Wavelet Transforms Associated with Finite Cyclic Groups

Giuseppe Caire, Robert L. Grossman, *Member, IEEE,* and H. Vincent Poor, *Fellow, IEEE*

***Abstract*— Multiresolution analysis via decomposition on wavelet bases has emerged as an important tool in the analysis of signals and images when these objects are viewed as sequences of complex or real numbers. An important class of multiresolution decompositions are the so-called *Laplacian pyramid* schemes, in which the resolution is successively halved by recursively low-pass filtering the signal under analysis and decimating it by a factor of two. Generally speaking, the principal framework within which multiresolution techniques have been studied and applied is the same as that used in the discrete-time Fourier analysis of sequences of complex numbers. An analogous framework is developed for the multiresolution analysis of finite-length sequences of elements from arbitrary fields. Attention is restricted to sequences of length 2^n for *n* a positive integer, so that the resolution may be recursively halved to completion. As in finite-length Fourier analysis, a cyclic group structure of the index set of such sequences is exploited to characterize the transforms of interest for the particular cases of complex and finite fields. This development is motivated by potential applications in areas such as digital signal processing and algebraic coding, in which cyclic Fourier analysis has found widespread applications.**

***Index Terms*— Multiresolution analysis, wavelet transforms, Laplacian pyramid, finite fields, cyclic groups, quadrature mirror filters.**

I. Introduction

Multiresolution analysis via decomposition on wavelet bases has emerged as an important tool in the analysis of signals and images when these objects are viewed as sequences over the real or complex field [1]–[7]. In particular, these techniques have proven to be superior to traditional Fourier analysis for many applications including, for example, acoustic signal detection [8], seismic signal analysis [9], edge detection in images [10], pattern recognition [11], and image coding [12]. An important class of multiresolution decompositions are the so-called *Laplacian pyramid* schemes [3], [6], [12], in which the resolution is successively halved by recursively low-pass filtering the signal under analysis and decimating it by a factor of two. The residual (i.e., the error incurred) at each stage of this process is referred to as the *detail* at that stage; and the sequence of details formed by this decomposition is the transform of interest. Suitable choice of the filters used in this process renders this transform invertible; and such suitable filters can be characterized through their discrete-time Fourier properties [3], [6].

Generally speaking, the principal framework within which multiresolution techniques have been studied and applied is the same as that used in the discrete-time Fourier analysis of sequences of complex numbers; that is, the sequence to be transformed is viewed as a mapping from the set of integers $\mathcal{Z}$, to the set of complex numbers $\mathcal{C}$. Of course, Fourier analysis can also be performed on finite-length sequences of complex numbers by viewing them as mappings from a finite cyclic group to $\mathcal{C}$ using the discrete Fourier transform (DFT). The DFT and its extension to the situation in which the complex field is replaced with a finite field (which we will refer to collectively as the *cyclic Fourier transform*) are of widespread utility in digital signal processing applications and algebraic coding [13], [14]. The purpose of this paper is to develop an analogous framework for the multiresolution analysis of finite-length sequences of elements from arbitrary fields. In order to preserve the Laplacian pyramid structure described above, we will primarily consider sequences of length 2^n for n a positive integer, so that the resolution may be recursively halved to completion. As in finite-length Fourier analysis, we will exploit a cyclic group structure of the index set of such sequences to characterize the wavelet transforms in the cases of most interest: the complex field and the finite fields. The development of cyclic wavelet transforms for these particular cases is of fundamental interest in view of the central roles played by cyclic Fourier analysis over these fields in the aforementioned applications of digital signal processing and algebraic coding.

This paper is organized as follows. In Section II, we give a brief overview of classical finite-length Fourier analysis. In Section III, we discuss the conventional structure of wavelet bases for multiresolution analysis via a Laplacian pyramid scheme of discrete-time series of numbers from the complex field, and we describe a finite-length version of this structure. Section IV treats the extension of the discrete-time wavelet transform to a cyclic wavelet transform for finite-length sequences of complex numbers. In this extension, it is assumed that the data length is a power of two, and multiresolution analysis is based on successive application of filtering and decimation in time by two, as noted above. In Section V, the cyclic wavelet transform is extended to finite fields, again for data lengths that are powers of two. Such transforms

Manuscript December 19, 1991. This research was supported in part by the Center for Communications Research in Princeton, New Jersey; and in part by the U.S. National Science Foundation under Grant NCR-90-02767. This work was presented at the 1992 Asilomar Conference, Pacific Grove, CA, October 26–28, 1992.

G. Caire is with the Dipartimento di Ingegneria Elettronica, Politecnico di Torino, Corso Duca degli Abruzzi 24, Torino 10129 Italy.

R. L. Grossman is with the Department of Mathematics, Statistics, and Computer Science, University of Illinois, Chicago, IL 60680.

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544.

IEEE Log Number 9209660.

are completely characterized in terms of simple conditions on the cyclic Fourier coefficients of a "mother" wavelet that determines the transform. In Section VI, we discuss briefly several further items of interest in this context, including the extension to such analysis at successive resolutions other than two.

II. Fourier Transforms Associated with Cyclic Groups

In this section, we give a brief review of Fourier transforms associated with finite cyclic groups, and we give several illustrative examples.

Suppose $\mathcal{F}$ is a field, and C_N is a finite cyclic group of order N. Suppose further that ϕ is a homomorphism

$$\phi\colon C_N \to \mathcal{F},$$

and let α denote the image under ϕ of a generator of C_N. Then $\alpha^N = 1$. In general, we will identify a function

$$v\colon C_N \to \mathcal{F},$$

with the vector $(v_0, v_1, \cdots, v_{N-1})'$ of elements from $\mathcal{F}$.

The *cyclic Fourier transform* of the function v is defined to be the function

$$\hat{v}\colon C_N \to \mathcal{F},$$

where

$$\hat{v}_k = \sum_{l=0}^{N-1} \alpha^{kl} v_l. \tag{2.1}$$

The inverse of the transform (2.1) is given by

$$v_k = N' \sum_{l=0}^{N-1} \alpha^{-kl} \hat{v}_l, \tag{2.2}$$

for a suitably chosen constant $N' \in \mathcal{F}$.

We illustrate the cyclic Fourier transform with its most commonly used examples.

Example 2.1: Suppose $\mathcal{F} = \mathcal{C}$ and N is a positive integer. Take C_N to be the cyclic group of rotations of the unit circle by $2\pi/N$. Then, with the natural homomorphism, we have $\alpha = \exp(i2\pi/N)$ and (2.1) defines the *finite-length Fourier transform*. Here, (2.2) with $N' = 1/N$ defines the inverse transform. This transform is often called the *discrete Fourier transform* or DFT. When the transform length N is chosen to be a power of two, the fast Fourier transform (FFT) can be used to calculate the DFT efficiently. (See, e.g., [15].)

Example 2.2: Suppose p and r are positive integers with p prime; and let $\mathcal{F} = GF(p^r)$, the Galois field with p^r elements. Suppose further that N is a divisor of $p^r - 1$. Then (2.1) defines the *finite-field Fourier transform*; and (2.2) with N' satisfying $NN' = p^r - 1$ is the inverse. This transform is often termed the *number-theoretic Fourier transform*, or the *Galois field Fourier transform*. For more details, see [16] or [17].

Example 2.3: In this example, we generalize the definition slightly. Suppose $\mathcal{F}$ and C_N are a field and cyclic group as above. For any divisor N_0 of N there is an α satisfying $\alpha^{N_0} = 1$, and (2.1) and (2.2) again define a transform.

Example 2.4: An important special case of Example 2.3 occurs when $N = 2^n$ for some positive integer n and $N_0 = 2$. In this case, $N' = 1/N$, and the transform (2.1)–(2.2) is known as the *Hadamard transform*.

