Nonlinear Analysis: Modelling and Control, Vol. 23, No. 6, 951–960 ISSN 1392-5113
https://doi.org/10.15388/NA.2018.6.9

The problem of the inverse Lyapunov exponent and its applications

Marcin Lawnik

Faculty of Applied Mathematics, Silesian University of Technology,
Kaszubska 23, 44-100 Gliwice, Poland
marcin.lawnik@polsl.pl

Received: May 7, 2018 / **Revised:** October 10, 2018 / **Published online:** October 31, 2018

Abstract. The problem of the inverse Lyapunov exponent was formulated and solved, involving to find such chaotic transformation for which the value of the Lyapunov exponent is given in advance. The solution procedure was presented by a numerical example. Furthermore, applications of the discussed model in chaos based cryptography were discussed.

Keywords: Lyapunov exponent, piecewise linear map, inverse problem.

1 Introduction

Chaotic functions play a very important role in many fields of science and technology. For example, they are used in cryptography as generators of pseudo-random numbers [1, 18] for advanced technical models of chemical reactors [5, 6, 20] or description of physical phenomena such as weather forecasts [24]. They are also applied outside the range of technical sciences, for example, in economics – for modelling certain processes [12, 15] or even medicine [28, 30].

One of the basic measures showing if a given function

$$x_{k+1} = f(x_k) \tag{1}$$

could generate chaotic solutions is the Lyapunov exponent. For maps in the form of (1), it may be expressed as

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln \left| f'(x_i) \right| \tag{2}$$

and measures the rate of the propagation of infinitely approximate trajectories of the system (1). Positive value of (2) is a necessary condition for function (1) to generate a chaotic solution; otherwise, the solution is stable.

The Lyapunov exponent for discrete dynamical systems may be easily determined in a numerical manner. Accordingly, for a logistics map expressed as

$$x_{k+1} = ax_k(1 - x_k), \tag{3}$$

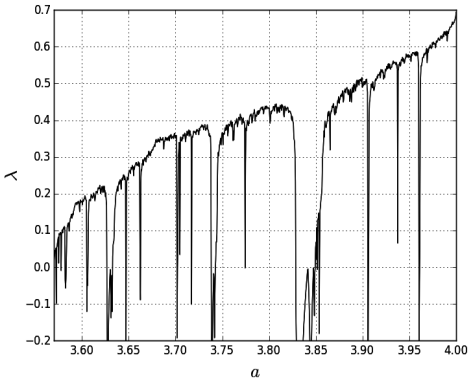

Figure 1. Lyapunov exponent λ of Eq. (3) in the interval $[3.57, 4]$. Outside this interval the value of λ is non-positive.

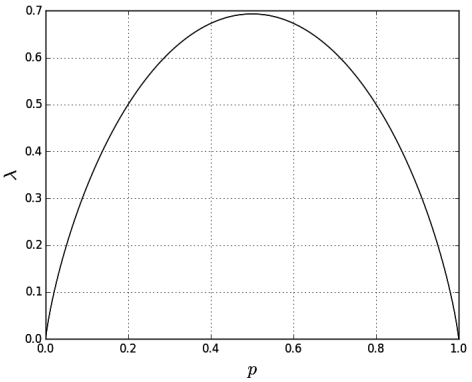

Figure 2. Lyapunov exponent λ given by Eq. (5).

where $a \in [0, 4]$ and $x \in [0, 1]$, the Lyapunov exponent is presented in the graph in Fig. 1. As shown in the graph, its structure is fairly complicated and has a fractal character. Moreover, its maximum value is $\ln 2$ for the parameter value $a = 4$.

Another example of a transformation for which the Lyapunov exponent may be designated in an easy manner is the asymmetric (skew) tent map given by the equation

$$x_{k+1} = \begin{cases} \frac{x_k}{p}, & 0 < x_k \leqslant p, \\ \frac{1-x_k}{1-p}, & p < x_k < 1, \end{cases} \tag{4}$$

where $p \in (0, 1)$. Its Lyapunov exponent λ is expressed as [2]

$$\lambda = -p \ln p - (1 - p) \ln(1 - p). \tag{5}$$

For each value of parameter p, the value of (5) is positive and its graph is plotted in Fig. 2. Likewise, in the case of (3) its maximum is $\ln 2$ for $p = 1/2$.

