in its main diagonal. Hence, the relation $(\mathbf{FC}_N^{II})^r = \mathbf{U}\Lambda^r\mathbf{U}^*$ holds. The least positive integer r such that $(\mathbf{FC}_N^{II})^r = \mathbf{I}$ also implies $\Lambda^r = \mathbf{I}$. From this condition, we conclude that the period r is the least common multiple among the multiplicative orders of the eigenvalues of $\mathbf{FC}_N^{II}$. For types II and III real-valued trigonometric transforms, there is a conjecture stating that no such r exists [9]. By definition, the periods of types II and III matrices are said to be zero. Naturally, for the FFTT case, r is always positive and finite.

Briefly, we can assert that the computation of types II and III FFTT matrices eigenvalues requires the computation of the roots of the respective charateristic polynomials. In this way, related eigenvectors can be constructed.

VI. BLIND SEQUENCE SEPARATION

In communications theory, the problem of separating information coming from different sources, after they are "mixed" under some assumptions, has been extensively studied [1], [2]. Among different techniques for recovering the data originally transmitted by each user, a particularly interesting case is the separation without explicit knowledge of the information related to each source (or user), that is, the blind separation. When different users share the same frequency band at the same time, well established techniques perform such a separation using statistical properties of sequences and codes used as "digital carriers".

In this section, using the above described scenario as reference, we show how the FFTT eigenstructure can be used for blind sequence separation. We consider a noise free finite field adder channel which is synchronously shared by different users [21]. The procedure consists in associating an eigenvalue and, therefore, a set of eigenvectors of a given FFTT to each user. The information to be sent by an user is mapped on such eigenvectors. Since eigenvectors related to different eigenvalues are orthogonal, after being summed by the channel, they can be recovered by solving a linear system of equations. This scheme is ilustrated in the following subsections.

A. 2-User Scheme

With the purpose of presenting a 2-user scheme, we consider an $N \geq 2$ length FFCT-I, although any other FFTT whose transform matrix has at least 2 distinct eigenvalues can be used. As demonstrated in Section III, the FFCT-I matrix has eigenvalues $\lambda_1 = 1$ and $\lambda_2 = -1$. We asssociate to these eigenvalues and to users 1 and 2, respectively, the eigenvectors $\mathbf{x}_1 = (x_{1,i})$ and $\mathbf{x}_2 = (x_{2,i})$, which are constructed according to Proposition 3.

From the vector $\mathbf{y} = (y_i)$ given by

$$y_i = x_{1,i} + x_{2,i}, \tag{9}$$

where "+" denotes componentwise addition, it is possible to recover the users sequences. By computing $\mathbf{Y} = (Y_k) = \mathbf{FC}_N^I \times \mathbf{y}^T$, we have

$$Y_k = \lambda x_{1,i} + \lambda_2 x_{2,i} = x_{1,i} - x_{2,i}. \tag{10}$$

Solving the linear system formed by Equations (9) and (10), the users sequences are recovered from $x_{1,i} = (y_i + Y_i)/2$ and $x_{2,i} = (y_i - Y_i)/2$. A block diagram ilustrating the recovering of the sequences $\mathbf{x}_1$ and $\mathbf{x}_2$ can be viewed in Figure 1.

An important aspect to be remarked concerns the arithmetic complexity involved in the described procedure. The number

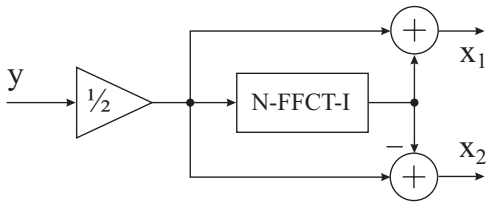

Fig. 1. Sequence recovering in a 2-user scheme.

of multiplications and additions necessary for separating the N-length vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ are, respectively, given by

$$M_2(N) = N + M_{FC^I}(N) \tag{11}$$

and

$$A_2(N) = 2N + A_{FC^I}(N), \tag{12}$$

In the above equations, the subscript "2" indicates the association with the 2-user scheme; $M_{FC^I}(N)$ and $A_{FC^I}(N)$ respectively, denotes the number of multiplications and additions for calculating an N-length FFCT-I, which can be done by fast algorithms. Exact numbers for $M_2(N)$ and $A_2(N)$ can be obtained by using closed formulae for $M_{FC^I}(N)$ and $A_{FC^I}(N)$ [22].

