COMBINING REED-SOLOMON CODES AND OFDM FOR IMPULSE NOISE MITIGATION: RS-OFDM

Geert Van Meerbergen ⋆*, Marc Moonen* ⋆

⋆ E.E. Dept., ESAT/SISTA, K.U.Leuven
Kasteelpark Arenberg 10, 3001 Leuven, Belgium
gvanmeer,moonen@esat.kuleuven.be

Hugo De Man ⋆†

† IMEC
Kapeldreef 75, 3001 Leuven, Belgium
deman@imec.be

ABSTRACT

In this paper, a joint solution to the design problem of a good error-correcting code for an OFDM scheme with a low Peak to Average Power Ratio (PAPR) in the case of impulse noise is presented. The PAPR problem is tackled by decomposing the circulant channel matrix into parallel channels by using DFT matrices in a Galois field of odd characteristic, rather than in a complex field. The modulo operation inherent to this field then limits the power of the modulated signal. More importantly, it is explained how this OFDM scheme can be seamlessly merged with a Reed-Solomon (RS) code, which due to its maximal Hamming distance is the preferred code for impulse noise cancellation. The overall scheme, referred to as RS-OFDM, shows an error correcting code that is matched to the OFDM-modulator. It is shown that the optimal Hamming distance of the RS code is preserved not only by the OFDM modulator, but also by the channel.

1. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) is a well known technique in wireline as well as in wireless communications. OFDM (DMT) is adopted in many standards like DAB, DVB, Wireless LAN and xDSL. It has several advantages over single carrier systems, e.g. it is resistant against dispersion in the transmission channels, and efficient hardware implementations exist for the equalizer and the DFT. Moreover, coded OFDM allows the exploitation of frequency diversity and it provides a greater immunity to impulse noise and fast fades. One of the major drawbacks of OFDM is its high Peak to Average Power Ratio (PAPR). This limits the transmission range and requires that the transmit amplifiers have a large input power back-off. In many low-cost operations, the disadvantages outweigh all the benefits of OFDM [1].

The idea of jointly solving the PAPR and the error correcting code (ECC) design problem is first adressed using block codes in [2]. Similarly, Davis *et al.* [3] obtain a class of low PAPR codes with a large minimum distance based on cosets of Reed-Muller codes. In this paper, the PAPR problem is tackled in yet another way; The usually complex field DFT operation is replaced by a DFT in a finite field. To be compatible with the channel, a Galois field of odd characteristic is chosen. The modulo operation inherent to this field then yields a low PAPR. More importantly, the finite field DFT operation can be seen as part of a Reed-Solomon (RS) code. Therefore, we rely on a critically subsampled filterbank representation for RS codes [4]. The OFDM modulator and ECC become effectively merged to yield one large RS code.

Geert Van Meerbergen is a Research Assistant with the F.W.O. Vlaanderen. 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, Research Project FWO nr.G.0196.02. The scientific responsibility is assumed by its authors.

It is also important to mention the relationship between OFDM and real-valued BCH codes as described in [5, 6]. Our methods differ from [6] in many respects: In our method, the DFT size is typically much smaller than the block length of the code. This leads to a scheme separating the coding aspect (addition of redundancy) from the modulator, which resembles a normal OFDM modulator. As a second difference, in our approach, all operations are performed in a Galois field of odd characteristic, i.e. $GF(p)$ with p a prime number. To be compliant with the channel operating in the complex field, the isomorphism between $GF(p)$ and the integers modulo p will be called upon.

The paper is organized as follows: In section 2, the basic OFDM principles are briefly recalled, and it is explained how (when) a channel can be diagonalized in the Galois field. In the next section, the filterbank structure of an RS code is presented. In section 4, it is explained how the filterbank merges with the OFDM modulator. The performance gain is illustrated using simulations. In this section, it is also briefly discussed how the receiver can be simplified.

