Filterbank Decompositions for BCH-codes with Applications to Soft Decoding and Code Division Multiple Acces systems

Geert Van Meerbergen ⋆, Marc Moonen ⋆
⋆ E.E. Dept., ESAT/SISTA, K.U.Leuven
Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium
Email: {gvanmeer,moonen}@esat.kuleuven.ac.be
Tel.: +32-16-32-{1817,1060}

Hugo De Man ⋆†
† IMEC,
Kapeldreef 75, 3001 Leuven, Belgium
Email: deman@imec.be
Tel.: +32 16 281 200

***Abstract*— Multirate systems and filterbanks are known to be powerfull tools in image and audio applications. Recently, they are also recognised to play an important role in communication systems. This paper covers the use of filterbanks in a coding context. It is shown that their inherent periodically time varying character matches remarkably well with the cyclic properties of the family of Bose-Chaudhuri-Hochquenghem (BCH) codes. In this paper, the important subclass of Reed-Solomon (RS) codes is dealt with first. This section of the paper proves that an RS code can be implemented by a critically subsampled filterbank. The redundancy is added by the subbandfilters, which are shown to be variants of non-primitive BCH codes. The second part of the paper deals with BCH codes. In this part, a BCH code is decomposed as a sum of critically subsampled filterbanks. The critical subsampling is an important aspect in a number of applications; The use of these filterbanks in a CDMA system and in a Soft-In Soft-Out (SISO) decoding context is briefly discussed.**

I. Introduction

Filterbanks have long been known to be a powerfull tool for image and audio processing. Recent work by Scaglione *et al.* [1] demonstrates the usefullness of filterbanks in communication systems. Many modulation schemes including CDMA, OFDM (DMT) and TDMA can actually be viewed as filterbanks that build input diversity (add redundancy) at the transmitter. Filterbanks that add redundancy with the purpose of error correction - and therefore work in finite fields - were also addressed by Fekri [2].

In this paper, another approach is taken. It starts with a discussion of Short-Time Fourier Transform (STFT) filterbanks [3]. These filterbanks became popular due to their ability to perform linear filtering operations. Typically, they are explicitly designed to ensure that they implement a Linear Time Invariant (LTI) system. However, if the number of bands is not chosen to be large enough, this filterbank behaves as a periodically time varying (PTV) system, as explained in [3]. Though this is normally considered an undesirable artefact, it is this periodicity that is exploited in this paper.

Moreover, it is proven that when the filterbank becomes critically subsampled, the impulse response at different time instances has some property that resembles a cyclic shift. Combined with the inherent cyclic character of BCH codes, this leads to a remarkable correspondence between filterbanks and BCH codes. It is not surprising that there exists a relationship with the quasi-cyclic character of certain codes, e.g. RS codes with non coprime length and dimension [4]. However, the filterbank representation also exists for codes which are not naturally quasi-cyclic by virtue of their dimension to length ratio.

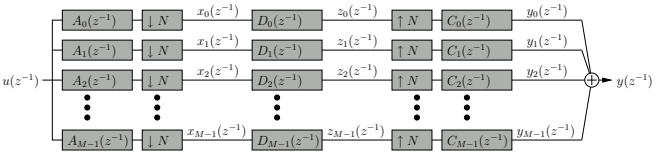

Fig. 1. *overlap-add* filterbank with M bands and N-fold subsampling.

The paper is structured as follows; In the first section, the STFT filterbank and its relation with PTV systems is explained. Based on Vetterli's work, the condition for a time invariant filterbank is recalled. In section II, our main theorem is presented about the construction of a critically subsampled filterbank implementing a RS code. In the next section, this result is extended to BCH codes, which can be broken into a sum of critically subsampled filterbanks. Finally, two applications are briefly discussed. The first one illustrates how such a filterbank can be used to build a SISO RS decoder. The second one shows the use of the filterbank in a multiuser CDMA context.

