16th IMEKO TC4 Symposium
Exploring New Frontiers of Instrumentation and Methods for Electrical and Electronic Measurements
Sept. 22-24, 2008, Florence, Italy

Statistical Characterization of a Chaotic Piecewise Linear Map for Uniform-Distributed Analog Noise Generation

Tommaso Addabbo[1], Ada Fort[1], Marco Mugnaini[1], Santina Rocchi[1], Valerio Vignoli[1]

[1] *Information Engineering Department, University of Siena, Via Roma, 56 – 53100 Siena (Italy).*
Phone: +39-0577-234608, Fax: +39-0577-233602, E-mail: ada@dii.unisi.it.

Abstract - In this paper a theoretical approach for studying the effects of parameter perturbations on the chaotic statistics of piecewise linear expanding transformations is summarized, with reference to the chaotic Sawtooth map. On this basis, the authors prove that is possible, both from a theoretical and from an experimental point of view, to obtain almost uniform distributed and uncorrelated analog samples from the Sawtooth map.

I. Introduction

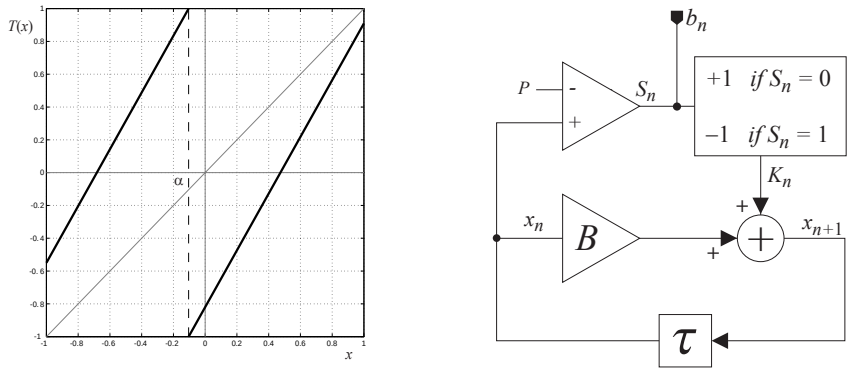
Noise generators are used in several fields, e.g., data encryption, instrumentation calibration, electronic circuits test and measurement, as well as statistical analysis via Monte Carlo simulations of analytically intractable problems [1]-[8]. Noise generators are intimately related to random bits generators since from an unpredictable and properly distributed numerical sequence, a noisy signal can be obtained via D/A conversion. In most applications random numbers are obtained using pseudo-random bit generators (PRBGs), that are hardware or software generators based on deterministic algorithms issuing binary sequences with finite period, and with statistical features, within the period, similar to those of random sequences. An alternative to PRBGs is represented by Truly Random Bits Generators (TRBGs) that issue non periodic and almost unpredictable sequences.
From the point of view of noise generation, all the mentioned systems based on PRBGs and TRBGs, provide a quantized output that causes the noise levels to belong to a finite discrete set. This inconvenience can be avoided relying on "analog to analog" electronic noise generators, which are traditionally based on the sampling of some intrinsically random physical processes (e.g. Johnson and Schottky noise). As a drawback, these approaches usually involve several electronic design problems related to the conditioning of feeble physical signals (e.g., due to electromagnetic interferences).
Recently, in alternative to traditional methods, the use of deterministic chaos was considered [6]-[9]. Several types of discrete time chaotic dynamical systems have been proposed for the implementation of stochastic sources with *tunable statistical characteristics*: in such cases, depending on the application, by changing the system parameters one or more statistical features of the source can be modulated (e.g., the stationary distribution, or the autocorrelation) [10]. Among the chaotic systems taken into account, *piecewise affine maps* (also called piecewise linear maps) are good candidates for being implemented by electronic circuits, since their analytical expressions typically involve simple algebraic operations. Nevertheless, the statistical characteristics of these dynamical systems turn out to be extremely sensible to any parameter change, and this aspect represents a critical issue when the tolerances of any implementation process are taken into account. This fact has been investigated, e.g., in [6], [8].

