Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 478253, 9 pages
doi:10.1155/2008/478253

Research Article

Multirate Filter Bank Representations of RS and BCH Codes

Geert Van Meerbergen and Marc Moonen

Deptartment of Electrical Engineering, Faculty of Engineering, ESAT, Katholieke Universiteit Leuven, Kasteelpark Arenberg 10, 3001 Leuven, Belgium

Correspondence should be addressed to Geert Van Meerbergen, gvanmeer@esat.kuleuven.be

Received 20 December 2007; Revised 1 July 2008; Accepted 12 September 2008

Recommended by Soura Dasgupta

This paper addresses the use of multirate filter banks in the context of error-correction coding. An in-depth study of these filter banks is presented, motivated by earlier results and applications based on the filter bank representation of Reed-Solomon (RS) codes, such as Soft-In Soft-Out RS-decoding or RS-OFDM. The specific structure of the filter banks (critical subsampling) is an important aspect in these applications. The goal of the paper is twofold. First, the filter bank representation of RS codes is now explained based on polynomial descriptions. This approach allows us to gain new insight in the correspondence between RS codes and filter banks. More specifically, it allows us to show that the inherent periodically time-varying character of a critically subsampled filter bank matches remarkably well with the cyclic properties of RS codes. Secondly, an extension of these techniques toward the more general class of BCH codes is presented. It is demonstrated that a BCH code can be decomposed into a *sum* of critically subsampled filter banks.

1. INTRODUCTION

Multirate filter banks have long been known to be powerful tools for image and audio processing [1], for example, in video/audio compression [2, Chapter 14]. Recent work by, for example, Scaglione et al. [3] demonstrates the usefulness of filter banks in communication systems. Many modulation schemes, including CDMA, OFDM (DMT), and TDMA, can actually be viewed as filter banks that build input diversity (add redundancy) at the transmitter. In this paper, filter banks are used in yet another application, namely, as error-correcting codes. In [4, 5], it is shown that *oversampled* filter banks are robust to subband errors and erasures. More specifically, in these papers, the resilience of filter banks (frame expansions) to subband erasures is studied. This resilience is a result of the redundancy introduced by the filter bank representation. Therefore, oversampled filter banks can readily be used as error-correcting codes (see [6–9]). In [6, 7], the main idea is to construct a parity check polynomial matrix corresponding to an oversampled filter bank.

There is, however, an important distinction between this work and the literature mentioned so far; the filter banks discussed in this paper operate in a *finite field* (Galois field) and represent Reed-Solomon or BCH codes. Filter banks that add redundancy with the explicit purpose of error correction and that work in finite fields were also addressed by Fekri et al. [10]. Recently, we developed a critically subsampled filter bank representation of RS codes, which is the starting point in building a novel SISO RS decoder [11, 12]. As a second application, RS codes have been merged with OFDM modulators, leading to a novel transmission scheme, called RS-OFDM [13], in which part of the RS code contributes to the OFDM modulator. Both applications rely extensively on the critically subsampled filter bank representation of RS codes. The goal of this paper is to present an in-depth study of the link between filter banks and error-correcting codes, opposed to the previous work where the focus was shifted towards the applications. Moreover, in this paper, a novel way to describe the correspondence between filter banks and RS codes is developed using a polynomial description. This approach has two important advantages. Firstly, it allows us to give a compact description of both filter banks and RS codes, and also to gain more insight in the link between the cyclic character of an RS code and the periodically time-varying character of a critically subsampled filter bank. Secondly, it allows us to extend the filter bank decomposition

from RS codes to the broader class of BCH codes. Hence, applications like filter-bank-based soft decoding [11] can be envisaged to work for BCH codes as well.

To fully understand the multirate signal processing aspects of the filter banks used here, we start with a discussion of short-time Fourier transform (STFT) filter banks [14]. These filter banks are known to provide cheap realizations of linear filtering operations. The filter banks are then explicitly designed to ensure that a linear time-invariant (LTI) system is realized. However, if the subsample factor is increased, the filter bank behaves as a linear periodically time-varying (LPTV) system, as explained in [15]. While this is usually considered as an undesirable artifact, it is this periodicity that is exploited in this paper. Moreover, it is proven that when the subsample factor is increased to the point where the filter bank becomes critically subsampled, its impulse response at different time instants has some property that resembles a cyclic shift. Combined with the inherent cyclic character of RS codes, this leads to a remarkable correspondence between critically subsampled filter banks and RS codes. It is not surprising that there exists a relationship with the quasicyclic character of certain codes, for example, RS codes with noncoprime length and dimension [16]. Remarkably, the filter bank representation also exists for codes that are not naturally quasicyclic by virtue of their dimension-to-length ratio.

As a final remark, note that the use of an STFT filter bank is not very surprising, seen the relation between RS (BCH) codes and the DFT. Since the publication of the seminal paper of Wolf [17], the relation between the DFT in the complex field and RS (BCH) codes has been extensively studied [18, 19]. In [20, 21], subspace-based methods are applied to simplify decoding of real valued codes. Again, these results are obtained in the complex field, rather than in the Galois field used in this paper.

The paper is structured as follows. In Section 1, the STFT filter bank is reviewed. Based on [14], the condition for a time-invariant filter bank is recalled in Section 2. In Section 3, our main theorem states how to construct a critically subsampled filter bank implementing an RS code. In Section 4, this result is then extended to BCH codes, which can be broken into a sum of critically subsampled filter banks.

Notation

Lower/upper case bold-face symbols represent vectors/matrices, respectively. The ith element of a vector $\mathbf{a}$ is denoted with $a[i]$ and the i, jth element of a matrix $\mathbf{A}$ is denoted with $A[i, j]$. The Z-transform of a vector $\mathbf{a} = [\, a[0] \;\; a[1] \;\; a[2] \;\; \cdots \,]^T$ is represented by the polynomial $a(z^{-1}) = a[0] + a[1]z^{-1} + \cdots$. $\mathcal{R}[\nu, \kappa]$ and $\mathcal{B}[\nu, \kappa]$ denote an RS code and a BCH code, respectively, of length ν and dimension κ. $u(z^{-1})$ and $y(z^{-1})$ denote dataword and codeword, respectively. A finite field of order q (Galois field) is denoted as $\mathbb{F}_q$. An nth root of unity in a finite field is denoted as α_n. $a \mid b$ denotes "a divides b."