III. The Finite-Length Wavelet Transform

The finite-length Fourier transform of Example 2.1, is of central importance in linear processing of finite-length signals. In this section, we describe an alternative transform, the *finite-length wavelet transform*, that is related to this finite-length Fourier transform. This transform is based on a form for the *discrete-time wavelet transform*, which we now describe briefly before defining its finite-length counterpart. This discrete-time wavelet transform is based on the Laplacian pyramid scheme for image compression proposed by Burt and Adelson [12]. Its general use in multiresolution analysis has been explored by Mallat, Meyer, and others. The reader is referred to [3] or [6] for a more detailed treatment of this scheme.

Note that the finite-length Fourier transform is a finite-length analog of the *discrete-time Fourier transform*, defined for a sequence $v \in l^2(\mathcal{Z})$, by

$$V(\omega) = \sum_{k=-\infty}^{\infty} v_k e^{i2\pi\omega k}, \qquad -\pi \leq \omega \leq \pi. \tag{3.1}$$

Here, and throughout the paper, $l^2(\mathcal{Z})$ denotes square-summable sequences of complex numbers. The *discrete-time wavelet transform* is an alternative tool for analyzing real or complex discrete-time sequences, which is closely related to the multiresolution analysis of such sequences. This transform is based on a successive decomposition and reconstruction algorithm described as follows.

Consider two bounded linear operators $\mathcal{G}$ and $\mathcal{H}$ on $l^2(\mathcal{Z})$ defined by

$$(\mathcal{G}x)_k = \sum_{l=-\infty}^{\infty} g_{l-2k} x_l, \qquad x \in l^2(\mathcal{Z}), \tag{3.2a}$$

and

$$(\mathcal{H}x)_k = \sum_{l=-\infty}^{\infty} h_{l-2k} x_l, \qquad x \in l^2(\mathcal{Z}), \tag{3.2b}$$

where g and h are sequences in $l^1(\mathcal{Z})$. Note that $\mathcal{G}$ and $\mathcal{H}$ as described can be thought of as filtering operations followed by decimation in time by a factor of two. A single decomposition step of this scheme consists of the computation from $v \in l^2(\mathcal{Z})$ of $c = \mathcal{H}v$ and $d = \mathcal{G}v$. The succeeding iteration of this decomposition consists of applying these same two computations to the sequence c obtained from the preceding iteration. A reconstruction step consists of the computation of v from c and d via $v = \mathcal{H}^*c + \mathcal{G}^*d$, where $\mathcal{G}^*$ and $\mathcal{H}^*$ denote the adjoints of the operators $\mathcal{G}$ and $\mathcal{H}$, respectively.[1]

[1] Note that an alternative discrete wavelet transform has recently been proposed in [18] in which this iteration is applied to both c and d, resulting in a binary tree of filtered sequences.

In order for this decomposition/reconstruction pair to describe an invertible transform, the operators $\mathcal{G}$ and $\mathcal{H}$ must be restricted so that

$$\mathcal{G}^*\mathcal{G} + \mathcal{H}^*\mathcal{H} = \mathcal{I}, \tag{3.3a}$$

where $\mathcal{I}$ denotes the identity operator in $l^2(\mathcal{Z})$. Moreover, it is desirable for the two components of v, namely $\mathcal{H}^*c$ and $\mathcal{G}^*d$, to be orthogonal, a condition that is assured if

$$\mathcal{H}\mathcal{G}^* = \mathcal{O}, \tag{3.3b}$$

where $\mathcal{O}$ denotes the zero operator on $l^2(\mathcal{Z})$. Note that a pair of filters having these properties required of the transformations $\mathcal{H}$ and $\mathcal{G}$ are known as *quadrature mirror filters* having the *perfect reconstruction property* (also known as *perfect reconstruction filters*). Such filters have been studied extensively in the digital signal processing literature (see, e.g., [19]–[21]).

The conditions (3.3) can be rewritten in terms of the discrete-time Fourier transforms of the decimated sequences $g^{(m)} = \{g_{2k+m}\}_{k=-\infty}^{\infty}$ and $h^{(m)} = \{h_{2k+m}\}_{k=-\infty}^{\infty}$ for $m = 0, 1$. In particular, on denoting the transforms (3.1) of $g^{(m)}$ and $h^{(m)}$ by β^m and δ^m, respectively, the conditions (3.3) can be rewritten as (see, e.g., [3, (3.12) and (3.13)]:

$$|\beta^0(\omega)|^2 + |\beta^1(\omega)|^2 = 1, \qquad -\pi \le \omega \le \pi, \tag{3.4a}$$

and

$$\delta^m(\omega) = (-1)^m e^{i2\pi\lambda(\omega)}\overline{\beta^{1-m}(\omega)}, \qquad -\pi \le \omega \le \pi, \qquad m = 0, 1, \tag{3.4b}$$

where λ is any real valued function such that $\lambda(\omega+2\pi)-\lambda(\omega)$ is integer valued. (Here, and elsewhere, an overbar denotes complex conjugation.)

Thus, g can be chosen to satisfy (3.4a), and then h is prescribed by (3.4b) for a convenient choice of λ. For example, with $\lambda(\omega) \equiv 0$ (3.4b) yields the relationship

$$h_k = (-1)^k\overline{g_{1-k}}, \qquad k \in \mathcal{Z}. \tag{3.5}$$

In practice, the sequences h and g used in the above scheme will be chosen to have only a few nonzero elements so that the transform can provide good resolution of the sequence characteristics at different time shifts. Moreover, it is usually desirable to require further that h satisfy the so-called *lowpass condition,*

$$\sum_{k\in\mathcal{Z}} h_k = \sqrt{2}, \tag{3.6a}$$

and that g satisfy the complementary *bandpass condition,*

$$\sum_{k\in\mathcal{Z}} g_k = 0. \tag{3.6b}$$

Within these latter conditions, the decomposition step can be viewed as a low-pass filtering and decimation to produce the lower resolution signal c, and a bandpass filtering and decimation to produce the *detail* or residual signal d. Thus, successive applications of the transform will provide information about the original sequence at successively lower resolutions. Such successive application of this type of decomposition is referred to as a Laplacian pyramid scheme; and the version with g taken to be a unit impulse sequence (i.e., $g_k = \delta_k$) was first proposed by Burt and Adelson [12] as a technique for representing images.

The Laplacian pyramid decomposition/reconstruction steps can be adapted to define an exact multiresolution wavelet transform for sequences of finite length $N = 2^n$, from an arbitrary field $\mathcal{F}$, where $n > 1$ is an integer. In order to construct such a transform, we first define a general formulation of the multiresolution analysis of the vector space $\mathcal{F}^N$ and then give a practical scheme for the decomposition and reconstruction of a sequence in $\mathcal{F}^N$.

Consider a ladder of nested vector spaces $V_n \subset V_{n-1} \subset \cdots V_0 = \mathcal{F}^N$ where $\dim(V_j) = 2^{n-j}$. For each $j = 1, 2, \cdots, n$, define the subspace W_j to be the orthogonal complement of V_j in V_{j-1} so that

$$V_{j-1} = W_j \oplus V_j. \tag{3.7}$$

Here, the notation $\oplus$ indicates the direct sum; i.e., (3.7) means that every element of V_{j-1} can be written in a *unique* way as the sum of an element of W_j and an element of V_j. From (3.7), it follows that V_0 can be written as

$$V_0 = W_1 \oplus W_2 \oplus \cdots \oplus W_n \oplus V_n. \tag{3.8}$$

This means that any sequence $v \in \mathcal{F}^N$ can be decomposed in a unique way as the sum of sequences $w^j \in W_j$, $j = 1, 2, \cdots, n$, and $v^n \in V_n$. We define the *multiresolution analysis mapping* (MA) to be the linear map that perform this decomposition; i.e.,

$$\text{MA: } v \to \{w^1, w^2, \cdots, w^n, v^n\}. \tag{3.9}$$

Since MA is bijective it has an inverse MA^{-1}, which we define to be the *multiresolution synthesis mapping* (MS):

$$\text{MS: } \{w^1, w^2, \cdots, w^n, v^n\} \to v = w^1 + w^2 + \cdots + w^n + v^n. \tag{3.10}$$

We now define an algorithm that implements an MA–MS pair. For $j = 1, 2, \cdots, n$ consider matrices H^j and G^j over $\mathcal{F}$ of dimension $2^{n-j} \times 2^{n-j+1}$, satisfying the conditions

$$(H^j)^*H^j + (G^j)^*G^j = N'^{-1}I_{2^{n-j+1}}, \tag{3.11}$$

where I_k denotes the $k \times k$ identity matrix, and where $N' \in \mathcal{F}$ is a constant whose choice will be discussed next.

