Available online at www.sciencedirect.com
ScienceDirect
Chaos, Solitons and Fractals 38 (2008) 132–139
CHAOS
SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

The Cramer-Rao bound for initial conditions estimation of chaotic orbits

Marcio Eisencraft [a,*], Luiz Antonio Baccalá [b]

[a] Universidade Presbiteriana Mackenzie, Escola de Engenharia, São Paulo, Brazil
[b] Universidade de São Paulo, Escola Politécnica, São Paulo, Brazil

Accepted 30 October 2006

Communicated by Prof. M.S. El Naschie

Abstract

We derive the Cramer-Rao Lower Bound (CRLB) for the estimation of initial conditions of noise-embedded orbits produced by general one-dimensional maps. We relate this bound's asymptotic behavior to the attractor's Lyapunov number and show numerical examples. These results pave the way for more suitable choices for the chaotic signal generator in some chaotic digital communication systems.

1. Introduction

Over the last decade many results associated with the application of chaotic signals in digital communication have appeared (e.g. [1–7] and references therein). In these systems, digital information is mapped directly onto wide-band chaotic waveforms in lieu of periodic waveforms. Due to their wideband features, such systems spread spectral energy and potentially mitigate both multipath and jamming effects [4,6,8].

Many systems can generate chaos and it is natural to ask whether a given chaotic signal generator may provide superior system performance over others. Whereas this question remains unanswered in general, the restricted yet important class of chaos generating systems based on one-dimensional piece-wise linear maps is among the more commonly used ones because of its simplicity. In its employment, however, there is very little concern about optimality issues associated with improving communication performance [2].

To compare generic one-dimensional chaos generating maps, we examine the Cramer-Rao lower bound (CRLB) for the estimation of the initial condition of chaotic orbits in the presence of additive observation noise. We show that the CRLB is related to the attractor's Lyapunov number L that is often used to measure ''chaoticness'' and whose numerical determination is achievable through a variety of techniques [9].

* Corresponding author.
E-mail addresses: marcioft@mackenzie.br (M. Eisencraft), baccala@lcs.poli.usp.br (L.A. Baccalá).
URLs: http://meusite.mackenzie.br/marcioft (M. Eisencraft), http://www.lcs.poli.usp.br/~baccala (L.A. Baccalá).

0960-0779/$ - see front matter © 2006 Published by Elsevier Ltd.
doi:10.1016/j.chaos.2006.10.067

Even though the CRLB represents just a performance limit, one must note that it is possible to derive estimators, such the maximum likelihood one, which attain this limit, being asymptotically unbiased and efficient [10,11].

This paper is organized as follows. In Section 2 we formulate the estimation problem while Section 3 contains the main theoretical results followed by three numerical illustrations in Section 4. Section 5 contains a brief discussion of the significance of these results.

2. Problem formulation

Let $f(\cdot)$ be a function whose domain and range space is the same set $U \subset \mathbb{R}$. The difference equation

$$s(n+1) = f(s(n)), \quad n \in \mathbb{N},\ s(0) \in U \tag{1}$$

defines a *discrete time dynamical system* or *map*. Each *orbit* of this map becomes defined by an *initial condition* s_0, being denoted as $s(n, s_0)$ where

$$s(n, s_0) = f^n(s_0), \tag{2}$$

with $f^n(\cdot)$ standing for the nth successive application of $f(\cdot)$. An orbit will be symbolized by $s(n)$ whenever s_0 is immaterial.

A sequence of N noise corrupted observations is given by

$$s'(n) = s(n, s_0) + r(n), \quad 0 \leqslant n \leqslant N-1, \tag{3}$$

where $r(n)$ is zero mean Additive White Gaussian Noise (AWGN) of variance σ_r^2. Our goal is to estimate the initial condition s_0.

