The Journal of Fourier Analysis and Applications
Volume 3, Number 4, 1997

On the Pseudodilation Representations of Flornes, Grossmann, Holschneider, and Torresani

Carolyn P. Johnston

1. Introduction

A version of the continuous wavelet transform for sequences of length p was recently developed by Flornes, Grossmann, Holschneider, and Torrésani [1]. Their approach was to apply the classical theory of square-integrable representations to the natural action of the affine ("ax+b") group G_p defined over the finite field $\mathbf{Z}_p$ on finite sequences of length p. Here p is an arbitrary prime.

One major difference between a dilated function defined on the reals, $D_a f(x) = \frac{1}{a} f(\frac{x}{a})$ ($a \in \mathbf{R}^*$), and the analogous dilated function on $\mathbf{Z}_p$, $D_a f(k) = f(a^{-1}k)$ ($a \in \mathbf{Z}_p^*$), is that the support of $f \in l^2(\mathbf{Z}_p)$ is not changed in measure by the application of D_a, as it is in the real case. This makes it difficult to interpret the dilated functions $D_a f(x)$ as sampled versions of dilated functions in $L^2(\mathbf{R})$; as the authors of [1] observed, the wavelet transforms appear to be "full of holes". As a possible remedy for this problem, they introduced the notion of a pseudodilation representation. They gave an example which showed that a pseudodilation representation can indeed give a smoother wavelet transform, which appears much more like a sampled version of a continuous wavelet transform. They pointed out that a complete understanding of all the pseudodilation representations on $l^2(\mathbf{Z}_p)$ would involve the solution of a group cohomology problem.

The present paper completes the classification of pseudodilation operators begun by Flornes, Grossmann, Holschneider, and Torrésani, framing these results in the more general context of all finite fields. Let F denote a finite field of order p^k, where p is a prime and k is an arbitrary positive integer; the discussion in [1] is easily extended from the setting of sequences defined over $\mathbf{Z}_p$ to that of sequences defined over F. We demonstrate a class of filters which satisfies the cocycle conditions that were shown in [1] to be necessary and sufficient for a filter to be a "compatible filter", and show that a class of compatible filters giving rise to unitary pseudodilation representations can be parametrized by the $p^k - 1$ torus T^{p^k-1}. The proof that this completely parametrizes the set of compatible filters is given by the solution of the cohomological problem mentioned in [1]; the details of this derivation are given in an appendix.

In the next section, the wavelet transform defined over the finite field F is derived, with descriptions of the irreducible components of the action of the "ax+b" group defined over F on $l^2(F)$, the vector space of real-valued functions on F. It is shown that the energy conservation property holds over all of $l^2(F)$ for certain admissible vectors in $l^2(F)$, allowing unitary wavelet transforms to be defined over all of $l^2(F)$. It should be noted that throughout this paper, $l^2(F)$

ISSN 1069-5869

denotes the space of functions defined over F, taking values in the complexes; elements of $l^2(F)$ are occasionally written as vectors.

In the final section, illustrative examples are given of compatible filters, pseudodilation representations, and wavelet transforms for some values of p^k.

2. Compatible Filters Defined Over F

The results of [1] are extendable, with very minor changes, from Z_p to arbitrary finite fields F. We can therefore define a standard wavelet transform, or a wavelet transform arising from a unitary pseudodilation representation, on sequences from $l^2(F)$. These sequences have length p^k, where p is a prime, and k is an arbitrary positive integer.

In what follows, we will introduce standard operators on $l^2(F)$, and state results that are analogous to those in [1]. These results will be stated without proof, except where the differences between F and Z_p make clarification necessary.

2.1 Finite fields F and operators on $l^2(F)$

First we give some well-known facts about finite fields. A convenient reference for the very few results we will need is [4].