II. Filterbanks and their link with Cyclic codes

Filterbanks and multirate systems in general are widely used in digital signal processing. Essentially, these systems work block oriented, i.e. the data is divided in blocks of N (with N the subsampling) and is processed accordingly. More precisely, filterbanks which calculate the *Discrete Fourier Transform* (DFT) of subsequent data blocks are said to be based on the STFT. In this section, some basic facts of STFT filterbanks are recalled to provide a clear understanding of the rest of the paper. Since error correcting codes in the Galois Field $GF(p^d)$ are targeted, this opportunity will be used to present the Galois Field counterpart of STFT filterbanks in the complex field. In this context, $\alpha \in GF(p^d)$ represents a (p^d-1)-th primitive root of unity. The $M \times M$ DFT matrix is then defined by $\mathbf{F}_{ij} = \beta^{ij}$ with $i,j = 0..M-1$ and β an M-th root of unity. This only exists if M divides p^d-1, in which case β is a power of $\alpha^{(p^d-1)/M}$. A general multirate system as shown in Figure 1, with M bands and subsampled by N. In the case of an STFT filterbank, the analysis, resp. synthesis bank consist

of the following filters

$$A_m(z^{-1}) = \sum_{n=0}^{N-1} \beta^{nm} z^{n+1-N} \quad (1)$$

$$C_m(z^{-1}) = \sum_{m'=0}^{M-1} \beta^{-mm'} z^{-m'} \quad (2)$$

This scheme is well known for its fast convolution properties, and is called overlap-add scheme. Swapping synthesis and analysis bank leads to its overlap-save counterpart. As shown in [3], this filterbank can implement an exact linear filtering when correctly designed. Therefore, define the subband filters as follows:

$$D_m(z^{-1}) = \sum_{l=0}^{L-1} \beta^{ml} d_l(z^{-1}) \quad (3)$$

Considering an input $u(z^{-1}) = z^j$ with $j = 0..N-1$, Vetterli [3] shows that the output of the filterbank

$$y(z^{-1}) = \sum_{l=0}^{L-1} z^{-mod(N-1-j+l,M)} d_l(z^{-N}) \quad (4)$$

$$= z^{-N+1+j} \sum_{l=0}^{L-1} z^{-l} d_l(z^{-N}) \text{ if } M \geq N+L-1. \quad (5)$$

If the condition $M \geq N+L-1$ is met, the filterbank behaves as an LTI system, implementing a linear filtering. However, if the L is too large, e.g. $L = M-N+1+d$, the last $d-j$ coefficients are folded back. Hence, this multirate system has different impulse responses on different time instants j that repeat periodically. Therefore, it is called a PTV system as opposed to the normal LTI system.

Example 1: Let us construct a filterbank which implements the convolution $y(z^{-1}) = g(z^{-1})u(z^{-1})$ with

$$g(z^{-1}) = \alpha^{10} + \alpha^9 z^{-1} + \alpha^{11} z^{-2} + \alpha^6 z^{-3} + \alpha^9 z^{-4} + z^{-5}$$

This is the generator polynomial of the $\mathcal{R}(15,10)$ RS code in $GF(2^4)$ with roots $\{\alpha^k\}_{k=3..7}$. It is used throughout the paper illustrate our techniques. $u(z^{-1})$ and $y(z^{-1})$ represent resp. dataword and (non-systematic) codeword. With $L = N = 3$,

$$g(z^{-1}) = \sum_{l=0}^{2} z^{-l} d_l(z^{-3}) \text{ with} \quad (6)$$

$$d_0(z^{-1}) = \alpha^{10} + \alpha^6 z^{-1} \quad (7)$$

$$d_1(z^{-1}) = \alpha^9 + \alpha^9 z^{-1} \quad (8)$$

$$d_2(z^{-1}) = \alpha^{11} + z^{-1} \quad (9)$$

Choosing $M = 5 > L+N-1$ and using Equation 3, the subband filters $D_m(z^{-1})$ are calculated leading to the filterbank shown in Figure 2. The output of this filterbank is a codeword of $\mathcal{R}(15,10)$ (at least when the first $N-1$ all-zero samples are ignored, which is assumed from now on). However, if $L = 4$, $d = L-M+N-1 = 1$ and the following impulse responses are obtained:

$$u(z^{-1}) = z^2 y(z^{-1}) = d_0 z^{-0} + d_1 z^{-1} + d_2 z^{-2} + d_3 z^{-3}$$
$$u(z^{-1}) = z^1 y(z^{-1}) = d_0 z^{-1} + d_1 z^{-2} + d_2 z^{-3} + d_3 z^{-4}$$
$$u(z^{-1}) = z^0 y(z^{-1}) = d_0 z^{-2} + d_1 z^{-3} + d_2 z^{-4} + d_3 \mathbf{z^{-0}}$$

