A Chaos theoretic Parallel Pseudorandom generator in RNC For Majority Voting and Pseudorandom Choice

Ka.Shrinivaasan (ka.shrinivaasan@gmail.com)

March 20, 2013

Abstract

In this article a Parallel Pseudorandom bit generator which exhibits Chaos theoretic behaviour and is in Randomized NC is presented.

1 Introduction

Theory of Chaotic systems and non-linear dynamics had created a widespread interest in the previous century and its applications were felt in numerous fields like weather forecast,economic phenomena like stock markets etc., As the Chaotic systems study non-linearity and inherent unpredictability or randomness in nature,they are the obvious choice for a pseudorandom source of stream of bits whose necessity often arises in Crptographic functions, Randomized Algorithms in class BPP(Monte carlo and Las Vegas algorithms).

2 Logistic function and Lorenz Strange Attractors

In the middle of previous century,longterm weather forecasting received a jolt when Lorenz discovered a chaotic behaviour in weather predictive model equations due to a floating point round-off error which made the computer generated predictions (also called Strange attractors due to oscillation of the attractor between two centroids) to sharply deviate from expected values. Proverbially, this sensitive dependence on initial conditions is described as "flapping butterfly causes hurricane in atlantic". Verhulst's logistic function used in actuarial science $x_{n+1} = lamda * x_n * (1 - x_n)$ is one such equation which exhibits chaotic behaviour.This recursive function initially oscillates with some periodicity and gradually chaos sets in to exhibit aperiodic, apparent randomness.

3 Parallel Pseudorandom bit generators in RNC with Chaotic behaviours

Lehmer's Prime Modulus Multiplicative Linear Congruence Pseudorandom Generators was one of the oldest Pseudorandom number generators and is defined as follows:

$$x_{n+1} = B * x_n \quad mod \quad M \quad where \quad B \quad > \quad 0 \tag{1}$$

and M is a large prime and $x_0 > 0$ is the initial condition.

Palmore's Pseudorandom generator which was a later PRNG, is defined as,

$$x_{n+1} = B * x_n \quad mod \quad 1 \tag{2}$$

where x_0 is the initial input fraction and B is the radix in which x is expressed.

Lehmer's and Palmore's Pseudorandom generators exhibit Chaotic behaviour due to sensitive dependence on initial input.Many Chaotic Pseudorandom number generators have been studied. [Tygar and Rief] gives an implementation of a parallel pseudorandom generator that is in Randomized NC. Each processor i in the parallel algorithm evaluates the function $B(k * s^i mod N)$ and gets set of bits from all processors in parallel, where

$$B(x) = 0 \quad if \quad x \quad < \quad N/2 \quad and \quad 1 \quad if \quad x >= N/2 \tag{3}$$

Input to function B can be replaced with Lehmer's or Palmore's pseudorandom generator in each processor of the Tygar-Rief algorithm giving a Chaotic Parallel Pseudorandom generator in Randomized NC.This PRG can be applied to the Randomized Circuits for Pseudorandom Choice and Majority Voting giving a RNC circuit (instead of a BPNC circuit).

4 Acknolwdgement

I dedicate this article to God.

5 Bibliography

References

[1] RANDOM NUMBER GENERATORS ARE CHAOTIC -Charles Herring and Palmore,CACM, Vol. 38, Nu. 1, Technical Correspondence. (Appeared in ACM SIGPLAN Notices, 11, October 1989)

[2] Efficient Parallel Pseudorandom number generation - Tygar and Reif, SIAM journal of computing,Vol 17 No.2,1988

[3] Various resources on Chaos theory,non-linear dynamics and attractors

[4] Lower Bounds For Majority Voting and Pseudorandom Choice - https://sites.google.com/site/kuja27/LowerBoundsForMajorityVotingPseudorandomChoice.pdf?attredirects=

[5] Circuit For Computing Error Probability of Majority Voting - https://sites.google.com/site/kuja27/CircuitForComputingErrorProbabilityOfMajorityVoting.pdf?attredirect

[6] Indepth analysis of a variant of Majority Voting with ZFC - https://sites.google.com/site/kuja27/IndepthAnalysisOfVariantOfMajorityVotingwithZFAOC.pdf?attredirect