Course 07/2

Random number generators (1/2)

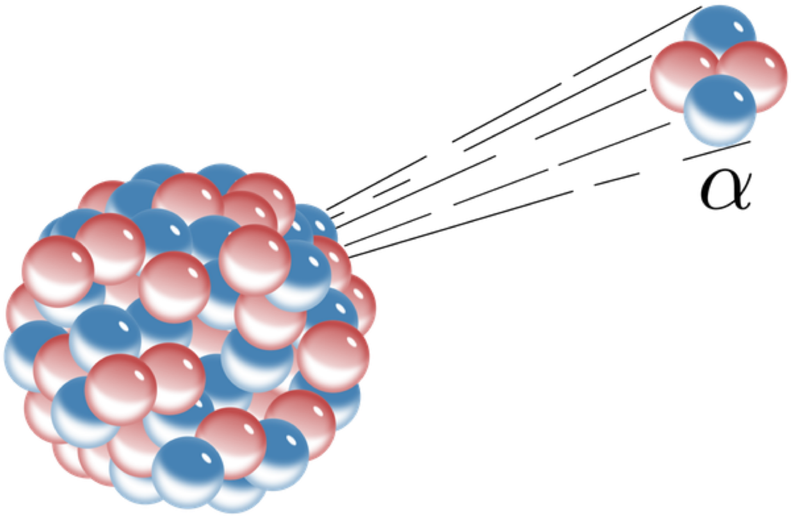
- Random numbers on the computer
- Modulo generator
  - Properties
  - Shuffle algorithm
  - L’Ecuyer’s algorithm

Random number on the computer

Pure or true random numbers

A true random number – to be truly *unpredictable* – must be taken from the physical world taking advantage e.g. of some underlying quantum mechanical property or of statistically random noise signals.

Example: decaying radioactive source
emission of α particles



After each interval of 20 ms

- Even number of events $\rightarrow$ 0
- Odd number of events $\rightarrow$ 1

Stored on an internet site? 10^6?
Limitations, unpractical.

Random number on the computer

Pseudo random numbers

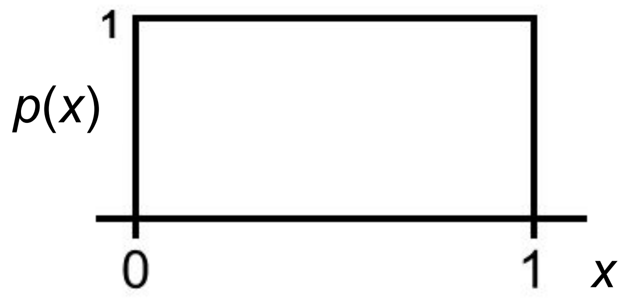
Numbers generated by a computer in a fully deterministic fashion using a mathematical formula and previously generated numbers.
Fully predictable!

Scope

Generate a sequence which is difficult to discern from a sequence of true random numbers. Depending on the properties requested (i.e. the application), this might be sufficient to operate as a true series of random numbers.

Criteria for series of pseudo random numbers

Uniformity



- For instance in the interval [0,1]
- Probability density $p(x)$, i.e. $p(x)dx$ is the probability of finding x in the interval $[\, x,\ x+dx \,]$.
- Uniformity: $\begin{cases} p(x) = 1 & \text{for} \quad 0 < x < 1 \\ p(x) = 0 & \text{elsewhere} \end{cases}$
- Nonuniform distributions are also possible.

Absence of correlations

- Probability for successive events x_i and x_{i+1} : $P(x_i, x_{i+1}) = P(x_i) \cdot P(x_{i+1})$
- Same for $P(x_i, x_j)$ with $j > i + 1$.
- Same for $P(x_i, x_j, x_k)$ or with distribution functions of more than three variables.

Random number generator: Modulo generator

- On the computer, we only have discrete values, which correspond to integers.
- Congruential algorithm:

$$x_{i+1} = (a \cdot x_i + c) \bmod m \qquad \text{for} \quad i > 0$$

where x_0 = “seed” and, usually, $c = 0$.

- By dividing by m, one gets values between 0 and 1.
- For $x_0 = 0$ (and $c = 0$), all $x_i = 0$ (sequence of “0”).
- $m - 1$ of possible different random numbers.
- We get indeed $m - 1$ different random numbers for special combinations of a and m.
- Example: $a = 12$, $m = 143$. We start with x_i.

$$x_{i+1} = (12\, x_i) \bmod 143$$

$$x_{i+2} = (12^2\, x_i) \bmod 143 = (144\, x_i) \bmod 143 = (143\, x_i + x_i) \bmod 143 = x_i$$

Cycle of 2!

- For r available bits, $m = 2^r - 1$. In a 32-bit computer, $r = 31$, because one bit is used to store the sign.

Random number generator: Modulo generator

Minimal standard (Park & Miller)

- $a = 7^5 = 16807$, $m = 2^r - 1$, $c = 0$.

Problems

1. Low order serial correlations
   - small a : small number followed by small number
   - (x_i , x_{i+1}) give lines in 2D and (x_i , x_{i+1} , x_{i+2}) planes in 3D.