2. OFDM SYSTEM MODEL

The core of the OFDM architecture is a block based system, processing data in a block-wise fashion. A data block $\mathbf{x}$ is modulated using the inverse M-point discrete Fourier transform (IDFT), obtaining $\mathbf{y}$, and is prepended with a cyclic prefix of length L. The multi-path propagation channel is modeled as a finite impulse response filter $h(z^{-1}) = h_0 + h_1 z^{-1} + h_2 z^{-2} + \dots$ with noise added. Assuming perfect symbol and block synchronization and that the channel order is not larger than L, inter block interference is avoided such that a $\tilde{\mathbf{y}}$ is received which is specified as follows:

$$\mathbf{y} = \mathbf{F}_M^{-1}\mathbf{x} \tag{1}$$

$$\tilde{\mathbf{y}} = \underbrace{\left[\mathbf{O}_{M,L} \mid \mathbf{I}_M\right]\mathbf{H}\begin{bmatrix}\mathbf{I}_L \mid \mathbf{0}_{L,M-L}\\ \mathbf{I}_M\end{bmatrix}}_{\tilde{\mathbf{H}}}\mathbf{y} + \mathbf{n} \tag{2}$$

$$\tilde{\mathbf{x}} = \mathbf{F}_M\tilde{\mathbf{y}} \tag{3}$$

In these equations, $\mathbf{F}_M$ represents an $M \times M$ DFT matrix with $[\mathbf{F}_M]_{i,j} = W_M^{i,j}$ and W_M is an M-th root of unity: $W_M = e^{2\pi j/M}$. The channel matrix $\mathbf{H}$ is defined as

$$\mathbf{H} = \begin{bmatrix} h_0 & & & & & \\ h_1 & \ddots & & & & \\ \vdots & \ddots & \ddots & & & \\ h_L & & \ddots & \ddots & & \\ & \ddots & & \ddots & \ddots & \\ & & h_L & \dots & h_1 & h_0 \end{bmatrix} \tag{4}$$

The cyclic prefix (CP) insertion and removal transforms the channel matrix $\mathbf{H}$ into a circulant matrix $\tilde{\mathbf{H}}$ which is diagonalized by $\mathbf{F}_M$ and $\mathbf{F}_M^{-1}$, i.e.

$$\tilde{\mathbf{E}} = \mathbf{F}_M \tilde{\mathbf{H}} \mathbf{F}_M^{-1} \tag{5}$$

Hence, an estimate of $\mathbf{x}$ can be obtained as

$$\hat{\mathbf{x}} = \tilde{\mathbf{E}}^{-1}\tilde{\mathbf{x}} = \mathbf{x} + \tilde{\mathbf{E}}^{-1}\mathbf{F}_M\mathbf{n}$$

Considering the transmission of multiple blocks, the baseband discrete-time model of an OFDM system is seen as a transmultiplexer structure in Figure 1. This representation makes it easier to make the link with the filterbanks further on. Moreover, the polyphase decomposition allows us to properly describe the block based system. Now, an input sequence $x(z^{-1}) = x_0 + x_1 z^{-1} + x_2 z^{-2} + \ldots$ is written as a block of M samples using its M-fold polyphase components:

$$\mathbf{x}_l^{[M]}(z^{-1}) = \sum_{k=0}^{\infty} x_{l+kM} z^{-k} \tag{6}$$

These polyphase components can be stacked into a vector

$$\mathbf{x}^{[\mathbf{M}]}(z^{-1}) = \left[x_0^{[M]}(z^{-1}) \quad x_1^{[M]}(z^{-1}) \quad \ldots \quad x_{M-1}^{[M]}(z^{-1}) \right]^T \tag{7}$$

Note that in the case of a single transmitted block, all polyphase components are scalars again and $\mathbf{x}^{[\mathbf{M}]} = \mathbf{x} = [x_0 x_1 \ldots x_{M-1}]^T$, just as before. Equations 1- 3 can now be rewritten using their polyphase components by simply replacing, e.g., $\mathbf{x}$ by $\mathbf{x}^{[\mathbf{M}]}(z^{-1})$. To satisfy $\mathbf{y}^{[\mathbf{M}]} = \mathbf{F}_M^{-1}\mathbf{x}^{[\mathbf{M}]}$ (Equation 1) and $\mathbf{x}^{[\tilde{\mathbf{M}}]} = \mathbf{F}_M \mathbf{y}^{[\tilde{\mathbf{M}}]}$ (Equation 3), the synthesis (analysis) filters need to be defined as

