Cyclic wavelet transforms for arbitrary finite data lengths

Sandip Sarkar\textsuperscript{a,},* H. Vincent Poor\textsuperscript{b}

\textsuperscript{a}Corporate Research and Development, QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, CA 92121, USA
\textsuperscript{b}Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

Received 16 September 1999; received in revised form 28 March 2000

Abstract

Multiresolution analysis via decomposition into wavelets has been established as an important transform technique in signal processing. A wealth of results is available on this subject, and particularly, the framework has been extended to treat finite length sequences of size $2^n$ (for positive integers $n$) over finite fields. The present paper extends this idea further to provide a framework for dealing with arbitrary finite data lengths. This generalization is largely motivated in part by the need for such transforms for building error correcting codes in the wavelet transform domain. Here we extend the previous two-band formulation of the transform to treat a $p$-band case in general (i.e. for data length $p^n$), where $p$ is a prime number, and we also give a general result for developing transforms over composite-length sequences. Potential applications and computational complexity issues are discussed as well. © 2000 Elsevier Science B.V. All rights reserved.

Zusammenfassung


Résumé

L’analyse multirésolution via une décomposition en ondelettes a été établie comme une technique de transformation importante en traitement de signaux. Un riche ensemble de résultats est disponible sur ce sujet et particulièrement, ce cadre a été étendu pour traiter des séquences de longueur finie de taille $2^n$ (pour $n$ des entiers positifs) sur des champs finis. L’article présente étend davantage cette idée pour fournir un cadre de travail permettant de traiter des longueurs de données finies arbitraires. Cette généralisation est largement motivée en partie par le besoin de construire des telles

\textsuperscript{*}This research was supported by the U.S. Office of Naval Research under Grant N00014-00-1-0141.

*Corresponding author. Tel.: 858-651-2357; fax: 858-658-5006.

E-mail address: ssarkar@qualcomm.com (S. Sarkar).
transformations des codes correcteurs d’erreurs dans le domaine transformé en ondelettes. Ici, nous étendons la formulation antérieure de la transformation à deux bandes pour traiter le cas à $p$ bandes en général (i.e. des données de longueur $p^n$), où $p$ est un nombre premier, et nous donnons aussi un résultat général pour développer des transformations sur des séquences de longueur composite. Nous discutons aussi des applications potentielles et des problèmes de complexité de calcul. © 2000 Elsevier Science B.V. All rights reserved.

**Keywords:** Perfect reconstruction; Finite fields; Multiresolution analysis; Wavelet transforms; Filter banks

1. Introduction

In this paper, we consider the problem of multi-resolution analysis of sequences via wavelet decomposition [4], a technique that has emerged as an important tool in the processing of signals and images (e.g. [6]) over the past decade. The nested vector space structure of the multiresolution analysis [11] has been used in [3] to extend the definition of wavelet transforms to finite-length sequences over possibly finite fields. In particular, the concept of a cyclic wavelet transform for sequences of length $2^n$ was introduced in [3] using a framework similar to that used for the number theoretic Fourier transform [2]. Recent work in the use of wavelet transforms to build multilevel error-correcting codes [13] motivates a need for similar cyclic wavelet transforms for sequences of arbitrary finite lengths. Such transforms would also be of interest in building filter banks for multirate signal processing on finite sequences. The purpose of this paper is to develop such transforms.

The structure of the wavelet transform lends itself to a well-known filter bank description. Filter banks have been widely studied in the digital signal processing literature, e.g. [5,8]. Initially studied in the context of quadrature mirror filter banks for two-band systems, a well-established theory now exists for $p$-bands ($p > 2$) as described in [15,14]. Such filter banks have been shown to significantly decrease the number of operations required for FIR filtering [10]. In this paper, we make use of the concept of a $p$-band filter banks in order to generalize the transform structure as presented in [3] to arbitrary finite data lengths.

The paper is organized as follows. After a brief review of the 2-band cyclic wavelet transform, we extend its definition to admit $p$-band transforms over the complex field, which allows for data lengths of the form $p^n$. A Fourier domain characterization of such transforms is presented, which helps in easily identifying and designing valid transforms. We also extend the notions to finite fields [9], treating in general the wavelet packet description. Then, we extend these definitions further to include arbitrary finite data lengths. Finally, we conclude the paper with a brief discussion of potential applications.

2. Two-band cyclic wavelet transforms

In this section, we provide a description of the cyclic wavelet transform for sequences of lengths $2^n$, as developed in [3]. This description is necessarily brief, and the reader is referred to [3] for further details.

2.1. Finite-length wavelet transforms

We will focus on the description of wavelet transforms in terms of perfect reconstruction filter banks [15]. An important class of such transforms 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. 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 wavelet transform of interest. Suitable choice of the filters used in this process renders this transform invertible (the so-called perfect reconstruction property); and such suitable filters can be characterized for the infinite-length case through their discrete-time Fourier properties (e.g. [11]).
As described in [3], the Laplacian pyramid 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. 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

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

and

$$(H^j)(G^j)^* = 0_{2^n-j+1},
$$
(2)

where $I_k$ denotes the $k \times k$ identity matrix, $0_k$ denotes the $k \times k$ matrix with all zero entries, and where $N' \in \mathcal{F}$ is a constant whose choice will be discussed below. (Here, the asterisk denotes the adjoint.) Eqs. (1) and (2) are the perfect reconstruction conditions for the finite-length cases.

