

# Shannon Capacity and Codes for Communicating with a Chaotic Laser \*

Renato M. de Moraes, Bartolomeu F. Uchôa-Filho, *Member, IEEE*,  
Cecilio Pimentel, *Member, IEEE*, Reginaldo Palazzo, Jr., *Senior Member, IEEE*,  
José Roberto Rios Leite

January 24, 2002

## Abstract

In this paper, we investigate a method of communicating with chaos described by Hayes, Grebogi, and Ott, which uses the idea of *controlling chaos* by *small perturbations*. Although allowing the electronics controlling the output signal to remain at the low-power level, this method unavoidably incurs a capacity loss, which we calculate for a chaotic CO<sub>2</sub> laser model. We first determine an approximation to the laser language, by means of a forbidden set representation, and then find its Shannon capacity. Results indicate that, since the capacity loss is not significant, the trade-off is worthwhile. Finally, we point to simple finite-state encoders that satisfy the constraints imposed by the language.

---

<sup>0</sup> R. M. de Moraes is with Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, 20742, USA (e-mail: rmariz@Glue.umd.edu).

<sup>0</sup> B. F. Uchôa-Filho is with Communications Research Group, Department of Electrical Engineering, Federal University of Santa Catarina, 88040-900, Florianópolis - SC, BRAZIL (e-mail: uchoa@eel.ufsc.br).

<sup>0</sup> C. Pimentel is with Communications Research Group, Department of Electronics and Systems, Federal University of Pernambuco, P.O. Box 7800, 50711-970, Recife - PE, BRAZIL (e-mail: cecilio@npd.ufpe.br).

<sup>0</sup> R. Palazzo, Jr. is with Department of Telematics, School of Electrical and Computer Engineering, State University of Campinas, P.O. BOX 6101, 13081-970, Campinas - SP, BRAZIL (e-mail: palazzo@dt.fee.unicamp.br).

<sup>0</sup> J. R. Rios Leite is with Department of Physics, Federal University of Pernambuco, 50670-901, Recife - PE, BRAZIL (e-mail: rios@df.ufpe.br).

\*This work was supported by the Brazilian Agencies: Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Financiadora de Estudos e Projetos (FINEP), Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), and Fundação de Amparo à Ciência e Tecnologia de Pernambuco (FACEPE). This paper was presented in part at the 2000 International Symposium on Information Theory and Its Applications, <sup>1</sup>Honolulu, Hawaii, U.S.A., November 5-8, 2000.

# 1 Introduction

In the past decade, much research on chaotic dynamical systems has been geared toward communications [1]-[16]. Applications of chaotic signals include chaotic encryption for secure communication [2], chaotic codes for spread spectrum communications [3, 4, 5], and chaotic digital modulation [6]. More recently, chaos was used to address diverse communications problems in [7, 8, 9, 10].

Chaotic systems are deterministic, since they are described by nonlinear differential equations or iterative mappings, and their time evolution is highly dependent on initial conditions and external perturbations. Based on these properties, Hayes, Grebogi, and Ott [1] proposed a method of communicating with chaos, whose efficiency (in a sense to be described) is evaluated in this paper. This method will be referred to as the HGO method, and may be described as follows. Each state variable (or phase) of a continuous chaotic system evolves as a time series of an apparently random sequence of pulses. All state variables or a subset of them produce a series of orbits which define the chaotic attractor. If one associates each pulse of a state variable or each orbit with a particular symbol, a sequence of symbols is readily obtained from the chaotic system. The HGO method uses the idea of *controlling chaos by small perturbations* (see details in [17]), thus manipulating the chaotic system, in order to generate controlled chaotic orbits whose associated symbol sequence corresponds to some user data sequence. The relevant feature of this approach is that any symbol sequence can be transmitted by weak signal perturbations applied to the chaotic system. Accordingly, the electronics controlling the system remains at the low-power level [17] for all messages. This clearly represents an advantage over the non-chaotic system since in this case a large amount of switching energy would be required to cause the laser to follow a particular symbol sequence.

In the absence of control, i.e., when the chaotic system runs freely, certain symbol sequences representing the orbits on the attractor are never produced. It is thus said that the system possesses its own *language* or rules specifying allowable and forbidden symbol sequences. In the HGO method, to keep up with small controls and hence avoid altering the basic topological structure of the orbits on the attractor, the symbol sequences intended to be transmitted must not deviate too much from the language of the free-running chaotic system [1]. Since *any* user data sequence is possible, an encoder is needed to translate the user data sequence into a sequence allowed by the language, similar to run-length constraints for magnetic recording channels [24]. Shannon [21] demonstrated that the maximum rate in bits per second at which information can be transmitted

through sequences of symbols belonging to a language, that is, the Shannon capacity, is lower if the language imposes more constraints. Therefore, the capacity loss due to the language in the HGO method may be used as a measure of its efficiency.

