Proceedings of the 1989 Winter Simulation Conference
E.A. MacNair, K.J. Musselman, P. Heidelberger (eds.)

RANDOM NUMBER GENERATION ON PARALLEL PROCESSORS

Masanori Fushimi
Department of Mathematical Engineering
and Information Physics
Faculty of Engineering
University of Tokyo
Bunkyo-ku, Tokyo 113, Japan

ABSTRACT

Recent development of high speed supercomputers has enabled us to perform large scale Monte Carlo simulations which need a tremendous amount of random numbers. There are two types of supercomputers, *i.e.* pipeline type and processor array type, and we will confine ourselves in this paper to the random number generation on a computer of the latter type. It is desired that not only a sequence of random numbers generated on each processor is of good quality but also sequences generated on different processors are uncorrelated. If we use a linear congruential method on a 32-bit supercomputer, the whole period may be consumed in several seconds to several minutes. Random numbers with a much longer period can be generated by a GFSR algorithm. Using this algorithm, we will propose a method to generate uncorrelated series of random numbers on parallel processors.

1. INTRODUCTION

The recent development of high speed parallel computers has enabled us to perform large scale Monte Carlo simulations which use tremendous amount of random numbers and this has increased interests in methods of generating many independent or uncorrelated sequences of random numbers with long periods. For example, a group of Japanese information scientists has been developing a parallel computer system called "PACS" since 1977 (Hoshino, et al. 1983); the present system has 240 processing units and this number will be doubled very shortly. The tasks allocated to each processing unit in this system are executed asynchronously. Oyanagi (1984) stresses the importance of generating random number sequences on these parallel processors which have good statistical properties both within and between sequences.

The most widely used method of generating random numbers on a computer is perhaps the Lehmer's linear congruential method, but it is not suitable for our present purpose because of the following reasons. The period of the sequence is limited by the bit-length of the computer; for example, a multiplicative congruential sequence with modulus 2^{31} has the period 2^{29} and a 32-bit supercomputer S820 at the University of Tokyo can produce the whole period in 1.3 second (Oyanagi 1988). The period can be made longer if we use a multiple precision arithmetic or combine several congruential sequences to obtain a single sequence as proposed by Wichmann and Hill (1982), but then it is not an easy problem to find many, say 512, good multipliers which pass various statistical tests. Moreover, it is difficult to assure good correlation properties between all pairs of sequences with different multipliers (Oyanagi 1984).

In this paper, we consider generators based on linear recurrences modulo two. Two types of generators in this class were proposed by Tausworthe (1965) and Lewis and Payne (1973). Lewis and Payne called their generator the generalized feedback shift register (GFSR) pseudorandom number algorithm. Fushimi (1983, 1989) showed an equivalence relation between these two sequence, and, as an application of it, proposed a fast initialization procedure for the GFSR generator. The method we propose in this paper for generating uncorrelated sequences of random numbers on parallel processors is another application of the equivalence relation mentioned above. So we will review the previous results related to the present paper in the next section.

2. PREVIOUS RESULTS

Let $\langle a_t \rangle$ be the sequence of 0's and 1's generated by the linear recurrence relation

$$a_t = c_1 a_{t-1} + c_2 a_{t-2} + \cdots + c_p a_{t-p} \pmod 2$$

whose characteristic polynomial

$$f(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_p D^p, \quad c_p = 1$$

is primitive over the Galois field GF(2), where the initial values $a_0, a_1, \cdots, a_{p-1}$ are not all zero. The sequence $\langle a_t \rangle$ is periodic with the least period $T = 2^p - 1$, and called by such names as an M-sequence, a PN-sequence, a feedback shift register sequence, *etc.* We will use the notation $\langle a_t(f) \rangle$ instead of $\langle a_t \rangle$ when it is necessary to specify the primitive polynomial associated with $\langle a_t \rangle$. Incidentally, the sequence $\langle a_t \rangle$ does not depend on the initial values except for the phase difference.

Let R be the set of integers defined by

$$R = \{r \mid 1 \le r < T,\ \gcd(r,T) = 1\},$$

then it forms a group under multiplication modulo T. The set

$$C_1 = \{1, 2, 2^2, \cdots, 2^{p-1}\}$$

is a normal subgroup of R, and there are $K \equiv \varphi(T)/p$ residue classes (including C_1) to be denoted by $C_1, C_2, \cdots, C_K$, where $\varphi(T) = |R|$ is Euler's totient function.

