Computer Generated Pseudo-Random Number Sequences

James A. Foster

September 17, 1997

List of Slides

Outline

1. Uses of PRNG sequences
2. PRNG algorithms
3. PRNG quality

Uses

- Unbiased choices: jury summons, IRS audits, lottery, games
- Statistical sampling of databases: census, polls
- Better algorithms
- Simulations

Simulation Examples

- Climate simulations: global warming, weather prediction
- City planning: demographics, traffic
- Epidemiology
- Marketing
- Viral evolution
- Simulating evolution to solve engineering problems

Better algorithms

- Primality testing (cryptography)
- Electing leaders (networking)
- Matching
- Optimization (hill-climbing)
- Sorting
- Evolutionary computing

PRNG Desiderata

- Lots of numbers (long *period*)
- (almost) no patterns
- Repeatable sequences
- Easy to compute
- Matches statistical predictions

Note: true randomness does not meet these!

Linear congruential

Formula:

$$n_{next} = (f \cdot n_{prev} + a) \pmod{m}$$

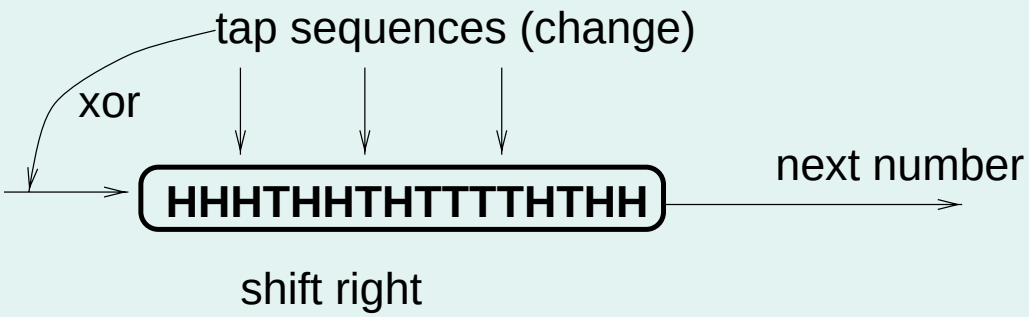
Bad choices: seed=1, f=5, a=7, m=15 (period=2)

$n_0 = ((5 \cdot 1) + 7) mod 15 = 12$, $n_1 = ((5 \cdot 12) + 7) mod 15 = 7$,
$n_2 = ((5 \cdot 7) + 7) mod 15 = 12$, etc.

Better: seed=1, f=2, a=7, m=15 (period=4)

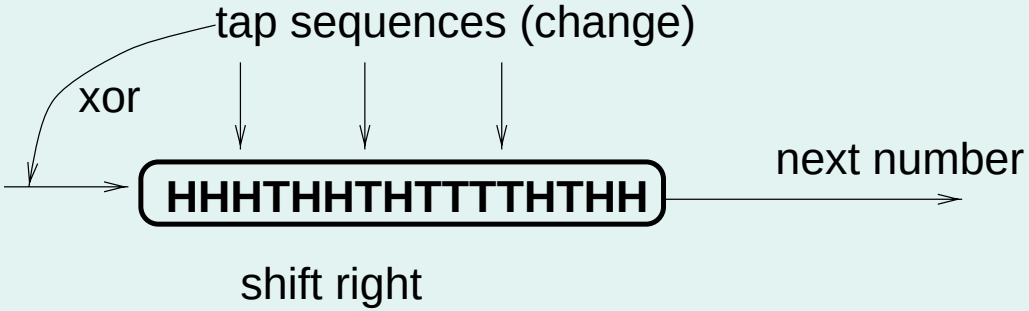
$n_0 = ((2 \cdot 1) + 7) mod 15 = 9$, $n_1 = ((2 \cdot 9) + 7) mod 15 = 10$,
$n_1 = ((2 \cdot 10) + 7) mod 15 = 12$, $n_1 = ((2 \cdot 12) + 7) mod 15 = 1$,
$n_1 = ((2 \cdot 1) + 7) mod 15 = 9$, etc.

Feedback shift register



1. Fill the register
2. XOR tap positions
3. Push into left end
4. Return what falls out the right
5. Go back to step 2

FSR PRNG example



Register	*Outgoing*
H H H T H H T H T T T T H T H H	
H H H H T H H T H T T T T H T H	H
T H H H H T H H T H T T T T H T	H
T T H H H H T H H T H T T T T H	T

Sequence returned: H H T ...

