PUNCTURED 8-PSK TURBO-TCM TRANSMISSIONS USING RECURSIVE SYSTEMATIC CONVOLUTIONAL GF$\left(2^N\right)$ ENCODERS

Calin Vladeanu[†] *and Safwan El Assad*[‡]

[†]Faculty of Electronics, Telecommunications, and Information Theory/Telecommunications Department,
University Politehnica of Bucharest
1-3 Iuliu Maniu, 061071, Bucharest, Romania
phone: +(40) 751 804068, fax: +(40) 21 4024765, email: calin@comm.pub.ro
[‡]École Polytechnique de l'Université de Nantes/IREENA
Rue Christian Pauc, 44306 Nantes, cedex 3, France
phone: +(33) 2 40 68 30 36, fax: +(33) 2 40 68 32 32, email: safwan.elassad@univ-nantes.fr

ABSTRACT

A new Galois field GF$\left(2^N\right)$ structure for designing recursive systematic convolutional (RSC) encoders is presented in this article. The proposed RSC encoders are used as components of a parallel-concatenated Turbo trellis coded modulation (TTCM) scheme. The GF$\left(2^N\right)$ RSC encoders include a nonlinear function named left-circulate (LCIRC), which is performing a left circulation over the N bits representation word. A closed-form expression was found for the minimum Euclidian distance of rate $(N-1)/N$ LCIRC-RSC encoders for $\left(2^N\right)$-ary PSK-TCM, and its values show that these RSC-LCIRC encoders are optimum, having the same performances as the corresponding conventional binary encoders. However, the RSC-LCIRC encoders are less complex than the corresponding binary encoders for a given encoding rate. TTCM transmission schemes with optimum RSC-LCIRC component encoders are investigated using the iterative symbol-by-symbol log-MAP decoding algorithm and symbol puncturing. The bit error rate (BER) is estimated by simulation for the proposed TTCM scheme with 8-PSK modulation when transmitting over additive white Gaussian noise (AWGN) channel.

1. INTRODUCTION

Channel encoded transmissions are used in all systems nowadays. Several types of channel encoding methods were proposed during the last decades. Almost all coding methods known in the literature use linear functions. The nonlinear functions were used lately in chaotic sequence generators to increase the security of communications systems. In [1] Frey proposed a nonlinear digital infinite impulse response (IIR) filter for secure communications. The Frey filter contains a nonlinear function named left-circulate function (LCIRC), which is used as typical basic accumulator operation in microprocessors. The above mentioned work considered the Frey encoder as a digital filter, operating over Galois field GF$\left(2^N\right)$. In [2] it was demonstrated that the Frey encoder with finite precision (wordlength of N bits) presented in [1] is a recursive convolutional encoder operating over GF$\left(2^N\right)$). New methods for enhancing the performances of the phase shift keying - trellis-coded modulation (PSK-TCM) transmissions over a noisy channel using the recursive convolutional LCIRC (RC-LCIRC) encoders were proposed in [3]. These encoders follow the rules proposed by Ungerboeck [4] for defining optimum TCM by proper set partitioning. The turbo coding scheme introduced by Berrou and Glavieux in [5] allow communications systems performances close to the Shannon limit, by concatenating in parallel recursive convolutional encoders in the transmitter and using iterative decoding algorithms in the receiver. Turbo schemes were developed as well for the TCM schemes [6]-[9].

In the present work, an improved version of the RC-LCIRC encoder from [3] is proposed. The encoder improvements consist in making it systematic and adapting it for a parallel turbo TCM (TTCM) transmission scheme. As compared to the TTCM scheme analyzed in [9] operating at low coding rates due to the lack of puncturing, the present paper introduces specific interleaving and puncturing methods for TTCM scheme. Moreover, the conventional logarithmic Maximum A-posteriori Probability (log-MAP) decoding algorithm is modified to operate in a symbol-by-symbol manner for punctured received sequences, following the method presented in [6] and [7]. The optimum set partitioning method is used for PSK punctured TTCM schemes. The performances of this scheme are analyzed in case of transmitting over a channel with additive white Gaussian noise (AWGN).