Within this framework, consider the following algorithm.

Decomposition: Given $c^0 = v$ and an integer $n > 0$, the algorithm computes a sequence $d^1, \cdots, d^n$, c^n as follows.

Step 1) Given c^0, compute

$$c^1 = H^1c^0, \qquad d^1 = G^1c^0.$$

Step 2) In general, for $j = 1, 2, \cdots, n-1$, compute

$$c^{j+1} = H^{j+1}c^j, \qquad d^{j+1} = G^{j+1}c^j.$$

Reconstruction: Given a decomposition $\{d^1, \cdots, d^n, c^n\}$, the algorithm reconstructs the original signal $v = c^0$.

Step 1) Compute $c^{n-1} = N'[(G^n)^* d^n + (H^n)^* c^n]$, where the superscript asterisk denotes the dual of the superscripted operator.

Step 2) In general, for $j = n-2, n-3, \cdots, 0$, compute

$$c^j = N'[(G^{j+1})^* d^{j+1} + (H^{j+1})^* c^{j+1}].$$

With respect to this algorithm, we have the following.

Proposition 1: The algorithm defined by Decomposition/Reconstruction with matrices chosen to satisfy (3.11) is an MA–MS pair.

Proof: First, we note that (3.11) holds only if for each j the matrices H^j and G^j have full rank (i.e., the row rank 2^{n-j}) and if the rows of H^j span the kernel of G^j. Thus the $2^{n-j+1} \times 2^{n-j+1}$ matrix

$$\begin{bmatrix} H^j \\ G^j \end{bmatrix}$$

is of full rank. On writing (3.11) as

$$[(H^j)^*(G^j)^*]\begin{bmatrix} H^j \\ G^j \end{bmatrix} = N'^{-1} I_{2^{n-j+1}},$$

and multiplying it from the right by $[(H^j)^*(G^j)^*]$, we obtain

$$[(H^j)^*(G^j)^*]\left[N'^{-1} I_{2^{n-j+1}} - \begin{bmatrix} H^j(H^j)^* & H^j(G^j)^* \\ G^j(H^j)^* & G^j(G^j)^* \end{bmatrix}\right] = 0_{2^{n-j+1}}, \quad (3.12)$$

where 0_k denotes the $k \times k$ matrix with all zero entries. Since the columns of $[(H^j)^*(G^j)^*]$ are linearly independent, (3.12) holds, if and only if

$$H^j(H^j)^* = N'^{-1} I_{2^{n-j}}, \quad (3.13a)$$

$$G^j(G^j)^* = N'^{-1} I_{2^{n-j}}, \quad (3.13b)$$

and

$$H^j(G^j)^* = 0_{2^{n-j}}. \quad (3.13c)$$

By using Decomposition/Reconstruction iteratively, we get:

$$v = N'(G^1)^* d^1 + N'(H^1)^* c^1 = w^1 + v^1,$$

where $w^1 \in W_1$ and $v^1 \in V_1$. Then, we get

$$v^1 = N'^2(H^1)^*(G^2)^* d^2 + N'^2(H^1)^*(H^2)^* c^2 = w^2 + v^2,$$

where $w^2 \in W_2$ and $v^2 \in V_2$, and so forth.

From this construction we get an explicit form for the subspaces V_j and W_j, and we can check that they match the construction of the multiresolution analysis. In particular, on neglecting the factor N' we have

$$V_j = (H^1)^*(H^2)^* \cdots (H^{j-1})^*(H^j)^* \mathcal{F}^{2^{n-j}}$$

and

$$W_j = (H^1)^*(H^2)^* \cdots (H^{j-1})^*(G^j)^* \mathcal{F}^{2n-j}.$$

It is easy to see that the condition $V_j \subset V_{j-1}$ is always satisfied since $(H^j)^* \mathcal{F}^{2^{n-j}}$ is always a subspace of $\mathcal{F}^{2^{n-j+1}}$. Moreover, V_j and W_j are orthogonal complements of the same dimension in V_{j-1} because of (3.13c). Thus we will get a valid MA–MS pair every time we consider matrices H^j and G^j that satisfy (3.11). □

Remark 3.1: Note that the decomposition of any sequence $v \in \mathcal{F}^N$ into the sum of sequences $w^j \in W_j$ and $v^n \in V_n$ is uniquely defined by the "coefficients" $\{d^1, d^2, \cdots, d^n, c^n\}$ once the matrices H^j and G^j at each step of the Decomposition/Reconstruction algorithm are fixed. These coefficients comprise a ***finite-length wavelet transform*** of the sequence v. In other words, for the case of a finite-dimensional vector space $\mathcal{F}^N$, for each multiresolution analysis defined by Decomposition/Reconstruction and (3.11), there is an associated finite-length wavelet transform (FLWT):

$$\text{FLWT: } v \Leftrightarrow \{d^1, d^2, \cdots, d^n, c^n\}. \quad (3.14)$$

Remark 3.2: Note that (3.11) defines a quadratic relationship among the elements of the matrices defining the finite-length wavelet transform. It may also be useful to specify lowpass and bandpass conditions analogous to (3.6). These conditions, and the structure imposed by (3.11), will be discussed in the following sections.

IV. The Cyclic Wavelet Transform

In the preceding section, we defined the finite-length wavelet transform in terms of the matrices $G^1, G^2, \cdots, G^n$ and $H^1, H^2, \cdots, H^n$ appearing in Decomposition/Reconstruction. As in the case of Fourier analysis, it is of interest to constrain this transform to define a *cyclic* multiresolution analysis of the space of the periodic sequences of period 2^n over $\mathcal{F}$. In this and the following section, we explore the constraints leading to such transforms, and we give a general construction of appropriate matrix sequences that satisfy the additional constraints.

Consider the situation in which the matrices H^j and G^j are constrained to be *2-circulants* [22] for each j; i.e., suppose these matrices are of the form:

$$G^j = \begin{pmatrix} g_0^j & g_1^j & g_2^j & \cdots & g_{N_j-1}^j \\ g_{N_j-2}^j & g_{N_j-1}^j & g_0^j & \cdots & g_{N_j-3}^j \\ g_{N_j-4}^j & g_{N_j-3}^j & g_{N_j-2}^j & \cdots & g_{N_j-5}^j \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_2^j & g_3^j & g_4^j & \cdots & g_1^j \end{pmatrix}, \quad (4.1a)$$

and

$$H^j = \begin{pmatrix} h_0^j & h_1^j & h_2^j & \cdots & h_{N_j-1}^j \\ h_{N_j-2}^j & h_{N_j-1}^j & h_0^j & \cdots & h_{N_j-3}^j \\ h_{N_j-4}^j & h_{N_j-3}^j & h_{N_j-2}^j & \cdots & h_{N_j-5}^j \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_2^j & h_3^j & h_4^j & \cdots & h_1^j \end{pmatrix}. \quad (4.1b)$$

where $N_j \triangleq 2^{n-j+1}$. Note that a 2-circulant matrix is defined completely by its first row; and thus we can write $G^j = 2\text{–cir}\{g^j\}$ and $H^j = 2\text{–cir}\{h^j\}$ where g^j and h^j

denote the first rows of G^j and H^j, respectively. Within this constraint, an interesting interpretation of the algorithm Decomposition/Reconstruction is possible if we consider the sequences c^j and d^j to be periodic sequences of period equal to their lengths (N_{j+1}).