Monsters

Do lots of strange manipulations

Testing PRNGs

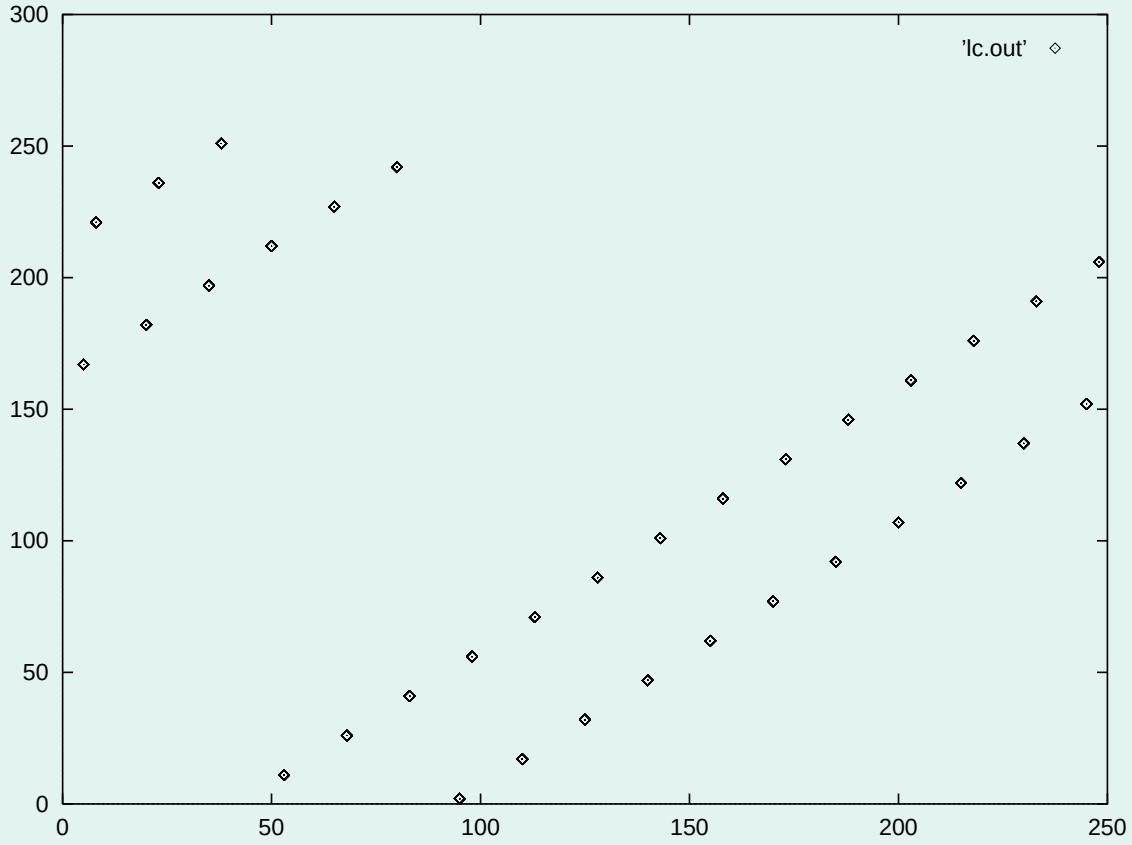
Statistical tests: compare predictions to observations, determine whether results are statistically significant (many test suites are available)

eyeballing for correlations: plot groups of random numbers, look for patterns

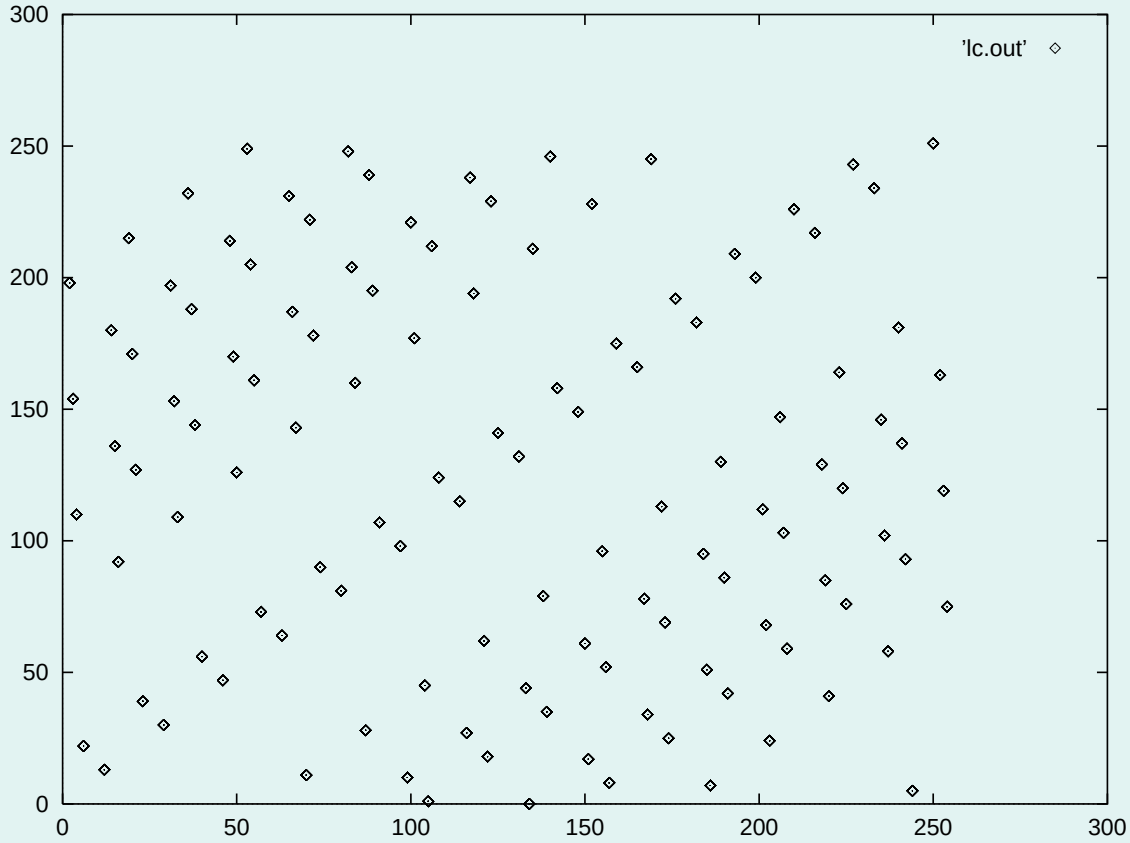
Measure their period (and sensitivity to the seed)