Let us now consider another example of piecewise linear map [25]:

$$x_{k+1} = \begin{cases} \frac{x_k}{p_1}, & x_k \in I_1, \\ \frac{x_k - p_1}{p_2}, & x_k \in I_2, \\ \vdots & \vdots \\ \frac{x_k - \sum_{i=1}^{n-1} p_i}{p_n}, & x_k \in I_{n-2}, \end{cases} \tag{6}$$

where $I_1 = [0, p_1]$, $I_i = [\sum_{j=1}^{i-1} p_j, \sum_{j=1}^{i} p_j]$ and $\sum_{i=1}^{n} p_i = 1$.

The Lyapunov exponent for (6) is expressed by the following equation [2]:

$$\lambda = -\sum_{i=1}^{n} p_i \ln p_i.$$

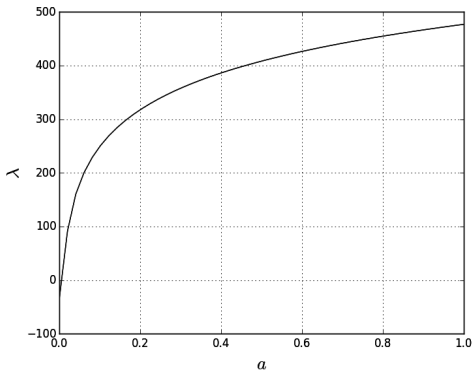

Figure 3. Lyapunov exponent for transformation (7) with $b = 123$ and $n = 100$.

Similarly to (5), for each set of p_i it has a positive value. Its maximum is equal to $\ln n$ for $p_i = 1/n$ $(i = 1, 2, \ldots, n)$. Furthermore, its value increases together with the increase of n.

An interesting function for which the Lyapunov exponent also increases indefinitely, is the so called Weierstrass recurrence given as [7, 17]

$$x_{k+1} = \sum_{i=0}^{n} a^i \cos\bigl(b^i \pi x_k\bigr). \tag{7}$$

Its Lyapunov exponent is shown in Fig. 3.

As inferred from the examples discussed above, despite the fact that the Lyapunov exponent may be expressed by means of complicated dependencies, it may also reach very high values. Nevertheless, while analysing the discussed cases, a question may arise whether it is possible to construct such chaotic function that would have a pre-determined value of the Lyapunov exponent. Such formulated problem may be labelled as the inverse designation of the Lyapunov exponent and will be discussed in the next part of the paper.

Such types of tasks are often analyzed in technical sciences, e.g. the inverse Stefan problem [13,29], which has wide applications in metals solidification. Moreover, it should also be emphasised that other inverse problems are considered in the theory of dynamical systems, for example, the inverse Frobenius–Perron problem [10, 11, 16, 27], involving the designation of a map with the assumed invariant density.

The posed problem can be used in cryptography based on the theory of chaos. In this case, the security of the algorithm depends on the used map and, consequently, from its properties. Mappings with a small and variable value of Lyapunov exponent are not the best solutions. More on this subject is given in Section 5.

2 Formulation of the problem

Let us assume a given λ value. The task is to find such chaotic function for which the value of the Lyapunov exponent is exactly equal to λ. Such task may be described as the *inverse Lyapunov exponent problem.*

3 Results

The problem of the inverse Lyapunov exponent will be solved by means of the following expression:

$$x_{k+1} = \begin{cases} nx_k, & x_k \in [0, \frac{1}{n}), \\ nx_k - 1, & x_k \in [\frac{1}{n}, \frac{2}{n}), \\ \vdots & \vdots \\ nx_k - n + 3, & x_k \in [\frac{n-3}{n}, \frac{n-2}{n}), \\ \frac{nx_k - n + 2}{np}, & x_k \in [\frac{n-2}{n}, \frac{n-2}{n} + p), \\ \frac{nx_k - n + 2 - np}{2 - np}, & x_k \in [\frac{n-2}{n} + p, 1], \end{cases} \tag{8}$$

where $n \geqslant 3$ and $p \in (0, 2/n)$. Its exemplary graph for settled values of $n = 4$ and $p = 0.1$ is plotted in Fig. 4

Let us now assume some basic facts concerning Eq. (8).

