APPLIED AND COMPUTATIONAL HARMONIC ANALYSIS **1**, 137–146 (1994)

Wavelets on Discrete Fields

K. FLORNES

Department of Mathematics, Norwegian Institute of Technology, University of Trondheim, 7034 Trondheim-NTH, Norway

AND

A. GROSSMANN, M. HOLSCHNEIDER, AND B. TORRÉSANI

Centre de Physique Théorique, CNRS-Luminy, Case 907, 13288 Marseille Cedex 09, France; and Groupement de Recherches "Ondelettes," CNRS

Communicated by Guido L. Weiss

Received July 19, 1993

An arithmetic version of continuous wavelet analysis is described. Starting from a square-integrable representation of the affine group of $\mathbb{Z}_p$ (or $\mathbb{Z}$) it is shown how wavelet decompositions of $\ell^2(\mathbb{Z}_p)$ can be obtained. Moreover, a redefinition of the dilation operator on $\ell^2(\mathbb{Z}_p)$ directly yields an algorithmic structure similar to that appearing with multiresolution analyses.

1. INTRODUCTION

Wavelet analysis can be seen today from essentially two different points of view. A first approach is connected with the theory of coherent states of quantum physics, and can be formulated in terms of group representation theory. The second approach basically consists in an "algorithmic" version of Littlewood–Paley analysis, and yields fast algorithms for computing the wavelet transform numerically.

The connection between these two approaches is quite difficult to handle, in particular because the first is a "continuous approach" and the second is essentially discrete. We discuss here an intermediate approach, based on the square-integrable representations of some finite groups, that could help to pave the way between the continuous and discrete aspects (we do not discuss here the purely discrete case, in which the signals also take values in a discrete field).

We consider the set $\ell^2(\mathbb{Z}_p)$ of finite energy sequences on $\mathbb{Z}_p$, the class of integers modulo p. When p is a prime number, $\mathbb{Z}_p$ has the structure of a number field, and a discrete affine group can be defined. The canonical action of this group on $\ell^2(\mathbb{Z}_p)$ is square-integrable, and systems of wavelets can be associated with it. Moreover, it is easy to see that in such a case, there is an associated "fast algorithm" for the computation of the corresponding wavelet transform.

The connection with multiresolution structures is made by considering possible deformations of the action of the affine group on $\ell^2(\mathbb{Z}_p)$. In particular, the deformation of the dilation operator directly yields an algorithmic structure similar to that associated with quadrature mirror filters.

The paper is organized as follows. After some algebraic preliminaries (Section 2) and general results on square-integrable group representations and associated systems of wavelets (Section 3), we describe the wavelets on $\ell^2(\mathbb{Z}_p)$ and give some numerical illustrations (Section 4). Then we study the possible deformations of the dilation operators and describe the corresponding wavelet systems (Section 5), and give some conclusions.

2. ALGEBRAIC BACKGROUND

2.1. Group Representations

Our discussion is based on a group theoretical approach to wavelets. In this section we recall the definition of a square integrable representation. Basic concepts such as a group, a field and a representation of a group on a Hilbert space are assumed to be known. For the reader who is not familiar with group theory, we refer to [6] for an introduction.

Our presentation is based on the theory of square-integrable group representations, the definition of which we recall here for convenience.

DEFINITION 1. Let $g \to U(g)$ be a strongly continuous unitary representation of a locally compact separable group G in a Hilbert space $\mathscr{H}(U)$. The representation U is said to be square integrable if

- U is irreducible.
- There exists at least one $\psi \in \mathscr{H}(U)$ such that

$$c_\psi = \int_G |\langle\psi, U(g)\psi\rangle|^2 d\mu(g) < \infty \qquad (1)$$

1063-5203/94 $6.00

where μ is the left invariant measure. Such a ψ is called an "admissible vector."

2.2. Number Theory

For the construction of wavelets on a finite field, we need some basic concepts from number theory. More precisely, we describe here some algebraic properties needed to introduce the affine group over $\mathbb{Z}_p$, referring to [4] for more details.

Two integers, a and b, which have the same remainder modulo n are said to belong to the same residue class modulo n. We write

$$a \equiv b \pmod{n} \quad (a \text{ is congruent to } b \bmod n), \tag{2}$$

which is equivalent to n divides $a - b$. The different remainders mod n are the numbers $0, 1, 2, \ldots, |n| - 1$.

THEOREM 1. *Let the integers a, b, n be given. The congruence*

$$ak + b \equiv 0 \pmod{n} \tag{3}$$

has exactly one solution mod n *if a and n are relatively prime.*

THEOREM 2 (Fermat). *For each a relatively prime to n,*

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(n)$ is the number of residue classes relatively prime to n (Euler's φ function).

If n is a prime number p, then $\varphi(p) = p - 1$ and we have the congruence

$$a^{p-1} \equiv 1 \pmod{p} \tag{4}$$

The set of remainders mod p is a field. We denote this field by the symbol $\mathbb{Z}_p$. The set $\mathbb{Z}_p^*$ contains the nonzero elements of $\mathbb{Z}_p$.

The main consequence for our purpose of this discussion is that if p is any prime number, the set $\mathbb{Z}_p \times \mathbb{Z}_p^*$ inherits a group structure, via the group operation

$$(b, a) \cdot (b', a') = (b + ab', aa'). \tag{5}$$

We denote by G_p the corresponding group, called the affine group on $\mathbb{Z}_p$.

3. GENERAL THEOREMS

In this section we present two useful theorems. The first one was presented by Grossmann, Morlet, and Paul in [3]. They introduced the wavelet transform in terms of square integrable representation theory, and obtained an isometric correspondence between the function and its transform. The second theorem and the following proposition state that such an isometry also exists even if the representation is not irreducible.

Let G be a locally compact group and U a square integrable representation of this group on the Hilbert space $\mathcal{H}(U)$. Following Grossmann, Morlet and Paul, we define the transform T_f of $f \in \mathcal{H}(U)$ by

$$T_f(g) = \frac{1}{\sqrt{c_\psi}} \langle f, U(g)\psi \rangle \quad g \in G, \tag{6}$$

where ψ is an admissible vector. c_ψ is the constant defined by (1).