In particular, for matrices satisfying (4.1), the jth step of Decomposition defines a finite-impulse-response (FIR) filtering of the periodic sequence c^{j-1} with the two FIR filters having impulse response h^j and g^j, followed by a decimation by 2. The periods of the input sequence c^{j-1} is 2^{n-j+1} while the period of the two output sequences c^j and d^j is 2^{n-j}. Similarly, Reconstruction can be considered to be interpolation by 2 followed by FIR filtering. Note that this filtering and decimation by 2 (or interpolation by 2 and filtering on the reconstruction side) is completely analogous to the sub-band decomposition scheme for infinite-length sequences described by the Laplacian pyramid of Section III.

Thus, we conclude that Decomposition/Reconstruction with the 2-circulant constraint (4.1) defines a *cyclic multiresolution analysis* and its associated *cyclic wavelet transform* (CWT) for the space of periodic sequences of period 2^n over $\mathcal{F}$ (which is isomorphic to $\mathcal{F}^N$ since it is a vector space of the same finite dimension). Moreover this algorithm is specified by a family of FIR filters and can be implemented in an efficient way by the known techniques for cyclic convolution (for example by using the FFT).

In order to design such transforms, we want to construct families of sequences $\{g^j, h^j \in \mathcal{F}^{2^{n-j+1}} \mid j = 1, 2, \cdots, n\}$ such that (3.11) is satisfied for all j with $G^j = 2\text{--cir}\{g^j\}$ and $H^j = 2\text{--cir}\{h^j\}$. Each such family defines an MA–MS pair and the relative CWT for the space of periodic sequences of period 2^n over the field $\mathcal{F}$. In this section, we consider the design of such transforms for the case in which $\mathcal{F} = \mathcal{C}$, the field of complex numbers. Finite fields will be considered in the following section. To construct the sequences of interest, we will first give a result characterizing 2-circulant matrices satisfying (3.11) for the case $j = 1$, and then we will give a method to derive a family of sequences $\{g^j, h^j\}, j = 2, \cdots, n$, from any two sequences g^1 and h^1 that satisfy the theorem. In following we will suppress the superscripts 1 on G^1, H^1, g^1, and h^1 for notational convenience.

For the case in which the field is $\mathcal{C}$, the set of possible pairs of sequences $g_0, g_1, \cdots, g_{N-1}$ and $h_0, h_1, \cdots, h_{N-1}$ such that $2\text{--cir}\{g\}$ and $2\text{--cir}\{h\}$ satisfy (3.11) is characterized by the following proposition, which is stated in terms of the following finite-length Fourier transforms:

$$\gamma_k^m = \sum_{l=0}^{N/2-1} g_{2l+m}\alpha^{2lk}, \quad k = 0, 1, \cdots, \frac{N}{2} - 1, \quad m = 0, 1, \tag{4.2a}$$

and

$$\eta_k^m = \sum_{l=0}^{N/2-1} h_{2l+m}\alpha^{2lk}, \quad k = 0, 1, \cdots, \frac{N}{2} - 1, \quad m = 0, 1, \tag{4.2b}$$

where α is the relevant Nth primitive root of unity: $\alpha = \exp\{2\pi i/N\}$.

Theorem 1: Consider the cyclic wavelet transform of length $N = 2^n$ over the complex field and let N' be any nonzero element. The matrices $G = 2\text{--cir}\{g_0, g_1, \cdots, g_{N-1}\}$ and $H = 2\text{--cir}\{h_0, h_1, \cdots, h_{N-1}\}$ satisfy (3.11), if and only if for each $k = 0, 1, \cdots, N/2 - 1$, we have

$$|\gamma_k^0|^2 + |\gamma_k^1|^2 = \frac{1}{N'}, \tag{4.3a}$$

and

$$\eta_k^m = (-1)^m \nu_k \overline{\gamma_k^{1-m}}, \qquad m = 0, 1, \tag{4.3b}$$

for some $\nu \in \mathcal{C}^{N/2}$ satisfying $|\nu_k|^2 = 1$, $k = 0, 1, \cdots, N/2 - 1$.

Proof: We note first that the dual of an operator represented by a matrix of complex numbers is the operator represented by the transpose of the matrix with each element replaced by its complex conjugate. As shown in the proof of Proposition 1, the condition (3.11) is equivalent to the three conditions given in (3.13). By conformal rearrangement of the columns of G and H, i.e., by rearranging the columns of G and H in the same way, the conditions (3.13) can be rewritten as

$$(A_0 \quad A_1)(A_0 \quad A_1)^* = (N')^{-1} I_{N-2}, \tag{4.4a}$$

$$(B_0 \quad B_1)(B_0 \quad B_1)^* = (N')^{-1} I_{N/2}, \tag{4.4b}$$

and

$$(A_0 \quad A_1)(B_0 \quad B_1)^* = 0_{N/2}, \tag{4.4c}$$

where, for $m = 0, 1$, A_m, and B_m denote the $N/2 \times N/2$ 1-circulant matrices with first rows $g_m, g_{m+2}, g_{m+4}, \cdots, g_{N-2+m}$ and $h_m, h_{m+2}, h_{m+4}, \cdots, h_{N-2+m}$, respectively.

Denote by F the $N/2 \times N/2$ (Fourier) matrix with $(k-1)$th element α^{2kl} for $k, l = 0, 1, \cdots, N/2 - 1$. Note that $F^*F = N/2 I_{N/2}$, and that the matrices A_m and B_m are diagonalized by F since they are 1-circulants [22]. Noting further that A_m and B_m have eigenvalues $\gamma_0^m, \gamma_1^m, \cdots, \gamma_{N/2-1}^m$, and $\eta_0^m, \eta_1^m, \cdots, \eta_{N/2-1}^m$, respectively, we can thus write

$$A_m = \frac{2}{N} F^* \Gamma_m F, \qquad m = 0, 1 \tag{4.5a}$$

and

$$B_m = \frac{2}{N} F^* \Lambda_m F, \qquad m = 0, 1 \tag{4.5b}$$

with $\Gamma_m = \operatorname{diag}\{\gamma_0^m, \gamma_1^m \cdots \gamma_{N/2-1}^m\}$, and $\Lambda_m = \operatorname{diag}\{\eta_0^m, \eta_1^m \cdots \eta_{N/2-1}^m\}$.

Substituting (4.5) into (4.4), yields the equivalent conditions

$$\Gamma_0\Gamma_0^* + \Gamma_1\Gamma_1^* = (N')^{-1} I_{N/2}, \tag{4.6a}$$

$$\Lambda_0\Lambda_0^* + \Lambda_1\Lambda_1^* = (N')^{-1} I_{N/2}, \tag{4.6b}$$

and

$$\Gamma_0\Lambda_0^* + \Gamma_1\Lambda_1^* = 0_{N/2}. \tag{4.6c}$$

In the form (4.6), the conditions imposed by (3.11) on $g_0, g_1, \cdots, g_{N-1}$ and $h_0, h_1, \cdots, h_{N-1}$ can be written in terms of the Fourier coefficients defined in (4.2) in decoupled form. In particular, we have the following three conditions for each $k = 0, 1, \cdots, N/2 - 1$:

$$|\gamma_k^0|^2 + |\gamma_k^1|^2 = \frac{1}{N'}, \tag{4.7a}$$

$$|\eta_k^0|^2 + |\eta_k^1|^2 = \frac{1}{N'}, \tag{4.7b}$$

and

$$\gamma_k^0\overline{\eta_k^0} + \gamma_k^1\overline{\eta_k^1} = 0. \tag{4.7c}$$

The sufficiency of the conditions (4.3) is seen quite easily from (4.7). In particular, we note that (4.7a) is identical to (4.3a); (4.7b) follows immediately from the substitution of (4.3b) into (4.3a); and finally (4.7c) follows by multiplying (4.3b) with $j = 1$ by $\overline{\gamma_k^0}$, multiplying (4.3b) with $j = 1$ by $\overline{\gamma_k^1}$, and then adding the two results.