Theorem 1. *The invariant density* $\rho(x)$ *of* (8) *is* 1.

Proof. The invariant density $\rho(x)$ for mapping (1) may be designated by solving the Frobenius–Perron equation in the following form [9]:

$$\rho(x) = \sum_{i=1}^{m} \frac{\rho(y_i)}{|f'(y_i)|}, \tag{9}$$

where y_i is the ith inverse image of point x ($f(y_i) = x$, $i = 1, 2, \ldots, m$). By transcribing Eq. (9) with (8) the following equation is derived:

$$\begin{aligned} \rho(x) = {} & \frac{1}{n}\rho\left(\frac{x}{n}\right) + \frac{1}{n}\rho\left(\frac{x+1}{n}\right) + \cdots + \frac{1}{n}\rho\left(\frac{x+n-3}{n}\right) \\ & + p\rho\left(\frac{npx + n - 2}{n}\right) + \left(\frac{2}{n} - p\right)\rho\left(\frac{x(2-np) + n - 2 + np}{n}\right). \end{aligned} \tag{10}$$

By substituting $\rho(x) = 1$ to (10), the equality is designated. □

Theorem 2. *The Lyapunov exponent for Eq.* (8) *is given by the following formula*:

$$\lambda = \frac{n-2}{n} \ln n - p \ln p - \left(\frac{2}{n} - p\right) \ln\left(\frac{2}{n} - p\right). \tag{11}$$

Proof. Let us take advantage of dependence [8]

$$\lambda = \int_0^1 \rho(x) \ln \left|f'(x)\right| \mathrm{d}x,$$

which bids the Lyapunov exponent with the invariant density.

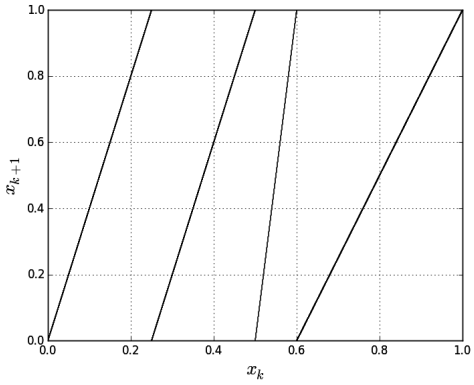

Figure 4. Exemplary transformation of (8) with $n = 4$ and $p = 0.1$.

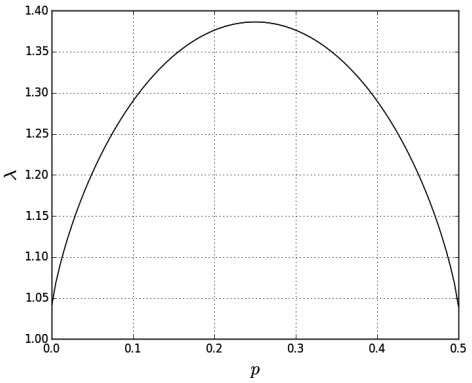

Figure 5. Lyapunov exponent (11) with $n = 4$.

On the grounds of the fact proven in Theorem 1 that $\rho(x) = 1$, the following equation is derived:

$$\begin{aligned}\lambda &= \int_0^{1/n} \ln n \,\mathrm{d}x + \int_{1/n}^{2/n} \ln n \,\mathrm{d}x + \cdots + \int_{(n-3)/n}^{(n-2)/n} \ln n \,\mathrm{d}x \\ &\quad + \int_{(n-2)/n}^{(n-2)/n+p} \ln \frac{1}{p} \,\mathrm{d}x + \int_{(n-2)/n+p}^{1} \ln \frac{1}{\frac{2}{n} - p} \,\mathrm{d}x \\ &= \frac{1}{n} \ln n + \frac{1}{n} \ln n + \cdots + \frac{1}{n} \ln n - p \ln p - \left(\frac{2}{n} - p\right) \ln\left(\frac{2}{n} - p\right) \\ &= \frac{n-2}{n} \ln n - p \ln p - \left(\frac{2}{n} - p\right) \ln\left(\frac{2}{n} - p\right). \qquad \square\end{aligned}$$

