Wavelet Transforms Associated with Finite Cyclic Groups

Giuseppe Caire
Dip. di Ingegneria Elettronica
Politecnico di Torino
Torino 10129 ITALY

Robert L. Grossman
Dept. of Mathematics
University of Illinois
Chicago, IL 60680 USA

H. Vincent Poor
Dept. of Electrical Engineering
Princeton University
Princeton, NJ 08544 USA

Abstract

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. This paper develops an analogous framework for the multiresolution analysis of finite-length sequences of elements from arbitrary fields. 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.

1 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. An important class of multiresolution decompositions are the so-called *Laplacian pyramid* schemes [1 - 3], 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 [2, 3].

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 [4, 5]. 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 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 applications.

This paper is an abbreviated version of [6], wherein proofs and other details can be found.

2 The Finite-length Wavelet Transform

The finite-length Fourier transform 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 in turn is based on the Laplacian pyramid scheme for image compression proposed by Burt and Adelson [1]. Its general use in multiresolution analysis

1058-6393/92 $03.00 © 1992 IEEE

has been explored by Mallat, Meyer, and others; and the reader is referred to [2] or [3] for a description of this scheme.

The discrete-time wavelet transform has been developed for sequences of complex numbers viewed as mappings from $\mathcal{Z}$, the set of integers, to $\mathcal{C}$, the set of complex numbers. The basic ideas behind this transform 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 $V_n \subset V_{n-1} \subset \ldots V_0 = \mathcal{F}^N$ where $\dim(V_j) = 2^{n-j}$. For each $j = 1, 2 \ldots, n$, define the subspace W_j to be the orthogonal complement of V_j in V_{j-1} so that

$$V_{j-1} = W_j \oplus V_j. \tag{2.1}$$

Here the notation $\oplus$ indicates the direct sum; i.e., (2.1) 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 (2.1) it follows that V_0 can be written as:

$$V_0 = W_1 \oplus W_2 \oplus \cdots \oplus W_n \oplus V_n. \tag{2.2}$$

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

$$\mathrm{MA} : v \rightarrow \{w^1, w^2, \ldots, w^n, v^n\}. \tag{2.3}$$

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

$$\mathrm{MS} : \{w^1, w^2, \ldots, w^n, v^n\} \rightarrow v = w^1 + w^2 + \ldots + w^n + v^n. \tag{2.4}$$

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

$$(H^j)^* H^j + (G^j)^* G^j = N'^{-1} I_{2^{n-j+1}}, \tag{2.5}$$

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

Within this framework, consider the following algorithm.

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

Step 1. Given c^0, compute

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

Step 2. In general, for $j = 1, 2, \ldots, n-1$, compute

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

Reconstruction. Given a decomposition $\{d^1, \ldots, d^n, c^n\}$, 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 $j = n-2, n-3 \ldots, 0$, 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 result, a proof of which can be found in [6].

Proposition 1: The algorithm defined by Decomposition/Reconstruction with matrices chosen to satisfy (2.5) is an MA-MS pair.

Remark 2.1 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" $\{d^1, d^2, \ldots, d^n, c^n\}$ 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 (2.5), there is an an associated finite-length wavelet transform (FLWT):

$$\mathrm{FLWT} : v \leftrightarrow \{d^1, d^2, \ldots, d^n, c^n\}. \tag{2.6}$$

Remark 2.2 Note that (2.5) defines a quadratic relationship among the elements of the matrices defining the finite-length wavelet transform. It may also be useful to specify other conditions, such as so-called "lowpass" and "bandpass" conditions analgous to those used in the discrete-time wavelet transform [2, 3]. These conditions, and the structure imposed by (2.5), will be discussed in the following sections.

