TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 357, Number 12, Pages 5031–5050
S 0002-9947(05)03656-1
Article electronically published on March 18, 2005

AN ALGEBRAIC APPROACH TO MULTIRESOLUTION ANALYSIS

RICHARD FOOTE

ABSTRACT. The notion of a weak multiresolution analysis is defined over an arbitrary field in terms of cyclic modules for a certain affine group ring. In this setting the basic properties of weak multiresolution analyses are established, including characterizations of their submodules and quotient modules, the existence and uniqueness of reduced scaling equations, and the existence of wavelet bases. These results yield some standard facts on classical multiresolution analyses over the reals as special cases, but provide a different perspective by not relying on orthogonality or topology. Connections with other areas of algebra and possible further directions are mentioned.

1. INTRODUCTION

The theory of multiresolution analyses and wavelets, which has its roots in papers by Mallat, Grossmann, Morlet, Paul, Daubechies and others in the 1980's, has flourished in recent years, and its uses have been numerous and profound (see [6], [11], [13], [16]). In particular, the theory has become a cornerstone of modern signal processing, with applications permeating areas such as digital image processing, data compression, pattern recognition, data mining, and the like. The multiresolution analysis framework, which is normally viewed in the larger context of Fourier analysis, provides, in particular, methods for extracting local information from data defined over a global spatial or temporal domain. Classical Fourier analysis via exponential Fourier series and transforms on the real line and on intervals is rooted in the representation theory of the unit circle group and its subgroups. Indeed generalizations, new applications, and deeper understandings of Fourier analysis were often achieved from the group-theoretic perspective. For instance, the Discrete Fourier Transform and Fast Fourier Transform are now clearly understood within the context of representations of finite cyclic groups. Generalizations and concomitant applications of these transforms based on other (possibly non-abelian) finite or compact groups or over other fields are emerging in greater number in the literature (see, in particular, [1], [2], [5], [15], [17], [18], [19], [20], [23] and the references therein; see also the introduction to [9] for a survey).

Likewise, it is known that a multiresolution analysis in $L^2(\mathbb{R})$ results from an action of a subgroup of the affine group on this space. The purpose of this paper is to pursue this representation-theoretic perspective by axiomatizing its essential

Received by the editors March 7, 2003 and, in revised form, January 14, 2004 and March 5, 2004.

2000 *Mathematics Subject Classification.* Primary 20C99; Secondary 42C40.

Key words and phrases. Multiresolution analysis, wavelets.

This work was partially supported by an AFOSR/NM grant.

algebraic features. This approach, which in some respects is simpler and more general than the original theory, applies over an arbitrary field and does not require an orthogonal form or a topology on the underlying representation space (so, in particular, it may be utilized in L^p-spaces other than L^2). From this vantage we give new proofs of some of the basic classical properties of multiresolution analyses and wavelets. For example, we see precisely how certain scaling functions lead to a wavelet basis over any field. We also mention possible connections to other areas of algebra and number theory, and suggest some avenues for further investigation to stimulate both theoretical and applications oriented research.

More specifically, the paper is organized as follows. In Section 2 we review the definition of a multiresolution analysis and extract some of its features to define a *weak multiresolution analysis (WMA)* over any field. In Section 3 we cast some aspects of WMAs into a ring-theoretic framework; this initiates some algebraic-geometric methods that are used subsequently, and also suggests connections between multiresolution analyses and other areas. Section 4 begins the main results of the paper: a classification of weak multiresolution analyses over arbitrary fields, and a determination of their submodules and quotient modules. In Section 5 we prove that every infinite-dimensional WMA has a "wavelet basis," and possesses a unique "reduced scaling equation" that characterizes it up to module isomorphism. In Section 6 we suggest some lines for possible further investigation.

This paper is intentionally self-contained and elementary, making it accessible to a general audience. Other papers that mention or pursue some representation-theoretic aspects of multiresolution analysis include [3], [6], [8], [9], [11], [12], [13], [21], [22], [26], [27], but these complement rather than overlap substantially with this paper. The work of Chirikjian and his collaborators, [5], [15], uses the tools of harmonic analysis on the affine group and motion groups in various pattern recognition problems.

2. Weak multiresolution analyses: Definitions and preliminary results

Following standard references such as [6], [14], [25], a *multiresolution analysis* is a vector subspace V of $L^2(\mathbb{R})$ together with subspaces V_i of V for each $i \in \mathbb{Z}$ satisfying the following axioms:

- MR1. For each $f \in V$, $f(x) \in V_i$ if and only if $f(2x) \in V_{i-1}$.
- MR2. The subspaces V_i are nested: $\cdots V_2 \subseteq V_1 \subseteq V_0 \subseteq V_{-1} \subseteq V_{-2} \cdots$.
- MR3. $\bigcup_{i\in\mathbb{Z}} V_i = V$ and V is dense in $L^2(\mathbb{R})$.
- MR4. $\bigcap_{i\in\mathbb{Z}} V_i = 0$.
- MR5. If $f(x) \in V_0$, then $f(x-k) \in V_0$ for all $k \in \mathbb{Z}$.
- MR6. There is a function $\phi(x)$ such that $\{\phi(x-k) \mid k \in \mathbb{Z}\}$ is an orthonormal basis of V_0.

Axioms 1 and 2 specify a "multiresolution" decomposition of V "scaled" by factors of two, where $f(2x)$ is thought of as a "finer" version of $f(x)$. Axioms 3 and 4 are standard in approximation theory. From the so-called *scaling function* ϕ, and assuming the subspaces V_i are closed in $L^2(\mathbb{R})$, these axioms easily lead to a *mother wavelet*, ψ, whose scaled and translated versions, $\{\psi(2^i x - j) \mid i, j \in \mathbb{Z}\}$, span a dense subset of $L^2(\mathbb{R})$, hence give "wavelet series" for square-integrable functions (see Section 5). The term "basis" in axiom 6 refers to a Hilbert space basis; however we shall restrict our attention to the class of multiresolution analyses where every element of V_0 is a (finite) linear combination of the translates of ϕ. This class includes all multiresolution analyses where the scaling function and corresponding wavelets have compact support.

We extract some essential features of such a multiresolution analysis by first observing that if Y is any nonempty set, there is a left group action by the real affine group on the set of all functions $f : \mathbb{R} \to Y$ by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} f(x) = f\left(\frac{x-b}{a}\right) \qquad \text{for } \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}).$$

In the case of real-valued functions, this action is $\mathbb{R}$-linear and restricts to an action on various subspaces such as $L^2(\mathbb{R})$ or the space of continuous functions. We single out some relevant subgroups and elements of this affine group:

$$G = \left\{ \begin{pmatrix} 2^a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z},\ b \in \mathbb{Z}[1/2] \right\},$$

(2.1)

$$\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B_j = \left\{ \begin{pmatrix} 1 & 2^j b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\}.$$

Under the action of G on $L^2(\mathbb{R})$ we easily see that some of the essential features that define a multiresolution analysis V with scaling function ϕ can now be couched in an algebraic framework:

MRa. V is a cyclic $\mathbb{R}G$-module with generator ϕ.

MRb. The "zero scale" subspace V_0 is the cyclic $\mathbb{R}B_0$-submodule of V generated by ϕ.

MRc. $V_i = \sigma^i V_0$ and $V_i \subseteq \sigma^{-1} V_i$ for all $i \in \mathbb{Z}$.

The fundamental perspective of this paper is to transport these properties to an arbitrary field, and to unravel consequences of this abstraction, recovering many of the properties of multiresolution analyses over $\mathbb{R}$ in the process. We note that the above properties distinguish B_0 from its conjugate subgroups B_i, so we also wish to work with a formulation which avoids this asymmetry.

Definition. Let F be any field and let G be the group in (2.1) above. For $j \in \mathbb{Z}$, a nonzero FG-module V is called a weak multiresolution analysis of level j over F with respect to v_0 if V is generated as a cyclic FG-module by v_0, and if we let $V_{j,0} = FB_j v_0$, then $\sigma^i V_{j,0} \subseteq \sigma^{i-1} V_{j,0}$ for all $i \in \mathbb{Z}$. We say V is a weak multiresolution analysis (or WMA) over F with respect to v_0 if it is a weak multiresolution analysis with respect to v_0 of level j for some $j \in \mathbb{Z}$.

We say V is a WMA if it is a WMA with respect to some generator v_0, and we call v_0 a *scaling function* for V. Thus a "classical" multiresolution analysis discussed above is a weak multiresolution analysis over $\mathbb{R}$ of level zero. We shall see examples where V is a WMA with respect to some generator v_0 but not with respect to some other cyclic generator, so explicit specification of a distinguished generator is often required.