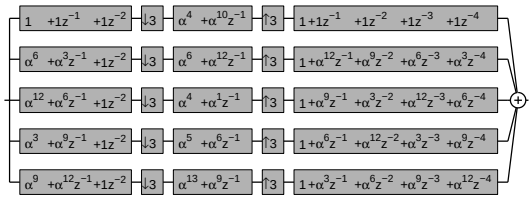

Fig. 2. Filterbank representation of $\mathcal{R}(15,10)$ with $M = 5, L = N = 3$. (example 1)

Note that d_3 is folded back onto z^{-0}. □

For the applications discussed in the section IV, it is crucial that the filterbanks are critically subsampled, i.e. the number of bands M equals the subsample factor N. Hence, the condition $M \geq L+N-1$ is violated. Therefore, critically subsampled filterbanks are not of much interest if subband filtering is aimed for. However, the upcoming theorem shows the PTV critically subsampled filterbanks are exceptionally well suited to implement RS codes and some other cyclic codes.

Theorem 1: Let $\mathcal{R}(\nu,\kappa)$ be a Reed-Solomon code over $GF(p^d)$ of length $\nu = p^d - 1$ and dimension κ. Consider an STFT-based critically subsampled filterbank with M bands ($M|\nu$), subsampled by $N = M$ and with analysis and synthesis bank (respectively $A_m(z^{-1})$ and $C_m(z^{-1})$) defined as in Equation 1. This filterbank will implement the RS code $\mathcal{R}(\nu,\kappa)$ if a root α^i of $\mathcal{R}(\nu,\kappa)$ is assigned to subband m if and only if $i \bmod M = m$. Stated otherwise,

$$D_m(\alpha^i) = 0 \Leftrightarrow \exists j \in \mathbb{Z} | i = Mj + m \quad (10)$$

proof: Introducing the notation d_{lk} and D_{mk}, with

$$d_l(z^{-1}) = \sum_{k=0}^{K-1} d_{lk} z^{-k} \quad (11)$$

$$D_m(z^{-1}) = \sum_{k=0}^{K-1} D_{mk} z^{-k} \quad (12)$$

the following relation holds (assuming $\beta = \alpha^{\nu/M}$, a primitive M-th root of unity):

$$d_{lk} = \sum_{m=0}^{M-1} \alpha^{-\nu ml/M} D_{mk} \quad (13)$$

The proof of theorem 1 consists in proving that the filterbank output is a codeword of $\mathcal{R}(\nu,\kappa)$ (up to an interleaving), for every input $u(z^{-1}) = z^j$ with $j = 0..N-1$. Therefore, let us recall that the filterbank output for $j = N-1$ equals $y(z^{-1}) = \sum_{l=0}^{L-1} z^{-l} d_l(z^{-N})$. Interleaving this $y(z^{-1})$ gives

$$y^{\Pi}(z^{-1}) = \sum_{l=0}^{L-1} z^{-\nu l/M} d_l(z^{-1}) \quad (14)$$

Now it is shown that $y^{\Pi}(z^{-1})$ is a codeword of $\mathcal{R}(\nu,\kappa)$ by calculating its Mattson-Solomon polynomial Δ [5]:

$$\Delta(z^{-1}) = \sum_{j=0}^{\nu/M-1} \sum_{m=0}^{M-1} \Delta_{Mj+m} z^{-Mj-m} \text{ with} \quad (15)$$

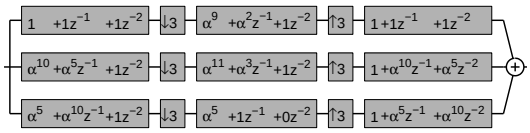

Fig. 3. Critically subsampled filterbank of $\mathcal{R}(15,10)$. (example 2)

$$\Delta_{Mj+m} = \sum_{l=0}^{L-1}\sum_{k=0}^{\nu/M-1} \alpha^{(\nu l/M+k)(Mj+m)} d_{lk} \quad (16)$$

$$= \sum_{l=0}^{L-1}\sum_{k=0}^{\nu/M-1} \alpha^{(\nu l/M+k)(Mj+m)} \sum_{m'=0}^{M-1} \alpha^{-\nu m' l/M} D_{m'k}$$

$$= \sum_{k=0}^{\nu/M-1} \alpha^{k(Mj+m)} \sum_{l=0}^{L-1}\sum_{m'=0}^{M-1} \alpha^{\nu l(Mj+m-m')/M} D_{m'k}$$