1. Each finite field contains p^k elements for some prime p, and some positive number k. The prime p is called the characteristic of F; for any element $f \in F$, we have $pf = 0$. Every finite field of order p^k is isomorphic as a field to every other field of order p^k. The finite field F of order p^k will be referred to as F_{p^k} when necessary.
2. The additive group of the finite field of order p^k is isomorphic as an abelian group to the abelian group $(Z_p)^k$, consisting of k-tuples of elements of Z_p. Therefore, the unitary dual $\widehat{F}$ of the additive group of F, consisting of homomorphisms (characters) from the additive group of F to the group of complex numbers of modulus 1, is isomorphic to $(Z_p)^k \cong \left(\widehat{Z_p}\right)^k$ via a natural isomorphism. Let $\chi(k) = e^{2\pi i k/p}$, $k \in Z_p$; then χ is a character of Z_p. We then have that every element $N = (n_1, ..., n_k) \in (Z_p)^k$ gives rise to a character of $(Z_p)^k$ as follows:
$$N \longmapsto \chi_N, \text{ where } \chi_N((m_1, m_2, ..., m_k)) = \chi(M \cdot N).$$
Here $M \cdot N = m_1 n_1 + m_2 n_2 + ... + m_k n_k \in Z_p$ is the standard dot product in $(Z_p)^k$. Every character of $(Z_p)^k$ is obtainable in this fashion.
3. The multiplicative group $F^* = F/\{0\}$ of the finite field F is isomorphic to the cyclic group of order $p^k - 1$. This surprising fact allows us to calculate $H^1(F^*, T^{p^k})$ and $H^1(F^*, \mathbf{C}^{*p^k})$ as easily as we calculated $H^1(Z_p^*, T^p)$ and $H^1(Z_p^*, \mathbf{C}^{*p})$, so that we can describe all of the unitary and non-unitary pseudodilation representations of the affine group of F.
4. In order to describe the Fourier transform on $l^2(F)$, we assume that we are given a Z_p-vector space isomorphism $\Phi : F \to (Z_p)^k$, so that we can identify elements of F with elements of $(Z_p)^k$ using Φ. We will write χ_k instead of $\chi_{\Phi(k)}$ for the character of F corresponding to $\Phi(k)$. The Fourier transform F on $l^2(F)$ is given by
$$Ff(k) = \sum_{b \in F} \chi_k(\Phi(b))\, f(b),$$
and the inverse Fourier transform is
$$F^{-1}\widehat{f}(b) = \frac{1}{p^k} \sum_{k \in F} \chi_b(-\Phi(k))\, \widehat{f}(k).$$

We have translation in $l^2(F)$:

$$T_b f(k) = f(k-b),$$

dilation:

$$D_a f(k) = f(a^{-1}k),$$

and modulation:

$$E_b f(n) = \chi_b(\Phi(n)) f(n).$$

As usual, we have that

$$FT_b = E_{-b}F, \ FD_a = D_{a^{-1}}F, \text{ and } FT_bD_a = E_{-b}D_{a^{-1}}F.$$

The scalar product in $l^2(F)$ is given by

$$\langle f, g\rangle = \sum_{k\in F} f(k)\overline{g(k)};$$

we define

$$\|f\|^2 = \frac{1}{p^k}\langle f, f\rangle,$$

and the Parseval (Plancherel) identity gives

$$p^k\langle f, g\rangle = \langle Ff, Fg\rangle, \text{ or } p^k\|f\|^2 = \|Ff\|^2.$$

We also have the convolution product:

$$f * g(n) = \sum f(r)g(n-r) = \left(\sum f(r)T_r g\right)(n),$$

which satisfies

$$F(f*g)(n) = Ff(n)Fg(n).$$

2.2 The Affine Group Defined Over F

We define the F-affine group as follows:

$$G_F = \{(b,a) : b \in F, a \in F^*\}, \text{ with multiplication } (b,a)(b',a') = (b+ab', aa').$$

