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

Călin Vlădeanu[1], Safwan El Assad[2], Jean-Claude Carlach[3], Raymond Quéré[4], and Ion Marghescu[1]

[1]Telecommunications Department, University Politehnica of Bucharest
1-3 Iuliu Maniu Bvd., Zip 061071, Bucharest, Romania
phone: + (40) 21 402 4765, fax: + (40) 21 402 4765, email: {calin, marion}@comm.pub.ro
[2]IREENA, École Polytechnique de l'Université de Nantes
Rue Christian Pauc, B.P. 50609, 44306 Nantes, cedex 3, France
phone: + (33) 2 40 68 30 36, fax: + (33) 2 40 68 32 32, e-mail: safwan.elassad@univ-nantes.fr
[3]France-Télécom R&D, RESA/WIN/CREM, site du CCETT-Rennes, France
[4]XLIM-CNRS, Université de Limoges, France

ABSTRACT

In this paper, phase shift keying – trellis coded modulation (PSK-TCM) schemes are designed using recursive systematic convolutional (RSC) 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 wordlengths at the input and the output, denoted as N_{in} and N, respectively. A generalized 1-delay GF(2^N) RSC encoder scheme using LCIRC is proposed for performance analysis and optimization, for any possible encoding rate, N_{in}/N. The minimum Euclidian distance is estimated for these PSK-TCM schemes and a general expression is found as a function of the wordlengths 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

The nonlinear functions were used lately in chaotic sequence generators to increase the security of communications systems.

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 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], and as in [4], the paper lacks of proof for the stated performance enhancement.

In [7] it was demonstrated that the Frey encoder with finite precision (wordlength of *N* bits) presented in [1] is a recursive systematic convolutional (RSC) encoder operating over GF(2^N). In [8], a new method is proposed for enhancing the performances of the chaotic PAM – trellis-coded modulation (PAM-TCM) transmission over a noisy channel. These encoders follow partially 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 [9].

In the present paper, a generalization of the optimum one-delay GF(4) encoder in [7] is performed, for any output wordlength *N* and for any possible encoding rate in phase shift keying TCM (PSK-TCM) schemes.

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) RSC encoder with LCIRC for a QPSK-TCM transmission. The trellis optimization method is presented in Section 3, first for a particular case, and then, for any output wordlength *N*. Therefore, in Section 3, a generalized optimum GF(2^N) RSC encoder scheme is proposed and an expression is provided for the minimum Euclidian distance of these encoders in a PSK-TCM transmission. 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 PSK-TCM SCHEMES WITH GF(2^N) RSC ENCODERS USING LCIRC

2.1 Nonlinear LCIRC Function over GF(2^N)

The main component of the chaotic encoder introduced by Frey in [1] and the RSC encoder presented in [7] is the nonlinear LCIRC function. This function is determining both the chaotic properties of the encoder in [1] and the trel-

This work was supported in part by the French ANR Project ASCOM and by Romanian UEFISCSU PN-2 Project 116/01.10.2007.

lis performances in [7], [8], and [9]. 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 wordlength 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:

$$y^U[n] = LCIRC(x^U[n]) = (2 \cdot x^U[n] + s[n]) \bmod 2^N, \quad (1)$$

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

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

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:

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

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

2.2 Rate 1 GF(4) RSC Encoder with LCIRC for a QPSK-TCM transmission

Let us consider a RSC 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 wordlength 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 wordlength N_{in} and the output wordlength N=N_{out} [7] [8], 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], [8]. This trellis has four states because the sample determining the encoder state takes four values, i.e., $x^U[n] \in \{0, 1, 2, 3\}$.

In Fig. 2, four different lines are used for representing the transitions corresponding to the input sample $u^U[n]$.