II. The Chaotic Sawtooth Map

In this paper a noisy analog sequence $\{x_n\}$ is generated using a discrete time dynamical system $x_{n+1} = T(x_n)$, where the function T:[−1,1)→ [−1,1) is [11] (Fig. 1a):

$$T(x) = \begin{cases} B(x-\alpha)+1, & \text{if } x < \alpha, \\ B(x-\alpha)-1, & \text{if } x \geq \alpha, \end{cases} \qquad (1)$$

with $|\alpha| < 0.15$ and $\sqrt{2} < B \leq 2/(1+|\alpha|)$. If $B > 2/(1+|\alpha|)$ the dynamics diverges, and almost all initial conditions $x_0 \in$[-1,1) trigger trajectories that are attracted to either plus or minus infinity. In the following we refer to (1) as the Sawtooth dynamical system. As discussed in the following, even if the



(a) (b)

Figure1. (a) The Sawtooth map (1) for $B = 1.7298$ and $\alpha = -0.1043$; (b) Block diagram for the implementation of (1).

analog sequence is ruled by a deterministic equation, the large sensitivity to the initial conditions of this chaotic system allows for the generation of a stochastic sequences.
In [8] it was proved that the system (1) represents a general *analytical model* that can be used to describe the dynamics of any system implemented by the block diagram of Fig. 1b, i.e., by varying the parameters B and P in the block diagram of Fig. 1b one can obtain a dynamical system with a statistical behaviour that can be equivalently[1] described by (1) when $\alpha = P(1-B)$.

A. Invariant Densities and Ergodic Properties

The theoretical tools for the statistical analysis of discrete time chaotic systems are provided by Ergodic Theory. In [11] the authors provided a review about the deep ergodic properties of the Sawtooth map (1) that will be briefly summarized in this subsection. The invariant probability density functions (pdf) play a key role in the analysis of the stochastic aspects of chaotic dynamics, since they provide the necessary information for retrieving any order statistics of the chaotic process [10]. Once assuming the state of the chaotic system as a random variable, invariant pdfs describe stationary distributions for such a variable, and the methods for computing and determining the shape of these densities are of interest [11]. The reason for which the state of a chaotic system is assumed to be a random variable is founded on the *sensitivity of the dynamics* to the initial condition, which physically manifests itself, as time passes, as an exponential growth of the uncertainty about the prediction of the dynamical evolution. As far as system (1) is concerned, the ergodic theory states that the Sawtooth map is an *ergodic stochastically stable system*. This means that, regardless of the pdf f_0 associated to the initial condition x_0 assumed as a random variable, the sequence of pdfs $\{f_n\}$ of the random variables $\{x_n\} = \{T^n(x_0)\}$ approaches one unique stationary pdf f^* *that only depends on the parameters B* and α. The approach to f^* is not slower than exponential, and in practical situations the system can be considered stabilized on its stationary distribution after a small number of iterations (typically less than 20 iterations). As an example, in Fig. 2 the evolution of a Gaussian distribution f_0 is depicted for the Sawtooth map with $B = 1.98$ and $\alpha = 0.002$. As it can be seen, after few iterations ($n > 7$) the system can be assumed stabilized on its stationary invariant distribution. Once stabilized, the stochastic process $\{x_n\}$ is strongly ergodic [11].

B. Modulation and robustness of the stationary distribution

By varying parameters B and α in (1) it is possible to modulate the system stationary distribution. We first state a fundamental property of the Sawtooth map [11].

Theorem 1. Let us assume $|\widetilde{\alpha}| < 0.15$ and $\sqrt{2} < \widetilde{B} \le 2/(1+|\widetilde{\alpha}|)$, and let us consider a sequence of

[1] i.e., the two systems exhibit two dynamics that are related by a linear transformation [8].