The necessity of the conditions (4.3) is also seen straightforwardly from (4.7). In particular, we need only show that (4.7) implies (4.3b). To do so, we first consider the case in which $\gamma_k^m = 0$ for either $m = 0$ or $m = 1$. Then, (4.7a) implies that $\gamma_k^{1-m} \neq 0$, which together with (4.7c) implies that $\eta_k^{1-m} = 0$. Equation (4.3b) thus follows by choosing $\nu_k = (-1)^m\eta_k^m/\overline{\gamma_k^{1-m}}$, which satisfies $|\nu_k|^2 = 1$ via (4.7a) and (4.7b). Now, if both γ_k^0 and γ_k^1 are nonzero, then (4.3b) follows if $\eta_k^0/\overline{\gamma_k^1} \equiv -\eta_k^1/\overline{\gamma_k^0}(\equiv \nu_k)$. But this is simply the orthogonality condition (4.7c). So, the necessity of (4.3b), and thus (4.3), is proven.

This completes the proof of Theorem 1. □

Remark 4.1: It is evident that the conditions (4.3) are the cyclic versions of the conditions (3.4) characterizing the discrete-time wavelet transform.

Theorem 1 allows us to construct sequences whose corresponding 2-circulant matrices satisfy (3.11) for the case $j = 1$. Given two such sequences, we now wish to construct a family of sequences $\{g^j, h^j \mid j = 1, 2, \cdots, n\}$ that specifies an MA–MS scheme as previously described. Such a construction is given by the following result, which is a straightforward corollary to Theorem 1. (See also [23].)

Corollary 1: Suppose $G = 2\text{–cir}\{g\}$ and $H = 2\text{–cir}\{h\}$ are $2^{n-1} \times 2^n$ matrices of complex numbers satisfying (3.11). For each $j = 1, 2, \cdots, n$, define two length-2^{n-j} sequences g^j and h^j by

$$g_{2l+m}^j = \text{DFT}^{-1}\{\{\gamma_{2^{j-1}k}^m \mid k = 0, 1, \cdots, 2^{n-j} - 1\}\}_l, \tag{4.8}$$

and

$$h_{2l+m}^j = \text{DFT}^{-1}\{\{\eta_{2^{j-1}k}^m \mid k = 0, 1, \cdots, 2^{n-j} - 1\}\}_l, \tag{4.9}$$

for $l = 0, 1, \cdots, 2^{n-j} - 1$ and $m = 0, 1$, where the sequences γ^0, γ^1, η^0, and η^1, are defined from g and h as in (4.2), and where the operation DFT indicates the discrete Fourier transform of appropriate length. Then, $G^j = 2\text{–cir}\{g^j\}$ and $H^j = 2\text{–cir}\{h^j\}$ satisfy (3.11) for each $j = 1, 2, \cdots, n$.

Remark 4.2: It is evident from their construction that the sequences g^j and h^j satisfy condition (4.3) of Theorem 1 for each j. In particular, the conditions of Theorem 1 are given on the Fourier transform of the even and odd coefficients of g and h, therefore any sequence obtained by "frequency sampling" those transforms will obviously satisfy the same conditions.

Remark 4.3: Corollary 1 defines g^j and h^j to be the sequences obtained by frequency sampling the original sequences g and h with a sampling factor 2^{j-1}. If we look at Decomposition as an FIR filtering followed by a decimation by 2 of a periodic sequence, we see that at each step j the filters constructed in this way have the same frequency characteristics as the two original filters g and h. In this case the frequency sampling procedure does not give any degradation in the filters' frequency responses since for periodic sequences (and thus for cyclic convolution) the Fourier transform coincides with the DFT and the frequency response matters only for specific frequency values.

Remark 4.4: It should be noted that the bandpass condition, $\sum_{k=0}^{N-1} g_k = 0$, is equivalent to the condition that $\gamma_0^1 = -\gamma_0^0$. The construction of Corollary 1 assures that this condition holds for all j if it holds for $j = 1$. If the bandpass condition is imposed, then Theorem 1 shows that we also must have $\eta_0^1 = \eta_0^0$, and further that

$$|\gamma_0^0| = |\gamma_0^1| = |\eta_0^0| = |\eta_0^1| = \frac{1}{\sqrt{2N'}}. \tag{4.10}$$

Thus, from (4.10) we see that a corresponding low-pass condition,

$$\left|\sum_{k=0}^{N-1} h_k\right| = \sqrt{2/N'}. \tag{4.11}$$

is also enforced for each j. (See also [24].)

Remark 4.5: We see from Theorem 1 that, in this $\mathcal{F} = \mathcal{C}$ case, the field element N' must be real and positive. Otherwise, the role of N' is not critical in this case, since varying it essentially results in a simple renormalization of the matrices G and H. In particular, there is no lost generality if we simply choose N' to be unity or some other convenient value. As we shall see in the following section, the choice of N' is not arbitrary in the case in which $\mathcal{F}$ is a finite field. This is essentially because the square-root arising in (4.11) will not be defined for all field elements in a finite field. This point will be discussed further.

Remark 4.6: From the necessary and sufficient conditions (4.3), we see that a cyclic wavelet transform can be designed by first selecting a sequence $g_0, g_1, \cdots, g_{N-1}$ to satisfy (4.3a) (this sequence plays the role of the so-called "mother" wavelet [3]), and then choosing $h_0, h_1, \cdots, h_{N-1}$ from (4.3b). The choice of $g_0, g_1, \cdots, g_{N-1}$ is further reduced to choosing, say, the even-indexed subset $g_0, g_2, \cdots, g_{N-2}$, to satisfy

$$N'|\gamma_k^0|^2 \leq 1, \tag{4.12}$$

and then choosing $g_1, g_3, \cdots, g_{N-1}$ compatibly via the inverse of the relationship (4.2a):

$$g_k = \frac{2}{N}\sum_{l=0}^{N/2-1} \gamma_l^1\alpha^{-lk}, \qquad k = 1, 3, \cdots, N-1. \tag{4.13}$$

Example 4.1: From a practical viewpoint, the sequence $g_0, g_1, \cdots, g_{N-1}$ should be chosen to have only a few nonzero elements. As an example, take $N' = 1/2$, and consider the choice

$$g_k = \delta_k, \qquad k = 0, 2, \cdots, N-2. \tag{4.14}$$

This choice is equivalent to $\gamma_k^0 \equiv 1$, which, through (4.3a), imposes the condition $|\gamma_k^1| \equiv 1$, or equivalently, $\gamma_k^1 = \alpha^{\xi_k}$, with $\xi_0, \xi_1, \cdots, \xi_{N/2-1}$, taken from the reals. Thus, any sequence of the form

$$g_k = \frac{2}{N} \sum_{l=0}^{N/2-1} \alpha^{-lk+\xi_l}, \qquad k = 1, 3, \cdots, N-1, \tag{4.15}$$

is compatible with the choice (4.14). Imposition of the bandpass condition restricts only ξ_0 (to be $N/2$). The simplest such sequence results from the choice $\xi_k = N/2 + k$, which leads to

$$g_k = -\delta_{k-1}, \qquad k = 1, 3, \cdots, N-1; \tag{4.16}$$

i.e., the mother wavelet in this case is $1, -1, 0, 0, \cdots, 0$.