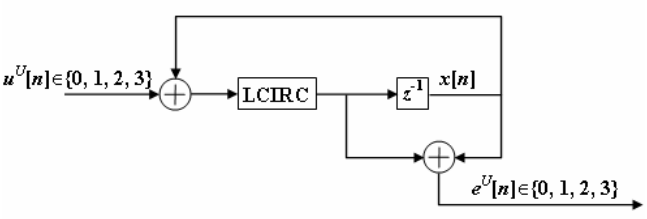

Figure 1 – Rate 1 GF(4) nonlinear encoder for 2 b/s/Hz.

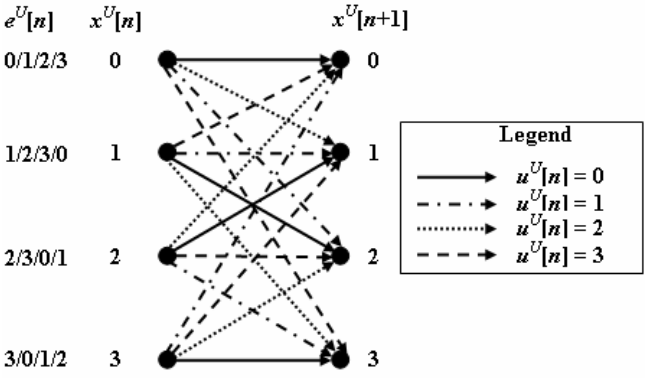

Figure 2 – Trellis for rate 1 GF(4) nonlinear encoder (2 b/s/Hz).

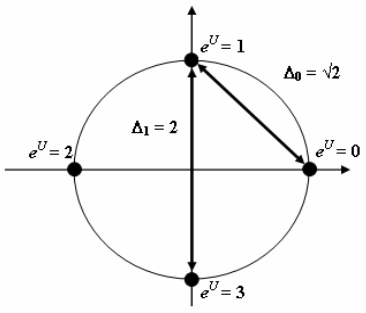

Figure 3 – Phase constellation for QPSK-TCM.

Each transition in Fig. 1 is associated to an unsigned output value $e^U[n] \in \{0, 1, 2, 3\}$. For each originating state, the values in the box, 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:

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

The phase constellation for the QPSK-TCM scheme using the encoder in Fig. 1 and the mapping in (4) is represented in Fig. 3.

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

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

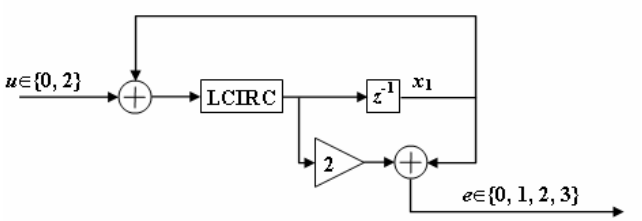

Figure 4 – Rate 1/2 optimum GF(4) RSC-LCIRC encoder for 1 b/s/Hz.

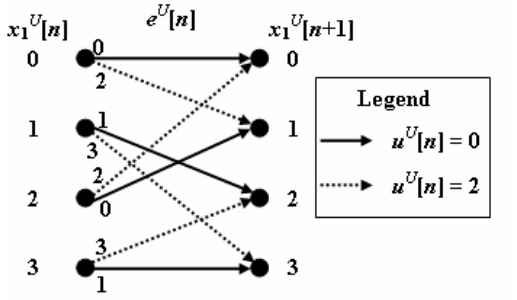

Figure 5 – Trellis for rate 1/2 optimum GF(4) RSC-LCIRC encoder (1 b/s/Hz).

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 in Fig. 3 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.

3. OPTIMUM PSK-TCM SCHEMES WITH GF(2^N) RSC ENCODERS USING LCIRC

3.1 Rate 1/2 Optimum GF(4) RSC LCIRC Encoder for a QPSK-TCM transmission

In this section, the potential of the nonlinear LCIRC function is showed, for designing efficient encoders.

Therefore, following the trellis optimization presented in [7] and [9], a simple nonlinear encoder operating over GF(4) was developed, which has a binary input. It is 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], [7]. The scheme of the rate 1/2 optimum GF(4) encoder is presented in Fig. 4. Here, the time variable is neglected and all the values are represented in the unsigned form.

