DECODING OF HALF-RATE WAVELET CODES; GOLAY CODE AND MORE

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

Center for Signal & Image Processing
Georgia Institute of Technology, Atlanta, GA 30332-0250
email: fekri@ee.gatech.edu , Tel: (404)894-8361

ABSTRACT

The primary goal of this paper is to give examples of the recently developed (finite-field) wavelet coding method by studying the encoder and decoder for some half-rate codes. We propose a decoding methodology based on estimating the polyphase components of the channel error pattern. To demonstrate the striking computational savings of the wavelet coding method over alternatives, we show that bounded-distance decoding of the (24,12,8) Golay code requires only weight computations (or at the worst case, it needs a cyclic lookup table of table size 12). The simplicity and computational savings that finite field wavelets offer for the encoding and decoding of wavelet block codes indicate their powerful capacities for error control coding applications.

1. INTRODUCTION

Recently, wavelet decompositions have been extended to signals that can be considered as sequences defined over finite fields, in particular, fields of characteristic two [1, 2]. The notion of performing error control coding using wavelet has evolved from our earlier studies of self-dual codes [3]. Later, we established a new framework to study block codes [4, 5] as well as convolutional codes [6]. Inspired by [3], in this paper we generalize the wavelet decoding strategy to correct multiple errors. To accomplish this, a method is proposed to remove the interference terms from the estimates of the polyphase components of the error pattern. As examples, we will give descriptions of the decoders for a (20,10,6) and Golay code. More in-depth study of half-rate wavelet codes can be found in [4].

1.1. Notations and Definitions

We use the following notation and definitions:

- The letters N, M and d are reserved for the code-length, message-length, and minimum distance, respectively.
- We reserve $\mathbf{F}[z^{-1}]$ to represent polynomial rings in z^{-1} over the field $\mathbf{F}$. We also use uppercase and lowercase letters with arguments (z) for polynomials in $\mathbf{F}[z^{-1}]$.
- $\mathbf{F}[z^{-1}]/(z^{-M}-1)$ designates the ring of polynomials of degree less than M in which the rules of polynomial addition and multiplication hold, except that polynomial multiplication is performed $\mathrm{mod}(z^{-M}-1)$.
- The upper and lower case Italic letters correspond to matrices and vectors, respectively.
- Let $a(z)=a_0+a_1z^{-1}+\cdots+a_{M-1}z^{-(M-1)}$ be a polynomial in $\mathbf{F}[z^{-1}]/(z^{-M}-1)$ defined by the vector of coefficients $a=[a_0,\ldots,a_{M-1}]$. We call $a^R=[a_0,a_{M-1},\ldots,a_1]$ the circular-reciprocal of the vector a, and the polynomial $a^R(z)$ the circular-reciprocal of $a(z)$.
- We define a cyclic LTI system as a linear time invariant (LTI) filter where the operation of linear convolution is replaced by circular convolution. This means that all of the time indices in a cyclic LTI systems are interpreted as modulo some number. Throughout the paper, we denote $((\cdot))_N$ for a modulo-N operation, or equivalently an N-point circular shift.
- We use q-circ(b) to represent q-circulant matrices. A q-circulant matrix is defined by its first row b. The ith row is equal to the left-to-right cyclic shift of the vector b by $(i-1)q$.
- Consider two finite sequences $x=[x_0,\ldots,x_{M-1}]^T$, $h=[h_0,\ldots,h_{M-1}]$ and define $y(n)=h(n)*x(n)$ as their circular convolution. Then we write the circular convolution in a matrix form $y=Hx$ in which $H=$ 1-circ(h^R).

2. STRUCTURE OF DOUBLE CIRCULANT WAVELET CODES

In the study of block codes, we will frequently exploit the isomorphism between the algebra of $M\times M$ one-circulant matrices over the field $\mathbf{F}$ and the algebra of polynomials in the ring $\mathbf{F}[z^{-1}]/(z^{-M}-1)$ [7]. In other words, the addition and multiplication of two polynomials in $\mathbf{F}[z^{-1}]/(z^{-M}-1)$ are equivalent to the addition and multiplication of their corresponding circulant matrices, respectively. In the following, we first give a formulation of cyclic filter banks in which all the filters, interpolators and decimators are cyclic.