THEOREM 3. *The correspondence $f \mapsto T_f$ is isometric from $\mathcal{H}(U)$ into $L^2(G, d\mu(g))$, that is, for every $f, h \in \mathcal{H}(U)$, we have*

$$\int_G T_f(g)\overline{T_h(g)}d\mu(g) = \langle f, h \rangle. \tag{7}$$

Proof. The proof, which is a direct consequence of Schur's lemma, be found in [3], for instance (as a part of a much stronger result). ∎

Theorem 3 is the classical result that is at the basis of continuous wavelet analysis. The irreducibility assumption can be weakened as follows.

THEOREM 4. *Let U be a unitary representation of a locally compact, separable group G on the Hilbert space $\mathcal{H}(U)$. If U can be decomposed into disjoint square integrable components U_i, then*

$$\int_G |\langle f, U(g)\psi \rangle|^2 d\mu(g) = \sum_i c_{P_i\psi} \|P_i f\|^2, \tag{8}$$

where P_i is the orthogonal projection operator from $\mathcal{H}$ into $\mathcal{H}_i$, μ is the left invariant measure and ψ is an admissible vector. The constant $c_{P_i\psi}$ is given by the formula

$$c_{P_i\psi} = \frac{1}{\|P_i\psi\|^2_{\mathcal{H}_i}} \int_G |\langle P_i\psi, U_i(g)P_i\psi \rangle|^2 d\mu(g). \tag{9}$$

Proof. Consider the L^2-norm of the Schur coefficients:

$$\begin{aligned}\int_G |\langle f, U(g)\psi \rangle|^2 d\mu(g) &= \sum_{i,j} \int_G \langle P_i f, U_i(g)P_i\psi \rangle \\ &\quad \times \langle U_j(g)P_j\psi, P_j f \rangle d\mu(g) \\ &= \sum_i \langle P_i f, A_{ii} f \rangle + \sum_{i \neq j} \langle P_i f, A_{ij} P_j f \rangle.\end{aligned}$$

It can easily be shown that the operator A_{ij} verifies the covariance equation

$$U_i(g)A_{ij} = A_{ij}U_j(g) \quad \forall g \in G \tag{10}$$

Using Schur's lemma we see that A_{ij} is equal to zero when $i \neq j$ and A_{ij} is a multiple of the identity operator in $\mathcal{H}_i$ when $i = j$,

$$\begin{aligned}\int_G |\langle f, U(g)\psi\rangle|^2 d\mu(g) &= \sum_i \int_G |\langle P_i f, U_i(g)P_i\psi\rangle|^2 d\mu(g)\\ &= \sum_i \langle P_i f, A_{ii}P_i f\rangle\\ &= \sum_i c_{P_i\psi}\|P_i f\|^2,\end{aligned}$$

where the constant $c_{P_i\psi}$ is given by Eq. (9). ■

We can now state the following proposition.

PROPOSITION 1. *If the constants $c_{P_i\psi} = c_\psi$ are the same for all the subspaces $\mathcal{H}_i$ then the correspondence $f \mapsto \langle f, U(g)\psi\rangle$ is an isometry up to a constant factor from $\mathcal{H}(U)$ into $L^2(G, d\mu(g))$.*

$$\begin{aligned}&\int_G |\langle f, U(g)\psi\rangle|^2 d\mu(g)\\ &\quad = \sum_i c_{P_i\psi}\|f\|^2 = c_\psi \sum_i \|P_i f\|^2 = c_\psi \|P_i f\|^2\end{aligned} \tag{11}$$

The case in which some of the components are unitarily equivalent can be handled in the same way. Note also that the proposition, applied to the affine group of $\mathbb{R}$, provides wavelet decompositions of $L^2(\mathbb{R})$, considered as the direct sum of its two irreducible subrepresentations $H^2_\pm(\mathbb{R})$.

4. WAVELETS ON $\mathbb{Z}_p$

Let p be a prime number. In Section 2.2, we considered the field $\mathbb{Z}_p$ and introduced the corresponding affine group G_p. We are now going to construct wavelets on $\mathbb{Z}_p$ and analyze sequences in the Hilbert space $\ell^2(\mathbb{Z}_p)$.

4.1. Notation

Let us first specify our conventions and introduce for convenience some useful operators.

Operators. Fourier transform:

$$Ff(k) = \hat{f}(k) = \sum_{n=0}^{p-1} e^{-2\pi i nk/p} f(n). \tag{12}$$

Inverse Fourier transform:

$$F^{-1}\hat{f}(n) = f(n) = \frac{1}{p}\sum_{k=0}^{p-1} e^{2\pi ikn/p}\hat{f}(k). \tag{13}$$

Note that the Fourier transform can be defined on $\mathbb{Z}_N$ for every integer N.

Translation:

$$T_b f(n) = f(n-b). \tag{14}$$

Dilation:

$$D_a f(n) = f(a^{-1}n). \tag{15}$$

Note that in order for a^{-1} to be meaningful, it is necessary that p be a prime number.

Modulation:

$$E_b f(n) = \omega^{bn} f(n), \tag{16}$$

where $\omega = e^{2\pi i/p}$.

All these operators are well defined on $\mathbb{Z}_p$. The following properties can be easily verified

1. $FT_b = E_{-b}F$.
2. $FD_a = D_{a^{-1}}F$.
3. $FT_bD_a = E_{-b}D_{a^{-1}}F$.

Scalar Product.

$$\langle f, h\rangle = \sum_{n=0}^{p-1} f(n)\bar{h}(n), \tag{17}$$

where $\bar{h}$ is the complex conjugate of h. (We use the notation $\bar{h}$ or h^* for the complex conjugate of h).

The Parseval identity reads

$$\langle Ff, Fh\rangle = p\langle f, h\rangle. \tag{18}$$

Convolution Product.

$$f * g(n) = \sum_{j=0}^{p-1} f(n-j)g(j). \tag{19}$$

4.2. The Affine Group

We consider the group of affine transformations of $\mathbb{Z}_p$,

$$n \in \mathbb{Z}_p \to an + b. \tag{20}$$

This group can be defined as the set $G_p = \{(b,a) \mid b \in \mathbb{Z}_p,\ a \in \mathbb{Z}_p^*\}$ with the multiplication

$$(b_1, a_1)(b_2, a_2) = (b_1 + a_1 b_2, a_1 a_2). \tag{21}$$

The identity in the group is the element $(0, 1)$. The inverse $(b,a)^{-1} = (b', a')$ has to fulfill the congruences

$$aa' \equiv 1 \quad (\mathrm{mod} : p) \tag{22}$$

$$b + ab' \equiv 0 \quad (\mathrm{mod}\ p) \Longleftrightarrow b' \equiv -a'b(\mathrm{mod}\ p). \tag{23}$$

We reserve the symbol a^{-1} for the integer a' that satisfies (22).

$$(b,a)^{-1} = (-a^{-1}b, a^{-1}) \tag{24}$$

We are concerned with the following representation of the group G_p in $\ell^2(\mathbb{Z}_p)$.