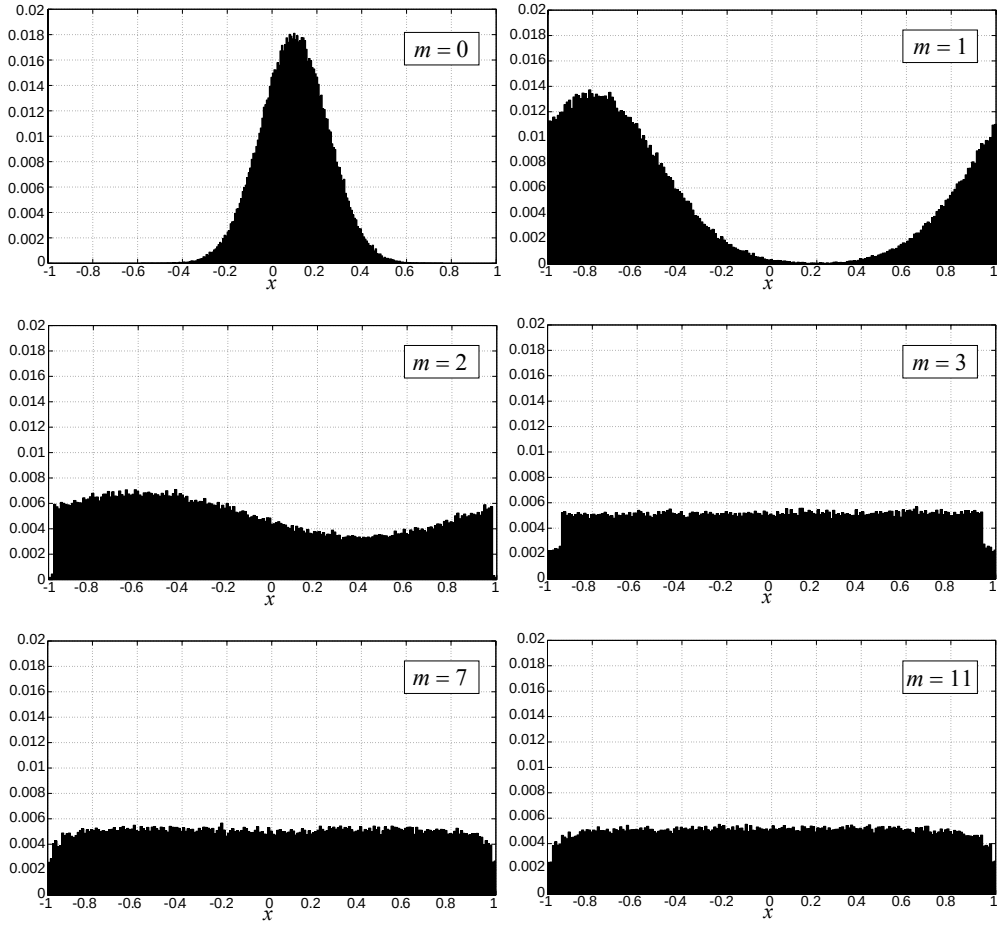


Figure 2. Evolution of a Gaussian pdf f_0 for the Sawtooth map (1) with $B = 1.98$, $\alpha = 0.002$.

parameters $\{B_k, \alpha_k\}$ such that, for all $k \in \mathbf{N}$, $|\alpha_k| < 0.15$ and $\sqrt{2} < B_k \le 2/(1+|\alpha_k|)$. If:

$$\lim_{k\to\infty}(B_k,\alpha_k) = (\widetilde{B},\widetilde{\alpha}) \tag{2}$$

then the sequence $\{f_k^*\}$ of unique invariant pdfs associated to the sequence of Sawtooth maps with parameters (B_k, α_k) converges in probability to the unique invariant pdf $\widetilde{f}^*$ of the Sawtooth map with parameters $(\widetilde{B},\widetilde{\alpha})$, i.e., for any measurable subset $A \subseteq [-1, 1)$:

$$\lim_{k\to\infty}\int_A f_k^*(x)\,dx = \int_A \widetilde{f}^*(x)\,dx. \tag{3}$$