To simplify notation, consider the vectors

$$\mathbf{s} = [s(0), s(1), \ldots, s(N-1)]^{\mathrm{T}}, \tag{4}$$

$$\mathbf{r} = [r(0), r(1), \ldots, r(N-1)]^{\mathrm{T}} \text{ and} \tag{5}$$

$$\mathbf{s}' = [s'(0), s'(1), \ldots, s'(N-1)]^{\mathrm{T}}. \tag{6}$$

The smallest attainable mean square error (mse) of any unbiased estimation method is given by

$$\mathrm{mse}(\hat{s}_0) \geqslant \frac{1}{-E\left[\frac{\partial^2 \ln p(\mathbf{s}';s_0)}{\partial s_0^2}\right]} \tag{7}$$

where $p(\mathbf{s}'; s_0)$ is the likelihood function of the observations [12]. The term on the right-hand side of (7) represents the *Cramer-Rao Lower Bound* (CRLB) for estimating s_0 in (3) [12].

Our main objectives are (a) to deduce an expression for this CRLB and (b) relate this bound to statistical properties of the attractor, specifically the Lyapunov number $L(s_0)$, defined as [13]

$$L(s_0) = \lim_{N\to\infty} \left(\prod_{n=0}^{N-1} \left| \frac{\mathrm{d}f}{\mathrm{d}s}\Big|_{s(n)} \right| \right)^{\frac{1}{N}} \tag{8}$$

if this limit exists.

3. CRLB for 1-D map initial condition estimation

Proposition 1 establishes the CRLB for the problem of estimating the initial condition of an orbit as a function of the derivatives of $f(\cdot)$.

Proposition 1. *Given the orbit $s(n, s_0)$ associated to (1) whose map $f(\cdot)$ possesses derivatives at all orbit points, the CRLB for estimating s_0 given $s'(n)$ and $f(\cdot)$, under the conditions represented by (3) is*

$$\mathrm{mse}(\hat{s}_0) \geqslant \frac{\sigma_r^2}{1 + \sum_{n=1}^{N-1} \left(\prod_{j=0}^{n-1} \frac{\mathrm{d}f}{\mathrm{d}s}\big|_{s(j,s_0)} \right)^2}. \tag{9}$$

Proof. Using the vectors defined in Eqs. (4)–(6) $\mathbf{s}'$ is given by

$$\mathbf{s}' = \mathbf{s}(s_0) + \mathbf{r}, \tag{10}$$

where the dependence on s_0 is shown explicitly. As $\mathbf{r}$ is composed of jointly independent gaussian random variables, the probability density function of $\mathbf{s}'$ is

$$p(\mathbf{s}'; s_0) = \frac{1}{(2\pi\sigma_r^2)^{\frac{N}{2}}} \exp\left[-\frac{1}{2\sigma_r^2}\sum_{n=0}^{N-1}(s'(n) - s(n, s_0))^2\right], \tag{11}$$

whose logarithm leads to

$$\frac{\partial \ln p(\mathbf{s}'; s_0)}{\partial s_0} = \frac{1}{\sigma_r^2}\sum_{n=0}^{N-1}(s'(n) - s(n, s_0))\frac{\partial s(n, s_0)}{\partial s_0}, \tag{12}$$

upon differentiating with respect to s_0. Further differentiation, produces

$$\frac{\partial^2 \ln p(\mathbf{s}'; s_0)}{\partial s_0^2} = \frac{1}{\sigma_r^2}\sum_{n=0}^{N-1}\left[(s'(n) - s(n, s_0))\frac{\partial^2 s(n, s_0)}{\partial s_0^2} - \left(\frac{\partial s(n, s_0)}{\partial s_0}\right)^2\right], \tag{13}$$

whose expected value is given by

$$E\left[\frac{\partial^2 \ln p(\mathbf{s}'; s_0)}{\partial s_0^2}\right] = -\frac{1}{\sigma_r^2}\sum_{n=0}^{N-1}\left(\frac{\partial s(n, s_0)}{\partial s_0}\right)^2. \tag{14}$$