The representation

$$U : G_F \to U(l^2(F))$$

defined by

$$U(b,a)f = T_bD_af$$

gives a natural action of G_F on $l^2(F)$; that is, $U(b,a)\cdot U(b',a') = U(b+ab', aa')$. In [1], the term "pseudodilation representation" was coined to refer to any representation of G_F of the form

$$U(b,a)f = T_b\widetilde{D}_a,$$

where $\widetilde{D}_a$ is an invertible operator on $l^2(F)$. If the $\widetilde{D}_a$ term is factored into a product of an invertible operator with the standard dilation operator D_a on $l^2(F)$, $\widetilde{D}_a = K_aD_a$, then it is easily seen that the operator K_a must commute with all translation operators T_b, $b \in F$; that is, K_a is a convolution operator, $K_a = \sum_{b\in F} c_bT_b$ for some set $\{c_b\} \in \mathbb{C}$. Therefore, any pseudodilation representation is determined by the map $a \in F^* \longrightarrow K_a$, where K_a is convolution by some function $M_a \in l^2(F)$. The vectors M_a satisfy the condition

$$M_{aa'} = M_a * D_aM_{a'},$$

which after being Fourier transformed turns out to be the more familiar cocycle condition

$$\widehat{M_{aa'}}(k) = \widehat{M_a}(k)\widehat{M_{a'}}(ak).$$

The functions $M : F^* \to l^2(F)$ are called compatible filters.

If the resulting representation is to be unitary, we must also have

$$\left|\widehat{M_a}(k)\right| = 1 \text{ for all } a \in F^*, \text{ and } k \in F.$$

Thus, we may regard the compatible filters giving rise to unitary pseudodilation representations as functions from F^* to T^F, where T^F denotes functions from F to the complex unit circle. In what follows, v denotes an element of T^F. There is a natural action of F^* on T^F, given by

$$a.v\,(b) = v\left(a^{-1}b\right).$$

Lemma 1.

Let $\tau \in F^*$ be a generator of the cyclic group F^*. Then the functions $M_{(\cdot)} : F^* \to T^F$ of the form

$$\widehat{M_a}(n) = \prod_{k=0}^{r-1}(\tau^k.v)(n), \text{ where } a = \tau^r \in F^*, n \in F,$$

are compatible filters giving rise to unitary pseudodilation representations. The elements $\tau^k.v$ are to be viewed as functions $F \to T$, and v must satisfy $\prod_{k\in F^*} v(k) = 1$ and $v(0)^{p^k-1} = 1$.

Functions of this form satisfy the cocycle condition for compatible filters. If $a, a' \in F^*$, suppose that $a = \tau^r$, and $b = \tau^s$. Then $aa' = \tau^{r+s}$, and

$$\widehat{M_{aa'}} = \prod_{k=0}^{r+s-1}(\tau^k.v) = \prod_{k=0}^{r-1}(\tau^k.v) \cdot \tau^r \prod_{k=0}^{s-1}(\tau^k.v) = \widehat{M}_a \cdot a.\widehat{M}_{a'}.$$

The conditions on v are necessary in order to assure that $M_{\tau^{p^k}} = M_\tau$; this must hold, since $\tau^{p^k} = \tau$.

This result gives an explicit description of a class of compatible filters which gives rise to unitary pseudodilation representations, parametrized by $T^{|F|-1} \times F^*$. These are, in fact, all of the unitary compatible filters. As shown above, the functions

$$\hat{M}_{(\cdot)} \longrightarrow T^F$$

must satisfy the cocycle condition

$$\widehat{M_{aa'}}(k) = \widehat{M_a}(k)\widehat{M_{a'}}(ak)$$

for all $a, a' \in F^*$ and $k \in F$, in order to give rise to unitary compatible filters. Therefore, they are representative elements of the cohomology classes which constitute $H^1\left(F^*, T^F\right)$. Since F^* is a cyclic group, some well-known results on the construction of cyclic group cohomologies apply, and the standard methods of constructing *all* the elements in the kernel of the appropriate coboundary map yield precisely the cocycle functions given above. The details of this derivation, and references, are given in an appendix.

