Period Extension and Randomness Compensation Using High-Throughput Self-Reseeding PRNG on the Digitized Logistic Map

1 Introduction

1.1 The importance of PRNG

1. simulation and communication... (the same as before)

1.2 History and categories

1. nonlinear map: BBS
   (a) Advantages: good randomness, unpredictable
   (b) Disadvantages: slow, complex

2. Chaos-based
   (a) Advantages: efficient
   (b) Disadvantage: limited period, truncation error, poor statistical properties

1.3 Contribution in this paper: Period Extension and Randomness Compensation

1. Method: reseeding+mixing (mutual prime)
   (a) Reseeding
      i. remove low-period (fine tune)
      ii. uniqueness: simple, efficient
      iii. fine tune
   (b) mixing
i. prolong period (coarse tune)

ii. uniqueness: effective, low area-overhead, period is known theoretically

2. Result

(a) long period: product of subsystems

(b) randomness compensation: pass the test

1.4 Organization

2 Background

1. the same as 5644

2. exhaustive simulation without reseeding

3 Self-reseeding

4 Hardware Design and Numerical Simulations

5 Comparisons

6 Conclusion