RECURSIVE GF(2^N) ENCODERS USING LEFT-CIRCULATE FUNCTION FOR OPTIMUM TCM SCHEMES

CĂLIN VLĂDEANU[1], SAFWAN EL ASSAD[2], ION MARGHESCU[1], ADRIAN FLORIN PĂUN[1]
JEAN-CLAUDE CARLACH[3], RAYMOND QUÉRÉ[4]

Key words: GF(2^N) encoders, Left-circulate function, Euclidian distance, Trellis-coded modulation.

In this paper, trellis coded modulation (TCM) schemes are designed using recursive encoders over Galois field GF(2^N). These encoders are designed using the nonlinear left-circulate (LCIRC) function. The LCIRC function performs a bit left circulation over the representation word. Different encoding rates are obtained for these encoders when using different representation word lengths at the input and the output, denoted as N_{in} and N, respectively. A generalized 1-delay GF(2^N) recursive encoder scheme using LCIRC is proposed for performance analysis and optimization, for any possible encoding rate, N_{in}/N. Several TCM schemes using pulse amplitude modulation (PAM), and phase shift keying (PSK) are considered. The minimum Euclidian distance is estimated for all schemes and a general expression is found as a function of the word lengths N_{in} and N. The symbol error rate (SER) is estimated by simulation for PSK-TCM transmissions over an additive white Gaussian noise (AWGN) channel.

1. INTRODUCTION

Several discrete time nonlinear functions were used lately to generate pseudo-random sequences in a recursive manner.

In [1], Frey proposed a chaotic digital infinite impulse response (IIR) filter for a secure communications system. The Frey filter contains a nonlinear function named left-circulate function (LCIRC), which provides the chaotic properties of the filter. In [2], Werter improved this encoder in order to increase the randomness between the output sequence samples. The performances of a pulse amplitude

[1] Faculty of Electronics, Telecommunications and Information Theory / Telecommunications Department, University "Politehnica" of Bucharest, 1-3 Iuliu Maniu, ZIP 061071, Bucharest, Romania, E-mail: {calin, marion}@comm.pub.ro; adi@radio.pub.ro.

[2] École Polytechnique de l'Université de Nantes / IREENA, Rue Christian Pauc, B.P. 50609, 44306 Nantes, cedex 3, France, E-mail: safwan.elassad@univ-nantes.fr.

[3] France-Télécom R&D / site du CCETT-Rennes, France, E-mail: jeanclaude.carlach@orange-ftpgroup.com.

[4] XLIM-CNRS / Université de Limoges, France, E-mail: raymond.quere@xlim.fr.

modulation (PAM) communication system using the Frey encoder, with additive white gaussian noise (AWGN) were analyzed in [3], by means of simulations. All previously mentioned papers considered the Frey encoder as a digital filter, operating over Galois field GF(2^N). Barbulescu and Guidi made one of the first approaches regarding the possible use of the Frey encoder in a turbo-coded communication system [4]. Zhou et al. did a similar analysis in [5].

In [7] it was demonstrated that the Frey encoder with finite precision (word length of N bits) presented in [1] is a recursive encoder operating over GF(2^N). New methods for enhancing the performances of the PAM – trellis-coded modulation (PAM-TCM) and the phase shift keying – trellis-coded modulation (PSK-TCM) transmissions over a noisy channel were proposed in [8] and [9], respectively. These modulation schemes follow entirely the rules proposed by Ungerboeck in [6] for defining optimum trellis-coded modulations by proper set partitioning. Two-dimensional (2D) TCM schemes using a different trellis optimization method for Frey encoder was proposed in [10].

In the present paper, a generalization of the optimum one-delay GF(4) encoder in [7] is performed, for any output word length N and for any possible encoding rate in PAM-TCM and PSK-TCM schemes. These schemes are compared with conventional TCM schemes using GF(2) convolutional encoders. The paper is organized as follows. Section 2 is presenting the LCIRC function definition and properties over GF(2^N), and its use for designing a rate-1 GF(4) recursive encoder with LCIRC for QPSK-TCM and 4PAM-TCM transmissions. The trellis optimization method is presented in Section 3, first for a particular case, and then, for any output word length N. Therefore, in Section 3, a generalized optimum GF(2^N) recursive encoder scheme is proposed and an expression is provided for the minimum Euclidian distance of these encoders in PSK-TCM and PAM-TCM transmissions schemes. The simulated symbol error rate (SER) performance is plotted in Section 4 for the optimum PSK-TCM transmissions. Finally, the conclusions are drawn and some perspectives are presented in Section 5.

