THEORY OF WAVELET TRANSFORM OVER FINITE FIELDS

F. Fekri, R. M. Mersereau, R. W. Schafer

Center for Signal & Image Processing
Georgia Institute of Technology
Atlanta, GA 30332

ABSTRACT

In this paper, we develop the theory of the wavelet transform over Galois fields. To avoid the limitations inherent in the number theoretic Fourier transform over finite fields, our wavelet transform relies on a basis decomposition in the time domain rather than in the frequency domain. First, we characterize the infinite dimensional vector spaces for which an orthonormal basis expansion of any sequence in the space can be obtained using a symmetric bilinear form. Then, by employing a symmetric, non-degenerate, canonical bilinear form we derive the necessary and sufficient condition that basis functions over finite fields must satisfy in order to construct an orthogonal wavelet transform. Finally, we give a design methodology to generate the mother wavelet and scaling function over Galois fields by relating the wavelet transform to a two channel paraunitary filter bank. Online relevant information can be found at http://www.ee.gatech.edu/users/fekri.

1. INTRODUCTION

Filter banks, and the wavelet transform have established themselves as powerful tools in the analysis of signals and images when these objects are viewed as sequences over real or complex fields. Recently, the extension of the wavelet transform to the situation in which the complex field is replaced with a finite field has become of interest. In [1] the authors show that unlike the real field case, there is no complete factorization technique for paraunitary FB over $GF(p)$, for p a prime. Relying on the Fourier transform defined over $GF(p^r)$, the authors of [2] construct a wavelet transform for finite dimensional sequences (periodic sequences of period 2^n) over fields with a characteristic other than 2, $p \neq 2$. An extensive review of finite field transforms can be found in [3]. Wavelets and filter banks over finite fields have potential applications in the cryptography, spread-signature CDMA systems, the theory of error correction codes [4], biosequence analysis [2], and the coding or analysis of halftone images [5]. While these applications need more investigations, this paper studies the theory of the wavelet transform of infinite dimensional sequences defined over any finite field $GF(p^r)$. Since we do not require the existence of the number theoretic Fourier transform [6], our formulation becomes more attractive particularly for the fields with characteristic 2, $GF(2^r)$.

Throughout this paper, all arithmetic is carried out in the finite field. If the field is $GF(p)$, p a prime, then addition and multiplication are defined modulo-p. In the fields of the form $GF(p^r)$, $r > 1$, a number a is represented by a polynomial $S^a(y)$ of degree $r-1$ where the coefficients lie in $GF(p)$. Then, addition is defined as addition of polynomials in $GF(p)$, and multiplication is defined to be polynomial multiplication modulo a fixed polynomial $q(y)$. The polynomial $q(y)$ is a monic irreducible polynomial of degree r over $GF(p)$ [7]. To simplify the notation, we will represent the numbers in $GF(p^r)$ by alphabetic variables instead of by their polynomial representations.

2. FINITE FIELD DISCRETE TIME BASIS

2.1. Non-degenerate Bilinear Form

Let v be a vector space over the finite field $\mathcal{F}$ with addition and multiplication defined on $\mathcal{F}$. We would like to construct the set of orthonormal basis functions $\{\theta_k(n)\}_{k\in\mathcal{Z}}$ such that any arbitrary sequence $x(n)$ in v can be written as:

$$x(n) = \sum_{k\in\mathcal{Z}} \langle \theta_k(n), x(n) \rangle \theta_k(n). \tag{1}$$

The proper characteristics of the vector space v that allows us to do this expansion will be discussed later in this paper. The problem with this expansion is that the space v is not an inner product space, because the positive definite property does not hold. For example, a sequence $s(n)$ in $GF(2)$ that contains an even number of ones is orthogonal to itself , $\langle s(n), s(n) \rangle = 0$.