Lemma 1. *The Lyapunov exponent given by Eq.* (11) *fulfils the dependence*

$$\frac{n-2}{n} \ln n - \frac{2}{n} \ln \frac{2}{n} \leqslant \lambda \leqslant \ln n, \quad n \geqslant 2.$$

Proof. Function (11) reaches its maximum value for $p = 1/n$, which proves the right side of the inequality. In turn, the lowest value of function (11) is obtained for $p = 0$ or $p = 2/n$, directly leading to the left side of the inequality. $\square$

Furthermore, we shall prove a supporting lemma enabling the solution of the discussed problem.

Lemma 2. *The following inequality holds*:

$$\frac{n-2}{n} \ln n - \frac{2}{n} \ln \frac{2}{n} \leqslant \ln(n-1), \quad n \geqslant 2.$$

Proof. We shall prove that

$$\ln(n-1) - \frac{n-2}{n}\ln n + \frac{2}{n}\ln\frac{2}{n} \geqslant 0. \tag{12}$$

By multiplying both sides of (12) by n we derive

$$n\ln(n-1) - (n-2)\ln n + 2\ln\frac{2}{n} \geqslant 0.$$

Next, by performing elementary procedures on the logarithms, we obtain

$$\ln\frac{4(n-1)^n}{n^n} \geqslant 0. \tag{13}$$

In consequence, inequality (13) leads to

$$\frac{4(n-1)^n}{n^n} \geqslant 1. \tag{14}$$

Dependence (14) is true for $n \geqslant 2$ as the sequence $a_n = (n-1)^n/n^n$ is incremental and $\lim_{n\to\infty} a_n = \mathrm{e}^{-1}$. □

Conclusion 1. *It is possible to find such representation of* (8)*, for which the Lyapunov exponent* (11) *fulfils the following dependence*:

$$\ln(n-1) \leqslant \lambda \leqslant \ln n. \tag{15}$$

Proof. The proof directly follows from Lemmas 1 and 2. □

On the grounds of Conclusion 1, it is possible to solve the inverse Lyapunov exponent by means of the method described below:

Method 1. Let λ denote the assumed value of the Lyapunov exponent. Then:

- If $\lambda \leqslant \ln 2$, the searched equation has the form of (4). The value of parameter p is designated by solving Eq. (5).
- If $\lambda \geqslant \ln 2$, the searched dynamical system has the form of (8). The first step involves the determination of the value of n in accordance with dependence (15). The value of parameter p is designated by solving Eq. (11).

4 Example

By applying Method 1 we shall find the chaotic map in the form of (8), for which the Lyapunov exponent $\lambda = 1.1$. $n = 4$ because

$$\ln 3 < 1.1 < \ln 4.$$

By solving numerically Eq. (11) with $\lambda = 1.1$ and $n = 4$, $p \sim 0.079787$ is derived. The obtained equation is presented in Fig. 6.

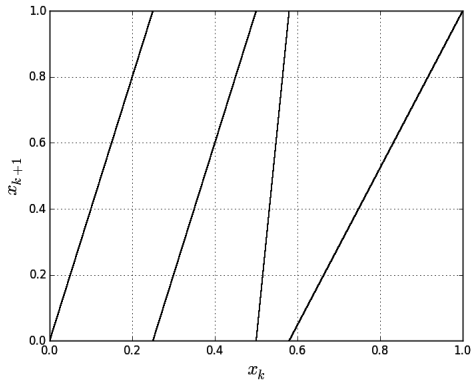

Figure 6. Transformation of the form of (8) with $\lambda = 1.1$.

5 Applications

Chaotic maps are used, for example, in chaotic cryptography, enabling, on the grounds of the values derived from the functions, construction of various algorithms for data protection. The secret keys for such algorithms are the values of parameters and initial conditions. Very frequently the logistics map (3) (among others, in [4, 23, 26, 31]) and the asymmetric tent map (4) (for example, in [14, 21, 22]) are used in such an encryption process. However, as far as cryptography is concerned, both types of these functions are often the weakest points of algorithms referred to in publications. This fact results, among other factors, from:

(i) nonuniform distribution of the iterated variable;
(ii) too narrow range of parameters values within which the chaotic solution is generated;
(iii) unstable value of the Lyapunov exponent, i.e. its value changes in the range $[0, \ln 2]$ (as in the case of logistic (3) and tent map (4)) and its very fragile, i.e. a small change in the parameter value eliminates the phenomenon of chaos (logistic map (3), see Fig. 1).