To obtain (9), one must write (14) in terms of $f(\cdot)$ derivatives. Using the chain rule and (2) one gets

$$\frac{\partial s(n, s_0)}{\partial s_0} = \frac{\mathrm{d}f^n}{\mathrm{d}s}\Big|_{s_0} = \begin{cases} \frac{\mathrm{d}f}{\mathrm{d}s}|_{s(0)} \cdot \frac{\mathrm{d}f}{\mathrm{d}s}|_{s(1)} \cdot \cdots \cdot \frac{\mathrm{d}f}{\mathrm{d}s}|_{s(n-1)}, & n \geqslant 1, \\ 1, & n = 0 \end{cases} \tag{15}$$

and substitution of (15) into (14) produces

$$E\left[\frac{\partial^2 \ln p(\mathbf{s}'; s_0)}{\partial s_0^2}\right] = -\frac{1}{\sigma_r^2}\left(1 + \sum_{n=1}^{N-1}\left(\prod_{j=0}^{n-1}\frac{\mathrm{d}f}{\mathrm{d}s}|_{s(j,s_0)}\right)^2\right), \tag{16}$$

which finally produces (9) using (7) thereby finishing the proof. □

Note that (9) holds for both chaotic and non-chaotic orbits. In general, the CRLB for the initial condition depends on the very value s_0 being estimated. For chaotic orbits, however, this dependence becomes less pronounced as N grows. This is a consequence of the tendency of $s(n, s_0)$ to roam all over the attractor, the *topological transitiveness* [14]. This property appears clearly in the next proposition.

Proposition 2. *Under the same conditions as in Proposition 1, the CRLB limit when $N \to \infty$ is*

$$\mathrm{mse}(\hat{s}_0) \geqslant \sigma_r^2 \frac{L^2 - 1}{L^{2N} - 1}, \tag{17}$$

where $L \equiv L(s_0) \neq 1$ is the Lyapunov number of the attractor to which the orbit $s(n, s_0)$ converges.

Proof. For sufficiently large n, we can use the Lyapunov number defined by Eq. (8) to approximately calculate

$$\left(\frac{\partial s(n, s_0)}{\partial s_0}\right)^2 = \left(\frac{\mathrm{d}f}{\mathrm{d}s}|_{s(0)} \cdot \frac{\mathrm{d}f}{\mathrm{d}s}|_{s(1)} \cdot \cdots \cdot \frac{\mathrm{d}f}{\mathrm{d}s}|_{s(n-1)}\right)^2 \approx L^{2n}(s_0). \tag{18}$$

Therefore,

$$\sum_{n=0}^{N-1}\left(\frac{\partial s(n, s_0)}{\partial s_0}\right)^2 \approx \sum_{n=0}^{N-1} L^{2n}(s_0) = \frac{L^{2N}(s_0) - 1}{L^2(s_0) - 1} \tag{19}$$

so that Eq. (14) reduces to

$$E\left[\frac{\partial^2 \ln p(\mathbf{s}';s_0)}{\partial s_0^2}\right] \approx -\frac{1}{\sigma_r^2}\frac{L^{2N}(s_0)-1}{L^2(s_0)-1}, \tag{20}$$

for large N.

Therefore, considering that the orbit converges to an attractor whose Lyapunov number is L, substituting (20) into (7) leads to (17) and the proposition is demonstrated. □

Even for fairly small values of N, (17) represents an approximation to the CRLB for chaotic orbits. This is so because L is a geometrical mean of the derivatives of the map at the orbit points and can adequately replace the true product of the derivatives at the first N orbit points. Thanks to the topological transitivity, this simplification yields reasonably accurate results.

For chaotic orbits, it is important to realize that increasing N implies an exponential decrease in the estimation error ϵ of s_0 (17), but that the uncertainty in computing $s(N-1,s_0)$ is $O(\max(s(N-1,s_0), \epsilon L^{N-1}))$ so that even minute estimation errors in s_0 are severely amplified in accord with the sensitive dependence that characterizes chaotic dynamics.

Hence, if a chaotic communication system can be built that relies on initial condition estimations, one can profit by choosing maps with high Lyapunov numbers even though one should not expect precise reconstruction of the whole orbit from such an estimated s_0.

A version of these results for piecewise linear maps was derived in [15]. This problem was also treated in different ways by [9,11,16]. None of the these works, however, provided general explicit formulae for the CRLB as a function of the map's Lyapunov number.

4. Numerical examples

This section examines three illustrative examples starting with the simple case of the tent map followed by the more general skew tent map family and ending with a quadratic (non-piecewise linear) map.