Within this framework, consider the following algorithm.

**Decomposition.** Given $c^0 = v \in \mathcal{F}^{2^n}$ and an integer $n > 0$, compute $d^1, \ldots, d^n, c^n$ as follows:

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

**Reconstruction.** Given a decomposition $\{d^1, \ldots, d^n, c^n\}$, reconstruct the original signal $v = c^0$ by computing, for $j = n - 1, n - 2, \ldots, 0$,

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

The perfect reconstruction conditions (1) and (2) assure that the mapping $v \rightarrow \{d^1, d^2, \ldots, d^n, c^n\}$ defined by decomposition/reconstruction is one-to-one, and this mapping specifies a finite-length wavelet transform.

2.2. Cyclic wavelet transforms for data lengths $2^n$

The finite-length wavelet transform is described 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 $\mathcal{F}$. This can be accomplished by constraining the matrices $H^j$ and $G^j$ to be $2$-circulants [7] for each $j$, i.e., they are constrained to be of the form

$$
A^j = \begin{pmatrix}
    a_0 & a_1 & a_2 & \cdots & a_{k-1} \\
    a_{k-2} & a_{k-1} & a_0 & \cdots & \vdots \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    a_2 & a_3 & a_4 & \cdots & a_0
\end{pmatrix},
$$
(3)

where $N_j \triangleq 2^{n-j+1}$. Since a $2$-circulant matrix is defined completely by its first row, 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. The vector $g^j$ is referred to as the mother wavelet.

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), the $(j + 1)$st step of decomposition defines a finite-impulse-response (FIR) filtering of the periodic sequence $c^{j-1}$ with 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 conventional Laplacian pyramid [11].

In addition to the perfect-reconstruction property, it is also customary to impose the lowpass condition:

$$
\sum_{k=0}^{N-1} h_k = \sqrt{2}, \quad j = 1, 2, \ldots, n
$$
(4)

and the complementary bandpass condition:

$$
\sum_{k=0}^{N-1} g_k = 0, \quad j = 1, 2, \ldots, n.
$$
(5)

This makes the scheme consistent with the idea of a filter with the perfect reconstruction property, that has been widely studied in signal processing literature (see e.g [15]). As shown in [3] (and as we shall discuss below), cyclic wavelet transforms can
be designed for the case in which $\mathcal{F}$ is the complex field or certain finite fields by first choosing the mother wavelet $g^1$ to have appropriate Fourier properties and then computing $g^2, \ldots, g^n$ and $h^1, \ldots, h^n$ from $g^1$ in a simple way.

Note that other properties like local support, vanishing moments or regularity can be obtained by enforcing similar constraints on the filter coefficients, depending on the application. It can be seen from the construction methods of such wavelets that these conditions only add additional constraints on a general class of transforms, which have a multitude of applications as outlined in [3]. One of the main uses of these kind of transforms comes from their application to building error correcting codes.

3. $p$-Band wavelet transforms

In order to define wavelet transforms for data lengths $p^n$, where $p$ is a prime, and $n$ is a positive integer, it is convenient to split the frequency domain into $p$, rather than 2 subbands [12]. To this end, for $j = 1, 2, \ldots, n$, we define matrices $G^j_1, G^j_2, \ldots, G^j_p$, over $\mathcal{F}$ of dimension $p^{n-j} \times p^{n-j+1}$. We would like the decomposition to have the perfect reconstruction property. Furthermore, the subbands should be orthogonal to each other. Hence, the following properties are desirable:

$$\sum_{i=1}^p (G^j_i)^* G^j_i = (N')^{-1}I_{p^{j-1}},$$  \hspace{1cm} (6)

where $N'$ is a non-zero element from the field (whose choice will be discussed later), and

$$G^j_i(G^j_i)^* = 0_{p^{j-1}}, \hspace{0.5cm} \forall i, k = 1, \ldots, p, i \neq k.$$  \hspace{1cm} (7)

We will refer to (6) as the perfect reconstruction property, and (7) as the orthogonality property.

It is interesting to note that (7) follows naturally if we choose the matrices such that they satisfy (6). In fact, the following theorem can be stated.

**Theorem 3.1.** The matrices $G^j_i$ satisfy the perfect reconstruction property if and only if they satisfy the orthogonality property and satisfy $G^j_i(G^j_i)^* = (N')^{-1}I_{p^{j-1}}$ for $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, n$.

