OPTIMAL DETECTION OF A CLASS OF CHAOTIC SIGNALS

Haralabos C. Papadopoulos and Gregory W. Wornell

Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, MA 02139

ABSTRACT

Chaotic signals are increasingly of interest for use in a range of engineering applications. This paper describes optimal estimation and detection algorithms for use with a potentially important class of discrete-time chaotic signals generated via tent maps. We develop and evaluate, in particular, Maximum Likelihood (ML) estimation algorithms for filtering, predicting, and smoothing these signals from noise-corrupted measurements, and present highly efficient, recursive implementations for these nonlinear algorithms. We also develop ML detection algorithms for discriminating among classes of chaotic signals generated from tent maps, and use the results to explore the viability of a simple paradigm for secure communication based on these chaotic signals.

1. INTRODUCTION

Chaotic signals, *i.e.*, signals which can be described as outputs of nonlinear dynamical systems exhibiting chaotic behavior are appealing candidates for use in a variety of engineering contexts. In terms of signal analysis, these signals constitute potentially useful models for a range of natural phenomena. In terms of signal synthesis, the special characteristics of chaotic signals are attractive in a number of broadband communication and radar applications. In order to exploit chaotic signals in both types of applications, there is a need for robust and efficient algorithms for the detection and estimation of these signals in the presence of various forms and amounts of distortion.

A variety of heuristically reasonable algorithms have been proposed for estimating a chaotic signal in backgrounds of additive, stationary white Gaussian noise given varying degrees of *a priori* information; see *e.g.*, [1] – [4]. However, the development of optimal estimators for these scenarios has generally proved to be rather difficult.

In this paper, we focus our attention on the particular class of first-order, discrete-time chaotic signals whose dynamics are governed by the so-called tent map. For these chaotic signals, we are able to develop estimators that are optimal in a Maximum Likelihood (ML) sense, and possess highly convenient recursive implementations. While this class of signals may be overly restrictive for many signal modeling applications, the results suggest a general estimator structure that may prove useful for a much larger class of chaotic signals.

In the second half of the paper, using a generalized likelihood ratio test formulation we develop optimal detection strategies for discriminating between two classes of chaotic signals derived from tent maps. We then consider a simplified secure communications paradigm based on chaotic signals, and use the detection algorithms and their performance characteristics to assess the viability of such applications. In addition, our results suggest more general algorithmic structures for discriminating among different classes of chaotic signals. In turn, these algorithms are of potential interest in a range of signal classification problems.

2. CHAOTIC SEQUENCES FROM TENT MAPS

The chaotic sequences $x[n]$ of interest in this work are generated according to the following one-dimensional dynamics

$$x[n] = F(x[n-1]), \tag{1}$$

where $F(\cdot)$ is a symmetric tent map, *i.e.*,

$$F(x) = \beta - 1 - \beta|x| \tag{2}$$

for some parameter $1 < \beta \leq 2$.

These mappings typically produce sequences which are ergodic [5] and whose values lie in the range $[-1, \beta - 1]$. However, their full first-order densities (*i.e.*, invariant distributions) cannot, in general, be readily described in closed form. Likewise, the time-averaged spectra of these processes are generally broadband, although their detailed characteristics are not easily described.

The Lypunov exponent λ of the map is a measure of the numerical sensitivity of the map, describing, in particular, the average rate at which successive iterates generated from nearby initial conditions $x[0]$ diverge. For the tent maps defined in (2),

$$\lambda = \log \beta. \tag{3}$$

For the map corresponding to $\beta = 2$, one can derive more detailed results. In particular, the invariant density is uniform [5], *i.e.*,

$$p(x) = \begin{cases} 1/2 & |x| < 1 \\ 0 & \text{otherwise} \end{cases}. \tag{4}$$

This work has been supported in part by the Advanced Research Projects Agency monitored by ONR under Contract No. N00014-89-J-1489, and the Air Force Office of Scientific Research under Grant No. AFOSR-91-0034.