3. Wavelet Transforms Defined from Pseudodilation Representations

Operators in the standard representation U of G_F on $l^2(F)$ act as permutations on the vectors in $l^2(F)$; therefore, they preserve the $p^k - 1$ dimensional subspace E of $l^2(F)$ consisting of sequences having mean 0 [i.e., if $\psi \in E$, $\psi = \left(a_0, a_1, ..., a_{p^k-1}\right)$, then $\sum a_i = 0$; equivalently, $\hat{\psi}(0) = 0$].

Lemma 2.

The representation U restricted to $E \subseteq l^2(F)$ is irreducible.

This lemma can be proved by direct calculation, using Schur's lemma. Now let ψ be a fixed element of $l^2(F)$.

Definition. The standard wavelet transform $T_\psi : l^2(F) \longrightarrow l^2(G_F)$ associated with ψ is defined by

$$T_\psi f(a, b) = < f, U(a, b)\psi >,$$

for $f \in l^2(F)$, and $(a, b) \in G_F$. □

If $\psi \in E \subseteq l^2(F)$, then standard results on square integrable representations give the following result (see [1], [2]). We will denote by π the subrepresentation of U given by restricting the operators $U(b, a)$ to the invariant subspace E.

Theorem 1.

For fixed $\psi \in E$, the mapping $T_\psi|_E : E \to l^2(G_F)$ given by

$$T_\psi f(b, a) = \langle f, \pi(b, a)\psi \rangle$$

is isometric up to a constant factor $\sqrt{c_\psi}$; we have

$$\|T_\psi f\|^2 = c_\psi \|f\|^2,$$

where

$$c_\psi = \frac{1}{\|\psi\|^2} \sum_{(b,a)\in G_F} |\langle \psi, \pi(b, a)\psi \rangle|^2 = \frac{p^{2k}}{p^k - 1} \|\psi\|^2.$$

The irreducible subrepresentation $U|_E$ accounts for $p^k - 1$ dimensions of the representation U on $l^2(F)$; the remaining irreducible component of the representation is the identity representation, arising from the restriction of U to the one-dimensional subspace K of constant elements of $l^2(F)$ (clearly dilation and translation can have no effect on this subspace).

The unitary representations of G_F are all either isomorphic to the $p^k - 1$ dimensional representation π, or are characters of F^*. This is a consequence of the Peter-Weyl Theorem, which states that for any compact topological group G, each of its irreducible unitary representations appears in the regular representation of G on $L^2(G)$ with multiplicity equal to its dimension; in the case of G_F, it is easily seen that after the $p^k - 1$ dimensional representation of G_F on E is accounted for, there are only $p^k - 1$ dimensions of the $p^{2k} - p^k$ - dimensional left regular representation left for other representations, and these are fully accounted for by the characters of F^*, which must be present since F^* is the "abelianization" of G_F.

For $\psi \in l^2(F)$, define $\gamma(\psi) = \sum_{b\in F} \psi(b)$. For T_ψ defined with arbitrary $\psi \in l^2(F)$, if T_ψ is unitary, we have

$$\|T_\psi f\|^2_{l^2(G_F)} = \|T_\psi P_E f\|^2 + \|T_\psi P_K f\|^2,$$

where $P_E f$ and $P_K f$ denote the orthogonal projections of f onto E and K, respectively [note that $P_K f$ is the constant function $P_K f(x) = \frac{1}{p^k}\gamma(f)$]. It is easy to see that

$$\langle T_\psi P_E f, T_\psi P_E f \rangle = \langle T_{P_E\psi} P_E f, T_{P_E\psi} P_E f \rangle, \text{ and } \langle T_\psi P_K f, T_\psi P_K f \rangle = \langle T_{P_K\psi} P_K f, T_{P_K\psi} P_K f \rangle,$$

and so, using Theorem 1, we have

$$\|T_\psi f\|^2_{l^2(G_F)} = \frac{p^{2k}}{p^k - 1} \|P_E f\|^2 \|P_E\psi\|^2 + \frac{1}{p^{4k}} (|\gamma(f)\gamma(\psi)|)^2$$

$$= \frac{p^{2k}}{p^k - 1}(\|f\|^2 \|P_E\psi\|^2 - \frac{1}{p^{2k}} |\gamma(f)|^2 \|P_E\psi\|^2) + \frac{1}{p^{4k}} (|\gamma(f)\gamma(\psi)|)^2$$

$$= \|f\|^2 \left(\frac{p^{2k}}{p^k - 1} \|P_E\psi\|^2\right) + |\gamma(f)|^2 \left(\frac{1}{p^{4k}} |\gamma(\psi)|^2 - \frac{1}{p^k - 1} \|P_E\psi\|^2\right).$$