The HGO method was illustrated in [1] using the double scroll chaotic oscillator. Here, we have chosen to examine a communication system whose front-end transmitter is a chaotic CO<sub>2</sub> laser with saturable absorber [18], because its chaotic behavior has been extensively studied [5, 12, 15, 18, 19]. Initially, we report on an approximation to the language of the CO<sub>2</sub> laser. More specifically, we use computer numerical solutions and electronic simulation [12] for the equations representing a chaotic CO<sub>2</sub> laser with saturable absorber to obtain long pulse series. By inspecting the (apparently random) pulse series, we identified sets of forbidden strings, which define the language. The Shannon capacity associated with the chaotic CO<sub>2</sub> laser language is then calculated. Since one of the main goals in this paper is to find the efficiency of the HGO method, we also calculate the capacity without constraints on the pulses emitted by the laser, and show that the capacity loss due to the language is less than 11 %, which is fairly acceptable. This fact allows us to conclude that the HGO method can be realized, under low-power control, without significantly sacrificing transmission rate. Another contribution of this paper is the construction of finite-state encoders to be used in the HGO method. The idea is to present finite-state machines that translate any arbitrary binary sequence into a sequence of symbols allowed by the language. Even though other justifying reasons for using the HGO method may be found in the literature, this information-theoretic one is, to the best of our knowledge, novel.

This paper is organized as follows. In the next section, a tutorial introduction to a communication system using a chaotic laser as the front-end transmitter is given. In Section 3, we obtain an approximation to the CO<sub>2</sub> laser language. The main subject of Section 4 is the calculation of the Shannon capacities based on the results obtained in Section 3. Within Section 5, the finite-state diagram representation of the laser language, a necessary step for the construction of finite-state encoders, is given in Subsection 5.1. The construction itself is the subject of Subsection 5.2. Finally, in Section 6, we make some concluding remarks.

## 2 Chaotic Laser and Communication System

The chaotic pulsation of a single mode CO<sub>2</sub> laser with an intra cavity saturable absorber (LSA) has been extensively studied [5, 12, 15, 18, 19], and has been adopted as a test system to verify

general properties of nonlinear dynamical systems [18]. Its dynamics is described by the nonlinear differential equations [18]:

$$\dot{I} = I(U - \bar{U} - 1); \quad (1)$$

$$\dot{U} = \epsilon [W - U(1 + I)]; \quad (2)$$

$$\dot{W} = \epsilon (A + bU - W); \quad (3)$$

$$\dot{\bar{U}} = \bar{\epsilon} [\bar{A} - \bar{U}(1 + aI)], \quad (4)$$

where  $\dot{X}$  denotes the first derivative of  $X(t)$  with respect to the time  $t$ , and the parameters are set to the standard values according to [18], which are listed in Table 1. The light intensity,  $I(t)$ , and the normalized pumping rate of the laser amplifier,  $A$ , are, respectively, the main dynamical variable and the important parameter in our study, while the variables  $U$ ,  $W$ , and  $\bar{U}$ , and the parameters  $\epsilon$ ,  $\bar{\epsilon}$ , and  $\bar{A}$ , describe other physical quantities of the system. A detailed explanation of all variables and parameters, including the physical behavior contained in (1)-(4), may be found in [18].

As the parameter  $A$  is increased from 1.4 to 2.1, the numerical solutions of (1)-(4) reveal a laser behavior that alternates between a periodic pulsation, denoted by  $P^{(n)}$ , and a chaotic pulsation, denoted by  $C^{(n)}$ , where  $n = 1, 2, 3, \dots$  is the order of the pulsation. The periodic pulsation  $P^{(n)}$  consists of a regular sequence of pulses  $p^{(n)}$  presenting  $n$  small undulations after a big spike, as shown in Figure 1, for  $n = 0, 1, 2, 3$ . The chaotic pulsation  $C^{(n)}$  contains an intermittent, seemingly stochastic, sequence of pulses  $p^{(0)}, \dots, p^{(n)}$ . Typical CO<sub>2</sub> LSA pulse series  $C^{(n)}$ , for  $n = 1, 2$ , are shown in Figure 1. In order to study the symbolic dynamics of the chaotic CO<sub>2</sub> laser, we have considered the map  $p^{(n)} \rightarrow n$  so that the chaotic pulsation  $C^{(n)}$  may be regarded as a sequence of symbols over the alphabet  $\{0, 1, \dots, n\}$ . For example, the sequence of symbols corresponding to  $C^{(2)}$  shown in Figure 1 is  $\{21022202021 \dots\}$ . The restrictions on the pulse sequences produced by a free-running chaotic pulsation will be identified in Section 3. In the next subsection, we describe a communication system based on the HGO method using a chaotic laser.

