# Chapter 25 Uniform Random Number Generation With Jumping Facilities

E. Jack Chen BASF Corporation, USA

# ABSTRACT

A facility for generating sequences of pseudorandom numbers is a fundamental part of computer simulation systems. Furthermore, multiple independent streams of random numbers are often required in simulation studies, for instance, to facilitate synchronization for variance-reduction purposes, and for making independent replications. A portable set of software utilities is described for uniform random-number generation. It provides for multiple generators (streams) running simultaneously, and each generator (stream) has its sequence of numbers partitioned into many long disjoint contiguous substreams. Simple procedure calls allow the user to make any generator "jump" ahead/back v steps (random numbers). Implementation issues are discussed. An efficient and portable code is also provided to implement the package. The basic underlying generator CMRG (combined multiple recursive generator) combines two multiple recursive random number generators with a period length of approximately  $2^{191}$  ( $\approx 3.1 \times 10^{57}$ ), good speed, and excellent theoretical properties.

## INTRODUCTION

As computer capacities and simulation technologies advance, simulation has become the method of choice for modeling and analysis. The fundamental advantage of simulation is that it can tolerate far less restrictive modeling assumptions, leading to an underlying model that is more reflective of reality and thus more valid, leading to better decisions (Lucas et al. 2015). Simulation studies are typically proceed by transforming in a more or less complicated way of a sequence of numbers between 0 and 1 produced by a pseudorandom generator into an observations of the measure of interest. A facility for generating sequences of pseudorandom numbers is a fundamental part of computer simulation systems. Furthermore, random number generators also play an important role in cryptography. A collection of random

DOI: 10.4018/978-1-5225-7368-5.ch025

variables  $x_1, x_2, ..., x_n$  is a random sample if they are independent and identically distributed. True random numbers cannot be produced by a deterministic algorithm, and hence, random numbers generated by using a recursive equation are referred to as pseudorandom numbers. The deterministic nature of these techniques is important because it can be reproduced in computations. A facility for generating sequences of pseudorandom numbers is a fundamental part of computer simulation systems. Usually, in practice, such a facility produces a deterministic sequence of values, but externally these values should appear to be drawn independently from a uniform distribution between 0 and 1, i.e., they are independent and statistically indistinguishable from a truly random sequence. Furthermore, multiple independent streams of random numbers are often required in simulation studies, for instance, to facilitate synchronization for variance-reduction purposes, and for making independent replications.

A random number generator (RNG) is an algorithm that starting from an initial seed (or seeds), produces a stream of numbers that behaves as if it were a random sample when analyzed using statistical tests. The RNG is closely related to the Deterministic Random Bit Generators (DRBGs). See L'Ecuyer (1990, 2013) and references therein for more information on RNGs. We describe a portable set of software utilities for uniform random-number generation. It provides for multiple generators (streams) running simultaneously, and each generator (stream) has its sequence of numbers partitioned into many long disjoint contiguous substreams, see L'Ecuyer et al. (2002). Simple procedure calls allow the user to make any generator "jump" ahead/back v steps (random numbers). Implementation issues are discussed. The basic underlying generator CMRG (Combined Multiple Recursive Generator) combines two multiple recursive random number generators with a period length of approximately  $2^{191} (\approx 3.1 \times 10^{57})$ , good speed, and excellent theoretical properties, e.g., the lattice structure, see Kroese et al. (2011) for a list of desired properties.

#### BACKGROUND

There are a number of methods for generating the random numbers, of which the most popular are the congruential methods (mixed, multiplicative, and additive). The (mixed) linear congruential generators (LCGs) are defined by

$$x_{i} = (ax_{i-1} + c)MOD \ m, \ u_{i} = \frac{x_{i}}{m}, x_{0} \in \{1, \dots, m-1\} \ i > 0.$$

where *m* (the modulus) is a positive integer (usually a very large primary number), *a* (the multiplier)  $\in \{1, ..., m-1\}$  and *c* (the increment) is a nonnegative integer. This mathematical notation signifies that  $x_i$  is the remainder of  $(ax_{i-1}+c)$  divided by *m*. Hence,  $x_i \in \{1, ..., m-1\}$ . Thus, random variable  $u_i$  is a uniform 0, 1 variable. Note that

$$x_{i+v} = \left(a^v x_i + rac{c\left(a^v - 1
ight)}{a-1}
ight) \mathrm{MOD} \ m \ .$$

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/uniform-random-number-generation-withjumping-facilities/213139

# **Related Content**

#### Electronic Payment Adoption in the Banking Sector of Low-Income Countries

Teshome Alemu, Tridib Bandyopadhyayand Solomon Negash (2018). *Technology Adoption and Social Issues: Concepts, Methodologies, Tools, and Applications (pp. 1042-1063).* www.irma-international.org/chapter/electronic-payment-adoption-in-the-banking-sector-of-low-income-countries/196717

## Active Citizens in a New Communication Society: WWW, Back to the Future! Examples to Aware Projects

(2024). Considerations on Cyber Behavior and Mass Technology in Modern Society (pp. 222-247). www.irma-international.org/chapter/active-citizens-in-a-new-communication-society/338257

#### Sixth Sense Technology: Exploring Future Opportunities in Human Computer Interaction

Zeenat S. AlKassimand Nader Mohamed (2016). *Handbook of Research on Human-Computer Interfaces, Developments, and Applications (pp. 188-215).* www.irma-international.org/chapter/sixth-sense-technology/158872

# Hand Gesture Recognition as Means for Mobile Human Computer Interaction in Adverse Working Environments

Jens Ziegler, Randy Döring, Johannes Pfefferand Leon Urbas (2014). *Emerging Research and Trends in Interactivity and the Human-Computer Interface (pp. 331-352).* 

www.irma-international.org/chapter/hand-gesture-recognition-as-means-for-mobile-human-computer-interaction-inadverse-working-environments/87052

# Comparing Bishop Score and Transvaginal Ultrasonographic Cervical Factors to Predict Labor Induction

Bahulekar Ashitoshand R. P. Patange (2023). Advances in Artificial and Human Intelligence in the Modern Era (pp. 286-296).

www.irma-international.org/chapter/comparing-bishop-score-and-transvaginal-ultrasonographic-cervical-factors-topredict-labor-induction/330412