Thus, T_ψ is a multiple of an isometry precisely when $\|P_E\psi\|^2$ is nonzero, and either $\gamma(f) = 0$ (i.e., $f \in E$) or $\frac{1}{p^{4k}} |\gamma(\psi)|^2 - \frac{1}{p^k-1} \|P_E\psi\|^2 = 0$. This last condition is equivalent to the condition that

$$\frac{1}{p^{2k}} \left|\hat{\psi}(0)\right|^2 = \frac{1}{p^k - 1} \sum_{a \neq 0 \in F} \left|\hat{\psi}(a)\right|^2,$$

which is a necessary condition on ψ for T_ψ to be a multiple of an isometry. If $\psi \in l^2(F)$ is a nonzero function satisfying this condition, then $\|P_E\psi\|^2 \neq 0$, and therefore this condition is also sufficient.

We now consider the case where the representation U is replaced by a pseudodilation representation. Any unitary, or indeed nonunitary, pseudodilation representation $\sigma : G_F \longrightarrow U\left(l^2(F)\right)$ fixes the subspace E of $l^2(F)$; this is because $\sigma(a, b) = T_b K_a D_a$, where K_a is a convolution, and convolution operators are merely linear combinations of translation operators, which fix the subspace E.

A unitary pseudodilation representation $\sigma(b, a)$ arising from a filter F_a is unitarily equivalent to π when restricted to E, and is unitarily equivalent to a character of F^* when restricted to the space of constant sequences in $l^2(F)$; the character of F^* to which it is equivalent is given by

$$\chi(a) = \chi(\tau^m) = e^{2\pi i r m / p^k - 1}, \text{ where } \widehat{F_a}(0) = e^{2\pi i r / p^k - 1}.$$

We pause at this point to observe that the usual representation U of G_F on $l^2(F)$ is the pseudodilation representation given by the filter F_a satisfying $\widehat{F_a}(k) = 1$ for all $k \in F$. Thus, the results we are about to obtain for admissibility of a vector $\psi \in l^2(F)$ are also applicable to the representation U.

We have, for the wavelet transforms T_ψ^σ given by the representation $\pi = \sigma|_E$, defined as $T_\psi f(b, a) = \langle f, \sigma_E(b, a)\psi\rangle$ for a vector $\psi \in E$, that

$$\left\|T_\psi f\right\|^2 = c_\psi \|f\|^2,$$

where

$$c_\psi = \frac{1}{\|\psi\|^2} \sum_{(b,a) \in G_F} |\langle\psi, \sigma(b, a)\psi\rangle|^2 = \frac{p^{2k}}{p^k - 1} \|\psi\|^2;$$

i.e., the constant c_ψ is unchanged by replacing $U|_E$ by $\sigma|_E$. For any $\psi \in l^2(F)$, we define the wavelet transform

$$T_\psi : l^2(F) \to l^2(G_F)$$

by

$$T_\psi f(b, a) = \langle f, \sigma_E(b, a)\psi\rangle .$$

We then have that, for all $\psi, f \in l^2(F)$,

$$\left\|T_\psi^\sigma f\right\|^2 = \|f\|^2 \left(\frac{p^{2k}}{p^k - 1} \|P_E\psi\|^2\right) + |\gamma(f)|^2 \left(\frac{1}{p^{4k}} |\gamma(\psi)|^2 - \frac{1}{p^k - 1} \|P_E\psi\|^2\right),$$

as before, where $\gamma(f) = \widehat{f}(0) = \sum_{k \in F} f(k)$. Thus, we have the following proposition.

