CHAOS 2009

2^{nd} Chaotic Modeling and Simulation International Conference

June 1 - 5, 2009 Chania Crete Greece www.chaos2009.net

Periodicity of One Dimensional Chaotic Map

Hassan N. Noura, Safwan El ASSAD
Ecole polytechnique de Nantes, Nantes, France
hassan.noura@univ-nantes.fr

Recently, chaotic systems have been widely used to design digital systems, such as: digital ciphers, pseudo-random number generators (PRNG) and digital communication systems. The chaotic map is realized in a finite precision; therefore, its orbits will eventually become periodic. However, the floating and fixed point representations are briefly studied and their impacts for cycle length are estimated by simulations. On the other hand, it is often required that the chaotic generators have very long cycle lengths to resist attacks. It had been found that the periods of chaotic trajectories can be rather short even the high-precision computation is applied. Furthermore, for each precision, the number of periodic orbits of computer realization is surprisingly small even if the precision is rather high. The obtained results show that the longest cycle length is smaller than the maximum possible one. It is believed that the problems of short period and small number of periodic orbits may seriously affect chaos' applications and result in either weak cryptography or secure communication. The goal of this work is to achieve long cycle lengths; therefore, two methods are proposed. The first one is a perturbation based on LFSR, and the second one consists of using a multiplexer with a few LFSR generator. Experimental and theoretical analyses show that the proposed methods have periods as large as practically unreachable

Keywords: Cycle length, fixed point,NIST Statistical properties, Balance of probability.