Random Number Generators

3/2/2009

Opening Discussion

- Midterm results.

Random Number Generators

- For obvious reasons we need good random numbers for our simulations.
- Text has some interesting history on getting random numbers, much of it prior to the use of computers.
- Use of the term random number isn't quite right. Author doesn't like pseudo-random.
- Really care about the properties of the sequence.

Properties of Good Random

- There are several properties we want from a random number generator. We are always talking about something that generates U(0,1).
  - Uniformly distributed and apparently uncorrelated.
  - Fast and small storage.
  - Reproducible.
  - Have ability to pull from separate streams.
  - Portable.

Linear Congruential Generators

$$Z_i = (aZ_{i-1} + c)(\mathrm{mod}\, m)$$
$$U_i = Z_i / m$$
$$0 < m, a < m, c < m, Z_0 < m$$

- Will eventually repeat. Length is called period. Optimally it takes m steps, but won't in all cases.

Requirements

- A LCG will have full period if:
  - m and c are relatively prime (only common divisor is 1)
  - If q is a prime number that divides m, the q divides a-1.
  - If 4 divides m, then 4 divides a-1.
- Mixed generators set m=2^b, c is odd, and a is divisible for 4. Make b the size of numbers on the machine.

Other Generators

- General Congruence generators
  - $Z_i=g(Z_{i-1},Z_{i-2},...)(\text{mod } m)$
- Composite Generators combine results from 2+ generators.
  - Shufflers use output of one as input to another.
  - Can use difference of two sequences.
- Feedback shift generators
  - Operate on the bits of a number.

Minute Essay

- ???