Theorem 2.
Let F_a be a compatible filter satisfying $\left|\widehat{F_a(k)}\right| = 1$ for all $k \in F$. Then the wavelet transform T_ψ defined using $\psi \in l^2(F)$ is a multiple of an isometry on all of $l^2(F)$ if and only if $\psi \neq 0$ satisfies

$$(p^k - 1)\left|\widehat{\psi}(0)\right|^2 = p^{2k} \sum_{k \in F^*} \left|\widehat{\psi}(k)\right|^2 .$$

If so, we have the reconstruction constant

$$\frac{\|T_\psi f\|^2}{\|f\|^2} = \frac{p^{2k}}{p^k - 1}\|\psi\|^2 \neq 0.$$

Proposition 1.
We then have, for all $f \in l^2(F)$, the reconstruction formula

$$f(n) = K \cdot \sum_{(b.a) \in G_F} T_\psi f(b, a)\left(\sigma(b, a)\psi\right)(n),$$

where K is a constant ([2]), $K = \left(\sum_{(b.a)\in G_F} \langle \sigma(b, a)\psi, \psi\rangle\right)^{-1}$.

4. Examples

In these sections, some simple, illustrative examples are given to demonstrate the construction of compatible filters and admissible vectors.

4.1 All Compatible Filters and Admissible Vectors for $p = 3$

The field Z_3 consists of the elements $\{0, 1, 2\}$, with multiplication and addition modulo 3. Lemma 1 states that a unitary compatible filter is completely determined by the choice of a function $v \in T^3$ satisfying $v(0)^2 = 1$, and $v(1) \cdot v(2) = 1$; thus $v(0) = a = \pm 1$, and $v(1) = v(2) = r$ for some r such that $|r| = 1$. Having made the choice of the function v, we have that $\widehat{M}_1 \equiv 1$ and $\widehat{M}_2 \equiv v$.

Letting ω denote a fixed primitive cube root of unity, we can find the compatible filter M by taking the inverse Fourier transform of the given functions. The function M_1, of course, is the convolution identity, the Dirac delta function centered at 0. The function M_2 is the inverse Fourier transform of v, given by

$$F^{-1}v(x) = \begin{cases} \frac{1}{3}\left(r + r^{-1} + a\right) & \text{if } x = 0 \\ \frac{1}{3}\left(a + \omega r + \omega^{-1} r^{-1}\right) & \text{if } x = 1 \\ \frac{1}{3}\left(a + \omega^{-1} r + \omega r^{-1}\right) & \text{if } x = 2 \end{cases} .$$

These give rise to one of two inequivalent unitary pseudodilations, depending on whether a is chosen to be 1 or -1.

The method given here for finding admissible vectors ψ which give rise to isometric wavelet transforms generalizes easily to find admissible vectors in $l^2(F)$ for any F; the component of ψ which belongs to E can be chosen freely, and a constant component can be added to $P_E\psi$ which causes the condition in Theorem 2 to be satisfied. For the case of Z_3, suppose $\widehat{P_E\psi} = (0, x, y)$ for some values $x, y \in \mathbb{C}$ (note that any function in E satisfies $\widehat{f}(0) = 0$). Then, to be admissible, ψ must satisfy $\left|\widehat{\psi}(0)\right|^2 = \frac{9}{2}\left(|x|^2 + |y|^2\right)$. This can be achieved by adding to $P_E\psi$ the constant function with value $P_K\psi \equiv \frac{\sqrt{2}}{2}s\sqrt{|x|^2 + |y|^2}$. $P_E\psi$ is obtained by taking the inverse Fourier transform of $(0, x, y)$.

4.2 Compatible Filters for $p^2 = 2^2 = 4$

The field $F = F_{2^2}$, which is the smallest finite field that is not of prime order, may be constructed by forming the polynomial ring $Z_2[x]$ over an indeterminate x, and defining addition and multiplication modulo the irreducible polynomial x^2+x+1. This is just like normal polynomial addition and multiplication, except that field operations are done modulo 2, and the relation $x^2 \equiv x+1$ holds. One is easily convinced that the field F consists of four elements: $0, 1, x$, and $x+1$. Since $F^* \simeq Z_3$ is a prime field, all members of F^* except for 1 are generators of the multiplicative group of F. Therefore, we fix a generator of F^*, $\tau = x$. Below is a table defining the multiplication in F.