$$c_m(z^{-1}) = \sum_{m'=0}^{M-1} W_M^{-mm'} z^{-m'} \tag{8}$$

$$a_m(z^{-1}) = \sum_{m'=0}^{M-1} W_M^{mm'} z^{-m'}. \tag{9}$$

Assuming that the channel is a Galois field channel, it can be similarly diagonalized if the M-th root of unity (defining the DFT-matrix) is re-defined accordingly:

$$W_M = \alpha^{(p-1)/M} \tag{10}$$

In this equation, α is a primitive $(p-1)$-th root of unity. Also note that the M-th root of unity (and thus the DFT matrix) only exists if M and $p-1$ are not coprime.

The channel however is always defined in the complex field. Nevertheless, by choosing a Galois field of odd characteristic $GF(p)$, and by applying a modulo operation at the receiver, the diagonalization of a channel in the complex field can indeed be obtained with finite field DFT matrices. This is due the well known fact that there exists an isomorphism between the elements of $GF(p)$ and the integers modulo p. Therefore, an addition (multiplication) performed by the channel (in the complex field) can be seen as an addition (multiplication) in $GF(p)$ if a modulo is taken at the output of the channel. In the rest of the section, this is explained in more detail.

The Galois field $GF(p)$ is uniqely defined by its primitive polynomial $s(x) = s_0 + x$. The primitive $p-1$-st root of unity α is a root of this primitive polynomial:

$$\alpha = -s_0 \bmod p \tag{11}$$

This equation defines the isomorphism between the elements of the Galois field and the integers modulo p:

$$\underline{a} = \alpha^i \rightarrow a = (-s_0)^i \bmod p \tag{12}$$

From a notational point of view, note that the Galois field representation of a (matrix) variable a is denoted by $\underline{\mathbf{a}}$. To limit the power of the signal, it is preferred to bound the integers between $-(p-1)/2 \ldots (p-1)/2$ instead of $0 \ldots p-1$. Hence, the modulo operation $x \bmod p$ is replaced by $(x)_p$:

$$(x)_p = \text{round}(x - p\lfloor (x + p/2)/p \rfloor). \tag{13}$$

Assume the channel coefficients h_i can be appropriately quantized to integers between $-(p-1)/2 \ldots (p-1)/2$ which incurs only a small quantization error if p is chosen large enough[1]. These coefficients define the matrix $\tilde{\mathbf{H}}$ which can be diagonalized in the Galois field:

$$\underline{\tilde{\mathbf{E}}} = \underline{\mathbf{F}}_M \underline{\tilde{\mathbf{H}}} \underline{\mathbf{F}}_M^{-1} \tag{14}$$

This decomposition can then be used to make an alternative OFDM scheme:

$$\underline{\mathbf{y}}^{[\mathbf{M}]} = \underline{\mathbf{F}}_M^{-1} \underline{\mathbf{x}}^{[\mathbf{M}]} \tag{15}$$

$$\tilde{\mathbf{y}}^{[\mathbf{M}]} = \left(\tilde{\mathbf{H}} \mathbf{y}^{[M]} + \mathbf{n} \right)_p \tag{16}$$

$$\underline{\tilde{\mathbf{x}}}^{[\mathbf{M}]} = \underline{\mathbf{F}}_M \tilde{\mathbf{y}}^{[\mathbf{M}]} \tag{17}$$

$$\underline{\hat{\mathbf{x}}}^{[\mathbf{M}]} = \underline{\tilde{\mathbf{E}}}^{-1} \underline{\tilde{\mathbf{x}}}^{[\mathbf{M}]} \tag{18}$$

In the above equations, all operations are Galois field operations, except Equation 16 which uses the integer representation $\mathbf{y}^{[M]}$ as input to the channel. After taking the modulo-like operation, the result $\tilde{\mathbf{y}}^{[\mathbf{M}]}$ is returned to the Galois field for equalization in Equation 18. The Galois field counterpart of Equation 16 is

$$\underline{\tilde{\mathbf{y}}}^{[\mathbf{M}]} = \underline{\tilde{\mathbf{H}}} \underline{\mathbf{y}}^{[M]} + \underline{\mathbf{n}}' \text{ with } \mathbf{n}' = (\mathbf{n})_p \tag{19}$$

Note that the Galois field operations (modulo operations) ensure the low PAPR of the modulated signal. In addition, note that this modulo operation has the same function as the modulo operation in a dirty paper coding scheme by limiting the power of the signal.