The above theorem assures the robustness property of the stationary distribution for the Sawtooth map with respect to parameter perturbations. Moreover, it states that the more we bring the system parameters B and α close to the target values $\widetilde{B},\widetilde{\alpha}$, the better any order statistics of the output sequence approximate the ones of the nominal case. From this point of view, according to the parameter space assumed in Theorem 1, it is interesting noting that $B = 2$ if and only if $\alpha = 0$, and in such case it has been proved that the unique ergodic pdf is a perfect ideal uniform one [6], [9]. About this issue, a correction algorithm based on a feedback strategy was proposed in [8] for the automatic control of the parameters in (1), that allows to bring B as much as possible close to 2 (from left), while

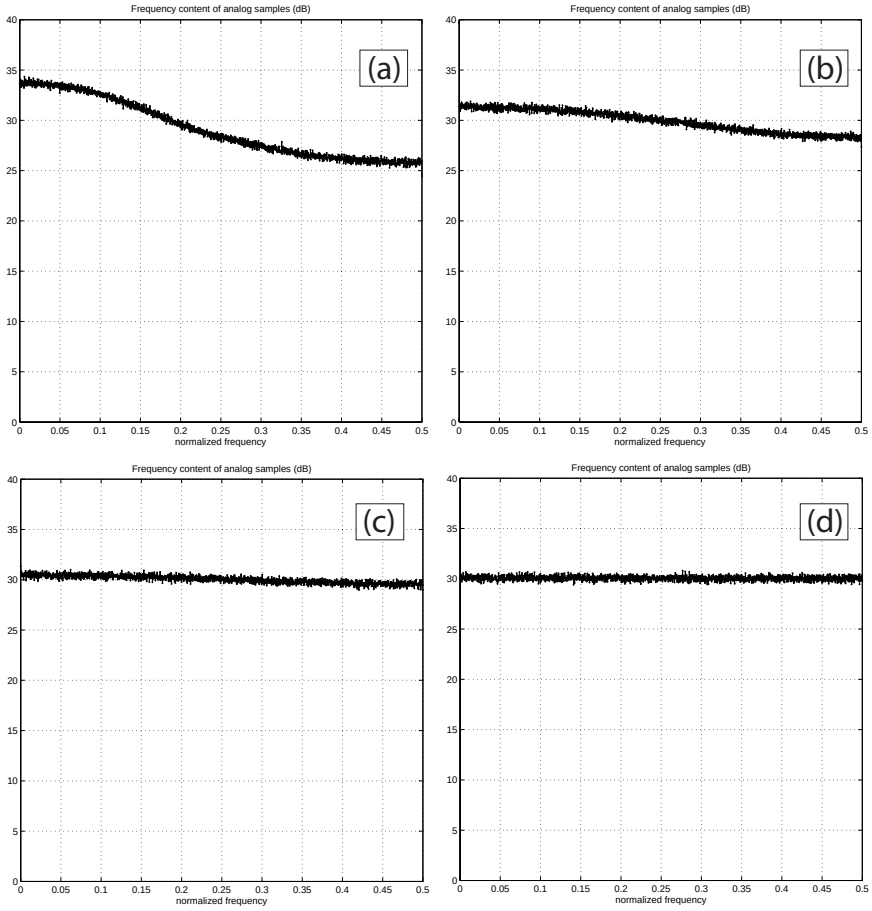


Figure 3. Pdf estimation of the analog sequence generated by (1) for different down-sampling factors k, obtained from a 10^7 sample sequence issued by the Sawtooth map with $B = 1.98$, and $\alpha = 0.002$: (a) $k = 1$, (b) $k = 2$, (c) $k = 3$, (d) $k = 4$.

minimizing $|\alpha|$. In real electronic circuits it was proved that this correction procedure allows for setting $B \geq 1.97$, obtaining ergodic distributions that are almost uniform within a wide interval of the domain [9] (see, e.g., Figure 2). The closeness to a uniform function depends on the system parameters, and on the considered interval [9].