3 The Cyclic Wavelet Transform

In the preceding section, we defined the finite-length wavelet transform in terms of the matrices $G^1, G^2, \ldots, G^n$ and $H^1, H^2, \ldots, H^n$ 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 the matrices G^j and H^j are constrained to be *2-circulants* [7] for each j; i.e., suppose G^j is of the form:

$$G^j = \begin{pmatrix} g_0^j & g_1^j & g_2^j & \cdots & g_{N_j-1}^j \\ g_{N_j-2}^j & g_{N_j-1}^j & g_0^j & \cdots & g_{N_j-3}^j \\ g_{N_j-4}^j & g_{N_j-3}^j & g_{N_j-2}^j & \cdots & g_{N_j-5}^j \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_2^j & g_3^j & g_4^j & \cdots & g_1^j \end{pmatrix}, \tag{3.1}$$

and where $N_j \triangleq 2^{n-j+1}$; and similarly for H^j. Note that a 2-circulant matrix is defined completely by its first row; and thus we can write $G^j = 2-\mathrm{cir}\{g^j\}$ and $H^j = 2-\mathrm{cir}\{h^j\}$ 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 (3.1), the j^{th} 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 2.

Thus, we conclude that Decomposition/Reconstruction with the 2-circulant constraint (3.1) 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 $\{g^j, h^j \in \mathcal{F}^{2^{n-j+1}} \mid j = 1, 2, \ldots, n\}$ such that (2.5) is satisfied for all j with $G^j = 2-\mathrm{cir}\{g^j\}$ and $H^j = 2-\mathrm{cir}\{h^j\}$. 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 (2.5) for the case $j = 1$, and then we will give a method to derive a family of sequences $\{g^j, h^j\}$, $j = 2, \ldots, n$, 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 $g_0, g_1, \ldots, g_{N-1}$ and $h_0, h_1, \ldots, h_{N-1}$ such that $2-\mathrm{cir}\{g\}$ and $2-\mathrm{cir}\{h\}$ satisfy (2.5) is characterized by the following proposition, (see [6] for a proof) which is stated in terms of the following finite-length Fourier transforms:

$$\gamma_k^j = \sum_{l=0}^{\frac{N}{2}-1} g_{2l+j}\alpha^{2lk}, \quad k = 0, 1, \ldots, \frac{N}{2}-1, \quad j = 0, 1, \tag{3.2a}$$

and

$$\eta_k^j = \sum_{l=0}^{\frac{N}{2}-1} h_{2l+j}\alpha^{2lk}, \quad k = 0, 1, \ldots, \frac{N}{2}-1, \quad j = 0, 1, \tag{3.2b}$$

where α is the relevant N^{th} 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 $G = 2-cir\{g_0, g_1, \ldots, g_{N-1}\}$ and $H = 2-cir\{h_0, h_1, \ldots, h_{N-1}\}$ satisfy (2.5) if and only if for each $k = 0, 1, \ldots, \frac{N}{2}-1$, we have

$$|\gamma_k^0|^2 + |\gamma_k^1|^2 = \frac{1}{N'}, \tag{3.3a}$$

and

$$\eta_k^j = (-1)^j \nu_k \overline{\gamma_k^{1-j}}, \quad j = 0, 1, \tag{3.3b}$$

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

Theorem 1 allows us to construct sequences whose corresponding 2-circulant matrices satisfy (2.5) for the case $j = 1$. Given two such sequences, we now wish to construct a family of sequences $\{g^j, h^j \mid j = 1, 2, \ldots, n\}$ that specifies an MA-MS scheme as described above. Such a construction is given by the following result, which is a straightforward corollary to Theorem 1.

