Beware of Linear Congruential Generators with Multipliers of the form $a = \pm 2^q \pm 2^r$

Pierre L'Ecuyer and Richard Simard

Linear congruential random number generators with Mersenne prime modulus and multipliers of the form $a = \pm 2^q \pm 2^r$ have been proposed recently. Their main advantage is the availability of a simple and fast implementation algorithm for such multipliers. This note generalizes this algorithm, points out statistical weaknesses of these multipliers when used in a straightforward manner, and suggests in what context they could be used safely.

Categories and Subject Descriptors: G.4 [**Mathematical Software**]: Algorithm design and analysis; I.6 [**Computing Methodologies**]: Simulation and Modeling

General Terms: Algorithms, Performance

Additional Key Words and Phrases: Random number generation, linear congruential generators, correlation test

1. INTRODUCTION

Wu [1997] proposed a clever-looking way to select the parameters and implement a linear congruential generator (LCG): Take a Mersenne prime modulus m, i.e., a prime of the form $m = 2^e - 1$ (see [Knuth 1997] for more on Mersenne primes), and a multiplier of the form

$$a = \pm 2^q \pm 2^r. \tag{1}$$

The usual LCG recurrence

$$x_n = a x_{n-1} \bmod m; \qquad u_n = x_n/m, \tag{2}$$

is then easily implemented by exploiting the fact that multiplying x by 2^q modulo $2^e - 1$ is equivalent to permuting the two blocs of bits comprised of the q most significant bits and the $e - q$ least significant bits (i.e., rotating the bits). This technique can in fact be generalized to moduli of the form $m = 2^e - h$ where h is small, as explained in §2.

However, with multipliers of the form (1), the numbers of 1's in the binary representations of x_{n-1} and of x_n (i.e., their Hamming weights) are likely to be strongly dependent, for permuting two blocks of bits in x_{n-1} does not change its Hamming weight, and x_n is obtained by simply adding or subtracting two such bit-rotated versions of x_{n-1}. As it turns out, there is indeed a strong dependence and this dependence is also found between the bits of u_{n-1} and u_n. In §3, we define a test of independence between the number of 1's in the binary representations of u_{n-1} and of u_n. In §4, we show that the specific LCGs proposed by Wu [1997], which

Address: Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal, H3C 3J7, Canada, e-mail: lecuyer@iro.umontreal.ca

otherwise perform well in the spectral test, fail this independence test in a decisive way. LCGs with multipliers that have a more complicated binary representation, pass this test. Extensive experiments confirm the bad statistical properties of the multipliers of the form (1).

2. IMPLEMENTATION FOR $m = 2^e - h$ WHEN h IS SMALL

Let $m = 2^e - h$ and $0 < x < m$. To compute $y = 2^q x \bmod m$, decompose x as $x = x_0 + 2^{e-q}x_1$ where $x_0 = x \bmod 2^{e-q}$. We have

$$y \;=\; 2^q(x_0 + 2^{e-q}x_1) \bmod (2^e - h) \;=\; (2^q x_0 + h x_1) \bmod (2^e - h). \qquad (3)$$

Assume that

$$h < 2^q \qquad \text{and} \qquad h(2^q - (h+1)2^{-e+q}) < m. \qquad (4)$$

Then $2^q x_0 \le 2^e - 2^q < m$ and $hx_1 \le h(m-1)/2^{e-q} = h(2^e - h - 1)/2^{e-q} = h(2^q - (h+1)2^{-e+q}) < m$, so each of the two terms of the last expression in (3) is less than m. To compute y, compute $2^q x_0$ by shifting x_0 by q positions to the left, then add h times x_1, and subtract m if the result exceeds $m-1$. Note that if h is a power of 2, this requires no multiplication, only shifts, additions, and subtractions. To multiply x by $a = \pm 2^q \pm 2^r$, repeat the above operation with r instead of q, and add (or subtract) the results modulo m. Figure 1 gives an example of how this technique can be coded in the C language, for $m = 2^{30} - 35$ and $a = 2^{15} + 2^{13}$.

```
#define m     1073741789  /* 2^30 - 35   */
#define h     35
#define q     15
#define emq   15          /* e - q       */
#define mask1 32767       /* 2^(e-q) - 1 */
#define r     13
#define emr   17          /* e - r       */
#define mask2 131071      /* 2^(e-r) - 1 */
#define norm  1.0 / m

long x;

double axmodm () {
  unsigned long k, x0, x1;
  x0 = x & mask1;   x1 = x >> emq;
  k = (x0 << q) + h * x1;
  x0 = x & mask2;   x1 = x >> emr;
  k += (x0 << r) + h * x1;
  if (k < m) x = k;
  else if (k < m * 2) x = k - m;
  else x = k - m * 2;
  return x * norm;
  }
```