DEFINITION 2. The unitary representation π,

$$\pi : G_p \to \mathcal{U}[\ell^2(\mathbb{Z}_p)], \tag{25}$$

where $\mathcal{U}[\ell^2(\mathbb{Z}_p)]$ is the set of unitary operators on $\ell^2(\mathbb{Z}_p)$, is defined by

$$\pi(g)f(n) = f(a^{-1}(n-b)) = f_{(b,a)}(n). \tag{26}$$

Using the operators of translation and dilation defined by (14) and (15), π can be written as

$$\pi(b,a) = T_b D_a. \tag{27}$$

Translations and dilations of a constant sequence do not change the sequence. The space of constant sequences is therefore an invariant subspace of π. It is then natural to work on spaces of sequences modulo a constant. Let $\mathbf{E} = \{f \in \ell^2(\mathbb{Z}_p) | \sum_{n=0}^{p-1} f(n) = 0\}$.

LEMMA 1. *The representation π restricted to the subspace $\mathbf{E}$ is irreducible.*

Proof. This follows from classical arguments, see, e.g., [6]. ■

Following the usual convention, we call a sequence ψ in $\ell^2(\mathbb{Z}_p)$ which satisfies certain additional conditions stated later in Theorems 5 and 6 an "analyzing wavelet." The family of sequences $\psi_{(b,a)}$ generated from translations and dilations of such an analyzing wavelet are called "wavelets."

4.3. Wavelet Transform

We are now in position to introduce the wavelet transform on ℓ^2 and state its general properties.

DEFINITION 3. The wavelet transform T_f associated with the analyzing wavelet ψ is the map

$$T_f : \ell^2(\mathbb{Z}_p) \to \ell^2(G_p)$$

$$T_f(b,a) = \langle f, \psi_{(b,a)} \rangle = \sum_{n=0}^{p-1} f(n) \overline{\psi}_{(b,a)}(n). \tag{28}$$

We can express the wavelet transform in terms of the Fourier transforms of f and ψ by using Parseval's identity and the relation $FT_b D_a = E_{-b} D_{a^{-1}} F$:

$$\begin{aligned} T_f(b,a) &= \langle f, \psi_{(b,a)} \rangle \\ &= \frac{1}{p} \langle \hat{f}, E_{-b} D_{a^{-1}} \hat{\psi} \rangle \\ &= \frac{1}{p} \sum_{n=0}^{p-1} \hat{f}(n) e^{2\pi i b n/p} \hat{\psi}(an)^*. \end{aligned} \tag{29}$$

As in the continuous case the wavelet transform can be inverted on its range, as shown by the two following theorems (corresponding respectively to the irreducible representation of G_p on $\mathbf{E}$ and the reducible one on ℓ^2).

THEOREM 5. *Let $\psi \in \ell^2(\mathbb{Z}_p)$ be such that*

$\psi \in \mathbf{E} \subset \ell^2(\mathbb{Z}_p)$, *where*

$$\mathbf{E} = \{f \in \ell^2(\mathbb{Z}_p) | \sum_{n=0}^{p-1} f(n) = 0\}\ ; \tag{30}$$

then the mapping $f \mapsto T_f$ is isometric up to a constant factor c_ψ from $\mathbf{E}$ into $\ell^2(G_p)$. There exists an inversion formula

$$f(n) = \frac{1}{c_\psi} \sum_{(b,a) \in G_p} T_f(b,a) \psi_{(b,a)}(n), \tag{31}$$

where the constant c_ψ is given by the formula

$$c_\psi = p \|\psi\|^2_{\ell^2(\mathbb{Z}_p)}. \tag{32}$$

Proof. The theorem follows from Theorem 3. It can also be proved by direct calculation. ■

THEOREM 6. *Let $\psi \in \ell^2(\mathbb{Z}_p)$ be such that*

$$(p-1)|\hat{\psi}(0)|^2 = \sum_{k=1}^{p-1} |\hat{\psi}(k)|^2; \tag{33}$$

then the mapping $f \mapsto T_f$ is isometric up to a constant factor c_ψ from $\ell^2(\mathbb{Z}_p)$ into $\ell^2(G_p)$. We have an inversion formula

$$f(n) = \frac{1}{c_\psi} \sum_{(b,a)\in G_p} T_f(b,a)\psi_{(b,a)}(n), \tag{34}$$

where the constant is given by

$$c_\psi = (p-1)|\hat{\psi}(0)|^2. \tag{35}$$

Proof. We observe first that the sequence space $\ell^2(\mathbb{Z}_p)$ can be written as a sum of the two subspaces

$$\ell^2(\mathbb{Z}_p) \cong \mathbb{C} \oplus \mathbf{E}.$$

Using Eq. (9) to calculate the constants $c_{P_i\psi}$ in the subspaces, we find that condition (33) states that these constants are equal. The theorem then follows from Proposition 1. ■

It is also very easy to check that the discrete wavelet transform on **E** shares with the continuous wavelet transform the usual properties, such as covariance with respect to dilations and translations, and existence of reproducing kernels in the image of **E** by the transform.

Theorems 5 and 6 can also easily be modified in the following way. It is always possible to use for the reconstruction a wavelet different than the analysis wavelet. This remark, that was used in a number of different contexts, is a consequence of the redundancy of the wavelet transform.

4.4. Some Practical Remarks and Illustrations

We make a few remarks concerning the transform and its interpretation before presenting some illustrations. We focus on the version of wavelet analysis provided by Theorem 5, which is closer to what we are used to.