## 2.1 The Communication System

A realization of the communication system is shown in Figure 2. The encoder must be used to convert the binary information message into a sequence belonging to the laser language. The encoded sequence feeds an electro-optical device (the chaotic trajectory controller) that, according

to the HGO method, inserts small perturbations in the CO<sub>2</sub> laser dynamics causing the sequence of transmitted pulses to follow the encoded sequence (the inverse map  $n \rightarrow p^{(n)}$  is used from the encoded symbols to the laser pulses). A concrete device for the CO<sub>2</sub> laser is a pair of Stark plates to modulate the energy levels of the saturable absorbing molecules within the laser cavity [20]. Such a modulation will act as a small variation on the value of  $\bar{A}$  in (1)-(4). It has been demonstrated [20] that the laser in chaotic oscillation can be set to follow synchronously the input of a weak electrical signal applied to the Stark cell, as long as the controlling signal adheres to the language of the laser pulsation. This element is attached to the chaotic CO<sub>2</sub> laser which emits infrared light pulses transmitted by optical wave guide or through the vacuum. In other words, we may state that the laser synchronizes to any low power input message and emits powerful light pulses sequences containing the encoded message. The advantage of such a system, which justifies its adoption, is that precision control has to be made on the low power electro-optical device and the powerful transmission laser is driven by the natural chaos synchronization. Finally, the receiver in Figure 2 has a detection photo-diode followed by a decoder.

### 3 An Approximation to the Laser Language

As mentioned earlier, in a given chaotic regime the free-running chaotic system gives rise to a set containing all allowable symbol sequences, which defines the system language. Determination of the exact language is notoriously difficult to obtain [19]. However, a good approximation to it may be obtained if we inspect a long pulse series generated by the chaotic system. Instead of trying to collect all allowable symbol sequences, we identify the patterns of symbols that never occur in the series. These are called the forbidden blocks (or strings) and the set of all forbidden strings is called the forbidden set. Specifically, we scan the long series with a sliding window of length  $m$  symbols and take note of the  $m$ -blocks that never occurred, for  $m = 1, 2, 3, \dots$ , in such a way that no sub-string of a forbidden  $m$ -block is declared forbidden. The forbidden set representation of languages is standard and its connection with symbolic dynamics [23] and discrete noiseless channels [21], including the calculation of Shannon capacity, will be detailed in the next section.

To produce the LSA pulse series, we used computer numerical solutions and electronic circuit simulation [12] for the equations (1)-(4), adopting exactly the same standard laser parameters in [18] and Table 1. By inspecting the simulated LSA pulse series, we have identified the forbidden sets for the chaotic regimes  $C^{(1)}$ ,  $C^{(2)}$ , and  $C^{(3)}$ . For each regime, we considered a pulse series

containing  $10^4$  pulses. As argued in [19], in determining the forbidden strings of length  $m$  a pulse series shorter than  $10^m$  leads to inaccurate results. Because of this, we should limit the maximum length of the forbidden strings to 4. On the other hand, chaotic systems with a finite number of forbidden strings have complexity, as defined in [19], equal to zero. Thus longer forbidden strings in each chaotic regime are expected to exist because of the non null complexity of this chaotic CO<sub>2</sub> laser [19]. Nevertheless, considering the analysis of the complexity of the chaotic CO<sub>2</sub> laser performed in [19], and the fact that this complexity increases with the order  $n$  of the chaotic regime, we may, at least for  $n = 1, 2$ , and  $3$ , assume that all forbidden strings of length higher than five would occur with very low probability. Therefore, the capacities calculated in the next section are very close to the exact capacities.

Denoting by  $\mathcal{F}_n$  the forbidden set for  $C^{(n)}$ ,  $n = 1, 2, 3$ , we have determined the following:

- $\mathcal{F}_1 = \{10100\}$
- $\mathcal{F}_2 = \{120, 201, 202, 2000, 2001\}$
- $\mathcal{F}_3 = \{0010, 0100, 0101, 0201, 1021, 1201, 1211, 2011, 2013, 2101, 2112, 2121\}$

From  $\mathcal{F}_1$ , note that no forbidden string of length up to 4 was found for  $C^{(1)}$ . On the other hand, only one five-symbol string was recognized as forbidden in the series. Since increasing the length of the series by an order of magnitude would demand a large computational effort, we shall consider this one-string forbidden set for the purpose of analysis. But we should be warned that, in the case of  $C^{(1)}$ , this may be a loose approximation.