The paper is organized as follows. Section 2 is presenting the recursive systematic convolutional LCIRC (RSC-LCIRC) encoder operating over Galois field GF$\left(2^N\right)$ and the optimum set partitioning for PSK modulation. In Section 3, a parallel TTCM transmission scheme using RSC-LCIRC component encoders with symbol puncturing is presented. A symbol-by-symbol log-MAP algorithm is used for the iterative detection. The simulated bit error rate (BER) performances in AWGN are presented and analyzed in Section 4 for the punctured 8-PSK TTCM transmission using three different interleaver sizes. Finally, the conclusions are drawn and perspectives are presented in Section 5.

2. OPTIMUM RSC-LCIRC ENCODER FOR TCM SCHEMES

In this section, a new family of RSC encoders operating over Galois field GF$\left(2^N\right)$ and their use for op-

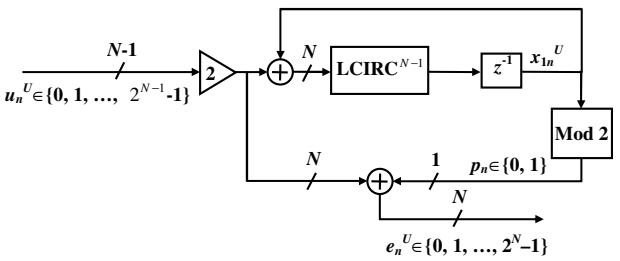

Figure 1: Rate $(N-1)/N$ optimum GF(2^N) RSC-LCIRC encoder.

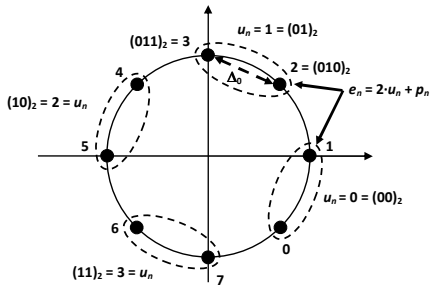

Figure 2: Optimum set partitioning for punctured 8-PSK TTCM.

timum TCM schemes are presented. The main component of the RSC encoder presented in the sequel is the nonlinear LCIRC function introduced by Frey in [1] for chaotic encryption. The use of the LCIRC function for channel encoding was considered for the first time in [2]. Optimum encoders using the LCIRC function for TCM schemes were introduced in [3]. However, despite being characterized by optimum Euclidian distances, these recursive convolutional encoders are non-systematic. Therefore, the coding performances of these non-systematic encoders are not optimum when used in turbo schemes. In this section, we introduce a new encoder operating over Galois field GF$\left(2^N\right)$, using the LCIRC function, which is systematic, i.e. the encoder output value specifies explicitly the input value. Let us denote by N the wordlength used for binary representation of each sample. The LCIRC function performs a bit rotation by placing the most significant bit to the least significant bit, and shifting the other $N-1$ bits one position to a higher significance. The block scheme for a rate $(N-1)/N$ optimum RSC-LCIRC encoder, using one delay element and the LCIRC function is presented in Fig. 1. For each moment n, u_n represents the input data sample, x_{1n} denotes the delay output or the encoder current state, and e_n is the output sample. The superscript U denotes that all the samples are represented in unsigned N bits wordlength, i.e., $u_n^U \in \left[0, 2^{N-1}-1\right]$, $e_n^U \in \left[0, 2^N-1\right]$. The encoding rate for the encoder in Fig. 1 is the ratio between the input wordlength $N_{in} = N-1$ and the output wordlength N, i.e., $R = N_{in}/N$ [2]. LCIRC^{N-1} represents the LCIRC function application for $N-1$ times consecutively. Both adders and the multiplier are modulo-2^N operators. The modulo-2 block extracts the least significant bit, denoted by p_n, from the encoder current state value, x_{1n}. p_n is the parity bit for the systematic rate $(N-1)/N$ encoder.