2. DESIGN OF TCM SCHEMES WITH GF(2^N) RECURSIVE ENCODERS USING THE LCIRC FUNCTION

2.1. NONLINEAR LCIRC FUNCTION OVER GF(2^N)

The main component of the chaotic encoder introduced by Frey in [1] and the recursive encoders presented in [7–10] is the nonlinear LCIRC function. This function is determining both the chaotic properties of the encoder in [1–3] and the trellis performances in [7–10]. The definition of this nonlinear function operating over finite sets and some of its properties will be presented in the sequel.

Let us denote by N the word length used for binary representation of each sample. The LCIRC function is used as a typical basic accumulator operation in microprocessors and performs a bit rotation by placing the most significant bit to the less significant bit, and shifting the other N–1 bits one position to a higher significance. This is the reason why the function is named left-circulate.

Considering the unsigned modulo-2^N operations for any sample moment n, the LCIRC consists in a modulo-2^N multiplication by 2 that is modulo-2^N added to the carry bit, and is given by the expression:

$$y^U[n] = LCIRC\left(x^U[n]\right) = \left(2 \cdot x^U[n] + s[n]\right) \bmod 2^N, \tag{1}$$

where the superscript U denotes that all the samples are represented in unsigned N bits word length, *i.e.* $x^U[n]$, $y^U[n] \in [0, 2^N–1]$, and the carry bit $s[n]$ is estimated as following:

$$s[n] = \begin{cases} 0, & \text{if} \quad 0 \le x^U[n] \le 2^{N-1} - 1 \\ 1, & \text{if} \quad 2^{N-1} \le x^U[n] \le 2^N - 1. \end{cases} \tag{2}$$

We can note from (2) that besides the nonlinearity in the modulo-2^N multiplications and additions, the carry bit $s[n]$ is determining the nonlinearity of the LCIRC function.

Applying N times consecutively the LCIRC function to an N bits wordlength unsigned value x^U, it results the original value:

$$LCIRC^N(x^U) \overset{\Delta}{=} \underbrace{LCIRC(LCIRC(...}_{N \text{ times}}(LCIRC(x^U)))) = x^U. \tag{3}$$

An example of a GF(4) recursive encoder using LCIRC function for a QPSK-TCM scheme is presented in the next section.

2.2. RATE-1 GF(4) RECURSIVE ENCODER WITH LCIRC FOR TCM

Let us consider a recursive encoder working over GF(4) using the LCIRC function. This scheme is presented in Fig. 1. Here, all the values are represented in the unsigned form. Let us assume that N denotes the word length used for binary representation of each sample. This encoder is composed by one delay element with a sample interval, two modulo-2^N adders, and a LCIRC block. For each moment n, $u[n]$ represents the input data sample, $x[n]$ denotes the delay output or the encoder current state, and $e[n]$ is the output sample. The encoding rate for the encoder in Fig. 1 is the ratio between the input word length N_{in} and the output word length $N = N_{out}$ [7–10], *i.e.*, $R = 1$, because $N_{in} = N_{out} = 2$. The trellis for the encoder in Fig. 1 is presented in Fig. 2 and does not follow the Ungerboeck rules [6], [7], [10]. This trellis has four states because the sample determining the encoder state takes four values, i.e., $x^U[n] \in \{0, 1, 2, 3\}$.

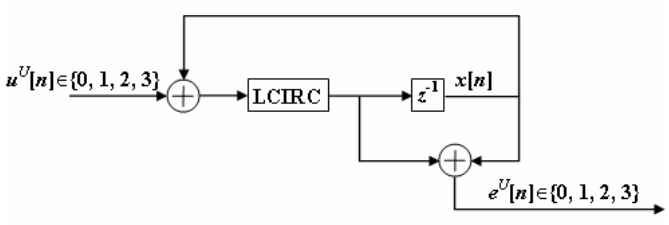

Fig. 1 – Rate-1 GF(4) nonlinear encoder for 2 b/s/Hz.