2. FILTER BANKS AND LINEAR TIME-INVARIANT SYSTEMS

Multirate filter banks essentially work in a block oriented fashion, that is, the data are divided in blocks of N (with N the subsampling) and are processed accordingly. These schemes became popular with the invention of the DFT and its fast FFT implementation. Filter banks that calculate the DFT of subsequent data blocks are referred to as STFT filter banks. In this section, some basic facts of STFT filter banks are recalled to provide a clear understanding of the rest of the paper. Since error-correcting codes in the Galois field (GF) are targeted, we will use this opportunity to present the GF counterpart of STFT filter banks in the complex field. In this context, α_{q-1} represents a primitive $q-1$-st root of unity in $\mathbb{F}_q$. An $M \times M$ DFT matrix only exists in $\mathbb{F}_q$ if M divides $q-1$, in which case an Mth root of unity α_M exists, for example, $\alpha_M = \alpha_{q-1}^{(q-1)/M}$. Often, a sum $\sum_{l=0}^{L-1}$ is denoted as $\sum_l$ if the indices can be easily derived from the context.

Consider a general multirate system as shown in Figure 1, operated in $\mathbb{F}_q$ with M bands and subsampled by N. In the case of an STFT filter bank, the analysis bank consists of the following filters:

$$a_m(z^{-1}) = z^{-N+1} a(\alpha_M^m z), \tag{1}$$

where the prototype filter $a(z^{-1})$ is defined as follows:

$$a(z^{-1}) = 1 + z^{-1} + z^{-2} + \cdots + z^{-N+1}. \tag{2}$$

Similarly, the synthesis bank filters are defined as

$$c_m(z^{-1}) = c(\alpha_M^m z), \tag{3}$$

with

$$c(z^{-1}) = 1 + z + z^2 + \cdots + z^{M-1}. \tag{4}$$

This scheme is well known for its fast convolution properties and is referred to as the overlap-add scheme. Swapping synthesis and analysis bank leads to the overlap-save counterpart. As we will recall below, this filter bank can implement an exact linear filtering when correctly designed. This explanation closely follows the approach of [14].

Let us define the subband filters as follows:

$$d_m(z^{-1}) = \sum_{l=0}^{L-1} \alpha_M^{ml} b_l(z^{-1}). \tag{5}$$

The filters $b_l(z^{-1})$ are seen to play an important role later. The latter relation can be inverted, leading to

$$b_l(z^{-1}) = \sum_{m=0}^{M-1} \alpha_M^{-ml} d_m(z^{-1}). \tag{6}$$

Considering an input $u(z^{-1}) = z^j$ with $j \in \{0, \ldots, N-1\}$, the analysis bank mth band output is

$$x_m(z^{-N}) = \alpha_M^{m(N-1-j)} \quad \forall m = 0, \ldots, M-1. \tag{7}$$

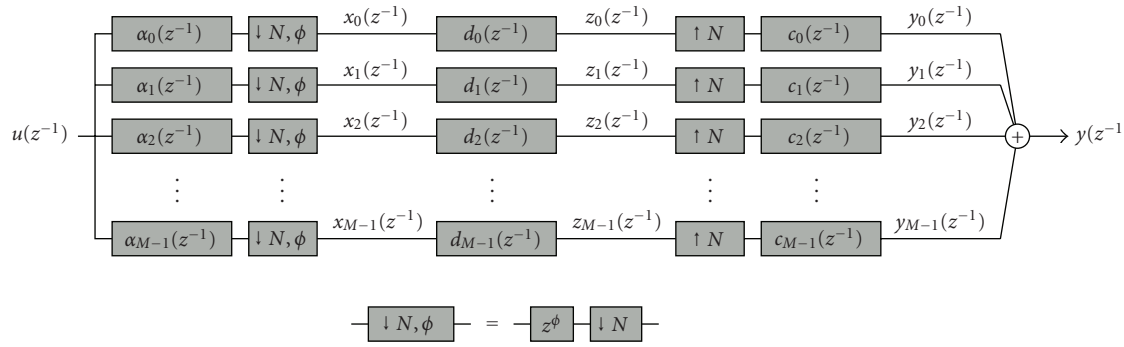

Figure 1: *Overlap-add* filter bank with M bands and N-fold subsampling.

This signal is filtered with $d_m(z^{-N})$ (because of the upsampling with N) and fed into the synthesis bank yielding an mth band output

$$\begin{aligned} y_m(z^{-1}) &= x_m(z^{-N})\, d_m(z^{-N})\, c_m(z^{-1}) \\ &= \sum_{m'=0}^{M-1} \alpha_M^{m(N-1-j)}\, d_m(z^{-N})\, \alpha_M^{-mm'} z^{-m'} \\ &= \sum_{m'=0}^{M-1} \sum_{l=0}^{L-1} \alpha_M^{m(N-1-j)}\, \alpha_M^{ml}\, b_l(z^{-N})\, \alpha_M^{-mm'} z^{-m'}. \end{aligned} \tag{8}$$

The filter bank output $y(z^{-1})$ is obtained as the sum over all bands:

$$\begin{aligned} y(z^{-1}) &= \sum_{m=0}^{M-1} y_m(z^{-1}) \\ &= \sum_{m=0}^{M-1} \sum_{m',l} \alpha_M^{m(N-1-j)}\, \alpha_M^{ml}\, b_l(z^{-N})\, \alpha_M^{-mm'} z^{-m'} \\ &= \sum_{l=0}^{L-1} b_l(z^{-N}) \sum_{m'=0}^{M-1} \sum_{m=0}^{M-1} \alpha_M^{m(N-1-j+l-m')} z^{-m'}. \end{aligned} \tag{9}$$

Looking closely to the double sum, it is seen that the only non-zero terms are those with $m' = l + N - 1 - j$, due to the orthogonality of the roots of unity. Indeed, if $m' \neq l+N-1-j$, the inner summation (over m) equals zero. Therefore,

$$y(z^{-1}) = z^{-N+1+j} \sum_{l=0}^{L-1} z^{-l} b_l(z^{-N}) \tag{10}$$

$$= u(z^{-1}) z^{-N+1} \sum_{l=0}^{L-1} z^{-l} b_l(z^{-N}), \tag{11}$$

which indeed represents a linear filtering operation. Note that if $L = N$, $b_l(z^{-1})$ are the polyphase components of the filter being implemented by the filter bank. The last equation only holds when M is chosen large enough, that is, $M \geq N + L - 1$. Before discussing in the next section what happens if this condition is not fulfilled, we will give an example of a filter bank implementing an RS code.