0-7803-0946-4/93 $3.00

Furthermore, since both $F(\cdot)$ and the invariant density (4) are even functions, it follows that

$$R[k] = E\left[x[n+k]\,x[n]\right] = E\left[x[n]\,F^{(k)}(x[n])\right] = (1/3)\delta[k],$$

where $F^{(k)}(\cdot)$ denotes the k-fold composition of $F(\cdot)$ with itself, and where $\delta[k]$ is the unit-sample. Hence $x[n]$ has a time-averaged spectrum that is white, *i.e.*,

$$S(\omega) = 1/3, \quad \text{all } \omega. \tag{5}$$

A particularly useful representation for chaotic sequences generated from one-dimensional maps is obtained from descriptions of the maps in terms of symbolic dynamics [6]. We now summarize the results for the case of tent maps defined in (2).

We begin by noting that $F(\cdot)$ is not invertible. However, because $F(\cdot)$ is unimodal and even, it has two inverse branches, *i.e.*, given $v = F(x)$, x can be determined from v to within a $\pm$ sign. We denote the two inverses of $F(\cdot)$ by

$$F_s^{-1}(v) = \frac{\beta - 1 - v}{\beta} \cdot s, \tag{6}$$

where $s = \pm 1$. Thus, we have the relation

$$v = F(x) \;\Rightarrow\; x = F^{-1}_{\operatorname{sgn} x}(v).$$

From this perspective, an alternative representation is obtained for a sequence

$$x[0],\, x[1],\, \ldots,\, x[N] \tag{7}$$

generated according to (1) using (2). In particular, for each n we have

$$x[n] = F^{-1}_{s[n]} \circ F^{-1}_{s[n+1]} \circ \ldots \circ F^{-1}_{s[N-1]}(x[N]) \tag{8}$$

with $F_s^{-1}(\cdot)$ as given by (6) and where

$$s[n] = \operatorname{sgn} x[n].$$

Hence,

$$s[0],\, s[1],\, \ldots,\, s[N-1],\, x[N] \tag{9}$$

is an equivalent representation for (7), and (8) defines the coordinate transformation.

3. ESTIMATION OF TENT MAP SEQUENCES

In this section, we consider the following scenario involving noisy observations

$$y[0],\, y[1],\, \ldots, y[N] \tag{10}$$

of chaotic tent map sequence. Specifically, suppose

$$y[n] = x[n] + w[n], \tag{11}$$

where $w[n]$ is a stationary, zero-mean white Gaussian noise sequence with variance σ_w^2, and where $x[n]$ is a tent map sequence generated by iterating some unknown $x[0] \in (-1, \beta - 1)$ according to (1) using the tent map (2) for some parameter β. The objective is to obtain ML estimates of

$$x[0],\, x[1],\, \ldots, x[N]$$

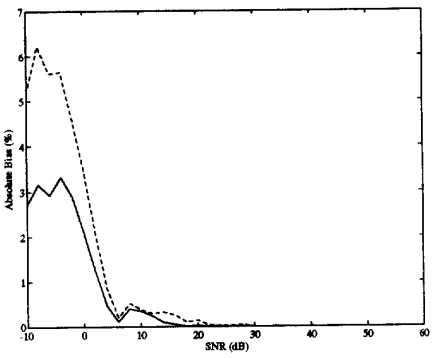

Figure 1: *Bias in the ML estimate ($\beta = 2$).*

from the noisy data.

Because ML estimates commute with invertible coordinate transformations we may equivalently recast the problem as one of finding ML estimates for either $x[0]$ or, in accordance with the results of Section 2, the coordinates (9). However, although estimating $x[0]$ directly is appealing, this leads to a difficult optimization problem. Indeed, as reported in [7], for chaotic maps of this type the likelihood function is typically a highly irregular function with fractal characteristics. Consequently, gradient descent algorithms cannot practically be applied.

However, the representation (9) turns out to be highly useful in deriving the ML estimates. The algorithm that results from this approach can be partitioned into two stages: filtering and smoothing.