- *Localization of the wavelet.* By a change of variable the wavelet transform can be written as

$$T_f(b,a) = \sum_{n=0}^{p-1} f(n)\bar{\psi}(a^{-1}(n-b)) = \sum_{n=0}^{p-1} f(an+b)\bar{\psi}(n). \tag{36}$$

  Suppose that ψ is concentrated somewhere; e.g., that it vanishes numerically outside a certain interval $I \subset \mathbb{Z}_p$. We can speed up our calculations by using the formula

$$T_f(b,a) = \sum_{n\in I} f(an+b)\bar{\psi}(n). \tag{37}$$

  Moreover, it is worth noting that the D_a dilation used here does not change the number of nonvanishing coefficients of the wavelet ψ (in some sense it may be called a dilation "with holes"). Then the previous formula is suitable for a fast implementation.

- *Reconstruction of signals which do not have mean* 0. Let $f \in \ell^2(\mathbb{Z}_p)$ and $s(n) = f(n) + k$, where k is a constant. $T_f = T_s$ if the analyzing wavelet ψ belongs to the set **E**. Suppose $\sum_{n=0}^{p-1} f(n) = c \neq 0$. With the reconstruction formula of Theorem 5 we actually reconstruct $f(n) - c/p$. From a practical point of view, this means that the mean value of an analyzed signal has to be stored before its wavelet decomposition is done.
- *Graphical conventions.* The modulus of the wavelet transform $T_f(b,a)$ is represented with gray levels inside the big box. The dilation parameter a varies vertically ($a = 1$ at the top and $a = p-1$ at the bottom). The translation parameter b varies horizontally from right to left (from $b = 0$ to $b = p-1$). The small box above the transform contains the real part of the signal and the two boxes below contain the real parts of the wavelet and the reconstructed signal. When there is a curve on the side of the wavelet transform, it indicates the energy e of the transform for the different scales $e(a) = \sum_{b=0}^{p-1} |T_f(b,a)|^2$.

Figure 1. (a) The wavelet is real-valued with five nonzero values and zero integral. The signal f vanishes everywhere except at $n = 26$ where $f(26) = 1.0$. This gives us that $T_f(b,a) = \psi(a^{-1}(26-b))$. "What disappears on one side reappears on the other." Moreover, as stressed before, the "with holes" dilation appears clearly here.
(b) The wavelet is real-valued with only three nonzero values and $\sum_{n=0}^{p-1} \psi(n) = 0$. The signal is a sine, and the corresponding wavelet transform has a structure similar to the continuous one (see, e.g. , [2]).

Figure 2. The signal is an exponential $f_1(n) = e^{3\cdot 2\pi k/p}$. The wavelet is also complex-valued $\psi(n) = e^{ik_1 n}e^{-k_2 n^2}$, and it is centered around a certain frequency ω_0. We have that $|T_f(b,a)| = |\hat{\psi}(\omega a)|$ where ω is the frequency of the signal. The modulus $|T_f(b,a)|$ has a maximum every time the parameter a is such that $\omega a \equiv \omega_0 \pmod p$. This explains the periodicity (with respect to scale) that we observe.

Figure 3. The signal is a superposition of the two exponentials with different frequencies and the wavelet is the same as in Fig. 2. In the image with the phase we have replaced the signal and the wavelet by their Fourier transforms.

5. PSEUDODILATION AND MULTIRESOLUTION STRUCTURE

In the preceding section we analyzed sequences and considered a purely discrete wavelet transform. We now look at the correspondence between a continuous signal and its sampled form. Following the philosophy of the algorithm

