APPLIED DYNAMICS GROUP SEMINAR

On the properties of nonlinear congruential number generators based on logistic maps

R MURAT DEMIRER
İstanbul Kültür University

Faculty of Science and Letters, Mathematics and Computer Department
E5 Karayolu Uzeri Bakirkoy 34156 Istanbul

Abstract: Pseudorandomness generates information on almost random sequences which finds applications in cryptography and in complexity theory. The focus of this talk is based on an efficient construction of a pseudorandom function incorporating chaotic maps into a modulo 2^M-based decorrelated polynomial in $F_p(x)$. After we will discuss an introduction to some chaotic maps and some theorems about number theory, we will focus more specifically on a new non-linear congruential pseudorandom number generator class. This class is built around a core of chaotic maps, namely, logistic maps here in this talk, $F_{C_{n+1}}(X) = X_{n+1} = C_{n+1}X_n(1 - X_n)$ for $F_C : [0, 1] \rightarrow [0, 1]$. The orbits begin very chaotic near $C = 3.56699$ for logistic maps. Higher order compositions of the logistic maps are placed into an a modulo 2^M-based polynomial with a certain congruential properties of which modulus numbers are generated by a set of prime numbers acquired from number theory. This prime number progression determined by this running modulus function constitutes up integer coefficients of a random polynomial structure which is responsible for decorrelation of the terms. Each term of random polynomial is obtained by compositions of successive logistic map terms. In other words, the structure of such a generator depends on chaotic disordered state of summation of higher order composition of logistic maps with the integer coefficients.

This approach generates a sequence of independent identically distributed random values on a probability space with values in $\aleph \cup 0$. The proposed polynomial includes successive compositions of logistic maps running in interval of $3.5669 < C_{n+1} \leq 4$ with a linear growth rate. Logistic maps takes the form of random logistic maps when all are summed in a polynomial structure with a congruent modulus number. It is then hard to differentiate this function from a uniformly distributed function as a black-box.