Example 4.2: In this example, we define a transform similar to the Hadamard transform, described in Example 2.4. To do this, we continue with the example above. In order to choose the sequence $h_0, h_1, \cdots, h_{N-1}$, it is interesting to rewrite the condition (4.3b) directly as a relationship between the cyclic Fourier transforms of the sequences $g_0, g_1, \cdots, g_{N-1}$ and $h_0, h_1, \cdots, h_{N-1}$, which we denote by $\gamma_0, \gamma_1, \cdots, \gamma_{N-1}$ and $\eta_0, \eta_1, \cdots, \eta_{N-1}$, respectively. In particular, by using the fact that $\alpha^{N/2} = -1$, (4.3b) can be rewritten straightforwardly as

$$\eta_k = -\nu_k \alpha^k \overline{\gamma_{k-N/2}}, \qquad k = 0, 1, \cdots, N-1, \tag{4.17}$$

where we have used the extension $\nu_k = \nu_{k-N/2}$, $k = N/2, \cdots, N-1$. The corresponding relationship between $g_0, g_1, \cdots, g_{N-1}$ and $h_0, h_1, \cdots, h_{N-1}$, is thus determined by the choice of the sequence $\nu_0, \nu_1, \cdots, \nu_{N/2-1}$. For example, with $\nu_k \equiv 1$, (4.17) is equivalent to

$$h_k = (-1)^k \overline{g_{[1-k]_N}}, \qquad k = 0, 1, \cdots, N-1, \tag{4.18}$$

where $[x]_N$ denotes x reduced modulo N. (Note the similarity of (4.18) to the discrete-time example of (3.5).)

Thus, an example of a pair of sequences generating a cyclic wavelet transform are those given by (4.1), (4.16), and (4.18); namely,

$$g = (1 \quad -1 \quad 0 \quad \cdots \quad 0 \quad 0), \tag{4.19a}$$

and

$$h = (-1 \quad -1 \quad 0 \quad \cdots \quad 0 \quad 0). \tag{4.19b}$$

A complete transform is thus specified by (4.19) and Corollary 1. For example, for the case $N = 8$, we obtain the filters

$$g^1 = (1, -1, 0, 0, 0, 0, 0, 0)$$
$$h^1 = (-1, -1, 0, 0, 0, 0, 0, 0)$$

$$g^2 = (1, -1, 0, 0) \qquad h^2 = (-1, -1, 0, 0)$$

$$g^3 = (1, -1) \qquad h^3 = (-1, -1).$$

Note that, in this case, the lower-order filter impulse responses are found by simply taking the first half of that of the preceding filter. In this particular case, this property will hold for any transform length. However, this property will not hold in general.

Example 4.3: The next level of transform complexity (aside from other choices of the sequence ν_k) arises from setting $g_k = 0$, for $k > 3$. Assuming that the coefficients of the mother wavelet are real, they are related through Theorem 1 by the equations:

$$g_0 g_2 = -g_1 g_3, \tag{4.20a}$$

and

$$(g_0)^2 + (g_1)^2 + (g_2)^2 + (g_3)^2 = \frac{1}{N'}. \tag{4.20b}$$

Note from (4.20a) that a mother wavelet consisting of exactly three consecutive nonzero elements is not allowed in this formulation. Also note that the roles of g_0 and g_2 [resp. g_1 and g_3] are interchangeable. If we assume a normalization such that $g_0 = 1$, and further impose the bandpass condition,

$$g_0 + g_2 = -g_1 - g_3, \tag{4.20c}$$

then, modulo the above noted symmetry, the mother wavelet is given for $N' < (3 + 2\sqrt{2})/8$, by

$$g_0 = 1, \tag{4.21a}$$

$$g_1 = \frac{\zeta - \sqrt{2 - \zeta^2}}{2 - \zeta - \sqrt{2 - \zeta^2}}, \tag{4.21b}$$

$$g_2 = -g_1 \frac{g_1 + 1}{g_1 - 1}, \tag{4.21c}$$

and

$$g_3 = \frac{g_1 + 1}{g_1 - 1}, \tag{4.21d}$$

where $\zeta \triangleq 1 - 2\sqrt{2N'}$. Note that this gives a family of mother wavelets parametrized by N'. (This parameterization results from the choice $g_0 = 1$. Alternatively, we could of course fix N' and consider g_0 to parametrize the family.)

With $N' = 1/2$, (4.21) reduces to the previous example, $g_1 = -1$, and $g_2 = g_3 = 0$. For other choices of N' the mother wavelet from (4.21) will differ nontrivially from (4.14), (4.16). For example, the choice $N' = 1/8$ yields the mother wavelet

$$g_0 = 1; \quad g_1 = \frac{1}{1 - \sqrt{2}}; \quad g_2 = 1; \quad g_3 = \sqrt{2} - 1. \tag{4.22}$$

Thus, on choosing h from (4.18), Corollary 1 gives the following $N = 8$ cyclic transform:

$$g^1 = \left(1, \frac{1}{1 - \sqrt{2}}, 1, \sqrt{2} - 1, 0, 0, 0, 0\right)$$

$$h^1 = \left(\frac{1}{1 - \sqrt{2}}, -1, 0, 0, 0, 0, \sqrt{2} - 1, -1\right)$$

$$g^2 = \left(1, \frac{1}{1-\sqrt{2}}, 1, \sqrt{2}-1\right)$$

$$h^2 = \left(\frac{1}{1-\sqrt{2}}, -1, \sqrt{2}-1, -1\right)$$

$$g^3 = (2, -2) \qquad h^3 = (-2, -2).$$

V. Finite-Field Wavelet Transforms

We now consider the cyclic wavelet transform described by Decomposition/Reconstruction with transform matrices as in (4.1) for the case in which $\mathcal{F}$ is a finite field: $\mathcal{F} = \mathrm{GF}(p^r)$. As before, we restrict the data length N to be a power of two, $N = 2^n$. We assume that the characteristic p of the field is an odd prime, and further that there is an element $\alpha_o \in \mathcal{F}^\times$ of order 2^{n-1}. Note that this latter restriction is equivalent to the condition that 2^{n-1} must divide $p^r - 1$.

Again we require the matrices G^j and H^j to be 2-circulants, and they are therefore defined by their first rows g^j and h^j, respectively. We wish to construct a family of sequences $\{g^j, h^j \in \mathcal{F}^{2^{n-j+1}} \mid j = 1, 2, \cdots, n\}$ such that (3.11) is satisfied for all j. Such a family defines an MA–MS pair and the relative CWT for the space of periodic sequences of period 2^n over the field $\mathcal{F}$.

Within this model, we state a result analogous to Theorem 1. To do so, we first define polynomials in $\mathcal{F}[x]$:

$$\gamma^m(x) = \sum_{l=0}^{N/2-1} g_{2l+m} x^l, \qquad m = 0, 1, \tag{5.1a}$$

and

$$\eta^m(x) = \sum_{l=0}^{N/2-1} h_{2l+m} x^l, \qquad m = 0, 1. \tag{5.1b}$$

Theorem 2: Consider the cyclic wavelet transform of length $N = 2^n$ over the field $\mathcal{F} = \mathrm{GF}(p^r)$. The sequences $g_0, g_1, \cdots, g_{N-1}$ and $h_0, h_1, \cdots, h_{N-1}$ satisfy (3.11), if and only if, for each $k = 0, 1, \cdots, N/2 - 1$, we have

$$\gamma^0(\alpha_o^{-k})\gamma^0(\alpha_o^k) + \gamma^1(\alpha_o^{-k})\gamma^1(\alpha_o^k) = \frac{1}{N'}, \tag{5.2a}$$

and

$$\eta^m(\alpha_o^k) = (-1)^m \nu(\alpha_o^k)\gamma^{1-m}(\alpha_o^{-k}), \qquad m = 0, 1, \tag{5.2b}$$

for some rational function $\nu(x)$ of order $N/2$ over $\mathcal{F}$ satisfying $\nu(\alpha_o^{-k})\nu(\alpha_o^k) = 1$, $k = 0, 1, \cdots, N/2 - 1$.

