Pseudo-random number generators

Eduarda T. C. Chagas, Alejandro C. Frery

July 28, 2020

Multiply-with-carry (MWC) PRNG

Multiply-with-carry (MWC) PRNG Marsaglia (1994) generated by the following expressions:

$$X_n = \mod \{aX_{n-1} + \text{carry}_{n-1}; 2^{32}\},$$
$$\text{carry}_n = \text{floor}\left(\frac{X_n}{2^{32}}\right).$$

The initial condition is random.

Mother

The generator identified as Mother Marsaglia (1994) given by:

$$X_n = \mod \{2111111111X_{n-4} + 1492X_{n-3} + 17776X_{n-2} + 5115X_{n-1} + \text{carry}_{n-1}; 2^{32}\},$$
$$\text{carry}_n = \text{floor}\left(\frac{X_n}{2^{32}}\right).$$

The initial condition is random.

Lehmer

Lehmer's algorithm Payne et al. (1969) for random number generation is defined in terms of two fixed parameters:

- modulus m, a fixed large prime integer,
- multiplier a, a fixed integer in $\mathcal{X}_m$.

The integer sequence $\{x_0, x_1, \dots\}$ is defined by the iterative equation:

$$x_{i+1} = a_x \mod m$$

$x_0 \in \mathcal{X}_m$ is called the initial seed.

References

Marsaglia, G. (1994), 'Yet another rng', *Posted to the electronic billboard sci. stat. math, August* **1**.

Payne, W., Rabung, J. R. & Bogyo, T. (1969), 'Coding the lehmer pseudo-random number generator', *Communications of the ACM* **12**(2), 85–86.