Example 1. Throughout this paper, the $\mathcal{R}[15, 10]$ code in $\mathbb{F}_{2^4}$ with roots $\{\alpha_{15}^3, \alpha_{15}^4, \alpha_{15}^5, \alpha_{15}^6, \alpha_{15}^7\}$ is used to illustrate our techniques. A (nonsystematic) codeword is obtained as the multiplication of the dataword $u(z^{-1})$ with the generator polynomial $g(z^{-1})$:

$$\begin{aligned} g(z^{-1}) &= \prod_{k=3}^{7} (z^{-1} - \alpha_{15}^k) \\ &= \alpha_{15}^{10} + \alpha_{15}^9 z^{-1} + \alpha_{15}^{11} z^{-2} + \alpha_{15}^6 z^{-3} + \alpha_{15}^9 z^{-4} + z^{-5}. \end{aligned} \tag{12}$$

With $L = N = 2$,

$$\begin{aligned} g(z^{-1}) &= \sum_{l=0}^{1} z^{-l} b_l(z^{-2}) \text{ with} \\ b_0(z^{-1}) &= \alpha_{15}^{10} + \alpha_{15}^{11} z^{-1} + \alpha_{15}^9 z^{-2}, \\ b_1(z^{-1}) &= \alpha_{15}^9 + \alpha_{15}^6 z^{-1} + z^{-2}. \end{aligned} \tag{13}$$

Choosing $M = 3 \geq L + N - 1$, the subband filters $d_m(z^{-1})$ are calculated according to (5) leading to the filter bank shown in Figure 2. Note that the first $N - 1$ all-zero output samples should obviously be ignored (see also (10)).

3. CRITICALLY SUBSAMPLED FILTER BANKS AND CYCLIC CODES

In this section, it is explained how the LTI system described in Section 2 transforms into an LPTV system if the condition $M \geq N + L - 1$ is not met. This is the basic step in understanding the link between some cyclic codes and their filter bank representations. Assume the subsample factor N is too large such that $N = M - L + 1 + d$, with $d \geq 0$. In this case, the only nonzero terms are those with $m' = l+N-1-j \bmod M$. Note the modulo operation that is added such that $0 \leq m' \leq M - 1$. Equation (10) becomes

$$y(z^{-1}) = \sum_{l=0}^{L-1} z^{-(N-1-j+l) \bmod M} b_l(z^{-N}). \tag{14}$$

This means that for $j = 0, \ldots, d-1$, the last $d - j$ coefficients are folded back. Hence, this multirate system has different

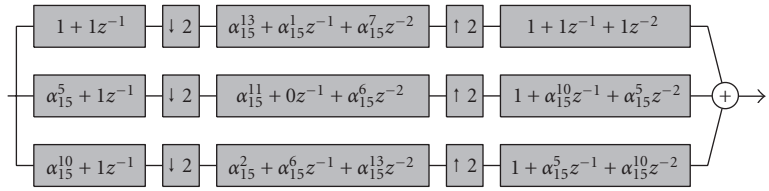

Figure 2: Filter bank representation of $\mathcal{R}[15, 10]$, with $M = 3$, $N = L = 2$ (Example 1).

impulse responses on different time instants j that repeat periodically, and so indeed realize an LPTV system. In a coding context, this characteristic is often referred to as *cyclic*. As will be shown, there is a strong link between critically subsampled filter banks and cyclic codes such as RS and BCH codes.

Example 2. Assume $M = 3$ and $L = 2$ as in the previous example. If N is increased to 3 (critically subsampled), then $d = L - M + N - 1 = 1$ and the following impulse responses are obtained:

$$\begin{aligned} u(z^{-1}) = z^{2} &\longrightarrow y(z^{-1}) = b_0 z^{-0} + b_1 z^{-1}, \\ u(z^{-1}) = z^{1} &\longrightarrow y(z^{-1}) = b_0 z^{-1} + b_1 z^{-2}, \\ u(z^{-1}) = z^{0} &\longrightarrow y(z^{-1}) = b_0 z^{-2} + b_1 \mathbf{z^{-0}}. \end{aligned} \tag{15}$$

Note that b_1 is folded back onto z^{-0}.

For the applications mentioned in Section 1, it is crucial that the filter banks are critically subsampled, that is, that the number of bands M equals the downsampling factor N. Hence, the condition $M \geq L + N - 1$ is indeed violated. Therefore, while critically subsampled filter banks are not of much interest if a cheap implementation of a linear filter is aimed for, it is shown in this paper that such filter banks are exceptionally well suited to implement RS codes and some other cyclic codes.

Theorem 1. *Let $\mathcal{R}[\nu, \kappa]$ be an RS code over $\mathbb{F}_q$ of length $\nu = q - 1$. Consider an STFT-based critically subsampled filter bank with M bands (M divides ν), subsampled by $N = M$ and with analysis and synthesis bank (resp., $a_m(z^{-1})$ and $c_m(z^{-1})$) as defined in (1) and (3). If the roots α_{q-1}^{r} of $\mathcal{R}[\nu, \kappa]$ are distributed over the subband filters, according to*

$$d_m(\alpha_{q-1}^{r}) = 0 \Longleftrightarrow r \bmod M = m, \tag{16}$$

then this filter bank implements the RS code $\mathcal{R}[\nu, \kappa]$.

Proof. Since M divides ν, let us define the shortcut notation $\nu' = \nu/M$. With

$$\begin{aligned} b_l(z^{-1}) &= \sum_{k=0}^{K-1} b_l[k] z^{-k}, \\ d_m(z^{-1}) &= \sum_{k=0}^{K-1} d_m[k] z^{-k}, \end{aligned} \tag{17}$$

the following relation holds (see (6)):

$$b_l[k] = \sum_{m=0}^{M-1} \alpha_{q-1}^{-\nu' ml} d_m[k]. \tag{18}$$

The proof will consist in showing that the filter bank output for every $u(z^{-1}) = z^{j}$, for all $j \in \{0, \ldots, N-1\}$ is a codeword of the original RS code, up to an interleaving. This done in two steps. In the first step, the filter bank output for $u(z^{-1}) = z^{N-1}$ is considered:

$$y(z^{-1}) = \sum_{l=0}^{L-1} z^{-l} b_l(z^{-N}). \tag{19}$$

Interleaving this $y(z^{-1})$ gives

$$y^{\Pi}(z^{-1}) = \sum_{l=0}^{L-1} z^{-\nu' l} b_l(z^{-1}). \tag{20}$$

Now, it is shown that $y^{\Pi}(z^{-1})$ is a codeword of $\mathcal{R}[\nu, \kappa]$ by calculating its Mattson-Solomon polynomial Δ:

$$\begin{aligned} \Delta(z^{-1}) &= \sum_{j=0}^{\nu'-1} \sum_{m=0}^{M-1} \Delta[Mj + m] z^{-Mj-m} \text{ with} \\ \Delta[Mj + m] &= \sum_{l=0}^{L-1} \sum_{k=0}^{\nu'-1} \alpha_{q-1}^{(\nu' l + k)(Mj+m)} b_l[k] \\ &= \sum_{l,k} \alpha_{q-1}^{(\nu' l + k)(Mj+m)} \sum_{m'=0}^{M-1} \alpha_{q-1}^{-\nu' m' l} d_{m'}[k] \\ &= \sum_{k} \alpha_{q-1}^{k(Mj+m)} \sum_{l,m} \alpha_{q-1}^{\nu' l (Mj+m-m')} d_{m'}[k]. \end{aligned} \tag{21}$$

This can further be simplified by noting that the double sum is nonzero only if $m = m'$, similar to (10):

$$\Delta[Mj + m] = \sum_{k=0}^{\nu'-1} \alpha_{q-1}^{k(Mj+m)} d_m[k] = d_m(\alpha_{q-1}^{Mj+m}). \tag{22}$$

If α_{q-1}^{Mj+m} is a root of $\mathcal{R}[\nu, \kappa]$, then $\Delta[Mj + m] = 0$ such that $y^{\Pi}(z^{-1})$ is a codeword of $\mathcal{R}[\nu, \kappa]$.