For the remainder of this section F is an arbitrary field, G is the group in (2.1), and V is a cyclic FG-module with generator v_0. Fix some $j \in \mathbb{Z}$ and let $V_{j,0} = FB_j v_0$ and $V_{j,i} = \sigma^i V_{j,0}$. We introduce some additional notation used throughout the paper:

$$\tau_j = \begin{pmatrix} 1 & 2^j \\ 0 & 1 \end{pmatrix}, \qquad B = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}[1/2] \right\}.$$

Observe that the following relations hold:

(i) $\tau_j^2 = \tau_{j+1}$ and $\sigma\tau_j\sigma^{-1} = \tau_{j+1}$, so $\sigma\tau_j = \tau_j^2\sigma$.
(ii) $\tau = \tau_0$ and $B_0 = \langle \tau \rangle$.
(iii) $\tau_j = \sigma^j\tau\sigma^{-j}$ and $B_j = \sigma^j B_0 \sigma^{-j} \cong \mathbb{Z}$ for all $j \in \mathbb{Z}$.
(iv) $\sigma^i B_j \sigma^{-i} = B_{j+i}$.
(v) $\cdots B_2 \subset B_1 \subset B_0 \subset B_{-1} \subset B_{-2} \subset \cdots$ and $\bigcup_{i=0}^{\infty} B_{-i} = B$.
(vi) $B \cong \mathbb{Z}[1/2]$ and B is a 2-divisible, locally cyclic group (i.e., every finitely generated subgroup is cyclic).
(vii) $G = \langle \tau, \sigma \rangle$, B is a characteristic subgroup of G, and G is the split extension of $\langle \sigma \rangle$ by B; all complements to B in G are conjugate to $\langle \sigma \rangle$ (i.e., $H^1(\langle \sigma \rangle, B) = 0$).
(viii) $B = G'$, and N is a nontrivial normal subgroup of G if and only if $B \subseteq N$.
(ix) Each $V_{j,i}$ is an FB_{j+i}-module, and hence is an FB_k-module for any $k \geq j+i$ as well.
(x) Let $w_0 \in V$, let $w_{-1} = \sigma^{-1}w_0$, and let $g(X)$ be any F-linear combination of integer powers of the variable X. Then $\sigma^{-1}g(\tau_j)w = g(\tau_{j-1})w_{-1}$.

In the special case where V is a classical multiresolution analysis over $\mathbb{R}$, the last observation is a restatement of the fact that $f(2x - b) = f(2(x - b/2))$.

Proposition 2.1. *In the notation of this section the following are equivalent:*

(1) *V is a WMA of level j with respect to the generator v_0.*
(2) *$V_{j,0} \subseteq V_{j,-1}$.*
(3) *$V_{j,i} \subseteq V_{j,i-1}$ for some $i \in \mathbb{Z}$.*
(4) *For some $\beta \in FB_j$ we have $v_0 = \sigma^{-1}\beta v_0$.*
(5) *There is an isomorphism $\Phi : FG/L \to V$ of left FG-modules with $\Phi(1) = v_0$ such that L is a left ideal of FG containing an element $\sigma - g(\tau_j)$, where $g(\tau_j) = \tau_j^{-n}f(\tau_j)$ for some polynomial f with coefficients from F and non-negative integer n.*

Proof. Since σ is a unit in FG, repeated applications of integer powers of σ to $V_{j,0}$ gives the equivalence of (1), (2) and (3). Since $V_{j,0}$ is a cyclic FB_j-module with generator v_0 and $V_{j,-1}$ is an FB_j-module and is the image of $V_{j,0}$ under σ^{-1}, we have $V_{j,0} \subseteq V_{j,-1}$ if and only if $v_0 \in V_{j,-1}$. This gives the equivalence of (3) and (4). Since V is a cyclic FG-module there is an FG-module homomorphism $\Phi : FG \to V$ with $\Phi(1) = v_0$ such that $\ker \Phi$ is the left ideal that annihilates the element v_0. By (4), V is a WMA of level j if and only if $v_0 = \sigma^{-1}\tau_j^{-n}f(\tau_j)v_0$, where the group ring element β is written as a polynomial in τ_j with the negative powers factored out. Thus V is a WMA of level j if and only if $1 - \sigma^{-1}\tau_j^{-n}f(\tau_j) \in L$. Multiplying this group ring element on the left by the unit σ now gives the equivalence of (5) with (4). $\square$

In the classical theory of multiresolution analyses over $\mathbb{R}$ (of level zero) the relation in (4) or (5) is called the *scaling* or *dilation* equation, and is usually written as

$$\phi(x) = \sqrt{2} \sum_{k=-N}^{M} h_k \phi(2x-k), \qquad h_k \in \mathbb{R}. \tag{2.2}$$

In a multiresolution of level j we would allow the translates k in (2.2) to lie in the group $2^j\mathbb{Z}$. We shall see that if V is an infinite-dimensional WMA over any field, then the corresponding scaling equation uniquely determines V (up to FG-module isomorphism).

Corollary 2.2. *If V is a WMA of level j with respect to v_0, then V is a WMA of level k with respect to v_0 for all $k \le j$. Furthermore, any cyclic FG-module V generated by v_0 is a WMA with scaling function v_0 if and only if $v_0 = \sigma^{-1}\beta v_0$ for some $\beta \in FB$.*

Proof. These assertions are immediate from Proposition 2.1(4) since $B_j \subseteq B_k$ for all $k \le j$, and B is the union of the B_j. □

Corollary 2.3. *Let V be a WMA. Then V is either a cyclic FB-module or it is not finitely generated over FB.*

Remark. The examples below show that both possibilities occur.

Proof. Assume V is finitely generated over FB by $v_1, \dots, v_n$. Pick $N \in \mathbb{Z}$ so that $v_i \in V_N$ for all i, and let $v_N = \sigma^N v_0$. Then $v_1, \dots, v_n \in FB_N v_N \subseteq FBv_N$, so v_N generates V as a cyclic FB-module. □

Corollary 2.4. *Let V be a WMA of level j with respect to v_0. For any FG-module W and FG-module homomorphism $\Phi : V \to W$, the image, $\Phi(V)$, is a WMA of level j with respect to $\Phi(v_0)$.*

Proof. This is immediate from the equivalence of (1) and (4) in Proposition 2.1. □

Remarks. 1. **Translation:** If v_0 is a scaling function at level j, write its scaling equation as $v_0 = \sigma^{-1}\tau_j^{-n} f(\tau_j)v_0$ for some integer n and some $f(X) \in F[X]$ with $f(0) \neq 0$. Replacing v_0 by $u_0 = \tau_j^n v_0$ results in a scaling equation $u_0 = \sigma^{-1} f(\tau_j)u_0$. Clearly u_0 is an FG-module generator for V as well. Thus, in particular, we lose no generality in assuming that the scaling equation for some scaling function v_0 has no "denominators" (negative powers of τ_j). For v_0 and f as above we call f the *scaling polynomial* and call the degree of this "normalized" polynomial f the *degree of the scaling function* v_0.

2. **Rescaling:** Let V be a WMA of level j with scaling function $v_{j,0}$ and scaling equation $v_{j,0} = \sigma^{-1} f(\tau_j)v_{j,0}$ for some $f(X) \in F[X]$. Then V is also a WMA of level zero with scaling function $v_0 = \sigma^{-j} v_{j,0} = v_{j,-j}$ and scaling equation (of level zero) $v_0 = \sigma^{-1} f(\tau)v_0$. Thus by replacing the scaling function we may rescale from level j to level zero (or vice versa) without changing the scaling polynomial $f(X)$.

Note that naïvely viewing a given scaling function at a higher level *does* change its scaling equation (as well as the scaling subspaces). For example, v_0 at level zero with scaling equation $v_0 = \sigma^{-1} f(\tau)v_0$ has scaling equation $v_0 = \sigma^{-1} f(\tau_{-1}^2)v_0$ if we let v_0 generate V as a level -1 WMA (i.e., the scaling polynomial is now $f(X^2)$). However, we may "rescale" from level j to level zero while keeping the same scaling function and scaling polynomial as follows. Define a new FG-module structure on V by calling $V^{(-j)} = V$, and making $V^{(-j)}$ into an FG-module by

$$\gamma \cdot v = \sigma^j \gamma \sigma^{-j}(v), \qquad \text{for all } \gamma \in FG.$$

This makes $V^{(-j)}$ into a WMA of level zero with scaling function $v_{j,0}$ and scaling equation $\sigma \cdot v_{j,0} = f(\tau) \cdot v_{j,0}$. Moreover, the map $V \to V^{(-j)}$ given by $v \mapsto \sigma^j v = \sigma^j \cdot v$ is an isomorphism of FG-modules. These observations show that we lose no generality in assuming all WMAs are of level zero.

Examples. 1. **Principal WMAs over F:** Let L be the principal left ideal of FG generated by $\sigma - c$ for some nonzero $c \in F$. We call $V(c) = FG/L$ a *principal WMA over F* with scaling function $v_0 = 1 + L$. Let $V = V(c)$, so that V is the regular representation for FB (a free rank 1 FB-module) and is induced from the 1-dimensional representation of $\langle \sigma \rangle$ with eigenvalue c. Explicitly, there is a basis $\{v_i\}$ of V indexed by the elements of $\mathbb{Z}[1/2]$ such that V is a WMA of level zero with respect to v_0, where $\tau(v_j) = v_{j+1}$ and $\sigma(v_j) = cv_{2j}$, for all $j \in \mathbb{Z}[1/2]$. With respect to this basis, $V_{0,i}$ is the span of the vectors $v_{2^i n}$ for $n \in \mathbb{Z}$, and the scaling equation is $v_0 = \sigma^{-1} c v_0$.

Note that $u_0 = v_{\frac{1}{2}}$ is clearly another generator of V as a cyclic FG-module. Let $U_0 = FB_0 u_0 = \mathrm{Span}\{v_{n+\frac{1}{2}} \mid n \in \mathbb{Z}\}$. Thus $\sigma u_0 = v_1 \notin U_0$, so V is not a WMA of level zero with respect to u_0, although V is a WMA of level -1 with respect to u_0.