Corollary 1: Suppose $G = 2 - \mathrm{cir}\{g\}$ and $H = 2 - \mathrm{cir}\{h\}$ are $2^{n-1} \times 2^n$ matrices of complex numbers satisfying (2.5). For each $j = 1, 2, \ldots, n$, define length-2^{n-j} sequences g^j and h^j by

$$g^j_{2\ell+m} = \mathrm{DFT}^{-1}\left\{\{\gamma^m_{2^{j-1}k} \mid k = 0, 1, \ldots, 2^{n-j} - 1\}\right\}_\ell, \tag{3.8}$$

and

$$h^j_{2\ell+m} = \mathrm{DFT}^{-1}\left\{\{\eta^m_{2^{j-1}k} \mid k = 0, 1, \ldots, 2^{n-j} - 1\}\right\}_\ell, \tag{3.9}$$

for $\ell = 0, 1, \ldots, 2^{n-j} - 1$, and $m = 0, 1$, where the sequences $\gamma^0, \gamma^1, \eta^0$, and η^1, are defined from g and h as in (3.2), and where the operation DFT indicates the discrete Fourier transform of appropriate length. Then $G^j = 2 - \mathrm{cir}\{g^j\}$ and $H^j = 2 - \mathrm{cir}\{h^j\}$ satisfy (2.5) for each $j = 1, 2, \ldots, n$.

Remark 3.1 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 3.2 It should be noted that the *bandpass condition*, $\sum_{k=0}^{N-1} g_k = 0$, is equivalent to the condition that $\gamma^1_0 = -\gamma^0_0$. 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 $\eta^1_0 = \eta^0_0$, and further that

$$|\gamma^0_0| = |\gamma^1_0| = |\eta^0_0| = |\eta^1_0| = \frac{1}{\sqrt{2N'}}. \tag{3.10}$$

Thus, from (3.10) we see that a corresponding *lowpass condition*,

$$\left|\sum_{k=0}^{N-1} h_k\right| = \sqrt{2/N'}. \tag{3.11}$$

is also enforced for each j.

Remark 3.3 We see from Theorem 1 that, in the 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.

Remark 3.4 From the necessary and sufficient conditions (3.3), we see that a cyclic wavelet transform can be designed by first selecting a sequence $g_0, g_1, \ldots, g_{N-1}$ to satisfy (3.3a) (this sequence plays the role of the so-called "mother" wavelet [3]), and then choosing $h_0, h_1, \ldots, h_{N-1}$ from (3.3b). The choice of $g_0, g_1, \ldots, g_{N-1}$ is further reduced to choosing, say, the even-indexed subset $g_0, g_2, \ldots, g_{N-2}$, to satisfy

$$N'|\gamma^0_k|^2 \le 1, \tag{3.12}$$

and then choosing $g_1, g_3, \ldots, g_{N-1}$ compatibly via the inverse of the relationship (3.2a).

Example 3.1 From a practical viewpoint, the sequence $g_0, g_1, \ldots, g_{N-1}$ should be chosen to have only a few nonzero elements. As an example, take $N' = 1/2$, and consider the choice

$$g_k = \delta_k, \quad k = 0, 2, \ldots, N-2. \tag{3.13}$$

This choice is equivalent to $\gamma^0_k \equiv 1$, which, through (3.3a), imposes the condition $|\gamma^1_k| \equiv 1$, or equivalently, $\gamma^1_k = \alpha^{\xi_k}$, with $\xi_0, \xi_1, \ldots \xi_{\frac{N}{2}-1}$, taken from the reals. Thus, any sequence of the form

$$g_k = \frac{2}{N} \sum_{l=0}^{\frac{N}{2}-1} \alpha^{-lk+\xi_l}, \quad k = 1, 3, \ldots, N-1, \tag{3.14}$$

is compatible with the choice (3.13). Imposition of the bandpass condition restricts only ξ_0 (to be $\frac{N}{2}$). The simplest such sequence results from the choice $\xi_k = \frac{N}{2} + k$, which leads to

$$g_k = -\delta_{k-1}, \quad k = 1, 3, \ldots, N-1; \tag{3.15}$$

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

Example 3.2 In this example, we define a transform similar to the Hadamard transform, described in Example 2.3. To do this, we continue with the example above. In order to choose the sequence $h_0, h_1, \ldots, h_{N-1}$, it is interesting to rewrite the condition (3.3b) directly as a relationship between the cyclic Fourier transforms of the sequences $g_0, g_1, \ldots, g_{N-1}$ and h_0,