Example 1 *In this example, GF(13) is chosen ($p = 13$) with primitive polynomial $11 + x$. The primitive $p-1$-th root of unity α is a root of this primitive polynomial:*

$$\alpha = -11 \bmod 13 = 2 \tag{20}$$

The isomorphism between the elements of the Galois field and the integers modulo 13 can now be constructed:

0	1	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}
0	1	2	4	-5	3	6	-1	-2	-4	5	-3	-6

Choosing $M = 3$, the DFT-matrix

$$\underline{\mathbf{F}}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^4 & \alpha^8 \\ 1 & \alpha^8 & \alpha^4 \end{bmatrix} \qquad \mathbf{F}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 3 & -4 \\ 1 & -4 & 3 \end{bmatrix} \tag{21}$$

can be used to decompose a circulant matrix $\tilde{\mathbf{H}}$ as follows:

$$\left(\underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & 3 & -4 \\ 1 & -4 & 3 \end{bmatrix}}_{\mathbf{F}_3} \underbrace{\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}}_{\tilde{\mathbf{H}}} \underbrace{\begin{bmatrix} -4 & -4 & -4 \\ -4 & 3 & 1 \\ -4 & 1 & 3 \end{bmatrix}}_{\mathbf{F}_3^{-1}} \right)_{13} = \underbrace{\begin{bmatrix} 6 & & \\ & -5 & \\ & & 2 \end{bmatrix}}_{\tilde{\mathbf{E}}}$$

[1] Note that an extra scaling does not change the results, e.g. the channel coefficients can be bounded between -1..1 if an extra scaling $(p-1)/2$ is applied.

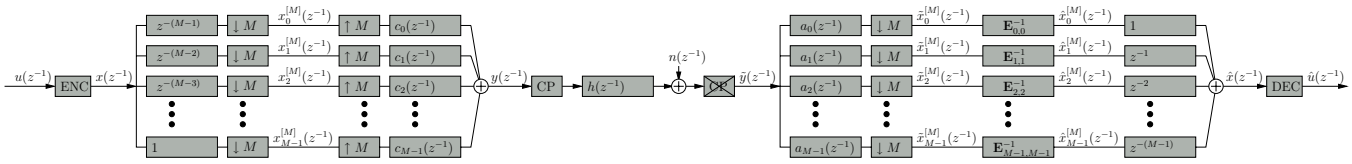

Fig. 1. Transmultiplexer structure of a baseband discrete-time model of an OFDM system.

In Equation 16, it is seen that a modulo operation is performed which - as we will now show - limits the applicability of this scheme in the case of *AWGN noise*. If the noise is larger than 0.5, a symbol error is always made. If a specific band however has a high SNR, e.g. if the corresponding coefficient of $\tilde{\mathbf{E}}$ reaches its maximum value $(p-1)/2$, one would expect to tolerate noise as large as $(p-1)/4$. In fact, in a classical OFDM scheme, this is obtained by the equalizer which in the complex field would down scale the noise by a factor of $(p-1)/2$. In the Galois field however, the noise will never be down scaled, thereby not exploiting the frequency bands with a high SNR. In the case of *impulse noise* however, the situation is completely different and the modulo in Equation 16 can be taken without compromising performance. To tackle impulse noise, error correcting coding must be applied. To minimize the word error rate by a (hard) ML decoder, the coded performance is determined by the Hamming distance of the code. The rest of this paper chooses RS codes given their Maximum Distance Separable (MDS) character. It is seen how these codes can seamlessly be integrated with the OFDM scheme presented. Therefore, we first explore the filterbank character of RS codes.

3. FILTERBANKS AND REED-SOLOMON CODES

Reed-Solomon codes are block-based error correcting codes with a wide range of applications in digital communications and storage. RS codes are non-binary codes; that is, we describe them in terms of symbols (in $GF(p^d)$) rather than bits: A block of κ data word symbols is encoded into a codeword of length ν with $\nu = p^d - 1$. Each polynomial associated with a codeword has a number of *consecutive* powers of $\alpha^i, i = 0..\nu - \kappa + 1$ among its roots. In [4], the following theorem is proven, which states that a critically subsampled filterbank representation exists for each RS.