4.1. The tent map $f_T(\cdot)$

This map is defined by

$$f_T(s) = 1 - 2|s|, \ -1 \leqslant s \leqslant 1. \tag{21}$$

As $f_T(\cdot)$ is piecewise linear and the absolute value of its derivative is constant, the approximation of (18) becomes exact for any chaotic orbit of this map whose Lyapunov number is $L(s_0) = L_T = 2$ irrespective of s_0. Thus (17) holds for all $N > 0$ and not just for $N \to \infty$ and the CRLB

$$\mathrm{mse}(\hat{s}_0) \geqslant \sigma_r^2 \frac{3}{4^N - 1} \tag{22}$$

is independent of s_0.

Fig. 1 shows the allied CRLB as a function of N when $\sigma_r = 1$. For comparison, the same plot contains the CRLB for the estimation of a constant under AWGN [12]. Even for fairly short observation sequences, we obtain low CRLB values. This translates, in principle, into the possibility of achieving very good initial condition estimates for the chaotic orbits of this map.

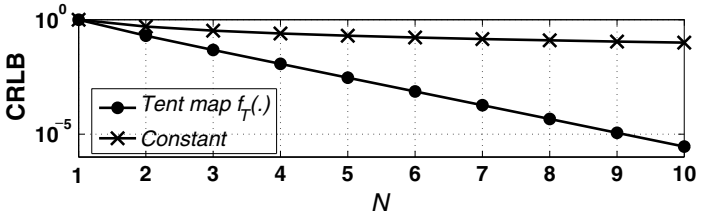

Fig. 1. CRLB for the initial condition estimation of an orbit of the tent map $f_T(\cdot)$ under AWGN of unit variance compared to estimating a constant value under the same noise conditions.

4.2. Skew tent maps $f_I(\cdot)$

This family of maps

$$s(n+1) = f_I(s(n)) = \begin{cases} \frac{2}{\alpha+1}s(n) + \frac{1-\alpha}{\alpha+1}, & -1 < s(n) < \alpha \\ \frac{2}{\alpha-1}s(n) - \frac{\alpha+1}{\alpha-1}, & \alpha \leqslant s(n) < 1 \end{cases} \tag{23}$$

is parameterized by $\alpha \in (-1,1)$, which determines the x-coordinate of the tent's peak and the chaotic orbits' Lyapunov number [17,18]

$$L_I = \left(\frac{2}{\alpha+1}\right)^{\frac{\alpha+1}{2}} \left(\frac{2}{1-\alpha}\right)^{\frac{1-\alpha}{2}}. \tag{24}$$

The maximum value of $L_I, L_{I\max} = 2$, is attained for $\alpha = 0$ when $f_I(\cdot)$ reduces to the tent map $f_T(\cdot)$ of the previous example.

As opposed to the previous case, the CRLB depends on the initial condition s_0 as well as on N and α. Fig. 2 depicts the CRLB when the initial condition $s_0 = 0$ is estimated as a function of α for several values of N assuming $\sigma_r = 1$. For each N, two curves are shown: the thick one, obtained via the right hand term of (9), and the dashed one that represents the right hand term of (17).

Despite the discontinuous appearance of the first one, it is important to note that both curves are deterministic. Clearly, the inequality of Proposition 2 is a good approximation for the CRLB even for small N.

The smallest values of the CRLB are in the vicinity of $\alpha = 0$ as expected. Note that this behavior is general and not due to the particular value of s_0 used in plotting the graph and reflects the general qualitative behavior of all s_0 values in the $(-1,1)$ range.

Among the $f_I(\cdot)$ maps, $f_T(\cdot)$ is the one with the most favorable CRLB for estimating s_0 under AWGN. This property becomes more significant as more points are used in the estimation.