B. 4-User Scheme

According to our previous discussions, we must choose types II or III FFTT for constructing a 4-user scheme. Moreover, if a transform over GF(p) is chosen, the eigenvalues used for implementing such a scheme should also be located in GF(p), in order to avoid computations in extension fields. As an example, let us consider the 4-length FFCT-II over GF(127). If the transform matrix is constructed using the unimodular element $\zeta = 119 + j119$, its eigenvalues are $\lambda_1 = 1$, $\lambda_2 = 20$, $\lambda_3 = 108$ and $\lambda_4 = 126$; the users sequences are, respectively, the eigenvectors $\mathbf{x}_1 = (x_{1,i})$, $\mathbf{x}_2 = (x_{2,i})$, $\mathbf{x}_3 = (x_{3,i})$ and $\mathbf{x}_4 = (x_{4,i})$.

Analogously to the 2-user scheme, the adder channel produces the vector $\mathbf{y} = (y_i)$. By computing successive transforms of $\mathbf{y}$, we have $\mathbf{Y}' = (Y'_k) = \mathbf{FC}_N^{II} \times \mathbf{y}^T$, $\mathbf{Y}'' = (Y''_k) = (\mathbf{FC}_N^{II})^2 \times \mathbf{y}^T$ and $\mathbf{Y}''' = (Y'''_k) = (\mathbf{FC}_N^{II})^3 \times \mathbf{y}^T$. Hence, the following linear system of equations is obtained:

$$\begin{cases} x_{1,i} + x_{2,i} + x_{3,i} + x_{4,i} &= y_i \\ \lambda_1 x_{1,i} + \lambda_2 x_{2,i} + \lambda_3 x_{3,i} + \lambda_4 x_{4,i} &= Y'_i \\ \lambda_1^2 x_{1,i} + \lambda_2^2 x_{2,i} + \lambda_3^2 x_{3,i} + \lambda_4^2 x_{4,i} &= Y''_i \\ \lambda_1^3 x_{1,i} + \lambda_2^3 x_{2,i} + \lambda_3^3 x_{3,i} + \lambda_4^3 x_{4,i} &= Y'''_i. \end{cases}$$

Substituting the values of λ_i, $i = 1, \ldots, 4$, in the above system, we have

$$\begin{cases} x_{1,i} + x_{2,i} + x_{3,i} + x_{4,i} &= y_i \\ x_{1,i} + 20\,x_{2,i} + 108\,x_{3,i} + 126\,x_{4,i} &= Y'_i \\ x_{1,i} + 19\,x_{2,i} + 107\,x_{3,i} + x_{4,i} &= Y''_i \\ x_{1,i} + 126\,x_{2,i} + 126\,x_{3,i} + 126\,x_{4,i} &= Y'''_i, \end{cases}$$

the solutions of which are

$$\begin{aligned} x_{1,i} &= 64\,y_i + 64\,Y'''_i, \\ x_{2,i} &= 49\,y_i + 36\,Y'_i + 78\,Y''_i + 91\,Y'''_i, \\ x_{3,i} &= 36\,y_i + 49\,Y'_i + 91\,Y''_i + 78\,Y'''_i, \\ x_{4,i} &= 106\,y_i + 42\,Y'_i + 85\,Y''_i + 21\,Y'''_i. \end{aligned}$$

Therefore, from $\mathbf{y}$, we obtain $\mathbf{Y}'$, $\mathbf{Y}''$ and $\mathbf{Y}'''$ and use the above equations for recovering each user sequence. A block diagram ilustrating this procedure is shown in Figure 2. The number of multiplications and additions necessary for separating the N-length vectors $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$ and $\mathbf{x}_4$ are, respectively, given by

$$M_4(N) = 7N + 3M_{FC^{II}}(N) \tag{13}$$

and

$$A_4(N) = 8N + 3A_{FC^{II}}(N). \tag{14}$$

In the above equations, $M_{FC^{II}}(N)$ and $A_{FC^{II}}(N)$ denote, respectively, the number of multiplications and additions for calculating an N-length FFCT-II. Following these principles, schemes with a larger number of simultaneous users can be implemented.