Theorem 1 *Let $\mathcal{R}(\nu, \kappa, \nu - \kappa + 1)$ 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 M as shown in Figure 2. The synthesis bank is defined the same way as in Equation 8. This filterbank will implement the RS code $\mathcal{R}(\nu, \kappa, \nu-\kappa+1)$ if a root α^i of $\mathcal{R}(\nu, \kappa, \nu-\kappa+1)$ is assigned to subband m if and only if $i \bmod M = m$. Stated otherwise,*

$$\underline{d}_m(\alpha^i) = 0 \Leftrightarrow \exists j \in \mathbb{Z} | i = Mj + m \tag{22}$$

If a dataword $\underline{u}(z^{-1})$ (length κ) is fed into the filterbank, it is (equally) split by the analysis bank into its M polyphase components $\underline{x}_m^{[M]}(z^{-1})$. If κ and M are coprime, then the analysis bank ensures that the bands with one root less receive one input sample more (See the example). Next, the subband filters $\underline{d}_m(z^{-1})$ add redundancy to each $\underline{x}_m^{[M]}(z^{-1})$, yielding exactly ν/M subband variables $\underline{x}_m^{[M]}(z^{-1})$. Finally, the subband samples $\underline{x}_m^{[M]}(z^{-1})$ are combined in the DFT-synthesis bank such that the output of the filterbank $\underline{y}(z^{-1})$ is a valid RS codeword. From a matrix point of view, the filterbank operations can be written as

$$\tilde{\underline{\mathbf{y}}}^{[\mathbf{M}]} = \underline{\mathbf{F}}_M^{-1} \text{diag}\left(\underline{\mathbf{d}}(z^{-M})\right) \underline{\mathbf{u}}^{[\mathbf{M}]} \tag{23}$$

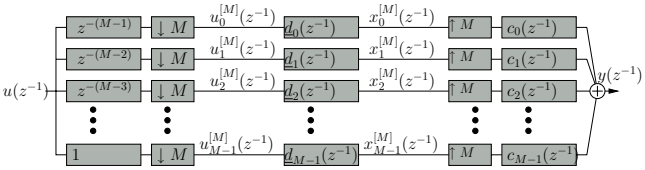

Fig. 2. Critically subsampled filterbank with M bands. According to theorem 1, each RS code (as long as its block length is not prime) can be represented as such a filterbank. Note the correspondence with the synthesis bank in Figure 1.

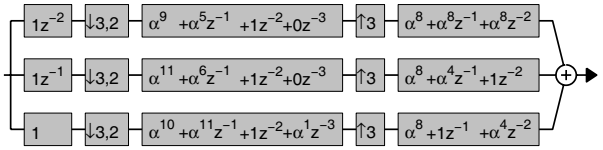

Fig. 3. Critically subsampled filterbank with 3 bands implementing $\mathcal{R}(12, 5, 8)$ (example 2).

Example 2 *Since Galois fields of prime characteristic are of special interest to us ($d = 1$), let us construct a filterbank which implements $\mathcal{R}(12, 5, 8)$ in GF(13). Its roots are chosen $\{\alpha^k\}_{k=2...8}$. Hence, each codeword is a multiple of the generator polynomial*

$$\underline{g}(z^{-1}) = \prod_{k=2}^{8} (z^{-1} - \alpha^k) \tag{24}$$

According to the theorem, these roots $\alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8$ are distributed among the polynomials $\underline{d}_m(z^{-1})$ as follows:

$$\begin{aligned} \alpha^3, \alpha^6 &\Leftarrow \underline{d}_0(z^{-1}) = \alpha^9 + \alpha^5 z^{-1} + z^{-2} \\ \alpha^4, \alpha^7 &\Leftarrow \underline{d}_1(z^{-1}) = \alpha^{11} + \alpha^6 z^{-1} + z^{-2} \\ \alpha^2, \alpha^5, \alpha^8 &\Leftarrow \underline{d}_2(z^{-1}) = \alpha^{10} + \alpha^{11} z^{-1} + z^{-2} + \alpha^1 z^{-3} \end{aligned}$$