Note: algorithm quality may depend *strongly* on quality of PRNG

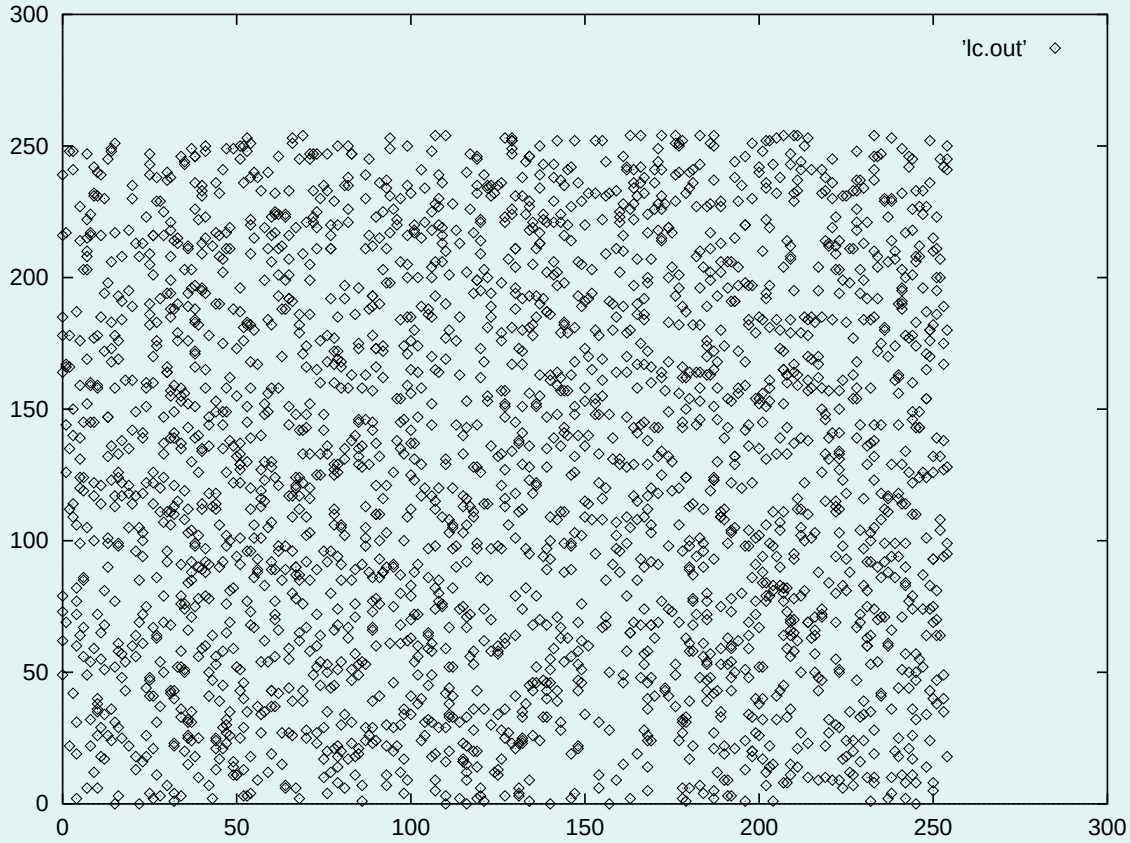
Bad parameters: f=18, a=77, m=255, seed=1, number-of-outputs=5000



Slightly better parameters: f=211, a=31, m=255, seed=1, number-of-outputs=5000



Much better: (using system defaults for rand(), and m=255, seed=1)



Summary

(fast) Algorithms exist for generating (good, long) pseudo-random number sequences

We can measure PRNG quality

PRNG sequences can be useful (or misleading)