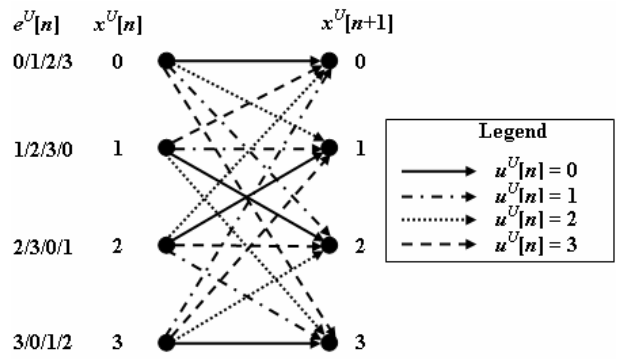

Fig. 2 – Trellis for rate-1 GF(4) nonlinear encoder (2 b/s/Hz).

In Fig. 2, four different lines are used for representing the transitions corresponding to the input sample $u^U[n]$. Each transition in Fig. 2 is associated to an unsigned output value $e^U[n] \in \{0, 1, 2, 3\}$. For each originating state, the values on the left side, from left to right, are associated to the transitions in the descending order.

Mapping an unsigned output symbol value $e^U[n]$ into an instant carrier phase value $\varphi^e[n]$ over the n-th sample interval, a 2^N levels PSK-TCM scheme is obtained. A simple phase mapping is given by:

$$\varphi^e[n] = e^U[n] \cdot \frac{2\pi}{2^N}, \quad e^U[n] \in \{0,\ 1,\ ...,\ 2^N - 1\} \tag{4}$$

For the M-PSK signal, we can write the following expressions of the Euclidian distances between the constellation points in the ascending order:

$$\Delta_k = 2 \cdot \sin\left[\frac{(k+1) \cdot \pi}{M}\right], \quad k \in \{0,\ 1,\ ...,\ \log_2(M) - 1\} \tag{5}$$

where M denotes the number of phase levels.

Considering the mapping in (4) and the distances' expressions in (5), it results that the QPSK-TCM signal trellis presents a minimum Euclidian distance of $d^2_{E,\ N=2,\ R=1,\ \mathrm{QPSK}} = 2\cdot\Delta_0^{\ 2} = \Delta_1^{\ 2} = 4$, offering no coding gain over the non-encoded binary PSK (BPSK) signal.

In the following, the same encoder scheme in Fig. 1 is used in conjunction with a PAM signal. In [1], Frey proposed a 2's complement representation form for all the computations in the scheme. For the ease of comparison, the 2's complement representation will be considered throughout the paper for all PAM signals [7, 8]. Hence, the signed signal takes equally probable values $x^S[n] \in \{-2^{N-1}, \ldots, -1, 0, 1, \ldots, 2^{N-1}-1\}$ with the following mean and variance values [7, 8]:

$$\overline{x^S[n]} = -1/2; \quad \sigma^2_{x^S[n]} = (2^{2N}-1)/12 . \tag{6}$$

In the following, it will be considered for the performance analysis that all PAM-TCM signals are normalized by their actual standard deviation in (6). Considering the above normalization, the quaternary PAM-TCM signal trellis in Fig. 2 presents a minimum Euclidian distance of $d^2_{E,\ N=2,\ R=1,\ \mathrm{PAM}} = (1/\sqrt{5/4}\,)^2 = 0.8$, offering no coding gain over the non-encoded binary 2's complement PAM signal.