It is important to demonstrate that the encoder is systematic, i.e., the encoder output binary representation codeword e_n^U includes the representation codeword of the encoder input u_n^U. Hence, the output is obtained by shifting the $N-1$ bits of the input representation codeword by one position to a higher significance, and adding the parity bit p_n to the least significant position, a position that was left empty inside the N bits output codeword by the previously mentioned shifting. The one position shifting presented above is equivalent by a multiplication by 2 in the GF$\left(2^N\right)$ field. Therefore, the encoder output value e_n^U is given by the following

Table 1: Minimum 2^N-ary PSK-TCM distances as function of N for optimum GF(2^N) RSC-LCIRC encoders.

N	R	Modulation	d_E^2
2	1/2	QPSK	10
3	2/3	8-PSK	≈ 4.5858
4	3/4	16-PSK	≈ 1.3238

GF$\left(2^N\right)$ equation:

$$e_n^U = 2 \cdot u_n^U + p_n = 2 \cdot u_n^U + x_{1n}^U \bmod 2 \qquad (1)$$

The trellis complexity of the codes generated with the scheme in Fig. 1 increases with the wordlength N, because the number of trellis states grows exponentially with the output wordlength, i.e., 2^N, while the number of transitions originating from and ending in the same state grows exponentially with the input wordlength, i.e., 2^{N-1}.

The optimum set partitioning for the punctured TTCM scheme was introduced in [6], and has two features. First of all, the set partitioning follows the Ungerboeck optimum set partitioning rules from [4], and secondly, the constellation points associated to the same group of $N-1$ systematic information bits, i.e., to the same input symbol u_n^U, but differing in the least significant bit, i.e., the parity bit p_n, should be placed at the minimum distance in the set, $\Delta_{0,2^N-\text{ary modulation}}$. Following these two requirements, the optimum set partitioning rule for 8-PSK is depicted in Fig. 2. The first feature maximizes the minimum Euclidian distance of the component TCM code, while the second feature minimizes the distance between elements of the subsets associated to identical systematic bits, denoted by ovals in Fig. 2, for the global punctured TTCM code. It can be easily demonstrated that the minimum Euclidian distance for the 2^N-ary TCM component encoder presented in Fig. 1, using the optimum constellation as in Fig. 2, has the following expression:

$$d_{E,R=(N-1)/N}^2 = 2 \cdot \Delta_{1,2^N-\text{PSK}}^2 + \Delta_{0,2^N-\text{PSK}}^2 \qquad (2)$$

In Table 1, there are presented a few values of the minimum distances of the TCM encoder in Fig. 1 for different values of N and for the PSK constellation. The associated coding rates are presented in the second column. It can be easily noticed from (2) that all the rate

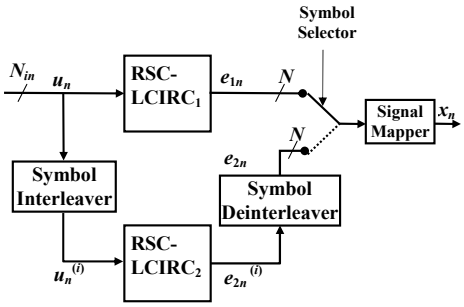

Figure 3: TTCM transmitter with RSC-LCIRC encoders and symbol puncturing.

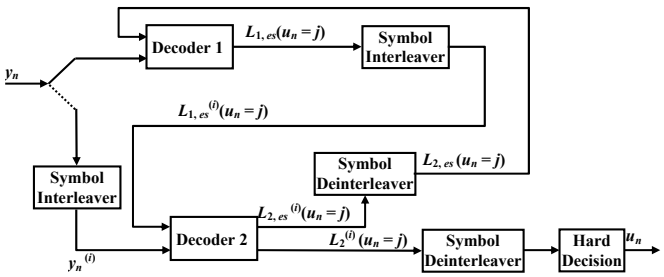

Figure 4: TTCM receiver using symbol log-MAP decoders and puncturing.