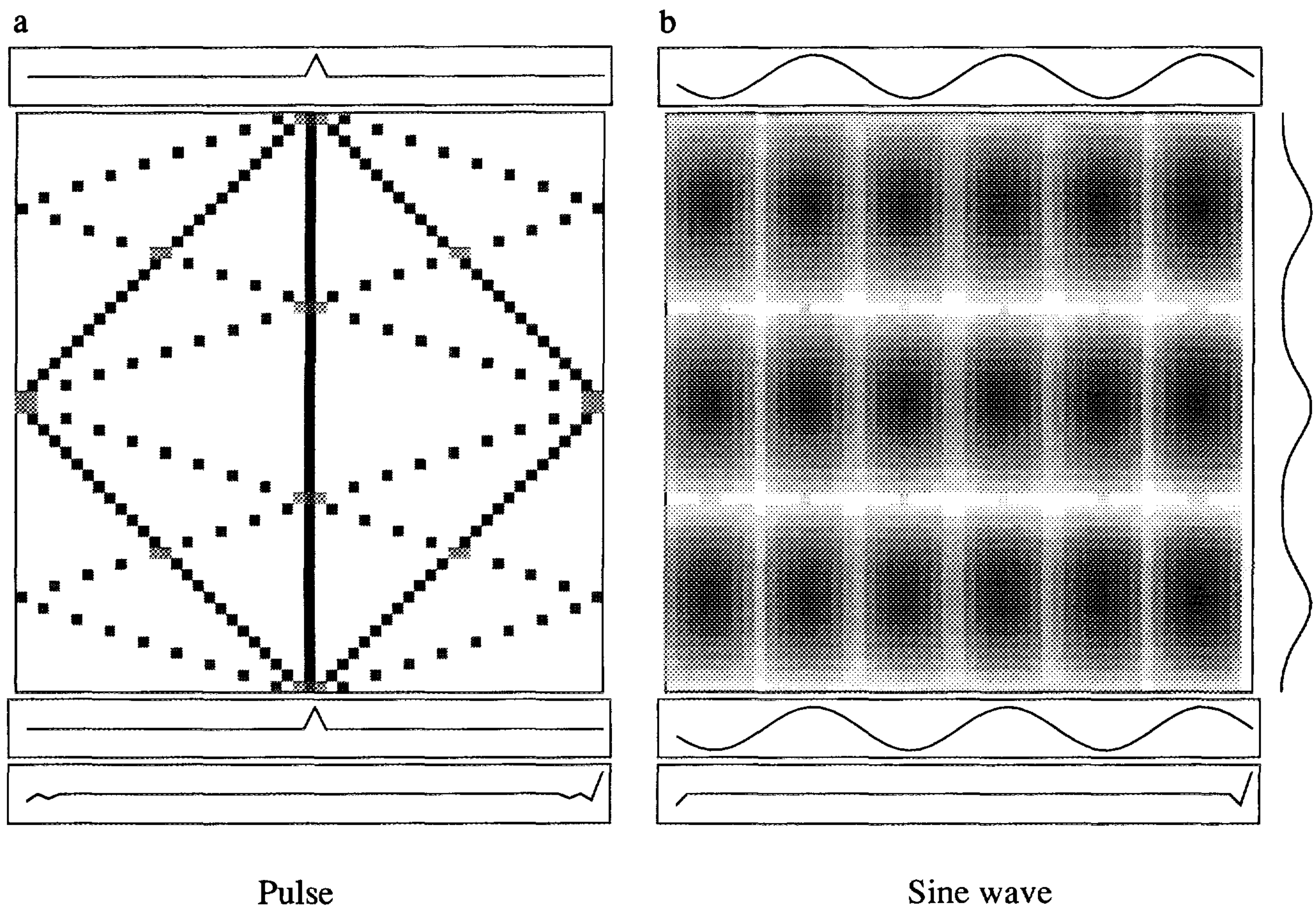

FIG. 1. Modulus of the wavelet transform of elementary functions ($p = 53$).

"à trous" presented in [5], we introduce interpolating filters.

Which changes need to be made to our transform if we want to interpret a sequence as a sampling of a continuous function ? In the continuous case the dilation operator $\tilde{D}_a$ is defined as

$$\tilde{D}_a f(x) = \frac{1}{a} f\left(\frac{x}{a}\right) \quad f \in L^2(\mathbb{R}). \tag{38}$$

Suppose that the continuous wavelet $g(x)$ oscillates in the interval $\langle -2, 2\rangle$ and is 0 outside. $\tilde{D}_2 g(x)$ then oscillates in the interval $\langle -4, 4\rangle$. When sampled by one, the function is left with seven nonzero values. Looking at Fig. 1, image 1 we observe that the discrete dilation operator D_a preserves the number of nonzero values of the wavelet. If we want to interpret the discrete case as a sampled version of the continuous case, our dilation does not possess the desired properties.

5.1. Pseudodilations

These observations lead us to introduce a pseudodilation $\mathcal{D}_a$ which not only dilates a sequence, but also "fills the holes." Let then K_a be a sequence of linear operators (labeled by the dilation parameters a) acting on ℓ^2, and set

$$\mathcal{D}_a = K_a D_a \tag{39}$$

The possible pseudo-dilation operators are constrained by the following fundamental lemma

Lemma 2. *The operators $\sigma(b, a) = T_b \mathcal{D}_a$ form a representation of G_p if and only if the K_a operator is a convolution operator*

$$\mathcal{D}_a = F_a * D_a \tag{40}$$

with a filter F_a that satisfies the compatibility relations

$$F_{aa'} = F_a * D_a F_{a'}, \tag{41}$$

or equivalently in the Fourier space

$$\hat{F}_{aa'}(k) = \hat{F}_a(k)\hat{F}_{a'}(ak). \tag{42}$$

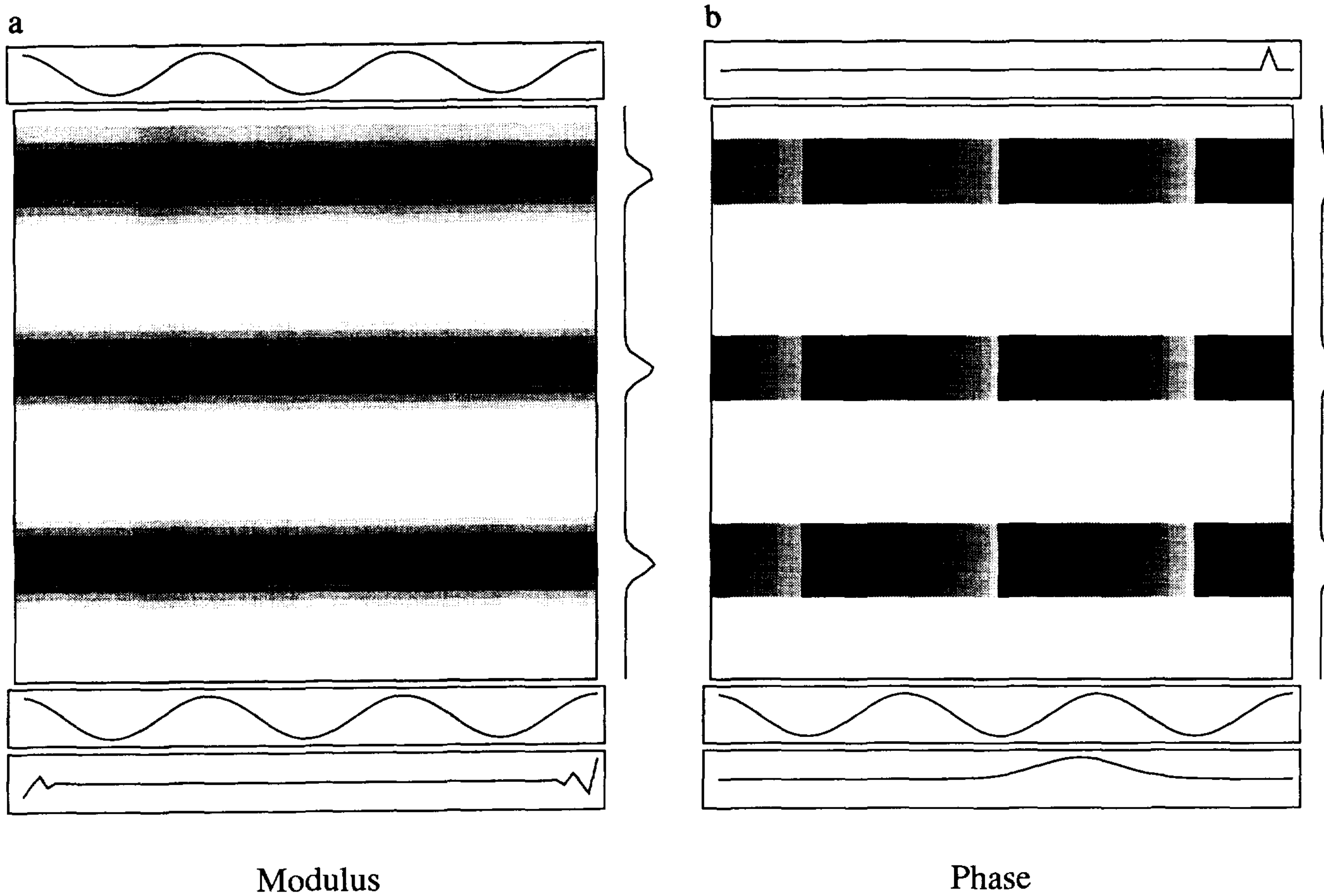

FIG. 2. Sine waves ($p = 71$).