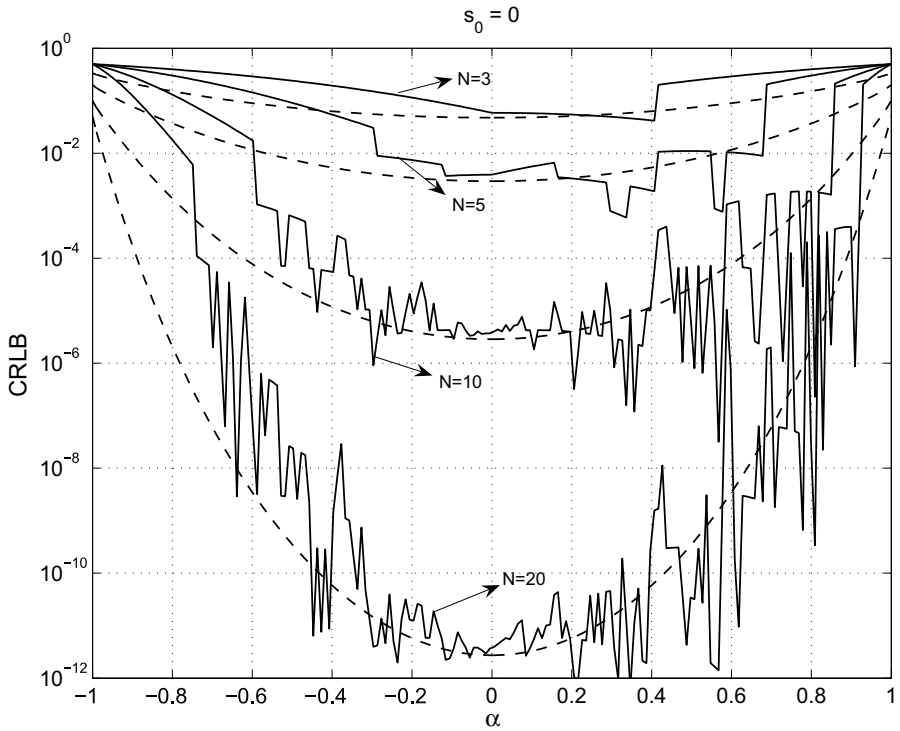

Fig. 2. CRLB for initial condition estimation of the orbit $s(n, 0)$ of $f_I(\cdot)$ as a function of α for $\sigma_r = 1$ and different values of N. The approximation given by (17) is shown by dashed lines.

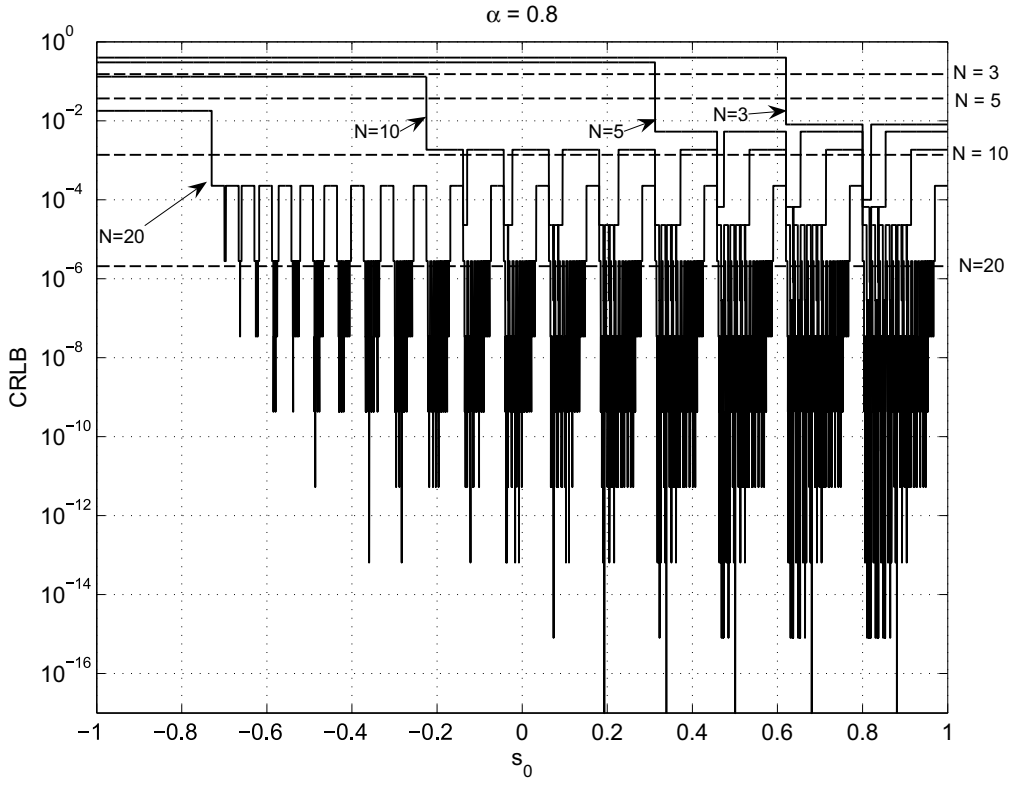

Fig. 3. CRLB for initial condition estimation of the orbit $s(n, s_0)$ of $f_I(\cdot)$ as a function of s_0 for $\alpha = 0.8$, $\sigma_r = 1$ and different values of N. The approximation given by (17) is shown by dashed horizontal lines.