The filterbank so obtained is shown in Figure 3. In this case, each band receives 2 polyphase samples in $\underline{u}_m^{[3]}(z^{-1})$, except the last band, which receives one. Next, the subband filters expand each $\underline{u}_m^{[3]}(z^{-1})$ to 4 subband samples $\underline{x}_m^{[3]}(z^{-1})$ per band. This is possible since the missing x sample in the last band is compensated by a longer subband filter $\underline{d}_2(z^{-1})$. Finally, the subband samples $\underline{x}_m^{[3]}(z^{-1})$ are combined in the DFT-synthesis bank such that the output of the filterbank $\underline{y}(z^{-1})$ is a valid RS codeword.

4. COMBINING RS AND OFDM:RS-OFDM

In the case of impulse noise, RS codes are normally applied around the core OFDM system as shown in Figure 1. Typically, the optimality of the overall system (combination ECC and modulator) is never questioned. However, with the filterbank representation of RS

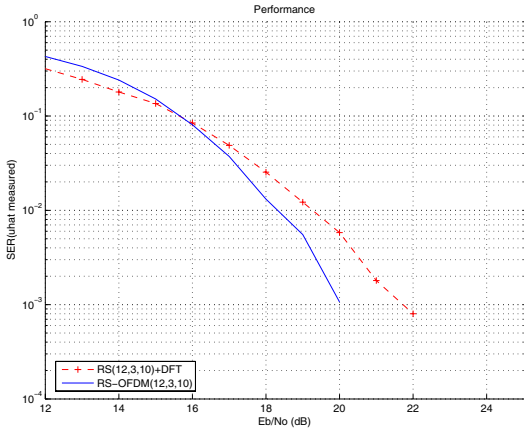

Fig. 4. Comparison of a concatenated scheme of $\mathcal{R}(12,3,10)$ followed by an OFDM modulator and the RS-OFDM scheme based on $\mathcal{R}(12,3,10)$. The RS-OFDM scheme has an overall Hamming distance of 10 compared to 4 for the concatenated scheme.

codes in mind, the DFT synthesis bank of an OFDM modulator (in the Galois field) is seen to be part of the RS code. Therefore, it is proposed to merge the two schemes, leading to a new scheme referred to as RS-OFDM. Mathematically, Equations 15 and 23 can be merged leading to

$$\underline{\tilde{\mathbf{y}}}^{[\mathrm{M}]} = \underline{\tilde{\mathbf{H}}}\underline{\mathbf{F}}_M^{-1}\mathrm{diag}\left(\underline{\mathbf{d}}(z^{-M})\right)\underline{\mathbf{u}}^{[\mathrm{M}]} + \underline{\mathbf{n}}' \tag{25}$$

In RS-OFDM using $\mathcal{R}(\nu,\kappa,\nu-\kappa+1)$, redundancy is added to the polyphase components of a dataword $u(z^{-1})$ before it is send into the DFT synthesis bank. This redundancy is added in such a way that the output of the synthesis bank is a RS codeword. Instead of concatenating an RS code with an OFDM modulator, the overall Hamming distance of the RS code is preserved doing RS-OFDM. This is further illustrated in the following example comparing a normal coded OFDM system vs. RS-OFDM.

Example 3 *In this example, a comparison is made between a typical concatenated scheme of a non-systematic* $\mathcal{R}(12,3,10)$ *(using* $g(z^{-1})$ *similar to Equation 24) followed by an OFDM modulator and the RS-OFDM scheme based on the same* $\mathcal{R}(12,3,10)$*. Both are using the same hard-ML decoder, using 13-PAM modulation. The RS-OFDM scheme has an overall Hamming distance of 10 compared to 4 for the concatenated scheme, resulting in a 2dB gain (Figure 4). This performance loss of the concatenated scheme is explained by the cancellation of the DFT inherent to the RS code with the DFT in the OFDM modulator. Also if the latter uses a DFT in the complex field, the Hamming distance is still 4.*