The above mentioned drawbacks have been noticed by some researchers and attempts made at determining other functions that could successfully replace logistic map (3) or skew tent map (4) [3, 19].

The presented map (8) is devoid of the above-mentioned disadvantages. It may be used as a function suitable for encryption, due to its features such as: uniform distribution of the iterated variable or the length of intervals of the parameter values where the function is chaotic. Moreover, Eq. (8) is a representant of the family of functions for which the Lyapunov exponent λ is designated by expression (11). Other equations that belong to this family are determined in such a manner that the direction coefficients of the straight lines in (8) are positive or negative with the same modulus value. Likewise, it is possible to re-permute the sub-intervals on which particular straight lines are designated. The number of such functions is determined by the lemma given below.

Lemma 3. *The number P_n of a piecewie linear chaotic functions in the form of* (8)*, for which the Lyapunov exponent λ is equal to* (11) *and the invariant density is $\rho(x) = 1$, is*

$$P_n = 2^n n(n-1).$$

Proof. By changing the signs of the direction components of the straight lines in (8) we derive 2^n maps. In turn, by changing the position of the sub-intervals in which parameter p is contained we obtain $n(n-1)$ new maps. The procedures described above do not alter the values of the Lyapunov exponent and invariant density. □

As it follows from Lemma 3, it is not only possible to hide the value of parameter p, but also the form of the function, rendering more opportunities for the selection of secret keys and making it more resistant, for example, to brutal attacks.

6 Conclusions

The problem of the inverse Lyapunov exponent was formulated and solved. The solution involved finding a chaotic function in the form of (1), for which the value of the Lyapunov exponent is assumed in advance. The solution was based on the construction of a piecewise linear model of (8), for which the Lyapunov exponent was given by dependence (11). The solution procedure was illustrated by a numerical example. Furthermore, it was indicated that the discussed model may be used in chaotic cryptography.

References

1. T. Addabbo, A. Fort, S. Rocchi, V. Vignoli, Digitized chaos for pseudo-random number generation in cryptography, in Kocarev L., Lian S. (Eds.), *Chaos-Based Cryptography*, Stud. Comput. Intell., Vol. 354, Springer, Berlin, Heidelberg, 2011, pp. 67–97.
2. V.M. Anikin, S.S. Arkadaksky, S.N. Kuptsov, A.S. Remizov, L.P. Vasilenko, Lyapunov exponent for chaotic 1D maps with uniform invariant distribution, *Bull. Russ. Acad. Sci., Phys.*, **72**(12):1684–1688, 2008.
3. D. Arroyo, G. Alvarez, V. Fernandez, On the inadequacy of the logistic map for cryptographic applications, in A.M. Hernandez (Ed.), *X Reunin Espanola sobre Criptologıa y Seguridad de la Informacion (X RECSI)*, Universidad de Salamanca, Salamanca, Spain, 2008, pp. 77–82.
4. M.S. Baptista, Cryptography with chaos, *Phys. Lett. A*, **240**(1–2):50–54, 1998.
5. M. Berezowski, Spatio-temporal chaos in tubular chemical reactors with the recycle of mass, *Chaos Solitons Fractals*, **11**:1197–1204, 2000.
6. M. Berezowski, D. Dubaj, Chaotic oscillations of coupled chemical reactors, *Chaos Solitons Fractals*, **78**:22–25, 2015.
7. M. Berezowski, M. Lawnik, Identification of fast-changing signals by means of adaptive chaotic transformations, *Nonlinear Anal. Model. Control*, **19**(2):172–177, 2014.
8. P. Biswas, H. Shimoyama, L.R. Mead, Lyapunov exponents and the natural invariant density determination of chaotic maps: An iterative maximum entropy ansatz, *J. Phys. A, Math. Theor.*, **43**:125103, 2010.