3. OPTIMUM TCM SCHEMES WITH GF(2^N) RECURSIVE ENCODERS USING LCIRC

3.1. RATE-1/2 OPTIMUM GF(4) RECURSIVE LCIRC ENCODER FOR TCM

In this section, the potential of the nonlinear LCIRC function is showed, for designing efficient encoders. Following the trellis optimization presented in [7–9], a simple nonlinear encoder operating over GF(4) was developed, which has a binary input. It was demonstrated that this encoder performs identically to an optimum rate-1/2 binary field RSC convolutional encoder. Both encoders offer maximum coding gain for 1 b/s/Hz [6]. The scheme of the rate-1/2 optimum GF(4) encoder is presented in Fig. 3. Here, the time variable is neglected and all the values are represented in the unsigned form. The trellis for the encoder in Fig. 3 is presented in Fig. 4 and follows all the Ungerboeck rules. Considering the mapping in (4), the QPSK-TCM signal trellis in Fig. 4 presents a minimum Euclidian distance of $d^2_{E,R=1/2,\mathrm{opt.},u^U \in \{0,2\},\mathrm{QPSK}} = 2\cdot\Delta_1^{\ 2} + \Delta_0^{\ 2} = \Delta_1^{\ 2} = 10$ for a spectral efficiency of 1b/s/Hz. Hence, this rate-1/2 code for 1b/s/Hz QPSK-TCM transmission is offering a coding gain of $10\log10(2.5) \approx 4$ dB over the rate-1 QPSK-TCM in Section 2.2. Considering the PAM-TCM scheme using the power normalization with the value in (6), the Euclidian distance is $d^2_{E,\ R=1/2,\ \mathrm{opt.},\ u^U \in \{0,2\},\ \mathrm{PAM}} = 9/(\sqrt{5/4})^2 =$

= 7.2. Hence, this rate-1/2 code for 1b/s/Hz PAM transmission is offering a coding gain of 10log10(9) = 9.54 dB over the rate-1 encoder in Section 2.2.

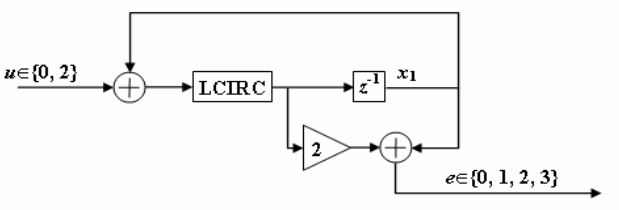

Fig. 3 – Rate-1/2 optimum GF(4) recursive LCIRC encoder for 1 b/s/Hz.

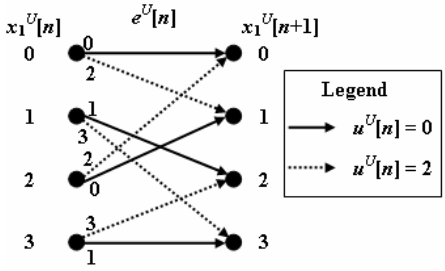

Fig. 4 – Trellis for rate-1/2 optimum GF(4) recursive LCIRC encoder (1 b/s/Hz).

3.2. GENERALIZED OPTIMUM RECURSIVE LCIRC ENCODER FOR TCM

Following the same design procedures as in Section 3.1, we can design optimum recursive encoders using LCIRC function, for any output word length N. In fact, for a fixed output word length N, an optimum recursive encoder will be determined for each input word length $N_{in} \in \{1, 2, \ldots, N-1\}$, for which the encoding rate is $R = \{1/N, 2/N, \ldots, (N-1)/N\}$. The general block scheme for a rate N_{in}/N optimum encoder, $N_{in} \in \{1, 2, \ldots, N-1\}$ using one delay element and the LCIRC function is presented in Fig. 5. LCIRC^{Nin} represents the LCIRC function application for N_{in} times consecutively, as it was defined in (3). Both adders and the multiplier are modulo-2^N operators. The trellis complexity of the codes generated with the scheme in Fig. 5 increases with the word length, because the number of trellis states grows exponentially with the output word length, *i.e.*, 2^N, while the number of transitions originating from and ending in the same state grows exponentially with the input word length, *i.e.*, $2^{N_{in}}$.

