A 4217th-order multiple recursive random number generator with modulus $2^{31}-69$

Hui-Chin Tang [*]
K. H. Hsieh
Hwapeng Chang
Department of Industrial Engineering and Management
National Kaohsiung University of Applied Sciences
Kaohsiung 80778
Taiwan, R.O.C.

Abstract

This research conducts a computerized search for the best spectral test performance in a full period 4217th-order *multiple recursive generator* (MRG) with the modulus $2^{31}-69$. Three special forms of MRG and two types of restriction on vector of multipliers are considered in this paper. Some good MRGs are presented for the different purposes of random number users to satisfy the requirements of today's computer simulation studies.

Keywords and phrases : *Full period, multiple recursive generator, random number, spectral test.*

1. Introduction

A kth-order *multiple recursive generator* (MRG) is based on the following linear recurrence

$$X_n \equiv a_1 X_{n-1} + a_2 X_{n-2} + \ldots + a_k X_{n-k} (\bmod\ m) \quad \text{for } n > k, \tag{1}$$

where m is the modulus usually chosen to be a prime number less than the computer's word size, $a_k \neq 0$, $a_j \neq 0$ for at least one j, $1 \leq j < k$, and $X_1, X_2, \ldots, X_k$ are starting values such that at least one is nonzero. The associated characteristic polynomial is $f(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_{k-1} x - a_k$. For more details, see references [3, 5, 7].

Three key issues for devising an ideal *random number* (RN) generator are full period, randomness and efficiency. One of two time-consuming steps to check the full period is the factorization of $r = \frac{m^k-1}{m-1}$. Since it is easier to do the primality testing than to do the factorization of $r = \frac{m^k-1}{m-1}$,

[*] *E-mail*: `tang@cc.kuas.edu.tw`

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 4, pp. 393–398