$h_1, \ldots, h_{N-1}$, which we denote by $\gamma_0, \gamma_1, \cdots, \gamma_{N-1}$ and $\eta_0, \eta_1, \cdots, \eta_{N-1}$, respectively. In particular, Eq. (3.3b) can be rewritten straightforwardly as

$$\eta_k = -\nu_k \alpha^k \overline{\gamma_{k-\frac{N}{2}}}, \quad k = 0, 1, \ldots, N-1, \qquad (3.16)$$

where we have used the extension $\nu_k = \nu_{k-\frac{N}{2}}$, $k = \frac{N}{2}, \ldots, N-1$. The corresponding relationship between $g_0, g_1, \ldots, g_{N-1}$ and $h_0, h_1, \ldots, h_{N-1}$, is thus determined by the choice of the sequence $\nu_0, \nu_1, \ldots, \nu_{\frac{N}{2}-1}$. For example, with $\nu_k \equiv 1$, (3.16) is equivalent to

$$h_k = (-1)^k \overline{g_{[1-k]_N}}, \quad k = 0, 1, \ldots, N-1, \qquad (3.17)$$

where $[x]_N$ denotes x reduced modulo N.

Thus, an example of a sequences generating a cyclic wavelet transform are those given by (3.1), (3.15), and (3.17); namely,

$$g = (1 \quad -1 \quad 0 \quad \cdots \quad 0 \quad 0), \qquad (3.18a)$$

and

$$h = (-1 \quad -1 \quad 0 \quad \cdots \quad 0 \quad 0). \qquad (3.18b)$$

A complete transform is thus specified by (3.18) and Corollary 1. For example, for the case $N = 8$, we obtain the filters

$$g^1 = (1,-1,0,0,0,0,0,0) \qquad h^1 = (-1,-1,0,0,0,0,0,0)$$
$$g^2 = (1,-1,0,0) \qquad h^2 = (-1,-1,0,0)$$
$$g^3 = (1,-1) \qquad h^3 = (-1,-1)$$

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 3.3 The next level of transform complexity (aside from other choices of the sequence ν_k) arises from setting $g_k = 0$, for $k > 2$. Assuming that the coefficients of the mother wavelet are real, they are related through Theorem 1 by the equations:

$$g_0 g_2 = -g_1 g_3, \qquad (3.19a)$$

and

$$(g_0)^2 + (g_1)^2 + (g_2)^2 + (g_3)^2 = \frac{1}{N'}. \qquad (3.19b)$$

Note from (3.19a) 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, then, modulo the above noted symmetry, the mother wavelet is given for $N' < (3 + 2\sqrt{2})/8$, by

$$g_0 = 1, \qquad (3.20a)$$

$$g_1 = \frac{\zeta - \sqrt{2 - \zeta^2}}{2 - \zeta - \sqrt{2 - \zeta^2}}, \qquad (3.20b)$$

$$g_2 = -g_1 \frac{g_1 + 1}{g_1 - 1}, \qquad (3.20c)$$

and

$$g_3 = \frac{g_1 + 1}{g_1 - 1}, \qquad (3.20d)$$

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

With $N' = 1/2$, (3.20) reduces to the previous example, $g_1 = -1$, and $g_2 = g_3 = 0$. For other choices of N' the mother wavelet from (3.20) will differ nontrivially from (3.13), (3.15). For example, the choice $N' = 1/8$ yields the mother wavelet

$$g_0 = 1; \quad g_1 = \frac{1}{1 - \sqrt{2}}; \quad g_2 = 1; \quad g_3 = \sqrt{2} - 1. \qquad (3.21)$$

Thus, for example, on choosing h from (3.17), Corollary 1 gives the following $N = 8$ cyclic transform.

