Modelling and Simulation of Systems
Exercise 3: Pseudorandom number generators

Agata Radys, Paweł Cejrowski, Łukasz Myśliński

November 10, 2016

Tester: Paweł Cejrowski

1 Generator 1

1.1 Equation

Numbers are generated according to equation 1.

$$x_{n+1} = x_n \oplus x_{n-1} \pmod{2^{32}} \tag{1}$$

where x_0 and x_1 are given.

1.2 Questions

- **What is the minimum(maximum) possible value of the period? Give an example of initial values for which the period is small(large).**
  Minimum value of period is equal 1, when both x_0 and x_1 are equal 0. Maximum value of period is 3 when x_0 or x_1 is different from 0(e.g. $x_0 = 0$ and $x_1 = 16$).

- **What is the minimum(maximum) possible mean value? Give an example of initial values for which the average value is small(large).**
  Minimum possible mean value is equal 0, when both x_0 and x_1 are equal 0. Maximum founded mean value of period is equal $\frac{2}{3} \cdot (2^{32} - 1) = 2863311530$, when $x_0 = x_1 = 2^{32} - 1$

- **What is the minimum(maximum) possible variance? Give an example of initial values for which the variance is small(large).**
  Minimum possible variance value is equal 0, when both x_0 and x_1 are equal 0. Maximum founded variance value of period is equal $4.0992764589155E + 18$, when $x_0 = x_1 = 2^{32} - 1$

- **Does the generator meet the requirements that good generators should satisfy? If not, which of the requirements are not satisfied and why?**
  The generator does **not** meet all requirements for good generators.
  Characteristics of good generators:

  1. **generated numbers distributions are as close as possible to the desired one**
     Not satisfied: 3 point distribution.
  2. **subsequences of the produced sequence are mutually independent**
     Not satisfied: each subsequence of length 3 contains the same 3 numbers.
  3. **long period, with length at least $\sqrt{n}$, where n is the length of the used subsequence**
     Not satisfied: short period with maximum length of 3.
  4. **the ability to make jumps, i.e. to compute x_j from x_i for every $j > i$**
     Not satisfied: x_j cannot be computed from single number x_i, at least one other number x_k, where $k(mod\ 3) \neq i(mod\ 3)$ needed.
  5. **repeatable, portable and efficient**
     Satisfied(with minor objections to efficiency, due to inability of making jumps).

- **Is the generator suitable for use in the cryptography? If not, why?**
  The generator is **not** suitable for use in the cryptography, because it does not satisfy any of the desired conditions.
  Characteristics of generators suitable for use in the cryptography:

  1. **it must be impossible to predict its seed and internal state even if we have a large sample of the numbers it produced**
     Not satisfied: it is very easy to predict the number when the period is at most 3 numbers long.
  2. **it must have a long period for every possible value of its seed**
     Not satisfied: do not have long period for any seed.
  3. **it should be unpredictable to the public, i.e. the probability of predicting the subsequent numbers should be low even if have a large sample of the numbers it produced**
     Not satisfied: having 3 consecutive numbers one can predict any other.

2 Generator 2

2.1 Equation

Numbers are generated according to equation 2.

$$x_{n+1} = 3 \cdot x_n - 1 \quad (mod\ 2^{32}) \tag{2}$$

where x_0 is given.

3 Generator 3

3.1 Equation

Numbers are generated according to equation 3.

$$\begin{cases} x'_{n+1} = x'_n \oplus x'_{n-1} \quad (mod\ 2^{32}) \\ x''_{n+1} = 3 \cdot x''_n - 1 \quad (mod\ 2^{32}) \\ x_{n+1} = x'_{n+1} \cdot x''_{n+1} \quad (mod\ 2^{32}) \end{cases} \tag{3}$$

where x'_0, x'_1 and x''_0 are given.