**Proof.** Consider the matrix

$$G^j_i = \begin{pmatrix} G^j_1 \\ G^j_2 \\ \vdots \\ G^j_p \end{pmatrix}.$$

Then, (6) can be recast in the form of a matrix equation

$$(G^j_i)^* G^j_i = (N')^{-1}I_{p^{j-1}}$$

$$\Rightarrow (N')^{-1}I_{p^{j-1}} = (G^j_i)^* G^j_i.$$  \hspace{1cm} (8)

As the identity matrix is commutative under matrix multiplication, we get

$$\Rightarrow (G^j_i)^* (N')^{-1}I_{p^{j-1}} - (G^j_i)^* G^j_i = 0_{p^{j-1}}.$$  \hspace{1cm} (9)

Note that the matrix $G^j_i$ must have full rank for it to satisfy the perfect reconstruction property. Hence it has an inverse. Multiplying both sides of the previous equation by $(G^j_i)^{-1}$, for $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, n$, we must have $G^j_i(G^j_i)^* = (N')^{-1}I_{p^{j-1}}$ and the orthogonality property.

Conversely, given the orthogonality property, and for each $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, n$, $G^j_i(G^j_i)^* = (N')^{-1}I_{p^{j-1}}$, form the product $(G^j_i)^* G^j_i$. Clearly, then the perfect reconstruction property holds. $\square$

Analogously with the 2-band framework, we can define a $p$-band wavelet transform through the following algorithm:

**Decomposition.** Given $c^0_i = v \in \mathcal{F}^{p^i}$ and an integer $n > 0$, for $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, n$, compute $c^{i+1}_j = G^{i+1}_j c^i_j$.

**Reconstruction.** Given a decomposition, reconstruct the original signal $v = c^0_1$ by computing for
that have the perfect reconstruction property, it is useful to look at a Fourier transform characterization. We again consider data lengths \( p^n \), and would like to find a set of matrices \( G_1 = p - \text{cir}\{g_1\}, \ldots, G_p = p - \text{cir}\{g_p\} \) such that the perfect reconstruction and orthogonality properties hold. As in [3], it is convenient to consider such conditions in the Fourier domain. To do so, we restrict attention for the moment to the complex field, \( \mathcal{F} = \mathbb{C} \).

Consider the \( p^2 \) Fourier transforms

\[
(g_{m}^{n})_{k} = \sum_{i=0}^{N/p-1} (g_{m})_{pt+m} \beta^{pk}, \quad k = 0, 1, \ldots, N/p - 1, \quad m = 0, 1, \ldots, p - 1, \quad i = 1, 2, \ldots, p, \tag{9}
\]

where \( N = p^n \) and \( \beta \) is the \( N \)th prime root of unity: \( \beta = e^{2\pi \xi/N} \). Let \( \xi \) denote the complex conjugate of the number \( \xi \). We can state the following:

**Theorem 4.1.** The matrices \( p - \text{cir}\{g_i\} \) satisfy (1) if and only if, for each \( k = 0, 1, \ldots, N/p - 1, \) and \( i = 1, \ldots, p \), we have

\[
\sum_{m=0}^{p-1} |(g_{m}^{n})_{k}|^2 = \frac{1}{N}, \tag{10}
\]

and

\[
\sum_{m=0}^{p-1} (g_{m}^{n})_{k} (g_{m}^{n})_{j} = 0, \quad j = 0, 1, \ldots, p - 1, \quad i \neq j. \tag{11}
\]

**Proof.** For \( m = 0, 1, \ldots, p - 1 \), consider the \( N/p \times N/p \) 1-circulant matrices \( A_{m}^{n} \) with first rows \((g_{m}^{n}, g_{m}^{n+p}, \ldots, g_{m}^{N/p+m})\). Then the perfect reconstruction property is also expressed by simple rearrangement of the rows of the matrices \( G_i \) as

\[
(A_{0}^{n} A_{1}^{n} \ldots A_{p-1}^{n})(A_{0}^{n} A_{1}^{n} \ldots A_{p-1}^{n})^* = (N)^{-1} I_{N/p} \tag{12}
\]

and by Theorem 3.1,

\[
(A_{0}^{n} A_{1}^{n} \ldots A_{p-1}^{n})(A_{0}^{n} A_{1}^{n} \ldots A_{p-1}^{n})^* = 0_{N/p},
\]

\[
i, j = 0, 1, \ldots, p - 1, \quad i \neq j. \tag{13}
\]

The matrices \( A_{m}^{n} \) are diagonalizable by Fourier matrices as they are 1-circulant matrices. Choose \( F \) such that \( (F)_{kl} = \beta^{kl} \) for \( k, l = 0, 1, \ldots, p - 1 \). Then the eigenvalues of the matrix \( A_{m}^{n} \) are

\[
j = n - 1, n - 2, \ldots, 0 \quad \text{and} \quad i = 1, 2, \ldots, p.
\]

\[
c_{i}^{j} = N \left[ \sum_{i=1}^{p} (G_{i}^{j+1}) c_{i}^{j+1} \right].
\]

It is easily verified that the mapping \( v \leftrightarrow \{c_{i}^{j}, c_{i}^{j+1}\} \) for \( i = 2, \ldots, p \) and \( j = 1, 2, \ldots, n \) defined by decomposition/reconstruction is one-to-one if (6) is satisfied. For this case \( v \leftrightarrow \{c_{i}^{j}, c_{i}^{j+1}\} \) defines a \( p \)-band finite-length wavelet transform.