## 4 The Shannon Capacity of the Chaotic CO<sub>2</sub> Laser

We denote by  $\mathcal{S}_n$  the set of all sequences of any length over  $\{0, 1, \dots, n\}$  allowed by the language of the chaotic pulsation  $C^{(n)}$ . The capacity of the set  $\mathcal{S}_n$ , denoted by  $C_n$ , was defined by Shannon [21] as:

$$C_n \triangleq \lim_{t \rightarrow \infty} \frac{\log_2 N_n(t)}{t} \quad (\text{bits/s}), \quad (5)$$

where  $N_n(t)$  is the number of sequences in  $\mathcal{S}_n$  of duration  $t$ . The normalized time duration of the pulse  $p^{(n)}$  (or the symbol  $n$ ) was determined to be approximately:

$$\tau^{(n)} \triangleq \frac{t^{(n)}}{t^{(0)}} \approx 1 + \frac{2n}{3}, \quad (6)$$

where  $t^{(n)}$  denotes the time duration in seconds of the pulse  $p^{(n)}$ . As observed in the previous section, the forbidden set is the only representation available for the chaotic laser language. We will calculate the capacity directly from the forbidden set  $\mathcal{F}_n$  by a systematic method based on standard combinatorial techniques, which was recently proposed [22].

For the forbidden sets  $\mathcal{F}_1$ ,  $\mathcal{F}_2$ , and  $\mathcal{F}_3$ , we calculated the corresponding Shannon capacities, namely,  $C_1 = 0.720T^{-1}$  bits/s,  $C_2 = 0.903T^{-1}$  bits/s, and  $C_3 = 1.04T^{-1}$  bits/s, where  $T$  seconds is the pulse  $p^{(0)}$  time duration. The actual Shannon capacities depend upon the specific value of  $t^{(0)} = T$ . For a CO<sub>2</sub> laser,  $T$  is about  $10\mu\text{s}$ . The capacities above are to be compared to the respective capacities for the unconstrained case:  $C_1^u = 0.767T^{-1}$  bits/s,  $C_2^u = 1.013T^{-1}$  bits/s, and  $C_3^u = 1.116T^{-1}$  bits/s. The capacity losses due to the language are 6.1 %, 10.8 %, and 6.8 %, respectively, which are very acceptable.

An interesting result derived is the asymptotic Shannon capacity, which we denote by  $C_\infty^u$ . The asymptotic Shannon capacity is a measure of the maximum rate (in bits/s) at which the laser would transmit information as the order  $n$  of the chaotic pulsation goes to infinity, and assuming no symbol sequence constraints. We have found that

$$C_\infty^u = 1.217T^{-1} \text{ bits/s.}$$

Due to the presence of the language at each order  $n$  the actual capacity for high values of  $n$  is smaller than  $C_\infty^u$ . It should be pointed out that  $C_3$  is not so distant from the asymptotic value and so the choice for using the system at high or low  $n$  value will be dictated by compactness and power transmission condition.

## 5 Codes Satisfying the Laser Constraints

### 5.1 Finite-State Diagram

An efficient implementation of the encoder of Figure 2 needed to transmit information using a chaotic laser is by means of a finite-state encoder [23, Chapter 5], as will be described in the next subsection. A finite-state diagram (FSD) representation for the language serves as an input to the majority of the algorithms that design finite-state encoders. An FSD is a directed graph with the edges labeled by symbols from  $\{0, 1, 2, \dots, n\}$ , such that the sequences allowed by the language are obtained by reading off the labels of edges along paths in the graph. In the following, we construct an FSD from each forbidden set. In this regard, we have used a systematic procedure [23, Chapter

3][24] that guarantees the minimality (with respect to the number of states) of the FSD. For  $\mathcal{F}_1$ , we obtained the FSD with 5 states shown in Figure 3(a). For the other two cases, the FSD is more easily obtained if we impose more restrictive constraints on  $\mathcal{F}_2$  and  $\mathcal{F}_3$ , giving rise to the new forbidden sets:

- $\tilde{\mathcal{F}}_2 = \{20\}$
- $\tilde{\mathcal{F}}_3 = \{01, 21\}$

It can be easily seen that the earlier constraints are still satisfied. For instance, note that if the string “20” does not occur within a given sequence, none of the strings in  $\mathcal{F}_2$  will. To quantify the capacity penalty due to simplification of forbidden sets we found the following capacities  $\tilde{C}_2 = 0.897T^{-1}$  bits/s and  $\tilde{C}_3 = 0.905T^{-1}$  bits/s for  $\tilde{\mathcal{F}}_2$  and  $\tilde{\mathcal{F}}_3$ , respectively. The capacity penalty is thus 0.6 % for the pulsation  $C^{(2)}$  and 13 % for the pulsation  $C^{(3)}$ .

By the same procedure used to find the FSD for  $\mathcal{F}_1$  we obtained, for  $\tilde{\mathcal{F}}_2$  and  $\tilde{\mathcal{F}}_3$ , the FSD’s with 2 and 3 states in Figures 3(b) and 3(c), respectively.

## 5.2 Finite-State Codes

In the following, we present finite-state codes to be used in the communication system depicted in Figure 2. Since the capacity penalty due to simplification of the forbidden set  $\mathcal{F}_2$  to  $\tilde{\mathcal{F}}_2$  is very small, and because the FSD of Figure 3(b) is the simplest one, we shall consider the chaotic pulsation  $C^{(2)}$  only. The idea is to present a way to translate any arbitrary binary sequence into an allowed sequence of symbols from the set  $\{0, 1, 2\}$ , of normalized time durations  $\tau^{(0)} = 1$ ,  $\tau^{(1)} = 1 + \frac{2}{3}$ , and  $\tau^{(2)} = 1 + \frac{4}{3}$ , respectively.

