Transmitters for chaos based communication: How chaotic is optimal?

Thomas Schimming

Swiss Federal Institute of Technology Lausanne EPFL
Laboratory of Nonlinear Systems LANOS, CH-1015 Lausanne, Switzerland
Phone: +41-21-69-32621, Fax: +41-21-69-36700
Email: thomas.schimming@epfl.ch

Abstract— In a systematic way, the impact of chaos present in transmitters for chaos based communications is discussed; based on arguments from information theory. Conditions for the optimality of communication systems involving chaos in the transmitter are developed. Based on these results which apply quite generally, different approaches to chaos based communications will be analyzed. In particular, what will be shown is that optimal performance in Shannon's sense implies that no information about the chaos (in the Shannon/Kolmogorov-Sinai sense) reaches the receiver. There are several ways to achieve this, some following previously known arguments, and some others that perhaps open new perspectives. In particular, it is shown that the emission of chaotic signals by the transmitter is not precluded in general, but for a number of common communication channels.

1. Introduction

The term "chaos based communications" summarizes several conceptually different approaches involving the transmission of (digital or analog) information across an imperfect (noisy) channel. The apparent common feature of all these methods is the presence of one or more chaotic systems in the transmitter of such a communication system. Depending on the method, the chaotic sequences generated by those systems, due to their statistical features, are employed either directly or indirectly to optimize the communications task.

In order to quantitatively demonstrate the impact of the general results, an example of a chaos shift keying scheme based on piecewise linear Markov maps with 2 segments is optimized with respect to the overall transmitter-receiver transmission error performance in a Gaussian noise channel. It turns out that the numerical results obtained are compatible with the general conditions derived, in the sense that the performance of the system tends to improve if the transmitter operates in a "less chaotic" regime. Other examples, including channel coding methods based on chaotic systems, are mentioned but not analyzed in particular detail.

It should be emphasized that the contribution, despite of the apparently absolute implications of the optimality conditions, leaves room to pursue each of the conceptually different approaches to chaos based communications, as a controlled sub-optimality with respect to error performance in the presence of other advantages is an acceptable engineering choice.

This work is supported by the Swiss National Science Foundation under contract number 2000-63789.00

However, the presented tools enable a more rigorous assessment of sources of performance loss in chaos based communication systems.

2. Transmitted reference systems

In the following, some properties of transmitted reference systems will be developed. Suppose B is a process of useful information to be communicated. The transmitter sends X onto the channel, based on a deterministic rule involving some side information S, which is modeled by another process. At the output of the channel, Y can be observed. Finally, an optimal receiver will recover as much information as possible about B from Y, forming an output process $\hat{B}$. This processing is illustrated in Fig. 1. It's pertinence to chaos based communication schemes is due to the observation that chaotic systems usually can be considered to be information sources.

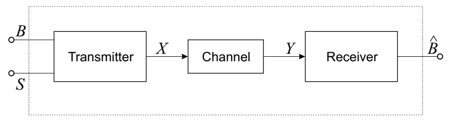

Figure 1: Information flow for a communication scheme with transmitted side information (transmitted ref.)

The aim of any communication system design is to optimally exploit the communication channel. In a more precise setting, this corresponds to communicating as much information from B to $\hat{B}$ as possible on the given channel [1]. Several important questions arise from the scheme given in Fig. 1, among them:

- What is the use of the side information S?
- Does S improve the performance of the receiver?
- Does the presence of S impair efficient communication from B to $\hat{B}$?

It turns out that these questions can be addressed while making only a minimal number of assumptions about the internals of such a scheme.