9. T. Bohr, T. Tél, The thermodynamics of fractals, in B.-L. Hao (Ed.), *Directions in Chaos, Vol. 2*, Ser. Dir. Condens. Matter Phys., Vol. 4, World Scientific, Singapore, 1988, pp. 194–237.
10. A. Boyarsky, P. Göra, *Laws of Chaos Invariant Measures and Dynamical Systems in One Dimension*, Springer, New York, 1997.
11. S. Grossmann, S. Thomae, Invariant distributions and stationary correlation functions of one-dimensional discrete processes, *Z. Naturforsch.*, **32**:1353–1363, 1977.
12. D. Guégan, Chaos in economics and finance, *Annu. Rev. Control*, **33**(1):89–93, 2009.
13. E. Hetmaniok, D. Słota, R. Wituła, A. Zielonka, Solution of the one-phase inverse Stefan problem by using the homotopy analysis method, *Appl. Math. Modelling*, **39**(22):6793–6805, 2015.
14. A. Kadir, A. Hamdulla, W.-Q. Guo, Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN, *Optik*, **125**(5):1671–1675, 2014.
15. J. Kemp, New methods and understanding in economic dynamics: An introductory guide to chaos and economics, *Economic Issues*, **2**(Part 1):1–26, 1997.
16. S. Koga, The inverse problem of Flobenius–Perron equations in 1D difference systems: 1D map idealization, *Prog. Theor. Phys.*, **86**(5):991–1002, 1991.
17. M. Lawnik, The approximation of the normal distribution by means of chaotic expression, *J. Phys., Conf. Ser.*, **490**:012072, 2014.
18. M. Lawnik, Generation of numbers with the distribution close to uniform with the use of chaotic maps, in M.S. Obaidat, J. Kacprzyk, T. Ören (Eds.), *Proceedings of the 4th International Conference on Simulation and Modeling Methodologies, Technologies and Applications, Vienna, August 28–30, 2014*, Scitepress, Setúbal, 2014, pp. 451–455.
19. M. Lawnik, Generalized logistic map and its application in chaos based cryptography, *J. Phys., Conf. Ser.*, **936**:012017, 2017.
20. M. Lawnik, M. Berezowski, Identification of the oscillation period of chemical reactors by chaotic sampling of the conversion degree, *Chem. Process Eng.*, **35**(3):387–393, 2014.
21. C. Li, G. Luo, K. Qin, C. Li, An image encryption scheme based on chaotic tent map, *Nonlinear Dyn.*, **87**(1):127–133, 2017.
22. X. Liao, Improved tent map and its applications in image encryption, *International Journal of Security and Its Applications*, **9**(1):25–34, 2015.
23. L. Liu, S. Miao, A new image encryption algorithm based on logistic chaotic map with varying parameter, *SprigerPlus*, **5**:289, 2016.
24. E.N. Lorenz, Deterministic nonperiodic flow, *J. Atmos. Sci.*, **20**(2):130–141, 1963.
25. N. Nagaraj, P.G. Vaidya, K.G. Bhat, Arithmetic coding as a non-linear dynamical system, *Commun. Nonlinear Sci. Numer. Simul.*, **14**:1013–1020, 2009.
26. N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, *Image Vision Comput.*, **24**(9):926–934, 2006.
27. D. Pingel, P. Schmelcher, F.K. Diakonos, Theory and examples of the inverse Frobenius–Perron problem for complete chaotic maps, *Chaos*, **9**(2):357–366, 1999.
28. J.E. Skinner, M. Molnar, T. Vybiral, M. Mitra, Application of chaos theory to biology and medicine, *Integr. Physiol. Behav. Sci.*, **27**(1):39–53, 1992.

29. D. Słota, Direct and inverse one-phase Stefan problem solved by the variational iteration method, *Comput. Math. Appl.*, **54**(7–8):1139–1146, 2007.

30. B.J. West, *Fractal Physiology and Chaos in Medicine,* 2nd ed., Stud. Nonlinear Phenom. Life Sci., Vol. 16, World Scientific, Singapore, 2012.

31. Y. Wu, J.P. Noonan, G. Yang, H. Jin, Image encryption using the two-dimensional logistic chaotic map, *J. Electron. Imaging*, **21**(1):1–16, 2012.