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

2

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

0 52 9
2 70 4
4 90 0
8 10 0
0 10 0

Generated numbers
.23 , .52,.70,.90,.10

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,…
- 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 ≠ 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 ≠ 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

Multiplicative Congruential Generator

- If c= 0, $X_{i+1}= (a X_i) \bmod m$ i =0,1,2,…
- Break the first condition of the thm. i.e. Not full period
- Its max period is 2^{b-1} where b is the # of digits (size of ward)
- Advantages:

Faster, Simpler, easy to implement

Linear Congruential Generator

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

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

- 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,…
- 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 = 66,* R_2 *= 0.66;*
- X_3 *= (17*66+32) mod 100 =,* R_3 *= 0.;*
- …

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 ≠ 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 ≠ 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

Multiplicative Congruential Generator

- If c= 0, $X_{i+1}= (a X_i) \bmod m$ i =0,1,2,…
- Break the first condition of the thm. i.e. Not full period
- Its max period is 2^{b-1} where b is the # of digits (size of ward)
- Advantages:

Faster, Simpler, easy to implement

Seed Selection

- Often we need random numbers for more than one variable in a simulation
- E.g., inter-arrival times, service times
- Then, we need to use multiple random number streams such that we do not introduce correlations between the two random variables owing to our choice of random numbers

Seed Selection

For a good selection of seeds:

- Do not use zero
- Avoid even values
- Use a separate seed for a separate stream such that random numbers do not overlap
- Do not use random seeds because they are hard to replicate

Need to test

- The above only tells us how to create RNs from RNG that will have a large period
- It does not guarantee the RNG output will be "random" (e.g., $x_{i+1} = (x_i + 1) \bmod m$ not random!)
- Need to apply statistical tests to validate that the RNG gives acceptably random results

Testing Random Number Generators

- Two categories of test
  - Test for uniformity …
  - Test for independence
- Passing a test is only a necessary condition and not a sufficient condition
  - i.e., if a generator fails a test it implies it is bad
  - but if a generator passes a test it does not necessarily imply it is good.

Testing Distributions

- Comparing Distributions: Tests for Goodness-of-Fit

Know how to compare between two distributions

  - Chi-Square Distribution (for discrete models)
  - Kolmogorov-Smirnov (K-S) Test (for continuous models)

Goodness-of-fit

- Statistical Tests enable us to compare between two distributions, also known as **Goodness-of-Fit**.
- The **goodness-of-fit** of a statistical model describes how well it fits a set of observations.
- Measures of goodness of fit typically summarize the discrepancy between observed values and the values expected under the model in question
- Goodness-of-fit means how well a statistical model fits a set of observations

(PEARSON'S) CHI-SQUARE TESTS FOR DISCRETE MODELS

The Pearson's chi-square test is to compare two probability mass functions of two distribution.

If the difference value (Error) is **greater** than the critical value, the two distribution are said to be different or the first distribution does not fit (well) the second distribution.

If the difference if **smaller** than the critical value, the first distribution fits well the second distribution

(Pearson's) Chi-Square test

- Pearson's chi-square is used to assess two types of comparison:
  - tests of goodness of fit: it establishes whether or not an observed frequency distribution differs from a theoretical distribution.
  - tests of independence. it assesses whether paired observations on two variables are independent of each other.

Steps in Test of Hypothesis

1. Determine the appropriate test
2. Establish the level of significance: α
3. Formulate the statistical hypothesis
   H_o : The two variables are independent
   H_1 : The two variables are not independent
4. Calculate the test statistic
5. Determine the degree of freedom
6. Compare computed test statistic against the critical value (from the table of the test)

- The critical tabled values are based on sampling distributions of the Pearson chi-square statistic
- If calculated χ^2 is greater than χ^2 table value, reject H_o

32

Testing

- Testing is not necessary if a well-known simulation package is used or if a well tested

  generator is used
- we focus on “empirical” tests, that is tests that are applied to an actual sequence of random numbers
- EX:

Chi-Square Test

Chi-Square Test

- Test is designed for discrete distributions and large sample sizes only. For continuous distributions, Chi-Square test is only an approximation (i.e. level of significance holds only for n).

$$\chi^2 = \sum \frac{(obs - \exp)^2}{\exp}$$

- *obs* is the observed data and *exp* is the expected frequency of the *i*th cell, *i=1,2,…k* cells.
- Compute the Chi-Square distribution with (k-1) degrees of freedom