The second step consists in showing that for all $u(z^{-1}) = z^{j}$, $j = 0 : N - 1$, the output of the filter bank belongs

to $\mathcal{R}[\nu,\kappa]$. In general, $y(z^{-1})$ is given by (14). Interleaving (same interleaver) results in

$$\begin{aligned} y^{\Pi}(z^{-1}) &= \sum_{l=0}^{L-1} z^{-\bmod(\nu(N-1-j+l),\nu' M)} b_l(z^{-1}) \\ &= z^{-\nu'(N-1-j)} \sum_{l=0}^{L-1} z^{-\nu' l} b_l(z^{-1}) \bmod 1+z^{-\nu}. \end{aligned} \tag{23}$$

This is a codeword too because it is the original codeword (see (20)) cyclically shifted by $\nu'(N-1-j)$, which proves the theorem. The only role of the interleaver is to transform the cyclic character modulo $1-x^M$ of the filter bank into the cyclic character of the RS code modulo $1-x^\nu$. □

Hence, the construction of a filter bank representation for an RS code is very simple. The roots of the subband filters $d_m(z^{-1})$ correspond to a well-defined subset of the roots of the RS code. In this fashion, the roots of the RS code are distributed among the subbands, each containing a smaller so-called subband code.

Example 3. Continuing our example of the $\mathcal{R}[15,10]$ code with $M=N=3$, the roots α_{15}^3, α_{15}^4, α_{15}^5, α_{15}^6, α_{15}^7 are distributed among the subband filters $d_m(z^{-1})$ as follows:

$$\begin{aligned} \alpha_{15}^3, \alpha_{15}^6 &\longrightarrow d_0(z^{-1}) = \alpha_{15}^9 + \alpha_{15}^2 z^{-1} + z^{-2}, \\ \alpha_{15}^4, \alpha_{15}^7 &\longrightarrow d_1(z^{-1}) = \alpha_{15}^{11} + \alpha_{15}^3 z^{-1} + z^{-2}, \\ \alpha_{15}^5 &\longrightarrow d_2(z^{-1}) = \alpha_{15}^5 + z^{-1}. \end{aligned} \tag{24}$$

Using (18), $b_l(z^{-1})$ is readily calculated:

$$\begin{aligned} b_0(z^{-1}) &= \alpha_{15}^1 + \alpha_{15}^{13} z^{-1}, \\ b_1(z^{-1}) &= 1 + \alpha_{15}^{12} z^{-1} + \alpha_{15}^5 z^{-2}, \\ b_2(z^{-1}) &= \alpha_{15}^{14} + \alpha_{15}^5 z^{-1} + \alpha_{15}^{10} z^{-2}. \end{aligned} \tag{25}$$

The critically subsampled filterbank can be found in Figure 3.

Note that the first subband filter is a non-primitive $\mathcal{B}[5,3]$ code in $\mathbb{F}_{2^4}$ with α_{15}^3 a primitive 5th root of unity. It is also cyclic and if ν' were not prime, the procedure can be applied recursively. The other subband filters are not cyclic. However, a filter bank can be found for them too, but this is out of the scope of this paper. The next section will further focus on BCH codes.

Secondly, note that this structure can be seen as a generalization of the quasicyclic structure of an RS code as found by Solomon and van Tilborg [16]. If M and κ are coprime, this quasicyclic structure does not exist, however the critically subsampled filter bank does exist. If M divides κ, the filter bank exactly implements the quasicyclic structure. For example, if $M=5$ is chosen (see Figure 4), it can be verified that this filter bank explicitly implements the quasicyclic structure of the RS code as described in [16].

4. FILTER BANK REPRESENTATIONS FOR BCH CODES

In the previous section, it is shown how the cyclic character of the RS code modulo $1-x^\nu$ is transformed by the filter bank into a cyclic character modulo $1-x^M$, with $M \mid \nu$. This condition is seen to be a crucial element in the derivation since, for RS codes, $\nu = q-1$ and thus $M \mid q-1$. The latter guarantees that an M-point DFT exists in $\mathbb{F}_q$. For the more general family of BCH codes, ν can differ from $q-1$ such that $M \mid \nu$ no longer guarantees the existence of an M-point DFT in $\mathbb{F}_q$. This section deals with filter bank representations for BCH codes.

4.1. Filter bank representation in an extension field

Let $\mathcal{B}[\nu,\kappa]$ be a BCH code in $\mathbb{F}_q$. Let n be the *multiplicative order of q modulo ν*, that is, n is the smallest integer such that $x^\nu - 1 \mid x^{q^n-1}-1$. Let $\alpha_\nu \in \mathbb{F}_{q^n}$ be a primitive νth root of unity in $\mathbb{F}_{q^n}$. Let M be a common divisor of ν and q^n-1 with M and $q-1$ coprime. Unless ν is prime, this is always possible since $\nu \mid q^n-1$. In the extension field $\mathbb{F}_{q^n}$, the M-point DFT transform exists, so that the filter bank representation of $\mathcal{B}[\nu,\kappa]$ can readily be constructed in the extension field, according to Theorem 1.

Example 4. Let us consider a BCH code $\mathcal{B}[10,5]$ in $\mathbb{F}_{3^2}$ ($\nu=10$, $\kappa=5$, $q=3^2$). Let α_8 be a primitive root of unity in $\mathbb{F}_{3^2}$. Since the multiplicative order of 9 mod 10 (i.e., $q \bmod \nu$) equals $n=2$, the extension field is $\mathbb{F}_{3^4}$. Therefore, let α_{80} and $\alpha_{10} = \alpha_{80}^8$ be a primitive, respectively, 10th root of unity in $\mathbb{F}_{3^4}$. Assume a set of roots is chosen that is symmetric around 1, for example, $\alpha_{10}^{-2} = \alpha_{10}^8$, $\alpha_{10}^{-1} = \alpha_{10}^9$, α_{10}^0, α_{10}^1, α_{10}^2. With

$$g(z^{-1}) = \alpha_8^4 + \alpha_8^7 z^{-1} + \alpha_8^6 z^{-2} + \alpha_8^2 z^{-3} + \alpha_8^3 z^{-4} + z^{-5}, \tag{26}$$

a maximum distance separable (MDS) BCH code $\mathcal{B}[10,5]$ is obtained. (Such a BCH code is called an *optimal BCH code*.) The techniques presented in Section 3 can directly be applied to this BCH code in the extension field $\mathbb{F}_{3^4}$. The resulting filter bank representation is shown in Figure 5. The filter coefficients in this filter bank are powers of α_{10}. Unfortunately, $\alpha_{10} \notin \mathbb{F}_{3^2}$. This imposes problems if the filter bank is used in the applications mentioned in Section 1; for example, the complexity of a SISO RS decoder based on the extension field filter bank is more complex than its counterpart in $\mathbb{F}_q$ Section 4.2 deals with a transformation of the filter bank in $\mathbb{F}_{3^4}$ to a filter bank in $\mathbb{F}_{3^2}$.