2.1. Channel utilization of transmitted reference systems

For the purpose of this paper, the communication system of Fig. 1 will be modeled as follows. At any instant ("channel use"), the uncertainty about the source B is it's entropy $H(B)$. In the same way, S is described by $H(S)$. With the standard notions of entropy and information [1], in particular the definition of trans-information or mutual information

$$I(U;V) = H(U) - H(U|V) = H(V) - H(V|U), \quad (1)$$

a symmetric quantity describing the information that two linked random variables U and V give about each other, several aspects of the communication system of Fig. 1 can be made precise. First, only good transmitters are considered, i.e. $I(B;X) = H(B)$. Also, B, S are independent, i.e. $I(B;S) = 0$. Furthermore, the transmitter is deterministic, i.e. $H(X|B,S) = 0$. This assumption is valid since the aim is to encapsulate any stochastic aspect of the transmitter in S. Similarly, a good receiver will extract all information about B from Y, thus $I(B;Y) = I(B;\hat{B})$. Thus, the receiver need not be considered here, provided that it is a good receiver in the above sense).

As described in [1], the amount of information that can be transmitted from the transmitter to the receiver is limited by the channel capacity

$$C = \max_{p(x)} I(X;Y), \quad (2)$$

achieved for some optimizing input distribution $p(x)$. In particular, for a given transmitter and channel, $I(X;Y) \leq C$ is the limiting factor of the communication system. Observe that $B \to X \to Y$ forms a Markov chain, i.e. $p(b,x,y) = p(b)p(x|b)p(y|x)$. The same holds for $S \to X \to Y$, the communication path of the side information. Thus, by the data processing inequality [1]

$$I(B;Y) \leq I(X;Y) \leq C \quad (3)$$
$$I(S;Y) \leq I(S;X) \quad (4)$$

which already gives some ideas about the relevance of the capacity limit on the transmitted payload information $I(B;Y)$. Also, a similar reasoning applies to the information about S in X and Y, respectively. However, this intermediate result would be more valuable if the conditions of equality in particular in (3) could be expressed. This leads to the next section.

2.2. Capacity achieving transmitted reference systems

The proper framework for analyzing the maximal rates at which a system like Fig. 1 can transmit information is that of the *broadcast channel* [1]. where independent information from a single source X is communicated to multiple receivers Y_1, Y_2 over separate channels. An interesting special case is the *degraded* broadcast channel $X \to Y_1 \to Y_2$, i.e. communication directed to Y_2 must first pass a common channel $X \to Y_1$, i.e. Y_2 is a degraded version of Y_1.

The transmitted reference system of Fig. 1 can be represented as a broadcast channel setup by setting $X = Y_1$ and $Y = Y_2$. This amounts to the scheme given in Fig. 2[1]

[1]The broadcast channel of Fig. 2 is slightly degenerate as the block linking X and Y_1 is an ideal channel. However, as the capacity of this channel is not of interest here, this is not a problem.

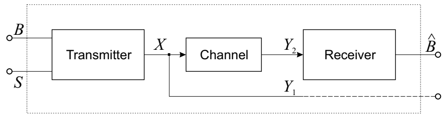

Figure 2: Transmitted reference system as a broadcast channel

A number of results exist for broadcast channels [1]. However, it is usually necessary to make some assumptions about the channels $X \to Y_1$ and $Y_1 \to Y_2$ in order to derive useful results. Let us first investigate what can be said in general.

Theorem 1. *The capacity region for sending independent information at rate R_1 to Y_1 and at rate R_2 to Y_2 over the degraded broadcast channel $X \to Y_1 \to Y_2$ is the convex hull of the closure of all (R_1, R_2) satisfying*

$$\begin{aligned} R_2 &\leq I(U;Y_2) \\ R_1 &\leq I(X;Y_1|U) \end{aligned} \quad (5)$$

for some joint distribution $p(u)p(x|u)p(y_1,y_2|x)$, where the auxiliary random variable U has cardinality bounded by $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$[2].

This result is well known, for a proof, see [1].

The auxiliary variable embodies the common information that both receivers, the one at Y_1 and the other at Y_2, can recover. Hence, for the system of Fig. 2, the auxiliary variable U is clearly identical with B, the payload information to be communicated to Y. Furthermore, the rate R_2 is the maximum rate at which payload information can be communicated. The following theorem addresses the question at which rate R_1 information can be communicated from S to Y_1 while exploiting the entire capacity of the channel $Y_1 \to Y_2$ for communicating B.

