ITERATIVELLY DECODING CHAOS ENCODED BINARY SIGNALS

Francisco J. Escribano[*], *Miguel A. F. Sanjuán*[†]

Nonlinear Dynamics and Chaos Group
Departamento de Matemáticas
y Física Aplicadas
y Ciencias de la Naturaleza
Universidad Rey Juan Carlos
28933 Móstoles, Madrid, Spain

Luis López

Laboratory of Distributed
Algorithmics and Networks
Departamento de Informática,
Estadística y Telemática
Universidad Rey Juan Carlos
28933 Móstoles, Madrid, Spain

ABSTRACT

In the present article we propose a new soft-input soft-output (SISO) decoding module for a chaos-channel encoded binary signal. When the chaos based channel encoder is used as inner encoder and a convolutional encoder is used as outer encoder in a serial concatenation scheme, the signal can be thus iterativelly and jointly decoded by means of the corresponding SISO decoders. This allows the transfer of bit extrinsic information for a final *Maximum a Posteriori* (MAP) decoding of the bit information. We believe that the design of this new chaos based SISO decoding module opens a road for new developments to make chaos based communications more robust and efficient.

1. INTRODUCTION

Chaotic signals offer good properties for their use in communication contexts, since they usually have low autocorrelation and are suitable for spread spectrum systems. After an initial outburst of research during the mid of the 90's, the interest on chaotic communications has somewhat dropped due to the bad performance of the systems proposed so far [1], in comparison to such simple modulation schemes as BPSK (Binary Phase Shift Keying). Nowadays, the arising of proposals outperforming traditional systems [2] has opened the way to look further into the possibilities of chaotic systems to act as channel encoders and decoders, taking advantage of their good intrinsic properties for some applications. In the past years, some decoding algorithms were presented for the kind of chaos based encoding we use in this paper [3]. The best results were given by the Maximum Likelihood Sequence Estimation (MLSE) approach based upon the Viterbi algorithm [4]. This algorithm is not optimal in terms of Bit Error Rate (BER) while a *Maximum A Posteriori* (MAP) approach is usually successful in lowering the final BER. This is one of the reasons for studying the adaptation of the soft-input soft-output MAP module proposed in [5] to the decoding of the chaotic signal. This certainly will allow us to introduce the chaos based channel encoder and the corresponding SISO decoder in a turbo-like framework, in which there will be a convolutional encoder acting as outer encoder and our chaos based encoder acting as inner encoder. The data from this serially concatenated scheme will be decoded iteratively using both a conventional SISO decoder (for the convolutional encoding) and the chaos based SISO decoder proposed here (for the chaos based encoding). Both SISO modules will exchange extrinsic bit information as in the known turbo encoding and decoding scheme [6], and in a way very similar to the turbo equalizer presented in [7]. We will show that this scheme is practical and boosts the performance in terms of BER. This opens a promising track in chaotic communications and makes it possible to introduce the sort of chaotic encoders based upon iterated maps in known concatenated coding and iterative decoding frameworks.

According to this aim, the next section will be devoted to the introduction of the chaos-channel encoder and to the channel model. In the following section, we will describe in detail the SISO module for the chaos-channel decoder and next, we will show the simulation results for a simple example. Finally, the last section is devoted to the conclusions, where we mention some of the possible future research tasks worth doing in this field.

2. TRANSMITTER

In order to encode a binary sequence denoted as $\{u_n\}$, where $u_n \in \{0, 1\}$ and $n = 1 \cdots N$, we make use of the method proposed in [8], substituting the aditive noise perturbation by an effect of truncation which will be explained in the sequel. The map we are interested in is the Bernoulli shift map defined as :

$$x_{n+1} = f(x_n) = \begin{cases} 2x_n & \text{if} \quad x_n \leq \frac{1}{2} \\ 2x_n - 1 & \text{if} \quad x_n > \frac{1}{2} \end{cases} \qquad (1)$$

[*] email: francisco.escribano@urjc.es

[†] We acknowledge financial support from the Spanish Ministry of Science and Technology under project BFM2003-03081 and from the Research Program of the Universidad Rey Juan Carlos, project number PPR-2004-03.