It can be easily demonstrated that the minimum Euclidian distance for the encoder in Fig. 5 has the following expression for PSK-TCM schemes [7]:

$$d^2_{E,\ R=N_{in}/N,\ 2^N-\text{PSK}} = \begin{cases} 2(\Delta_{2^{N-N_{in}}-1})^2 + \sum_{i=0}^{2^{N-N_{in}}-2} (\Delta_i)^2, & \text{for } N_{in} \in \left\{1,\ \ldots,\ \frac{N}{2}-1,\ \frac{N}{2}+1,\ \ldots,\ N-1\right\} \\ 2(\Delta_{2^{N-N_{in}}-1})^2 + (\Delta_0)^2, & \text{for } N_{in} = \frac{N}{2}. \end{cases} \quad (7)$$

For example, let us consider the optimum encoders for the output word length equal to 3, *i.e.*, $N = 3$. The input word length may take three values $N_{in} \in \{1, 2\}$, and the corresponding encoding rates are $R \in \{1/3,\ 2/3\}$. For the rate-1/3 encoder the scheme in Fig. 5 is set with all the values corresponding to $N_{in} = 1$. From (7) results that the minimum distance of this code is $d^2_{E,\ R=1/3,\ \text{opt., 8-PSK},\ u^U \in \{0,4\}} = 14$, having a coding gain of $10\cdot\log10(d^2_{E,\ R=1/3,\ \text{opt., 8-PSK},\ u^U \in \{0,4\}} / d^2_{E,R=1,N=3,\ \text{opt., 8-PSK}}) = = 10\cdot\log10(14/1.1716) \approx 10.77$ dB over the optimum 8PSK ($N = 3$) using a rate-1 encoder. For the rate-2/3 encoder ($N_{in} = 2$) the minimum distance of this code is $d^2_{E,\ R=2/3,\ \text{opt.,\ 8-PSK},\ u^U \in \{0,2,4,6\}} = 4 + 4 \cdot \sin^2(\pi/8) \approx 4.5858$, having a coding gain of approximately 5.93 dB over the optimum 8PSK ($N = 3$) using a rate-1 encoder. The rate 1 optimum encoder is obtained for $N_{in} = N$, for any value of N, considering that $LCIRC^0(x^U) = LCIRC^N(x^U) = x^U$ assumes no bit circulation. This rate-1 optimum encoder offers a minimum distance of $d^2_{E,\ R=1,\ \text{opt. } N=3,\ \text{opt., 8-PSK}} = 8\cdot\sin^2(\pi/8) \approx 1.1716$.

In Table 1 there are presented a few values of the minimum distances of the encoder in Fig. 5 for different values of N_{in} and N. The resulted coding rates are presented in the third column. Analyzing the values in Table 1 it can be noted that the minimum distance of a code decreases when its coding rate increases, for any value of N. This fact is well known, *i.e.*, the code performances decrease with the rate increases. Unfortunately, this dependency affects the spectral efficiency.

For the codes presented in Table 1, having the encoder structure in Fig. 5, the spectral efficiency for the PSK transmission is equal to the input word length N_{in}. Hence, the code performances increase is paid by a spectral efficiency decrease. All TCM schemes presented above were using PSK modulation. Even if PSK is used in practice only for small spectral efficiencies, *i.e.*, up to 3b/s/Hz, optimum LCIRC encoders can be designed for any spectral efficiency value, using the scheme in Fig. 5 with minimum distances given by (7).

Considering the PAM-TCM scheme it can be demonstrated that the minimum Euclidian distance for the encoder in Fig. 5 has the following expression [8]:

$$d^2_{E,\ R=N_{in}/N} = \begin{cases} 4\dfrac{7\cdot 2^{2(N-N_{in})}-1}{2^{2N}-1},\ \text{for } N_{in} \in \left\{0,\ 1,\ \ldots,\ \frac{N}{2}-1,\ \frac{N}{2}+1,\ \ldots,\ N-1\right\} \\ 12\dfrac{2^{2(N-N_{in})+1}+1}{2^{2N}-1},\ \text{for } N_{in} = \dfrac{N}{2}. \end{cases} \quad (8)$$

In Table 2 there are presented a few values of the minimum distances of the encoder in Fig. 5 for different values of N_{in} and N. The notes made previously for coding properties of the PSK-TCM schemes are also valid here.

It can be easily noticed that all the rate-(N–1)/N, for any N value, the optimum recursive LCIRC encoders are offering the same minimum distance as the corresponding binary optimum encoders determined by Ungerboeck in [6]. However, the GF(2^N) optimum recursive LCIRC encoders are less complex than the corresponding binary encoders.