2.1. Cyclic Wavelet Transforms over the Field F

It is well known that wavelet decomposition and reconstruction can be implemented as the analysis and synthesis components of a perfect reconstruction filter bank, respectively. Figure 1 shows the analysis and synthesis banks of a two-channel perfect reconstruction filter bank in which the synthesis filters $g_0(n)$ and $g_1(n)$ are the scaling sequence and mother wavelet, respectively. In [1] the authors show how to decompose a vector space V over a finite-field $\mathbf{F}$ onto two orthogonal subspaces. In particular, a design methodology is presented in [1] and [2] to obtain the analysis and synthesis filters over the fields of characteristic 2, $GF(2^r)$, that results in a two-channel perfect-reconstruction orthogonal filter bank.

Since the codewords of half-rate block codes have finite even length, the vector space $\mathcal{V}$ is considered to be a vector space of finite dimension $N=2M$. It can also be regarded as a space of periodic sequences of period N. Next, we characterize the two-channel cyclic multirate systems that are used in the construction of half-rate codes. Consider a two-channel perfect reconstruction filter bank with the scaling sequence $g_0(n)=\{g_0(0),g_0(1),\cdots,g_0(N-1)\}$ and the mother wavelet $g_1(n)=\{g_1(0),g_1(1),\cdots,g_1(N-1)\}$. In the analysis bank of Fig. 1, the operation of filtering

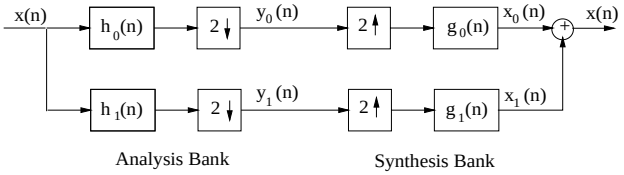

Fig. 1. Diagram of the two-band filter bank

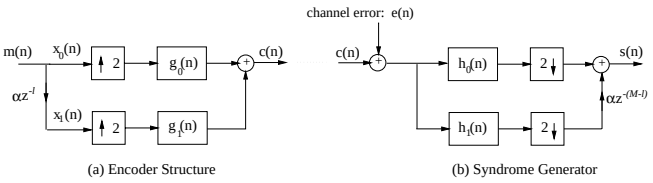

Fig. 2. Filter bank structure of the half-rate encoder and syndrome generator

periodic signals followed by decimation by a factor of two can be described using 2-circulant matrices

$$\begin{aligned} y_0(n) &= \textstyle\sum_{i=0}^{N-1} x(i)h_0((2n-i))_N = (H_0x)(n) \\ y_1(n) &= \textstyle\sum_{i=0}^{N-1} x(i)h_1((2n-i))_N = (H_1x)(n), \end{aligned} \tag{1}$$

in which $H_0 = 2\text{-circ}(h_0^R)$ and $H_1 = 2\text{-circ}(h_1^R)$ are 2-circulant matrices defined by the analysis filters $h_0(n)$ and $h_1(n)$.

Similarly, in the synthesis bank, the upsampling of periodic signals by a factor of two followed by the filtering operation can be described by (column-wise) 2-circulant matrices $G_0 = [2\text{-circ}(g_0)]^T$ and $G_1 = [2\text{-circ}(g_1)]^T$:

$$\begin{aligned} x(n) &= \sum_{i=0}^{M-1} y_0(i)g_0((n-2i))_N + \sum_{i=0}^{M-1} y_1(i)g_1((n-2i))_N \\ &= (G_0y_0)(n) + (G_1y_1)(n). \end{aligned} \tag{2}$$

The above formulation holds for the general class of two-channel cyclic filter banks. The properties of H_i and G_j and their relation to each other were discussed in [5]

2.2. Structure of Encoder and Syndrome Generator

Figure 2a shows the encoder for the (N, M, d) wavelet-code over a finite field $\mathbf{F}$. The encoder is realized by the synthesis portion of the two-band filter bank in which $g_o(n)$ and $g_1(n)$ are an orthonormal wavelet basis of length N over $\mathbf{F}$. According to Fig. 2a, the encoder takes a message block $m(n)$ of size $M = N/2$ and maps it to the codeword $c(n)$ (of size N) by expanding it by a factor of two through the interpolator.