This can further be simplified noting that the double sum is only nonzero if $m = m'$, due to the orthogonality of the M-th roots of unity.

$$\Delta_{Mj+m} = \sum_{k=0}^{\nu/M-1} \alpha^{k(Mj+m)} D_{mk} = D_m(\alpha^{Mj+m}) = 0$$

The next step is to show that for all $j = 0 : N-1$, the output of the filterbank belongs to $\mathcal{R}(\nu,\kappa)$. In general, $y(z^{-1})$ is given by equation 4. Interleaving results in

$$y^{\Pi}(z^{-1}) = \sum_{l=0}^{L-1} z^{-mod(\nu(N-1-j+l)/M,\nu M/M)} d_l(z^{-1}) \quad (17)$$

$$= z^{-\nu(N-1-j)/M} \sum_{l=0}^{L-1} z^{-\nu l/M} d_l(z^{-1}) \bmod (1+z^{-\nu})$$

This is a codeword too because it is the original codeword (at $j = N-1$) cyclically shifted by $\nu(N-1-j)/M$, which proves the theorem. ■

Example 2: Continuing our example of the $\mathcal{R}(15,10)$ code, the roots $\alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7$ are distributed among the polynomials $D_m(z^{-1})$ as follows:

$$\alpha^3, \alpha^6 \Leftarrow D_0(z^{-1}) = \alpha^9 + \alpha^2 z^{-1} + z^{-2} \quad (18)$$

$$\alpha^4, \alpha^7 \Leftarrow D_1(z^{-1}) = \alpha^{11} + \alpha^3 z^{-1} + z^{-2} \quad (19)$$

$$\alpha^5 \Leftarrow D_2(z^{-1}) = \alpha^5 + z^{-1} \quad (20)$$

Using equation 13, $d_m(z^{-1})$ is readily calculated:

$$d_0(z^{-1}) = \alpha^1 + \alpha^{13} z^{-1} \quad (21)$$

$$d_1(z^{-1}) = 1 + \alpha^{12} z^{-1} + \alpha^5 z^{-2} \quad (22)$$

$$d_2(z^{-1}) = \alpha^{14} + \alpha^5 z^{-1} + \alpha^{10} z^{-2} \quad (23)$$

Hence, the output of the filterbank ($j = N-1 = 2$) $y(z^{-1}) = \alpha^1 + z^{-1} + \alpha^{14} z^{-2} + \alpha^{13} z^{-3} + \alpha^{12} z^{-4} + \alpha^5 z^{-5} + \alpha^5 z^{-7} + \alpha^{10} z^{-8}$. According to the theorem, $y^{\Pi}(z^{-1}) = \alpha^1 + \alpha^{13} z^{-1} + z^{-5} + \alpha^{12} z^{-6} + \alpha^5 z^{-7} + \alpha^{14} z^{-10} + \alpha^5 z^{-11} + \alpha^{10} z^{-12}$ is a codeword of the $\mathcal{R}(15,10)$ code. This can be verified by calculating its Mattson-Solomon polynomial $\Delta(z^{-1})$ of which the coefficients of z^{-3} up to z^{-7} are zero. □

Note that if M divides κ, the filterbank implements the quasi-cyclic structure for a RS code [4]. If M and κ are coprime, this quasi-cyclic structure does not exist, however the critically subsampled filterbank does exist. An example is shown in Figure 4 for the $\mathcal{R}(15,10)$ code with $M = 5$.