Note that when F has characteristic $\neq 2$, then $w = v_0 + v_1$ *is a generator for V* as an FG-module, but *is not a scaling function* at any level: $\sigma w = v_0 + v_2 \notin FBw$. In particular, $FGw \neq FBw$.

If $c_1 \neq c_2$, then $V(c_1)$ and $V(c_2)$ are nonisomorphic FG-modules since each has a unique 1-dimensional eigenspace for σ with eigenvalues c_1 and c_2, respectively. Observe also, for example, that $\sigma - \tau$ and $\sigma - 1$ generate isomorphic WMAs by preceding remarks.

We return to this example in Corollary 4.2 and in Section 5.

2. **The Haar WMA over F:** If L is the principal left ideal of FG generated by $\sigma - (\tau + 1)$, then $V = FG/L$ is called the Haar weak multiresolution analysis. If $v_0 = 1 + L$ is the scaling function and $v_{-1} = \sigma^{-1} v_0$, then the scaling equation for V is $v_0 = v_{-1} + \tau_{-1} v_{-1}$. This module is usually defined over $\mathbb{R}$ but is now seen to have an analog over any field. We shall return to this example in Section 5.

It is an exercise to see that if $F = \mathbb{R}$ and V is the classical multiresolution analysis with $v_0 = \chi_{[0,1)}$ the characteristic function of the unit interval (with $V \subseteq L^2(\mathbb{R})$), then V is not finitely generated over $\mathbb{R}B$.

3. Structure of the group ring FG

Proposition 2.1(5) suggests that one method for studying WMAs is to determine the quotients of the group ring FG by certain left ideals. We take this approach by first viewing this group ring as a twisted polynomial ring with coefficients from a Bezout domain.[1] One advantage of this formalism is that it suggests analogies with other important fields of study such as Drinfeld modules (additive polynomials) and differential algebra (see [10]). This sort of observation begins to place the study of MRA within a commutative algebra and algebraic geometry context.

[1] A Bezout domain is an integral domain in which every finitely generated ideal is principal.

Since $B_0 \cong \mathbb{Z}$, the group ring FG is isomorphic to the ring $F[T, T^{-1}]$ of polynomials in the variable T and its inverse, where $\tau^i \mapsto T^i$ for $i \in \mathbb{Z}$. This ring is the localization of the polynomial ring $F[T]$ at the set of nonnegative powers of T, hence by elementary means or standard results on localization is a principal ideal domain ([7, Section 15.4]). In particular, every nonzero ideal is generated by a unique, monic polynomial $p(T) \in F[T]$ with $p(0) \neq 0$; and $F[T, T^{-1}]/(p(T)) \cong F[T]/(p(T))$ is vector space over F of dimension $\deg p$. Each group ring FB_j is likewise isomorphic to the P.I.D. $R_j = F[T^{2^j}, T^{-2^j}]$ for $j \in \mathbb{Z}$, where $\tau_j = \sigma^j \tau \sigma^{-j} \mapsto T^{2^j}$. The nesting $B_j \subseteq B_{j-1}$ is reflected in the relation $R_j \subseteq R_{j-1}$, and

$$R = \bigcup_{j=0}^{-\infty} F[T^{2^j}, T^{-2^j}] \cong FB.$$

Since R is an increasing union of P.I.D.s, it is a Bezout domain. Finally, since FG is a free left module over its subring FB with basis the integer powers of σ, we may define a "twisted polynomial ring" over R in the variables S and S^{-1} as follows. Let $R\{S, S^{-1}\}$ be the ring whose elements are uniquely expressed as formal sums:

$$R\{S, S^{-1}\} = \left\{ \sum_{i=-N}^{M} r_i(T) S^i \mid r_i(T) \in R,\ M, N \in \mathbb{Z}^{\geq 0} \right\},$$

with addition by adding coefficients of like powers of S, and multiplication given by the relation $\sigma\tau = \tau^2\sigma$:

$$\left(\sum_{i=-N}^{M} a_i(T) S^i \right) \left(\sum_{j=-P}^{Q} b_j(T) S^j \right) = \sum_{k=-N-P}^{M+Q} \sum_{i+j=k} a_i(T) b_j(T^{2^i}) S^k,$$

where $b_j(T^{2^i})$ indicates replacing each power T^{2^t} in the expression for $b_j(T) \in R$ by $T^{2^{t+i}}$, for all $i, t \in \mathbb{Z}$. These operations in $R\{S, S^{-1}\}$ give a well-defined ring structure since they are simply a transport of the ring structure of FG to this "polynomial" setting. Note that the units in R are the union of the units in the R_j for $j \in \mathbb{Z}$, hence are of the form aT^b for some $a \in F - \{0\}$ and $b \in \mathbb{Z}[1/2]$.

Under this isomorphism between FG and $R\{S, S^{-1}\}$ each cyclic FG-module with generator v_0 is isomorphic to $R\{S, S^{-1}\}/\mathcal{L}$, where $\mathcal{L}$ is a left ideal of $R\{S, S^{-1}\}$ and $v_0 \mapsto 1 + \mathcal{L}$. By Proposition 2.1(5), V is a WMA of level j when $\mathcal{L}$ contains $S - g$, for some $g \in R_j$. In the latter case, $V_{j,i} \cong R_{j+i}/(R_{j+i} \cap \mathcal{L})$.

Note that there is some latitude in the specification of a ring isomorphism from FG to $R\{S, S^{-1}\}$: it is possible to map (σ, τ) to $(T^{-b}S, T)$ or map (σ, τ) to (S, T^{2^i}), for any $b \in \mathbb{Z}[1/2]$ or $i \in \mathbb{Z}$, since these mappings correspond to following the originally specified isomorphism by conjugation in $R\{S, S^{-1}\}$ by the units T^b and S^i, respectively. For conjugations of the first type, if the ideal $\mathcal{L}$ contains $S - g$ for $g \in R_j$, then the conjugate ideal $T^b \mathcal{L} T^{-b}$ also contains $T^{-b}S - g$ and hence contains $S - T^b g$; and if $T^b \in R_j$, then this conjugation preserves the level j of the WMA. Conjugation by S^i maps $S - g$ to $S - S^i g S^{-i}$; so if $g \in R_j$, then $S^i g S^{-i} \in R_{j+i}$. Thus conjugation by S^i maps WMAs of level j to ones of level $j + i$. These conjugations are simply translating and rescaling, as remarked upon previously.

The next result is a special case of a "left division algorithm" in $R\{S, S^{-1}\}$.

Proposition 3.1. *Let $F = S - g \in R\{S, S^{-1}\}$ for some $g \in R$. Then for any $H \in R\{S\}$ there is some $Q \in R\{S\}$ such that*

$$H = QF + r, \qquad \text{for some } r \in R.$$

Proof. Since $S - g$ is monic in the variable S, the proof of this result is the same as that of the usual Division Algorithm [7, Theorem 3, Section 9.2]. □

Proposition 3.2. *If $\mathcal{L}$ is a left ideal of $R\{S, S^{-1}\}$ that contains $F = S - g$, for some $g \in R$, then either $\mathcal{L}$ is the principal left ideal $R\{S, S^{-1}\}F$ or $\mathcal{L} \cap R \neq 0$.*

Proof. If $\mathcal{L}$ is not the principal left ideal generated by $S - g$, then there is some $H \in \mathcal{L}$ that is not a left multiple of F. Multiplying H on the left by a power of S, we may assume $H \in R\{S\}$. By the preceding result, $H = QF + r$ for some $r \in R$. Thus $r = H - QF$ is a nonzero element of $\mathcal{L} \cap R$, as needed to complete the proof. □

4. Characterizations of WMAs, submodules, and quotient modules

Continuing the notation from the previous section, V is a cyclic FG-module with generator v_0. We initially focus on when V is infinite-dimensional. By Proposition 7.1 in Section 7, such results apply to a classical multiresolution analysis over $\mathbb{R}$.

Theorem 4.1. *Let V be a WMA over F with scaling function v_0 and, as in Proposition 2.1(5), let L be the left ideal of FG annihilating v_0. The following are equivalent:*

1. *V is infinite dimensional over F.*
2. *L is the principal left ideal generated by $\sigma - \beta$, for some nonzero $\beta \in FB$.*
3. *$L \cap FB = 0$.*
4. *There is a unique $\beta \in FB_0$ such that $\sigma v_0 = \beta v_0$ (i.e., the scaling equation for v_0 is unique).*

In particular, an infinite-dimensional WMA over any field is determined by its scaling equation.

Proof. (3) ⇒ (2): This is Proposition 3.2 interpreted in FG by our identification with $R\{S, S^{-1}\}$.

(2) ⇒ (3): Again working in $R\{S, S^{-1}\}$, assume $\mathcal{L}$ is the principal left ideal generated by $S - g$, for some nonzero $g \in R$. If $p(S)(S - g) \in \mathcal{L} \cap R$ for some $p(S) \in R\{S, S^{-1}\}$, then by examining the highest power S in the product—which is obtained by multiplying the nonzero term in p having the highest power of S, times S—we see that all powers of S in $p(S)$ must be negative. Likewise, the lowest power of S in the product is the lowest nonzero term in p times g, and so p can have no nonzero negative terms, i.e., $p = 0$ as desired.