3.1. FILTERING

The filtering stage provides, for $n = 0, 1, \ldots, N$, ML estimates $\hat{x}[n|n]$ of $x[n]$ given $y[k]$ for $k \le n$. These estimates are be obtained in a computationally efficient forward pass through the data using a recursive algorithm. In particular, we have

$$\hat{x}[n|n] = \frac{(\beta^2 - 1)\beta^{2n}\, y[n] + (\beta^{2n} - 1)\,\hat{x}[n|n-1]}{\beta^{2(n+1)} - 1}, \tag{12}$$

where $\hat{x}[n|n-1]$ is a one-step prediction, *i.e.*,

$$\hat{x}[n|n-1] = F(\hat{x}[n-1|n-1]),$$

and where the recursion is initialized with $\hat{x}[0|0] = y[0]$.

In general, these ML estimates are biased. In Fig. 1, the dashed curve indicates the bias in the filtered signal estimates as a function of signal-to-noise ratio (SNR), *i.e.*, $-10\log_{10}\sigma_w^2$, for the case $\beta = 2$. As this plot suggests, however, the ML estimates are asymptotically unbiased at high SNR.

The Cramér-Rao bound on $\hat{x}[n|n]$ in this case turns out to be

$$\operatorname{var} \hat{x}[n|n] \ge (3/4)\sigma_w^2 \cdot \left[1 - (1/4)^{n+1}\right]^{-1} \tag{13}$$

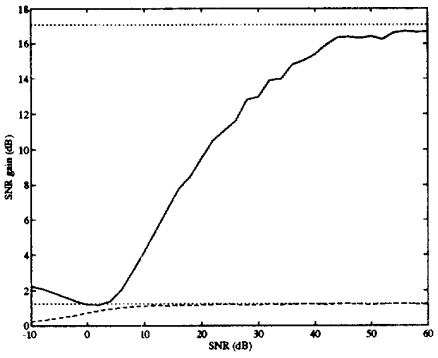

Figure 2: *SNR gain in the ML estimate ($\beta = 2$).*

which decays to $(3/4)\sigma_w^2$ as $n \to \infty$. Hence, the filtering gain is at most

$$10\log_{10}(4/3) \approx 1.25 \text{ dB} \tag{14}$$

which is notably small. In Fig. 2, the dashed curve depicts the SNR gain (over simply hard-limiting $y[n]$) in the filtered signal estimates as a function of SNR for the case $\beta = 2$, and a dotted line indicates the bound (14). Note that at high SNR the Cramér-Rao bound is attained asymptotically, *i.e.*, the estimates are asymptotically efficient.

3.2. SMOOTHING

The smoothed ML estimates, which we denote by $\hat{x}[n|N]$, correspond to estimates of each $x[n]$ using the entire data set (10). These estimates are obtained by a backward propagation of the filtered estimates. In particular,

$$\hat{x}[n|N] = F_{\hat{s}[n]}^{-1}(\hat{x}[n+1|N]) \tag{15}$$

where

$$\hat{s}[n] = \hat{s}[n|N] = \hat{s}[n|n] = \operatorname{sgn} \hat{x}[n|n]. \tag{16}$$

In this case, the recursion is initialized with $\hat{x}[N|N]$, the last estimate obtained from the filtering stage. Note, however, that this backward pass doesn't require any further access to the data but only to the filtered estimates. Consequently, the estimation can be implemented so as to be efficient not only in terms of computation but also in terms of storage. In particular, each $y[n]$ may be replaced in storage with $\hat{x}[n|n]$ immediately after it is computed.