A finite-state encoder  $(\mathcal{S}, \ell)$  accepts, at each time interval, an input string of length  $p = \log_2 \ell$  bits, and generates a string of output symbols of length  $q$ . The output string and the next state are both determined by the current state and the input string. The concatenation of output strings in any path of the graph encoder must be a sequence allowed by the language  $\mathcal{S}$ . The parameter  $\ell$  is the number of outgoing edges in every state of the encoder graph, which must be a power of 2 so that, at each time interval,  $\log_2 \ell$  information bits specify a particular outgoing edge. There are many possibilities for an encoder, as will be exemplified next.

The first encoder for  $\ell = 2$  is obtained very easily. Note that by eliminating the edge loop labeled by the symbol 1 from the graph of Figure 3(b), we have 2 edges leaving each of the two

states. The resulting graph is indeed a finite-state encoder, as presented in Figure 4. The notation  $x/y$  on each edge specifies the input and output strings, respectively. The rate  $R$  of this code is determined as follows. First we should calculate the expected time,  $E\{\tau\}$ , spent to transmit an output string  $y$ , which is given by:

$$E\{\tau\} = E\{\tau | a\} \pi(a) + E\{\tau | b\} \pi(b),$$

where  $E\{\tau | s\}$  is the conditional expected time spent to transmit an output string  $y$  given that the machine is at state  $s$ , and  $\pi(s)$  is the stationary probability of state  $s$ . We assume that the data sequence is an independent and identically distributed binary sequence. We then have

$$E\{\tau | a\} = \frac{\tau^{(0)} + \tau^{(2)}}{2} = 1.667T,$$

and

$$E\{\tau | b\} = \frac{\tau^{(1)} + \tau^{(2)}}{2} = 2T.$$

Thus,

$$E\{\tau\} = \frac{1.6667 + 2}{2} = 1.833T,$$

where in this case  $\pi(a) = \pi(b) = 1/2$ . The transmission rate is then given by

$$R = \frac{1}{E\{\tau\}} = 0.545T^{-1} \text{ bits/s},$$

since from any state a single data bit is transmitted every time an output string (a laser symbol in this case) is sent. We should observe that the size of the laser alphabet (3 symbols in this case) is not a power of 2. But this is not really a problem. The important property the graph for such a finite-state code must have is that the number of edges leaving any state be a power of 2. From this observation, we can see that binary transmission can be made possible through the use of finite-state codes for any chaotic pulsation. Comparing now the transmission rate above with the capacity  $\tilde{C}_2 = 0.897T^{-1}$  bits/s, we see that this finite-state code has an efficiency, defined as the ratio  $R/C$ , of 60.7 percent.

To construct a second code, now with  $\ell = 4$ , we first need to determine the second higher power graph [23, Section 2.3] of the original graph of Figure 3(b). This graph has the same states as the original graph, and precisely one edge from state  $s_1$  to state  $s_2$  for each path in the original graph of length 2 symbols from state  $s_1$  to state  $s_2$ . This graph has eight edges leaving state  $a$  and five edges leaving state  $b$ , as shown in Figure 5. The finite-state encoder with  $\ell = 4$  is obtained

simply by eliminating 3 edges leaving state  $a$  and 1 edge leaving state  $b$  from the graph of Figure 5, resulting in the encoder graph shown in Figure 6. To keep the transmission rate as high as possible, an effort has been made to eliminate the edges labeled by the longest output strings. The transmission rate is obtained in the same way as it was done for the first code, but for the second code the stationary state probabilities are  $\pi(a) = 3/4$  and  $\pi(b) = 1/4$ . The corresponding transmission rate is  $R = 0.696 T^{-1}$  bits/s. So this code is 77.5 percent efficient.

We can improve transmission rate further if we allow for a non-uniform number of outgoing edges from a state. Note that while state  $b$  in Figure 5 has 5 outgoing edges, state  $a$  has 8, already a power of 2. So, if we only eliminate the edge loop labeled by the string 22 (state  $b$ ) in Figure 5, the number of outgoing edges from any state will be a power of 2. The corresponding transmission rate is  $R = 0.791 T^{-1}$  bits/s. So this code is 88.1 percent efficient. Additional improvement is possible and transmission rate can get close to the Shannon capacity through the use of the State Splitting Algorithm for designing finite-state codes [23].

## 6 Final Remarks

In this paper, the symbolic dynamics of a chaotic CO<sub>2</sub> laser with saturable absorber has been investigated. We used computer numerical solutions for the nonlinear differential equations representing the chaotic laser to identify sets of forbidden strings, which define the laser language. Next, we calculated the channel capacity for three chaotic pulsations. The loss of maximum information rate due to the constraints was found to be insignificant, as can be seen from the difference between  $C_n$  and  $C_n^u$ . This allows us to conclude that the HGO scheme is very attractive.