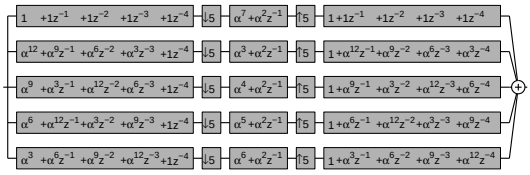

Fig. 4. Critically subsampled filterbank for $\mathcal{R}(15,10)$ with $M = 5$ bands, implementing quasi-cyclic structure of $\mathcal{R}(15,10)$ as described in [4]

Secondly, remark that in a critically subsampled filterbank, $x_m(z^{-1})$ and $z_m(z^{-1})$ have κ/M, resp. μ/M coefficients, called subband variables. Therefore, the coefficients of $x_m(z^{-1})$ can be seen as input variables. Hence, a filterbank with the analysis bank replaced by a simple serial to parallel converter implements a RS code too, which is equivalent to the original. In this case

$$A_m(z^{-1}) = z^{m+1-N}. \quad (24)$$

Finally, note that the first subband filter is a non-primitive BCH code $\mathcal{B}(5,3)$ [5] in $GF(2^4)$ with α^3 a primitive 5-th root of unity. It is also cyclic and if ν/M were not prime, it can be shown that theorem 1 can be applied recursively. The other subband filters are not cyclic. However, a filterbank 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.

III. BCH Codes

The previous technique relies on the existence of a DFT in the considered field $GF(p^d)$. It is possible however to construct the filterbank in an extension field $GF(p^{\mu d})$ (where a DFT matrix is defined) before transforming the filterbank back into the original Galois field. This technique is especially useful in the context of BCH codes. In this section, we restrict ourselves to fields of characteristic $p = 2$. Let $\mathcal{B}(\nu,\kappa)$ be a BCH code over $GF(p^d)$ of length ν and designed distance δ. Let $GF(p^{\mu d})$ be an extension field with μ the multiplicative order of $p^d \bmod \nu$. With $\sigma \in GF(p^{\mu d})$ a primitive ν-th root of unity, the roots of $\mathcal{B}(\nu,\kappa)$ are denoted as $\sigma^b, \sigma^{b+1}, ..., \sigma^{b+\delta-2}$. Let $\mathcal{B}_e(\nu,\kappa)$ be the non-primitive BCH code over $GF(p^{\mu d})$ with the same roots. Theorem 1 can be easily extended to this type of non-primitive BCH codes over $GF(p^{\mu d})$ with roots in $GF(p^{\mu d})$. The critically subsampled filterbank for $\mathcal{B}_e(\nu,\kappa)$ is found by properly distributing its roots among the subband filters. The problem is how to transform this filterbank back into $GF(p^d)$. Let us start with an instructive example:

Example 3: Let $\mathcal{B}(9,6)$ be an optimal BCH code over $GF(2^3)$ of length $\nu = 9$. $\mathcal{B}_e(\nu,\kappa)$ represents the BCH code over the extension field $GF(2^6)(\mu = 2)$. With $\rho \in GF(2^6)$ the 63-th root of unity, the subfield $GF(2^3)$is the field generated by ρ^9. To obtain a simple relation between the generators $\alpha \in GF(p^d)$ and $\rho \in GF(p^{\mu d})$, the primitive polynomial of $GF(2^6)$ is chosen the μd-th Conway polynomial of characteristic p (In this case $1 + x + x^3 + x^4 + x^6$). ρ is then a root of that polynomial. The relation between the generators is $\alpha = \rho^{\frac{p^{\mu d}-1}{p^d-1}} = \rho^9$. With $\sigma = \rho^7$ a 9-th root of unity, the roots of $\mathcal{B}_(e)$ are $\{\sigma^{-1}, \sigma^0, \sigma^1\}$. Hence, the generator polynomial equals $1+\rho^{27}z^{-1}+\rho^{27}z^{-2}+z^{-3} = 1+\alpha^3 z^{-1}+\alpha^3 z^{-2}+z^{-3}$.

