Physica D 332 (2016) 34–40

Contents lists available at ScienceDirect

Physica D

journal homepage: www.elsevier.com/locate/physd

Entropy rates of low-significance bits sampled from chaotic physical systems

Ned J. Corron [*], Roy M. Cooper, Jonathan N. Blakely

Charles M. Bowden Laboratory, U.S. Army Research, Development and Engineering Command, Redstone Arsenal, AL 35898, USA

HIGHLIGHTS

- Entropy of low-significance bits in digital measurements of chaos is examined.
- Low-significance bits yield a two-symbol partition with a corrugated structure.
- Corrugation at low-significance bits better approximates a generating partition.
- Entropy rate estimation using lower-significance bits requires longer block lengths.
- Considering only short block lengths can overestimate entropy of physical system.

ARTICLE INFO

Article history:
Received 12 August 2015
Received in revised form
7 June 2016
Accepted 8 June 2016
Available online 16 June 2016
Communicated by A. Pikovsky

Keywords:
Chaos
Entropy
Symbolic dynamics
Partition

ABSTRACT

We examine the entropy of low-significance bits in analog-to-digital measurements of chaotic dynamical systems. We find the partition of measurement space corresponding to low-significance bits has a corrugated structure. Using simulated measurements of a map and experimental data from a circuit, we identify two consequences of this corrugated partition. First, entropy rates for sequences of low-significance bits more closely approach the metric entropy of the chaotic system, because the corrugated partition better approximates a generating partition. Second, accurate estimation of the entropy rate using low-significance bits requires long block lengths as the corrugated partition introduces more long-term correlation, and using only short block lengths overestimates the entropy rate. This second phenomenon may explain recent reports of experimental systems producing binary sequences that pass statistical tests of randomness at rates that may be significantly beyond the metric entropy rate of the physical source.

Published by Elsevier B.V.

1. Introduction

Recently a number of reports have demonstrated the potential of using chaotic dynamics for high-speed generation of physical, true-random bit sequences [1–10]. These developments are driven by a growing demand for truly random bit sequences for robust cryptography and large-scale Monte Carlo simulations [11–13]. In many of the reported experiments, a chaotic system is sampled using an analog-to-digital converter (ADC) with a fixed number of bits of precision. Empirically, it is often found that sequences of the most significant bits from the ADC fail standard statistical tests of randomness, such as provided by the US National Institute of Standards and Technology (NIST) [14]. However, a number of reports have also shown that sequences obtained using bits of lower significance do pass these tests [4–10]. Furthermore, to achieve the fastest random bit rates, many reports have shown that using multiple low-significance bits from each measurement can multiply the effective bit rate and still pass the statistical tests [4–8].

In deriving random sequences from deterministic chaos, it is critical to consider the metric entropy of the chaotic physical system [15–17]. The capacity of a chaotic system to generate new information or randomness is quantified by its positive Lyapunov exponents or, equivalently, its metric entropy [18–22]. Importantly, any random bit sequence exceeding the metric entropy necessarily exhibits biases or correlations consistent with the deterministic dynamics of the system. For any reported study that does not consider the metric entropy of the physical device, there is a concern that high bit rates may exceed this theoretical limit. In such a case, it is not correct to describe the collected bit sequences as truly random. The use of bits derived at such rates must then be considered similar to the use of pseudorandom number generators, which actually have zero

[*] Correspondence to: U.S. Army RDECOM, RDMR-WDS-WO, Redstone Arsenal, AL 35898, USA.

E-mail address: ned.j.corron.civ@mail.mil (N.J. Corron).

http://dx.doi.org/10.1016/j.physd.2016.06.003
0167-2789/Published by Elsevier B.V.

entropy but are practically unpredictable and can pass statistical tests of randomness [20,23].

For any real physical system, it is also important to consider the effects of the measurement process, which may be viewed as a communication channel with noise [24,25]. For noisy measurements, additional entropy can be added to a bit sequence [8]. The effect of measurement noise would be more significant for sequences from bits of low significance compared to those using the most significant bits. However, the number of reports from various research groups using different experimental systems strongly suggests that fast random bit sequences are not simply derived from measurement noise.

In this paper we seek to understand the nature of randomness derived from measurements of chaotic dynamics using low-significance bits under the assumption that measurement noise is negligible. Specifically, we examine how the use of bits of different significance affects an estimate of the entropy of the source. We begin by considering a noise-free model of the measurement process applied to a chaotic system. We recognize that there is a two-symbol partition of the measurement space corresponding to each bit of the analog-to-digital conversion. Notably, the partition corresponding to a bit of low significance has a periodic or "corrugated" structure with a characteristic length scale that depends on the bit significance. In turn, an estimation of entropy using such a partition is also scale dependent.