4.2. Transforming the filter bank from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$

Before tackling this general problem, let us first investigate how a single element of $\mathbb{F}_{q^n}$ can be decomposed into elements of $\mathbb{F}_q$. Any set $\boldsymbol{\lambda}$ of linearly independent elements of $\mathbb{F}_q$ can serve as a basis for $\mathbb{F}_{q^n}$ [22]. For example, if the field $\mathbb{F}_{p^m}$ (p prime) is constructed starting from $\mathbb{F}_p$ using a primitive polynomial $\mathcal{P}(x)$, the normal basis $\boldsymbol{\lambda} = [1 \;\; \alpha_{q-1} \;\; \alpha_{q-1}^2 \;\; \cdots]$ is used. However, also other bases can be used. What is needed is a mathematical tool that allows us to easily

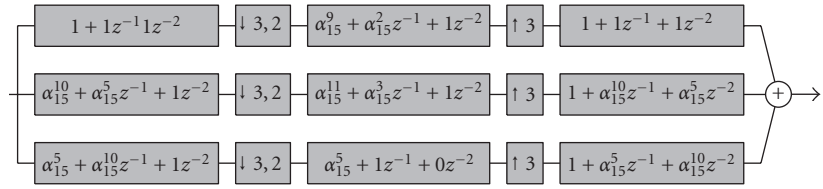

Figure 3: Filter bank with component codes in each subband for the $\mathcal{R}[15, 10]$ (Example 3).

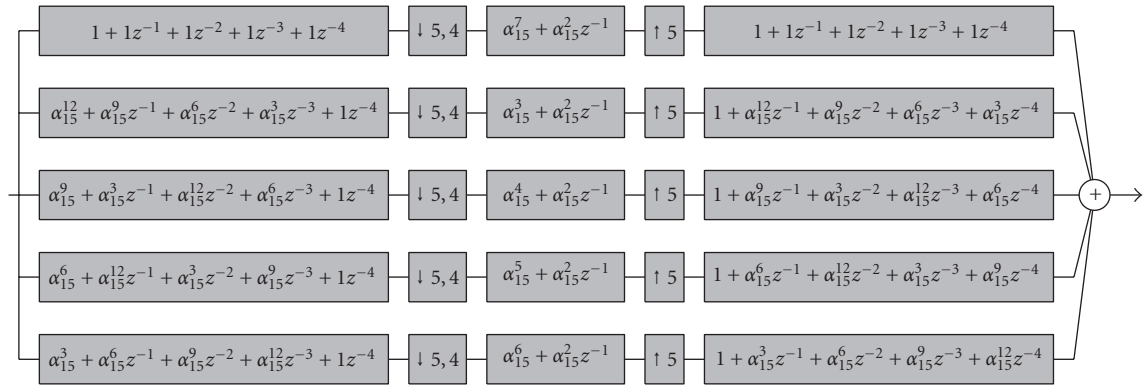

Figure 4: Filter bank with component codes in each subband for the $\mathcal{R}[15, 10]$ (Example 3).

decompose elements of a Galois field along a specified basis. This tool is called the *trace* [22].

Definition 1. The trace of $a \in \mathbb{F}_{q^n}$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined as

$$\mathrm{Tr}_n(a) = \sum_{j=0}^{n-1} a^{q^j} \in \mathbb{F}_q. \tag{27}$$

This is a useful property for decomposing an element a along a specified basis $\boldsymbol{\lambda} = [\ \lambda[0]\ \ \cdots\ \ \lambda[n-1]\ ]$, as we will see. First, we define the complementary basis. A basis $\overline{\boldsymbol{\lambda}} = [\ \overline{\lambda}[0]\ \ \cdots\ \ \overline{\lambda}[n-1]\ ]$ is said to be complementary to $\boldsymbol{\lambda}$ if

$$\mathrm{Tr}_n(\overline{\lambda}[i]\lambda[i]) = \delta_{ij}, \tag{28}$$

with δ_{ij} the Kronecker delta. Each element $a \in \mathbb{F}_{q^n}$ can now be written as [22]

$$a = \sum_{i=0}^{n-1} a^{\{i\}}\lambda[i] \tag{29}$$

with

$$a^{\{i\}} = \mathrm{Tr}_n(a\overline{\lambda}[i]) \in \mathbb{F}_q. \tag{30}$$

Two properties of the trace will be used here:

$$\begin{aligned} \mathrm{Tr}_n(a+b) &= \mathrm{Tr}_n(a) + \mathrm{Tr}_n(b) \quad \forall a, b \in \mathbb{F}_{q^n}, \\ \mathrm{Tr}_n(a\cdot b) &= a\cdot\mathrm{Tr}_n(b) \quad \forall a \in \mathbb{F}_q, b \in \mathbb{F}_{q^n}. \end{aligned} \tag{31}$$

Example 5. As an example, the trace can be used to obtain the polynomial representation of, for example, $a = \alpha_8^5 \in \mathbb{F}_{3^2}$ defined by $\mathcal{P}(x) = x^2 + 2x + 2$. The complementary basis $\overline{\boldsymbol{\lambda}}$ of the normal basis $\boldsymbol{\lambda} = [\ 1\ \ \alpha_8\ ]$ is calculated:

$$\overline{\boldsymbol{\lambda}} = \left[\alpha_8\ \ \alpha_8^2\right]. \tag{32}$$

Now, the traces are calculated according to (27):

$$\begin{aligned} \mathrm{Tr}_2(\overline{\lambda}[0]a) &= \mathrm{Tr}_2(\alpha_8^1\cdot\alpha_8^5) = \alpha_8^1\cdot\alpha_8^5 + \alpha_8^{1^3}\cdot\alpha_8^{5^3} = 0, \\ \mathrm{Tr}_2(\overline{\lambda}[1]a) &= \mathrm{Tr}_2(\alpha_8^2\cdot\alpha_8^5) = \alpha_8^2\cdot\alpha_8^5 + \alpha_8^{2^3}\cdot\alpha_8^{5^3} = \alpha_8^4 = 2. \end{aligned} \tag{33}$$

According to (29), $\alpha_8^5 = 0\cdot\alpha_8^0 + 2\cdot\alpha_8^1$ which can be easily verified.