The trellis for the encoder in Fig. 4 is presented in Fig. 5 and follows all the Ungerboeck rules.

Considering the mapping in (4), the QPSK-TCM signal trellis in Fig. 5 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.

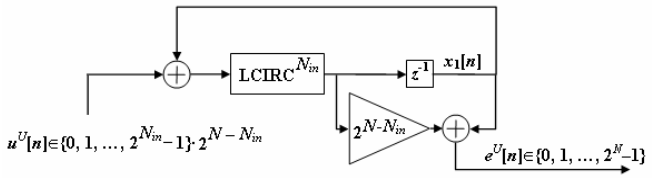

Figure 6 – Rate N_{in}/N optimum GF(2^N) RSC LCIRC encoder for N_{in} b/s/Hz.

TABLE 1
MINIMUM PSK-TCM DISTANCES AS FUNCTION OF N AND N_{IN} FOR OPTIMUM GF(2^N) RSC-LCIRC ENCODERS

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	$8\cdot\sin^2(\pi/8) \approx 1.1716$

3.2 Generalized Optimum RSC LCIRC Encoder for a PSK-TCM transmission

Following the same design procedures as in Section 3.1, we can design optimum RSC encoders using LCIRC function, for any output wordlength N. In fact, for a fixed output wordlength N, an optimum RSC encoder will be determined for each input wordlength $N_{in} \in \{1, 2, \ldots, N\text{-}1\}$, 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 PSK-TCM encoder, $N_{in} \in \{1, 2, \ldots, N\text{-}1\}$ using one delay element and the LCIRC function is presented in Fig. 6. 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. 6 increases with the wordlength, because the number of trellis states grows exponentially with the output wordlength, i.e., 2^{2N}, while the number of transitions originating from and ending in the same state grows exponentially with the input wordlength, i.e., $2^{2N_{in}}$.

It can be easily demonstrated that the minimum Euclidian distance for the encoder in Fig. 6 has the following expression:

$$d^2_{E,R=N_{in}/N,2^N-\mathrm{PSK}} = \begin{cases} 2(\Delta_{2^{N-N_{in}}-1})^2 + \sum_{i=0}^{2^{N-N_{in}}-2}(\Delta_i)^2, & \text{for } N_{in} \in \left\{1,\ldots,\frac{N}{2}-1,\frac{N}{2}+1,\ldots,N-1\right\} \\ 2(\Delta_{2^{N-N_{in}}-1})^2 + (\Delta_0)^2, & \text{for } N_{in} = \frac{N}{2} \end{cases} . \quad (6)$$

For example, let us consider the optimum encoders for the output wordlength equal to 3, i.e., N=3. The input wordlength 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. 6 is set with all the values corresponding to N_{in}=1. From (5) and (6) results that the minimum distance of this code is $d^2_{E,\,R=1/3,\,\mathrm{opt.},\,8\text{-PSK},\,u^U\in\{0,4\}} =$

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. 6 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, these performances are related to the spectral efficiency of these PSK transmissions. For the codes presented in Table 1, having the encoder structure in Fig. 6, the spectral efficiency for the PSK transmission is equal to the input wordlength N_{in}. Hence, the code performances increase is paid by a spectral efficiency decrease.

It can be easily noticed that all the rate $(N-1)/N$, for any N value, the optimum RSC LCIRC encoders are offering the same minimum distance as the corresponding binary optimum encoders determined by Ungerboeck in [6]. However, the GF(2^N) optimum RSC LCIRC encoders are less complex than the corresponding binary encoders. The memory size of the binary encoders increases logarithmically with the number of states in the trellis, while the GF(2^N) optimum RSC LCIRC encoders include only one delay element, no matter what is the trellis complexity.

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 RSC LCIRC encoders can be designed for any spectral efficiency value, using the scheme in Fig. 6 with minimum distances given by (5) and (6).