Similar investigation with other chaotic systems may be worth conducting. For instance, chaotic diode lasers [16], whose attractors obey other restrictions, make strong candidates to be studied for their pulsation time falls in the picosecond duration range [25], i.e., they are more attractive for communication purposes. Since the results presented here are based on simulation of a very accurate laser model [18], we should mention the relevance of future work with a real experimental system.

## Acknowledgment

The authors would like to thank the anonymous reviewers for their constructive comments and suggestions.

## References

- [1] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, no. 20, pp. 3031-3034, May 1993.
- [2] F. Dalchelt, K. Kelber, and W. Schwarz, "Discrete-time chaotic encryption system - Part III: Cryptographical analysis," *IEEE Trans. Circ. Syst.*, vol 40, no. 9, pp. 983-988, Sept. 1998.
- [3] J. M. Lipton and K. P. Dabke, "Spread spectrum communications based on chaotic systems," *Int. J. Bifurcation and Chaos*, vol. 6, no. 12A, pp. 2361-2374, 1996.
- [4] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communications through modulation of chaos," *Int. J. Bifurcation and Chaos*, vol. 3, no. 2, pp. 469-477, 1993.
- [5] R. M. de Moraes, L. B. Oliveira-Neto, and J. R. Rios Leite, "Simulation of masked communication with chaotic lasers," *Journal of the Brazilian Telecommunications Society*, vol. 12, no. 2, pp.123-128, Dec. 1997.
- [6] K. M. Cuomo, A. V. Oppenheim, and A. V. Strogatz, "Synchronization of Lorentz based chaotic circuits with applications to communications," *IEEE Trans. Circ. Syst.*, vol. CAS-40, no. 10, pp. 626-633, Oct. 1993.
- [7] B. Chen and G. W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 881-890, July 1998.
- [8] E. Costamagna, L. Favalli, P. Gamba, and P. Savassi, "Block-error probabilities for mobile radio channels derived from chaos equations," *IEEE Commun. Lett.*, vol. 3, no. 3, pp. 66-68, Mar. 1999.
- [9] A. Müller and J. M. H. Elmirghani, "Blind channel estimation and echo cancellation using chaotic coded signals," *IEEE Commun. Lett.*, vol. 3, no. 3, pp. 72-74, Mar. 1999.
- [10] M. Kennedy, G. Kolumbán, and G. Kis, "Chaotic modulation for robust digital communications over multipath channels," *Int. J. Bifurcation and Chaos*, Vol. 10, no. 4, pp. 695-718, Apr. 2000.
- [11] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65-68, July 1993.

- [12] R. M. de Moraes, L. de B. Oliveira Neto, and J. R. Rios Leite, "Analog circuits simulation of communication with chaotic lasers," *Appl. Phys. Lett.*, vol. 70, no. 11, pp. 1357-1359, Mar. 1997.
- [13] D. R. Frey, "Chaotic digital encoding: an approach to secure communications," *IEEE Trans. Circ. Syst.*, vol. CAS-40, no. 10, pp. 660-666, Oct. 1993.
- [14] E. Bolt, Y-C Lai, and C. Grebogi, "Coding, channel capacity, and noise resistance in communication with chaos," *Phys. Rev. Lett.*, vol. 79, no. 19, pp. 3787-3790, Nov. 1997.
- [15] R. M. de Moraes, "Coding and channel capacity of a chaotic laser," M. Sc. Thesis, State University of Campinas, Campinas, São Paulo, Brazil, Aug. 1998.
- [16] C. Mirasso, P. Colet, and P. García-Fernandes, "Synchronization of chaotic semiconductor laser: Application to encoded communications," *IEEE Photonics Technology Letters*, vol. 8, no. 2, pp. 299-301, Feb. 1996.
- [17] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.*, vol 64, no. 11, pp. 1196-1199, Mar. 1990.
- [18] M. Lefranc, D. Hennequin, and D. Dangoisse, "Homoclinic chaos in a laser containing a saturable absorber," *J. Opt. Soc. Am. B*, vol. 8, no. 2, pp. 239-249, Feb. 1991.
- [19] D. Hennequin and P. Glorieux, "Symbolic dynamics in a passive Q-switching laser," *Europhys. Lett.*, vol. 14, no. 3, 237-242, Feb. 1991.
- [20] T. Tsukamoto, M. Tashikawa, T. Tokei, T. Hirano, T. Kuga, and T. Shimizu, "Synchronization of a laser to a modulation signal artificially constructed from its strange attractor", *Phys. Rev. E* 56, 6564-6568, Dec. 1997.
- [21] C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication*, Univ. Illinois Press, Urbana, 1963.
- [22] C. Pimentel and B. F. Uchôa-Filho, "A combinatorial approach to finding the capacity of the discrete noiseless channel," *Proceedings of the 2000 International Symposium on Information Theory and its application (ISITA 2000)*, Honolulu, USA, pp. 693-696, Nov. 2000.
- [23] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge University Press, Cambridge, 1995.