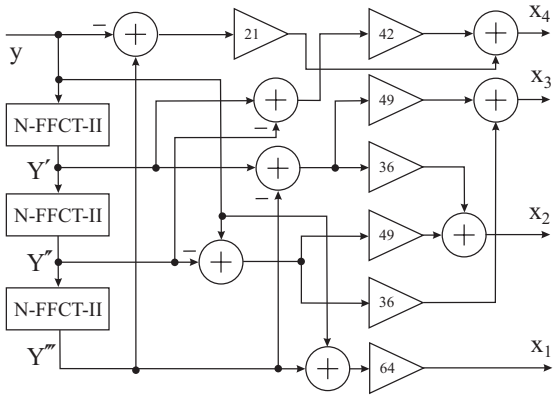

Fig. 2. Sequence recovering in a 4-user scheme.

C. Discussion

1) Computational complexity: Since we assume the eigenvalues used in a specific scheme are fixed, the system of equations from which the users sequences are recovered has to be solved only once. In fact, the solution has to be applied again for each received vector $\mathbf{y}$. However, such a solution is already known. Furthermore, from the previous results, it is possible to conclude that the sequence recovering in schemes using N-length transforms involves $\mathcal{O}(N \log N)$ operations and can be implemented by standard DSPs.

2) A multiuser communication hierarchy over the finite field adder channel: As we remarked, the presented blind sequence separation method restricts the number of simultaneous users of a channel to the number of distinct eigenvalues of the used FFTT. However, similarly to the time division multiplexing (TDM) and the frequency division multiplexing (FDM), it is possible to implement a hierarchic scheme. This strategy

allows a larger number of users being multiplexed, when different signals are combined in order to form a new hierarchic level. Figure 3 ilustrates an example of such a procedure applied to the eigenstructure based multiuser communication. In this case, in order to provide the appropriate diversity of eigenvectors, an extension field mapping and, consequently, a transform over such a field is required.

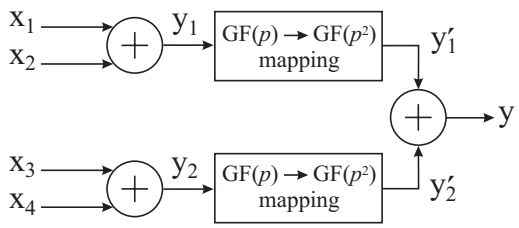

Fig. 3. A two-level hierarchy of the eigenstructure based multiuser communication.

3) Analogy with DS-CDMA: Other interesting aspects of multiuser communication based on FFTT eigenstructures can be revealed by performing a comparison with the direct sequence code division multiple access (DS-CDMA) [1], [2]. In this sense, the above presented schemes can be viewed as DS-CDMA where the spreading sequences (user signatures) are eigenvectors of a finite field transform, instead of Walsh codes or pseudo-noise sequences. Different from DS-CDMA receivers, which use autocorrelation and cross-correlation properties of the spreading sequences, in our approach, the successful separation of each user sequence depends on the orthogonality between distinct eigenspaces.

4) Energy requirements and noisy channel analysis: Although the purpose of this paper is not a complete description of a multiuser communication practical scenario, it is relevant to mention some of its requirements. The maximum allowed energy in the considered channel, for example, would require a limitation over the energy of each used eigenvector. This means that they have to be conveniently scaled. Moreover, a clear definiton of the spreading procedure should be done, which depends on the nature of the information to be mapped on eigenvectors. Finally, since most practical channels cannot be assumed noise free, an error analysis would be necessary. Concerning this point, the eigenvectors of a transform can be treated as words of a linear error-correcting code. This interpretation suggests studying the error susceptibility of the presented schemes as a problem of decoding a linear block code. Preliminary investigations suggest that the error control capacity of a given scheme is related to the number of eigenvalues used. This means an interesting compromise between the number of users that simultaneously access the channel and the error immunity of the system.

VII. Concluding Remarks

In this paper, the eigenstructure of the finite field trigonometric transforms was discussed. As part of the requirements for examining this theme, the generalized finite field Fourier transform was introduced and its eigenstructure was also studied. Blind sequence separation schemes based on the FFTT eigenstructures were shown and their main theoretic aspects were discussed. Implementations of such schemes can be done via standard DSPs. In practical environments, additional aspects concerning the developed theory should be considered. Moreover, other application scenarios for the presented eigenstructures may be investigated. As examples, we cite error correcting codes and public-key watermarking.