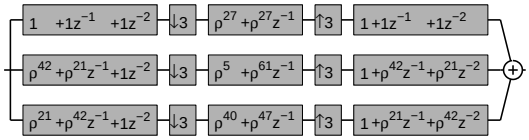

Fig. 5. Critically subsampled filterbank representation ($M = N = 3$) of $\mathcal{B}_e(9, 6, 4)$ in the extension field $GF(2^6)$. (Example 3)

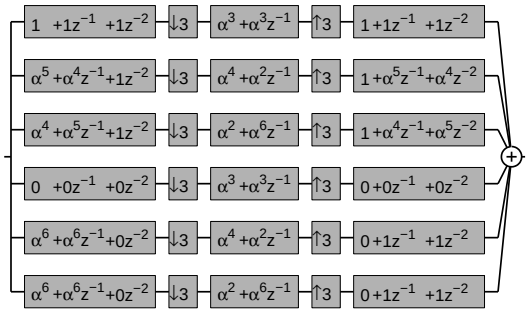

Fig. 6. $\mathcal{B}(\nu, \kappa)$ decomposed as a sum of 2 critically subsampled filterbanks, each subsampled with a factor $N = 3$. (Example 3)

Applying (an extended version of) theorem 1 with $M = 3$ (dividing ν and $p^{\mu d}$) leads to the filterbank shown in Figure 5. It is clear that some filter coefficients belong not to $GF(2^3)$. The following theorem shows that $\mathcal{B}(\nu, \kappa)$ can be implemented as a sum of $\mu = 2$ critically subsampled filterbanks in $GF(2^3)$, shown in Figure 6. □

Before defining the theorem, the following notation is needed: The particular coordinate basis used to expand each element of $GF(p^d)$ is the natural basis $\rho^0..\rho^{\mu-1}$. This means that any element $a \in GF(p^{\mu d})$ can be written as $\sum_{i=0}^{\mu-1} a^{[i]}\rho^i$ with $a^{[i]}$ defined as follows:

$$a^{[i]} = \mathrm{Tr}_d^{\mu d}(\gamma_i a) = \sum_{k=0}^{\mu-1} (\gamma_i a)^{p^{kd}}. \tag{25}$$

In this equation, the trace of an element [5] $a \in GF(p^{\mu d})$ is denoted with Tr and $\gamma_0..\gamma_{m-1}$ is the dual basis [5], i.e.

$$\sum_{k=0}^{\mu-1} \rho^{jp^{kd}} \gamma_i^{p^{kd}} = \delta_{ij} \tag{26}$$

with δ_{ij} denoting the *Kronecker delta*. Multiplying $c = ab \in GF(p^{\mu d})$ can now be written using their coordinates in $GF(p^d)$. Writing out this product by hand, it is easily seen that the following property holds:

$$c^{[i]} = \sum_{j=0}^{\mu-1}\sum_{k=0}^{\mu-1} \mathrm{Tr}_d^{\mu d}(\rho^{k+j}\gamma_i) a^{[k]} b^{[k]} \tag{27}$$

Let us denote the inner summation as follows: $a^{[m,n]} = \sum_{k=0}^{\mu-1} \mathrm{Tr}_d^{\mu d}(\rho^{k+j}\gamma_i) a^{[k]}$. This is simplified in the following lemma (without proof):

Lemma 1:

$$a^{[i,j]} = \mathrm{Tr}_d^{\mu d}(a\gamma_i\rho^j) \tag{28}$$

All the notation is now defined to properly state the main theorem:

Theorem 2: Let $\mathcal{B}(\nu, \kappa), \mathcal{B}_e(\nu, \kappa)$ be BCH codes as defined before. Let M be a common divisor of ν and $p^{\mu d} - 1$. A critically subsampled filterbank with M bands for $\mathcal{B}_e(\nu, \kappa)$ can be found using (an extended version of) theorem 1. The filters $A_m(z^{-1}), D_m(z^{-1})$ and $C_m(z^{-1})$ are defined according to the equations 1, 2 and 10 where $\beta \in GF(p^d)$ is replaced with τ, an M-th root of unity in $GF(p^{\mu d})$. Then $\mathcal{B}(\nu, \kappa)$ can be implemented as a sum of μ critically subsampled filterbanks with analysis, resp. synthesis bank of the n-th filterbank (band m) defined as $A_m^{[n,0]}(z^{-1})$, resp. $C_m^{[0,n]}(z^{-1})$. The subband filters $\tilde{D}_m(z^{-1})$ are the same for each filterbank[1]:

$$\tilde{D}_m(z^{-1}) = \sum_{k=0}^{\mu-1} a_k D_m^{p^{dk}}(z^{-1}) \tag{29}$$

with a_k a solution of the following system:

