

몬테카를로 방사선해석 (Monte Carlo Radiation Analysis)

Random Number Generator (RNG)

Random Number Generation

➤ Desirable Attributes:

- Uniformity: RNs distributed uniformly on $(0, 1)$
- Independence: no correlation b/w RNs
- Efficiency: fast and minimal need for storage
- Replicability*
 - debugging
 - compare various scenarios or different systems
- Long Cycle Length

➤ Independent and identically distributed (i.i.d.) RV

➤ *Independent and identically distributed (i.i.d.) RV*

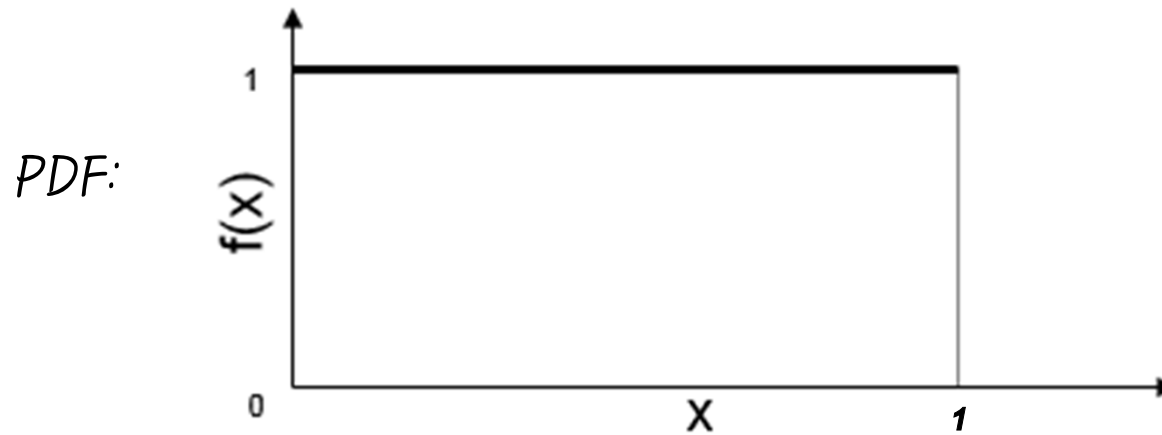
- *Identically Distributed means that there are no overall trends: the distribution doesn't fluctuate and all items in the sample are taken from the same probability distribution.*
- *Independent means that the sample items are all independent events. In other words, they aren't connected to each other in any way.*

Random Number Generation (cont.)

- Each random number R_t is an independent sample drawn from a continuous uniform distribution between 0 and 1

$$\text{pdf: } f(x) = \begin{cases} 1, & 0 \leq x \leq 1 \\ 0, & \text{otherwise} \end{cases}$$

Random Number Generation (cont.)



$$E(R) = \int_0^1 x dx = [x^2/2]_0^1 = 1/2$$

$$\begin{aligned} V(R) &= \int_0^1 x^2 dx - [E(R)]^2 \\ &= [x^3/3]_0^1 - (1/2)^2 = 1/3 - 1/4 = 1/12 \end{aligned}$$

Random Number Generation (cont.)

➤ Most random-number generators are of the form:

1. Start with a seed number X_0 .

2. Generate $X_n = f(X_{n-1})$ for $n = 1, 2, 3, \dots$.

3. Obtain $R_n = g(X_n)$

where f is a pseudo-random generator and g is the output function

Random Number Generation Method #1

➤ Midsquare Method

$$X_0 = 7182 \text{ (seed)}, X_0^2 = 51\underline{5811}24$$

$$\implies R_1 = 0.5811$$

$$X_1^2 = (5811)^2 = 337\underline{677}21$$

$$\implies R_2 = 0.7677$$

➤ Midsquare Method (cont.)

Note: Cannot choose a seed that guarantees that the sequence will not degenerate and will have a long period. Also, zeros, once they appear, are carried in subsequent numbers.

$$\text{Ex 1. } X_0 = 5197 \text{ (seed), } X_0^2 = \underline{27008809}$$

$$\implies R_1 = 0.0088, X_1^2 = \underline{00007744}$$

$$\implies R_2 = 0.0077$$

$$\text{Ex 2. } X_0 = 4500 \text{ (seed), } X_0^2 = \underline{20250000}$$

$$\implies R_1 = 0.2500, X_1^2 = \underline{06250000}$$

$$\implies R_2 = 0.2500$$

Note: Modular Mathematics

- ✓ When we divide a number into two integers, we will have an equation that looks like the following:

$$A / B = Q \text{ with remainder } R$$

A is the dividend; B is the divisor; Q is the quotient; and R is the remainder.

- ✓ Sometimes, we are only interested in what the remainder will be when we divide A by B. For these cases there is an operator called the modulo operator (abbreviated as mod).