Observed values

$R :=$

0.34	0.90	0.25	0.89	0.87	0.44	0.12	0.21	0.46	0.67
0.83	0.76	0.79	0.64	0.70	0.81	0.94	0.74	0.22	0.74
0.96	0.99	0.77	0.67	0.56	0.41	0.52	0.73	0.99	0.02
0.47	0.30	0.17	0.82	0.56	0.05	0.45	0.31	0.78	0.05
0.79	0.71	0.23	0.19	0.82	0.93	0.65	0.37	0.39	0.42
0.99	0.17	0.99	0.46	0.05	0.66	0.10	0.42	0.18	0.49
0.37	0.51	0.54	0.01	0.81	0.28	0.69	0.34	0.75	0.49
0.72	0.43	0.56	0.97	0.30	0.94	0.96	0.58	0.73	0.05
0.06	0.39	0.84	0.24	0.40	0.64	0.40	0.19	0.79	0.62
0.18	0.26	0.97	0.88	0.64	0.47	0.60	0.11	0.29	0.78

Uniform distribution in [0 .. 9]

Compute terms:

Observed: Expected: Difference: Difference^2: Normalized:

$O =$

	0
0	8
1	8
2	10
3	9
4	12
5	8
6	10
7	14
8	10
9	11

$E =$

	0
0	10
1	10
2	10
3	10
4	10
5	10
6	10
7	10
8	10
9	10

$O - E =$

	0
0	-2
1	-2
2	0
3	-1
4	2
5	-2
6	0
7	4
8	0
9	1

$(O - E)^2 =$

	0
0	4
1	4
2	0
3	1
4	4
5	4
6	0
7	16
8	0
9	1

$T =$

	0
0	0.4
1	0.4
2	0
3	0.1
4	0.4
5	0.4
6	0
7	1.6
8	0
9	0.1

$$\chi 2 := \sum_{i=0}^{9} \frac{(O_i - E_i)^2}{E_i}$$

$\chi 2 = 3.4$

$\chi^2_{0.05,9} = 16.9$

$$T_i := \frac{(O_i - E_i)^2}{E_i}$$

Chi-Square Table

Critical Values of the χ^2 Distribution

df \ p	0.995	0.975	0.9	0.5	0.1	0.05	0.025	0.01	0.005	df
1	.000	.000	0.016	0.455	2.706	3.841	5.024	6.635	7.879	1
2	0.010	0.051	0.211	1.386	4.605	5.991	7.378	9.210	10.597	2
3	0.072	0.216	0.584	2.366	6.251	7.815	9.348	11.345	12.838	3
4	0.207	0.484	1.064	3.357	7.779	9.488	11.143	13.277	14.860	4
5	0.412	0.831	1.610	4.351	9.236	11.070	12.832	15.086	16.750	5
6	0.676	1.237	2.204	5.348	10.645	12.592	14.449	16.812	18.548	6
7	0.989	1.690	2.833	6.346	12.017	14.067	16.013	18.475	20.278	7
8	1.344	2.180	3.490	7.344	13.362	15.507	17.535	20.090	21.955	8
9	1.735	2.700	4.168	8.343	14.684	16.919	19.023	21.666	23.589	9
10	2.156	3.247	4.865	9.342	15.987	18.307	20.483	23.209	25.188	10
11	2.603	3.816	5.578	10.341	17.275	19.675	21.920	24.725	26.757	11
12	3.074	4.404	6.304	11.340	18.549	21.026	23.337	26.217	28.300	12
13	3.565	5.009	7.042	12.340	19.812	22.362	24.736	27.688	29.819	13
14	4.075	5.629	7.790	13.339	21.064	23.685	26.119	29.141	31.319	14
15	4.601	6.262	8.547	14.339	22.307	24.996	27.488	30.578	32.801	15

EX.

.34	.9	.25	.89	.87	.44	.12	.21	.46	.67
.83	.76	.79	.64	.7	.81	.94	.74	.22	.74
.96	.99	.77	.67	.56	.41	.52	.73	.99	.02
.47	.3	.17	.82	.56	.05	.45	.31	.78	.05
.79	.71	.23	.19	.82	.93	.65	.37	.39	.42
.99	.17	.99	.46	.05	.66	.1	.42	.18	.49
.37	.51	.54	.01	.81	.28	.69	.34	.75	.49
.72	.43	.56	.97	.3	.94	.96	.58	.73	.05
.06	.39	.84	.24	.4	.64	.4	.19	.79	.62
.18	.26	.97	.88	.64	.47	.6	.11	.29	.78