JOURNAL OF COMPUTATIONAL PHYSICS 77, 267–269 (1988)

Note

Long Range Correlations in Linear Congruential Generators*

The construction of random number generators is an old art and a recent science. There are two extreme questions that naturally arise, and a plethora of intermediate ones. One extreme is whether one really needs a sequence to simulate randomness for a given computational task; here, little has been done since the fascinating start by Richtmyer [1] years ago. The other extreme is that of devil's advocate: does the structure that creeps into any random number algorithm act to render suspect, or even wrong, its application to a given task? A fairly recent paper of Filk *et al.* [2] has addressed this question in the context of lattice gas simulations in which stepping by powers of two is an intrinsic structural component of a typical program. They showed that a primitive linear congruential random number generator introduces correlations among elements separated sequentially by powers of two, which thereby introduce errors into Monte Carlo procedures unless palliative measures are taken. We would like to indicate in this note that the phenomenon is not restricted to this special generator, but is a simultaneous property of all linear congruential generators with fixed multiplier using a power of two as modulus.

The general linear congruential generator takes the form

$$x_n \equiv a x_{n-1} + b \qquad (\mathrm{mod}\ m), \tag{1}$$

generating a sequence of integers between 0 and m, or dividing by m, of fractions between 0 and $(m-1)/m$; the choice $m = 2^\beta$ is essentially mandatory for efficient programming of binary-based digital computers. The iteration of (1) is readily carried out, yielding the formally explicit

$$x_n \equiv a^n x_0 + \frac{a^n - 1}{a - 1} b \qquad (\mathrm{mod}\ 2^\beta). \tag{2}$$

It is easy to see that if $a \equiv 1 \pmod 4$ and b is odd, then $\{x_0, x_1, ..., x_{m-1}\}$ is a permutation of $\{0, 1, 2, ..., m-1\}$. For a fixed k, we now ask whether there exists a guaranteed linear relation among entries in the chain separated by 2^k:

$$\sum_0^p c_j x_{n+j2^k} \equiv 0 \qquad (\mathrm{mod}\ 2^\beta). \tag{3}$$

* This work was supported by the Applied Mathematical Sciences Program of the U.S. Department of Energy under Contract DE-AC02-76ER03077.

0021-9991/88 $3.00

Substituting (2) into (3), this will be the case for given x_0 and b if

$$\begin{aligned} f(a)\, x_0 &\equiv 0 \qquad (\mathrm{mod}\ 2^\beta), \\ \frac{f(a)-f(1)}{a-1}\, b &\equiv 0 \qquad (\mathrm{mod}\ 2^\beta), \end{aligned} \tag{4}$$

where $f(a) = \sum_0^p c_j a^{j2^k}$.

The case $b = 0$, a odd, was studied by Filk *et al.* [2]; here one only requires

$$f(a) \equiv 0 \qquad (\mathrm{mod}\ 2^\beta), \tag{5}$$

independently of x_0. The basic relation of type (5) is the Euler totient formula [3] which becomes in the present case

$$a^{2^{\beta-1}} - 1 \equiv 0 \qquad (\mathrm{mod}\ 2^\beta). \tag{6}$$

However, there are numerous polynomials of lower degree that satisfy (5). For relations between $\{x_n\}$ separated by 2^k, these are most readily generated from the primitive case

$$a^{2^k} - 1 \equiv 0 \qquad (\mathrm{mod}\ 2^{\gamma(k)}) \tag{7}$$

for suitable $\gamma(k)$. The totient formula [3] guarantees that $\gamma(k) \geqslant k+1$, but the decomposition

$$a^{2^k} - 1 = (a-1) \prod_{j=0}^{k-1} (a^{2^j} + 1) \tag{8}$$

establishes at once the result that if $a \equiv 1\ (\mathrm{mod}\ 2^\alpha)$, then $\gamma(k) \geqslant k + \alpha$. If in addition $a \not\equiv 1\ (\mathrm{mod}\ 2^{\alpha+1})$ then (8) guarantees that $\gamma(k) = k + \alpha$. In any event, we see at once from (7) that, for example,

$$(a^{2^k} - 1)^{\{\beta/\gamma(k)\}} \equiv 0 \qquad (\mathrm{mod}\ 2^\beta), \tag{9}$$

where $\{c/d\} = 1 + [(c-1)/d]$ is the smallest integer $\geqslant c/d$. Thus (3) holds, with

$$c_j = (-1)^j \binom{\{\beta/\gamma(k)\}}{j}. \tag{10}$$

The specialization $b = 0$ in (1) is unnecessary and is in fact completely inappropriate for vector random number generators which are natural components of highly parallel programs. Proceeding then to the more standard generators in which b is merely odd, we require in addition to (5)

$$\frac{f(a)-f(1)}{a-1} \equiv 0 \qquad (\mathrm{mod}\ 2^\beta) \tag{11}$$

now independently of x_0 and b. Indeed, (11) implies (5) if we impose the condition

$$f(1)=0, \tag{12}$$

which we shall do. Suppose now that

$$a \equiv 1 \pmod{2^\alpha}$$

but

$$a \not\equiv 1 \pmod{2^{\alpha+1}}. \tag{13}$$

Then (11) with (12), is equivalent to

$$f(a) \equiv 0 \pmod{2^{\alpha+\beta}}. \tag{14}$$

The discussion of the previous paragraph hence applies and we conclude at once that

$$f(a) = (a^{2^k}-1)^{\{(\alpha+\beta)/(k+\alpha)\}} \tag{15}$$

generates a linear recursion relation of type (3) for all x_0 and b. Thus, aside from a possible slight increase in the order of the recursion relation, the correlation structure of the $b=0$ case applies here as well, and care must be taken—e.g., by skipping members of the sequence or by random changes in b—to avoid computational artifacts in a wide variety of applications.

REFERENCES

1. R. D. RICHTMYER, "A nonrandom sampling method based on congruences for Monte Carlo Problems," Atomic Energy Commission Computer and Applied Mathematics Center, New York University, NYO-8674, 1958 (unpublished).
2. T. FILK, M. MARCU, AND K. FREDENHAGEN, *Phys. Lett. B.* **165**, 125 (1985); D. E. KNUTH, *The Art of Computer Programming, Vol.* II, (Addison–Wesley, Reading, MA, 1981), Sect. 3.2.1.3 for the associated concept of "potency."
3. G. H. HARDY AND E. M. WRIGHT, *The Theory of Numbers, 4th Ed.* (Clarendon Press, Oxford, 1960).

RECEIVED: June 26, 1987; REVISED: September 18, 1987

ORA E. PERCUS
JEROME K. PERCUS
Courant Institute of Mathematical Sciences,
New York University,
251 Mercer Street, New York, New York 10012