To resolve this dilemma we employ the symmetric bilinear form that is defined for two vectors X and Y as:

$$\langle X, Y \rangle = X^T A Y,$$

where A is a symmetric matrix associated with the basis set for the space. One can verify that, like the inner product, the bilinear form has the bilinearity and symmetry properties. However, it allows for a nonzero sequence to be self-orthogonal. Furthermore, to implement the finite field wavelet transform using a filter bank, we use the canonical bilinear form (also known as the canonical inner product [8]). It can be shown that every bilinear form can be written as a canonical form. The canonical bilinear form of two sequences $a(n)$ and $b(n)$ is given by:

$$\langle a, b \rangle = \sum_i a(i) b(i), \tag{2}$$

where the arithmetics is carried out in the finite field $\mathcal{F}$.

Definition: With the canonical bilinear form defined in (2), a set $B = \{\theta_k(n)\}_{k\in\mathcal{Z}}$ is called an orthogonal basis for the space v if they satisfy $\langle\theta_i, \theta_j\rangle = 0$ for $i \neq j$ and $\{\theta_k(n)\}_{k\in\mathcal{Z}}$ is a spanning set for the space v.

This definition allows that some of the basis functions to be self-orthogonal. Note that the set B is an orthonormal basis, if every θ_m that is not self-orthogonal satisfies $\langle\theta_m, \theta_m\rangle = 1$. We need to borrow two definitions from abstract algebra: the null space of a canonical bilinear form and the non-degenerate form. For the given canonical bilinear form, a vector $w \in v$ is called a null vector if $\langle w, u\rangle = 0$ for all $u \in v$. Therefore, the null space of the canonical bilinear form is defined by:

$$N_v = \{w \in v \ : \ \langle w, u\rangle = 0 \quad \forall\ u \in v\}.$$

A canonical bilinear form is said to be non-degenerate if its null space is $\{0\}$.

Theorem 1 [9]: Suppose that the set of discrete functions $\{\theta_k(n)\}_{k\in\mathcal{Z}}$ is an orthogonal basis for the vector space v. Then, the canonical bilinear form associated with this basis set is non-degenerate if and only if $\langle\theta_k, \theta_k\rangle \neq 0 \ \ \forall k \in \mathcal{Z}$.

Remark 1: Theorem 1 establishes the fact that the mother wavelet and the scaling function in the wavelet decomposition of the space v cannot be self-orthogonal sequences. This will be discussed later.

The theory of multiresolution analysis for discrete time signals over real or complex fields has been developed in [10], and for periodic signals in [2]. To develop a wavelet transform over finite fields we need only to give a formulation of the wavelet decomposition of the space v onto two orthogonal subspaces V_0 and W_0. Then, for the multiresolution analysis of the space v, we repeat this decomposition on V_0 similar to the idea developed in [10]. Our wavelet transform formulation relies on the basis decomposition in the time domain rather than in the frequency domain. This is mainly because the number theoretic Fourier transform may not exist in the given finite field [6]. The existence of the number theoretic DFT requires the existence of an element of order L (assuming the signal length to be L) over $GF(p^r)$. This requires that L divides $p^r - 1$ which is a strong restriction.

2.2. Orthonormal Wavelet Basis Over Finite Fields

In this section we derive the formulation of the wavelet decomposition of a space v into the direct sum of two orthogonal subspaces V_0 and W_0 as $v = V_0 \oplus W_0$. Proposition 1 characterizes the properties of the canonical bilinear form over the subspaces V_0 and W_0.

Proposition 1 [9]: Suppose two subspaces V_0 and W_0 are orthogonal complements of each other. Then $V_0 \cap W_0 = \{0\}$ if and only if the canonical bilinear form is non-degenerate on both V_0 and W_0.

From Proposition 1, we conclude that in the orthogonal wavelet decomposition of the space v as the direct sum of two subspaces, the canonical bilinear form must stay non-degenerate on V_0 and W_0. This results in Fact 1 immediately:

Fact 1: For a successful orthogonal wavelet decomposition of the vector space v over finite field $\mathcal{F}$, the canonical bilinear form must be non-degenerate over v.