Fig. 1. Implementation of an LCG with $a = 2^{15} + 2^{13}$ and $m = 2^{30} - 35$

3. A SIMPLE INDEPENDENCE TEST

We want to test the independence between the Hamming weights of the leading bits of u_n and those of u_{n-1}, for LCGs with multipliers of the form (1). We write the binary representation of u_n as $u_n = \sum_{j=1}^{\infty} u_{n,j} 2^{-j}$ and define Y_n as the number of 1's among the first ℓ bits, $u_{n,1}, \ldots, u_{n,\ell}$, where ℓ is a constant. Under the null hypothesis $\mathcal{H}_0$: "The u_n's are i.i.d. $U(0,1)$ random variables", the Y_n's are i.i.d. binomials with parameters $(\ell, 1/2)$.

Take a large positive integer N and let $C_{i,j}$ be the number of values of n for which $(Y_{2n-1}, Y_{2n}) = (i,j)$, for $1 \le n \le N$ and $0 \le i,j \le \ell$. Under $\mathcal{H}_0$, $C_{i,j}$ has the binomial distribution with parameters $(N, p_{i,j})$ where

$$p_{i,j} = P[(Y_{2n-1}, Y_{2n}) = (i,j)] = P[Y_{2n-1} = i]P[Y_{2n} = j] = \frac{1}{2^{2\ell}} \binom{\ell}{i} \binom{\ell}{j}.$$

The standardized variable

$$Z_{i,j} = \frac{C_{i,j} - Np_{i,j}}{\sqrt{Np_{i,j}(1 - p_{i,j})}}$$

has mean 0 and variance 1, and is approximately $N(0,1)$ (standard normal) when $Np_{i,j}$ is large enough. If several of the $|Z_{i,j}|$ are larger than 5 (say), this certainly indicates that something is wrong.

For a formal test, let $\Psi = \{(i,j) : Np_{i,j} \ge 5\}$, $p_0 = 1 - \sum_{(i,j)\in\Psi} p_{i,j}$, $C_0 = N - \sum_{(i,j)\in\Psi} C_{i,j}$, and consider the chi-square test statistic

$$Q = \frac{(C_0 - Np_0)^2}{Np_0} + \sum_{(i,j)\in\Psi} \frac{(C_{i,j} - Np_{i,j})^2}{Np_{i,j}}.$$

This is a standard chi-square test where we have regrouped all the boxes for which $Np_{i,j} < 5$ into a single cell. Under $\mathcal{H}_0$, Q has approximately the chi-square distribution with $k = |\Psi|$ degrees of freedom, so we can easily compute the p-value of the test, defined as $p = P[Q > x \mid \mathcal{H}_0]$ where x is the value taken by Q. The null hypothesis is rejected when p is deemed too close to 0. (It would also be possible to base the test on the *overlapping* pairs (Y_n, Y_{n+1}), $1 \le n \le N$, in which case the results of Wegenkittl [1998] could be used to find the asymptotic distribution of Q.)

4. TEST RESULTS

We applied the above independence test, with $\ell = 30$, to the two LCGs with modulus $m = 2^{31} - 1$ proposed by Wu [1997]. The multipliers are $a = 2^{15} - 2^{10}$ and $a = -2^{16} - 2^{11}$, respectively. For comparison, we applied the same tests to the well-known LCGs with the same modulus and with multipliers $a = 16807$, 630360016, and 742938285 (see [Fishman 1996; L'Ecuyer 1998; Wu 1997] for details and references about these multipliers). We also applied the test with $\ell = 50$, to the two other LCGs with modulus $m = 2^{61} - 1$ proposed by Wu [1997]. Their multipliers are $a = 2^{30} - 2^{19}$ and $a = 2^{42} - 2^{31}$.

Figures 2 to 5 give pictorial representations of the $Z_{i,j}$'s for four of these LCGs, with $\ell = 30$ and sample size $N = 2^{20}$ for the first three, whose modulus is $m = 2^{31} - 1$, and with $\ell = 50$ and sample size $N = 2^{26}$ for the last one, whose modulus is $m = 2^{61} - 1$. Each little square in the picture represents one pair (i,j). White

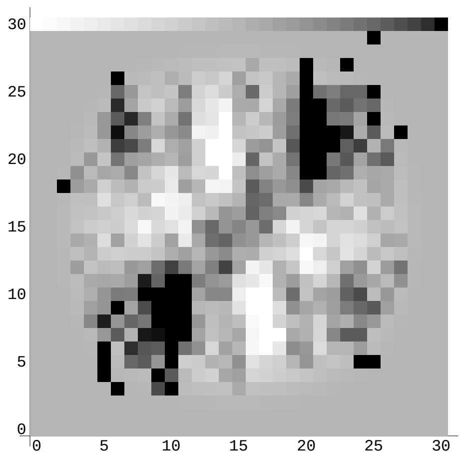

Fig. 2. Map of the $Z_{i,j}$'s for $m = 2^{31} - 1$, $a = 2^{15} - 2^{10}$, $\ell = 30$, $N = 2^{20}$