**3.1. \( p \)-Band cyclic wavelet transform**

To get a cyclic wavelet transform from this structure, we restrict the matrices \( G_{i}^{j} \) to be \( p \)-circulants, i.e., they are of the form

\[
A_{i}^{j} = \begin{pmatrix}
    a_{0} & a_{1} & a_{2} & \ldots & a_{N_{j}-1} \\
    a_{N_{j}-p} & a_{N_{j}-p+1} & a_{N_{j}-p+2} & \ldots & a_{N_{j}-p-1} \\
    \vdots & \vdots & \vdots & & \vdots \\
    a_{p} & a_{p+1} & a_{j} & \ldots & a_{p-1}
\end{pmatrix}.
\tag{8}
\]

In this case, the decomposition can be thought of as a filtering operation followed by decimation by a factor of \( p \). This is illustrated in Fig. 1 for the case \( p = 3 \).

**4. Fourier domain characterization for lengths \( p^n \)**

So far, we have characterized a set of matrices that define wavelet transforms. To find the matrices

![Fig. 1. Implementing the wavelet transform.](image-url)
\((g^m_i)_{0 \leq i \leq 1, \ldots , \text{and } i^m_{N/p-1}}\). Hence, we have, for \(m = 0,1,\ldots , p - 1\),

\[
A_i^m = \frac{p}{N} F^* I_i^m F,
\]

where \(I_i^m = \text{diag}\{(g^m_i)_{0 \leq i \leq 1, \ldots , \text{and } i^m_{N/p-1}}\}\). Then, we get for each \(i = 0,1,\ldots , p - 1\)

\[
p^{-1} \sum_{m=0}^{p-1} \|I_i^m(I_j^m)^*\| = (N^{-1}) I
\]

and

\[
p^{-1} \sum_{m=0}^{p-1} \|I_i^m(I_j^m)^*\| = 0, i,j = 0,1,\ldots , p - 1, i \neq j.
\]

It is now obvious that the required conditions on the Fourier transforms are, for each \(k = 0,1,\ldots , N/p - 1\),

\[
p^{-1} \sum_{m=0}^{p-1} |(g^m_i)_{k}|^2 = (N^{-1})
\]

and

\[
p^{-1} \sum_{m=0}^{p-1} |(g^m_i)_{k}| = 0, i,j = 1,\ldots , p, i \neq j.
\]

Hence, the theorem is proved. \(\Box\)

### 4.1. Algorithm for constructing p-band wavelets over \(\mathbb{C}\)

The above result suggests an algorithm for constructing the vectors \(g_i\) to satisfy the perfect reconstruction property. Let \(\langle \mu | v \rangle\) denote the standard inner product of \(\mu\) and \(v\) over \(\mathbb{C}^p\). For each \(k\), let \(\gamma_k = (g^0_1, g^1_2, \ldots , g^{p-1}_p), i = 1,2,\ldots , p\). Choose a linearly independent set of \(p\) non-zero \(p\)-vectors over \(\mathbb{C}\) \(\{\eta_i, i = 1,2,\ldots , p\}\). Obtain an orthogonal linearly independent set of vectors \(\{\xi_i, i = 1,2,\ldots , p\}\) from them by the Gram–Schmidt process, i.e.

\[
\zeta_1 = \eta_1,
\]

\[
\zeta_2 = \eta_2 - \frac{\langle \eta_2 | \zeta_1 \rangle}{||\zeta_1||^2} \zeta_1,
\]

\[
\vdots
\]

\[
\zeta_p = \eta_p - \sum_{i=1}^{p-1} \frac{\langle \eta_p | \zeta_i \rangle}{||\zeta_i||^2} \zeta_i.
\]

Let \(\gamma_1 = \sqrt{\text{Area}}||\zeta_1||\).

Take the inverse Fourier transform to get

\[
(g^m_i)_{p+m} = \frac{p}{N} \sum_{k=0}^{N/p-1} \langle \gamma^m_i | k \rangle b^{-pk}.
\]

Then, the vectors \(g_i\) specify one level of a wavelet transform. This is obvious from the previous theorem. It states that the Fourier transforms must be a set of orthogonal linearly independent vectors such that their norm is \(1/\sqrt{N}\). But this is exactly how we constructed these vectors. Hence, they meet our requirements.