(3) ⇒ (1): If (3) holds, then the infinite-dimensional space FB maps injectively into $FG/L \cong V$. This gives (1).

(1) ⇒ (3): Let V be a WMA of level j, and let $V_i = V_{j,i-j}$ for all i. Working again with $V \cong R\{S, S^{-1}\}/\mathcal{L}$, assume $R \cap \mathcal{L} \neq 0$. Then for some $i \in \mathbb{Z}$, $\mathcal{L} \cap R_i$ is a nonzero ideal in R_i, hence has finite codimension in R_i by a previous observation. Thus $V_i \cong R_i/(\mathcal{L} \cap R_i)$ is finite dimensional over F. Since σ^{-1} is an isomorphism from V_i onto V_{i-1} and $V_i \subseteq V_{i-1}$ we obtain $V_i = V_{i-1}$. By applying powers of σ we then get that $V_i = V_k$ for all i, k, and hence $V = V_i$ is finite dimensional. Thus if (1) holds, we must have $R \cap \mathcal{L} = 0$, which is (3).

(3) $\Leftrightarrow$ (4): The scaling function v_0 satisfies scaling equations $\sigma v_0 = \beta_i v_0$ for $i = 1, 2$ if and only if $\beta_1 - \beta_2 \in FB \cap L$. This gives the equivalence of (3) and (4).

The final remark is a recapitulation of the result that when the dimension of V is infinite, its isomorphism type is uniquely determined by its scaling equation by (2) and Proposition 2.1(5). □

Corollary 4.2. *If V is an infinite-dimensional WMA that is finitely generated over FB, then V is isomorphic to a principal WMA.*

Proof. Assume V is an infinite-dimensional WMA that is finitely generated over FB, hence $V = FBv_0$ for some $v_0 \in V$ by Corollary 2.3. Then $\sigma^{-1}v_0 = \beta v_0$ for some $\beta \in FB$. By the same reasoning as the Remarks on translating and rescaling in Section 2, we may assume v_0 is chosen with $\sigma^{-1}v_0 = f(\tau)v_0$ for some $f(X) \in F[X]$ with $f(0) \neq 0$. Thus $v_0 = f(\tau^2)\sigma v_0$. By Theorem 4.1(3), FB_0v_0 is free of rank 1. Since $f(\tau^2)v_0$ is a generator for this module, $f(\tau^2)$ must be a unit in $FB_0 \cong F[X, X^{-1}]$. It follows that $f(X) = c$ for some $c \in F^\times$. Thus V has a scaling function v_0 with scaling equation $v_0 = \sigma^{-1}c^{-1}v_0$, and so V is isomorphic to a principal WMA by Theorem 4.1, as claimed. □

Theorem 4.3. *Let V be an infinite-dimensional WMA of level zero with respect to v_0 with $v_0 = \sigma^{-1}f(\tau)v_0$ for some $f(X) \in F[X]$. Let W be any proper, nonzero FG-submodule of V. Then there are polynomials $p(X), q(X) \in F[X]$ such that the following hold:*

1. *$p(X)$ is monic with nonzero constant term, $p(X^2) = q(X)p(X)$, and the roots of $p(X)$ are $(2^m - 1)^{st}$ roots of unity, for some $m \in \mathbb{Z}^+$.*
2. *$p(X)$ and $f(X)$ are relatively prime.*
3. *The submodule W is a WMA of level zero with scaling function $w_0 = p(\tau)v_0$ and scaling equation $w_0 = \sigma^{-1}q(\tau)f(\tau)w_0$.*
4. *The quotient module $\overline{V} = V/W$ is a WMA of level zero and finite dimension with $\overline{V} = \overline{V_{0,i}}$ for all $i \in \mathbb{Z}$.*
5. *The minimal polynomial of τ^{2^i} acting on $\overline{V}$ is $p(x)$, for all $i \in \mathbb{Z}$.*

Proof. Let $V_i = V_{0,i}$ for all i. Let W be any nonzero, proper FG-submodule of V, and let overbars denote the natural projection of V onto V/W. By Corollary 2.4, $\overline{V}$ is a WMA of level zero with respect to $\overline{v_0}$. Let L be the annihilator in FG of the scaling function v_0, and let L_1 be the left ideal of FG which is the preimage of W under the presentation homomorphism Φ in Proposition 2.1(5). Let $\mathcal{L}$ and $\mathcal{L}_1$ be the ideals in $R\{S, S^{-1}\}$ corresponding to L, L_1, respectively.

Since $\mathcal{L} \subset \mathcal{L}_1$, by Proposition 3.2, $\mathcal{L}_1 \cap R \neq 0$. As in the proof of Theorem 4.1, there is a positive integer n, independent of i, such that $R_i \cap \mathcal{L}_1$ has codimension n in R_i for all i. Moreover,

$$\overline{V_i} \cong R_i/(R_i \cap \mathcal{L}_1) \text{ has dimension } n \text{ over } F, \text{ for all } i \in \mathbb{Z}.$$

Again as in Theorem 4.1, since σ^{-1} maps $\overline{V_i}$ onto the subspace $\overline{V_{i-1}}$ containing it,

$$\overline{V} = \overline{V_i} \text{ has dimension } n \text{ over } F.$$

Since R_i is a principal ideal domain, there is a unique, monic polynomial p_i in the variable T^{2^i} with $p_i(0) \neq 0$ such that $\overline{V_i} \cong F[T^{2^i}]/(p_i)$; moreover, (p_i) is the minimal polynomial of τ_i acting on $\overline{V_i} = \overline{V}$, and the degree of p_i in its variable T^{2^i} is n. Since τ_i is conjugate to τ_{i+1} in G, their minimal polynomials are the same: $p_i(X) = p_{i+1}(X)$ for all i, where X is an independent variable.

Let $p(X) = p_i(X)$. Since τ is conjugate to τ^{2^i}, $p(X)$ divides $p(X^{2^i})$ in $F[X]$, for all $i \in \mathbb{Z}^+$. It follows easily that for some m dividing $n!$, each root, λ, of p (in an algebraic closure of F) satisfies $\lambda^{2^m} = \lambda$. Thus the roots of p are $(2^m - 1)^{\text{st}}$ roots of unity.

We next show that $p(X)$ and $f(X)$ are relatively prime. If $d(X)$ is their g.c.d., then $\sigma\overline{v_0} = f(\tau)\overline{v_0} \subseteq d(\tau)\overline{V}$. Note that $d(\tau)\overline{V}$ is a subspace of $\overline{V}$ stable under τ and annihilated by a polynomial in τ which is a divisor of p. Since p is also the smallest degree polynomial in τ that annihilates $\sigma\overline{v_0}$, we must have $d(\tau)\overline{V} = \overline{V}$ and so $d = 1$ as claimed.

Finally, we show that W is a WMA. Let $w_0 = p(\tau)v_0$, so that $\overline{w_0} = \overline{0}$, i.e., $w_0 \in W$. Let $W' = FGw_0$. By the preceding discussion W' has finite codimension n' in V, where n' equals the codimension of $W' \cap V_0$ in V_0. By construction, however, the codimension of FB_0w_0 in V_0 equals $\deg p$. Thus $n' \leq \deg p = \operatorname{codim} W$. Since W' is a submodule of W, we must have $W' = W$, i.e., w_0 is a cyclic generator for W. To find the scaling equation for w_0 let $p(X^2) = q(X)p(X)$ in $F[X]$. Then

$$\sigma w_0 = \sigma p(\tau)v_0 = p(\tau^2)\sigma v_0 = p(\tau^2)f(\tau)v_0 = q(\tau)p(\tau)f(\tau)v_0 = q(\tau)f(\tau)w_0.$$

This establishes (3), and completes all parts of the proof. □

To complete the picture we now give some characterizations of finite-dimensional WMAs.

Theorem 4.4. *Let V be a finite-dimensional WMA of level zero over a field F with $\operatorname{char} F \neq 2$. Let $p(X) \in F[X]$ be the minimal polynomial of τ acting on V, and assume also that F contains all roots of p. Then the following hold:*

1. *$V = V_{0,i}$ for all $i \in \mathbb{Z}$.*
2. *$p(X) = p_1(X) \cdots p_r(X)$, where for each $i \in \{1, \ldots, r\}$ there is a root λ_i of $p_i(X)$ such that $\lambda_i, \lambda_i^2, \ldots, \lambda_i^{2^{m_i-1}}$ are all the distinct roots of $p_i(X)$, and $\lambda_i^{2^{m_i}} = \lambda_i$.*
3. *$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ is a decomposition of V into FG-submodules, where V_i is annihilated by $p_i(\tau)$.*
4. *Let $\dim V_i = e_i m_i$ and let J_i be the $e_i \times e_i$ elementary (lower triangular) Jordan block with eigenvalue λ_i. Then there is a basis of V_i such that τ and σ acting on V_i with respect to this basis have matrices*

$$(4.1)\quad [\tau] = \begin{pmatrix} J_i & & & 0 \\ & J_i^2 & & \\ & & \ddots & \\ 0 & & & J_i^{2^{m_i-1}} \end{pmatrix} \quad \textit{and} \quad [\sigma^{-1}] = \begin{pmatrix} 0 & 0 & \ldots & 0 & A \\ I & 0 & \ldots & \ldots & 0 \\ 0 & I & 0 & \ldots & \vdots \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & \ldots & I & 0 \end{pmatrix},$$

where I is the $e_i \times e_i$ identity matrix, and A is an $e_i \times e_i$ matrix that is uniquely (and explicitly) determined by the scaling equation for V and the polynomial p.