$$\begin{bmatrix} \gamma_0 & \gamma_0^{p^d} & \gamma_0^{p^{2d}} & \cdots & \gamma_0^{p^{(\mu-1)d}} \\ \gamma_0^{p^{(\mu-1)d}} & \gamma_0 & \gamma_0^{p^d} & \cdots & \gamma_0^{p^{(\mu-2)d}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{p^d} & \gamma_0^{p^{2d}} & \gamma_0^{p^{3d}} & \cdots & \gamma_0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{\mu-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{30}$$

proof: Considering an input $u(z^{-1}) = z^{j'}$ with $j' = 0..N-1$, the filterbank output for $\mathcal{B}_e(\nu, \kappa)$ can be written as

$$\begin{aligned} y_e(z^{-1}) &= \sum_{m=0}^{M-1} C_m(z^{-1}) D_m(z^{-N}) x_m(z^{-1}) \text{ with} \\ x_m(z^{-1}) &= \tau^{m(N-1-j')} \end{aligned} \tag{31}$$

The filterbank output for the n-th filterbank of $\mathcal{B}(\nu, \kappa)$

$$y_n(z^{-1}) = \sum_{m=0}^{M-1} C_m^{[0,n]}(z^{-1}) \tilde{D}_m(z^{-N}) x_m^{[n,0]}(z^{-1}) \tag{32}$$

Substitutions of $\tilde{D}_m(z^{-1})$ (equation 29) and

$$C_m^{[0,n]}(z^{-1}) = \sum_{i=0}^{\mu-1} (C_m(z^{-1})\gamma_0\rho^n)^{p^{id}} \tag{33}$$

$$x_m^{[n,0]}(z^{-1}) = \sum_{j=0}^{\mu-1} (\gamma_n x_m)^{p^{jd}} \tag{34}$$

and summing over all filterbanks (n) while using

$$\sum_{n=0}^{\mu-1} \rho^{np^{id}} \gamma_n^{p^{jd}} = \delta_{ij} \tag{35}$$

(formula 26) leads to

$$y(z^{-1}) = \sum_{m=0}^{M-1}\sum_{k=0}^{\mu-1} a_k \sum_{i=0}^{\mu-1} \gamma_0^{p^{id}} C_m^{p^{id}}(z^{-1}) D_m^{p^{kd}}(z^{-N}) x_m^{p^{id}}(z^{-1}).$$

Grouping terms with $p - k$ constant ($i = p - k \bmod \mu$) gives:

$$y(z^{-1}) = \sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1} a_j \gamma_0^{p^{(j-i)d}} \sum_{m=0}^{M-1} C_m^{p^{(j-i)d}}(z^{-1}) D_m^{p^{jd}}(z^{-N}) x_m^{p^{(j-i)d}}(z^{-1}) \tag{36}$$

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

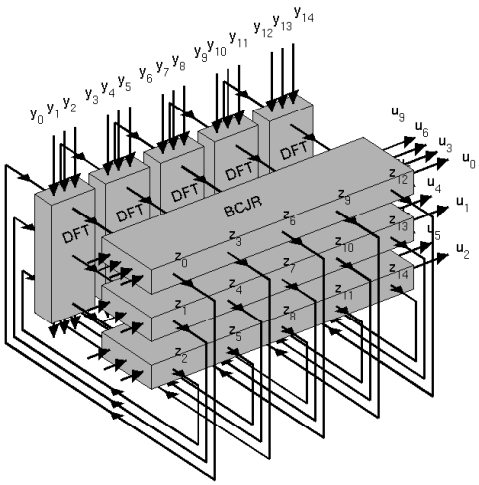

Fig. 7. Block scheme of SISO decoder for $\mathcal{R}(15, 10)$ based on the filterbank shown in Figure 3. The subband variables z_n are used to exchange information between the codeword y_n and the dataword u_n. In each iteration, using the a priori information (u_n: left; y_n: top) an update of the a posterior probabilities is returned (u_n: right; y_n: bottom).