This procedure simplifies for the two-band case. To see this, fix \(k\), and choose a linearly independent set of vectors \(\delta = (\delta_0, \delta_1)\) and \(\epsilon = (\epsilon_0, \epsilon_1)\), which form a basis for \(\mathbb{C}^2\). Let \(\gamma \triangleq \sqrt{N} ||\delta||\). Applying the Gram–Schmidt process, we get

\[
\zeta_0 = \epsilon_0 - \gamma \frac{\epsilon_0 \gamma_0^* + \epsilon_1 \gamma_1^*}{|\gamma_0|^2 + |\gamma_1|^2} |\gamma_0|^2 - |\gamma_1|^2
\]

\[
= \gamma \left( |\gamma_0|^2 - |\gamma_1|^2 \right)
\]

A similar calculation shows that

\[
\zeta_1 = -\gamma \frac{\epsilon_0 \gamma_1^* - \epsilon_1 \gamma_0^*}{|\gamma_0|^2 + |\gamma_1|^2} |\gamma_0|^2 + |\gamma_1|^2
\]

Let \(\gamma_1 \triangleq \gamma_1\) and \(\gamma_2 \triangleq \eta\). Then, we will have

\[
\eta \triangleq \frac{\gamma}{\sqrt{N} ||\gamma||}.
\]

Hence, after normalization, the function \((1/\sqrt{N} ||\gamma||) (\epsilon_0 \gamma_1^* - \epsilon_1 \gamma_0^*/(|\gamma_0|^2 + |\gamma_1|^2)) \triangleq \psi\) is such that \(|\psi|^2 = 1\). As we had fixed \(k\) for the whole discussion, the above must hold for each \(k\). This gives us the explicit formula for a previously known result:

**Theorem 4.2** (See Caire et al. [3]). Let \(N' \in \mathbb{R}\) be any positive non-zero element and \(N = 2^a\). The matrices \(G = 2 - \text{cir} \{(g_0)_0, (g_1)_1, \ldots , (g_{N-1})_{N-1}\}\) and \(H = 2 - \text{cir} \{(h_0)_0, (h_1)_1, \ldots , (h_{N-1})_{N-1}\}\) satisfy (1) if.

\(\forall k \in \{0,1,\ldots , N/2 - 1\}\), we have

\[
|\gamma_0|^2 + |\gamma_1|^2 = \frac{1}{N}
\]

(19)
Corollary 4.1

The lower-order transforms straightforwardly from the first-level transform.

Corollary 4.1 (See also Caire et al. [3]). Suppose $G = p - \text{circ}(g)$ and $H = p - \text{circ}(h)$ are two $p^{n-1} \times p^n$ matrices satisfying (1). For each $j = 1, 2, \ldots, n$, define $p$ length-$p^{n-j}$ sequences $g^j_i$, $i = 1, \ldots, p$ by

$$
(g^j_i)_{pl+m} = \text{DFT}^{-1}\{\{c^j_i\}_{p^{-j}k}|k = 0, 1, \ldots, p^{n-j} - 1, i = 1, \ldots, p\}_{pl+m}
$$

for $l = 0, 1, \ldots, p^{n-j} - 1$ and $m = 0, 1, \ldots, p - 1$, where the sequences $c^j_i$ are defined as in Eq. (9). Then the matrices $G^j = p - \text{circ}[g^j]$ satisfy (1) for each $j = 1, 2, \ldots, n$.

As frequency sampling does not degrade the frequency response, this method gives us an efficient way to calculate the lower-order transforms. Fig. 2 illustrates this concept for the case $p = 2$.

5. Finite-field wavelet transforms

We now consider the cyclic wavelet transform described by decomposition/reconstruction with transform matrices as in (3) for the case in which $\mathcal{F}$ is a finite field: $\mathcal{F} = \mathbb{GF}(q^\kappa)$, where $q$ is an odd prime and $\kappa$ is a positive integer. We again restrict the data length $N = p^n$; and we assume that $p^{n-1}$ divides $q^\kappa - 1$. This latter condition implies the existence of an order-$p^{n-1}$ element $\alpha$ of the multiplicative sub-group of $\mathcal{F}$. We will comment further about this requirement later.

Within this model, we can characterize cyclic wavelet transforms by considering the Fourier properties of $g^1_1, g^2_1, \ldots, g^n_1$, for $i = 1, 2, \ldots, p$. To do so, for a given transform level, we first define polynomials

$$
\gamma^m_i(x) = \sum_{r=0}^{N/p-1} (g_i)_{pr+m}x^r, \quad m = 0, 1, \ldots, p - 1.
$$

Theorem 5.1. The matrices $p - \text{circ}[g^j_i]$ satisfy (1) if and only if, for each $k = 0, 1, \ldots, N/p - 1$, and $i = 1, \ldots, p$, we have

$$
\sum_{m=0}^{p-1} \gamma^m_i(x^{-k})\gamma^m_i(x^k) = \frac{1}{N^\kappa}, \quad \text{for each } j = 1, 2, \ldots, n.
$$

and

$$
\sum_{m=0}^{p-1} \gamma^m_i(x^k)\gamma^m_i(x^{-k}) = 0, \quad j = 0, 1, \ldots, p - 1, i \neq j.
$$

The theorem is essentially proved the same way as for the complex case, translating the symbols so as to make sense over the finite field.