Proof. The first point is that K_a has to commute with translations, i.e., must be a convolution operator. Moreover, we impose on the pseudodilation possesses the composition property of a true dilation, that is to say,

$$\mathscr{D}_{aa'} = \mathscr{D}_a \mathscr{D}_{a'}. \quad (43)$$

For the filters this means that we have to impose

$$F_{aa'} = F_a * D_a F_{a'} \iff \hat{F}_{aa'}(k) = \hat{F}_a(k)\hat{F}_{a'}(ak), \quad (44)$$

which proves the theorem. ■

The filters that satisfy Eq. 44 are called *compatible filters*.

It is also interesting to note that the theorem also holds in the $\ell^2(\mathbb{Z})$ context, i.e., in the case where all products aa' and ak in Equation 44 are products in $\mathbb{Z}$ and not modulo p.

Remarks.

1. It is important to note that the representation of G_p is not unitary, so that it is not possible to use directly the general results of Section 3 to get inversion formulas for the new transform. We come back to this inversion problem later on.
2. Consider for simplicity the case of $\ell^2(\mathbb{Z})$ (the case of $\ell^2(\mathbb{Z}_p)$ is completely similar) and Eq. (44) with only powers of 2 as scale parameters. Then we have

$$\mathscr{D}_{2^j}\psi = F_{2^j} * D_{2^j}\psi = D_{2^{j-1}}F_2 * F_{2^{j-1}} * D_{2^j}\psi, \quad (45)$$

so that the new wavelet transform of a sequence f reads

$$\begin{aligned} T_f(b, 2^j) &= D_{2^j}\tilde{\psi} * (\tilde{F}_{2^j} * f)(b) \\ &= D_{2^j}\tilde{\psi} * (D_{2^{j-1}}\tilde{F}_2 * (\tilde{F}_{2^{j-1}} * f))(b) \end{aligned}$$

(as usual, $\tilde{h}(n) = h(-n)^*$). Then we recover here the same algorithmic structure as the one that appears with multiresolution analysis. The computation of the wavelet coefficients at different scales (here of the form 2^j) can be performed through a pyramidal algorithm involving only (truly) dilated copies of two filters: F_2 (which stands for the low-pass filter) and ψ (band-pass filter). Moreover, since the invoved dilation

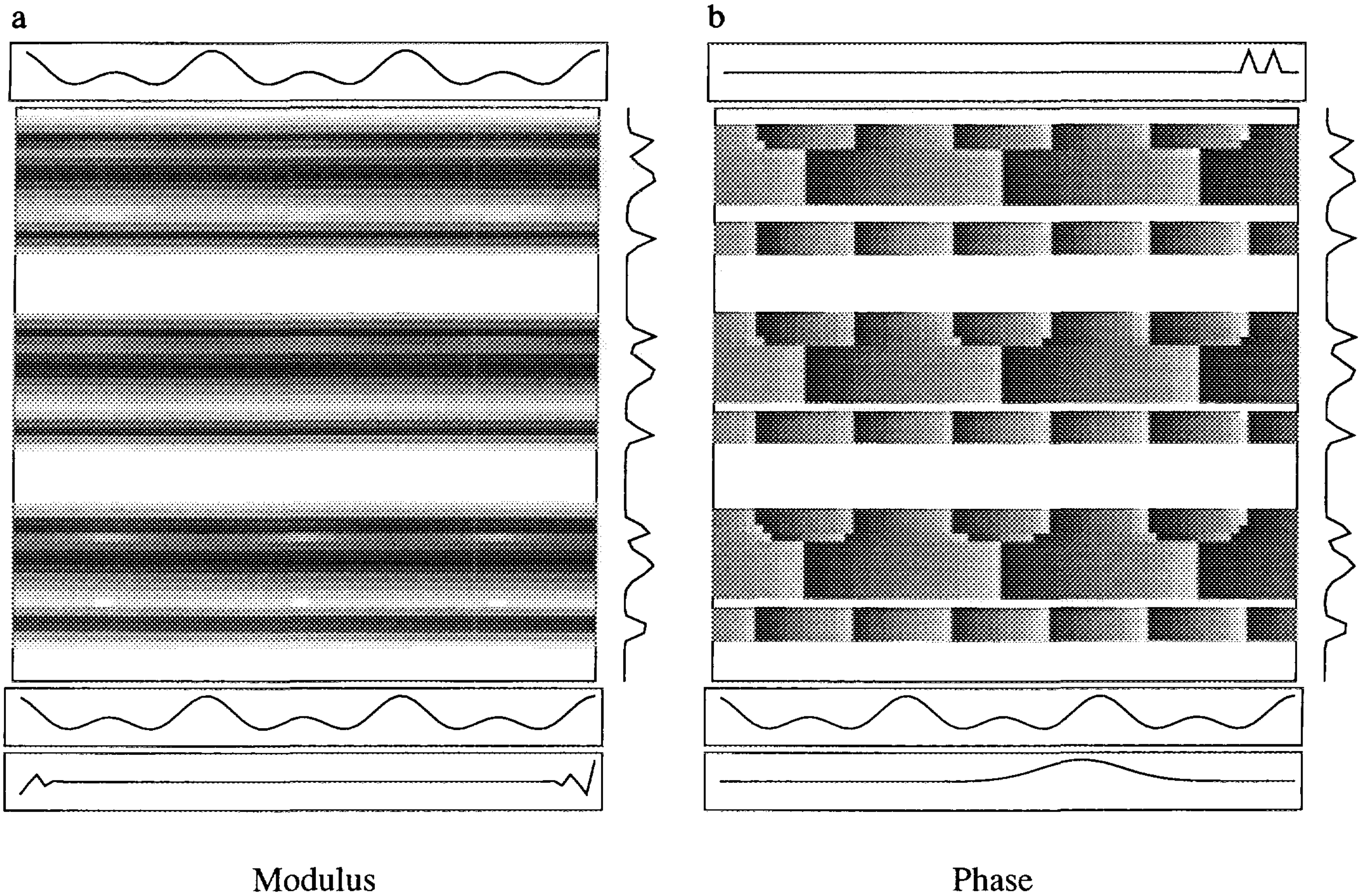

FIG. 3. Superposition of sine waves ($p = 71$).

is the true one (i.e., D_2) and not the pseudo dilation $\mathscr{D}_2$, all such filters are of constant length, so that we still have a "fast" algorithm.

