Linear Algebra and its Applications 494 (2016) 245–262

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

The eigenstructure and Jordan form of the Fourier transform over fields of characteristic 2 and a generalized Vandermonde-type formula

M. Barone [a], J.B. Lima [b,*], R.M. Campello de Souza [b]

[a] *Department of Mathematics, Federal University of Pernambuco, Av. Jornalista Aníbal Fernandes, S/N – Cidade Universitária, Recife, PE, 50740-560, Brazil*
[b] *Department of Electronics and Systems, Federal University of Pernambuco, Av. da Arquitetura, S/N, 4° andar – Cidade Universitária, Recife, PE, 50740-550, Brazil*

A R T I C L E   I N F O

Article history:
Received 20 April 2015
Accepted 24 December 2015
Available online 21 January 2016
Submitted by P. Semrl

MSC:
12E20
15A18
15B33
43A32

Keywords:
Eigenstructure
Fields of characteristic 2
Vandermonde's formula
Finite field Fourier transforms

A B S T R A C T

In this paper, we describe the eigenstructure and the Jordan form of the Fourier transform matrix generated by a primitive N-th root of unity in a field of characteristic 2. We find that the only eigenvalue is $\lambda = 1$ and its eigenspace has dimension $[\frac{N}{4}]+1$; we provide a basis of eigenvectors and a Jordan basis. The problem has already been solved, for number theoretic transforms, in any other finite characteristic. However, in characteristic 2 classical results about geometric multiplicity do not apply and we have to resort to different techniques in order to determine a basis of eigenvectors and a Jordan basis. We make use of a modified version of the Vandermonde's formula, which applies to matrices whose entries are powers of elements of the form $x + x^{-1}$.

* Corresponding author. Tel.: +55 81 91140396; fax: +55 81 21267650.
E-mail addresses: marco@dmat.ufpe.br (M. Barone), juliano_bandeira@ieee.org (J.B. Lima), ricardo@ufpe.br (R.M. Campello de Souza).

http://dx.doi.org/10.1016/j.laa.2015.12.021

1. Introduction

Fourier transforms defined over finite fields have played an important role in several theoretical and application scenarios [1]. In digital signal processing, for instance, such transforms are usually defined over prime finite fields and known as number-theoretic transforms (NTT); in this framework, NTT are mainly employed in fast algorithms for computing linear convolutions, which can be implemented by using fixed-point arithmetic operations and, in some cases, by means of multiplication-free architectures [2,3]. On the other hand, Fourier transforms defined over extension fields, including fields of characteristic two, are generally related to algebraic codes for data transmission, where they can be used to decode Reed–Solomon codes [4–6]. The finite field Fourier transform (FFFT, henceforth) can also be used in fast algorithms for solving Toeplitz systems of equations [7], fragile watermarking schemes [8], video filtering [9], among other application scenarios. In these contexts, the characterization of the FFFT with respect to its eigenstructure constitutes a relevant research theme and new potential applications for this mathematical tool can be investigated.

In particular, results concerning the eigenstructure of the FFFT contain several gaps and are restricted to Fourier matrices over prime fields $\mathrm{GF}(p)$ of odd characteristic [10]. In the latter, four eigenvalues and explicit bases of the eigenspaces are provided. The interest in resuming investigations related to eigenvectors and eigenvalues of the FFFT is due to their close connection to the recently introduced fractional Fourier transforms over finite fields [11,12]. More specifically, some strategies for defining a fractional FFFT require the construction of an orthonormal set of eigenvectors of the corresponding transform matrix. In this paper, we consider FFFT over fields of characteristic two and present a description of their eigenstructures. The paper is organized as follows: in Section 2, we describe the FFFT matrix and, after setting up notations and providing two examples, we compute its Jordan form, distinguishing two cases, depending on the remainder class of matrix size modulo 4. We also compute the dimension of the eigenspace and show a set of (possibly linearly dependent) eigenvectors. In Section 3, we provide a modified version of the Vandermonde formula for matrices of type $(a_i^j + a_i^{-j})$ over any field and apply the formula to a matrix related to the FFFT matrix, in order to prove the independence of a system of eigenvectors. Finally, in Section 4, we complete the system found to provide a basis for the eigenspace and a Jordan basis.

2. FFFT over fields of characteristic 2: the Jordan form and the dimension of the eigenspace

Definition 1. Let K be any field of characteristic 2. If K is finite, of order 2^r, we will denote it by $\mathrm{GF}(2^r)$. Let $\alpha \in K$ be an element of finite multiplicative order $N > 3$. We define the Fourier transform matrix associated with α to be