Looking more in detail at the inner sum with $i = 0$, it is seen that:

$$\sum_{m=0}^{M-1} C_m^{p^{jd}}(z^{-1}) D_m^{p^{jd}}(z^{-N}) x_m^{p^{jd}}(z^{-1}) = y_e(z^{-1}) \qquad (37)$$

Indeed, according to theorem 1, the inner sum represents the output of the critically subsampled filterbank for $\mathcal{B}_e(\nu, \kappa)$ since $\tau^{p^{jd}}$ is also an M-th root of unity in $GF(2^{\mu d})$. For $i \neq 0$, it can be seen that the inner sum is again independent of j. Summing over all i, $y(z^{-1}) = y_e(z^{-1})$ if a_k is a solution of the system in equation 30 which proves the theorem. ■

IV. Applications: SISO RS decoder & CDMA system

The first application which is discussed briefly is a SISO decoder for $\mathcal{R}(15, 10)$ (See figure 7). It is based on the filterbank in Figure 3 with a simplified analysis bank (Equation 24). Given soft information (probability vectors) for each codeword symbol y_n, $n = 0..\nu$, the probabilities of the subband variables z_n can be calculated since there exists a DFT relation between each block of them. Five SISO DFT decoders perform this operation in parallel. The probabilities hold so called *extrinsic information* which is send to 3 SISO decoders corresponding to the 3 subband filters $D_m(z^{-1})$. Since the length of this filters is small, *BCJR's algorithm* in a terminated trellis is used to obtain an estimate of the *a posterior probabilities* (APP) of the dataword u_n in conjunction with extrinsic information about the subband variables z_n. This extrinsic information is fed back to the SISO DFT decoders, which can now deliver APP for the codeword too. After several Gallager-like iterations[2], the probabilities (hopefully) converge. For an in depth discussion and simulation results, the interested reader is referred to [6].

The second application illustrates the usefulness of the filterbanks described in this paper in a multiuser context. Typically, in a Direct-Sequence Code-Division Multiple-Access (DS-CDMA) system each user has its own error correcting code, which is designed separately from its spreading code. Using the techniques in this paper, the error correcting code and spreading code are jointly designed such that the overall code is a RS code. An example is given in Figure 8, where for each user an (error-correcting) code, related with $\mathcal{B}(3, 1)$, is combined with a (spreading) code such that the overall code is $\mathcal{R}(12, 4)$ in $GF(13^1)$. Note that $d = 1$, since the addition in Figure 8 is performed by the channel itself (and this in $\mathbb{C}$). Therefore, at the receiver a modulo operation is taken first.

[2]This principle of exchanging information using several iterations is also called the *Turbo-principle*

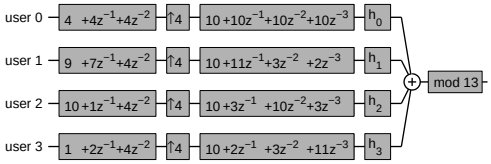

Fig. 8. DS-CDMA system with 4 users. The error-correcting code and spreading code are jointly designed using the techniques in this paper such that the overall code is $\mathcal{R}(12, 4)$ in $GF(13^1)$. h_m are one-tap channels which do not destroy the RS code, and for which one should compensate using a proper equalization.

V. Conclusion

This paper focuses on the role of filterbanks in coding applications. Our discussion begins with STFT filterbanks. In most applications this filterbank is explicitly designed to ensure that the filtering operations are linear. However, if the number of bands is not chosen to be large enough, this filterbank acts as a periodically time varying system. Though this is normally considered an undesirable artifact, it is this periodicity that is exploited to build critically subsampled filterbanks for the family of BCH codes. In the case of RS codes, this paper proves that a proper distribution of its roots over the subbands is the key element in constructing such a filterbank. For the more general case of BCH codes, it is shown that they can be broken into a sum of critically subsampled filterbanks. Finally, two possible applications are briefly mentioned. The first one discusses a SISO RS decoder based on a filterbank decomposition. The second one explains how such filterbanks can be used to jointly design the spreading and error correcting codes of a DS-CDMA system.

References

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

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

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

[4] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math*, vol. 37, no. 2, pp. 358–369, Oct. 1979.

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

[6] G. Van Meerbergen, M. Moonen, and H. De Man, "Soft-In Soft-Out Reed-Solomon decoding using Critically Subsampled Filterbanks," in *Submitted to the IEEE Information Theory Workshop on Coding and Complexity (ITW), Rotorua, New-Zealand*, Aug 29-Sept 1 2005.