Proof. As usual, we may assume the scaling equation for V is $v_0 = \sigma^{-1}f(\tau)v_0$ for some $f(X) \in F[X]$. Since V is a homomorphic image of the WMA FG/L, where L is the principal left ideal generated by $\sigma - f(\tau)$, we may apply Theorem 4.3 to obtain parts (1) and (2), where p_i is the product of all factors whose roots lie in an orbit of the group of 2-power maps acting on the roots of p.

Next note that if λ is any root of p, then $\lambda^{2^m-1} = 1$ for some m. Thus since F has odd characteristic, $-\lambda$ is not a root of p, i.e., $\lambda^{2^{m-1}}$ is the unique square root of λ that is a root of p. Thus for any positive integer k we have $(\tau^2 - \lambda^2)^k v = 0$ if and only if $(\tau - \lambda)^k v = 0$. To obtain (3) note that if $(\tau - \lambda)^k v = 0$ for some $v \in V$, then

$$0 = (\tau - \lambda)^k v = (\tau^2 - \lambda^2)^k v = (\sigma(\tau - \lambda^2)^k \sigma^{-1})v = (\tau - \lambda^2)^k(\sigma^{-1}v).$$

Thus if V_λ is the $(X - \lambda)$-primary component of τ acting on V, then $\sigma^{-1}V_\lambda = V_{\lambda^2}$. In particular, $\langle \sigma \rangle$ permutes the primary components associated to roots that are 2-powers of each other, and so (3) follows.

To establish (4) we may simplify notation by assuming $V = V_1$ and the distinct roots of p are $\lambda, \lambda^2, \ldots, \lambda^{2^{m-1}}$. Also let $V = U_0 \oplus \cdots \oplus U_{m-1}$, where $U_i = V_{\lambda^{2^i}}$, and $\sigma^{-1}U_i = U_{i+1}$ with the indices read mod n. Note that

$$p(X) = \prod_{i=0}^{m-1} (X - \lambda^{2^i})^e \qquad \text{where } e = \dim U_i \text{ for all } i.$$

Let $\mathcal{B}$ be an ordered basis of U_0 for which the matrix, J, of τ is the $e \times e$ lower triangular Jordan block with eigenvalue λ. For each $i = 1, 2, \ldots, m-1$ let $\mathcal{B}_i = \sigma^{-i}\mathcal{B}$ (with the corresponding basis ordering). It follows that $\mathcal{B}_i$ is a basis of U_i and the matrix of τ on U_i with respect to $\mathcal{B}_i$ is J^{2^i}. Let A be the $e \times e$ matrix representing the action of σ^{2^m} on U_0 with respect to $\mathcal{B}$. All parts of the theorem now follow once we have established the uniqueness of the matrix A in (4.1).

By construction, $\mathcal{B} = \{v_0, v_1, \ldots, v_{e-1}\}$, where $(\tau - \lambda)v_i = v_{i+1}$, i.e., τ has matrix $J = J_\lambda$. Let A be the matrix of σ^{-2^m} with respect to this basis (which is the same A as above). Since $AJ^{2^m}A^{-1} = J$, the matrix A is a change of basis that converts J^{2^m} into its Jordan form on U. We calculate one specific such change of basis matrix, P, as follows. A basis for which τ^{2^m} is in Jordan form is $u_0, u_1, \ldots, u_{e-1}$, where $u_i = (\tau^{2^m} - \lambda)^i v_0$, for $i = 0, 1, \ldots, e-1$. To compute the change of basis matrix explicitly let $N = 2^m$ and let

$$\Phi(X) = \frac{X^N - \lambda^N}{X - \lambda} = \sum_{j=0}^{N-1} \lambda^j X^{N-j-1}.$$

Then

$$\begin{aligned} u_i = (\tau^N - \lambda)^i v_0 &= (\tau^N - \lambda^N)^i v_0 \\ &= \Phi(\tau)^i (\tau - \lambda)^i v_0 = \Phi(\tau)^i v_i. \end{aligned} \tag{4.2}$$

Thus, writing $\Phi(\tau)^i v_i$ in terms of the basis $\mathcal{B}$ gives the i^{th} column of the matrix P^{-1}.

Finally, to establish the uniqueness in part (4), if A is the matrix that represents σ^{-2^m} with respect to $\mathcal{B}$, then $A^{-1}JA = J^{2^m} = P^{-1}JP$. Thus $PA^{-1} = C$ commutes with J. Now by repeated iterations of the scaling equation we obtain

$$\sigma^{2^m} v_0 = f_1(\tau) v_0 \qquad \text{for some } f_1(X) \in F[X],$$

where f_1 is uniquely determined by f and the power 2^m (which is determined by p). Since the scaling function v_0 for V projects onto a cyclic generator of U_0—which was arbitrary and also denoted by v_0—we have

$$Cv_0 = PA^{-1}v_0 = P\sigma^{2^m}v_0 = Pf_1(\tau)v_0. \tag{4.3}$$

Thus C is uniquely determined on v_0 by the explicit matrix P, the scaling polynomial f and the power 2^m. Since C commutes with $(\tau-\lambda)^i$ for all i, the matrix of C with respect to the fixed basis $\mathcal{B}$ is uniquely determined on U_0, hence so is A, as needed. $\square$

Observe that by choosing A as the explicitly computed matrix P above, the matrices in (4.1) determine a representation of G on the vector space V. However, this representation need not satisfy a given scaling equation (hence the introduction of the matrix C in (4.3) to highlight the latitude in choices for A). It is also easily seen that C is necessarily a polynomial in J of degree at most $e-1$.

From (4.2) we may compute the i,i diagonal entry of the matrix P to be $\Phi(\lambda)^{i-1} = 2^{m(i-1)}$. In particular, if these powers of 2 are distinct in F, then σ^{2^m} is similar to a diagonal matrix over F (with respect to a different basis, not necessarily preserving the "Jordan form" of τ).

A special case of Theorem 4.4 is worth recording:

Corollary 4.5. *In the notation of Theorem* 4.4*, if $p(X) = (X-1)^e$, then a representation for G is obtained by mapping τ to the $e\times e$ Jordan block J with eigenvalue* 1*, and mapping σ to $P^{-1} = (a_{i,j})$, where*

$$a_{i,j} = \begin{cases} 0, & \text{if } i<j,\\ 2^{2j-i-1}\binom{j-1}{i-j}, & \text{if } i \geq j. \end{cases}$$

Up to equivalence, all representations are then obtained by replacing P by PC, where C is invertible and a polynomial in J of degree at most $e-1$.

Proof. In this case $r=1$, $m_1=1$ and $(a_{i,j})$ is the matrix P^{-1} computed from (4.2) with $\Phi(X) = X+\lambda$. The coefficients are thus obtained directly from the binomial expansion. $\square$

5. Wavelets

In this section V is an infinite-dimensional WMA with scaling function v_0. By the Remarks following Corollary 2.4 we may assume V is of level zero and the scaling equation is $v_0 = \sigma^{-1}f(\tau)v_0$, for some polynomial $f(X)\in F[X]$. For each integer i let $V_i = V_{0,i}$. It follows from Theorem 4.1(3) that $V_{-1} = \sigma^{-1}V_0$ is a free FB_{-1}-module of rank 1, and a free FB_0-module of rank 2 (since B_0 is of index 2 in B_{-1}). Moreover, if we let

$$v_{-1} = \sigma^{-1}v_0 \qquad \text{and} \qquad v_{-1}^* = \tau_{-1}v_{-1},$$

then $\{v_{-1}\}$ is an FB_{-1}-basis and $\{v_{-1}, v_{-1}^*\}$ is an FB_0-basis for V_{-1}.

Definition. Let V be an infinite-dimensional WMA of level zero with respect to the scaling function v_0. Say V has a wavelet basis with respect to v_0 if the FB_0-submodule FB_0v_0 is a direct summand (or pure submodule) of V_{-1} considered as an FB_0-module. If V has such a wavelet basis, then a mother wavelet is any element in V_{-1} that generates an FB_0-module direct sum complement to FB_0v_0 in V_{-1}.

The importance of a wavelet basis is in obtaining successively "finer" resolutions, as follows. If V_0 is a direct summand of V_{-1} considered as an FB_0-module, then for all $i\geq 0$, V_{-i} is likewise an FB_{-i}-module direct summand of V_{-i-1}, and so

$V_{-i-1} = V_{-i} \oplus W_{-i}$, for some cyclic FB_{-i}-module W_{-i}. Thus we obtain for all positive i a decomposition

$$V_{-i} = V_{-i+1} \oplus W_{-i+1} = V_0 \oplus W_0 \oplus W_{-1} \oplus W_{-2} \oplus \cdots \oplus W_{-i+1}, \tag{5.1}$$

where the W_{-j} are free FB_0-modules with bases given by sets of scaled and translated versions of the "mother wavelet" generating W_0 (cf. the Introduction). The V_{-i+1} component of a vector in V_{-i} may be thought of as an approximation to a vector (or function), and the "error" in this approximation is its component in W_{-i+1}. Successively refining this process as in (5.1) is integral to the efficacy of a multiresolution analysis. Note that this process cannot be carried through V_i for $i > 0$ for want of an FB_0-module structure (although the arbitrary choice of "level zero" in the resolution can be tailored to the degree of detail or resolution needed in a given application).