0-7803-9243-4/05/$20.00 ©2005 IEEE

It is a well known property of the Bernoulli shift map [3] that, if we define the symbolic state of the system r as

$$r = \sum_{m=1}^{N} u_m 2^{-m}, \tag{2}$$

and we define the initial condition for the chaotic sequence as $x_0 = r$, then the binary sequence is encoded into the chaotic sequence generated by x_0 and the information can be retrieved following:

$$u_n = \left\lfloor x_n + \frac{1}{2} \right\rfloor, \tag{3}$$

where $\lfloor x \rfloor$ is the nearest integer rounding towards zero.
For a real system, where the length N of the message, even when sent in packet mode, could reach thousands of bits, the proposed encoding process is not practical, since it implies an almost infinite precision. In this case, the method can be used by encoding blocks of D bits, in the following form:

$$x'_n = r'_n \quad = \quad \sum_{m=n}^{n+D-1} u_m 2^{-m+n-1}. \tag{4}$$

It can be shown that the resulting truncated sequence $\{x'_n\}$ is close to the original one, in a process equivalent to the addition of noise in order to control the chaotic sequence, $x'_n = x_n + \eta_n$, where $\eta_n < 2^{-D}$ is approximately a random white noise whose power decreases as D becomes larger. In the sequel, we will refer to the thus controled sequence as $\{x_n\}$. To perform the encoding process shown in (4), the bit sequence is padded with $D-1$ zeroes after u_N.
On the receiver side, the sequence received $\{y_n\}$ will be

$$y_n = x_n + n_n, \tag{5}$$

where n_n is an average white gaussian noise (AWGN) with zero mean and power σ^2. This is a useful and well known channel model in telecommunications.

In Figure 1 we can see the transmitter chain when using a concatenated turbo-like scheme. The original information bit sequence $\{b_n\}$ (independent and equiprobably distributed) is first convolutionally encoded to $\{c_n\}$, then interleaved to $\{u_n\}$ and, finally, this bit sequence is transformed into a chaotic sequence $\{x_n\}$ as stated before. It is worth noting that this kind of chaos based encoder has a rate $R = 1$.

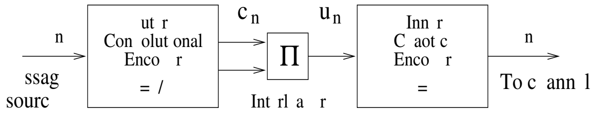

Fig. 1. Transmitter model.

3. CHAOS BASED SISO MODULE

The chaotic sequence $\{x_n\}$ can be dealt with under a symbolic dynamics basis [9], [10], where a quantization of the phase space $[0, 1]$ is needed. The interval $[0, 1]$ is divided into a series of nonoverlapping intervals I_i with limits $\frac{i}{P}$ and $\frac{i+1}{P}$ for $i = 0, \cdots, P-1$ and center in $c_i = \frac{i}{P} + \frac{1}{2P}$. P is the number of intervals, taken as a power of 2, so that the threshold point $\frac{1}{2}$ is the upper point of one interval and the lower one of another. In this way, with the only knowledge that a point x_n lies in the interval I_i, we can ascertain whether it has to be decoded as a 1 or as a 0. If we substitute the original sequence by the sequence of intervals where the corresponding symbol lies, we get a symbolic representation of the sequence that can be described as a first order Markow process[1], with a corresponding transition matrix $\mathbf{T}$. The term t_{ij} in this matrix means the transition probability between the interval I_i and the interval I_j. In the case of the Bernoulli shift map, each interval maps exactly into two contiguous intervals with equal probability. For example, in the case of $P = 4$, this transition matrix is:

$$\mathbf{T} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}. \tag{6}$$

When the number of bits D taken into account to encode the signal is such that $P = 2^D$, then the correspondence is exact, as there will be only a possible symbol x_n for each interval considered. When D is such that $P < 2^D$, the symbolic dynamics principle mentioned is also valid, but there will be more than one representative per interval. Instead of substituting the signal by its representation in terms of intervals, we can work with states and transitions between states. We say that the Markow process is in state $s_n = i$ at time $n = 1 \cdots N$ if x_n lies in I_i. Examining matrix (6), we see that there are only two possible transitions for each state, each one corresponding to a different bit value[2]. Taking this into account, we can define the edges of a trellis section, which is all we need to adapt the algorithms in [5] to build our chaos based SISO decoding module. This trellis is such that, if the input bit is u_n, and the current state is