Fig. 3 shows the CRLB as a function of the estimated s_0 for $\alpha = 0.8$ and $\sigma_r = 1$. The discontinuity of the curves is a consequence of the discontinuity in the derivative of $f_I(\cdot)$. Each horizontal segment corresponds to initial conditions associated with orbits whose N first points are in subintervals where $f_I(\cdot)$ has identical derivatives, resulting into equal CRLB values given by (9). As N grows, these segments become smaller and the curves acquire a more complicated shape.

The same figure contains a dashed approximation to the CRLB as a function of N, (17), which can readily be seen as a mean of the true CRLB calculated over all initial conditions.

4.3. Quadratic map $f_Q(\cdot)$

As a final example, consider the map

$$s(n+1) = f_Q(s(n)) = -2s(n)^2 + 1, \tag{25}$$

whose CRLB as a function of s_0 and increasing values of N is contained in Fig. 4 ($\sigma_r = 1$). For $N = 3$, the CRLB is strongly dependent on the initial condition. The bound attains the highest values next to the point $s_0 = 0$ where the derivative of $f_Q(\cdot)$ is zero and in the vicinity of $s_0 = \pm 1/\sqrt{2}$ for which $f_Q(s_0) = 0$. This is because, next to these points, orbits need more iterations to split from one another, which makes their initial condition more difficult to estimate. As N increases, the dependence of the CRLB on s_0 becomes more complicated and the observed peaks spread over all the interval $(-1, 1)$.

As for the map $f_T(\cdot)$, applying Proposition 2 and using the fact that the Lyapunov number of the chaotic orbits of $f_Q(\cdot)$ is $L_Q = 2$ [13], we once more obtain (22), whose values are represented using dashed horizontal lines in Fig. 4. This time, however, this expression is exact only as $N \to \infty$.