The following properties of M-sequences are well known (Golomb 1967). The n-wise decimated sequence $\langle a_{nt} \rangle = \langle a_0, a_1, a_2, \cdots \rangle$ is again an M-sequence with the same period T as $\langle a_t \rangle$ if and only if $\gcd(n,T) = 1$; if both $\gcd(n_1,T) = 1$ and $\gcd(n_2,T) = 1$, then $\langle a_{n_1 t} \rangle \cong \langle a_{n_2 t} \rangle$ if and only if n_1 and n_2 belong to the same residue class, where the symbol $\cong$ means that the two sequences are equivalent except for the starting point. There are exactly K primitive polynomials with degree p. We denote by $f_1(D)$ the primitive polynomial associated with $\langle a_t \rangle$ and by $f_i(D)$ one associated with $\langle a_{nt} \rangle, n \in C_i, 2 \le i \le K$.

Using the M-sequence $\langle a_t(f) \rangle$, we construct two sequences of ℓ-bit $(2 \le \ell \le p)$ binary integers as follows.

Tausworthe sequence $\langle X_t(f;\sigma) \rangle$:

$$X_t = a_{\sigma t} a_{\sigma t+1} a_{\sigma t+2} \cdots a_{\sigma t+\ell-1}, \quad \sigma \in R$$

GFSR sequence $\langle Y_t(f;\tau) \rangle$:

$$Y_t = a_t a_{t+\tau} a_{t+2\tau} \cdots a_{t+(\ell-1)\tau}, \quad \tau \in R$$

Then we have the following theorems.

THEOREM 1 (Tausworthe 1965). If $\sigma \ge \ell$, then the sequence $\langle X_t(f;\sigma) \rangle$ is k-distributed for $1 \le k \le \lfloor p/\sigma \rfloor$, and has a good autocorrelation property for lags up to $\lfloor (T-\ell)/\sigma \rfloor$.

THEOREM 2 (Fushimi and Tezuka 1983). The GFSR sequence $\langle Y_t(f;\tau) \rangle$ is k-distributed if and only if the $k\ell$ elements of the M-sequence $\langle a_t(f) \rangle$ contained in the initial k values $Y_0, Y_1, \cdots, Y_{k-1}$ of the sequence are linearly independent.

THEOREM 3 (Fushimi 1983, 1989). For any p and ℓ $(2 \le \ell \le p)$, the following equivalence relations between Tausworthe and GFSR sequences hold.

$$\langle X_t(f_1;\sigma) \rangle \cong \langle Y_t(f_i;\sigma^{-1}) \rangle \quad \text{if } \sigma \in C_i$$

$$\langle Y_t(f_1;\tau) \rangle \cong \langle X_t(f_j;\tau^{-1}) \rangle \quad \text{if } \tau \in C_j$$

Here, σ^{-1} and τ^{-1} are inverses of σ and τ, respectively, in the multiplicative group R.

3. GENERATING UNCORRELATED RANDOM SEQUENCES ON PARALLEL PROCESSORS

Suppose there are m parallel processors and we want to generate an ℓ-bit random sequence on each processor. Our idea is to use the same recurrence relation on all processors but give different initial values so that the sequences on different processors are uncorrelated. The maximum order of equidistribution is the same for all the sequences and is independent of the initial values.

Our method is conceptually as follows. We think of an ℓm-bit Tausworthe sequence $\langle X_t(f_1;\sigma) \rangle$ with $\sigma \ge \ell m$ and initialize it by any means. Then we "slice" each of these p initial values into m ℓ-bit integers and distribute them to m processors as initial values. More specifically, initial values for the sequence $\langle Y_t^{(n)} \rangle$ on the n-th processor are set as follows:

$$Y_t^{(n)} = a_{\sigma t+\ell n} a_{\sigma t+\ell n+1} \cdots a_{\sigma t+\ell n+\ell-1}$$

$$(0 \le t \le p-1, \quad 0 \le n \le m-1).$$

If we give the initial values for $\langle a_t(f_1) \rangle$ and distribute this information to all the processors, then every processor can compute, independently of the other processors, the elements of $\langle a_t(f_1) \rangle$ which are necessary for initializing its sequence very quickly by using a technique described in Fushimi and Tezuka (1983). Once the initialization is over, we use the recurrence relation

$$f_i(D) Y_t^{(n)} = 0$$

on every processor if $\sigma \in C_i$, where D is the operator which decreases the subscript by 1 and the addition is understood to be bitwise addition modulo 2 (exclusive-or operation).

