Random number generation

Goldsmiths Computing

January 13, 2019

Motivation

Random numbers needed for

- simulations
- games
- statistical software
- randomized algorithms

Definition

A random number is a number generated by some unpredictable process

- but: Laplace's demon

Pseudorandom Numbers

A pseudorandom number is a number generated by some process which is predictable and deterministic, but whose parameters are unknown
A pseudorandom number generator is an object which can generate a (long) sequence of pseudorandom numbers.

Operations

next! return the next random number from the generator (and update the generator's state)

seed![o] set the random number generator's state to something reproducible from the object o

Linear Congruential Generators

- single word of state, X
- generate the next pseudorandom number by computing $aX + c \bmod m$
- update the state to the new pseudorandom number

Example

LCG$_{256}$(29,35): $29X + 35 \bmod 256$

- 64, 99, 90, 85, 196, 87, 254, 233, 136, 139
- 93, 172, 159, 38, 113, 240, 83, 138, 197, 116
- 122, 245, 228, 247, 30, 137, 168, 43, 2, 93

Requirements

For full period of length m:

- m and c must be relatively prime
- $a - 1$ must be divisible by all prime factors of m
- $a - 1$ must be divisible by 4 if m is divisible by 4

(Hull-Dobel Theorem)

Problems with Linear Congruential Generators

- low period of some bits
  - *e.g.* in $29X + 35 \bmod 256$, sequence alternates odd/even
- serial correlations
  - choosing points in (2D-/3D-)space by generating successive random numbers severely restricts possibilities
- predictability
  - knowing m, can deduce a and c with only three successive random numbers

Take home message:

Do not use Linear Congruential Generators

- C `rand`
- C++ `minstd_rand`
- Java `java.util.Random`
- Javascript `Math.random`

(unless you know what you're doing)

Alternative random number generators

Mersenne Twister 19937

- period 2^{19937}-1; 19937 state bits
- (not cryptographically secure)
- (pathological zero states)

xorshift, xoroshiro

- period 2^{128}-1; up to 128 bits of state;
- fast, non-correlated outputs
- (not cryptographically secure)
- (lowest bit linear-feedback weakness)

ISAAC, arc4random

- based on RC4, cryptographically secure

Work

1. Reading
   - CLRS, chapter 5
   - TIFU by using Math.random()
   - Dual EC: A Standardized Back Door