References

[1] V. Ipatov, *Spread Spectrum and CDMA Principles and Applications*, Wiley, 2005.

[2] H. Schulze and C. Lüders, *Theory and Applications of OFDM and CDMA*, Wiley, 2005.

[3] R. M. Campello de Souza and H. M. de Oliveira, "Eigensequences for multiuser communication over the real adder channel," in *Proc. of the International Telecommunications Symposium*, Fortaleza, Brasil, 2006.

[4] J. H. McClellan and T. W. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Transactions on Audio and Electroacoustics*, vol. AU-20, no. 1, pp. 66–74, January 1972.

[5] J. B. Lima and R. M. Campello de Souza, "Uma técnica de múltiplo acesso baseado na auto-estrutura das transformadas trigonométricas," in *Anais do XXIII Simpósio Brasileiro de Telecomunicações*, Recife, Brasil, 2007.

[6] J. B. Lima and R. M. Campello de Souza, "New trigonometric transforms over prime finite fields for image filtering," in *Proc. of the International Telecommunications Symposium*, Fortaleza, Brasil, 2006.

[7] C.-C. Tseng, "Eigenvalues and eigenvectors of generalized DFT, generalized DHT and DST-IV matrices," *IEEE Transactions on Signal Processing*, vol. 50, no. 4, pp. 866–877, April 2002.

[8] S.-C. Pei and M. H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Transactions on Signal Processing*, vol. 49, no. 6, pp. 1198–1207, June 2001.

[9] G. Cariolaro, T. Erseghe, and P. Kraniauskas, "The fractional discrete cosine transform," *IEEE Transactions on Signal Processing*, vol. 50, no. 4, pp. 902–911, April 2002.

[10] R. M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, and A. J. A. Paschoal, "Trigonometry in finite fields and a new Hartley transform," in *Proc. IEEE Int. Symp. Information Theory (ISIT'98)*. IEEE, 1998, p. 293.

[11] D. M. Burton, *Elementary Number Theory*, Addison-Wesley Publishing Company, 1994.

[12] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*, Addison-Wesley Reading, 1985.

[13] M. M. Campello de Souza, H. M. de Oliveira, R. M. Campello de Souza, and M. M. Vasconcelos, "The discrete cosine transform over prime finite fields," in *International Conference on Telecommunications*, J. N. Campello de Souza, P. Dini, and P. Lorenz, Eds., Berlin, 2004, Lecture Notes in Computer Science, pp. 482–487, Springer.

[14] J. B. Lima and R. M. Campello de Souza, "Uma marca d'água digital baseada na transformada do cosseno sobre corpos finitos," in *Anais do XXII Simpósio Brasileiro de Telecomunicações*, Campinas, Brasil, 2005.

[15] R. M. Guralnick and M. Lorenz, "Orders of finite groups of matrices," http://www.citebase.org/abstract?id=oai:arXiv.org:math/0511191, 2005.

[16] J. M. Pollard, "The fast Fourier transform in a finite field," *Mathematics of Computation*, vol. 114, no. 25, pp. 82–100, April 1971.

[17] D. T. Birtwistle, "The eigenstructure of the number theoretic transforms," *Signal Processing*, vol. 4, no. 4, pp. 287–294, July 1982.

[18] J. Konvalina and V. Matache, "Palindrome-polynomials with root on the unit circle," *C. R. Math. Acad. Sci. Soc. R. Can.*, vol. 26, no. 2, pp. 39–44, 2004.

[19] J. von zur Gathen and D. Panario, "Factoring polynomials over finite fields: a survey," *J. Symbolic Computation*, vol. 31, no. 1-2, pp. 3–17, January 2001.

[20] G. Z. Karabulut, D. Panario, and A. Yongaçoglu, "Integer to integer Karhunen Loève transform over finite fields," in *Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Montreal, Canada, 2004, pp. 213–216.

[21] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3498–3516, October 2007.

[22] S. C. Chan and K. L. Ho, "Direct method for computing sinusoidal transforms," *IEEE Proceedings*, vol. 137, no. 6, pp. 433–442, December 1990.