Let us now investigate how elements in $\mathbb{F}_{q^n}$ can be multiplied using $\mathbb{F}_q$ arithmetic. This leads to an extension of the concept of a trace. Assume $a, b, c = a\cdot b \in \mathbb{F}_{q^n}$. Using (29), a and b can be decomposed as follows:

$$\begin{aligned} a &= \sum_{i=0}^{n-1} a^{\{i\}}\lambda[i], \\ b &= \sum_{i=0}^{n-1} b^{\{i\}}\lambda[i]. \end{aligned} \tag{34}$$

Using (30) and assuming a normal basis ($\overline{\lambda}[i] = \alpha_{q^n-1}^i$), the ith coordinate of c becomes

$$c^{\{i\}} = \mathrm{Tr}_n(a\cdot b\overline{\lambda}[i]) \tag{35}$$

$$= \mathrm{Tr}_n\left(\overline{\lambda}[i]\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} b^{\{j\}}a^{\{k\}}\alpha_{q^n-1}^{k+j}\right) \tag{36}$$

$$= \sum_{j=0}^{n-1} b^{\{j\}}\sum_{k=0}^{n-1} a^{\{k\}}\mathrm{Tr}_n(\overline{\lambda}[i]\alpha_{q^n-1}^{k+j}). \tag{37}$$

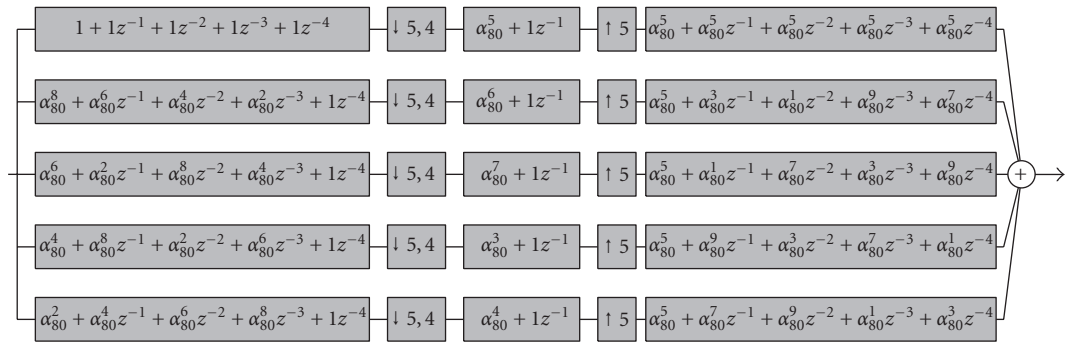

FIGURE 5: Critically subsampled filter bank representation over $\mathbb{F}_{q^n}$ of the BCH code $\mathcal{B}[10, 5]$.

The last equation is obtained using the properties of the trace in (31). The inner sum will be denoted in a special way:

$$\begin{aligned} a^{\{i,j\}} &= \sum_{k=0}^{n-1} a^{\{k\}} \mathrm{Tr}_n(\overline{\lambda}[i]\alpha_{q^n-1}^{k+j}) \\ &= \sum_{k=0}^{n-1} \mathrm{Tr}_n(a^{\{k\}}\overline{\lambda}[i]\alpha_{q^n-1}^{k+j}) \\ &= \mathrm{Tr}_n\left(\sum_{k=0}^{n-1} a^{\{k\}}\overline{\lambda}[i]\alpha_{q^n-1}^{k+j}\right) \\ &= \mathrm{Tr}_n\left(\overline{\lambda}[i]\alpha_{q^n-1}^{j}\sum_{k=0}^{n-1} a^{\{k\}}\alpha_{q^n-1}^{k}\right) \\ &= \mathrm{Tr}_n(\overline{\lambda}[i]\alpha_{q^n-1}^{j}a). \end{aligned} \tag{38}$$

Using this notation, (35) becomes

$$c^{\{i\}} = \sum_{j=0}^{n-1} a^{\{i,j\}} b^{\{j\}}, \tag{39}$$

which resembles a matrix multiplication. Indeed, defining the $n \times 1$ vectors $\mathbf{c}$ and $\mathbf{b}$ and the $n \times n$ matrix $\mathbf{A}$ as $c[i] = c^{\{i\}}$, $b[i] = b^{\{i\}}$, and $A[i, j] = a^{\{i,j\}}$,

$$\mathbf{c} = \mathbf{A}\mathbf{b}. \tag{40}$$

Example 6. Let us define $\mathbb{F}_{3^4}$ by its primitive polynomial $\mathcal{P}(x) = 2 + 2x^3 + x^4$, with root α_{80} such that $\alpha_8 = \alpha_{80}^{10} \in \mathbb{F}_{3^2}$. With $a = \alpha_{80}^{11}$, $b = \alpha_{80}^{23}$, c becomes α_{80}^{34}. The complementary basis $\overline{\boldsymbol{\lambda}}$ of the normal basis $\boldsymbol{\lambda} = [\ 1 \quad \alpha_{80}\ ]$ is calculated:

$$\overline{\boldsymbol{\lambda}} = \begin{bmatrix} \alpha_{80}^{14} & \alpha_{80}^{45} \end{bmatrix}. \tag{41}$$

The elements a and b can be expanded according to this basis resulting in the following vectors/matrices:

$$\underbrace{\begin{bmatrix} \alpha_8^7 \\ \alpha_8^2 \end{bmatrix}}_{\mathbf{c}} = \underbrace{\begin{bmatrix} 0 & \alpha_8^6 \\ \alpha_8^1 & \alpha_8^4 \end{bmatrix}}_{\mathbf{A}} \underbrace{\begin{bmatrix} \alpha_8^2 \\ \alpha_8^1 \end{bmatrix}}_{\mathbf{b}}. \tag{42}$$

As can be verified, $\boldsymbol{\lambda}\mathbf{c} = c = \alpha_{80}^{34}$.

All necessary notation is now defined to properly state the theorem.