Proof: The analogy between Theorems 1 and 2 is clear. The only differences of substance between the two cases are the connections between complex conjugation, Fourier inversion, and duality that are present in the complex case but not in the finite-field case. In particular, in the case of a finite field, the dual operator a linear operator represented by a matrix T is represented by the transpose of T. Nevertheless, the key properties used from these relationships are still valid here, and thus the proof follows very similarly to that of Theorem 1. In particular, if we replace F^* with the matrix whose elements are α_o^{-kl}, $k, l = 0, 1, \cdots, N/2-1$, and we replace γ_k^m, η_k^m, $\overline{\gamma_k^m}$, and $\overline{\eta_k^m}$ with $\gamma^m(\alpha_o^k)$, $\eta^m(\alpha_o^k)$, $\gamma^m(\alpha_o^{-k})$, and $\eta^m(\alpha_o^{-k})$, respectively, then the proof of Theorem 2 is identical to that of Theorem 1 after we make use of the following simple result.

Lemma 1: Suppose f, g, and h are polynomials of order $N/2 - 1$ over $\mathcal{F}$. Then,

$$f(\alpha_o^k) = g(\alpha_o^{-k})h(\alpha_o^k), \qquad k = 0, 1, \cdots, \frac{N}{2} - 1,$$

implies

$$f(\alpha_o^{-k}) = g(\alpha_o^k)h(\alpha_o^{-k}), \qquad k = 0, 1, \cdots, \frac{N}{2} - 1.$$

Remark 5.1: Note that we exclude fields of characteristic 2 in the above formulation because the equation $FF^* = (N/2)I$ is not particularly useful unless $n = 1$, since we otherwise have $N/2 = 0$.

Given two sequences g and h that satisfy Theorem 2, we wish to construct a family of sequences $\{g^j, h^j \mid j = 1, 2, \cdots, n\}$ that specifies an MA–MS scheme as previously described. Analogously to Corollary 1 in the preceding section, such sequences are specified by the following result.

Corollary 2: Suppose $G = 2\text{–cir}\{g\}$ and $H = 2\text{–cir}\{h\}$ are $2^{n-1} \times 2^n$ matrices of elements of $\mathcal{F}$ satisfying (3.11). For each $j = 1, 2, \cdots, n$, define two length-2^{n-j} sequences g^j and h^j by

$$g^j_{2l+m} = \mathrm{DFT}^{-1}[\{\gamma^m(\alpha_o^{2^{j-1}k}) \mid k = 0, 1, \cdots, 2^{n-j} - 1\}]_l, \tag{5.3}$$

and

$$h^j_{2l+m} = \mathrm{DFT}^{-1}[\{\eta^m(\alpha_o^{2^{j-1}k}) \mid k = 0, 1, \cdots, 2^{n-j} - 1\}]_l, \tag{5.4}$$

for $l = 0, 1, \cdots, 2^{n-j} - 1$ and $m = 0, 1$, where the sequences γ^0, γ^1, η^0, and η^1, are defined from g and h as in (5.1), and where the operation DFT indicates the number theoretic discrete Fourier transform of appropriate length. Then $G^j = 2\text{–cir}\{g^j\}$ and $H^j = 2\text{–cir}\{h^j\}$ satisfy (3.11) for each $j = 1, 2, \cdots, n$.

In view of Theorem 2, we see that a procedure for specifying a finite-field cyclic wavelet transform is to choose a mother wavelet g to satisfy (5.2a), to choose h according to (5.2b), and then to choose the lower-order filters from Corollary 2.

Example 5.1: Analogously with the complex case (4.18), it is interesting to consider the choice $\nu(x) \equiv 1$, in which case we have

$$h_k = (-1)^k g_{[1-k]_N}, \qquad k = 0, 1, \cdots, N - 1. \tag{5.5}$$

Example 5.2: A situation often used in finite field Fourier analysis is that in which $\mathcal{F} = \mathrm{GF}(2^q + 1)$ for an integer q such that $2^q + 1$ is prime. Cyclic wavelet transforms can be defined for such fields for all $n \leq q + 1$. Except in the case $n = q + 1$, the element α_o will simply be a power of the primitive element α of order 2^q in $\mathcal{F}^{[\times]}$. In particular, we have $\alpha_o = \alpha^{2(q-n+1)}$.

Example 5.3: The sequence (4.21) is a finite-field mother wavelet for any choice of $n > 1$, and for any choice of N' such that $\sqrt{2N'}$ and $\sqrt{1+4\sqrt{2N'}+8N'}$ exist in $\mathcal{F}$. In the case $\mathcal{F} = \mathrm{GF}(2^q+1)$, with 2^q+1 prime, exactly half of the nonzero elements of $\mathcal{F}$—in particular, those elements that are even powers of the primitive element α of order 2^q—have square roots in $\mathrm{GF}(2^q+1)$ (see, e.g., [13]). Thus, these conditions imply that N' must be of the form $\alpha^{2k}/2$ for some integer k in order to $\sqrt{2N'}$ to exist, and it must also be of the form $(1 \pm \alpha^l)^2/2$ for some integer l in order for $\sqrt{1+4\sqrt{2N'}+8N'}$ to exist. Note that the second condition is identical to the first, since all elements of $\mathrm{GF}(2^q+1)$ can be generated in the form $1 \pm \alpha^l$.

Example 5.4: As a specific example of the form described in Example 5.3, consider GF(17) (i.e., $q = 4$). Here, we have $\alpha = 6$ and $\alpha^2 = 2$, so the possible choices of N' are 1, 2, 4, 8, $9(\equiv \frac{1}{2})$, $13(\equiv \frac{1}{4})$, $15 \equiv \frac{1}{8}$, and 16. So, for example, the choice $N' = 9$ yields the mother wavelet

$$g = (1 \quad 16 \quad 0 \quad \cdots \quad 0 \quad 0), \tag{5.6}$$

which is the GF(17) equivalent of (4.19a). In this case, cyclic transforms can be specified for any length up to 32. Thus, for example, together with the choices (5.3)–(5.5), we have a complete length-16 transform:

$$\begin{aligned}
&g^1 = (1,\, 16,\, 0,\, 0, \cdots, 0,\, 0);\\
&h^1 = (16,\, 16,\, 0, \cdots, 0,\, 0,\, 0)\\
&g^2 = (1,\, 16,\, 0,\, 0,\, 0,\, 0,\, 0,\, 0);\\
&h^2 = (16,\, 16,\, 0, 0,\, 0,\, 0, 0, 0)\\
&g^3 = (1,\, 16,\, 0,\, 0); \qquad h^3 = (16,\, 16,\, 0,\, 0)\\
&g^4 = (1,\, 16); \qquad h^4 = (16,\, 16).
\end{aligned}$$

Example 5.5: As another example in GF(17), the choice $N' = 15$ in Example 5.3 gives the GF(17) equivalent of the mother wavelet of (4.22); namely,

$$g = (1 \quad 10 \quad 1 \quad 5 \quad 0 \quad \cdots \quad 0 \quad 0). \tag{5.7}$$

So, for example, on using the choice (5.3)–(5.5), another complete length-16 transform over GF(17) is thus specified by

$$\begin{aligned}
&g^1 = (1,\, 10,\, 1,\, 5,\, 0, \cdots, 0);\\
&h^1 = (10,\, 15,\, 0, \cdots, 0,\, 5,\, 16)\\
&g^2 = (1,\, 10,\, 1,\, 5,\, 0,\, 0,\, 0,\, 0);\\
&h^2 = (10,\, 15, 0,\, 0, 0,\, 0, 5,\, 16)\\
&g^3 = (1,\, 10,\, 1,\, 5); \qquad h^3 = (10,\, 15,\, 5,\, 16)\\
&g^4 = (2,\, 15); \qquad h^4 = (15;\, 15).
\end{aligned}$$