A classical multiresolution analysis over $\mathbb{R}$ (assuming the V_i are closed subspaces) always has a wavelet basis since the submodule FB_0v_0 has an orthogonal complement in V_{-1} that is also an FB_0-submodule. Since orthogonality is not generally available for WMAs over F, not every WMA need have a wavelet basis with respect to a given generator. We shall see, however, that every WMA has a wavelet basis with respect to *some* generator.

Theorem 5.1. *Let V be an infinite WMA of level zero with scaling function v_0 whose scaling equation is a polynomial in τ. Write the scaling equation as*

$$v_0 = \sigma^{-1}(\tau^{2n_1}\tau f_1(\tau^2) + \tau^{2n_2} f_2(\tau^2))v_0, \qquad f_1(T), f_2(T) \in F[T],\ n_1, n_2 \in \mathbb{Z}^{\geq 0},$$

where each of $f_1(T)$ and $f_2(T)$ is either zero or has nonzero constant term. Then V has a wavelet basis with respect to v_0 if and only if one of the following holds:

(1) *Exactly one of f_1 or f_2 is zero and the other is a nonzero constant.*
(2) *Both f_1 and f_2 are nonzero and they are relatively prime in $F[T]$.*

Proof. By collecting the odd and even power monomial terms of τ, and factoring out integer powers of τ, the scaling equation may always be written in the form described; and f_1, f_2 cannot both be zero. We may then rewrite the scaling equation as

$$v_0 = (\tau^{n_1}\tau_{-1} f_1(\tau) + \tau^{n_2} f_2(\tau))\sigma^{-1}v_0 = \tau^{n_1} f_1(\tau)v_{-1}^* + \tau^{n_2} f_2(\tau)v_{-1}.$$

By observations preceding this theorem, this is the unique expression of v_0 with respect to the FB_0-basis elements v_{-1}^* and v_{-1}. Since V_{-1} is a module over the Principal Ideal Domain $FB_0 \cong F[T, T^{-1}]$, by [7, Theorem 12.4] a nonzero element w generates a direct summand if and only if w is not of the form gv for any nonunit $g \in FB_0$ and any $v \in V_{-1}$. Equivalently, w generates a direct summand if and only if its coefficients, when expressed in terms of a basis, have no common nonunit divisor. Since the powers of T are units in $F[T, T^{-1}]$, after removing these as we did to normalize the basis coefficients, the theorem now follows immediately from the fact that the g.c.d. of two polynomials in $F[T]$ is the same (up to units) as their g.c.d. in $F[T, T^{-1}]$. □

Corollary 5.2. *Let V be a WMA with respect to v_0 with scaling equation $v_0 = \sigma^{-1}f(\tau)v_0$ for $f(X) \in F[X]$. Then V has a wavelet basis with respect to v_0 if and only if we cannot write $f(X) = g(X^2)h(X)$ for some $g(X), h(X) \in F[X]$ with g not a constant times a power of X.*

Proof. This is immediate from Theorem 5.1. □

Corollary 5.3. *In the notation of Theorem* 5.1*, V has a wavelet basis with respect to v_0 if and only if*

$$1 = a(T)f_1(T) + b(T)f_2(T), \qquad \textit{for some } a(T), b(T) \in F[T].$$

In this case the element $b(\tau)v_{-1}^* - a(\tau)v_{-1}$ is a mother wavelet.

Proof. The first assertion is the familiar property of g.c.d.s in a P.I.D. When this condition holds, let $w_1 = v_0$ and $w_2 = b(\tau)v_{-1}^* - a(\tau)v_{-1}$. Then the transition matrix from the basis $\{v_{-1}^*, v_{-1}\}$ to the set $\{w_1, w_2\}$ is seen to have determinant a unit in $F[T, T^{-1}]$. This implies the latter set is a basis, as needed. $\square$

The condition that f_1 and f_2 be relatively prime is easily (and rapidly) checked by the Euclidean Algorithm, or by computing the resultant of f_1 and f_2; see [7] for both methods.

Corollary 5.4. *Assume V has a wavelet basis with respect to v_0 and, in the notation of Corollary* 5.3*, let $w_2 = b(\tau)v_{-1}^* - a(\tau)v_{-1}$. Then w is a mother wavelet for V if and only if $w = \beta_1 v_0 + c\tau^k w_2$, for some $\beta_1 \in FB_0$, $k \in \mathbb{Z}$, and $c \in F - \{0\}$.*

Proof. This is a restatement of the observation that if $\{v_0, w_2\}$ is a basis of a free module, then $\{v_0, w\}$ is also a basis if and only if the 2×2 transition matrix is invertible, i.e., has unit determinant. The determinant for the specified transition equals the coefficient of w_2 when writing w in terms of $\{v_0, w_2\}$. Since the units in $F[T, T^{-1}]$ are nonzero constants times integer powers of T, the result follows. $\square$

Definition. Let V be an infinite-dimensional WMA of level j with respect to the scaling function v_0 whose scaling equation is $v_0 = \sigma^{-1}f(\tau_j)v_0$ for some $f(X) \in F[X, X^{-1}]$. We say the scaling function or scaling equation is reduced if $f(X) \in F[X]$, $f(0) \neq 0$, and we cannot write $f(X) = g(X^2)h(X)$ for some $g(X), h(X) \in F[X]$ with g not a constant times a power of X.

We also say the scaling polynomial $f(X)$ is reduced if the corresponding equation is reduced. By the Remarks following Corollary 2.4, every scaling function may be replaced by a translated scaling function whose scaling equation is a polynomial with nonzero constant term. Furthermore, V may be rescaled so the scaling function is of level zero, with the same scaling polynomial (so we lose no generality in assuming the scaling function is of level zero). By Corollary 5.2, reduced scaling functions are those for which V has a wavelet basis.

Theorem 5.5. *Let V be an infinite-dimensional WMA.*

(1) *Then V has a reduced scaling function of level zero, hence has wavelet basis with respect to that scaling function. More specifically, over all scaling functions of level zero, if v_0 is one of minimal degree, then v_0 is reduced.*
(2) *Any two reduced scaling functions in V have the same scaling equation.*

Proof. (1): Choose a scaling function v_0 of level zero so that its scaling equation is $v_0 = \sigma^{-1}f(\tau)v_0$ with $f(X) \in F[X]$ of minimal degree. If v_0 is not reduced, we may write

$$f(X) = g(X^2)h(X), \qquad \text{for some } g, h \in F[X] \text{ with } g(X) \neq cX^n.$$

Let $w_0 = h(\tau_{-1})v_{-1}$. Since $v_0 = g(\tau)h(\tau_{-1})\sigma^{-1}v_0 = g(\tau)w_0 \in FGw_0$ we have that w_0 is a cyclic generator for V. Now

$$\sigma w_0 = \sigma h(\tau_{-1})v_{-1} = h(\tau)\sigma v_{-1} = h(\tau)v_0 = h(\tau)g(\tau)w_0$$

so w_0 is a scaling function of level zero and of smaller degree than v_0, a contradiction. This establishes (1).

(2): As in the Remarks following Corollary 2.4, by replacing the given scaling functions by suitable σ-powers times them (which does not alter their scaling equations) we may assume v_0 and u_0 are reduced scaling functions of level zero. Now there is some smallest nonnegative integer k such that $v_0 \in U_{-k}$, where, as usual, $U_i = FB_iu_i$, where $u_i = \sigma^i u_0$. Since U_{-k} is an FB_0-module, $V_0 \subseteq U_{-k}$. Likewise there is some $m \geq k$ such that $u_{-k} \in V_{-m}$, and hence $U_{-k} \subseteq V_{-m}$. Considering all modules over FB_0, since v_0 is a reduced scaling function, by (5.1) V_0 is a direct summand of V_{-m}, hence is a direct summand of the submodule U_{-k} of V_{-m} containing it. Likewise U_0 is a direct summand of U_{-k}. Since V_{-m} is a free module over the P.I.D. FB_0, either $U_0 = V_0$ or $U_0 \cap V_0 = 0$.

If $U_0 = V_0$, then $u_0 = \alpha v_0$ for some unit $\alpha \in FB_0$. In this case $\alpha = c\tau^i$ for some $c \in F^\times$ and $i \in \mathbb{Z}$. Since the scaling equations for u_0 and v_0 are both reduced, it follows that $i = 0$ and the equations are the same.

Consider when $U_0 \cap V_0 = 0$. In this case, since u_0 is a scaling function, $\sigma^m u_0 \in U_0$. But $\sigma^m u_0 \in \sigma^m V_{-m} = V_0$, and so $\sigma^m u_0 \in U_0 \cap V_0 = 0$, a contradiction. This completes the proof. □

Remarks. The method of proof of Theorem 5.5 shows how to obtain a scaling function which possesses a wavelet basis from any given scaling function: iterate the process of "removing" factors of the form $g(X^2)$ from the scaling equation (which clearly terminates by degree considerations). Also, each infinite-dimensional WMA V has a unique reduced scaling equation (or polynomial) associated to it, namely that of any reduced scaling function in V. We call this *the reduced scaling equation for* V. In particular, we now immediately obtain the following uniqueness result.