- [24] B. Marcus, R. Roth, and P. Siegel, "Constrained systems and coding for recording channels," in *Handbook of Coding Theory*, V. S. Pless and W. Huffman, Eds. Amsterdam:Elsevier, 1999, pp. 1635-1764.
- [25] R. J. Jones, P. Reeds, P. S. Spencer, and K. A. Shore, "Chaos and synchronization of self-pulsating laser diodes," *J. Opt. Soc. Am. B*, vol 18, 166-172, 2001.

## Figure Captions

**Figure 1:** Typical CO<sub>2</sub> LSA pulse series obtained with an analog circuit simulator [12] for different pulsation. The periodic regimes  $P^{(n)}$  consist of regular sequences of pulses  $p^{(n)}$ ,  $n = 0, 1, 2, 3$ . Chaos  $C^{(1)}$  and  $C^{(2)}$  are illustrated showing the irregular appearance of  $p^{(n)}$ .

**Figure 2:** Scheme of a communication system using a chaotic CO<sub>2</sub> laser.

**Figure 3:** Finite-state diagrams for the chaotic laser language at (a) the  $C^{(1)}$ , (b) the  $C^{(2)}$  and (c) the  $C^{(3)}$  pulsation. Numbers associated with edges correspond to laser pulse symbols.

**Figure 4:** Finite-state encoder of rate  $R = 0.545 T^{-1}$  bits/s for the chaotic laser language at the  $C^{(2)}$  pulsation.

**Figure 5:** Second higher power graph of the graph of Figure 3(b).

**Figure 6:** Finite-state encode of rate  $R = 0.696 T^{-1}$  bits/s for the chaotic laser language at the  $C^{(2)}$  pulsation.

## Table Caption

**Table 1: Standard Parameter Values.**

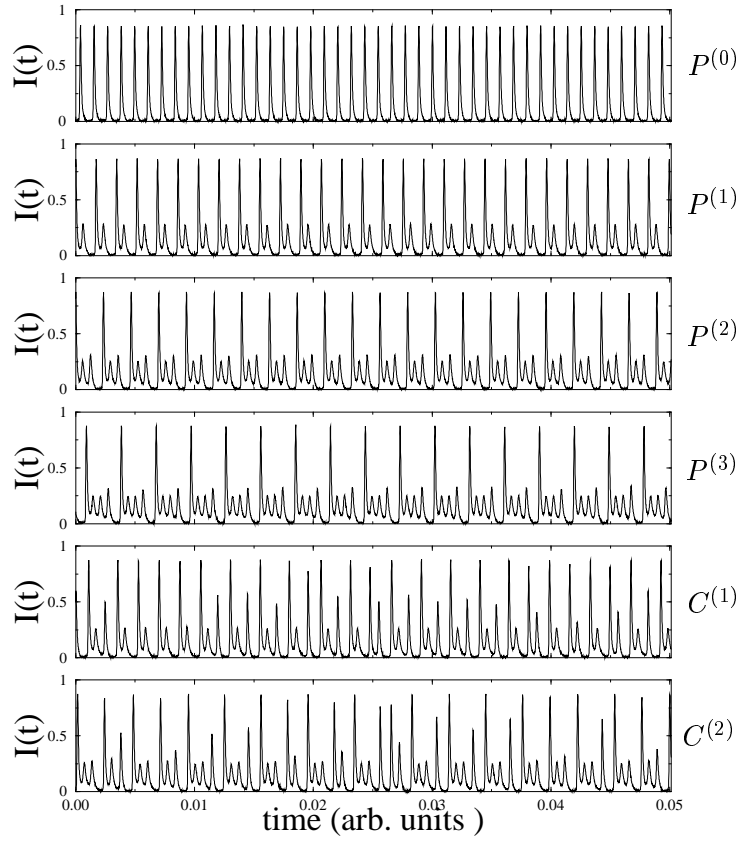


Figure 1: Typical CO<sub>2</sub> LSA pulse series obtained with an analog circuit simulator [12] for different pulsation. The periodic regimes  $P^{(n)}$  consist of regular sequences of pulses  $p^{(n)}$ ,  $n = 0, 1, 2, 3$ . Chaos  $C^{(1)}$  and  $C^{(2)}$  are illustrated showing the irregular appearance of  $p^{(n)}$ .