   → shuffle algorithm

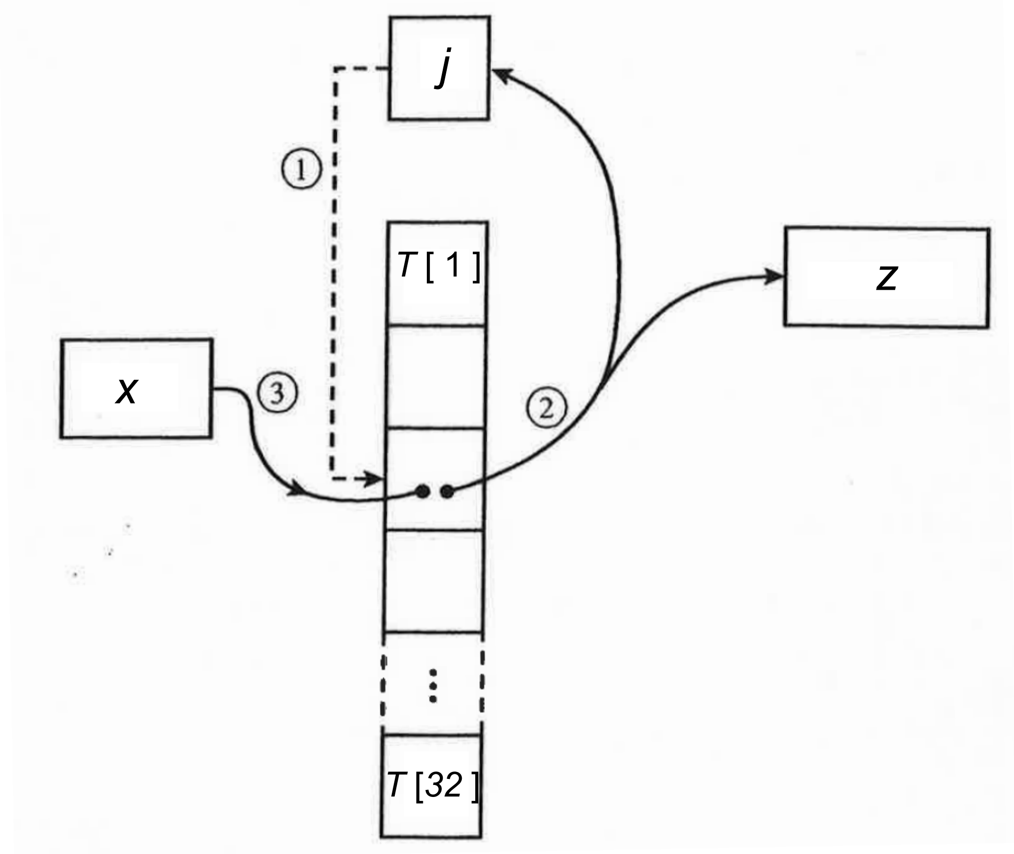
2. Small period

   → combination of different random number series

Random number generator: Modulo generator

Shuffle algorithm

- Congruential series: .... x_i , x_{i+1} , x_{i+2} ,.....
- Memory table : T [1], ...T [j], ... T [32] (32 slots)
- Scope: generation of series .... z_i , z_{i+1} , z_{i+2} ,..... without low-order serial correlations.



- Fill the memory table T
- Suppose that we have z_i and that we want to determine z_{i+1}.

1. Use memory slot j determined from z_i.
2. Take z_{i+1} = T [j].
3. Shuffle x_{i+1} into T [j].

In this way, the outgoing z number originates from a previous x number that has been put in the table, 32 steps earlier on average.

Random number generator: Modulo generator

Combination of different series (L'Ecuyer 1988)

- We illustrate this point through an example.
- Suppose we have two congruential series:

$$x_n = 40014\, x_{n-1} \mod (2^{31} - 85)$$

$$y_n = 40692\, y_{n-1} \mod (2^{31} - 249)$$

- Their periods are (factorial decomposition):

$$m_x - 1 = 2 \cdot 3 \cdot 7 \cdot 631 \cdot 81031 \qquad \sim 2 \cdot 10^9$$
$$m_y - 1 = 2 \cdot 19 \cdot 31 \cdot 1019 \cdot 1789 \qquad \sim 2 \cdot 10^9$$

- New random number series:

$$z_n = (x_n - y_n) \mod m_x$$

- Period of new series :

$$\frac{(m_x - 1) \cdot (m_y - 1)}{2} \approx 2.3 \cdot 10^{18} \approx 2^{62}$$

- Periods that can be achieved today with more sophisticated tricks: 2^{1500}.

Random number generator: RAN2

Algorithm proposed by *“Numerical Recipes”*

- Congruential (modulo) algorithm – Minimal Standard.
- Shuffle algorithm to break low-order serial correlations.
- L’Ecuyer’s algorithm to increase the period.

Course 07/2

Random number generators (1/2)

- Random numbers on the computer
- Modulo generator
  - Properties
  - Shuffle algorithm
  - L'Ecuyer's algorithm