Fact 1 *The following holds in the encoder of Fig. 2a.*

- *The (N, M, d) wavelet code is a linear code. This can be verified by the linearity and invertibility of the wavelet transform.*
- *The code is double circulant. The double circulant property requires that if $c(n) = \{c(0), c(1), \ldots, c(N-1)\}$ is a codeword, then $c((n-2))_N$ is also a codeword. To prove this, let $c(n)$ be a codeword associated with the message $m(n)$, then by the property of the multirate filters, there exists a message datum $m((n-1))_M$ that is mapped to the codeword $c((n-2))_N$.*
- *It can be shown that $G = G_0 + G_1$ is the generator matrix for the wavelet-code (i.e., $c = Gm$) in which the two matrices G_0 and G_1 are obtained by (**??**).*

In the following we show that the structure in Fig. 2.b constructs the syndrome of the code. We write:

$$s = (H_0 + H_1)(c + e), \tag{3}$$

in which e is the error pattern due to the communication channel. Using the equality $c = (G_0 + G_1)m$ and the relations that we developed for cyclic orthogonal filter banks, it can be verified that:

$$s = (H_0 + H_1)e. \tag{4}$$

Therefore, the output of the system in Fig. 2b depends only on the error pattern.

It is worth noting that both the encoder and syndrome generator in Fig. 2 can be implemented by a polyphase structure efficiently [5].

3. DECODING WAVELET CODES

In [3], the authors gave a full description of the complete-decoder for the (12,6,4) binary self-dual code. Here, we show that the strategy for decoding wavelet codes (that correct more than one bit error in a block) is very similar to that of the (12,6,4) code (that corrects one bit error). First we give a bounded-distance decoder for a (20,10,6) code (not a self-dual code). Then, we describe bounded-decoding of the (24,12,8) wavelet-Golay code.

3.1. Bounded-Distance Decoding of (20,10,6) Double Circulant Wavelet Code

It can be verified that the (20,10,6) code can be constructed by the wavelet-encoder of Fig. 2a by choosing the scaling function $g_0(n) = \{88015\}$ and the mother wavelet $g_1(n) = \{FBB9E\}$ (The filter coefficients result by converting the Hexadecimal numbers to binary). Note that $g_0(n)$ and $g_1(n)$ construct a cyclic biorthogonal filter bank whose relationship to the analysis bank filters has been discussed in [4].

As shown in Fig. 3 , the syndrome of the error can be generated by filtering followed by decimation by a factor of two in which the filter coefficients are $h(n) = \{B9DC5\}$ [5]. The polyphase components of $H(z)$ are $u_{00}(n)$ and $u_{01}(n)$. The remaining problem is to interpolate the low (M) dimensional syndrome $s(n)$ into the higher (N) dimensional error pattern $e(n)$. Since more than one error pattern is mapped into the same low dimensional syndrome, the interpolator should choose (out of those possible valid choices) the error pattern that is most likely (has minimum weight) to achieve the maximum likelihood ML decoder performance.

We build a bounded-distance decoder that is guaranteed to correct all errors of weight one and two. Our approach to design the decoder is based on inverting the polyphase filters $u_{00}(n) = h(2n)$ and $u_{01}(n) = h(2n+1)$ of the syndrome generator filter $h(n)$. Let $r_{00}(n)$ and $r_{01}(n)$ be two filters with the z-transform in $\mathbf{F}[z^{-1}]/(z^{-M} - 1)$ satisfying:

$$R_{0i}(z)U_{0i}(z) = 1 \mod (z^{-M} - 1) \qquad i = 0, 1. \tag{5}$$

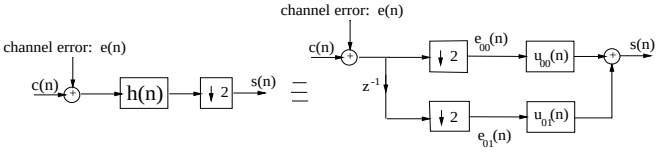

Fig. 3. Polyphase representation of the syndrome generator

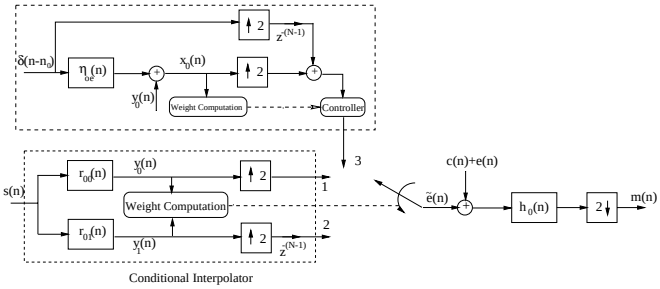

Fig. 4. Decoder of the double circulant (20,10,6) code that reconstructs the message sequence from the syndrome.