$(N-1)/N$, for any N value, the optimum RSC-LCIRC encoders are offering the same minimum distance as the corresponding binary optimum encoders determined by Robertson in [6], and Vucetic in [7]. In addition, the $\mathrm{GF}(2^N)$ optimum RSC-LCIRC encoders are less complex than the corresponding binary encoders in terms of memory usage. The memory size of the binary encoders increases logarithmically with the number of states in the trellis, while the $\mathrm{GF}(2^N)$ optimum RSC-LCIRC encoders include only one delay element, no matter what the trellis complexity is. As another advantage of these encoders, we can also mention the Euclidian distance compact expression (2) as a function of N.

3. RSC-LCIRC ENCODER IN TURBO-TCM SCHEME

Fig. 3 shows the turbo TCM transmitter for 2^N-ary PSK modulation. The information 2^{N-1}-ary symbol sequence u_n and its block-wise interleaved version $u_n^{(i)}$ are fed into two identical component encoders RSC-LCIRC$_1$ and RSC-LCIRC$_2$ of rate $(N-1)/N$. The encoders' outputs are selected alternatively and mapped into 2^N-ary modulated symbol sequence x_n. The output of the bottom encoder is deinterleaved according to the inverse operation of the interleaver. This ensures that at the input of the symbol selector, the $N-1$ information bits from the 2^{N-1}-ary input symbol, partly defining the encoded 2^N-ary symbols of both the upper and lower input, are identical [6]. Therefore, if the selector is switched on a symbol base, the mapper output is a punctured version of the two encoded sequences, and the $N-1$ information bits appear only once, mapped in a single transmitted symbol selected either from e_{1n} sequence or from e_{2n} sequence. Nevertheless, the remaining parity bit carried by the transmitted symbol is taken alternatively from the upper and lower encoder. Hence, the overall coding rate for the scheme in Fig. 3 is $(N-1)/N$. The 2^N-levels modulated symbol sequence is transmitted over an AWGN noisy channel. The received signal over the n-th symbol interval is given by:

$$y_n = x_n + w_n \tag{3}$$

where w_n is a zero-mean complex AWGN sequence with $E\left[|w_n|^2\right] = N_0$, and x_n denotes the 2^N-levels symbol value mapped from the encoders output sequences (e_{1n}, e_{2n}) by puncturing over the n-th symbol interval. The receiver structure, shown in Fig. 4, has two component decoders that use the symbol-by-symbol log-MAP algorithm introduced in [6]. The decoding process is similar to the binary turbo decoding in [5], except that the symbol probability is used as the extrinsic information rather than the bit probability [6], [7]. The log-MAP decoder computes the log likelihood ratio (LLR) for each group of information bits transmitted at the n-th symbol interval u_n, embedded in the 2^{N-1}-ary input symbol taking one of the integer values $j \in \{0, 1, ..., 2^{N-1}-1\}$ as [7]

$$\begin{aligned} L(u_n = j) &= \log \frac{P(u_n = j|\mathbf{y})}{P(u_n = 0|\mathbf{y})} \\ &= \log \frac{\sum_{(l',l)\in B_n^j} \alpha_{n-1}(l')\,\gamma_n^j(l',l)\,\beta_n(l)}{\sum_{(l',l)\in B_n^0} \alpha_{n-1}(l')\,\gamma_n^0(l',l)\,\beta_n(l)} \end{aligned} \tag{4}$$

where $\mathbf{y}$ is the received signal vector, B_{n^j} represents the set of trellis transitions at the n-th symbol interval determined by an input symbol $u_n = j$, denoted as $(S_{n-1} = l' \to S_n = l)$ where S_n is the trellis state at moment n, and the probabilities $\alpha_n(l)$, $\beta_n(l)$, and $\gamma_n(l',l)$, denoting the forward, backward, and the transition metrics, are computed recursively as in [7]. The symbol-by-symbol log-MAP decoder operates on an L symbols block basis. Hence, in all equations the symbol time variable n takes values between 1 and L. The receiver transition metric is given by:

$$\gamma_n^j(l',l) = \begin{cases} \frac{P(u_n=j)}{P(u_n=0)} \exp\left(-\frac{|y_n - x_n|^2}{2\sigma^2}\right), & \text{if } (l',l) \in B_n^j \\ 0, \quad \text{otherwise} \end{cases} \tag{5}$$

