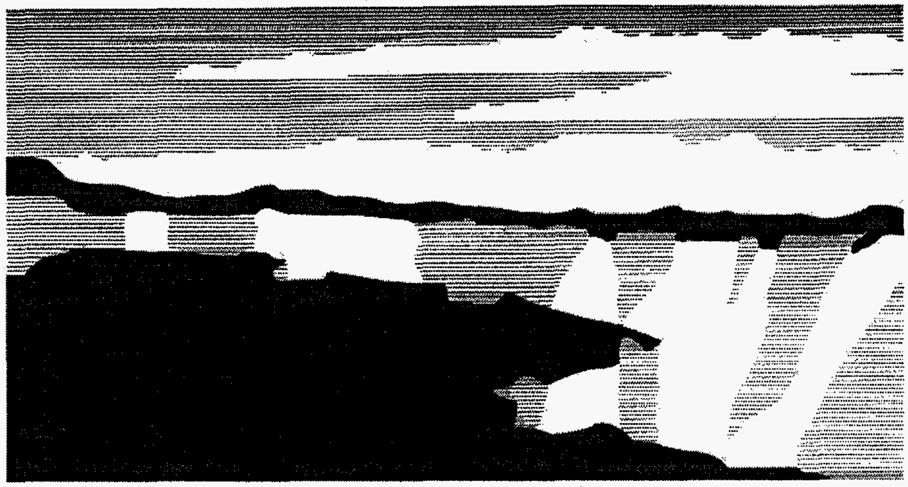
LA-UR-96-1885 (Revision 1)

Title:

A New Class of Random Number Generators Required for Advanced Computer Architectures

Author(s): T. T. Warnock, CIC-3
W. A. Beyer, T-7/AFF
W. W. Wood, T-12/AFF

Submitted to: DOE Office of Scientific and Technical Information (OSTI)



Los Alamos
NATIONAL LABORATORY

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

A New Class of Random Number Generators Required for Advanced Computer Architectures

Tony Warnock*, William Beyer, and William W. Wood

Abstract

This is the final report of a three-year, Laboratory-Directed Research and Development (LDRD) project at the Los Alamos National Laboratory (LANL). The advent of ever more powerful computers allows one to run Monte Carlo computations of unprecedented length. Currently used random number generators (RNGs) do not have the cycle length necessary for these computations. It is possible to cycle completely through most RNGs used on workstations in a few minutes computations. Even having a long period may not qualify a RNG as suitable. We are developing tests that will allow us to develop high quality RNGs for use in long computations.

1. Background and Research Objectives

Reliability of Monte Carlo methods ultimately rests upon the quality of "random" numbers used in a computation. These numbers are not truly random, but are generated by some deterministic mathematical process. Such random number generators (RNGs) can only produce a finite sequence of numbers before repeating themselves. Advanced computer architectures and fast scientific workstations are capable of exhausting the entire sequence of many presently used generators in a single computation. A new class of RNGs is required or else these new computing capabilities will be of limited value for complex Monte Carlo simulations.

Many of the currently used RNGs are inadequate for the future. For example, many computations on workstations are done with an RNG whose cycle is only 2^{32} (about 4,000,000,000). A 25 Mhz workstation that takes 10 cycles to generate a new random number would exhaust the RNG in about 30 minutes. In addition, the cycle need not be exhausted to exhibit problems. For example, if one were to run a problem on a lattice of size 256^3 using a

*Principal investigator, e-mail: ttw@lanl.gov

RNG of cycle lenght 2^{46} (as a CRAY computers), there would only be 2^{22} possible states of the entire system, about 4,000,000.

Large-scale computations will also benefit from using RNGs in a tree structure that requires a family of RNGs, each with a very long cycle length. Such structures are required for reproducibility in problems run on a variety of architectures. Our generators are designed so that they can be used in tree structures. Another consideration is that selection of parameters entering into a generator is as important as choosing the type of generator. Poor choice of parameters will make any type of generator fail. As an extreme example, consider the linear congruential generator (LCG) with multiplier 1 and additive constant 1; that is,

$$x_{n+1} = x_n + 1 \pmod{2^{64}}. \tag{1}$$

It has along cycle, but certainly it is not very random.