Using the same A, B, Q, and R as above, we would have:

$$A \text{ mod } B = R$$

We would say this as "A modulo B is congruent to R". Where B is referred to as the modulus.

e.g. $13/5 = 2$ with remainder 3, or $13 \text{ mod } 5 = 3$

Random Number Generation Method #2

➤ Linear Congruential Generator

- Basic Relationship

$$X_i = (a X_{i-1} + c) \bmod m, \text{ where } a \geq 0 \text{ and } m \geq 0$$

$$R_i = X_i / m$$

- Most natural choice for m is one that equals to the capacity of a computer word.
- $m = 2^b$ (binary machine), where b is the number of bits in the computer word.
- $m = 10^d$ (decimal machine), where d is the number of digits in the computer word.

➤ *Linear Congruential Generator (cont.)*

- *16-bit machine*

$$a = 1217, c = 0, X_0 = 23, m = 2^{15} - 1 = 32767$$

$$X_1 = (1217 * 23) \bmod 32767 = 27991$$

$$R_1 = 27991 / 32767 = 0.85424$$

$$X_2 = (1217 * 27991) \bmod 32767 = 20134$$

$$R_2 = 20134 / 32767 = 0.61446$$

➤ Linear Congruential Generator (cont.)

$$X_{i+1} = (a X_i + c) \bmod m, \text{ where } m > 0, 0 < a < m \text{ and } 0 \leq c < m.$$

- The maximum period, P

- (case 1) For $c \neq 0$,

$P = m$ provided that c is prime to m (greatest common divisor of c and m is 1) and the multiplier $a-1 = 4k$, where k is an integer.

- (case 2) For $m = 2^b$, and $c = 0$,

$P = m/4 = 2^{b-2}$ provided that the seed X_0 is odd and the multiplier $a = 3 + 8k$ or $a = 5 + 8k$ for some $k = 0, 1, \dots$

- (case 3) For $m = a$ prime number and $c = 0$,

$P = m-1$ provided that the multiplier, a , has the property that the smallest integer k , such that $a^k - 1$ is divisible by m , is $k = m - 1$,

➤ Multiplicative Congruential Generator

$$X_i = aX_{i-1} \pmod{m}, \text{ where } m > 0 \text{ and } a > 0$$

$$R_i = X_i/m$$

- Can not have full period ($P=m$), but can have $P = m-1 = 2^b-1$

➤ Additive Congruential Generator

$$X_i = (X_{i-1} + X_{i-k}) \pmod{m}, \quad i = 1, 2, \dots$$

$$R_i = X_i/m$$

- With consecutive numbers ($k=2$) R_{n-2} , R_{n-1} , and R_n , it will never happen that $R_{n-2} < R_n < R_{n-1}$ or $R_{n-1} < R_n < R_{n-2}$, which occurs by $1/6$ for true uniform variables.

➤ Choosing the initial seed

- e.g., time (wall-clock and since boot),

➤ *Linear Congruential Generator (cont.)*

$$X_i = (a X_{i-1} + c) \bmod m, \text{ where } a \geq 0 \text{ and } m \geq 0$$

$$R_i = X_i / m$$

- *Examples*

- For $(a, c, m) = (1, 5, 13)$ and $z_0 = 1$, we get the sequence 1, 6, 11, 3, 8, 0, 5, 10, 2, 7, 12, 4, 9, 1, which has full period of 13. (case 1)
- For $(a, c, m) = (2, 5, 13)$ and $z_0 = 1$, we get the sequence 1, 7, 6, 4, 0, 5, 2, 9, 10, 12, 3, 11, 1, which has a period of 12. With $z_0 = 8$, we get the sequence 8, 8, 8, (period of 1).

➤ *Linear Congruential Generator (cont.)*

$$X_i = (a X_{i-1} + c) \bmod m, \text{ where } a \geq 0 \text{ and } m \geq 0$$

$$R_i = X_i / m$$

- *Examples*

Using the multiplicative congruential method, find the period of the generator for $a = 13$, $m = 2^6$, $c=0$ (case 2) and $X_0 = 1, 2, 3$, and 4 . The solution is given in next slide. When the seed is 1 and 3 , the sequence has period 16 . However, a period of length eight is achieved when the seed is 2 ; and a period of length four occurs when the seed is 4 .

- *Example results.*

i	X_i	X_i	X_i	X_i
0	1	2	3	4
1	13	26	39	52
2	41	18	59	36
3	21	42	63	20
4	17	34	51	4
5	29	58	23	
6	57	50	43	
7	37	10	47	
8	33	2	35	
9	45		7	
10	9		27	
11	53		31	
12	49		19	
13	61		55	
14	25		11	
15	5		15	
16	1		3	