

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, \dots, 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

$$x_i = (ax_{i-1} + c) \text{MOD } m, \quad u_i = \frac{x_i}{m}, x_0 \in \{1, \dots, m-1\} \quad i > 0.$$

where m (the modulus) is a positive integer (usually a very large primary number), a (the multiplier) $\in \{1, \dots, m-1\}$ 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, $x_i \in \{1, \dots, m-1\}$. Thus, random variable u_i is a uniform 0, 1 variable. Note that

$$x_{i+v} = \left(a^v x_i + \frac{c(a^v - 1)}{a - 1} \right) \text{MOD } m.$$

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-with-jumping-facilities/213139

Related Content

A Probe into the Effectiveness of Non-English Majors' SMS-Based English Idiom Acquisition in China

Jiahong Jiang (2016). *Human-Computer Interaction: Concepts, Methodologies, Tools, and Applications* (pp. 148-161).

www.irma-international.org/chapter/a-probe-into-the-effectiveness-of-non-english-majors-sms-based-english-idiom-acquisition-in-china/139034

Recognizing Value of Mobile Device for Learning

Young Park and Yongju Jung (2016). *Human-Computer Interaction: Concepts, Methodologies, Tools, and Applications* (pp. 768-784).

www.irma-international.org/chapter/recognizing-value-of-mobile-device-for-learning/139063

Non-Human Actors, Human Consequences: A Sociological Inquiry Into the Social Restructuring by Artificial Intelligence

Marta Loro and Aras Bozkurt (2026). *Rethinking Education and Agency in the Age of Human-Generative AI Interaction* (pp. 399-418).

www.irma-international.org/chapter/non-human-actors-human-consequences/392449

A Practical Setup for Projection-Based Augmented Maps

Filippo Bergamasco, Andrea Albarelli and Andrea Torsello (2014). *Advanced Research and Trends in New Technologies, Software, Human-Computer Interaction, and Communicability* (pp. 13-22).

www.irma-international.org/chapter/a-practical-setup-for-projection-based-augmented-maps/94213

Affective Computing in E-Learning Modules: Comparative Analysis With Two Activities

Mahima Maharjan, Soonja Yeom, Soo-Hyung Kim and Si Fan (2020). *Interactivity and the Future of the Human-Computer Interface* (pp. 169-189).

www.irma-international.org/chapter/affective-computing-in-e-learning-modules/250752