3. The same remark applies for arbitrary scale parameters: assuming that a family of filters satisfying Eq. (44) have been specified, we have

$$T_f(b, aa') = D_{aa'}\tilde{\psi} * (\tilde{F}_{aa'} * f) \quad (46)$$

$$= D_{aa'}\tilde{\psi} * D_a\tilde{F}_{a'} * (\tilde{F}_a * f). \quad (47)$$

Then (assuming the existence of appropriate filters) there exists a pyramidal algorithm for the computation of the transform for arbitrary values of the scale. This generalizes the usual pyramidal algorithms.

4. Now the main question is that of the existence of filters satisfying Eq. (44). The problem may be simplified by using decompositions of integers into prime factors. If F_q is known for any prime q, F_a may be defined for any a by using Eq. (44). The only compatibility equations that remain are the ones involving the F_q with q prime numbers.

5. As a consequence, the only filters used in the algorithm are filters of constant length, dilated copies (with holes) of the F_q filters with prime qs.

5.2. *Existence of appropriate filters*

It turns out that Eqs. (44) are in fact very restrictive, because of the requirement that they must hold for any a and a' in the field of reference. In the case of $\mathbb{Z}_p$ for instance, this amounts to solving $(p-1)^3$ nonlinear equations with $(p-1)^2$ variables. In other words, the F_a filters with different values of a must satisfy some compatibility relations.

The characterization of such filters is a difficult problem (which can actually be identified with a group cohomology problem), and we do not know whether the answer is already known.

Here is a possible strategy for the construction of such filters in the case of $\ell^2(\mathbb{Z})$. We shall see that in some cases it provides explicit examples.

1. Consider a candidate for the dyadic filter F_2 (for example, one of those used in the usual multiresolution analyses).
2. Let (as in the usual multiresolution scheme)

$$\hat{\phi}(k) = \prod_{j=1}^{\infty} \hat{F}_2(2^{-j}k). \tag{48}$$

Under some well known assumptions (see, e.g. , [1]) the infinite product converges to an L^2 function.

3. For $a > 2$ we define the other filters $\hat{F}_a$ as the quotients

$$\hat{F}_a(k) = \mu(a) \frac{\hat{\phi}(ak)}{\hat{\phi}(k)}, \tag{49}$$

where μ is any multiplier of $\mathbb{Z}^*$ (i.e., any function defined on $\mathbb{Z}^*$ such that for any $a, a' \in \mathbb{Z}^*$, $\mu(aa') = \mu(a)\mu(a')$). Clearly, such functions satisfy Eq. (44):

$$\begin{aligned}\hat{F}_{aa'}(k) &= \mu(aa') \frac{\hat{\phi}(aa'k)}{\hat{\phi}(k)} \\ &= \mu(a') \frac{\hat{\phi}(aa'k)}{\hat{\phi}(ak)} \mu(a) \frac{\hat{\phi}(ak)}{\hat{\phi}(k)} \\ &= \hat{F}_{a'}(ak)\hat{F}_a(k).\end{aligned} \tag{50}$$

At this point there still are open questions concerning the possible use of the above defined filters in our scheme. Namely, the $\hat{F}_a$ functions must be 2π-periodic functions. Another important question is that of the length of the filters. We provide examples of compactly supported filters, associated with B-spline scaling functions.

Another question is that of the existence of such filters in the ℓ^2 context. We see that the B-spline type filters also work in the finite case.

5.3. Examples of Filters

There is a simple family of examples for which the above method provides filters satisfying Eq. 44. It is the case of B-spline filters. They correspond to scaling functions $\hat{\phi}$ (see Eq. 48) which are powers of $\sin(\pi k)/\pi k$.

Consider, for instance, the simplest candidate, that is, the filter that interpolates linearly (up to a factor only depending on a),

$$F_a(n) = a\left(\delta_0 + \frac{1}{a}\sum_{q=1}^{a-1}(a-q)(\delta_q + \delta_{-q})\right), \tag{51}$$

where $\delta_q(n) = \delta_{n,q}$. In the Fourier space we have

$$F_a(k) = \frac{\hat{\phi}(ak)}{\hat{\phi}(k)} = \left(\frac{\sin a\pi k/p}{\sin \pi k/p}\right)^2 \tag{52}$$

and it is obvious to check that such filters fulfill the compatibility relations. Thus the only filters appearing in the algorithm are given by

$$\hat{F}_q(k) = \left(\frac{\sin(q\pi k/p)}{\sin(\pi k/p)}\right)^2 \tag{53}$$

and they are all finite length filters.

This example generalizes directly to any even power of $\sin(q\pi k/p)/\sin(\pi k/p)$, yielding B-spline interpolation of various orders. In the case of odd powers, it is necessary to change the formulas slightly, and to consider

$$\hat{F}_q(k) = \left(\frac{1 - e^{2i\pi qk/p}}{1 - e^{2i\pi k/p}}\right)^{2N+1} \tag{54}$$

to keep the compatibility in $\mathbb{Z}_p$.

We do not yet know other examples of compatible filters.

As an illustration, let us give the example of the equivalent of Fig. 1 with the dilation replaced by the pseudodilation. One easily sees that the pseudodilation actually does the job it was introduced for, i.e. it "fills the holes." (See Fig. 4.)

5.4. Reconstruction

As we have seen previously, the pseudodilation does not yield a unitary representation of the affine group G_p, and then it it not possible to use directly the general results on square-integrable representations to get an inversion formula for the new wavelet transform.