In order to construct a family of sequences $\{g^j_i|j = 1, 2, \ldots, n\}$ that specifies a cyclic transform as described above, we can again apply frequency decimation to the mother wavelet; i.e. we have

Corollary 5.1. Suppose $p - \text{circ}[g^j_i]$ satisfy (1). For each $j = 2, \ldots, n$, define a length-$p^{n-j}$ sequences $g^j_i$ by

$$
(g^j_i)_{pl+m} = \text{DFT}^{-1}\{\gamma^m_i(x^{p^{n-j}k})|k = 0, 1, \ldots, p^{n-j} - 1\}_{pl+m}
$$

for $l = 0, 1, \ldots, p^{n-j} - 1$, and $m = 0, 1, \ldots, p - 1$ where the sequences $\gamma^m_i$ are as above, and where the operation DFT indicates the number theoretic discrete Fourier transform of appropriate length. Then $G^j = p - \text{circ}[g^j]$ and satisfy (1) for each $j = 2, \ldots, n$. 

Fig. 2. Algorithm for generating family of filters.
In view of the above, we see that a procedure for specifying a finite-field cyclic wavelet transform is to choose a mother wavelet \(g_1\) and the other \(p\)-bands by the algorithm above, and then to choose the lower-order filters from the corollary.

An example would help to clarify the principle.

**Example 5.1.** Consider the field \(\mathcal{F} = GF(5^2)\). As \(3|24\), we can define a transform of length 9 on this field. Consider the field to be generated by indexing polynomial \(x^2 + x + 2\). Then, let \(\varphi\) be a root of the equation which is the generator for the field. (Consult the appendix for a listing of the exponents and indices for this field.) Then, the following vectors define a wavelet transform:

\[
g_1 = (1, \varphi, \varphi^7, 0, 0, 0, 0, 0, 0),
g_2 = (0, 0, 0, 1, \varphi, \varphi^7, 0, 0, 0),
g_3 = (0, 0, 0, 0, 0, 0, 1, \varphi, \varphi^7).
\]

It is readily checked that \(\langle g_i | g_i \rangle = 1 + \varphi^2 + \varphi^{14} = 1\) for \(i = 1, 2, 3\). The orthogonality property is evident from the structure of the vectors.

### 5.1. Wavelet packets

The way we have presented the development of the finite-field wavelet theory, we have split each signal into a detail \((c_j)\) and residual part \((d_j)\). We have then split up the \(c_j\)'s into further subbands. We are not constrained to do this. In fact, at any stage, we may choose to split up either or both of the subbands into further frequency bands. The condition for perfect reconstruction remains the same. All that we need to worry about is to go up in the tree while reconstructing in the same order as we went down it while decomposing. Such a description is referred to as a wavelet packet description. The simple example given below will illustrate the point.

**Example 5.2.** Let us consider a length-8 wavelet transform described by the matrices \(G\) and \(H\). Consider an input data vector \(v\) and the following scheme of decomposition:

\[
c^0 = v,\]

\[
c^1 = G^1v, \quad d^1 = H^1v,
\]

\[
c^2 = G^2d^1, \quad d^2 = H^2d^1,
\]

\[
c^3 = G^3d^2, \quad d^3 = H^3d^2.
\]

Then, a possible MA-MS pair is \(v \leftrightarrow \{c^1, c^2, c^3, d^3\}\) and the corresponding reconstruction steps are

\[
d^2 = N'[\langle G^2 c^3 + (H^3)d^3 \rangle],
\]

\[
d^1 = N'[\langle G^2 c^2 + (H^2)d^2 \rangle],
\]

\[
v = N'[\langle G^1 c^1 + (H^1)d^1 \rangle].
\]

Similarly, any path through the tree shown in Fig. 3 would provide an invertible decomposition.

### 6. Wavelet transform for composite data lengths

We will now build up the structure of the above cyclic transform for composite data lengths. As any positive integer can be factored into prime powers, it is sufficient to define the transform for data lengths \(p^rq\), where \(p\) is a prime number, \(q\) and \(r\) are integers. Note that the particular transform is dependent on how we choose to factorize the data length. To facilitate our discussion, we start with the structure of the transform for data lengths \(2^n\), where \(n, s \geq 1\) are integers.
6.1. Certain definitions

We first present a few definitions and notations. For \( i = 1, 2, \ldots, n \), let \( A_i \) be a square matrix of order \( k_i \). Then, the square block diagonal matrix

\[
A = \begin{pmatrix}
A_1 & 0 & \cdots & 0 \\
0 & A_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & A_n
\end{pmatrix} = \text{diag}(A_1, A_2, \ldots, A_n),
\]

of order \( \sum_{i=1}^{n} k_i \) is called the direct sum of \( A_1, \ldots, A_n \) and is denoted by

\[ A = A_1 \oplus A_2 \oplus \cdots \oplus A_n. \tag{24} \]

Let \( A \) and \( B \) be \( m \times n \) and \( p \times q \), respectively. Then the Kronecker or tensor or direct product of \( A \) and \( B \) is defined to be the \( mp \times nq \) matrix whose entries are

\[
A \otimes B = \begin{pmatrix}
 a_{11}B & a_{12}B & \cdots & a_{1n}B \\
a_{21}B & a_{22}B & \cdots & a_{2n}B \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1}B & a_{m2}B & \cdots & a_{mn}B
\end{pmatrix}.
\]

The Kronecker product has several interesting properties, of which the one that is important to us is

\[
(A \otimes B)(C \otimes D) = (AC) \otimes (BD). \tag{25}
\]

6.2. Wavelet transform for data lengths \( 2^n \)s

From Section 2.2, we know how to define a wavelet transform for data lengths \( 2^n \). Let \( G = 2 - \text{cirl}_{g} \) and \( H = 2 - \text{cirl}_{h} \) be the matrices used to define such a transform. Then, consider the matrices \( G' = G \oplus G \oplus \cdots \oplus G \), i.e. the direct sum of \( s \) copies of the matrix \( G \), and \( H' = H \oplus H \oplus \cdots \oplus H \).

