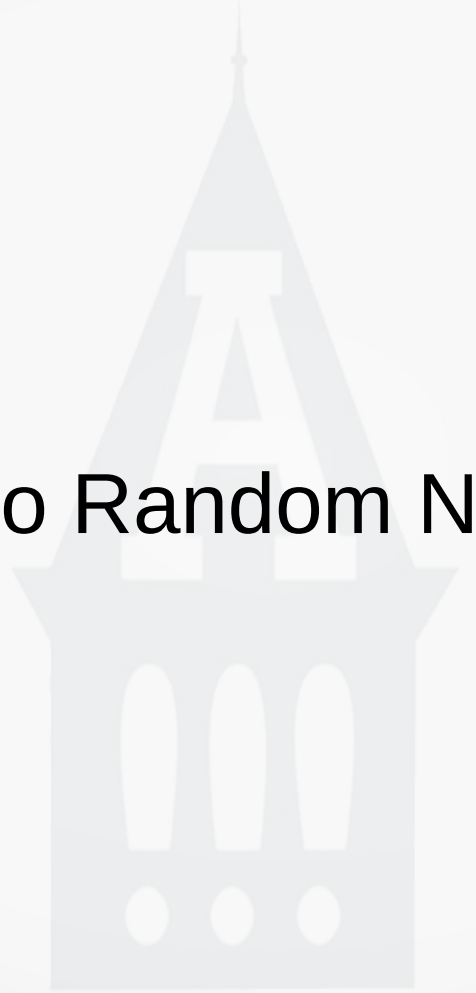
CS 5410

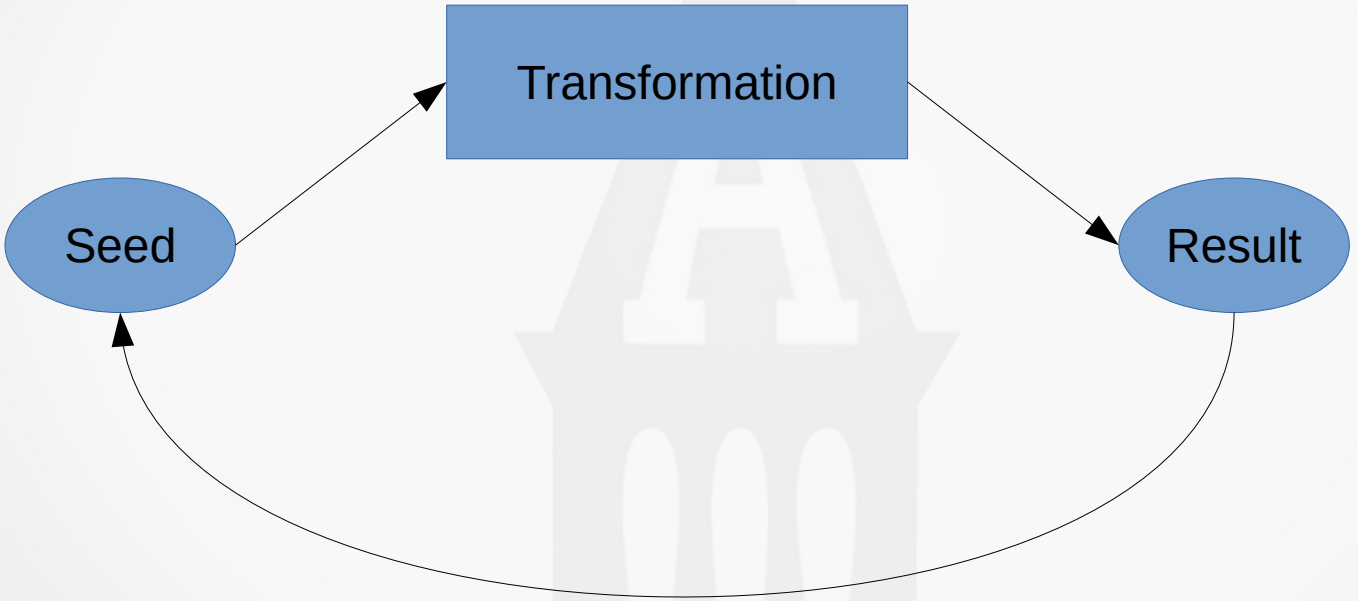


Intro to Random Numbers

Generating Random Numbers

- True Random Number: www.random.org
- Pseudo Random Number Generator (PRNG)
  - Linear Congruential Generator (LCG)
    - https://en.wikipedia.org/wiki/Linear_congruential_generator
  - Mersenne Twister (MT)
    - https://en.wikipedia.org/wiki/Mersenne_Twister
  - XorShift
    - https://en.wikipedia.org/wiki/Xorshift
  - PCG Family
    - http://www.pcg-random.org/
- Tests of Randomness
  - https://en.wikipedia.org/wiki/Randomness_tests
- Very good analysis of random number techniques & performance
  - https://www.pcg-random.org/posts/bounded-rands.html
  - https://www.pcg-random.org/

Generating Random Numbers



Simple Example - LCG

$$X_{n+1} = (aX_n + c) \bmod m$$

- X_0 is the initial “seed”
- X_n is the previous result
- X_{n+1} is the next result
- If c = 0
  - (or) m may be prime
  - (or) m may be power of 2
- a – 1 should be divisible by m’s prime factors; if m is not prime
- c and m should be coprime
  - coprime : Have no common factors other than 1
  - e.g., 21 and 22 are coprime
    - factors for 21 are : 1, 3, 7, 21
    - factors for 22 are : 1, 2, 11, 22

Example RNG Results

Random Numbers - Misc

- Multi-Threading (The Biggest Bug!)

Random Numbers - Misc

- Multi-Threading (The Biggest Bug!)
- Distributed

Random Numbers - Misc

- Multi-Threading (The Biggest Bug!)
- Distributed
- Replay Reproducibility

Random Numbers - Misc

- Multi-Threading (The Biggest Bug!)
- Distributed
- Replay Reproducibility
- Other Distributions
  - Over integer range
  - Gaussian distribution
  - Circle perimeter
  - Area distribution (rectangle, triangle, circle, ...)
  - others…

Random Numbers - Misc

- Multi-Threading (The Biggest Bug!)
- Distributed
- Replay Reproducibility
- Other Distributions
  - Over integer range
  - Gaussian distribution
  - Circle perimeter
  - Area distribution (rectangle, triangle, circle, ...)
  - others…
- Pre-compute, store in memory

More Misc

- Custom Distribution
  - [1: 20, 2: 10, 3: 5, 4: 1] – 36 numbers
    - Generate rnd [1 to 36], pick accordingly

More Misc

- Custom Distribution
  - [1: 20, 2: 10, 3: 5, 4: 1] – 36 numbers
    - Generate rnd [1 to 36], pick accordingly
- Replacement
  - With – Put number back in
  - Without – Don’t put number back in