The objective of this project was to extend current random number generators to much greater cycle lengths, to develop other types of generators, and to develop tests of usefulness of random nubmer generators.

2. Importance to LANL's Science and Technology Base and National R&D Needs

Monte Carlo techniques are used in solving the most difficult problems in computational science; for example, in the evaluation of large-dimensional integrals, computations in statistical physics, simulations of computer systems, computations of stochastic processes such as radiation transport, in many types of statistical simulations, and particularly bootstrapping. The above fields, which impact all of the Laboratory's technical directorates, will benefit from improvement in random number generation.

This project has produced a set of parameters for long-cycle random number generators that are independent of any particular computer architecture. Use of our versions of random number generators should improve the reliability of Monte Carlo computations.

3. Scientific Approach and Results

We have developed methods for generating good multipliers for linear congruential random number generators having the form

$$x_{n+1} = ax_n + b \pmod{m}, \tag{2}$$

with the modulus $m = 2^{64}$, the multiplier $a \equiv 5 \pmod 8$, and b odd. Such generators are known to have cycles of length 2^{64}. Points obtained by taking successive k-tuples of numbers are known to lie on a lattice (strictly speaking, a grid) in k-dimensional space, with the structure of the lattice being dependent on the modulus, the multiplier, and the dimensionality, but independent of the additive constant b. Our multipliers are numbers that have continued-fraction expansions with small partial quotients. Each multiplier was tested as to its lattice structure by calculating the Beyer ratio of its Minkowski-reduced basis (this ratio is the length of the longest basis vector divided by the length of the shortest one) for demension $k = 2$ to 20, and the "specral" criterion

$$S_k = \gamma_k / d_k m^{1/k} \tag{3}$$

for $k = 2$ to 8 (the number-theoretical constants γ_k are known only up to $k = 8$; d_k is the maximum distance between adjacent hyperplanes of the lattice). In addition to those theoretical tests, some empirical, multidimensional tests of randomness were performed.

A set of 6139 multiplier candidates was produced by assembling small partial quotients (1, 2, and 3) into fractions with denominator 2^{64}. These multipliers were further screened by computing a Minkowski-reduced basis for each multiplier in dimensions 2 through 20. Such bases were computed both for the usual method of taking ($x_1, x_2, \ldots, x_k$) for the first point, then ($x_2, x_3, \ldots, x_{k+1}$), etc., for the rest of the points, as well as for the normal computational practice of using ($x_{k+1}, x_{k+2}, \ldots, x_{2k}$), etc., for the second and succeeding points. The resulting lattices are different, though related. There were 39 multipliers that had Beyer ratios of less than two in all dimensions from 2 to 20, for both methods of generating points.

This set of 39 multipliers was further screened by eliminating those for which the spectral criterion S_k was less than one-half for any $k \leq 8$. There then remained the following 28 multipliers:

4976020386757901309
5142405999627351477
5404219024714966693
5454419945275071789
5474134856495893365
5478328130623540933
6820021792522912829
6821073945445402613
6821074018538075053
6824416601091123613
7003684266848454309
7006533158028555197
7012110274515832637
7041280070492449437
7048403008459888517
7621901501671773125
7726229154173057221
7750298656492540853
7785624254559075453
7793308859335717829
10650576889336859413
10661099470315462429
10824572664270259317
11315494558352192797
11439446807260005845
11632581878285320405
11694411052079579749
13304262757101967421

Any of these multipliers can be used as the multiplier *a* in a linear congruential random number generator of the form (2).

It has been known for some time that the Minkowski-reduced basis for a given lattice need not be unique, even leaving aside such trivial differences as changes of the signs of basis vectors and the ordering of basis vectors of equal length. This has the consequence that a given LCG may have more than one Beyer ratio for a given dimension, depending on for which reduced basis it is computed. These facts are not often mentioned in the literature of the lattice structure of LCGs. We have noticed such occurrences in generators having small moduli, i.e., for $a = 45$, $m = 2^9$, $k = 20$, and for $a =4912069$, $m = 2^{23}$, $k = 33$, but we found non for our multipliers, $m = 2^{64}$ and $k \leq 20$. The pattern of the occurrences that we have seen is such that we would not expect to see them for our parameters until *k* becomes much larger than the values considered here.