The smoothed estimates are also asymptotically unbiased at high SNR, as the solid curve in Fig. 1 indicates for the case $\beta = 2$. Furthermore, at high SNR and large N, we have the geometric error variance progression

$$\operatorname{var} \hat{x}[n|N] \approx (1/\beta^2)^{(N-n)}(3/4)\sigma_w^2$$

since with high probability

$$\hat{s}[n] = s[n] = \operatorname{sgn} x[n]$$

in this regime. In this case, the average estimation error is

$$\frac{1}{N+1}\sum_{n=0}^{N} \operatorname{var} \hat{x}[n|N] \approx \frac{\sigma_w^2}{N+1}. \tag{17}$$

The solid curve in Fig. 2 indicates the SNR gain in the smoothed estimates over a range of SNR when $N = 50$ for the case $\beta = 2$, and the upper dotted line indicates the asymptotic smoothing gain

$$10\log_{10}(N+1) \approx 17 \text{ dB}$$

obtained via (17). Note that the smoothing yields dramatically better signal estimates than filtering alone, particularly in the high SNR regime. Clearly, the backward filtering stage in the smoothing algorithm is critical to achieving good signal estimation performance.

3.3. PREDICTION

One-step ML predictors arose rather naturally in the solution to the filtering problem. More generally, K-step predictors can also be derived. In particular, using $\hat{x}[N+K|N]$ to denote the ML estimate of $x[N+K]$ for $K \geq 1$ given the data set (10), it can be shown that

$$\hat{x}[N+K|N] = F^{(K)}(\hat{x}[N|N])$$

where $\hat{x}[N|N]$ is obtained via the filtering algorithm of Section 3.1. It is relatively straightforward to show that the error in these estimates satisfies, for large N, small K, and high SNR

$$\operatorname{var} \hat{x}[N+K|N] \approx \beta^{2K}(3/4)\sigma_w^2.$$

Note that the error variance grows exponentially with K at a rate given by the Lyapunov exponent (3), consistent with the "sensitivity to initial conditions" characteristic of these chaotic maps.

4. DETECTION OF TENT MAP SEQUENCES

One potential application area for chaotic signals is in secure communications. To explore the basic viability of the concept, in this section we optimize and evaluate a simplified spread spectrum scheme that employs chaotic waveforms.

In the signaling scheme of interest, each successive bit in the data stream is represented by a chaotic sequence generated from one of two "antipodal" tent maps. More specifically, in the k-th signaling interval the transmitter codes the binary symbol $b[k]$ with an $(N+1)$-point sequence

$$\sqrt{E_0}x[(N+1)k],\ \sqrt{E_0}x[(N+1)k+1],\ \ldots,\ \sqrt{E_0}x[(N+1)k+N]$$

generated according to

$$x[n] = \begin{cases} +F(x[n-1]) & \text{if } b[k] = 0 \\ -F(x[n-1]) & \text{if } b[k] = 1 \end{cases} \tag{18}$$

where $F(\cdot)$ is as defined in (2) with $\beta = 2$, where the $x[(N+1)k] \in (-1, 1)$ are randomly generated, and where E_0 is the peak transmitter power. Using (4), it is straightforward

to determine that the resulting transmission has a peak-to-average power ratio given by

$$10\log_{10}\left(1/E\left[x^2[n]\right]\right) = 10\log_{10} 3 \approx 4.8 \text{ dB}.$$

and some attractive pseudorandom properties. In particular, owing to the properties of the tent map (*cf.*, (5)), the time-averaged spectrum of the transmitted sequence is white.

Consider an optimal incoherent receiver structure for a chaotic signaling scheme of this type. We assume that the received data is of the form (11) where, again, $w[n]$ is real-valued, zero-mean, stationary, additive white Gaussian noise of variance σ_w^2. We further assume that $b[k]$ is a random bit stream, and that the $x[(N+1)k]$ are not known or available to the receiver. Without loss of generality, it suffices to consider the case of the particular signaling interval corresponding to $k = 0$.

Detection of $b[0]$ may be phrased in terms of a composite hypothesis test [8]. In this case, the corresponding generalized likelihood ratio test with a minimum probability of error criterion reduces to the following detection rule:

$$\hat{b}[0] = \arg\max_{b[0],\mathbf{x}} p(\mathbf{y}|b[0],\mathbf{x}), \tag{19}$$

where

$$\begin{aligned}\mathbf{x} &= (x[0],\, x[1],\, \ldots,\, x[N])\\ \mathbf{y} &= (y[0],\, y[1],\, \ldots,\, y[N]).\end{aligned}$$