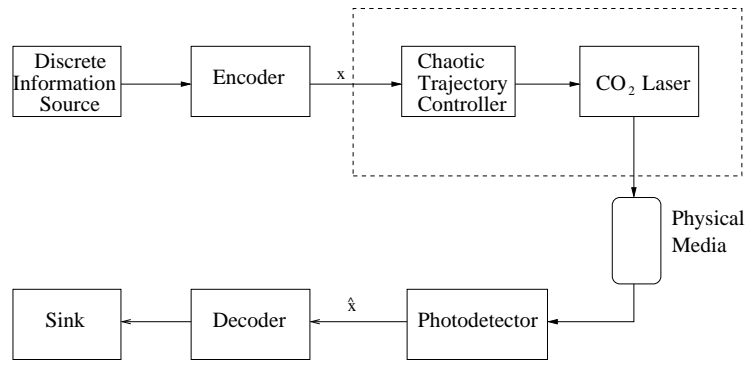


Figure 2: Scheme of a communication system using a chaotic CO<sub>2</sub> laser.

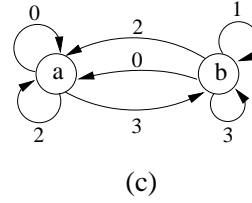
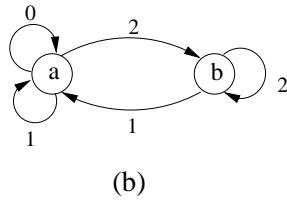
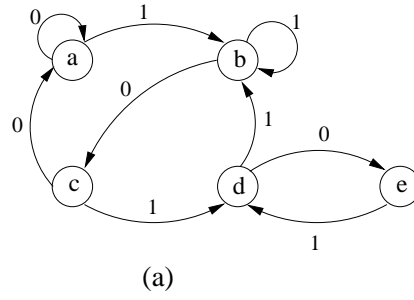


Figure 3: Finite-state diagrams for the chaotic laser language at (a) the  $C^{(1)}$ , (b) the  $C^{(2)}$  and (c) the  $C^{(3)}$  pulsation. Numbers associated with edges correspond to laser pulse symbols.

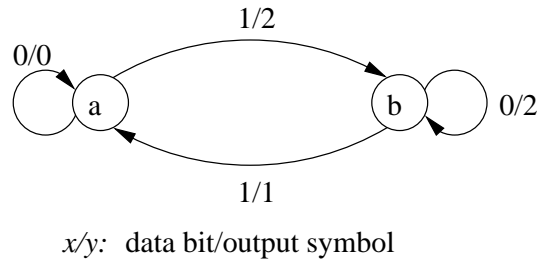


Figure 4: Finite-state encoder of rate  $R = 0.545 T^{-1}$  bits/s for the chaotic laser language at the  $C^{(2)}$  pulsation.

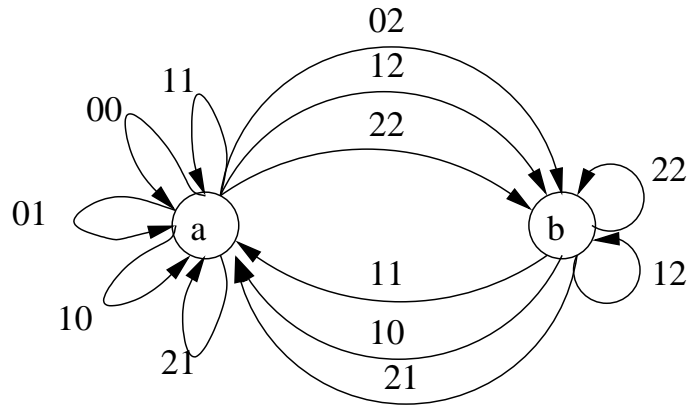


Figure 5: Second higher power graph of the graph of Figure 3(b).

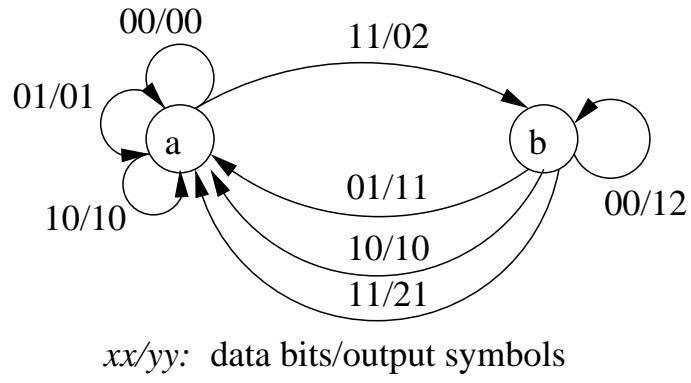


Figure 6: Finite-state encode of rate  $R = 0.696 T^{-1}$  bits/s for the chaotic laser language at the  $C^{(2)}$  pulsation.

Table 1: Standard Parameter Values.

Parameter	Value
$A$	1.4 to 2.1
$\bar{A}$	2.16
$\epsilon$	0.137
$\bar{\epsilon}$	1.2
$b$	0.85
$a$	4.1