Available online at www.sciencedirect.com
SCIENCE DIRECT®
Physica A 354 (2005) 281–300
PHYSICA A
www.elsevier.com/locate/physa

Statistical complexity measure of pseudorandom bit generators

C.M. González[a], H.A. Larrondo[a], O.A. Rosso[b,*]

[a]*Facultad de Ingeniería, Universidad Nacional de Mar del Plata, Juan B. Justo 4302, 7600 Mar del Plata, Argentina*
[b]*Chaos & Biology Group, Instituto de Cálculo, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Pabellón II, Ciudad Universitaria, 1428 Ciudad de Buenos Aires, Argentina*

Received 20 October 2004
Available online 18 April 2005

Abstract

Pseudorandom number generators (PRNG) are extensively used in Monte Carlo simulations, gambling machines and cryptography as substitutes of ideal random number generators (RNG). Each application imposes different statistical requirements to PRNGs. As L'Ecuyer clearly states "the main goal for Monte Carlo methods is to reproduce the statistical properties on which these methods are based whereas for gambling machines and cryptology, observing the sequence of output values for some time should provide no practical advantage for predicting the forthcoming numbers better than by just guessing at random". In accordance with different applications several statistical test suites have been developed to analyze the sequences generated by PRNGs. In a recent paper a new statistical complexity measure [Phys. Lett. A 311 (2003) 126] has been defined. Here we propose this measure, as a randomness quantifier of a PRNGs. The test is applied to three very well known and widely tested PRNGs available in the literature. All of them are based on mathematical algorithms. Another PRNGs based on Lorenz 3D chaotic dynamical system is also analyzed. PRNGs based on chaos may be considered as a model for physical noise sources and important new results are recently reported. All the design steps of this PRNG are described, and each stage increase the PRNG randomness using different strategies. It is shown that the MPR statistical

*Corresponding author. Tel./fax: +54 11 4576 3375.
E-mail addresses: cmgonzal@fi.mdp.edu.ar (C.M. González), larrondo@fi.mdp.edu.ar (H.A. Larrondo), oarosso@fibertel.com.ar, rosso@ba.net (O.A. Rosso).

doi:10.1016/j.physa.2005.02.054

complexity measure is capable to quantify this randomness improvement. The PRNG based on the chaotic 3D Lorenz dynamical system is also evaluated using traditional digital signal processing tools for comparison.

PACS: 03.67. −a; 89.70. + c; 03.65.Bz

Keywords: Random number generators; Statistical complexity

1. Introduction

Random number generators (RNGs) are essential in statistical studies in several fields. They may be based on physical noise sources or on mathematical algorithms, but in both cases truly random numbers are not obtained because of data acquisition systems in the first case or because machine precision in the second case. Instead, any real implementation actually produces a pseudorandom number generator (PRNG). In spite of this restriction PRNGs have been developed to fulfill many statistical properties required in applications, mainly Monte Carlo simulations, gambling machines and cryptography [1]. Chaotic dynamical systems are models of a lot of physical phenomena [2]. Their sensitivity to initial conditions and their broadband spectrum make them good candidates to generate PRNGs with a behavior very similar to physical noise sources. New important research papers have recently appeared concerning this kind of PRNGs [3–11].

There are several basic properties any good PRNG must fit: long cycle length, randomness, speed, reproducibility and portability. Several test suites [12] are readily available to researchers in academia and industry who wish to analyze their newly developed PRNG. Some general purpose test suites are *Diehard* by George Marsaglia [13], *Crypt-XS* by Helen Gustafson of the Queensland University of Technology [14], the National Institute of Standards and Technology Statistical Test Suite [15]. Additional requirements are imposed in view of the specific application. As L'Ecuyer clearly states "the main goal for Monte Carlo methods is to reproduce the statistical properties on which these methods are based whereas for gambling machines and cryptology, observing the sequence of output values for some time should provide no practical advantage for predicting the forthcoming numbers better than by just guessing at random" [16]. Of course a statistical test can never prove that a sequence generated by a PRNG is random (*because it is not !*), but it helps to detect certain kinds of weaknesses a generator may have. Furthermore none of these tests can prove that a given generator is reliable in all applications. Vattulainen et al. [17], for example, proposed three additional physical tests, to detect deficiencies of several PRNGs used in Monte Carlo simulations.

In the framework of dynamical system theory, the statistical characterization of deterministic sources of apparent randomness was studied by many authors. Tools as metric entropy, Lyapunov exponents, and fractal dimension [18,19] have shed much light into the intricacies of dynamical behavior by describing the