$$s_{n-1} = \sum_{j=0}^{log_2(P)} w_j 2^j, \tag{7}$$

where the variables w_j take values 0 or 1, then the resulting state s_n is

$$s_n = \sum_{j=1}^{log_2(P)} w_{j-1} 2^j + u_n. \tag{8}$$

As the chaos based SISO module will act as inner decoder in a concatenated scheme, it is only necessary to calculate the output probabilities $\{\pi_n(u; O)\}$. We use the notation introduced in [5], where $\pi_n(u; O) = log\left[P(u_n = u; O)\right]$,

[1] This symbolic sequence contains exactly the same information as the original one in point of *bit information*.

[2] This is easy to see considering $P = 2^D$: from state/interval 00 we can go to 00 or 01, which means that the encoder has *received* as input bit a 0 or a 1, respectively.

meaning the logarithm of the extrinsic values of the *a posteriori* probability of the data $\{u_n\}$ given the *a priori* probability $\pi_n(u;I) = log\,[P(u_n = u;I)]]$ and the outputs from the channel $\{y_n\}$. Following the mentioned paper, the output of the SISO module will be obtained as:

$$\pi_n(u;O) =$$
$$log\left[\sum_{\frac{s_{n-1}\to s_n}{u_n=u}} exp\left\{\alpha[s_{n-1}] + \pi_n(y;I) + \beta[s_n]\right\}\right] \quad ,$$

where the summation is over all valid transitions between pairs of states s_{n-1} and s_n given by the input bit $u_n = u$. α and β are calculated through a forward-backward algorithm as:

$$\alpha[s_n] =$$
$$log\left[\sum_{s_{n-1}} exp\left\{\alpha[s_{n-1}] + \pi_n(y;I) + \pi_n(u;I)\right\}\right]$$
$$\beta[s_n] =$$
$$log\left[\sum_{s_{n+1}} exp\left\{\beta[s_{n+1}] + \pi_{n+1}(y;I) + \pi_{n+1}(u;I)\right\}\right] \quad .$$

The summations are for all the valid transitions between s_{n-1} and s_n, and between s_n and s_{n+1}, including the corresponding input bits which determine the transitions, u_n and u_{n+1}. In all cases, $n = 1 \cdots N$. The *a priori* values from the channel are $\pi_n(y;I)$,

$$\pi_n(y;I) = log\left(\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(y_n - c_{s_n})^2}{2\sigma^2}}\right), \qquad (9)$$

where c_{s_n} is the center of the interval corresponding to the state s_n. Both $\alpha[s_0]$ and $\beta[s_N]$ are initialized to $log\left(\frac{1}{P}\right)$, since the starting and ending states of the process are not known nor set to 0 as is usual in convolutional encoders.

In Figure 2 we can see the receiver model, where the SISO inner decoder is as explained so far and the SISO outer decoder is a conventional convolutional SISO decoder [5]. The input of the *a priori* information for the convolutional SISO module $\{\pi_n(b;I)\}$ is not shown as it is constant and only depends on the *a priori* probability of the information bit sequence (which is independent and identically distributed). As it may be seen, the *a posteriori* output extrinsic values of the outer SISO decoder for the convolutionally encoded data $\{c_n\}$ are used as input *a priori* probabilities in each iterative step for the chaos based SISO decoder. In turn, the *a posteriori* output extrinsic values from the chaos based SISO decoder are used as input *a priori* probabilities for the convolutional SISO decoder. The *a posteriori* values for the information binary sequence $\{b_n\}$ are finally hard decoded and provided as estimated bit values to evaluate the resulting BER.

