Random Number Generator
Chapter 7

- In simulations, we generate random values for variables with a specified distribution
- Ex., model service times using the exponential distribution
- Generation of random values is a two step process

  Random number generation: Generate random numbers uniformly distributed between 0 and 1

  Random variate generation: Transform the random numbers generated above to obtain numbers satisfying the desired distribution

Sources of Randomness for Common Simulation Applications

Type of system	Sources of randomness
Manufacturing	Processing times, machine times to failure, machine repair times
Defense-related	Arrival times and payloads of missiles or airplanes, outcome of an engagement
Communications	Interarrival times of messages, message types, message lengths
Transportation	Ship-loading times, interarrival times of customers to a subway

Random Numbers

- True Random Numbers
- Pseudo random numbers
- Quasi random numbers

True Random Numbers

- The most desirable random numbers
- Generated only from physical experiment
- EX: - Ten sided die
  - Throwing a coin assuming 1 for head (0 for tail)
  - Recording the times the customers arrive
  - Physical devices “ Geiger counter”, recording the interval between the decay of a radioactive material

Disadvantages of True Random Numbers

- Slow
- Inconvenient
- Expensive to build
- Not reproducible

Pseudo Random Numbers

- Algorithms can automatically create long runs (for example, millions of numbers long) of random numbers with good random properties but eventually the sequence repeats.
- determine the next random number as a function of the previously generated random number (i.e., recursive calculations are applied)
- Random numbers generated, are therefore, deterministic. That is, sequence of random numbers is known given the starting seed.
- Random number generators have a cycle length (or period) that is measured by the count of unique numbers generated before the cycle repeats itself.

Pseudo Random Numbers

- Most computer programming languages include functions or library routines that surport random number generators.
- Such library functions often have poor statistical properties and some will repeat patterns after only tens of thousands of trials. These functions may provide enough randomness for certain tasks but are unsuitable where high-quality randomness is required, such as in cryptographic applications, statistics or numerical analysis.

Advantages of Pseudo Random Numbers

- Uniformly distributed between 0, 1
- Satisfiably independent: produce output satisfying statistical tests of randomness
- Reproducible: ability to reproduce random number stream if necessary
- Not repeated for a long desired length
- Generated fast
- Does not need big memory to store: easy to move random number generator to a new machine

❖ Form clusters and empty regions in higher dimensions

Quasi Random Numbers

- Also Called low discrepancy sequences
- Discrepancy of a sequence is a measure of its uniformity
- Computed by comparing the actual numbers of points in multidimensional space to the number assuming full uniform distribution
- Not random at all.
- Yet, Uniformly fill the space

Why is this Important?

- Validity
  - The simulation model may not be valid due to cycles and dependencies in the model
- Precision
  - You can improve the output analysis by carefully choosing the random numbers

Von Neuman Midsquare method 1940

- Let m = the number of digits requires after the decimal pt
- Start with a seed
- Square the seed
- Consider only the m middle digits
- EX: m = 2 , seed = 23
- Halt when you get 0 or

equal numbers

Generated numbers

.23 , .52,.70,.90,.10

0 52 9

2 70 4

4 90 0

8 10 0

0 10 0

Linear Congruential Generator

- Producing a sequence of integers, x_0, x_1, x_2, … between *0 and m-1 by following a recursive* relationship:

$$X_{i+1} = (a\,X_i + c) \bmod m \qquad i = 0,1,2,\ldots$$

- The selection of the values for *a, c, m, and* X_0 affects the statistical properties and the cycle length.
- The random integers are being generated [*0,m-1],*
  and to convert the integers to random numbers:
- $R_i = X_i/m$, $i = 1,2,\ldots$
- Halt when a number is repeated

LCG Ex.

- Use X_0 *= 27, a = 17, c = 43, and m = 100.*

$$X_{i+1} = (a\, X_i + c) \bmod m$$

The X_i *and* R_i *values are:*

- X_1 *= (17*27+43) mod 100*

  = 502 mod 100 = 2, R_1 *= 0.02;*
- X_2 *= (17*2+32) mod 100 = 77,* R_2 *= 0.77;*
- X_3 *= (17*77+32) mod 100 = 52,* R_3 *= 0.52;*
- *…*

LCG

Remarks:

- c = 0, the generator is called Multiplicative LCG.
- If c ≠ 0, the generator is called Mixed LCG.
- The length of the cycle is called its Period, can be at most?
- m should be chosen to be big
- Choose m of the form 2^k for efficient computation

LCG

Remarks:

- c = 0, the generator is called Multiplicative LCG.
- If $c \neq 0$, the generator is called Mixed LCG.
- The length of the cycle is called its Period, can be at most m-1
- m should be chosen to be big
- Choose m of the form 2^k for efficient computation

LCG

Theorem:

If $c \neq 0$, LCG has full period

iff

- Integers *m* and *c* are relatively prime (the only positive integer that divides both *m* and c is 1)
- Every prime number that is a factor of *m* is also a factor of a-1
- If integer *m* is a multiple of 4, a-1 is also a multiple of 4