How (Pseudo)Random is this?

Some Random Advice

Perrin Westrich

Outline

- What is Random?
- Pseudo Random
- Pseudo Random Number Generators(PRNG)
- PRNG Quality

Outline

- Types of PRNGs
- Diehard Battery of Tests of Randomness
- Analysis
- Results

Random Sequence

- No deterministic pattern
- Probability distribution
- Water balloons!

Pseudo Random

- Computers are deterministic
- Approximation of random
- Pseudo Random Number Generator (PRNG)

PRNG

- Uniform distribution
- Initialization
- Period

PRNG Examples

- Linear Congruential Generator (LCG)

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

- Inversive Generator

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

- Mersenne Twister

PRNG Quality

- Unpredictability
- Long Period
- Stands up to Statistical attacks

Diehard Battery of Tests of Randomness

- Overlapping Permutations
- Birthday Spacings
- Craps Tests

Analysis

- C/C++ Standard PRNG (LCG): Failed
- Inversive Generator: Passed Majority
- Mersenne Twister: Passed Majority

Conclusion

- Use built in if quality is not an issue
- Inversive Generator not particularly good
- Mersenne Twister quick, and high quality

Summary

- Definitions
- Types of PRNGs
- Diehard
- Analysis/Results

References

- Diehard
- Diehard Program. George Marsaglia
- Diehard_Tests
- http://en.wikipedia.org/wiki/Diehard_tests
- GCD_Test
- http://www.jstatsoft.org/v07/i03/paper
- MT_Marsaglia
- http://groups.google.com/group/sci.crypt/browse_thread/thread/305c507efbe85be4
- LCG
- http://en.wikipedia.org/wiki/Linear_congruential_generator
- Randomness
- http://en.wikipedia.org/wiki/Randomness
- PRNG
- http://en.wikipedia.org/wiki/Pseudo-random_number_generator
- RANDU
- http://en.wikipedia.org/wiki/RANDU
- MT
- http://en.wikipedia.org/wiki/Mersenne_twister