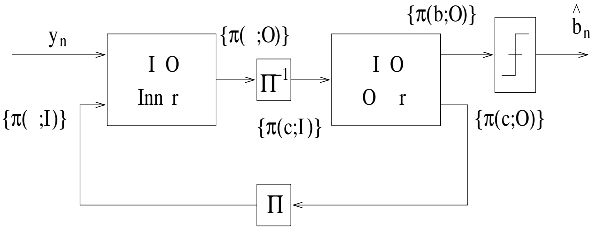

Fig. 2. Iterative receiver model.

4. SIMULATION RESULTS

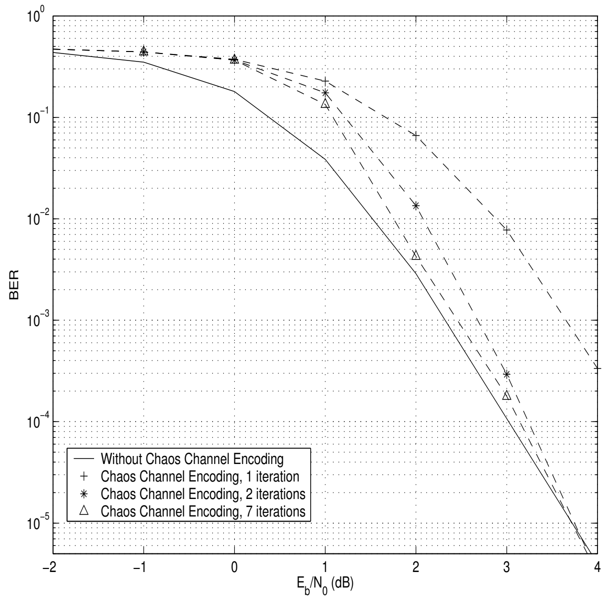

Fig. 3. BER results for the case where no chaos channel encoding is applied, and for the case with turbo decoding after 1, 2 and 7 iterations.

To test the SISO module proposed, we have simulated a system with a convolutional encoder of rate $\frac{1}{2}$, memory 8 and generating polynomials 101110001 and 111101011. The interleaver is a 500×500 block interleaver and we have chosen $D = 20$ in the chaos based encoder, so that, in practice, the quantization effect over $\{x_n\}$ is negligible. The number of states of the chaos based SISO decoder, together with the number of quantized intervals is $P = 32$. In Figure 3 we can see the results (BER against $\frac{E_b}{N_0}$)[3] when performing turbo decoding after several number of iterations, together with the performance when no chaos based encoding is used[4]. The convergence of the iterative process is very fast, so that, from the 5th iteration and on, no further gain is achieved. The final result is not so good as directlly sending the convolutionally encoded data, at least to a simulated BER of 10^{-5}. This is not surprising, since, when encoding with the Bernoulli shift map and when no additional channel encoding is present, the results are neither better than the results obtained for a simple BPSK modulation [11]. However, the transmitter system presented here and the iterative decoding is at least able to greatly improve the much poorer performance obtained when separately decoding both encoding processes. This provides a hint that, with further arrangements, a convolutional chaos based turbo system could be devised to outperform the results shown by these simulations.

[3] $\frac{E_b}{N_0} = \frac{\sigma_x^2}{2R_c\sigma^2}$, where $\sigma_x^2 = \frac{1}{12}$ is the power of the signal and R_c the rate of the code.

[4] In this case, the data $\{c_n\}$ is BPSK modulated and sent into the channel, and SISO decoded without further processing.

5. CONCLUSIONS

In this paper we have extended the concept of the SISO decoding module to a chaos channel encoder based upon the Bernoulli shift map, and we have checked its behaviour when placed in a serially concatenated scheme. As seen in the previous section, the results obtained do not justify the introduction of the chaos channel encoder when facing the results against the possibility of using a BPSK modulation and the same convolutional encoder. Nevertheless, this study shows how to improve the overall performance, and getting a performance at least as good as with BPSK is already a big fact, since the properties of the chaotic signal make it suitable for spread spectrum systems, while a BPSK signal would need further processing.

With respect to future developments, a deep study is lacking on which chaotic maps and convolutional encoders are able to provide better convergence behaviour (for example, through the use of EXIT charts [12]). We suspect that the fast convergence shown in our example could easily be explained by an excessive correlation in the data because of the specific encoders we used, so that not all the mutual information available from the codes is properly exploited. Other possible reason for the poor results is the instability of the iterative dynamics, which, when not properly managed, can lead to roundabout or overflow errors [5].