Corollary 5.6. *Two infinite-dimensional WMAs are isomorphic as FG-modules if and only if they have the same reduced scaling equations.*

Finally, if w is a mother wavelet, we may write

$$w = g_1(\tau)\tau v_{-1} + g_2(\tau)v_{-1}, \qquad g_1(\tau), g_2(\tau) \in FB_0.$$

This is called a *wavelet equation*. In the absence of orthogonality, a mother wavelet is not uniquely determined, hence the wavelet coefficients g_i are not unique either. We also note that a mother wavelet, w, by the proof of Theorem 5.5(2), is not a scaling function of level zero. The following examples show that a mother wavelet may be a scaling function of level -1, or it may be a generator for V as an FG-module but not a scaling function of any level, or indeed it need not even generate V as an FG-module (although by Theorem 4.3 it generates a WMA of finite codimension in V).

Examples. Following the notation and results of the Examples after Corollary 2.4:

1. **Principal WMAs over *F***: Evidently $V_{-1} = FB_0v_0 \oplus FB_0v_{\frac{1}{2}}$. Thus $v_{\frac{1}{2}}$ is a mother wavelet. Note that $v_{\frac{1}{2}}$ is also a scaling function for V of level -1. On the other hand, if the characteristic of $F \neq 2$, then, as mentioned before, the mother wavelet $w = v_0 + v_{\frac{1}{2}}$ is a generator for V as an FG-module, but is not a scaling function at any level. Finally, the mother wavelet $w' = v_0 - v_{\frac{1}{2}}$ is not a generator for V as an FG-module, since it lies in the image in V of the augmentation ideal of FB (of codimension 1 in V).

2. **The Haar WMA over F**: Assume $\operatorname{char} F \neq 2$. In this example, since v_{-1}, v_{-1}^* is an FB_0-module basis for V_{-1}, by Corollary 5.3 $w = v_{-1} - v_{-1}^*$ is a mother wavelet, called the *Haar wavelet* over F. This vector does not generate V as an FG-module because it lies in the image of the augmentation ideal of FB which lies in a proper FG-submodule (in the classical language, it and all its scaled translates have zero mean).

Note that, for example, v_{-1}^* is also a mother wavelet for the Haar WMA and it is a scaling function of level -1.

3. **Battle–Lemarié WMAs**: These wavelets in $L^2(\mathbb{R})$, described in detail in [6, Section 5.4], are constructed for each $N \geq 0$ from a function ϕ which is a B-spline of degree N with knots at the integers. The Haar wavelets are the degree zero Battle–Lemarié wavelets. For $N \geq 1$ the translates of ϕ are not orthogonal, so ϕ must be modified by an "orthogonalization trick" to produce a multiresolution analysis in $L^2(\mathbb{R})$; the scaling function that results from this process does not have compact support. Since the translates of ϕ are linearly independent, however, we may use ϕ itself to generate a *weak* multiresolution analysis and (algebraic) wavelet basis.

We illustrate the results of this section in the $N = 2$ case. The quadratic B-spline ϕ has support $[-1, 2]$ and is defined on this interval by

$$\phi(x) = \begin{cases} \frac{1}{2}(x+1)^2, & -1 \leq x \leq 0, \\ \frac{3}{4} - (x - \frac{1}{2})^2, & 0 \leq x \leq 1, \\ \frac{1}{2}(x-2)^2, & 1 \leq x \leq 2. \end{cases}$$

The scaling equation for ϕ is

$$\phi(x) = \tfrac{1}{4}\phi(2x+1) + \tfrac{3}{4}\phi(2x) + \tfrac{3}{4}\phi(2x-1) + \tfrac{1}{4}\phi(2x-2).$$

With G acting in the usual fashion on $L^2(\mathbb{R})$ (see Section 1), translate ϕ as in the Remarks in Section 2 by setting $v_0 = \phi(x-1)$ so that the scaling equation becomes a polynomial in τ—in the notation of Theorem 5.1 it is

$$v_0 = \sigma^{-1}(\tau(\tfrac{3}{4}\tau^0 + \tfrac{1}{4}\tau^2) + (\tfrac{1}{4}\tau^0 + \tfrac{3}{4}\tau^2))v_0.$$

Hence $f_1(T) = \frac{3}{4} + \frac{1}{4}T$ and $f_2(T) = \frac{1}{4} + \frac{3}{4}T$. These polynomials are clearly relatively prime, and $\frac{3}{2}f_1 - \frac{1}{2}f_2 = 1$. By Corollary 5.3, a mother wavelet is $-\frac{1}{2}\sigma^{-1}\tau v_0 - \frac{3}{2}\sigma^{-1}v_0$. Since $v_{-1} = \sigma^{-1}v_0$ and $v_{-1}^* = \sigma^{-1}\tau v_0$, this mother wavelet is seen to be

$$\psi(x) = -\tfrac{1}{2}\phi(2x-1) - \tfrac{3}{2}\phi(2x-2).$$

Note that $\int_{-\infty}^{\infty} \psi(x)\, dx = -1$. By Corollary 5.4, the function $\psi_1(x) = \psi(x) + \phi(x-1)$ is another mother wavelet; it enjoys the additional property that $\psi_1(x + \frac{3}{2})$ is an odd function; so, in particular, the mother wavelet ψ_1 satisfies an "admissibility" condition: $\int_{-\infty}^{\infty} \psi_1(x)\, dx = 0$. Note that the scaling equation may be read in any field of characteristic not equal to 2, thereby giving analogs of the quadratic B-spline wavelets in different settings.

6. Further directions

One of the main purposes of this paper is to place the theory of multiresolution analyses in a larger algebraic setting, with the intent of stimulating additional theoretical and practical developments. We suggest some possible lines of further research.

1. Generalizing to other groups. There is an obvious definition of WMAs for arbitrary integral scaling factors $N \geq 2$, obtained by replacing "2" by "N," and evidently the results herein carry over mutatis mutandis to such groups. An N-scale MRA theory for $L^2(\mathbb{R})$—which falls under the general rubric of "multiwavelets"—has been mentioned by others, and is developed systematically in $L^2(\mathbb{R})$ in [4]. In the general algebraic setting, N-scale WMAs lead to the notion of an (algebraic) wavelet basis, although the direct sum complements to V_0 in V_{-1} are free of rank $N-1$, so there is not a single "mother wavelet" when $N > 2$ (which is the case in $L^2(\mathbb{R})$ as well). Examples, such as the N-scale analogs of the Haar wavelets, require the underlying field to contain N distinct N^{th} roots of unity in order to formulate mother wavelets analogous to the DFT basis functions (which are eigenfunctions for an action of a cyclic group of order N).

Generalized multiresolution analyses for other groups are explored in papers cited in the Introduction. In particular, Section VI of [9] discusses generalized multiresolution analyses for finite and profinite groups. Combining ideas from these papers with ones in this work may lead to new productive notions of WMAs for other groups, with concomitant harmonic analyses. In particular, other higher-dimensional affine groups may lead to new perspectives on multi-dimensional multiresolution analyses—an area of considerable interest in signal processing.

2. *p*-adic weak multiresolution analyses. Some recent work on wavelets over local fields appears in [1] and [2]. In the context of WMAs it seems natural to pass to a completion and consider FG^*-modules, where

$$G^* = G^*(\nu) = \left\{ \begin{pmatrix} \pi^n & b \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z},\ b \in K_\nu \right\},$$

and where K_ν is a field with a discrete valuation ν and uniformizing parameter π. Here π would essentially play the role of 2 (or p) in the theory, and for a cyclic FG^*-module V^* generated by v_0^* let $V_0^* = FB_0^* v_0^*$, where B_0^* is the unipotent subgroup of G^* with entries from the ring of integers in K_ν. To define a WMA in this context we might require $v_0^* \in \sigma^{-1} V_0^*$, where $\sigma = \operatorname{diag}(\pi, 1)$. In order to place the theory within the mainstream of representation theory of p-adic groups ([24]) it may be necessary to impose further restrictions on the representation (e.g., smoothness, admissibility, etc.), and so V^* may need to be a projective limit of finite-dimensional modules (cf. Section 4).

Specifically for a 2-adic theory, it would be instructive to seek ties to trees and wreath product multiresolution analyses, as described in [9]. More generally, the affine buildings for linear groups over K_ν may be brought to bear for further insight.

A coherent p-adic theory of WMAs may then lead naturally to an adelic formulation by taking suitable restricted direct products of p-adic WMAs over all primes. In both p-adic and adelic theories it may be instructive to revisit the classical theory of dense submodules of $L^2(\mathbb{R})$ in order to glean "Fourier analytic" insights whenever possible.

3. Other types of multiresolution analyses. In the notation of Section 3, it might be productive to consider FG-modules $R\{S, S^{-1}\}/\mathcal{L}$ for principal left ideals $\mathcal{L}$ other than those generated by a monic linear "polynomial" in S. In particular, which such modules appear as dense submodules of $L^2(\mathbb{R})$, and what subsequent analytic theories do they yield? One might also consider $Q\{S, S^{-1}\}$-modules, where Q is the field of fractions of R. Alternatively, as in the p-adic case, the ring R, which is a union of polynomial rings, might be replaced by a corresponding union of (formal) power series rings in order to mimic the classical MRA theory wherein the scaling equation may express a scaling function $\phi(x)$ as an infinite series of translates of $\phi(2x)$ rather than a finite sum, as we have imposed. In the same vein, as noted in Section 3, the ring $R\{S, S^{-1}\}$ is linked by analogy to the theory of Drinfeld modules and to differential algebra—these connections might be investigated more thoroughly for potential cross-fertilization.