From now on, we will refer to v as a non-degenerate vector space over a finite field without mentioning the underlying bilinear form. The scaling function $\varphi(n)$ and the mother wavelet $\psi(n)$ defined over the finite field $\mathcal{F}$ construct a wavelet transform if they satisfy:

$$\begin{array}{ll} V_0 = \overline{span\{\varphi(n-2j)\}} & j \in \mathcal{Z} \\ W_0 = \overline{span\{\psi(n-2j)\}} & j \in \mathcal{Z} \end{array} \tag{3}$$

and they should meet the following conditions:

$$\begin{array}{ll} \langle\varphi(n-2k), \varphi(n-2l)\rangle = 0 & \forall\ l \neq k \\ \langle\psi(n-2k), \psi(n-2l)\rangle = 0 & \forall\ l \neq k \\ \langle\varphi(n-2k), \psi(n-2l)\rangle = 0 & \forall\ l, k. \end{array} \tag{4}$$

Furthermore, since the two subspaces V_0 and W_0 are non-degenerate spaces, as a result of Theorem 1 the following conditions must be satisfied as well (note that the Theorem only requires a nonzero value, but we further normalize the sequences):

$$\begin{array}{l} \langle\varphi(n), \varphi(n)\rangle = 1 \\ \langle\psi(n), \psi(n)\rangle = 1. \end{array} \tag{5}$$

It is worth noting that the result of the bilinear forms in (5) can be zero in other forms (eg., biorthogonal wavelet transform) of wavelet transform over finite fields.

2.3. Completeness of the Orthonormal Set

The interesting question is whether the functions $\varphi(n)$ and $\psi(n)$ that satisfy the quadratic equations (4) and (5) construct an orthonormal basis set for the space v or not. In other words, given the solution of the quadratic equations, is it possible to write any arbitrary sequence in the non-degenerate space v as:

$$\begin{aligned} x(n) = &\sum_{j\in\mathcal{Z}} \langle\varphi(n-2j), x(n)\rangle\varphi(n-2j) \\ &+ \sum_{j\in\mathcal{Z}} \langle\psi(n-2j), x(n)\rangle\psi(n-2j)? \end{aligned} \tag{6}$$

The problem is that the vector space v defined over a finite field with the canonical bilinear form is not a normed vector space. Consequently, ℓ_2-norm convergence does not apply to the infinite sum (6) on v unlike the case where the wavelets are defined over the real field. In the next section we show that the infinite sum in (6) converges componentwise to $x(n)$. Using an equivalent condition, we show that $\varphi(n)$ and $\psi(n)$ that satisfy (4) and (5) construct a complete spanning set, $\{\varphi(n-2k)\}_{k\in\mathcal{Z}} \cup \{\psi(n-2k)\}_{k\in\mathcal{Z}}$, over the non-degenerate space v.

The discrete wavelet transform (DWT) and its inverse (IDWT) are easily recognized as the analysis and synthesis banks of the two band filter banks (in Fig. 1), respectively. By choosing $h_0(n) = \varphi(-n)$ and $h_1(n) = \psi(-n)$, we easily observe that:

$$\begin{array}{l} y_0(n) = \langle x(m), \varphi(m-2n)\rangle \\ y_1(n) = \langle x(m), \psi(m-2n)\rangle. \end{array}$$

The synthesis bank that consists of synthesis filters $g_0(n) = \varphi(n)$ and $g_1(n) = \psi(n)$ constructs an approximation of $x(n)$ (IDWT) by computing (6). Therefore, the solutions of the

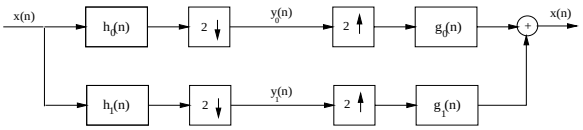

Figure 1: Diagram of the two band filter bank.