III. Correlation of output samples

We are interested in analysing the autocorrelation function of the stochastic process ruled by (1). Even if the output samples are distributed according to a stationary ergodic pdf, the deterministic relationship (1) that exists between the random variables x_{n+1} and x_n causes the autocorrelation function $r_{xx}(m)$ of the stochastic process $\{x_n\}$ not to be delta-shaped. In detail if we have the following

Theorem 2. Let us assume $B = 2$ and $\alpha = 0$. Then $r_{xx}(m) = 2^{-m}/3$.

Proof. For $B = 2$ and $\alpha = 0$ the Sawtooth map T: $[-1, 1) \rightarrow [-1, 1)$ in (1), and the Bernoulli map $S(y) = 2y \bmod 1$, with S: $[0, 1) \rightarrow [0, 1)$, are topologically conjugated by a linear homeomorphism h: $[0, 1) \rightarrow [-1, 1)$ defined as $h(\xi) = 2\xi - 1$. Since the unique ergodic pdf over $[0, 1)$ for the Bernoulli map is the uniform pdf $\phi(y) = 1$, by denoting with r_{yy} the autocorrelation function of the process $\{y_n = S(y_{n-1})\}$, we have:

$$r_{yy}(m) \int_0^1 y S^m(y) \phi(y) dy = \int_0^1 y \cdot (2^m y) \bmod 1 \, dy \, . \qquad (4)$$

Using the variable substitution $z = 2^m y$ we have:

$$r_{yy}(m) = \int_0^{2^m} \frac{z \cdot (z) \bmod 1}{2^{2m}} dz = \sum_{k=1}^{2^m} \int_{k-1}^{k} \frac{z(z) \bmod 1}{2^{2m}} dz = \sum_{k=1}^{2^m} \int_0^1 \frac{(\theta + k - 1)\theta}{2^{2m}} d\theta = \frac{3 \cdot 2^m + 1}{12 \cdot 2^m}. \quad (5)$$

Being $E\{y\} = ½$, and since:

$$r_{xx}(m) = E\{xT^m(x)\} = E\{(2y-1)(2S^m(y)-1)\} = E\{4yS^m(y) - 2S^m(y) - 2y + 1)\} = 4\, r_{yy}(m) - 1, \quad (6)$$

using (5) we have:

$$r_{xx}(m) = \frac{1}{3 \cdot 2^m}, \quad (7)$$

concluding the proof. □

For almost any B value smaller than 2 the analytical computation of the autocorrelation function is unfeasible, with the exception of few special values that make the system describable by a small order Markov chain [11]. However, thanks both to Theorem 1, and to other properties of the Sawtooth map discussed in [11], the expression (7) can be considered as a reliable approximation for the autocorrelation function when B is sufficiently close to 2. Numerical simulations, and measurements from an actual electronic realization of the circuit, confirm the validity of this assumption when $B \geq 1.97$ [9]. On the basis of (7), it is possible to select a down-sampling factor k that allows to obtain an almost uncorrelated sequence, with a pdf that can be in principle arbitrarily close to the uniform one within a subset of the domain. Assuming a down-sampling factor k, and denoting with r'_{xx} the autocorrelation function for the down-sampled sequence, expression (7) becomes:

$$r'_{xx}(m) = \frac{1}{3 \cdot 2^{m \cdot k}} = E\{xT^{k \cdot m}(x)\}. \quad (8)$$