Nevertheless, it is still possible to use the freedom given

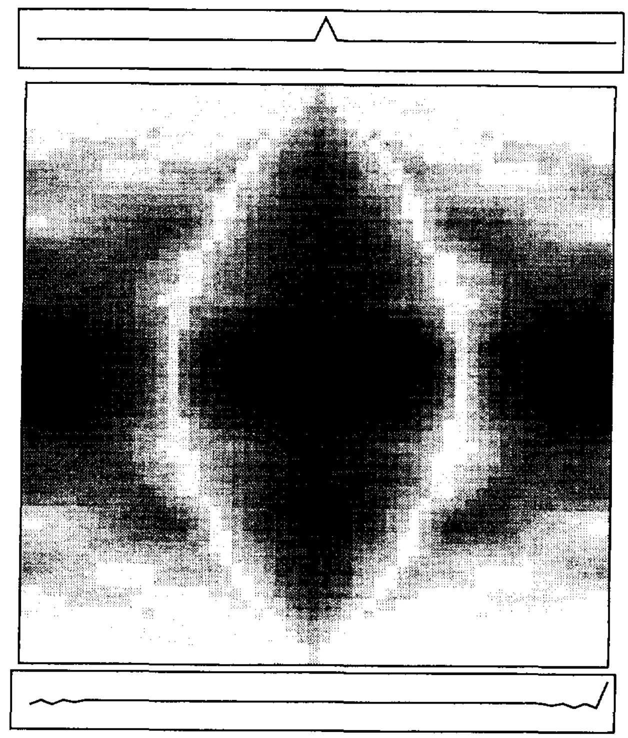

FIG. 4. The modulus of the wavelet transform ($p = 53$).

by the redundancy of the transform, and to look for a reconstruction wavelet χ, so that

$$f = \sum_{b=1}^{p}\sum_{a=1}^{p-1}\langle f, \sigma(b,a)\cdot\psi\rangle\sigma(b,a)\cdot\chi$$
$$= \sum_{b=1}^{p}\sum_{a=1}^{p-1} T_f(b,a)F_a * D_a\chi(n-b). \quad (55)$$

A sequence $\chi(n)$ such that Eq. (55) is fulfilled is called a *reconstruction wavelet*. A direct computation shows that

LEMMA 3. *The function $\chi(n)$ is a reconstruction wavelet if and only if it satisfies*

$$\sum_{a=1}^{p-1} |\hat{F}_a(k)|^2\, \hat{\psi}(ak)^*\hat{\chi}(ak) = 1 \;\; \forall k = 1, \ldots p-1. \quad (56)$$

This condition is equivalent to a matrix equation

$$\begin{pmatrix} |\hat{F}_1(1)|^2 & |\hat{F}_2(1)|^2 & \cdots & |\hat{F}_{p-1}(1)|^2 \\ |\hat{F}_{2^{-1}}(2)|^2 & |\hat{F}_1(2)|^2 & \cdots & |\hat{F}_{2^{-1}(p-1)}(2)|^2 \\ \vdots & \vdots & \ddots & \\ |\hat{F}_{(p-1)^{-1}}(p-1)|^2 & |\hat{F}_{(p-1)^{-1}2}(p-1)|^2 & \cdots & |\hat{F}_1(p-1)|^2 \end{pmatrix}$$
$$\times \begin{pmatrix} \hat{\psi}(1)^*\hat{\chi}(1) \\ \hat{\psi}(2)^*\hat{\chi}(2) \\ \vdots \\ \hat{\psi}(p-1)^*\hat{\chi}(p-1) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

that can at least be solved numerically. Thus, for a given analyzing wavelet and a given family of filters, one can obtain a reconstruction wavelet. It is important to note that since we used the $\sigma(b, a)$ action of G_p, the reconstruction algorithm is also a pyramidal algorithm.

6. CONCLUSIONS

We have developed in this paper a wavelet decomposition formalism adapted to the case of periodic sampled signals (with the assumption that the number of samples is a prime number). The problem was formulated as an algebraic approach to wavelet decompositions of $\ell^2(\mathbb{Z}_p)$, in terms of square-integrable representations of the corresponding affine group.

Surprisingly enough, the study of the possible deformations of the dilation operators (which appears to be unconvenient if the analyzed sequence is to be interpreted as a sampled continuously defined signal) led us to an "algorithmic structure" quite similar to the multiresolution structure, with associated low-pass and band-pass filters. Moreover, we were able to provide explicit examples of such low-pass and band-pass filters, namely some filters associated with B-spline approximations. The problem of classification of all possible such filters amounts to a group cohomology problem.

It is now very likely that a similar analysis (in the case where p is replaced by some power of 2, and the possible scales are also restricted to powers of 2) could (at least partly) fill the gap between the group-theoretic and the Littlewood–Paley approaches to wavelets.

REFERENCES

1. A. Cohen, *"Ondelettes et traitement du signal numérique,"* Thèse de doctorat, CEREMADE, 1991.
2. A. Grossmann, R. Kronland-Martinet, and J. Morlet, *Reading and understanding continuous wavelet transforms, in* "Wavelets: Time–Frequency Methods and Phase Space" (J. M. Combes, A. Grossmann, and Ph. Tchamitchian, Eds.), Inverse Problems and Theoretical Imaging, pp.2–20, Springer, Berlin/New York, 1989.
3. A. Grossmann, J. Morlet, and T. Paul, *Transforms associated to square integrable group representation, J.Math. Phys.* **26**(1985), 2473–2479.
4. E. Hecke, *"Lectures on the Theory of Algebraic Numbers,"* Springer, Berlin/New York, 1981.
5. M. Holschneider, R. Kronland-Martinet, J. Morlet, and Ph. Tchamitchian, *A real-time algorithm for signal analysis with the help of wavelet transform, in* "Wavelets: Time–Frequency Methods and Phase Space" (J. M. Combes, A. Grossmann and Ph. Tchamitchian, Eds.), Inverse Problems and Theoretical Imaging, pp. 286–297, Springer, Berlin/New York, 1989; *The Algorithme à trous*, preprint, Centre de Physique Thèorique, CNRS-Luminy, Marseille, 1988.
6. A. Kirillov, *"Eléments de la Théorie des Représentations,"* Editions Mir, 1974.
7. M. A. Muschietti, and B. Torrésani, *Pyramidal algorithms for Littlewood–Paley decompositions*, preprint CPT-93/P.2910, 1993.
8. T. Paul, *"Ondelettes et mecanique quantique,"* Thèse de Doctorat, Faculté de Sciences de Luminy, CPT-85/P.1841.