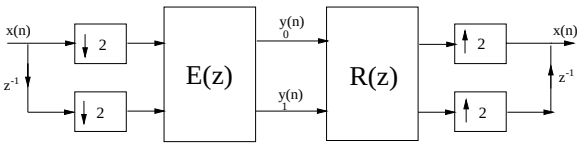

Figure 2: Polyphase representation of two band filter bank.

quadratic equations (4) and (5) construct a complete orthonormal basis for the non-degenerate space v, if and only if the associated filter bank is an orthogonal perfect reconstruction filter bank.

3. DESIGN METHODOLOGY

In our construction, we represent every sequence $x(n)$ by a polynomial in a polynomial ring $\mathcal{F}(z)$ over the field $\mathcal{F}$ as: $X(z) = \sum x(n)z^{-n}$ where z^{-1} is an undetermined variable. Then the polynomial representation of the convolution of two sequences $x(n)$ and $h(n)$ can be written as $X(z)H(z)$ in which the arithmetic is done over the field $\mathcal{F}$. Using this polynomial representation, we can represent the filter bank in Fig. 1 with its polyphase components as Fig. 2.

Like the real field case, we can easily verify that in any finite field the scaling function and the mother wavelet of the orthogonal wavelet transform have even length [9]. Consequently the filters are of odd orders. Now, suppose that $H_s(z)$, $s = 0, 1$, has order $2N + 1$ with its polyphase components as $E_{s0}(z)$ and $E_{s1}(z)$. Using the polyphase representation for a 2-band orthogonal filter bank, we write the polyphase components of $H_1(z)$ in terms of the polyphase components of $H_0(z)$ as [9]:

$$E_{10}(z) = z^{-N}E_{01}(z^{-1}) \quad , \quad E_{11}(z) = -z^{-N}E_{00}(z^{-1}). \quad (7)$$

In a perfect reconstruction orthogonal filter bank, the polyphase matrix $E(z) = [E_{si}(z)]$, $0 \le s, i \le 1$ must satisfy the paraunitary constraint $E^T(z^{-1})E(z) = I$. Therefore, the necessary and sufficient condition for an orthogonal perfect reconstruction filter bank is obtained as:

$$E_{00}(z)E_{00}(z^{-1}) + E_{01}(z)E_{01}(z^{-1}) = 1. \quad (8)$$

Here, $E_{00}(z)$ and $E_{01}(z)$ are polynomials in the polynomial ring $\mathcal{F}(z)$ defined as:

$$E_{00}(z) = \sum_{i=0}^{M} e_{0i}z^{-i}, \quad e_{00} \neq 0 \quad , \quad e_{0i} \in GF(p^r)$$

$$E_{01}(z) = \sum_{i=0}^{N} e_{1i}z^{-i}, \quad e_{1N} \neq 0 \quad , \quad e_{1i} \in GF(p^r)$$

where M is a positive integer satisfying $M \le N$.

In (8), we do not require any additional constraints on the polyphase components of $H_0(z)$. The properties of the filters in filter banks over finite fields (equivalently, the characteristic of the two subspaces V_0 and W_0) will be determined by the applications that these new wavelet transforms are formed for. From (8) we conclude that:

$$e_{1i} = 0 \quad i = 0, \ldots, N - M - 1. \quad (9)$$

Moreover, with some manipulation we can show that (8) is equivalent to:

$$A(z)A^c(z) + B(z)B^c(z) = z^M \quad (10)$$

where $A(z)$ and $B(z)$ are polynomials in $\mathcal{F}(z)$ defined as:

$$A(z) = \sum_{i=0}^{M} a_i z^i, \quad a_0 \neq 0 \quad , \quad B(z) = \sum_{i=0}^{M} b_i z^i, \quad b_M \neq 0. \quad (11)$$

In our notation, the superscript "c" means the reciprocal of the polynomial. The reciprocal polynomial of $G(z)$ of degree M is defined as $G^c(z) = z^M G(z^{-1})$. The coefficients of two polynomials $A(z)$ and $B(z)$ are related to those of the polyphase components $E_{00}(z)$ and $E_{01}(z)$ by:

$$a_i = e_{0i} \quad , \quad b_i = e_{1(N-M+i)} \quad for \quad i = 0, \ldots, M. \quad (12)$$

In the following, we give a general procedure to construct a 2-band orthogonal perfect reconstruction filter bank over $GF(p^r)$. Assume that the desired filter order is $2N+1$.