It is also worth studying the performance of the system taking into account the property of its *minimum distance* and it is also necessary to test how the performance is affected by the use of other and more robust kinds of interleavers (like the S-random interleavers [13]) and by the length of the same.

Other possibility for future research is the design of chaos based *recursive* encoders, as a known property of the serially concatenated schemes is that, when the outer encoder is not recursive but the inner one is, there is a steady gain in its final BER [5]. Finally, it could be interesting trying to adapt the SISO decoding module introduced here to more efficient chaos based encoders, as the ones presented, for example, in [14], or even to extend the principle to chaos based encoders with rates greater than $R = 1$.

6. REFERENCES

[1] A. S. Dimitriev, M. Hasler, A. I. Panas, and K. V. Zakharchenko, "Basic Principles of Direct Chaotic Communications," *Nonlinear Phenomena in Complex Systems*, vol. 6, no. 1, pp. 488–501, 2003.

[2] T. Schimming and M. Hasler, "Coded Modulations Based on Controlled 1-D and 2-D Piecewise Linear Chaotic Maps," in *ISCAS*, Bangkok, Thayland, May 2003, vol. 3, pp. 762–765.

[3] B. Chen and G. W. Wornell, "Analog Error-Correcting Codes Based on Chaotic Dynamical Systems," *IEEE Transactions on Communications*, vol. 46, no. 7, pp. 881–890, July 1998.

[4] A. Kisel, H. Dedieu, and T. Schimming, "Maximum Likelihood Approaches for Noncoherent Communications with Chaotic Carriers," *IEEE Transactions on Communications*, vol. 48, no. 5, pp. 533–542, May 2001.

[5] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "A Soft-Input Soft-Output Maximum a Posteriori (MAP) Module to Decode Parallel and Serial Concatenated Codes," Tech. Rep. 42-127, Jet Propulsion Laboratory, California Institute of Technology, November 1996.

[6] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes," in *Proceedings of the International Conference on Communications*, Geneve, Switzerland, May 1993, vol. 2, pp. 1064–1070.

[7] R. Koetter, A. C. Singer, and M. Tuchler, "Turbo Equalization," *IEEE Signal Processing Magazine*, vol. 21, no. 1, pp. 67–80, January 2004.

[8] M. S. Baptista and L. Lopez, "Information Transfer in Chaos-based Communication," *Phys. Rev. E*, vol. 65, pp. 055201–1,055201–4, May 2002.

[9] J. Schweizer and T. Schimming, "Symbolic Dynamics for Processing Chaotic Signals-I: Noise Reduction of Chaotic Sequences," *IEEE Transactions on Circuits and Systems*, vol. 48, no. 11, pp. 1269–1282, November 2001.

[10] J. Schweizer and T. Schimming, "Symbolic Dynamics for Processing Chaotic Signals-II: Communication and Coding," *IEEE Transactions on Circuits and Systems*, vol. 48, no. 11, pp. 1283–1295, November 2001.

[11] S. Kozic, K. Oshima, and T. Schimming, "Minimum Distance Properties of Coded Modulations Based on Iterated Cahotic Maps," in *Proceedings of the 11th International IEEE Workshop on Nonlinear Dynamics of Electronic Systems*, Scuol, Switzerland, May 2003, pp. 141–144.

[12] S. ten Brink, "Convergence Behaviour of Iteratively Decoded Parallel Concatenated Codes," *IEEE Transactions on Communications*, vol. 49, no. 10, pp. 1727–1737, October 2001.

[13] C. Heegard and S. Wicker, *Turbo Coding*, Kluwer Academic Publishing, Boston, 1999.

[14] S. Kozic, K. Oshima, and T. Schimming, "How to Repair CSK Using Small Perturbation Control - Case Study and Performance Analysis," in *Proceedings of the European Conference on Circuit Theory and Design*, Krakow, Poland, 1-4 September 2003.

[5] Not to forget that the chaotic sequence does not begin or end in known states, and this can easily hinder the final performance.