The transition metric in (5) is normalized over all input symbol values, as follows:

$$\gamma_n(l',l) = \log \sum_{j=0}^{2^{N-1}-1} \gamma_n^j(l',l) \tag{6}$$

The first term in (5) denotes the apriori information for the transmitted input symbol j. The number of trellis states for each component RSC-LCIRC encoder is 2^N. The forward normalized metric is estimated as following:

$$\alpha_n(l) = \log \sum_{l'=0}^{2^N-1} \exp\left[\alpha_{n-1}(l') + \gamma_n(l',l)\right] \tag{7}$$

The recurrence in (7) is initialized with

$$\alpha_0(0) = 0; \quad \alpha_0(l)|_{l\neq 0} = -\infty \tag{8}$$

The backward normalized metric is estimated as:

$$\beta_n(l) = \log \sum_{l'=0}^{2^N-1} \exp\left[\beta_{n+1}(l') + \gamma_{n+1}(l', l)\right] \tag{9}$$

and the recurrence in (9) is initialized with

$$\beta_L(0) = 0; \quad \beta_L(l)|_{l\neq 0} = -\infty \tag{10}$$

The input symbol j with the largest LLR in (4) is chosen as the hard decision output.

In contrast to the binary turbo codes, in TTCM case we can not separate the influence of the information and parity-check components within one symbol. The systematic information and the extrinsic information are not independent. Thus, both systematic and extrinsic information will be exchanged between the two component decoders. The joint extrinsic and systematic information of the first log-MAP decoder, denoted as $L_{1,es}(u_n = j)$, is computed as

$$L_{1,es}(u_n = j) = L_1(u_n = j) - \log \frac{P(u_n = j)}{P(u_n = 0)} \tag{11}$$

The last term in (11) represents the a priori information symbol knowledge fed by the other decoder.

The joint extrinsic and systematic information $L_{1,es}(u_n = j)$ is used as the estimate of the a priori LLR at the next decoding stage. After interleaving this term is denoted as $L^{(i)}_{1,es}(u_n = j)$. The joint extrinsic and systematic information of the second decoder is given by

$$L_{2,es}(u_n = j) = L_2(u_n = j) - L^{(i)}_{1,es}(u_n = j) \tag{12}$$

In the next iteration the a priori term in (11) is replaced by the deinterleaved joint extrinsic and systematic information from the second decoding stage, denoted as $L^{(i)}_{2,es}(u_n = j)$.

It must be stated that for the symbol-by-symbol log-MAP decoding, each component decoder should avoid using the same systematic information twice in every iterative decoding step. In TTCM scheme, each decoder alternately receives the noisy output of its own encoder and that of the other encoder. As mentioned before, the parity bit in every second received symbol was generated by the other encoder, due to the symbol puncturing in the transmitter. The decoder ignores this symbol by setting the branch metric to zero. The only input at this decoding step consists in the a priori component obtained from the other decoder, which contains the systematic information. All the mentioned LLRs and the relations between them are represented in the TTCM receiver scheme from Fig. 4.

The iterative metric computation presented above assumes that the a priori LLR is already available. Nevertheless, in the first iteration, the a priori LLR for the first decoder is unavailable. Considering the symbol mapping presented in Fig. 2, the a priori information for the first decoder regarding the punctured symbols, i.e., the input symbols encoded by the second encoder and transmitted in the even positions n, is determined partially by the systematic information input symbol u_n, and also by the unknown parity bit $p_n \in \{0, 1\}$ generated by the second encoder (see equation (1)). Using the mixed Bayes' rule the a priori probability is given by [6]