Theorem 2. *Let $\mathcal{B}[\nu, \kappa]$ be a BCH code in $\mathbb{F}_q$. M is a common divisor of ν and $q^n - 1$. Let $a_m(z^{-1})$, $d_m(z^{-1})$, and $c_m(z^{-1})$ be the analysis, subband, and synthesis filters of a critically subsampled filter bank over $\mathbb{F}_{q^n}$, as defined by (1), (16), and (3), respectively. Then $\mathcal{B}[\nu, \kappa]$ can be implemented as a sum of n critically subsampled filter banks over $\mathbb{F}_q$. The analysis and synthesis banks of the n'th filter bank ($n' = 0 : n - 1$, band m) are defined, respectively, as ${a_m}^{\{n',0\}}(z^{-1})$, ${c_m}^{\{0,n'\}}(z^{-1})$. The subband filters $\widetilde{d}_m(z^{-1})$ are the same for each filter bank:*

$$\widetilde{d}_m(z^{-1}) = \sum_{k=0}^{n-1} a[k] d_m^{q^k}(z^{-1}) \tag{43}$$

with

$$\mathbf{a} = \begin{bmatrix} a[0] \\ a[1] \\ \vdots \\ a[n-1] \end{bmatrix}, \tag{44}$$

a solution of the following system of equations:

$$\begin{bmatrix} \overline{\lambda}[0] & \overline{\lambda}[0]^q & \overline{\lambda}[0]^{q^2} & \cdots & \overline{\lambda}[0]^{q^{n-1}} \\ \overline{\lambda}[0]^{q^{n-1}} & \overline{\lambda}[0] & \overline{\lambda}[0]^q & \cdots & \overline{\lambda}[0]^{q^{n-2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \overline{\lambda}[0]^q & \overline{\lambda}[0]^{q^2} & \overline{\lambda}[0]^{q^3} & \cdots & \overline{\lambda}[0] \end{bmatrix} \mathbf{a} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{45}$$

(Given a polynomial $a(z^{-1})$, $ab(z^{-1})$ denotes the polynomial with each coefficient raised to the power b.)

Proof. Considering an input $u(z^{-1}) = z^{j'}$ with $j' \in \{0, \ldots, N-1\}$, the filter bank output (impulse response) for $\mathcal{B}[\nu, \kappa]$ can be written as

$$y(z^{-1}) = \sum_{m=0}^{M-1} c_m(z^{-1}) d_m(z^{-N}) x_m(z^{-1}) \tag{46}$$

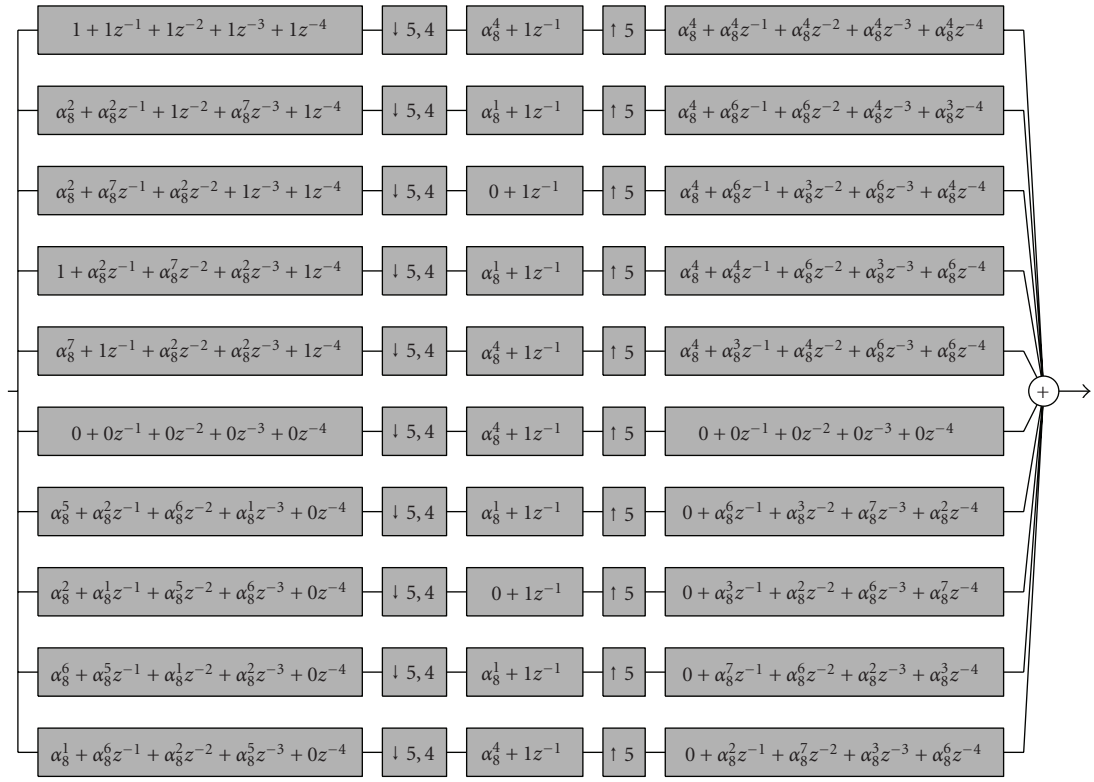

FIGURE 6: Critically subsampled filter bank representation over $\mathbb{F}_q$ of the BCH code $\mathcal{B}[10, 5]$ $(n = 2)$.

with

$$x_m(z^{-1}) = \alpha_M^{\gamma' m(N-1-j')}. \tag{47}$$

We show that the filter bank output $y'(z^{-1})$ of the filter bank in $\mathbb{F}_q$ equals $y(z^{-1})$. The filter bank output of the n'th filter bank of $\mathcal{B}[\nu, \kappa]$ equals

$$y_{n'}(z^{-1}) = \sum_{m=0}^{M-1} c_m^{\{0,n'\}}(z^{-1}) \widetilde{d}_m(z^{-N}) x_m^{\{n',0\}}(z^{-1}). \tag{48}$$

Substitutions of $\widetilde{d}_m(z^{-1})$ (see (43)) and

$$\begin{aligned} c_m^{\{0,n'\}}(z^{-1}) &= \sum_{i=0}^{n-1} \left(c_m(z^{-1}) \overline{\lambda}[0] \rho^{n'}\right)^{q^i}, \\ x_m^{\{n',0\}}(z^{-1}) &= \sum_{j=0}^{n-1} \left(\overline{\lambda}[n'] x_m\right)^{q^j} \end{aligned} \tag{49}$$

and summing over all filter banks $(n' = 0, \ldots, n-1)$ while using

$$\sum_{n'=0}^{n-1} \alpha_{q^n-1}^{n' q^i} \overline{\lambda}[n']^{q^j} = \delta_{ij}, \tag{50}$$

(28) leads to

$$y(z^{-1}) = \sum_{m=0}^{M-1} \sum_{k=0}^{n-1} a[k] \sum_{i=0}^{n-1} \overline{\lambda}[0]^{q^i} c_m^{q^i}(z^{-1}) d_m^{q^k}(z^{-N}) x_m^{q^i}(z^{-1}). \tag{51}$$

Grouping terms with $k - j$ constant $(i = k - j \bmod n)$ gives

$$y(z^{-1}) = \sum_{k,j} a[k] \overline{\lambda}[0]^{q^{k-j}} \sum_m c_m^{q^{k-j}}(z^{-1}) d_m^{q^k}(z^{-N}) x_m^{q^{k-j}}(z^{-1}). \tag{52}$$