**Theorem 6.1.** The matrices \( G' \) and \( H' \) specify the first level of a wavelet transform for the data length \( 2^n \)s, where \( n \) and \( s \) are positive integers.

**Proof.** To prove the statement, note that

\[
G'^* = G^* \oplus G^* \oplus \cdots \oplus G^*,
\]

\[
H'^* = H^* \oplus H^* \oplus \cdots \oplus H^*.
\]

Then,

\[
G'H'^* = GH^* \oplus GH^* \oplus \cdots \oplus GH^* = 0
\]

and

\[
G'G'^* + H'H'^*
\]

\[
= (GG^* + HH^*) \oplus (GG^* + HH^*) \oplus \cdots \oplus (GG^* + HH^*)
\]

\[
= I_2 \oplus I_2 \oplus \cdots \oplus I_2
\]

\[
= I_2^s.
\]

Further, if \( G \) and \( H \) satisfy the lowpass and bandpass conditions, so do \( G' \) and \( H' \). Thus, they define a wavelet transform.

In the above, we considered \( n \) copies of the same matrix. Note, however, that we could have used \( n \) distinct matrices, provided each satisfied the required conditions for a wavelet transform.

Note further that this result applies to a single level of transform. However, we can use frequency-domain decimation to obtain wavelets of shorter lengths.

To implement this transform, we break up the data into pieces of length \( 2^n \). Each piece can then be passed through a filter followed by decimation by a factor of 2. This was earlier illustrated in Fig. 1 for the case \( p = 3 \).

Before proceeding to describe the wavelets of arbitrary data lengths, note that the matrices mentioned above can also be described in a different way : \( G' = I_2 \otimes G \) and \( H' = I_2 \otimes H \). This observation leads us to a more general formulation.

6.3. Wavelet transform for arbitrary composite data lengths

Consider now the problem of defining the wavelet transform for a data length \( p^r q \), where \( p \) is a prime and \( q, r \) are strictly positive natural numbers. We now modify the definition and let \( G^r = A_q \otimes G \) and \( G^r = B_q \otimes G^* \). Here \( G \) is of dimension \( p^r \times p^r - 1 \) and \( A, B \) are of dimension \( q \times q \). Similarly define \( H^r = A_q \otimes H \) and \( H^r = B_q \otimes H^* \). It should be noted that in this formulation, the matrices \( G \) and \( H \) must be \( p \)-circulants instead of \( 2 \)-circulants.
Theorem 6.2. If \( A_q B_q = I_q \) and \( G \) and \( H \) satisfy the perfect reconstruction property, the matrices \( G^1 \) and \( H^1 \) also satisfy the perfect reconstruction property.

Proof. Observe that

\[
G^1 G^1 = (A_q \otimes G)(B_q \otimes G^*) = A_q B_q \otimes GG^*
\]

and

\[
H^1 H^1 = (A_q \otimes H)(B_q \otimes H^*) = A_q B_q \otimes HH^*.
\]

Now, if we restrict \( A_q B_q = I_q \), then

\[
G^1 G^1 + H^1 H^1 = I_q \otimes (GG^* + HH^*) = I_{p^r}.
\]

Also,

\[
G^1 H^1 = I_q \otimes GH^* = 0.
\]

Hence they satisfy the perfect reconstruction property. \( \square \)

It is also easily seen that, if \( G \) and \( H \) satisfy the bandpass and lowpass condition, then so do \( G^1 \) and \( H^1 \). Thus, they can be used to specify a wavelet transform.

It is clear that the formulation of Section 6.2 is actually a subclass of this formulation for \( A_q = B_q = I_q \). The approach adopted in the previous formulation was to break up the data into smaller pieces for which the transform is well defined. But, that may not always be desirable. In particular, for data with block correlation, one may wish to consider diagonally dominant matrices that weigh the block under consideration the most, and assigns less weight to the other blocks. Permutation matrices are another choice for such matrices.

Note that matrix multiplication can be essentially thought of as a filtering operation, and the scheme outlined above is easily implementable. All that we now need to do is to find an efficient way of calculating the mother wavelets. This problem was addressed in the previous sections of the paper.

Thus, for data length \( N = p^r v \), we divide the data into \( v \) pieces, each of length \( p^r \), and apply the transform to each of these. Note that our previous restriction about the existence of an element of order \( p^r-1 \) can be relaxed here. If the factor \( p^r \) occurs in the prime factorization of the data length \( N \), then we only require the existence of an element of order \( p^\epsilon \), where \( \epsilon \neq 0 \). This is equivalent to the prime factorization of the data length \( N = p^{\epsilon+1} q \), and application of the above procedure. In the trivial case of \( \epsilon = 1 \), we get only one level of transform, and it is the identity transform.