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. 7 as a function of the SNR.

The PSK-TCM schemes using rate 1 optimum nonlinear RSC 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. 7.

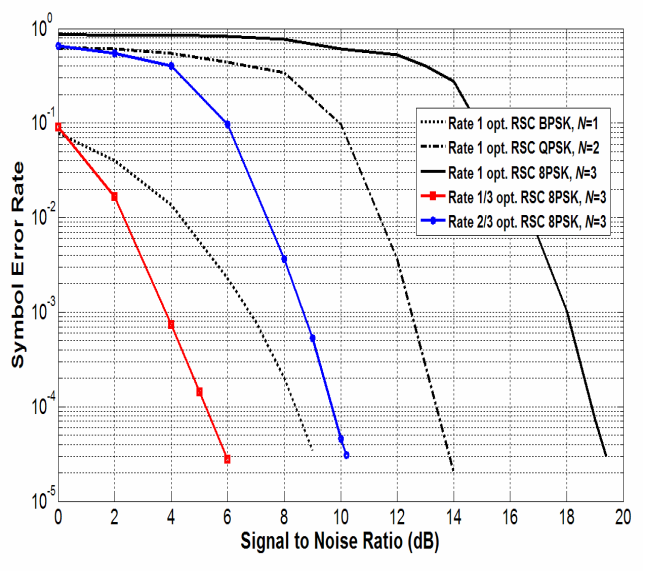

Figure 7 – SER performance for PSK-TCM schemes using optimum GF(2^N) nonlinear RSC encoders.

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 (6), for optimum GF(2^N) RSC 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. 7 show larger coding gains between these two encoders for a given spectral efficiency.

5. CONCLUSIONS AND PERSPECTIVES

It was demonstrated that optimum RSC encoders over GF(2^N) can be designed using the LCIRC function. A generalized 1-delay GF(2^N) RSC encoder scheme using LCIRC was defined, for any possible encoding rate. A general expression is found for the minimum Euclidian distance of PSK-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.

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 RSC encoders over GF(2^N).

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, October 1993.

[2] M. J. Werter, "An improved chaotic digital encoder," IEEE Trans. Circuits and Systems – II: Analog and Digital Signal Processing, vol. 45, pp. 227–229, February 1998.

[3] T. Aislam and J.A. Edwards, "Secure communications using chaotic digital encoding," IEE El. Letters, vol. 32, pp. 190-191, February 1996.

[4] S. A. Barbulescu, A. Guidi, and S. S. Pietrobon, "Chaotic turbo codes," *Proc. IEEE Int. Symp. Inf. Theory*, Sorrento, Italy, June 25-30, 2000, pp. 123.

[5] X. Zhou, J. Liu, W. Song, and H. Luo, "Chaotic turbo codes in secure communication," *Proc. IEEE Int. Conf. Trends in Communications - EUROCON 2001*, Bratislava, Slovakia, July 5-7, 2001, pp. 199 - 201.

[6] G. Ungerboeck, "Channel coding with multilevel/phase signals," IEEE Trans. Information Theory, vol. IT-28, no. 1, pp. 55-67, January 1982.

[7] C. Vlădeanu, S. El Assad, J.-C. Carlach, and R. Quéré, "Improved Frey Chaotic Digital Encoder for Trellis-Coded Modulation," accepted to IEEE Trans. Circuits and Systems – II, to appear (vol. 56, no. 6, June 2009).

[8] C. Vlădeanu, S. El Assad, J.-C. Carlach, R. Quéré, and 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, to be published.

[9] C. Vlădeanu, S. El Assad, J.-C. Carlach, R. Quéré, and C. Paleologu, "Chaotic Digital Encoding for 2D Trellis-Coded Modulation," accepted to *IEEE 5th Advanced Int. Conf. on Telecomm. - AICT 2009*, Venice, Italy, May 24-28, 2009, to be published.