It can be verified that the inner sum with $j = 0$ is independent of k:

$$\sum_{m=0}^{M-1} c_m^{q^k}(z^{-1}) d_m^{q^k}(z^{-N}) x_m^{q^k}(z^{-1}) = y(z^{-1}). \tag{53}$$

For $j \neq 0$, it can be seen that the inner sum is again independent of j. Summing over all i, $y(z^{-1}) = y'(z^{-1})$ if $a[k]$ is a solution of the system in (45) which proves the theorem. □

Example 7. In this example, the filter bank over $\mathbb{F}_{3^4}$ as shown in Figure 5 is transformed into a filter bank over $\mathbb{F}_{3^2}$ as stated by the previous theorem. In this case, the system of equations in (45) becomes

$$\begin{bmatrix} \alpha_{80}^{14} & \alpha_{80}^{46} \\ \alpha_{80}^{46} & \alpha_{80}^{14} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \tag{54}$$

with solution $\mathbf{a} = \begin{bmatrix} \alpha_{80}^{59} \\ \alpha_{80}^{51} \end{bmatrix}$. The filter bank so obtained can be found in Figure 6.

5. CONCLUSION

This paper presents an in-depth investigation of filter bank representations for RS and BCH codes, motivated by a number of applications presented earlier. STFT filter banks are the starting point. In most applications, these filter banks are explicitly designed to ensure a linear time-invariant operation. However, if the subsample factor is increased, the filter bank acts as a periodically time-varying system. Although this is normally considered as an undesirable artefact, it is this periodicity that is exploited to build critically subsampled filter bank representations for the family of RS codes. In this case, a proper distribution of the roots of the RS code over the subbands is the key element in constructing such a filter bank. In the more general case of a BCH code, similar filter bank structures exist. The same techniques used for RS codes can first be applied to obtain a critically subsampled filter bank representation in an extension field. Finally, it is explained how this filter bank can be transformed from the extension field into the base field.

ACKNOWLEDGMENTS

This paper was presented in part at the IEEE International Symposium on Information Theory (ISIT), 4–9 September, 2005, Adelaide, Australia [23]. This research work was carried out at the ESAT laboratory of the Katholieke Universiteit Leuven, in the frame of the Interuniversity Poles of Attraction Programme P5/11.

REFERENCES

[1] M. Vetterli and J. Kovacevi'c, *Wavelets and Subband Coding*, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.

[2] G. Strang and T. Nguyen, *Wavelets and Filter Banks*, Wellesley College, Wellesley, Mass, USA, 1996.

[3] A. Scaglione, G. B. Giannakis, and S. Barbarossa, "Redundant filterbank precoders and equalizers. I. Unification and optimal designs," *IEEE Transactions on Signal Processing*, vol. 47, no. 7, pp. 1988–2006, 1999.

[4] V. K. Goyal, J. Kovačević, and J. A. Kelner, "Quantized frame expansions with erasures," *Applied and Computational Harmonic Analysis*, vol. 10, no. 3, pp. 203–233, 2001.

[5] J. Kovačević, P. L. Dragotti, and V. K. Goyal, "Filter bank frame expansions with erasures," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1439–1450, 2002.

[6] F. Labeau, L. Vandendorpe, and B. Macq, "Oversampled filter banks as error correcting codes," in *Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications (WPMC '02)*, vol. 3, pp. 1265–1269, Honolulu, Hawaii, USA, October 2002.

[7] F. Labeau, J.-C. Chiang, M. Kieffer, P. Duhamel, L. Vandendorpe, and B. Macq, "Oversampled filter banks as error correcting codes: theory and impulse noise correction," *IEEE Transactions on Signal Processing*, vol. 53, no. 12, pp. 4619–4630, 2005.

[8] S. Marinkovic and C. Guillemot, "Joint source-channel coding based on cosine-modulated filter banks for erasure-resilient signal transmission," *EURASIP Journal on Applied Signal Processing*, vol. 2005, no. 4, pp. 510–524, 2005.

[9] S. Marinkovic and C. Guillemot, "Joint source-channel coding by means of an oversampled filter bank code," *EURASIP Journal on Applied Signal Processing*, vol. 2006, Article ID 82023, 12 pages, 2006.

[10] F. Fekri, R. M. Mersereau, and R. W. Schafer, "Two-band wavelets and filterbanks over finite fields with connections to error control coding," *IEEE Transactions on Signal Processing*, vol. 51, no. 12, pp. 3143–3151, 2003.

[11] G. Van Meerbergen, M. Moonen, and H. De Man, "Critically subsampled filterbanks for SISO Reed-Solomon decoding," *IEEE Transactions on Signal Processing*, vol. 54, no. 11, pp. 4446–4460, 2006.

[12] G. Van Meerbergen, M. Moonen, and H. De Man, "Filterbank decompositions for (non)-systematic Reed-Solomon codes with applications to soft decoding," *IEEE Transactions on Signal Processing*, vol. 55, no. 12, pp. 5681–5694, 2007.

[13] G. Van Meerbergen, M. Moonen, and H. De Man, "Reed-Solomon codes implementing a coded single-carrier with cyclic prefix scheme," accepted for publication in *IEEE Transactions on Communications, 2009*.

[14] M. Vetterli, "Running FIR and IIR filtering using multirate filter banks," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 36, no. 5, pp. 730–738, 1988.

[15] P. Vaidyanathan, *Multirate Systems and Filter Banks*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1993.

[16] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM Journal on Applied Mathematics*, vol. 37, no. 2, pp. 358–369, 1979.

[17] J. Wolf, "Redundancy, the discrete fourier transform, and impulse noise cancellation," *IEEE Transactions on Communications*, vol. 31, no. 3, pp. 458–461, 1983.

[18] G. Rath and C. Guillemot, "Performance analysis and recursive syndrome decoding of DFT codes for bursty erasure recovery," *IEEE Transactions on Signal Processing*, vol. 51, no. 5, pp. 1335–1350, 2003.

[19] G. R. Redinbo, "Decoding real block codes: activity detection, Wiener estimation," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 609–623, 2000.

[20] G. Rath and C. Guillemot, "Subspace-based error and erasure correction with DFT codes for wireless channels," *IEEE Transactions on Signal Processing*, vol. 52, no. 11, pp. 3241–3252, 2004.

[21] G. Rath and C. Guillemot, "Subspace algorithms for error localization with quantized DFT codes," *IEEE Transactions on Communications*, vol. 52, no. 12, pp. 2115–2124, 2004.

[22] N. Sloane and F. MacWilliams, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[23] G. Van Meerbergen, M. Moonen, and H. De Man, "Filterbank decompositions for BCH-codes with applications to soft decoding and code division multiple acces systems," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '05)*, pp. 2389–2393, Adelaide, Australia, September 2005.