LA-UR-96- 1885

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

RECEIVED
JUL 19 1996
OSTI

Author(s): Tony Warnock, CIC-3
William Beyer, T-7
William W. Wood, T-12

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.

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 mathematical formula. Such random number generators (RNGs) can only produce a finite number of terms before repeating themselves. Advanced computer architectures and fast scientific workstations are capable of exhausting the entire sequence of 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.

None of the currently used RNGs are adequate for the future. For example, many computations on workstations are done with a RNG whose cycle is only 232 (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. The cycle need not be exhausted to exhibit problems. For example, if one were to run a problem on a lattice of size 2563 using a RNG of cycle length 246 (as on CRAY computers), there would only be 222 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 with a very long cycle length. Such structures are required for

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

reproducibility in problems run on a variety of architectures. Our generators will be designed so that they can be used in tree structures. Another consideration is that selecting of parameters entering into any generator is as important as choosing of the type of generator. Poor choice of parameters will make any type of generator fail. As an extreme example, consider the Lehmer generator with multiplier 1 and additive constant 1; that is, $X_i = X_{i-1} + 1$. It has a long 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 number 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, and in many types of statistical simulations, particularly bootstrapping. The above fields, which impact all of the Laboratory's technical directorates, will benefit from improvement in random number generation.

This project will produce a set of parameters for long-cycle random-number generators that will be independent of any particular computer architecture. We also will produce improved versions of lattice-based tests of random number generators. 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 multipliers for congruential random number generators that should have good properties. These multipliers are numbers that have continued-fraction expansions with small partial quotients. We are developing lattice structure tests in many dimensions. Multipliers that are generated with small partial quotients are then tested as to their lattice structure. As an adjunct to these theoretical tests, empirical, multidimensional tests of randomness are performed.

A set of 6139 multiplier candidates were produced by assembling small partial quotients (1,2,3) 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. These bases are computed both for the mathematically usual method of computing $\langle x(1),x(2),x(3)\rangle$

for the first point then shifting to <x(2),x(3),x(4)>, etc. for the rest of the points and for the normal computational practice of using <x(4),x(5),x(6)>, etc. for succeeding points. The Minkowski bases for the resulting lattices are different. There were 39 multiplier that had Beyer ratios of less than two in all dimensions from 2 to 20 and for both methods of generating a lattice. The Beyer ratio is the ratio of the longest basis vector to the shortest. A multiplier having a large Beyer ratio will generate random numbers that tend to fall into low-dimensional hyperplanes.

The 39 surviving multipliers are:

4976020386757901309
5142405999627351477
5404219024714966693
5454419945275071789
5474134856495893365
5478328130623540933
5479845096888076901
6819902100659376941
6820021792522912829
6821073945445402613
6821074018538075053
6824416601091123613
7003684266848454309
7006533158028555197
7012110274515832637
7041280070492449437
7046354309346571677
7048403008459888517
7149348675631157317
7621901501671773125
7643477398828078917
7726229154173057221
7750298584879264957
7750298656492540853
7785624254559075453
7793308859335717829

1065057688933685941 3
10661099470315462429
10720510645986104933
10824572664270259317
11315494558352192797
11384690040334915805
11439446807260005845
11632581878285320405
11666126007410198461
11694411052079579749
13301982656252922541
13302396341289466077
13304262757101967421

Any of these multipliers can be used as the multiplier A in a linear congruential random number generator of the form

$$X(i) = A * X(i-1) + b \text{ (Modulo } 2^{64}\text{)}$$

with b any odd integer.

A surprising finding was that the Minskowski reduced basis for a lattice need not be unique. The Beyer ratio has been used for over twenty years as a measure of the quality of a random number generator. The lack of uniqueness of the Minkowski basis means that a random number generator may have more than one associated Beyer ratio. This only seems to happen when the dimensionality is large compared to the multiplier. No examples were found for the above multipliers.

DISCLAIMER