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

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

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

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

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

4 Finite-field Wavelet Transforms

We now consider the cyclic wavelet transform described by Decomposition/Reconstruction with transform matrices as in (3.1) 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 $\{g^j, h^j \in \mathcal{F}^{2^{n-j+1}} \mid j = 1, 2, \ldots, n\}$ such that (2.5) is satisfied for all j.

Within this model, we state a result analagous to Theorem 1. (Again, the proof can be found in [6].) To do so, we first define polynomials in $\mathcal{F}[x]$:

$$\gamma^j(x) = \sum_{l=0}^{\frac{N}{2}-1} g_{2l+j} x^l, \quad j = 0, 1, \tag{4.1a}$$

and

$$\eta^j(x) = \sum_{l=0}^{\frac{N}{2}-1} h_{2l+j} x^l, \quad j = 0, 1. \tag{4.1b}$$

Theorem 2: Consider the cyclic wavelet transform of length $N = 2^n$ over the field $\mathcal{F} = \mathrm{GF}(p^r)$. The sequences $g_0, g_1, \ldots, g_{N-1}$ and $h_0, h_1, \ldots, h_{N-1}$ satisfy (2.5) if and only if, for each $k = 0, 1, \ldots, \frac{N}{2} - 1$, we have

$$\gamma^0(\alpha_o^{-k})\gamma^0(\alpha_o^k) + \gamma^1(\alpha_o^{-k})\gamma^1(\alpha_o^k) = \frac{1}{N'}, \tag{4.2a}$$

and

$$\eta^j(\alpha_o^k) = (-1)^j \nu(\alpha_o^k)\gamma^{1-j}(\alpha_o^{-k}), \quad j = 0, 1, \tag{4.2b}$$

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

Analogously to Corollary 1 in the preceding section, we also have the following result.

Corollary 2: Suppose $G = 2 - \mathrm{cir}\{g\}$ and $H = 2 - \mathrm{cir}\{h\}$ are $2^{n-1} \times 2^n$ matrices of elements of $\mathcal{F}$ satisfying (2.5). For each $j = 1, 2, \ldots, n$, define two length-2^{n-j} sequences g^j and h^j by

$$g^j_{2\ell+m} = \mathrm{DFT}^{-1}\left[\{\gamma^m(\alpha_o^{2^{j-1}k}) \mid k = 0, 1, \ldots, 2^{n-j} - 1\}\right]_\ell, \tag{4.3}$$

and

$$h^j_{2\ell+m} = \mathrm{DFT}^{-1}\left[\{\eta^m(\alpha_o^{2^{j-1}k}) \mid k = 0, 1, \ldots, 2^{n-j} - 1\}\right]_\ell, \tag{4.4}$$

for $\ell = 0, 1, \ldots, 2^{n-j} - 1$, and $m = 0, 1$, where the sequences $\gamma^0, \gamma^1, \eta^0$, and η^1, are defined from g and h as in (4.1), and where the operation DFT indicates the number theoretic discrete Fourier transform of appropriate length. Then $G^j = 2 - \mathrm{cir}\{g^j\}$ and $H^j = 2 - \mathrm{cir}\{h^j\}$ satisfy (2.5) for each $j = 1, 2, \ldots, n$.

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 (4.2a), to choose h according to (4.2b), and then to choose the lower-order filters from Corollary 2.

Example 4.1 Analogously with the complex case (3.17), it is interesting to consider the choice $\nu(x) \equiv 1$, in which case we have

$$h_k = (-1)^k g_{[1-k]_N}, \quad k = 0, 1, \ldots, N - 1. \tag{4.5}$$

Example 4.2 A situation often used in finite field Fourier analysis is that in which $\mathcal{F} = \mathrm{GF}(2^m + 1)$ for an integer m such that $2^m + 1$ is prime. Cyclic wavelet transforms can be defined for such fields for all $n \leq m + 1$. Except in the case $n = m + 1$, the element α_o will simply be a power of the primitive element α of order 2^m in $\mathcal{F}^{[\times]}$. In particular, we have $\alpha_o = \alpha^{2^{(m-n+1)}}$.