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

. Unitary compatible filters are now functions $M : F^* \simeq Z_3 \to l^2(F)$, and again, a compatible filter is completely determined by its defining function $v \in T^4$, which must satisfy $v(0)^3 = 1$ and $v(1) \cdot v(x) \cdot v(x+1) = 1$. We have, from Lemma 1, that $\widehat{M}_1 \equiv 1$, $\widehat{M}_x = v$, and $\widehat{M}_{x+1} = v \cdot x.v$, where $x.v$ denotes the action of x on v by $x.v(a) = v\left(x^{-1}a\right) = v((x+1)a)$. This gives

$$\begin{aligned}\widehat{M}_{x+1} &= \left(\widehat{M}_{x+1}(0), \widehat{M}_{x+1}(1), \widehat{M}_{x+1}(x), \widehat{M}_{x+1}(x+1)\right) \\ &= \left(v(0)^2, v(x+1)\,v(1), v(1)\,v(x), v(x)\,v(x+1)\right).\end{aligned}$$

In general, we set $v(0) = \omega$ for ω a primitive cube root of unity, and set $v(1) = r$ and $v(x) = s$ for some r, s of unit modulus, with $v(x+1) = (rs)^{-1}$ of necessity. Then we have $\widehat{M}_x = \left(\omega, r, s, (rs)^{-1}\right)$ and $\widehat{M}_{x+1} = \left(\omega^2, s^{-1}, rs, r^{-1}\right)$. The compatible filters themselves can be found by taking the inverse Fourier transforms of $\widehat{M}_x$ and $\widehat{M}_{x+1}$.

A computational caveat; the Fourier transform taking values in the complexes, and defined over the field of order 2^k, bears little relation to the standard Fourier transform of length 2^k; in addition, it is complex-valued, and so bears no relation to the binary-valued Fourier transforms used in coding theory to define cyclic linear codes. It can be seen from the definition of Fourier transform that the finite field Fourier transform over the field of order 2^k contains only *second* roots of unity, and no primitive roots of higher order. Since only the factors ± 1 are involved in computations, however, Fourier transforms over finite fields of order 2^k are easily programmed and quickly computed.

5. Appendix: $H^1\left(F^*, T^F\right) \simeq Z_{|F|-1}$

In this appendix, it is shown that all the functions from F^* to $T^F = \{f : F \to \mathbb{C} : |f(x)| = 1 \text{ for all } x\}$ are given by the construction outlined in Lemma 1. For simplicity of notation, we restrict the discussion to $F = Z_p$ for some prime p; however, the discussion generalizes to F of order p^k, since F^* is always cyclic.

Consider the action of Z_p^* on the p-torus T^p, consisting of p-tuples of complex numbers of modulus 1, given by

$$a.C = a.(c_1, c_2, \ldots, c_p) = (c_{a.1}, c_{a.2}, \ldots, c_{a.p}).$$

The cocycle condition on the $\widehat{F_a}$, together with the requirement that the pseudodilation be unitary, means that the desired functions F map Z_p^* into T^p and are actually cocycle representatives of the cohomology group $H^1(Z_p^*, T^p)$.

The group Z_p^* is isomorphic to the cyclic group of order $p-1$, and we can compute $H^1(Z_p^*, T^p)$ using some well-known theorems for calculating cyclic group cohomologies, which apply also to the calculation of $H^1\left(F^*, T^F\right)$

The following material is developed in [3, Sec. VI.7]. We think of T^p as a Z_p^*-module as given above. Cocycles are functions $\sigma : Z_p^* \to T^p$, which satisfy $\sigma(aa') = \sigma(a) \cdot a.\sigma(a')$.