We conclude this section with an example: Consider only two subbands. Let \( g = g_1 \) and \( h = g_2 \).

Example 6.1. Let the field under consideration be \( GF(5) \). Let \( N' = 3( \equiv \frac{3}{2}) \). A routine calculation gives us a length 4 transform as

\[
g_1 = (1,4,0,0),
\]

\[
h_1 = (4,4,0,0),
\]

\[
g_2 = (1,4),
\]

\[
h_2 = (4,4).
\]

Note that 4 \( \equiv -1 \) (mod 5), so the number 4 can be looked upon as \(-1\) over \( GF(5) \). This gives the filters their high pass and low pass characteristics. To get a length-12 transform out of this, consider, for example the matrix

\[
A = \begin{pmatrix} 1 & 1 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\]

and its inverse

\[
B = \begin{pmatrix} 3 & 2 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\]

Then

\[
G^1 = \begin{pmatrix} 1 & 4 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 4 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 0 & 0 \\ 4 & 4 & 0 & 0 & 0 & 4 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 4 & 0 & 0 & 4 & 4 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 4 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 0 \end{pmatrix}
\]

\[
H^1 = \begin{pmatrix} \end{pmatrix}
\]

and

\[
G^1 H^1 = I_{p^r} \otimes (GH^*) = I_{p^r}.
\]
Appendix

Table 1

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,1</td>
<td>0</td>
</tr>
<tr>
<td>1,0</td>
<td>1</td>
</tr>
<tr>
<td>4,3</td>
<td>2</td>
</tr>
<tr>
<td>4,2</td>
<td>3</td>
</tr>
<tr>
<td>3,2</td>
<td>4</td>
</tr>
<tr>
<td>4,4</td>
<td>5</td>
</tr>
<tr>
<td>0,2</td>
<td>6</td>
</tr>
<tr>
<td>2,0</td>
<td>7</td>
</tr>
<tr>
<td>3,1</td>
<td>8</td>
</tr>
<tr>
<td>3,4</td>
<td>9</td>
</tr>
<tr>
<td>1,4</td>
<td>10</td>
</tr>
<tr>
<td>3,3</td>
<td>11</td>
</tr>
<tr>
<td>0,4</td>
<td>12</td>
</tr>
<tr>
<td>4,0</td>
<td>13</td>
</tr>
<tr>
<td>1,2</td>
<td>14</td>
</tr>
<tr>
<td>1,3</td>
<td>15</td>
</tr>
<tr>
<td>2,3</td>
<td>16</td>
</tr>
<tr>
<td>1,1</td>
<td>17</td>
</tr>
<tr>
<td>0,3</td>
<td>18</td>
</tr>
<tr>
<td>3,0</td>
<td>19</td>
</tr>
<tr>
<td>2,4</td>
<td>20</td>
</tr>
<tr>
<td>2,1</td>
<td>21</td>
</tr>
<tr>
<td>4,1</td>
<td>22</td>
</tr>
<tr>
<td>2,2</td>
<td>23</td>
</tr>
</tbody>
</table>

This defines the complete wavelet transform for the sequence. Similar computations can be carried out for the reconstruction of the sequence.

7. Discussion and potential applications

An important advantage of the cyclic wavelet analysis over cyclic Fourier analysis is lower computational complexity. If the rows of the matrices \( G_l \) and each have at most \( M \) non-zero elements, then the the full decomposition requires at most \( p(2M - 1)(N - 1) \sim O(N) \) operations. By comparison, the FFT has \( O(N \log_2(N)) \) complexity. Thus, if wavelet transforms can be used to perform tasks that are normally performed using FFT’s, some practical advantage may be gained. However, like their discrete-time counterparts, these transforms may be fundamentally better suited to some tasks than are Fourier transforms.

Potential applications areas for finite-field wavelet transforms are similar to those for the cyclic Fourier transform, or for the discrete wavelet transform. Alternatively, the multiscale/multilocalization aspects of the cyclic wavelet transform make then useful in searching for structure in long strings of elements from a finite field. An application of this idea is found in biosequence analysis, in which various structural analyses on very long sequences of amino acids (of which there are finitely many) are of interest (see, e.g., [1]). These transforms have also been used in detection of transient signals as in SONAR or seismic signals, or characterize cyclic linear systems. As mentioned before, such transforms have already been used to develop codes capable of multilevel error protection [13].

Here is the listing of the field \( \text{GF}(5^2)/x^2 + x + 2 \).

Table 1 is to be interpreted as follows: If the exponent is \( n \), it refers to the element \( \varphi^n \) in the field. To add any two elements, do modulo 5 addition on each of the coordinates of the exponent, and look up the resultant from Table 1. For example,

\[
1 \ast 1 + \varphi \ast \varphi + \varphi^7 \ast \varphi^7 = 1 + \varphi^2 + \varphi^{14} = (01) + (43) + (12) = (01) = \varphi^0 = 1.
\]

References