Example 4.3 The sequence (3.20) 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 $\mathcal{F} = \mathrm{GF}(2^m + 1)$, with $2^m + 1$ 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^m - have square roots in $GF(2^m + 1)$ (see, e.g., [4]). Thus, the above conditions imply that N' must be of the form $\frac{\alpha^{2k}}{2}$ for some integer k in order for $\sqrt{2N'}$ to exist, and it must also be of the form $\frac{(1 \pm \alpha^\ell)^2}{2}$ 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 $GF(2^m + 1)$ can be generated in the form $1 \pm \alpha^\ell$.

Example 4.4 As a specific example of the form described in Example 4.3, consider $GF(17)$ (i.e., $m = 4$). 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

$$g = (1 \quad 16 \quad 0 \quad \cdots \quad 0 \quad 0), \tag{4.6}$$

which is the $GF(17)$ equivalent of (3.18a). In this case, cyclic transforms can be specified for any length

up to 32. Thus, for example, together with the choices (4.3)-(4.5), we have a complete length-16 transform:

$$g^1 = (1,16,0,0,\cdots,0,0) \quad ; \quad h^1 = (16,16,0,\cdots,0,0,0)$$
$$g^2 = (1,16,0,0,0,0,0,0) \quad ; \quad h^2 = (16,16,0,0,0,0,0,0)$$
$$g^3 = (1,16,0,0) \quad ; \quad h^3 = (16,16,0,0)$$
$$g^4 = (1,16) \quad ; \quad h^4 = (16,16)$$

Example 4.5 As another example in $GF(17)$, the choice $N' = 15$ in Example 4.3 gives the $GF(17)$ equivalent of the mother wavelet of (3.21); namely,

$$g = (1 \quad 10 \quad 1 \quad 5 \quad 0 \quad \cdots \quad 0 \quad 0). \tag{4.7}$$

So, for example, on using the choice (4.3)-(4.5), another complete length-16 transform over $GF(17)$ is thus specified by

$$g^1 = (1,10,1,5,0,\cdots,0) \quad ; \quad h^1 = (10,15,0,\cdots,0,5,16)$$
$$g^2 = (1,10,1,5,0,0,0,0) \quad ; \quad h^2 = (10,15,0,0,0,0,5,16)$$
$$g^3 = (1,10,1,5) \quad ; \quad h^3 = (10,15,5,16)$$
$$g^4 = (2,15) \quad ; \quad h^4 = (15,15)$$

Remark 4.2 As a final remark, we note that the choice of N' is generally constrained as above if we impose a bandpass condition. In particular, in the finite-field context, this condition together with (4.2a) implies that

$$\gamma^1(1) = -\gamma^0(1) = \pm\frac{1}{\sqrt{2N'}}. \tag{4.8}$$

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

$$\eta^0(1) = \eta^1(1) = \pm\frac{\nu(1)}{\sqrt{2N'}}. \tag{4.9}$$

5 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, parametrized by finite sequences of field elements satisfying the quadratic constraints (2.5). 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.

Acknowledgment

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.

References

[1] 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. 1982.

[2] I. Daubechies, "Orthonormal bases of compactly supported wavelets," *Comm. Pure Appl. Math.*, Vol. 41, pp. 909-996, 1988.

[3] S. G. Mallat, "A Theory of multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 11, pp. 674–693, 1989.

[4] R. E. Blahut, *Theory and Practice of Error Control Codes.* Addison-Wesley, Reading, MA, 1982.

[5] R. E. Blahut, *Fast Algorithms for Digital Signal Processing.* Addison-Wesley, Reading, MA, 1983.

[6] G. Caire, R. L. Grossman, and H. V. Poor, "Wavelet transforms associated with finite cyclic groups," *IEEE Trans. Inform. Theory*, to appear.

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