In the previous example, it is explained that the Hamming distance of the RS code is not destroyed by the OFDM modulator. In this paragraph, we will see that also the channel can not reduce the Hamming distance of the code. Recalling Equation 25

$$\underline{\tilde{\mathbf{y}}}^{[\mathrm{M}]} = \underline{\tilde{\mathbf{H}}}\underline{\mathbf{F}}_M^{-1}\mathrm{diag}\left(\underline{\mathbf{d}}(z^{-M})\right)\underline{\mathbf{u}}^{[\mathrm{M}]} + \underline{\mathbf{n}}' \tag{26}$$

$$= \underline{\mathbf{F}}_M^{-1}\underline{\tilde{\mathbf{E}}}\mathrm{diag}\left(\underline{\mathbf{d}}(z^{-M})\right)\underline{\mathbf{u}}^{[\mathrm{M}]} + \underline{\mathbf{n}}' \tag{27}$$

$$= \underline{\mathbf{F}}_M^{-1}\mathrm{diag}\left(\underline{\mathbf{d}}(z^{-M})\right)\underbrace{\underline{\tilde{\mathbf{E}}}\underline{\mathbf{u}}^{[\mathrm{M}]}}_{\underline{\tilde{\mathbf{u}}}^{[\mathrm{M}]}} + \underline{\mathbf{n}}' \tag{28}$$

The last equation shows that the same $\tilde{\mathbf{y}}^{[\mathrm{M}]}$ can be obtained by encoding a different dataword $\underline{\tilde{\mathbf{u}}}^{[\mathrm{M}]}$. In other words, the channel output is also a codeword (up to the noise). This means that at the receiver, one can first e.g. use *Berlekamp-Massey's algorithm* to find the ML-solution for $\underline{\tilde{\mathbf{u}}}^{[\mathrm{M}]}$, and then perform an equalization on the data according to

$$\underline{\tilde{\mathbf{E}}}\underline{\mathbf{u}}^{[\mathrm{M}]} = \underline{\tilde{\mathbf{u}}}^{[\mathrm{M}]} \tag{29}$$

In this case, equalization and decoding are separated without compromising optimality (no joined decoding-equalization necessary) and can even be swapped.

As a final remark, note the low PAPR of the p-PAM constellation that is transmitted. It is also worth mentioning that the techniques can be extended to QAM constellations. In this case, $GF(p^2)$ will be used. However, a detailed explanation is beyond the scope of this paper.

5. CONCLUSION

In this paper, an OFDM scheme is presented where the circulant channel matrix is decomposed using DFT matrices in a Galois field. In order to be compatible with the finite field operations, the channel is assumed to be quantized and a modulo operation must be added at the receiver. In the case of impulse noise, this modulo operation does not compromise system performance. Using a filterbank representation of an RS code, it is explained how this OFDM scheme can be seamlessly merged with a Reed-Solomon code, designed for impulse noise cancellation. The overall scheme shows an RS code which matches the OFDM-modulator. Simulations show the advantage of the jointly designed RS-OFDM scheme. It is shown that the optimal Hamming distance of the RS code is preserved not only by the OFDM modulator, but also by the channel. In addition to the performance gain, an RS-OFDM scheme shows a reduced PAPR. Moreover the complexity can be reduced since the whole RS-OFDM system can be seen as one large RS code, such that low complexity RS decoders can be applied in practice.

6. REFERENCES

[1] K.G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios," *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 1974–1987, Sept. 2000.

[2] A.E. Jones, T.A. Wilkinson, and S.K. Barton, "Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes," *Electronics Letters*, vol. 30, no. 25, pp. 2098–2099, Dec 1994.

[3] J.A. Davis and J. Jedwab, "Peak-to-mean power control in ofdm, golay complementary sequences, and reed-muller codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2397 – 2417, Nov 1999.

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

[5] J. Wolf, "Redundancy, the discrete fourier transform, and impulse noise cancellation," *IEEE Trans. Commun.*, vol. 31, no. 3, pp. 458 – 461, 1983.

[6] Jr. Marshall, T., "Coding of real-number sequences for error correction: A digital signal processing problem," *IEEE J. Select. Areas Commun.*, vol. 2, no. 2, pp. 381 – 392, Mar 1984.