It is easy to see from previous results that the sequences $\langle Y_t^{(n)} \rangle$ have the following properties.

(1) Every sequence $\langle Y_t^{(n)} \rangle$ is equivalent in the sense of $\cong$. The phase difference between $\langle Y_t^{(0)} \rangle$ and $\langle Y_t^{(n)} \rangle$ is $n\ell\sigma^{-1}$.

(2) The sample autocorrelation function between sequences of length N on any pair of processors has the mean value almost equal to zero and the variance of $O(N^{-1})$ for lags up to approximately $\ell\sigma^{-1} - N$.

(3) The maximum order of equidistribution of every sequence guaranteed by theorem 1 is $\lfloor p/\sigma \rfloor \leq \lfloor p/\ell m \rfloor$. Since we usually use $p = 521$ or 607 and $\ell = 16$ or 32, this upper bound is zero if m is large. On the other hand, the maximum possible order of equidistribution is $\lfloor p/\ell \rfloor$, and we can check whether or not this order is attained using the algorithm proposed by Fushimi and Tezuka (1983) based on Theorem 2.

ACKNOWLEDGEMENTS

Main parts of this paper are based on the author's previous paper (Fushimi 1983) and he is grateful to a referee for useful comments on an earlier version. He also wishes to thank Prof. Y. Oyanagi for suggesting the importance of the problem of generating uncorrelated random sequences on parallel processors.

REFERENCES

Fushimi, M.(1983). A reciprocity theorem on the random number generation based on m-sequences and its applications (in Japanese). *Transactions of the Information Processing Society of Japan* **24**, 576-579.

Fushimi, M. (1989). An equivalence relation between Tausworthe and GFSR sequences and applications. *Applied Mathematics Letters* **2**, 135-137.

Fushimi, M. and Tezuka, S.(1983). The k-distribution of the generalized feedback shift register pseudorandom numbers. *Communications of the ACM* **26**, pp. 516-523.

Golomb, S. W.(1967): *Shift Register Sequences.* Holden-Day, San Francisco.

Hoshino, T., et al. (1983). PACS: A parallel microprocessor array for scientific calculations. *ACM Transactions on Computer System* **1**, 195-221.

Lewis, T. G. and Payne, W. H.(1973): Generalized feedback shift register pseudorandom number algorithms. *Journal of the ACM* **21**, 456-468.

Oyanagi, Y. (1984). Random number generation in large-scale Monte Carlo calculations. In *RIMS Kokyuroku* **537**, Research Institute for Mathematical Sciences, Kyoto University, Japan, 112-122.

Oyanagi, Y. (1988). Vectorization of Lewis-Payne random number generation on HITAC S810 and S820. In *Proceedings of a Japan Society for the Promotion of Science Seminar: Trends in Supercomputing* (Y. Kanada and C.K. Yuen, eds.) World Scientific, Singapore, 47-50.

Tausworthe, R. C.(1965). Random numbers generated by linear recurrence modulo two. *Mathematics of Computation* **19**, 201-209.

Wichmann, B.A. and Hill, I.D. (1982). Algorithm AS 183: An efficient and portable pseudo-random number generation. *Applied Statistics* **31**, 188-190.

AUTHOR'S BIOGRAPHIES

MASANORI FUSHIMI is a professor in the Department of Mathematical Engineering and Information Physics at the University of Tokyo. He received B. Eng., M. Eng., and Dr. Eng. degrees in mathematical engineering from the University of Tokyo in 1963, 1965, and 1968 respectively. His current research interests include statistical computations, random number generation, sequential decision procedures, and numerical analysis.

Masanori Fushimi
Department of Mathematical Engineering
and Information Physics
Faculty of Engineering
University of Tokyo
Bunkyo-ku, Tokyo 113, Japan
(03)812-2111 ext. 6920