Scale-dependent entropies have been previously used for characterizing deterministic and stochastic processes [19,20]. Such methods calculate an entropy using coarse-grained partitions characterized by a length scale ε. In particular, the entropy $h(\varepsilon)$ is defined as the infimum over all possible partitions comprising individual cells no larger than the characteristic scale ε. For small ε, the number of partitions, and the corresponding alphabet size, can be very large. In contrast, in this paper we focus on a particular partition motivated by the nature of analog-to-digital conversion. As we consider lower significant bits, the scale of the partition decreases, potentially resolving finer detail. However, at all scales the corrugated partition uses only two symbols. The effects of this partition manifest in the estimation of entropy as we show in this paper, with practical consequences for evaluating random number generators based on measurements of chaotic processes.

Using numerical simulations, we observe two phenomena in the estimation of the entropy of a bit sequence resulting from a corrugated partition. First, entropy rate estimates based on sequences derived from low-significance bits more closely approach the metric entropy than do those from high-significance bits. We attribute this effect to the corrugated partition for lower significance bits more closely approximating a generating partition than that for higher significance bits. Second, accurate estimation of the entropy rate using low-significance bits requires the use of longer block lengths than for high-significance bits. The corrugated partition appears to produce more long-term correlation that is only detected using long block lengths. We observe these same phenomena at work in an experimental system of a chaotic electronic oscillator sampled using a digital data acquisition system. Altogether, these results indicate care must be taken to properly characterize the metric entropy of a physical device before assuming bits collected at a high rate are truly random.

2. The partition corresponding to a measurement process

When sampling a physical signal exhibiting chaos using a measurement instrument, the measurement scale is typically chosen for practical reasons. For example, from among a discrete set of scales on a digital oscilloscope, one chooses the vertical scale to maximize the dynamic range while avoiding out-of-range values or saturation. To each bit in the representation of the samples there is a corresponding partition of the state space. For example, the most-significant bit partitions the space into two regions separated by a threshold at the middle of the input range of the measurement device. Typically, the partition is misplaced, meaning it is not generating [26]. As such, there exist different trajectories in the physical dynamics that cannot be distinguished using the partition, and symbol sequences derived from the partition will have less entropy per symbol than the metric entropy. However, in what follows we will show that the partition corresponding to a lower significant bit more closely approximates a generating partition and thus provides symbols with more entropy.

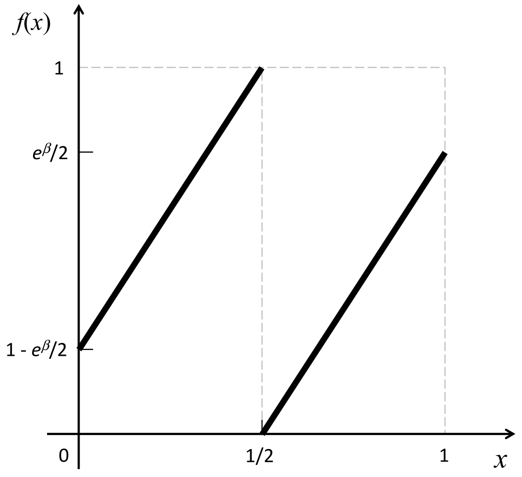

Fig. 1. Iterated map function.

To illustrate this idea in a toy model, we consider iterations of a simple one-dimensional chaotic map. That is, we consider the iterated map

$$x_{i+1} = f(x_i) \tag{1}$$

where

$$f(x) = \begin{cases} 1 + e^{\beta}(x - 1/2), & x < 1/2 \\ e^{\beta}(x - 1/2), & x \geq 1/2 \end{cases} \tag{2}$$

and $0 < \beta \leq \ln 2$ is a map parameter. The map function is shown in Fig. 1. This piecewise-linear map is closed on the unit interval and both segments have slope $e^{\beta} > 1$. As such, the iterated map is chaotic with positive Lyapunov exponent β and metric entropy

$$h = \frac{\beta}{\ln 2} \tag{3}$$

where the denominator provides the units of bits per iterate.

Using this simple dynamical system, we emulate a physical measurement process using scaled iterates as samples. That is, we let the ith measurement sample be

$$y_i = K \cdot x_i \tag{4}$$

where $0 < K \leq 1$ represents an arbitrary scaling that projects the physical values into the selected range of the measuring instrument. We then model an N-bit ADC by approximating the sample using the truncated binary sequence

$$y_i \cong \sum_{n=1}^{N} b_{i,n} \cdot 2^{-n} \tag{5}$$

where each $b_{i,n}$ is a bit with value 0 or 1. The subscript n indicates the significance of these bits in the sampling process. The set of all bits $b_{i,n}$ can then be subdivided into N sequences of bits according to significance. For example, the sequence $b_{i,1}$ is a sequence derived