On Pseudo Random Numbers Generator

MCT

May 10, 2023

1 Introduction

In computer sciences, huge contributions were introduced in the literature, as sequence of numbers basicly expressed as :

$$\begin{cases} x_0 \text{ given} \\ x_{n+1} = (ax_n + b) \mod m. \end{cases}$$

G. Marsaglia (2003) describe a set of pseudo-random numbers generator (PRNGs) with their proprieties. Here is some basic PRNGs for 16-32 bits random numbers :

1. **Multiply with carry algorithm**

```
    Xi = [(A * Xi-1) + Ci-1] Mod M
    Ci = Integer[((A * Xi-1) + Ci-1) / M]
Where:
    Xi-1 is the previous integer (seed value)
    Xi is the next seed integer
    Ci-1 is the previous carry integer
    Ci is the next carry
    A = 4,164,903,690
    M = 2^32 = 4,294,967,296 (the modulus)
Note:
    B = (A * M) - 1 = 17,888,125,139,539,722,239
    P = (B - 1) / 2 = 8,944,062,569,769,861,119
    B and P are both prime.
    The period of the generator is P.
    Period =~ 8.944 * 10^18 =~ 2^63.
```

2. **Fibonnaci algorithm**

$$\begin{cases} x_0 = x_1 = 1 \\ x_{n+1} = (x_n + x_{n-1}) \mod 2^{32}. \end{cases}$$

3. **Congruential generator**

$$\begin{cases} x_0 = x_1 = 1 \\ x_{n+1} = (69069x_n + 1234567) \mod 2^{32}. \end{cases}$$

This PRNGs are constructed to get a sequence from a given burn-in integer $n_0 > 50$.

The main work on this project, is to implement and test the efficiency of this PRNGs, by generating sequences between 0 and $2^m - 1$ ($m = 16$ or 32), and deducing the uniform sequence given by $x_n/2^m$ (to get values between 0 and 1). We assume that this sequence is a sample of the standard uniform distribution in $[0, 1]$.

Then, the procedure is to calculate the sample obtained by a transformation of the previous sequence using the relation $Z = -\frac{1}{\lambda}\ln(1 - U), \lambda > 1$. The resulting sequence is assumed to be distributed according to the exponential distribution of parameter λ.

Procedure of test : Since the sample obtained after the transformation is assumed from a n exponential distribution of parameter λ, then its average value will be approximately close to $\frac{1}{\lambda}$, and its standard deviation close to $\frac{1}{\lambda}$.

The same procedure is to be checked according to other probability distributions.