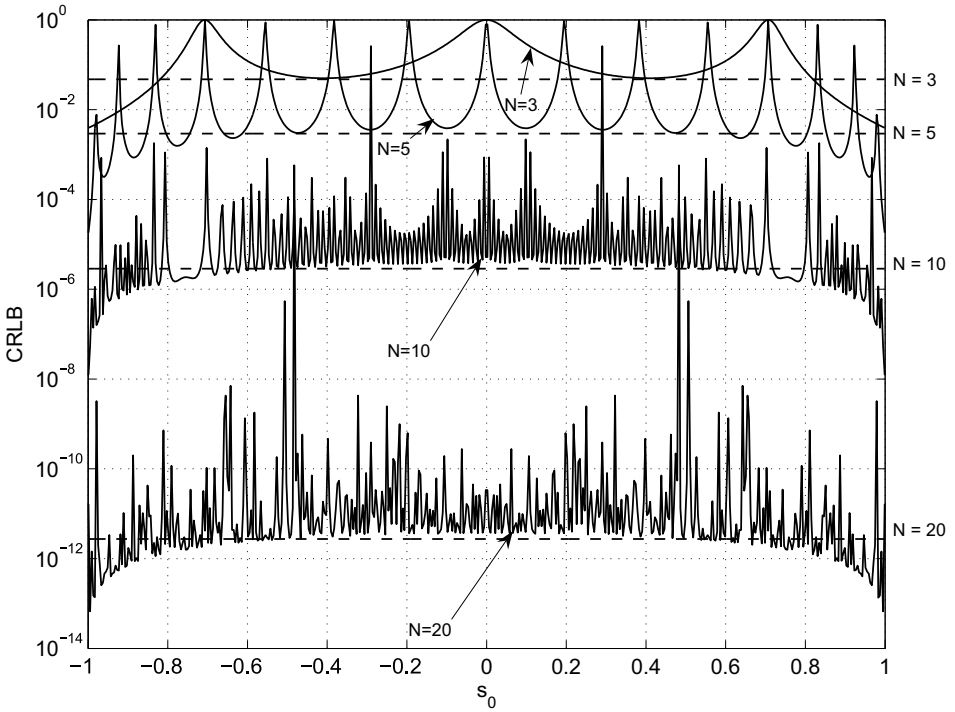

Fig. 4. CRLB for initial condition estimation of the orbit $s(n, s_0)$ of $f_Q(\cdot)$ as a function of s_0 for $\sigma_r = 1$ and different values of N. The approximation given by (17) is shown using dashed horizontal lines.

5. Conclusions

Propositions 1 and 2, the main results of this paper, provide the CRLB for the estimation of s_0 under AWGN.

Applicable to any one-dimensional map with known derivative, these results furnish a criterion for choosing which one-dimensional chaotic signal generating map to use when the initial condition needs to be recovered from a finite corrupted observation sequence. In fact, if one can find an efficient estimator for s_0, choosing maps with larger Lyapunov numbers implies that estimates with smaller mean square error are possible.

Another interesting conclusion following (17) is that semi-conjugative maps [14] have the same CRLB performance for initial condition estimation when N is large because they share the same Lyapunov number. For instance, the quadratic $f_Q(\cdot)$ and $f_T(\cdot)$ maps perform identically for large N as $L_T = L_Q = 2$. When N is small, however, performance becomes a function of s_0 and more detailed analysis is necessary.

In spite of the fact that these results reflect only performance limits and not actual estimator performances, they show that the adequate choice of the map may bring benefits for chaotic communication systems specially for those based on maximum likelihood estimation [17].

References

[1] Kennedy MP, Rovatti R, Setti G. Chaotic electronics in telecommunications. CRC Press; 2000.
[2] Lau FC, Tse CK. Chaos-based digital communication systems. Springer Verlag; 2003.
[3] Feki M. An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons & Fractals 2003;18:141–8.
[4] Feki M, Robert B, Gelle G, Colas M. Secure digital communication using discrete-time chaos synchronization. Chaos, Solitons & Fractals 2003;18:881–90.
[5] Li Z, Xu D. A secure communication scheme using projective chaos synchronization. Chaos, Solitons & Fractals, 24, 477–481.
[6] Chien TI, Liao TL. Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization. Chaos, Solitons & Fractals, 2005;24:241–55.
[7] Lu JG. Multiple access chaotic digital communication based on generalized synchronization. Chaos, Solitons & Fractals 2005;25:221–7.

[8] Haykin SS. Communication systems. Wiley; 2000.
[9] Abarbanel HDI. Analysis of observed chaotic data. Springer; 1996.
[10] Eisencraft M, Baccalá LA. Estimating the initial conditions of chaotic orbits: performance bounds. In: First IFAC conference on analysis and control of chaotic systems, Reims, 2006. CHAOS'06: A preprints volume, 2006, pp. 291–295.
[11] Kay SM. Asymptotic maximum likelihood estimator performance for chaotic signals in noise. IEEE Trans Signal Process 1995;43(4):1009–12.
[12] Kay SM. Fundamentals of statistical signal processing. Prentice Hall PTR; 1993.
[13] Alligood KT, Sauer TD, Yorke JA. Chaos – an introduction to dynamical systems. Springer; 1996.
[14] Devaney RL. An introduction to chaotic dynamical systems. Westview Press; 2003.
[15] Papadopoulos HC, Wornell GW. Optimal detection of a class of chaotic signals. In: IEEE conference on acoustic, speech and signal processing, Minneapolis: Proc. ICASSP; 1993, vol. 3, 1993, p. 117–120.
[16] Kay SM, Nagesha V. Methods for chaotic signal estimation. IEEE Trans Signal Process 1995;43(8):2013–6.
[17] Kisel A, Dedieu H, Schimming T. Maximum likelihood approaches for noncoherent communications with chaotic carriers. IEEE Trans Circuits Systems – I, Fundamental Theory Appl 2001;48(5):533–42.
[18] Billings L, Bollt EM. Probability density function of some skew tent maps. Chaos, Solitons & Fractals 2001;12:365–76.