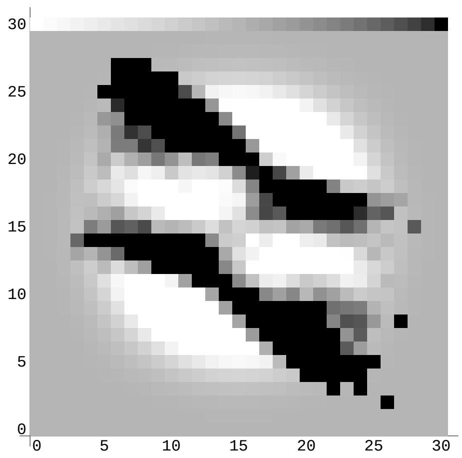

Fig. 3. Map of the $Z_{i,j}$'s for $m = 2^{31} - 1$, $a = -2^{16} - 2^{11}$, $\ell = 30$, $N = 2^{20}$

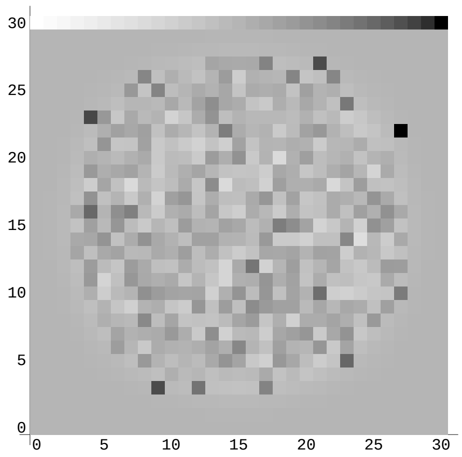

Fig. 4. Map of the $Z_{i,j}$'s for $m = 2^{31} - 1$, $a = 16807$, $\ell = 30$, $N = 2^{20}$

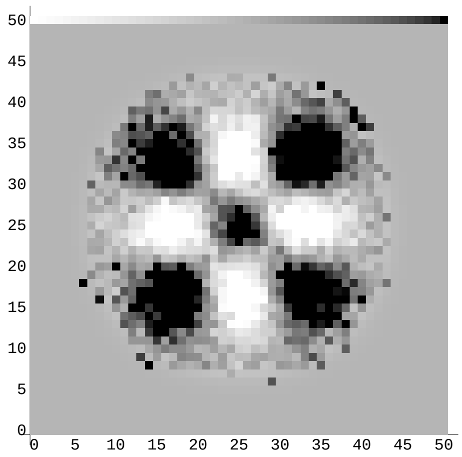

Fig. 5. Map of the $Z_{i,j}$'s for $m = 2^{61} - 1$, $a = 2^{30} - 2^{19}$, $\ell = 50$, $N = 2^{26}$

Table 1. The p-values for Q for the two LCGs with $m = 2^{31} - 1$ proposed by Wu; $Np \geq 5$

N	$a = 2^{15} - 2^{10}$	$a = -2^{16} - 2^{11}$
2^{12}		3.8×10^{-3}
2^{13}		1.8×10^{-3}
2^{14}		1.8×10^{-15}
2^{15}	1.7×10^{-3}	$< 10^{-15}$
2^{16}	3.5×10^{-11}	$< 10^{-15}$
2^{17}	$< 10^{-15}$	$< 10^{-15}$

Table 2. The p-values for Q for the two LCGs with $m = 2^{61} - 1$ proposed by Wu; $Np \geq 5$

N	$a = 2^{30} - 2^{19}$	$a = 2^{42} - 2^{31}$
2^{17}		
2^{18}		
2^{19}		1×10^{-6}
2^{20}	2×10^{-12}	6.4×10^{-7}
2^{21}	$< 10^{-15}$	$< 10^{-15}$
2^{22}	$< 10^{-15}$	$< 10^{-15}$

means $Z_{i,j} \leq -5$, black means $Z_{i,j} \geq 5$, and grey shades represent the values in between according to the scale displayed at the top of each figure (darker is larger). Note that the black and white values are 5 standard deviations or more away from the mean. It is quite clear from the figures that the multipliers $a = 2^{15} - 2^{10}$, $a = -2^{16} - 2^{11}$ and $a = 2^{30} - 2^{19}$ are unacceptable. The multiplier $a = 16807$ behaves well (although we *do not* recommend such a small LCG, whatever be the multiplier). We tried the other LCGs mentioned above, as well as several other recommendable random number generators (such as those proposed by L'Ecuyer [1999a], for example), and their displays were similar to that of Figure 4, i.e., they behaved in agreement with $\mathcal{H}_0$.