Theorem 2. *Under the given assumptions, $R_2 = I(X;Y)$ implies $I(S;Y) = 0$, i.e. in order for the payload to achieve capacity, no side information S may be communicated to the receiver.*

Proof. From theorem 1, achieving capacity implies equality in (5), hence

$$R_2 = I(B;Y) \quad (6)$$
$$R_1 = I(X;X|B) = H(X|B) \quad (7)$$

Expanding $I(B;X,Y)$ in two different ways, using $B \to X \to Y$,

$$\begin{aligned} I(B;X,Y) &= I(B;Y) + I(B;X|Y) \quad (8) \\ &= I(B;X) + \underbrace{I(B;Y|X)}_{=0} \quad (9) \\ &= H(X) - H(X|B) \quad (10) \end{aligned}$$

[2]For a random variable X defined on an input alphabet $\mathcal{X}$, the cardinality $|\mathcal{X}|$ is the number of symbols in $\mathcal{X}$ in the discrete case. For the continuous case, the problem of defining cardinality is not as obvious [1].

Thus,

$$R_2 + I(B; X|Y) = H(X) - R_1 \tag{11}$$
$$R_2 = I(X; Y) - R_1 + H(X|B, Y) \tag{12}$$

where $R_2 = I(X; Y)$ if and only if

$$R_1 = H(S) = H(X|B, Y) \tag{13}$$
$$\leq H(S|Y) \tag{14}$$
$$I(S; Y) \leq 0. \tag{15}$$

Since mutual information is nonnegative, $R_2 = I(X; Y)$ thus implies $I(S; Y) = 0$. □

Corollary 3. *As a direct result of theorem 2, $R_2 = I(X; Y)$ also implies $I(X; Y|B) = 0$.*

This follows directly by using the same technique as in (8) and is more useful for checking particular systems, as then it is sufficient to analyze the information transmitted over the channel for fixed symbols b.

The above result provides a tool for analyzing given transmitter–channel pairs for their potential of achieving capacity, that is, optimally exploiting the communication channel of the underlying transmitted reference system. Furthermore it illustrates the very fact that notion *transmitted reference* implies sub-optimality since, in it's intuitive sense, it implies $I(S; Y) > 0$, otherwise the receiver would not observe the reference.

3. Chaotic system or chaos?

Based on the results of the previous section, comments about the implications of chaos for achieving capacity can now be given. In particular, as it will turn out that in principle, the presence of chaos will make achieving capacity problematic, the alternative of considering chaotic systems in the absence of chaos will also be discussed as one potential solution to the problem.

3.1. Chaos based modulations as transmitted reference systems

It is known that chaotic systems can be represented as information sources, that is, they gradually expose more and more information about their initial state during their evolution in time. In fact, sensitive dependence on initial conditions means in terms of an information source, that on one hand this flow of information will never stop and on the other hand, that the infinite precision is necessary to exactly characterize a particular trajectory eventually revealed as the system evolves and $t \to \infty$. For the continuous valued chaotic sources, a usual measure for this information production is the Kolmogorov-Sinai entropy [2] while in the context of information theory, the appropriate view of the problem is that of *entropy rate*. Note that the Kolmogorov-Sinai entropy (or *metric entropy*) leads to the proper notion of entropy rate and is therefore compatible with Shannon's information theoretic framework.

3.1.1. Entropy rate of chaotic systems

A positive entropy rate is connected with the very nature of chaotic dynamical systems, with *chaos* itself. To see this, note that the Kolmogorov-Sinai entropy is equal to the sum of the *positive* Lyapunov exponents. Take as an example the evolution of iterated piecewise linear Markov (PWLM) maps $f(\cdot)$. In this case, the of the entropy rate discussion is simplified considerably. As shown in [3], for PWLM there exists a natural discretization which defines a symbolic sequence $\boldsymbol{s}$ and consequently a symbolic dynamics that includes the entire behavior relevant to an information theoretic treatment. The discretization in fact assigns symbols to each linear region (piece) of the map. Following the above discussion, the entropy rate of a PWLM map is precisely defined by the entropy rate of it's symbolic sequence.