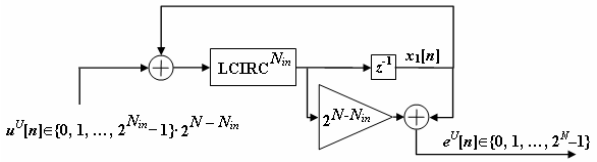

Fig. 5 – Rate N_{in}/N optimum GF(2^N) recursive LCIRC encoder for N_{in} b/s/Hz.

Table 1

Minimum distances for optimum gf(2^n) recursive encoders in psk-t cm schemes

N	N_{in}	R	d_E^2
1	1	1	8
2	1	1/2	10
2	2	1	4
3	1	1/3	14
3	2	2/3	$4 + 4 \cdot \sin^2(\pi/8) \approx 4.5858$
3	3	1	$8 \cdot \sin^2(\pi/8) \approx 1.1716$

Table 2

Minimum distances for optimum gf(2^n) recursive encoders in pam-tcm schemes

N	N_{in}	R	d_E^2	N	N_{in}	R	d_E^2
1	1	1	8	3	3	1	0.3810
2	1	1/2	7.2	4	1	1/4	7.0118
2	2	1	1.6	4	2	1/2	1.5529
3	1	1/3	7.0476	4	3	3/4	0.4235
3	2	2/3	1.7143	4	4	1	0.0941

4. SIMULATIONS RESULTS

The PSK-TCM schemes presented in Section 2 and Section 3 using all optimum encoders in Table 1 were considered for simulations. The SER performances for these encoding schemes using multilevel PSK signals and Viterbi decoding were analyzed in the presence of AWGN. The SER is plotted in Fig. 6 as a function of the SNR.

The PSK-TCM schemes using rate-1 optimum recursive encoders for the same spectral efficiencies as both optimum encoder PSK-TCM schemes for $N = 3$, were considered for comparison. For example, the rate-1/3 encoder for $N = 3$ is having the same spectral efficiency as the rate-1 encoder for $N = 1$, *i.e.*, 1b/s/Hz,

and the rate-2/3 encoder for $N = 3$ and the rate-1 encoder for $N = 2$ have an efficiency of 2b/s/Hz. These cases are considered in Fig. 6.

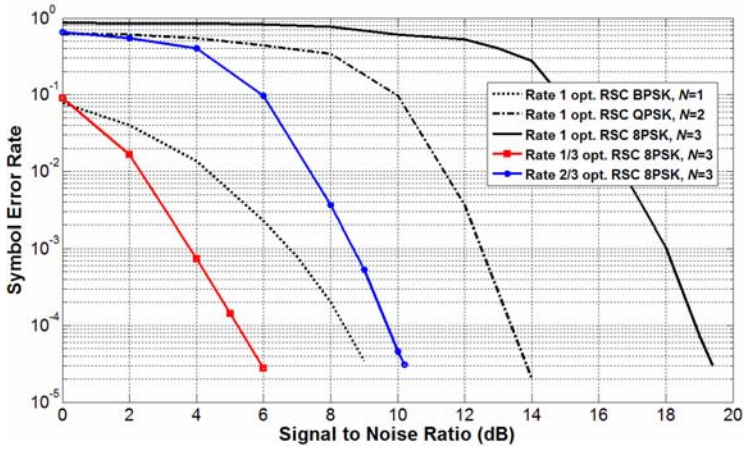

Fig. 6 – SER performance for PSK-TCM schemes using optimum GF(2^N) recursive encoders.

Analyzing the SER curves it can be noticed that the rate-1/3 encoder for $N = 3$ performs better than the rate-1 encoder for $N = 1$ by more than 3 dB (instead of a gain of approx. 2.43 dB, in theory; see Table 1), and the rate-2/3 encoder for $N = 3$ performs better than the rate-1 encoder for $N = 2$ by more than 3.8 dB (approx. 0.6 dB, in theory). The average multiplicity of error events with the minimum distance in (7), for optimum GF(2^N) recursive encoders, is smaller than multiplicity of minimum distance error events for the rate-1 encoders, for all encoders with $N_{in} < N$. This is the reason why the simulation results in Fig. 6 show larger coding gains between these two encoders for a given spectral efficiency.