Obviously, the greater is k, the less correlated are the output samples, and the lower is the throughput. Anyway, it is interesting noting that an equivalent down-sampling effect can be obtained with a direct implementation of the k-iterated Sawtooth map T^k, which is a feasible solution for small values of k, e.g., for $k = 2$ or 3. As an example, for $k = 2$ we have:

$$T^2(x) = \begin{cases} B^2(x-\alpha) + B + 1, & if\ -1 \leq x < \dfrac{\alpha + B\alpha - 1}{B}, \\ B^2(x-\alpha) + B - 1, & if\ \dfrac{\alpha + B\alpha - 1}{B} \leq x < \alpha, \\ B^2(x-\alpha) - B + 1, & if\ \alpha \leq x < \dfrac{\alpha + B\alpha + 1}{B}, \\ B^2(x-\alpha) - B - 1, & if\ \dfrac{\alpha + B\alpha + 1}{B} \leq x < 1. \end{cases} \quad (9)$$

Depending on B, α, and k, an almost flat spectrum can be obtained (e.g., as it can be seen in Fig. 3, $k = 4$ provides almost uncorrelated samples for B=1.98, and α=0.002). The curves reported in Fig. 3 were obtained estimating the pdf in 4096 frequency points, using a 10^7 output sample sequence.

IV. Conclusions

In this paper it was shown that the Sawtooth chaotic map can be a suitable source for almost uniform distributed samples in a wide subset of the domain. This is true also when actual circuit implementations are considered, for which the slope B of the Sawtooth chaotic map is < 2 but enough close to 2 (e.g., B>1.97). Moreover, the authors theoretically proved that, in the above hypothesis, the generated samples present an exponentially decreasing autocorrelation function, that can be reduced performing a proper down-sapling of the Sawtooth map output.

References

[1] J.E.Gentle, Random Number Generation and Monte Carlo Method, 2nd Ed, New York: Springer, 2005.
[2] M.G.C..Flores, M.Negreiros, L.Carro, A.A.Susin, "A noise generator for analog-to-digital converter testing", IEEE Integrated CAS Design, 2002. *Proc. 15th Symposium*, 9-14 Sept. 2002 pp. 135 – 140.
[3] D.U.Lee, W.Luk, J.Villasenor, P.Y.K.Cheung, "A hardware Gaussian noise generator for channel code evaluation", *IEEE Field-Programmable Custom Computing Machines*, 2003. FCCM 2003. 9-11 April 2003 pp. 69 – 78.
[4] Chun-Yu Chen; Chieh-Hsiun Kuan, "Design and calibration of a noise measurement system"; *IEEE Transactions on Instrumentation and Measurement*, Vol. 49, 1, Feb. 2000 pp. 77 – 82.
[6] T. Stojanovski and L. Kocarev, "Chaos based random number generators Part I: Analysis," IEEE Trans. Circuits Syst. I, vol. 48, no. 3, pp. 281-288, Mar. 2001.
[7] M. Delgado-Restituto and A. Rodriguez-Vazquez, "Integrated Chaos Generators", Proc. IEEE , vol. 90, pp. 747-767, May 2002.
[8] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, V. Vignoli, "A Feedback Strategy to Improve the Entropy of a Chaos-Based Random Bit Generator", *IEEE Trans. Circuits Syst. I*, vol. 53, no. 2, Feb. 2006 pp: 326 - 337.
[9] T.Addabbo, M.Alioto, A.Fort, S.Rocchi and V.Vignoli, "Uniform-Distributed Noise Generator Based on a Chaotic Circuit", *IMTC 2006, Proceedings of the 23rd IEEE Instrumentation and Measurement Technology Conference, 2006*, SORRENTO (ITALY), April 24-27, 2006, Page(s): 1156-1160.
[10] S. Callegari, R. Rovatti, and G. Setti, "Generation of constant-envelope spread-spectrum signals via chaos-based FM: Theory and simulation results," *IEEE Trans. Circ. Systems I*, vol. 50, pp. 3–15, 2003.
[11] T. Addabbo, A. Fort, D.Papini, S. Rocchi, and V. Vignoli, " Invariant Measures of Tunable Chaotic Sources: Robustness Analysis and Efficient Computation" *submitted to IEEE Trans. Circ. Systems I*, 2008.