$$\begin{aligned} P(u_n = j) &= \text{const} \cdot \sum_{k\in\{0,1\}} p(y_n | u_n = j,\, p_n = k) \\ &= \text{const} \cdot \sum_{k\in\{0,1\}} \exp\left(-\frac{|y_n - x_n^{j,k}|^2}{2\sigma^2}\right) \end{aligned} \tag{13}$$

where const is a constant value, assuming that all the values of u_n and p_n are equally probable, and the 2^N-ary modulated symbol x_n, transmitted by the second encoder, is given by $x_n^{j,k} = 2 \cdot u_n + p_n = 2 \cdot j + k$. The a priori LLR is computed by normalizing the values in (13)) by their sum estimated for all the values of $j \in \{0, 1, ..., 2^{N-1} - 1\}$. If the first decoder operates over the odd symbols x_n, the a priori LLR is initialized with equally probable values assuming that $\Pr(u_n = j) = 1/2^{N-1}$.

4. SIMULATIONS RESULTS

The TTCM scheme presented in Section 3 using the RSC-LCIRC encoders presented in Section 2 was tested for 8-PSK modulation by means of simulations over an AWGN channel. Both component encoders in the TTCM scheme are identical rate-2/3 RSC-LCIRC encoders. The modulation is using the optimum set partitioning for the punctured TTCM scheme as presented in Section 2. The symbol interleavers used for simulations are pseudo-random and operate independently on even and odd positions, respectively, as presented in [6]. The symbol-by-symbol log-MAP decoding algorithm is used in the receiver. Each of the following simulation results is represented as BER performances versus E_s/N_0, where E_s is the signal energy per symbol and N_0 is the variance of the AWGN noise sequence. The interleaver block includes 1024 symbols and the number of decoding iterations is eight. Further iterations do not improve significantly the detector performances. The BER performances for TTCM transmission using 8-PSK with bandwidth efficiency of 2b/s/Hz are represented in Fig. 5. As a reference, we considered for the same simulation scenario the corresponding rate-2/3 optimum binary encoder with 8 states, determined in [6] for 8-PSK TTCM with the generator polynomials in ascending order, represented in octal notation $[11, 02, 04]$. The simulation results show a perfect match of the BER performances between the rate-2/3 RSC-LCIRC encoder and its binary counterpart. This is explained by the fact that both encoders have similar trellises with identical minimum Euclidian distance values. The common minimum Euclidian distance is presented in Table 1. Eight iterations are enough to reach a BER of $3 \cdot 10^{-5}$ for $E_s/N_0 = 7.2$dB. In Fig. 6 BER

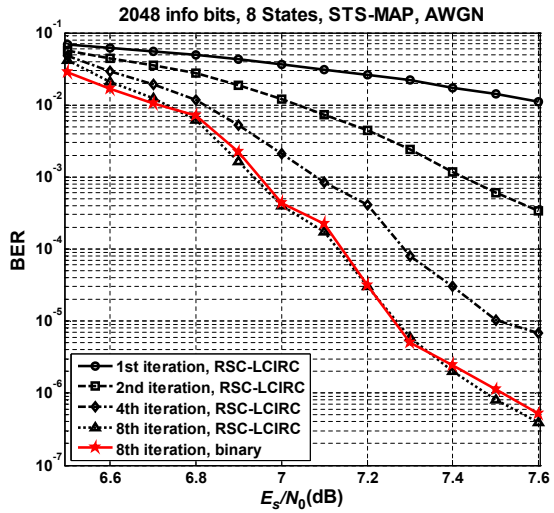

Figure 5: BER performance for punctured 8-PSK-TTCM scheme using RSC-LCIRC encoders over an AWGN channel.