For the chi-square test based on Q, Table 1 gives the p-values smaller than 0.01 for different sample sizes N, for the two generators with modulus $m = 2^{31} - 1$ proposed by Wu. The p-values for $N = 2^\nu$ and $\nu \geq 17$ are all smaller than 10^{-15}. A rather small sample size suffices for rejecting $\mathcal{H}_0$. For comparison, the LCGs with modulus $m = 2^{31} - 1$ and multipliers $a = 16807$, 630360016, and 742938285 had no p-value less than 0.01 for $N = 2^\nu$ and $15 \leq \nu \leq 24$. They started to fail at sample size around $N = 2^{26}$. Table 2 gives the p-values smaller than 0.01 for the two generators with modulus $m = 2^{61} - 1$ proposed by Wu. The p-values for $N \geq 2^{22}$ are all less than 10^{-15}.

We made additional tests on LCGs of the form (1–2) as follows. For $e = 12, \ldots, 40$, we took m equal to the largest prime less than 2^e, and found a good multiplier a of the form (1) based on the spectral test up to 8 dimensions, as was done by L'Ecuyer [1999b] for general LCGs without conditions on a. We then applied the Q test above to the two families of LCGs: (a) those satisfying (1) and (b) those listed in Table 2 of L'Ecuyer [1999b]. In each case we took $\ell = e - 1$ and $N = 2^\nu$ for $11 \leq \nu \leq e$. The LCGs in (b) had no difficulty with these tests for N nearly as large as m, whereas those in (a) failed the tests typically with p-values $p < 10^{-15}$ for $N \ll m$.

5. CONCLUSION

The spectral test is recognized as the most powerful test for analyzing the structure of LCGs and MRGs [Knuth 1997]. It tests a very important aspect of the point set produced by the generator: its lattice structure. It is clear, however, that like any other test, the spectral test cannot test every statistical property of the generator. It has been pointed out on several occasions (e.g., [Compagner 1995; L'Ecuyer 1998]) that generators should not be based on recurrences whose structure is too simple. In particular, the bits should be well mixed. Otherwise, one gets into problems such as those illustrated by the present paper. The MRGs proposed by L'Ecuyer [1996, 1999a], selected on the basis of the spectral test, do not have this problem because the binary representation of their multipliers contains a good mixture of 0's and 1's.

The idea of choosing multipliers of the form (1) to speed up implementation can be trivially extended to multiple recursive generators (MRGs), i.e., linear congruential generators based on recurrences of higher order [L'Ecuyer 1998; Knuth 1997; Niederreiter 1992]. However, the resulting LCGs or MRGs should not be used in their plain form. On the other hand, the idea, and the generalization that we developed in § 2, can be used fruitfully for implementing *combined* LCGs or MRGs, e.g., with the combination methods proposed by L'Ecuyer [1996]. Work in that direction is under way.

ACKNOWLEDGMENTS

This work has been supported by the National Science and Engineering Research Council of Canada grants # ODGP0110050 and SMF0169893, by FCAR-Québec grant # 93ER1654.

REFERENCES

COMPAGNER, A. 1995. Operational conditions for random number generation. *Physical Review E 52*, 5-B, 5634–5645.

FISHMAN, G. S. 1996. *Monte Carlo: Concepts, Algorithms, and Applications.* Springer Series in Operations Research. Springer-Verlag, New York.

KNUTH, D. E. 1997. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* (Third ed.). Addison-Wesley, Reading, Mass.

L'ECUYER, P. 1996. Combined multiple recursive random number generators. *Operations Research 44*, 5, 816–822.

L'ECUYER, P. 1998. Random number generation. In J. BANKS Ed., *Handbook of Simulation*, pp. 93–137. Wiley. chapter 4.

L'ECUYER, P. 1999a. Good parameters and implementations for combined multiple recursive random number generators. *Operations Research 47*, 1, 159–164.

L'ECUYER, P. 1999b. Tables of linear congruential generators of different sizes and good lattice structure. *Mathematics of Computation 68*, 225, 249–260.

NIEDERREITER, H. 1992. *Random Number Generation and Quasi-Monte Carlo Methods*, Volume 63 of *SIAM CBMS-NSF Regional Conference Series in Applied Mathematics.* SIAM, Philadelphia.

WEGENKITTL, S. 1998. *Generalized ϕ-Divergence and Frequency Analysis in Markov Chains.* Ph. D. thesis, University of Salzburg. `http://random.mat.sbg.ac.at/team/`.

WU, P.-C. 1997. Multiplicative, congruential random number generators with multiplier $\pm 2^{k_1} \pm 2^{k_2}$ and modulus $2^p - 1$. *ACM Transactions on Mathematical Software 23*, 2 (June), 255–265.