4. Applications. It was not the intent of this paper to provide new applications of multiresolution analyses, but rather to lay some mathematical foundations for possible future uses of WMAs in settings where, for instance, orthogonal forms are not available. It might be desirable, for example, to pursue WMAs over finite fields and their application to codes, monochrome image processing, etc. One measure of the success of this approach will therefore lie in advances that accrue from the algebraic perspective espoused herein.

7. Appendix: WMAs over $\mathbb{R}$

We include a proof that every nonzero $\mathbb{R}B_0$-module contained in $L^2(\mathbb{R})$ is infinite dimensional. Thus the results for infinite-dimensional WMAs in Sections 4 and 5 apply to every WMA in $L^2(\mathbb{R})$. Although this fact may be proved by topological/analytic means, it may be nicely deduced from the basic theory of modules over P.I.D.s.

Proposition 7.1. *If V is a nonzero subspace of $L^2(\mathbb{R})$ such that $f(x-b) \in V$ for every $f \in V$ and $b \in \mathbb{Z}$, then V is infinite dimensional.*

Proof. Assume by way of contradiction that V is finite dimensional, so we may assume that V is an irreducible $\mathbb{R}B_0$-module. By previous remarks on the structure of $\mathbb{R}B_0$, V is isomorphic to $\mathbb{R}[T]/(p(T))$, for some monic irreducible polynomial $p(T)$. In particular, V is either one or two dimensional.

If $p(T) = T - \alpha$ for some $\alpha \in \mathbb{R}$ and f is a generator for V, then $f(x-1) = \alpha f(x)$ for all $x \in \mathbb{R}$. In this case

$$\int_0^1 f(x-n)^2\,dx = \int_{-n}^{1-n} f(u)^2\,du = \alpha^{2n}\int_0^1 f(x)^2\,dx.$$

Since $f \in L^2(\mathbb{R})$, $\lim\limits_{n\to\pm\infty} \int_{-n}^{1-n} f(u)^2\,du = 0$. But $\alpha \neq 0$ since τ is invertible and so $\int_0^1 f(x)^2\,dx = 0$. Translating this over all intervals $[k, k+1]$ for $k \in \mathbb{Z}$ shows that $||\, f\,||_2^2 = 0$, a contradiction.

Consider now when $p(T) = (T-\alpha)(T-\overline{\alpha})$ is an irreducible quadratic, for some complex number α. Writing $\alpha = re^{i\theta}$ there is a basis $\{f_1, f_2\}$ of V such that with respect to this basis τ has matrix

$$[\tau] = r\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.$$

It follows from De Moivre's formulas that

$$\begin{aligned} f_1(x-n)^2+f_2(x-n)^2 &= (\tau^n f_1(x))^2 + (\tau^n f_2(x))^2\\ &= r^{2n}(\cos^2 n\theta + \sin^2 n\theta) f_1(x)^2 + r^{2n}(\sin^2 n\theta + \cos^2 n\theta) f_2(x)^2\\ &= r^{2n}(f_1(x)^2 + f_2(x)^2). \end{aligned}$$

As before, integrating over unit intervals and taking the limit as $n \to \pm\infty$ shows $\| f_1 \|_2^2 + \| f_2 \|_2^2 = 0$, a contradiction. This completes the proof. $\square$

Acknowledgment

The author thanks Gagan Mirchandani and Dan Rockmore for their invaluable assistance with this work. He also thanks the AFOSR for its grant support. Thanks also to the referee for numerous suggestions and references that have significantly improved the paper.

References

[1] J. Benedetto and R. Benedetto, *A wavelet theory for local fields and related groups*, submitted for publication.

[2] R. Benedetto, *Examples of wavelets over local fields*, Contemporary Mathematics (2003).

[3] R. Bernanardini and J. Kovačević, *Local orthogonal bases I and II*, Multidim. Syst. Signal Process. **7** (1996), 331-370 and 371–400.

[4] O. Bratteli and P. Jorgensen, *Isometries, Shifts, Cuntz Algebras and Multiresolution Wavelets of Scale N*, Integral Equations Operator Th. **28** (1997), 382–443. MR1465320 (99k:46094b)

[5] G. Chirikjian and A. Kyatkin, *Engineering Applications of Noncommutative Harmonic Analysis*, CRC Press, 2000. MR1885369 (2003g:42001)

[6] I. Daubechies, *Ten Lectures on Wavelets*, CBMS-NSF Regional Conf. Series in Applied Math., SIAM, 1992. MR1162107 (93e:42045)

[7] D. Dummit and R. Foote, *Abstract Algebra, Third Edition*, John Wiley & Sons, Inc, NJ, 2004.

[8] K. Flornes, A. Grossman, M. Holschneider and B. Torrésani, *Wavelets on discrete fields*, Appl. Comput. Harmon. Anal. **2** (1994), 137–146. MR1310638 (95h:42031)

[9] R. Foote, G. Mirchandani, D. Rockmore, D. Healy and T. Olson, *A wreath product group approach to signal and image processing: part I—multiresolution analysis*, IEEE Trans. on Signal Processing **48** (2000), 102–132. MR1736279 (2001c:94007)

[10] D. Goss, *Basic Structures of Function Field Arithmetic*, vol. 35, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, NY, 1996. MR1423131 (97i:11062)

[11] A. Grossmann, *Wave functions on subgroups of affine canonical transformations*, Resonances —Models and Phenomena, vol. 211, Lecture Notes in Phys., 1984, pp. 128–138. MR0777335 (86f:81042)

[12] A. Grossmann and J. Morlet, *Decomposition of Hardy functions into square integrable wavelets of constant shape*, SIAM J. Math. Anal. **15** (1984), 723–736. MR0747432 (85i:81146)

[13] A. Grossmann, J. Morlet and T. Paul, *Transforms associated to square integrable group representations, I and II*, J. Math. Phys., and Ann. Inst. H. Poincaré Phys. Théor., **26, 45** (1985, 1986), 2473–2479 and 293–309 resp. MR0803788 (86k:22013); MR0868528 (88d:22011)

[14] M. Kirby, *Geometric Data Analysis*, John Wiley & Sons, Inc, NJ, 2001. MR1874451 (2003h:94002)

[15] A. Kyatkin and G. Chirikjian, *Algorithms for fast convolutions on motion groups*, Appl. Comp. Harm. Anal. **9** (2000), 220–241. MR1777127 (2001g:65177)

[16] S. Mallat, *Multiresolution approximations and wavelet orthonormal bases of l^2*, Trans. Amer. Math. Soc. **315** (1989), 69–87. MR1008470 (90e:42046)

[17] D. Maslen, *Sampling of functions and sections for compact groups*, Modern Signal Processing, D. Rockmore and D. Healy, eds., Cambridge University Press, Cambridge, to appear.

[18] D. Maslen, *Efficient computation of Fourier transforms on compact groups*, J. Fourier Anal. Appl. **1** (1998), 19–52. MR1650948 (99k:43002)

[19] D. Maslen and D. Rockmore, *The Cooley–Tukey FFT and group theory*, Notices Amer. Math. Soc. **10** (2001), 1151–1160. MR1861656 (2002k:20022)

[20] D. Maslen and D. Rockmore, *Generalized FFTs—a survey of some recent results*, Groups and Computation, II (New Brunswick, NJ, 1995), Amer. Math. Soc., Providence, RI, 1997, pp. 183–237. MR1444138 (98k:20020)

[21] G. Mirchandani, R. Foote, D. Rockmore, D. Healy and T. Olson, *A wreath product group approach to signal and image processing: part II—convolution, correlation, and applications*, IEEE Trans. on Signal Processing **48** (2000), 749–767. MR1765933 (2001f:94003)

[22] M. Özaydin and T. Przebinda, *Platonic orthonormal wavelets*, Appl. Comput. Harmon. Anal. **4** (1997), 351–365. MR1474094 (99c:42071)

[23] D. Rockmore, *Some applications of generalized FFTs*, Proceedings of the DIMACS Workshop on Groups and Computation, June 7–10, 1995, L. Finkelstein and W. Kantor, eds., 1997, pp. 329–369. MR1444144 (98e:65116)

[24] A. Silberger, *Introduction to Harmonic Analysis on Reductive p-adic Groups*, vol. 23, Mathematical Notes, Princeton University Press, Princeton, NJ, 1979. MR0544991 (81m:22025)

[25] G. Strang and T. Nguyen, *Wavelets and Filter Banks*, Addison-Wesley, NY, 1996. MR1411910 (98b:94003)

[26] B. Yazici, *Group invariant methods in signal processing*, Proc. Conf. on Information Science and Systems, Johns Hopkins Univ., MD, 1997.

[27] B. Yazici, *Stocastic deconvolution over groups*, IEEE Trans. in Info. Th., to appear.

Department of Mathematics and Statistics, University of Vermont, Burlington, Vermont 05405

E-mail address: `foote@math.uvm.edu`