- Set $M = 1$
- Find every pair of polynomials $A(z)$ and $B(z)$ over the polynomial ring $\mathcal{F}(z)$ that satisfy (10). Each pair of polynomials specifies the filters of the filter bank by (9) and (12).
- Increment M by one and repeat the previous step as long as $M \le N$.

The above procedure generates all possible orthogonal perfect reconstruction filter banks. Therefore, in this full search method we start with $A(z)$ and apply an appropriate method such as Berlekamp's algorithm to factorize $z^M - A(z)A^c(z)$ over the field $\mathcal{F}$ [7]. As an alternative to the full search method using polynomial factorization algorithms, we also provide a method to find the majority of the possible solutions for the fields with characteristic 2 (i.e, $GF(2^r)$). It is worth noting that if the pair $\{A(z), B(z)\}$ constructs an orthogonal perfect reconstruction filter bank, then each of the pairs $\{A^c(z), B(z)\}$, $\{A(z), B^c(z)\}$, $\{A^c(z), B^c(z)\}$, $\{B(z), A(z)\}$,$\{B^c(z), A(z)\}$, $\{B(z), A^c(z)\}$ and $\{B^c(z), A^c(z)\}$ is a solution as well. However, those pairs may or may not generate distinct pairs of filters $H_0(z)$ and $H_1(z)$.

Example 1: Let us derive all the orthogonal filter banks of the lowest nontrivial order, 3, over $GF(5)$. It can be justified that the only solution pair for (10) is $A(z) = 2+2z$ and $B(z) = 3 + 2z$ that constructs four distinct orthogonal perfect reconstruction filter banks. For one set of solutions, the filters of the analysis bank are:

$$\begin{cases} H_0(z) = 2 + 3z^{-1} + 2z^{-2} + 2z^{-3} \\ H_1(z) = 2 + 3z^{-1} + 3z^{-2} + 3z^{-3}. \end{cases}$$

Table 1: ALL ORTHOGONAL PERFECT RECONSTRUCTION FB OVER $GF(2)$ UP TO ORDER ELEVEN.

M	Order	$H_0(z)$	$H_1(z)$
2	5	37	3B
2	7	9D	B9
2	9	235	2B1
4	9	3EF	3DF
4	9	323	313
2	11	895	A91
4	11	989	919
4	11	BED	B7D
5	11	DE7	E7B
5	11	DB7	EDB

3.1. 2-Band Orthogonal Filter Banks Over $GF(2^r)$

Fields with characteristic 2 have the property that $2k = 0$ for any k in $GF(2^r)$. This property enables us to obtain the symmetric solutions of (10), as we explain later.

Example 2: Let us determine all the orthogonal filter banks of the lowest nontrivial order, 3, over $GF(2^r)$. Without loss of generality, we can consider $H_0(z)$ as a monic polynomial, and consequently $B(z)$ is a monic polynomial of degree one. It can be verified that the general solution for (10) is:

$$\begin{cases} A(z) = a(1+a)^{-1} + az \\ B(z) = a^2(1+a)^{-1} + z \end{cases} \qquad a \neq 1 \quad , \quad a \in GF(2^r).$$