5. CONCLUSIONS AND PERSPECTIVES

It was demonstrated that optimum recursive encoders over GF(2^N) can be designed using the LCIRC function. A generalized 1-delay GF(2^N) recursive encoder scheme using LCIRC was defined, for any possible encoding rate. A general expression is found for the minimum Euclidian distance of PSK-TCM and PAM-TCM schemes using these optimum encoders. As advantage of this generalized encoder, we can mention its reduced complexity. Hence, using only one delay element and multiple bit circulations we designed encoders having complex trellises and large Euclidian distances. In addition, it was shown that the nonlinear encoders offer the same performances as conventional binary encoders

for the rate-(N–1)/N schemes. Another advantage is that compact expressions were determined for the minimum Euclidian distances for the TCM schemes, as function of N_{in} and N. Also, the scheme of this encoder shows structural universality; the coding performances are controlled only by N_{in} and N.

In perspective, we intend to apply the presented method to other nonlinear structures and develop efficient trellis-coded modulation systems using these encoders. In addition, we will address the performances evaluation for the proposed TCM schemes over fading channels. Considering the properties of the encoders presented in this paper, we also aim to analyze the turbo coding scheme with optimum recursive encoders over GF(2^N).

ACKNOWLEDGEMENTS

This work was supported in part by the UEFISCSU Romania under Grant PN-II-"Idei" no. 116/01.10.2007 and the French ANR Project ASCOM.

Received on July 28, 2009

REFERENCES

1. D. R. Frey, Chaotic digital encoding: *An approach to secure communication*, IEEE Trans. on Circuits and Systems – II: Analog and Digital Signal Processing, **40**, *10*, pp. 660–666 (1993).
2. M. J. Werter, *An improved chaotic digital encoder*, IEEE Trans. Circuits and Systems – II: Analog and Digital Signal Processing, **45**, *2*, pp. 227–229 (1998).
3. T. Aislam, J.A. Edwards, *Secure communications using chaotic digital encoding*, IEE El. Letters, **32**, *2*, pp. 190–191 (1996).
4. S. A. Barbulescu, A. Guidi, S. S. Pietrobon, *Chaotic turbo codes*, IEEE Int. Symp. Inf. Theory, Sorrento, Italy, June 25–30, 2000.
5. X. Zhou, J. Liu, W. Song, H. Luo, *Chaotic turbo codes in secure communication*, IEEE Int. Conf. Trends in Communications EUROCON 2001, Bratislava, Slovakia, July 5–7, 2001.
6. G. Ungerboeck, *Channel coding with multilevel/phase signals*, IEEE Trans. on Information Theory, **IT-28**, *1*, pp. 55–67 (1982).
7. C. Vlădeanu, S. El Assad, J.-C. Carlach, R. Quéré, *Improved Frey Chaotic Digital Encoder for Trellis-Coded Modulation*, IEEE Trans. Circuits and Systems – II, **56**, *6*, pp. 509–513 (2009).
8. C. Vlădeanu, S. El Assad, J.-C. Carlach, R. Quéré, I. Marghescu, *Optimum PAM-TCM Schemes Using Left-Circulate Function over GF(2^N)*, accepted to IEEE 9th Int. Symp. on Signals, Circuits and Systems – ISSCS 2009, Iaşi, Romania, July 9–10, 2009.
9. C. Vlădeanu, S. El Assad, J.-C. Carlach, R. Quéré, I. Marghescu, *Optimum GF(2^N) Encoders Using Left-Circulate Function for PSK-TCM Schemes*, accepted to 17th European Signal Proc. Conf. – EUSIPCO 2009, Glasgow, Scotland, Aug. 24–28, 2009, to be published.
10. C. Vlădeanu, S. El Assad, J.-C. Carlach, R. Quéré, C. Paleologu, *Chaotic Digital Encoding for 2D Trellis-Coded Modulation*, IEEE 5th Advanced Int. Conf. on Telecomm., AICT 2009, Venice, Italy, May 24–28, 2009.