In other words, these two filters are the circular inverses of $u_{00}(n)$ and $u_{01}(n)$, respectively. For the (20,10,6) code we have:

$$\begin{aligned} r_{00}(n) &= \{1,0,0,0,0,1,0,1,1,1\} \\ r_{01}(n) &= \{1,0,1,1,1,1,0,1,1,0\}. \end{aligned} \quad (6)$$

Now, define $e_{00}(n)$ and $e_{01}(n)$ as the polyphase components of the error signal $e(n)$. In this way, we distinguish between those errors that occur in the even time indexes from those occur in the odd time indexes.

Figure 4 shows the structure of the multirate filters that estimate the error signal from the syndrome sequence and then extracts the message from the corrected received signal. Table 1 describes the logic that governs the decoder. The first and second columns of this table are the weights of the polyphase components of $e(n)$. As shown in Fig. 3, these polyphase components are inputs for the two filters $u_{00}(n)$ and $u_{01}(n)$. The third and fourth columns give the weight of the response of the filters $r_{00}(n)$ and $r_{01}(n)$ to the syndrome, respectively. Note that the interference term $\zeta_{eo}(n)$ is induced by $e_{00}(n)$ on $y_1(n)$. Similarly, the interference term $\zeta_{oe}(n)$ is induced by $e_{01}(n)$ on $y_0(n)$. Define:

$$\eta_{oe}(n) = u_{01}(n) * r_{00}(n) \qquad \eta_{eo}(n) = u_{00}(n) * r_{01}(n). \quad (7)$$

Since we only consider error patterns of weight up to two, it can be verified that $\zeta_{oe}(n) = \eta_{oe}((n-n_0))_M$ and $\zeta_{eo}(n) = \eta_{eo}((n-n_1))_M$ for some integers n_0 and n_1. The fifth and sixth columns of the table gives the weight of the outputs $y_0(n)$ and $y_1(n)$, respectively. Finally, the last column specifies the node whose output is used as an estimate of the error pattern $\tilde{e}(n)$. The decoding algorithm works as following. First, the decoder determines the weight of the error in its even and odd time indexes. In other words, the decoder should determine $wt(e_{00}(n))$ and $wt(e_{01}(n))$. As shown in the table this can be done by just computing $wt(y_0(n))$ except for the case when $wt(e_{00}(n)) = wt(e_{01}(n)) = 1$ (the last row of the table) which can be confused with the case $wt(e_{00}(n)) = 0$ and $wt(e_{01}(n)) = 2$ (the fifth row in the table). Therefore, whenever $wt(y_0(n))$ is equal to either 4 or 6, the decoder should compute $wt(y_1(n))$ to determine whether the case lies on the fifth row or on the last row of the table. The second step after computing the weight of $e_{00}(n)$ and $e_{01}(n)$, is to estimate $e(n)$. It is clear from the table that except for the case where $wt(e_{00}(n)) = wt(e_{01}(n)) = 1$, the correct estimate appears at either node 1 or node 2 in Fig. 4. For the case $wt(e_{00}(n)) = wt(e_{01}(n)) = 1$, the decoder needs to determine the interference term $\zeta_{oe}(n) = \eta_{oe}((n-n_0))_M$. This is equivalent to finding the integer n_0 which is the appropriate cyclic shift of $\eta_{oe}((n-n_0))_M$. This requires trying all ten possible n_0 and computing the weight of $x_0(n)$. It can be shown that the value of n_0 for which $wt(x_0(n)) = 1$ corresponds to the exact interference term. For this value of n_0, the polyphase components of the error $e(n)$ are $x_0(n) = e_{00}(n)$ and $e_{01}(n) = \delta(n-n_0)$. Once $e(n)$ is determined by its polyphase components (the output of the node 3 in Fig. 4), it can be used to correct the received code word which further passes through the filter $h_0(n)$ and the downsampler (one of the branches of the analysis bank) to extract the message block.

Table 1. Description of the logic that governs the bounded-decoding of (20,10,6) code.

$wt(e_{00})$	$wt(e_{01})$	$y_0(n)$	$y_1(n)$	$wt(y_0)$	$wt(y_1)$	output
0	0	zero	zero	0	0	-
1	0	$e_{00}(n)$	$\zeta_{eo}(n)$	1	7	node 1
0	1	$\zeta_{oe}(n)$	$e_{01}(n)$	5	1	node 2
2	0	$e_{00}(n)$	$\zeta_{eo}(n)$	2	4,6	node 1
0	2	$\zeta_{oe}(n)$	$e_{01}(n)$	4,6	2	node 2
1	1	$e_{00}(n)+\zeta_{oe}(n)$	$e_{01}(n)+\zeta_{eo}(n)$	4,6	6,8	node 3

3.2. Bounded-distance Decoding of the Wavelet-Golay Code

In [4], it has been shown that any double circulant self-dual code can be constructed by a cyclic orthogonal wavelet system. It can be verified that the (24,12,8) Golay code can be constructed by the wavelet-encoder of Fig. 2a by choosing the scaling function and mother wavelet as $g_0 = \{A80011\}$ and $g_1 = \{40DD55\}$, respectively. Figure 3 generates the syndrome of the error in which the syndrome generator filter is $h(n) = \{915D8B\}$.