3.1.2. Chaotic systems in the transmitted reference framework

From what has been shown, any communication scheme in which chaotic signals are used in the transmitter, involves a positive entropy process S (as shown in the block scheme Fig. 1). Therefore, quite generally one will be able to separate the transmitter into a chaos source part (furnishing S, however complicated) and some deterministic, non-chaotic post processing combining B and S (transmitter part). Take for example DCSK as defined in . For each transmitted symbol B, a vectorial $\boldsymbol{S}$ of length $N/2$ with entropy $H(\boldsymbol{S})$ equal to $N/2$ times the entropy rate of the chaotic system generating S are combined in the transmitter. Thus, it can be concluded that the use of chaos results in sub-optimal performance of the communication scheme in Shannon's sense, as long as the chaotic sequence can be observed at the receiver, i.e. $I(S; Y) > 0$. In particular, it is intuitively clear that any chaos based communication scheme involving (chaos-) synchronization at the receiver [4] is sub-optimal as this clearly contradicts $I(X; Y|B) = 0$ from corollary 3. In [5] it is shown that in AWGN sub-optimality can be demonstrated even if synchronization is still possible even at vanishing noise levels. In fact, then, $I(S; X) > 0$ is already enough to ascertain that capacity can no longer be reached.

4. CSK with tent maps: a case study

In the previous sections, a rather general approach to judging the use of chaos in the transmitter has been presented. These results shall now be illustrated by means of a simple example, namely a transmitter for chaos shift keying (CSK). For this scheme, the optimal receiver [4] is available (for the AWGN channel), thus it is possible to study the influence of the transmitter and to draw conclusions based on the best design parameters leading to optimal performance. In order to keep the setup simple, binary CSK is considered, such that for a symbol period of N samples (discrete time), the state is iterated by applying a skewed tent map f_1 with breakpoint parameter a_1 if 1 is to be communicated, and an inverted skewed tent map with breakpoint parameter a_2 for transmitting 0. This scheme is well known and studied for $a_1 = a_2$. Little has been done to understand if this particular pair of maps represents a good choice for the overall performance of the communication system.

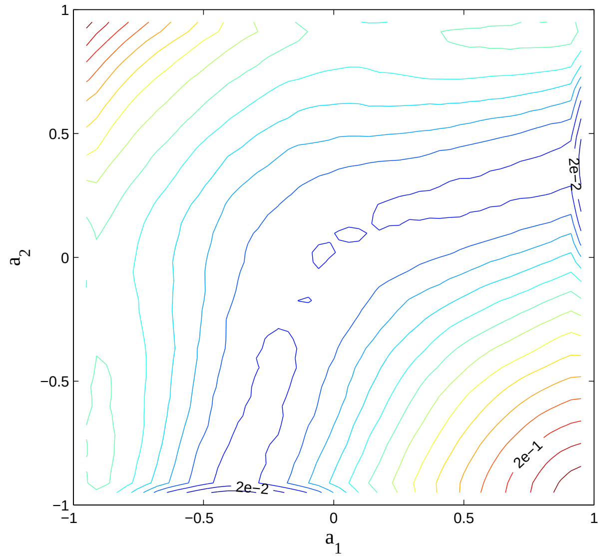

Figure 3: BER for binary CSK (regular and inverted skew tent map, skew a_1, a_2), block length $N = 4$, SNR 15 dB).