Using this solution, we can construct the orthogonal filter bank of order 3 over $GF(2^3)$. In order to construct the extension field $GF(2^3)$, let us choose the primitive polynomial $q(y) = 1 + y + y^3$ as an irreducible polynomial over $GF(2)$. Then, by arbitrarily choosing $a = 2$ (the polynomial representation of this number in the extension field is $a = y$), the filters are specified as:

$$\begin{cases} H_0(z) = 7 + 5z^{-1} + 2z^{-2} + z^{-3} \\ H_1(z) = 1 + 2z^{-1} + 5z^{-2} + 7z^{-3}. \end{cases}$$

In the field $GF(2^r)$ we can rewrite (10) as $A(z)A^c(z) + z^M = B(z)B^c(z)$ and we look for the pair of polynomials of the form (11) satisfying this equation for any $M \leq N$. In fields with characteristic 2, whenever M is an even number, the above equation can be written as:

$$\{A(z) + z^{M/2}\}\{A(z) + z^{M/2}\}^c = B(z)B^c(z)$$

provided that $A(z)$ is a symmetric polynomial, $A(z) = A^c(z)$. Obviously in this case any $B(z)$ equal to $A(z) + z^{M/2}$ is also a symmetric polynomial.

Fact 2: If M is an even number, the polynomial pair $A(z)$ and $A(z) + z^{M/2}$ is a solution to (10) over $GF(2^r)$, Where $A(z)$ is any arbitrary symmetric polynomial of degree M with a nonzero constant coefficient.

Table 1 gives all the possible distinct orthogonal perfect reconstruction filter banks up to order eleven over $GF(2)$. The first column of Table 1 lists the values of M for which a solution for (10) can be obtained. The second, third and and fourth columns show the filter order, the coefficients of $H_0(z)$ and $H_1(z)$, respectively. Note that the filter coefficients are represented in Hexadecimal (by padding sufficient zeroes to the left) form with the LSB bit as the coefficient of the highest degree. We include the nonsymmetric solutions in this Table as well. It can be verified that there exist some solutions only for $M = 5$.

4. CONCLUSION

In this paper, we have studied the theory of the wavelet transform of discrete-time signals in non-degenerate vector spaces. The conditions that the scaling function and the mother wavelet should meet were described. Furthermore, we present a design methodology for orthogonal two channel filter banks over finite fields. In particular, we pointed out a method to construct these filter banks over the fields with characteristic 2. The low complexity of the finite field wavelet transform makes it a promising tool for communication and signal processing applications.

5. REFERENCES

[1] S. Phoong and P. P. Vaidyanathan, "Paraunitary filter banks over finite fields," *IEEE Trans. Signal Proc.*, vol. 45, pp. 1443–1457, June 1997.

[2] G. Caire, R. L. Grossman, and H. V. Poor, "Wavelet transforms associated with finite cyclic groups," *IEEE Trans. on Information Theory*, vol. 39, July 1993.

[3] F. Fekri, *Transform Representation of Finite Field Signals.* A qualifying examination report available at http://www.ee.gatech.edu/users/fekri, Georgia Institute of Technology, June 1998.

[4] H. V. Poor, "Finite field wavelet transform," in *Information Theory and Applications II, 4th Canadian workshop*, pp. 225–238, Lac Delage, Que., Canada, 1996.

[5] M. D. Swanson and A. H. Tewfik, "A binary wavelet decomposition of binary images," *IEEE Trans. Image Processing*, vol. 5, pp. 1637–1650, Dec. 1996.

[6] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing.* Englewood Cliffs, NJ:Prentice-Hall, 1979.

[7] R. Lidi and H. Niederreiter, *Finite Fields.* Addison-Wesley Publishing Company, 1983.

[8] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer-Verlag, 1993.

[9] F. Fekri, R. M. Mersereau, and R. W. Schafer, "Theory of wavelet transform over finite fields," *to be submitted to IEEE Trans. Signal Proc.*

[10] O. Rioul, "A discrete-time multiresolution theory," *IEEE Trans. Signal Proc.*, vol. 41, pp. 2591–2606, August 1993.