The decoder acts very similar to the decoder described for the (20,10,6) code. Figure 5 shows the structure of the multirate filters that estimate the error signal from the syndrome sequence and then extract the message from the corrected received signal. The filters $u_{00}(n)$, $u_{01}(n)$, $r_{00}(n)$, and $r_{01}(n)$ are specified using $h(n)$ by the relations described for the (20,10,6) code. One can verify that:

$$\begin{aligned} r_{00}(n) &= \{1,0,0,1,0,1,0,0,1,0,0,1\} \\ r_{01}(n) &= \{1,0,1,1,0,0,1,1,0,1,1,0\}. \end{aligned} \quad (8)$$

Table 2 describes the logic that governs the decoder. Note that the interference term $\zeta_{eo}^{(i)}(n)$ that is induced by $e_{00}(n)$ on $y_1(n)$ have a superscript (i) that shows the number of bits in $e_{00}(n)$ that contribute to the interference. A similar convention applies to the $\zeta_{oe}^{(i)}(n)$. To describe the logic of the decoder, we divide the table into different regions. The first region, the upper rows of the table, are the cases for which $wt(y_0)$ and $wt(y_1)$ uniquely specify whether we need to choose the output at node 1 or node 2 as

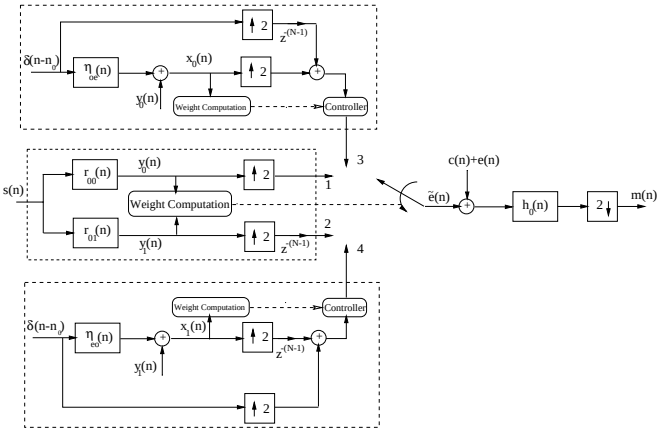

Fig. 5. Decoder for the Golay code that reconstructs the message sequence from the syndrome.

Table 2. Description of the logic that governs the bounded-decoding of (24,12,8) wavelet-Golay code. In this table the letter X means: do not care.

$wt(e_{00})$	$wt(e_{01})$	$y_0(n)$	$y_1(n)$	$wt(y_0)$	$wt(y_1)$	output
0	0	zero	zero	0	0	-
1	0	$e_{00}(n)$	$\zeta_{eo}^{(1)}(n)$	1	7	node 1
0	1	$\zeta_{oe}^{(1)}(n)$	$e_{01}(n)$	7	1	node 2
2	0	$e_{00}(n)$	$\zeta_{eo}^{(2)}(n)$	2	6,10	node 1
0	2	$\zeta_{oe}^{(2)}(n)$	$e_{01}(n)$	6,10	2	node 2
3	0	$e_{00}(n)$	$\zeta_{eo}^{(3)}(n)$	3	X	node 1
0	3	$\zeta_{oe}^{(3)}(n)$	$e_{01}(n)$	X	3	node 2
1	1	$e_{00}(n)+\zeta_{oe}^{(1)}(n)$	$e_{01}(n)+\zeta_{eo}^{(1)}(n)$	6,8	6,8	node 3
2	1	$e_{00}(n)+\zeta_{oe}^{(1)}(n)$	$e_{01}(n)+\zeta_{eo}^{(2)}(n)$	5,7,9	5,7,9,11	node 3
1	2	$e_{00}(n)+\zeta_{oe}^{(2)}(n)$	$e_{01}(n)+\zeta_{eo}^{(1)}(n)$	5,7,9,11	5,7,9	node 4