Choose a generator $\tau \in Z_p^*$, and define the maps

$$\phi : T^p \to T^p, \ \phi(C) = \tau.C \cdot C^{-1},$$

$$\psi : T^p \to T^p, \ \psi(C) = \prod_{k=0}^{p-2} \tau^k.C.$$

Then Proposition 7.1 of [3] says that $H^1(Z_p^*, T^p) \cong \ker(\psi)/\operatorname{im}(\phi)$.

Ker (ψ) can be easily calculated once one observes that the product is over all the elements of Z_p^*. Suppose $C \in \ker(\psi)$; since $C = (c_1, ..., c_p)$, and the action of Z_p^* fixes the element c_p, we must have $c_p^{p-1} = 1$, so that c_p must be a $p-1$th root of unity. Since each nonzero element of Z_p is a generator of the additive group Z_p, we will have $\psi(C) = (k, ..., k, c_p^{p-1})$, where k is the product of all the c_i, $i \neq p$. Therefore, $C \in \ker(\psi)$ if and only if $k = 1$ and c_p is a $p-1$th root of unity. Thus, we have $\ker(\psi) = \left\{C \in T^p : C = (c_1, ...c_{p-2}, (c_1..c_{p-2})^{-1}, c_p), \text{ where } c_p^{p-1} = 1\right\}$. On the other hand, Im $(\phi) = \left\{\tau.C \cdot C^{-1} : C \in T^p\right\} = \left\{(c_1^{-1}c_{\tau(1)}, c_2^{-1}c_{\tau(2)}, ..., c_p^{-1}c_{\tau(p)}), c_i \in T\right\}$. Since each τ fixes p, we have $c_p^{-1}c_{\tau(p)} = 1$ for any τ. Since $\operatorname{Im}(\phi) \cong T^p/\ker(\phi)$, we calculate $\ker(\phi)$. $\operatorname{Ker}(\phi) = \{C \in T^p : C \text{ is } \tau\text{-fixed}\} = \left\{C \in T^p : C \text{ is } Z_p^*\text{-fixed}\right\}$, since τ is a generator of Z_p^*; if C is Z_p^*-fixed, it is easy to see that $C = (a, a, ..., a, b)$, where $a, b \in T$. Therefore, $\operatorname{Im}(\phi)$ is isomorphic to the subgroup of T^p consisting of elements of the form $C = (\beta_1, \beta_2, ..., \beta_{p-2}, \left(\beta_1\beta_2...\beta_{p-2}\right)^{-1}, 1)$.

This proves the following proposition:

Proposition 2.

$H^1(Z_p^*, T^p) \cong \ker(\psi)/Im(\phi) \cong Z_p^* \cong Z_{p-1}$.

As a final note, we observe that the value of $\widehat{M_\tau}(0)$, which must satisfy $\widehat{M_\tau}(0)^{p-1} = 1$, determines which cohomology class the cocycle representative $\widehat{M} : Z_p^* \to T^p$ actually lies in; furthermore, the pseudodilation representations derived from compatible filters coming from different cohomology classes are inequivalent because the restrictions of these representations to the space of constant functions $K \in l^2\left(Z_p\right)$ are inequivalent characters. Conversely, those compatible filters that come from the same cohomology class are unitarily equivalent representations.

References

[1] Flornes, K., Grossmann, A., Holschneider, M., and Torrésani, B. (1994). Wavelets on discrete fields. *Appl. Computational Harmonic Analysis.* 1, (2), 137–146.

[2] Grossmann, A., Morlet, J., and Paul, T. (1985). Transforms associated to square-integrable group representations, I, General results. *J. Math. Phys.,* 26, 2473–2479.

[3] Hilton, P., and Stammbach, U. (1971). A Course in Homological Algebra. Graduate Texts in Mathematics series No. 4, Springer-Verlag, Berlin.

[4] Lidl, R. and Pilz, G. (1984). Applied Abstract Algebra. Undergraduate Texts in Mathematics Series, Springer-Verlag, Berlin.

Received December 4, 1994
Revised received January 16, 1997

VEXCEL, Image Information Engineering, Boulder, CO 80301