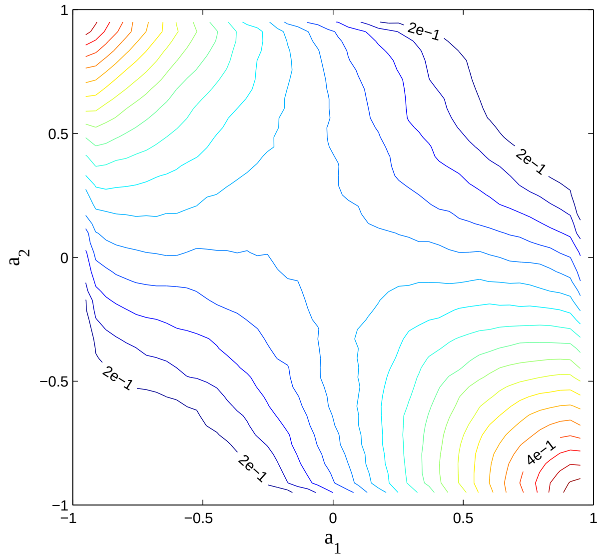

Figure 4: BER for binary CSK (regular and inverted skew tent map, skew a_1, a_2), block length $N = 4$, SNR 9 dB).

Shown in Figs. 3 and 4 for two different signal to noise ratios is the bit error rate performance for any pair a_1, a_2, each describing a particular CSK receiver. These results have been obtained numerically by simulating the optimal receiver [5]. It can be observed from those figures that the best performance, in particular for low SNR, is obtained for *degenerated* pairs of maps, i.e. values of a_1, a_2 close to ± 1. This is consistent with the theory developed before, as for such values, the entropy rates of the involved chaotic systems is minimal. One may now proceed to a more thorough analysis of CSK designs by using the information theoretic tools developed above, in order to gain insights on how to improve the performance.

5. Conclusions

In this paper, the impact of chaos present in transmitters for chaos based communications has been discussed, based on arguments from information theory, in a systematic way. It has been shown that optimality (achieving capacity) and the fact that a chaotic signal is "visible" at the receiver represent a contradiction. This has been set forth in general and also been illustrated by means of a very simple example exploring a particular class of transmitters for one that optimizes overall performance.

Note though that the actual performance penalty depends upon the value of $I(S;Y)$ (or, equivalently, $I(X;Y|B)$), which provide a lower bound on the loss of capacity in the system. Furthermore, the performance of the overall system further depends on the transmitter's ability to optimally use the remaining channel capacity $I(X;Y|S)$. In fact, the above discussion is not necessarily a reason to be pessimistic about chaos based communications. It is well known that for example BPSK [6] is suboptimal for high SNR. There are many other modulation schemes in current use which do not utilize the channel optimally, but gain advantages in implementation. Thus, a chaos based communication system can be worthwhile provided that the communication of side information over the channel $I(S;Y)$ is not too high. If this intrinsic price of the use of chaos is known at design time, it permits a realistic analysis of the tradeoff between the advantages of chaos (such as it's simple generation and easily achieved broad band nature) and the systematic performance penalty with respect to the efficiency of the system in terms of exploiting the capacity of the communication channel in an information theoretic sense.

6. Acknowledgement

The author would like to thank Prof. Martin Hasler and Prof. Emre Telatar for many useful discussions on the topic.

References

[1] T.M. Cover and J.A. Thomas, "Elements of Information Theory", *Wiley*, NY, 1991.

[2] M. Pollicott and M. Yuri, "Dynamical Systems and Ergodic Theory", Cambridge Univ. Press, 1998.

[3] T. Schimming "Chaos Based Modulations From An Information Theory Perspective", *Proc. ISCAS 2001*, Sydney, Australia.

[4] M. Hasler and T. Schimming. "Optimal and suboptimal chaos-receivers", *Proc. IEEE*, May, 2002.

[5] T. Schimming "Statistical Analysis and Optimization of Chaos Based Broadband Communications", Ph.D. thesis, EPFL, 2002

[6] J.G. Proakis, *Digital Signal Processing*, Macmillan Publishing, New York, 1992.