Remark 5.2: As a final remark, we note that the choice of N' is generally constrained as before if we impose the bandpass condition (3.6b). In particular, in the finite-field context, this condition together with (5.2a) implies that

$$\gamma^1(1) = -\gamma^0(1) = \pm\frac{1}{\sqrt{2N'}}. \tag{5.8}$$

Thus, N' is constrained in this case to be such that $2N'$ has a square root in $\mathcal{F}$. Note that the corresponding low-pass condition is

$$\eta^0(1) = \eta^1(1) = \pm\frac{\nu(1)}{\sqrt{2N'}}. \tag{5.9}$$

VI. Conclusion

In this paper, we have defined a wavelet transform associated with finite cyclic groups over arbitrary fields. For each cyclic group and field, there are a variety of transforms, parameterized by finite sequences of field elements satisfying the quadratic constraints (3.11). We have characterized such transforms in terms of the Fourier transforms of the corresponding sequences for the cases in which the field is the complex field or a finite field. The similarities between these two cases suggests a generalization of this characterization to arbitrary fields. Moreover, in the finite-field case, the rich structure of finite fields may yield further interesting properties of the finite-field wavelet transform. These are topics of interest for further study.

Potential applications areas for these transforms are similar to those for the cyclic Fourier transform, or for the discrete wavelet transform. For example, the finite-field wavelet transform might be applicable to the development of useful families of linear communication codes based on the use of Decomposition/Reconstruction as the coding/decoding algorithm. Alternatively, the multiscale/multilocation aspects of the cyclic wavelet transform might be useful in searching for transient structures in streams of data, analogously to what is done in searching for transient sonar signals with ordinary discrete-time wavelets. For example, this aspect of the wavelet transform might be useful in constructing communication codes with that allow efficient detection of error bursts.

Note that an important advantage of the cyclic wavelet transforms over cyclic Fourier analysis is lower computational complexity. If the rows of the matrices G^j and H^j each have at most M nonzero elements, then the jth stage of Decomposition/Reconstruction requires at most $MN2^{1-j}$ multiplications, and $(M-1)N2^{1-j}$ additions. So, the full decomposition requires at most $(2M-1)N\sum_{j=0}^{n-1} 2^{-j} = 2(2M-1)(N-1) \sim O(N)$ operations. By comparison, the FFT has $O(N\log_2(N))$ complexity.

In this paper, we have focused on decomposition algorithms that involve successive halvings of resolution. However, it is also possible to define analogous decompositions in which the resolution is decimated by some other integral amount, say q, at each stage. In this context, it would be of interest to consider data lengths that are powers of q. Note, however, that certain symmetries are lost when $q \neq 2$, since the two elements of the decomposition (i.e., c and d) would necessarily be of different lengths in this case. Nevertheless, the characterizations for the $q = 2$ transforms should generalize straightforwardly to this case. For example, the 2-circulant structure exploited in Theorem 1 would become a q-circulant structure; and the decomposition (4.2) of the mother wavelet on "even" and "odd" cuts would be replaced with a set of cuts at q distinct phases. Some recent results along these lines in the context of the conventional discrete-time wavelet transform are reported in [24].

Acknowledgment

The authors are grateful for the helpful comments and suggestions of the anonymous referees, which have improved the presentation of these results.

References

[1] J. Benedetto, "Gabor representations and wavelets," in *Commutative Harmonic Analysis*, D. Colella, Ed. Providence, RI: American Mathematical Society 1989.

[2] G. Beylkin, R. Coifman, and V. Rokhlin, "Fast wavelet transforms and numerical algorithms I," *Commun. Pure Appl. Math.*, vol. 44, pp. 141–185, Mar. 1991.

[3] I. Daubechies, "Orthonormal bases of compactly supported wavelets," *Commun. Pure Appl. Math.*, vol. 41, pp. 909–996, 1988.

[4] ——, "The wavelet transform, time-frequency localization and signal analysis," *IEEE Trans. Inform. Theory*, vol. 36, pp. 961–1005, Sept. 1990.

[5] C. Heil and D. Walnut, "Continuous and discrete wavelet transforms," *SIAM Rev.*, vol. 31, pp. 628–666, 1989.

[6] S.G. Mallat, "A theory of multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 11, pp. 674–693, 1989.

[7] G. Strang, "Wavelets and dilation equations: A brief introduction," *SIAM Rev.*, vol. 31, pp. 614–627, Dec. 1989.

[8] M.R. Dellomo and G.M. Jacyna, "Wigner transforms, Gabor coefficients, and Weyl–Heisenberg wavelet," *J. Acoust. Soc. Am.*, vol. 89, pp. 2355–2361, May 1991.

[9] P. Goupillaud, A. Grossman, and J. Morlet, "Cycle-octave and related transforms in seismic signal analysis," *Geoexploration*, vol. 23, pp. 85–102, 1984/85.

[10] A. Grossman, "Wavelet transforms and edge detection," in *Stochastic Processing in Physics and Engineering*, S. Albeverio, *et al.*, Eds. Dordrecht, The Netherlands: Reidel, 1988, pp. 149–157.

[11] R. Kronland-Martinet, J. Morlet, and A. Grossman, "Analysis of sound patterns through wavelet transforms," *Int. J. Pattern Recogn. and Artificial Intell.*, vol. 1, pp. 273–302, 1987.

[12] P.J. Burt and E.H. Adelson, "The Laplacian pyramid as a compact image code," *IEEE Trans. Commun.*, vol. COM-31, pp. 532–540, Apr. 1983.

[13] R.E. Blahut, *Theory and Practice of Error Control Codes.* Reading, MA: Addison-Wesley, 1983.

[14] ——, *Fast Algorithms for Digital Signal Processing.* Reading, MA: Addison-Wesley, 1984.

[15] J.W. Cooley, P.A. Lewis, and P.D. Welch, "The finite Fourier transform," *IEEE Trans. Audio Electroacoust.*, vol. AU-17, pp. 77–85, 1969.

[16] J.M. Pollard, "The fast Fourier transform in a finite field," *Math. of Computat.*, vol. 25, pp. 365–374, 1971.

[17] R.E. Blahut, *Algebraic Methods for Signal Processing and Communications Coding.* New York: Springer-Verlag, 1992.

[18] R.R. Coifman and M.V. Wickerhauser, "Entropy-based algorithms for best basis selection," *IEEE Trans. Inform. Theory*, vol. 38, no. 2, pt. II, pp. 713–718, Mar. 1992.

[19] G. Pirani and V. Zingarelli, "Analytical formula for design of quadrature mirror filters," *IEEE Trans. Acoust., Speech Signal Processing*, vol. ASSP-32, pp. 645–648, 1984.

[20] P.P. Vaidyanathan, "Quadrature mirror filter banks, M-band extensions and perfect-reconstruction techniques," *IEEE ASSP Mag.*, vol. 4, pp. 4–21, July 1987.

[21] ——, "Multirate digital filters, filter banks, polyphase networks, and applications: A tutorial," *Proc. IEEE*, vol. 78, no. 1, pp. 65–93, Jan. 1990.

[22] P.J. Davis, *Circulant Matrices.* New York: John Wiley, 1979.

[23] J.C. Pesquet, "Orthonormal wavelets for finite sequences," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Processing*, San Francisco, CA, Mar. 23–26, 1992, pp. IV-609–IV-612.

[24] D. Pollen, "$SU_I(2, F[z, \frac{1}{z}])$ for F a subfield of C," *J. Am. Math. Soc.*, vol. 3, pp. 611–624, July 1990.

[25] H. Zou and A. Tewfik, "Discrete orthogonal M-band wavelet decompositions," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Processing*, San Francisco, CA, March 23–26, 1992, pp. IV-605–IV-608.