the estimate of the channel error pattern $e(n)$. The case corresponding to $wt(e_{00}) = wt(e_{01}) = 1$, which we refer to it as the Case $1e1o$, can be distinguished from other cases by using $wt(y_0)$ and $wt(y_1)$. However, both $y_0(n)$ and $y_1(n)$ contain an interference term. Therefore, to find $e(n)$, we have to compute the interference term. Since the interference in $y_0(n)$ is due to $\zeta_{oe}^{(1)}(n)$, the decoder specifies the interference term by cyclic shifting of $\eta_{oe}((n-n_0))_M$ until $wt(x_0(n)) = 1$, similar to the decoding of the (20,10,6) code. This requires trying all 12 possible values of n_0 and computing the weight of $x_0(n)$. Finally the last region of the table, are the cases in which 2 bits error lie in $e_{00}(n)$ and one bit error lies in $e_{01}(n)$ (Case $2e1o$) or vice versa (Case $1e2o$). Having the information about $wt(y_0)$ and $wt(y_1)$ does not specify whether we are in Case $2e1o$ or Case $1e2o$. It turns out that decoding these two cases are very similar to the Case $1e1o$. We first assume that it is Case $2e1o$, and we repeat the same procedure that is described for the Case $1e1o$. In other words, we try 12 different possible interference terms $\eta_{oe}^{(1)}((n-n_0))_M$ and find n_0 for which $wt(x_0(n)) = 2$. Once n_0 is found the decoder selects the output at node 3 as estimate of $e(n)$. If no n_0 was found, then the assumption was wrong. Thus the case must be ($1e2o$), and we try 12 different possible interference terms $\eta_{eo}^{(1)}((n-n_0))_M$ and find n_0 for which $wt(x_1(n)) = 2$. Then $e(n)$ is obtained from node 4.

The description of the wavelet-Golay code shows that most of the time the decoder only needs to compute $wt(y_0)$ and $wt(y_1)$ to find the error pattern $e(n)$. In the worst cases ($1e2o$ and $2e1o$) the decoder needs 12 (or at most 24) cyclic shift and add operations. Consequently, the computation cost for wavelet-Golay decoding is much smaller than that of bounded-distance decoding of the Golay code with the conventional table lookup method which requires 2324 syndrome comparisons. As a final remark, note that the decoding strategy that has been described for (20,10,6) and (24,12,8) codes can be generalized similarly for other codes that have higher error correction property.

4. CONCLUSION

We have reported an example of using finite-field wavelet transform for error control coding. We addressed three issues. First, we described how the two-channel cyclic wavelet transform can be used to construct some of the double circulant half-rate codes. Second, we introduced a decoding technique for the wavelet codes based on a polyphase filter inversion methodology. Third, we demonstrated the striking simplicity and computational saving of wavelet decoding method by describing the decoders of the (20,10,6) and (24,12,8) Golay code.

5. REFERENCES

[1] F. Fekri, R. M. Mersereau, and R. W. Schafer, "Theory of wavelet transforms over finite fields," in *Proc. Int. Conf. Acoust. Speech, and Signal proc.*, pp. 605–608, March 1999.

[2] F. Fekri, R. M. Mersereau, and R. W. Schafer, "Realization of paraunitary filter banks over fields of characteristic two," in *Proc. Int. Conf. Acoust. Speech, and Signal proc.*, June 2000.

[3] F. Fekri, S. W. McLaughlin, R. M. Mersereau, and R. W. Schafer, "Double circulant self-dual codes using finite field wavelet transforms," *Springer Verlag Lecture Notes in Computer Science (LNCS);Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp. 355–364, 1999.

[4] F. Fekri, S. W. McLaughlin, R. M. Mersereau, and R. W. Schafer, "Error control coding using finite field wavelet transforms, Part II: Double circulant codes," *submitted to IEEE Trans. on Information Theory*, Decemebr 1999.

[5] F. Fekri, S. W. McLaughlin, R. M. Mersereau, and R. W. Schafer, "Rate $1/l$ block codes using finite field wavelets; a new family of maximum distance-separable codes and more," in *Proc. Conf. on Information Siences and Systems*, Princeton, NJ, March 2000.

[6] F. Fekri, S. W. McLaughlin, R. M. Mersereau, and R. W. Schafer, "Convolutional coding using finite-field wavelet transforms." in Proc. Thirty-Eighth Annual Allerton Conference, 2000.

[7] P. J. Davis, *Circulant matrices*. John Wiley and Sons, New York, 1979.