We note that detection of $b[0]$ requires that ML estimates of $\mathbf{x}$ be computed in the process using the algorithms of Section 3. Specifically, the optimal receiver computes ML estimates of $\mathbf{x}$ both for $b[0] = 0$ and for $b[0] = 1$, and chooses for $\hat{b}[0]$ the value of $b[0]$ which yields the larger likelihood value, *i.e.*,

$$\hat{b}[0] = \arg\min_{b[0]} \sum_{n=0}^{N} \left(y[n] - \hat{x}[n|N, b[0]]\right)^2,$$

where $\hat{x}[n|N, b[0]]$ denotes the ML estimate of $x[n]$ given $\mathbf{y}$ and $b[0]$.

It is convenient to interpret the resulting coding scheme as one in which, during each signaling interval, 1's and 0's are represented by randomly chosen elements from one of two ensembles of codewords. In general, the properties of these ensembles strongly affect the performance of the resulting signaling scheme. Let $d_N(u, v)$ be the distance between a codeword in one ensemble generated from the initial condition u and a codeword in the other ensemble generated from initial condition v, *i.e.*,

$$d_N^2(u, v) = \sum_{n=0}^{N} \left[F^{(n)}(u) - (-F)^{(n)}(v)\right]^2.$$

Then, in particular, the RMS and minimum values of d_N are important quantities in characterizing the performance of the coding. It is relatively straightforward to show that

$$d_{\min}(N) = \min_{u,v} d_N(u, v)$$

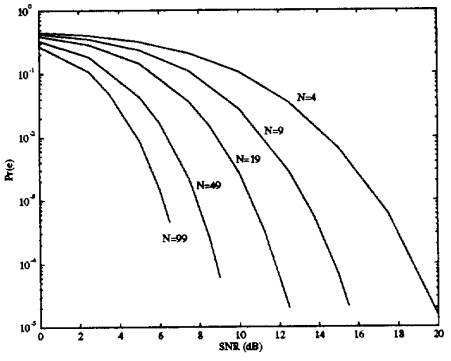

Figure 3: *Probability of error performance of chaotic signaling.*

satisfies $d_{\min}(N) > 0$ for $N \geq 2$, and $d_{\min}(N) \to \infty$ as $N \to \infty$. The last of these two results implies, in particular, that the bit error rate can be made arbitrarily small provided N is chosen sufficiently large.

Monte-Carlo simulations provide more detailed results concerning the performance of the incoherent receiver derived in this section. In Fig. 3, we plot (uncoded) bit-error probability as a function of SNR for several values of N. Obviously, other aspects of the scheme that warrant investigation in future work include immunity to jamming, other forms of interference, and detection by unintended receivers.

REFERENCES

[1] A. C. Singer, G. W. Wornell, and A. V. Oppenheim, "Modeling and estimation of nonlinear and chaotic signals in the presence of noise," *IEEE Trans. Signal Processing*, 1992. Submitted for publication.

[2] M. D. Richard, "Probabilistic state estimation with discrete-time chaotic systems," RLE Tech. Rep. No. 571, M. I. T., Cambridge, MA, Mar. 1992.

[3] C. Myers, A. Singer, B. Shin, and E. Church, "Modeling chaotic systems with hidden Markov models," in *Proc. Int. Conf. Acoust. Speech, Signal Processing*, 1992.

[4] M. Casdagli, S. Eubank, J. D. Farmer, and J. Gibson, "State space reconstruction in the presence of noise," *Physica D*, vol. 51, pp. 52–98, 1991.

[5] A. Lasota and M. C. Mackey, *Probabilistic Properties of Deterministic Systems*. Cambridge University Press, 1985.

[6] B.-L. Hao, "Symbolic dynamics and characterization of complexity," *Physica D*, vol. 51, pp. 161–176, 1991.

[7] C. Myers, S. Kay, and M. Richard, "Signal separation for nonlinear dynamical systems," in *Proc. Int. Conf. Acoust. Speech, Signal Processing*, 1992.

[8] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I.* New York, NY: John Wiley and Sons, 1968.