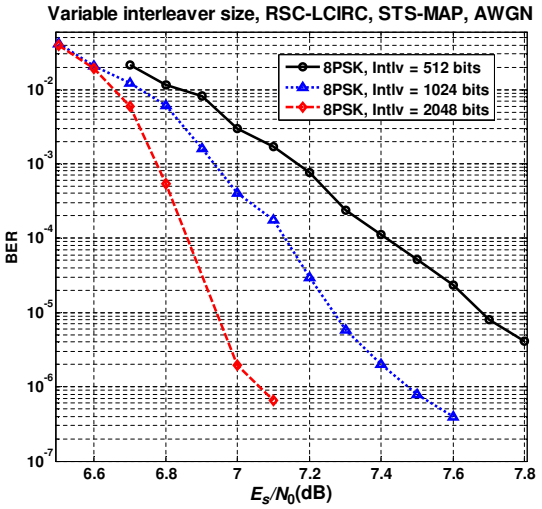

Figure 6: BER performance for punctured RSC-LCIRC-8-PSK-TTCM scheme over an AWGN channel with variable interleaver size.

performances after eight iterations, for the same modulation schemes, are depicted when the interleaver size is varied. Therefore, the interleaver block is including consecutively 512, 1024, and 2048 symbols. When the interleaver size is doubled a coding gain of approximatively 0.4dB is obtained.

5. CONCLUSIONS AND PERSPECTIVES

It was shown that the proposed optimum RSC-LCIRC encoder can be used as a component encoder in turbo-TCM schemes with punctured parity check bits (symbols). Also, due to the inner non-binary operation of the RSC-LCIRC encoder, the symbol-by-symbol log-MAP algorithm proves to be suitable for iterative decoding. The nonlinear LCIRC function drives to low complexity encoder, while the systematic property attains good performances in punctured schemes. Another advantage of this generalized encoder consists in the compact expression for the minimum Euclidian distance for PSK-TCM encoders, as function of the symbol representation wordlength N. In further studies it is necessary to evaluate the actual complexity gain over the binary encoding counterparts. Also, the performances of these turbo TCM schemes should be investigated using EXIT charts. In addition, the scheme performances analysis when transmitting over a channel with fading requires further attention.

Acknowledgment

This work was supported in part by the Romanian contract POSDRU/89/1.5/S/62557 and by the Romanian UEFISCSU PN-2 RU-TE Project no. 18/12.08.2010.

REFERENCES

[1] D. R. Frey, "Chaotic digital encoding: An approach to secure communication," *IEEE Trans. Circuits and Systems - II: Analog and Digital Signal Processing*, vol. 40, pp. 660-666, Oct. 1993.

[2] C. Vladeanu, S. El Assad, J.-C. Carlach, and R. Quéré, "Improved Frey Chaotic Digital Encoder for Trellis-Coded Modulation," *IEEE Trans. Circuits and Systems - II*, vol. 56, pp. 509-513, Jun. 2009.

[3] C. Vladeanu, S. El Assad, J.-C. Carlach, R. Quéré, I. Marghescu, "Recursive GF(2^N) Encoders Using Left-Circulate Function for Optimum PSK-TCM Schemes," *Signal Processing*, vol. 90, pp. 2708-2713, Sep. 2010.

[4] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Information Theory*, vol. IT-28, pp. 55-67, Jan. 1982.

[5] C. Berrou and A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo-Codes," *IEEE Trans. on Comm.*, vol. 44, pp. 1261-1271, Oct. 1996.

[6] P. Robertson and T. Worz, "Bandwidth-Efficient Turbo Trellis-Coded Modulation using Punctured Component Codes," *IEEE Trans. on Sel. Areas in Comm.*, vol. 16, pp. 206-218, Feb. 2000.

[7] B. Vucetic and J. Yuan, *"Turbo Codes: Principles and Applications*," Springer, 2000.

[8] H. Ogiwara, A. Mizutome, and K. Koike, "Performance Evaluation of Parallel Concatenated Turbo Trellis Coded Modulation," *IEICE Trans. Fundamentals*, vol. E84-A, pp. 2410-2417, Oct. 2001.

[9] A.F. Paun, C. Vladeanu, I. Marghescu, S. El Assad, and A. Martian, "On the QAM Parallel Turbo-TCM Schemes using Recursive Convolutional GF(2^N) Encoders," in *Proc. 18th European Signal Conf. - EUSIPCO 2010*, Aalborg, North Denmark, Aug. 23-27, 2010, pp. 1414-1418.