Proceedings of the 1995 Winter Simulation Conference
ed. C. Alexopoulos, K. Kang, W. R. Lilegdon, and D. Goldsman

COMBINATION OF MULTIPLICATIVE CONGRUENTIAL RANDOM-NUMBER GENERATORS WITH SAFE PRIME MODULUS

Munetaka Sakamoto
Susumu Morito

Department of Industrial Engineering and Management
School of Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo 169, JAPAN

ABSTRACT

Two or more multiplicative congruential random-number generators with prime modulus combined by means of a method proposed by Wichmann and Hill yield a random-number generator equivalent to a multiplicative congruential random-number generator with modulus equal to the product of the moduli of the component multiplicative congruential generators. The period of a random-number sequence obtained by the Wichmann–Hill method is equal to the least common multiple of the periods of the combined sequences. One of the two purposes of this paper is to present a necessary and sufficient set of efficiently verifiable conditions, for the period to be equal to its maximum, which is the maximum of the least common multiple. Each of the conditions will be always satisfied or will be more easily verifiable, when the modulus of each of the component generators is safe prime. The other purpose is to derive an efficiently evaluatable formula for serial correlations of the maximum-period sequences by the Wichmann–Hill method. The authors recommend (i) to make the modulus of each of the component generators safe prime, and (ii) to chose the multipliers of the components so as to (a) maximize the period and (b) make the serial correlations small in absolute value.

1 INTRODUCTION

Random numbers are requisite variables for random sampling, discrete-event simulation, etc. In random sampling, throwing icosahedral dice or consulting a table of random digits could suffice, but generating random numbers in a computer is no worse; in discrete-event simulation, a method of generating random numbers (to be precise, pseudo-random numbers) in a computer is indispensable. (Quasi-random numbers are more suitable for numerical integration with a fixed-dimensional integrand and for global optimization, than pseudo-random numbers are (Section 6.2 of Bratley, Fox, and Schrage 1987); for more information about quasi-random numbers, we refer to the profound book by Harald Niederreiter (1992).)

The common method of computer generation of random numbers is the multiplicative congruential generator (MCG). However, the period of the sequence obtained by the MCG cannot exceed the maximum size of integer representable on the computer; this limitation on the period can be fatal to applications in a high-speed computer where the number of required random numbers exceeds the period.

Wichmann and Hill (1982) have proposed a method of combining three MCG's with prime modulus representable on computers with a word size of at least 16 bits. Their combination yield a random-number sequence with a very large period for applications in 16-bit computers; indeed, the period of the sequence obtained by their method is equal to the least common multiple of the periods of the combined MCG sequences, even when the number of component MCG's with prime modulus is arbitrary (L'Ecuyer and Tezuka 1991).

In this paper, we shall see a necessary and sufficient set of conditions, for the period of a Wichmann–Hill sequence to be equal to its maximum, which is the maximum of the least common multiple. It can be efficiently verified whether each of the conditions holds or not, without evaluation of the least common multiple.

A prime number p greater than two is said to be safe prime, if $(p-1)/2$ is also a prime number (Marsaglia and Zaman 1994). A safe prime number is a proper modulus of an MCG, for two reasons (Marsaglia and Zaman 1994): A safe prime modulus guarantees

(i) that approximately half of all the candidate values for the multiplier of the MCG satisfy the maximum-period condition, and

(ii) that the period of the sequence of non-

overlapping t-tuples from the maximum-period sequence by the MCG is at least half of the maximum period, with few exceptions in the value of t.

Let J denote the number of MCG's combined by the Wichmann–Hill method. An MCG with safe prime modulus is a proper component of the Wichmann–Hill combination, for two reasons: A safe prime modulus of each of the J component MCG's assures

(i) that approximately $1 - 1/2^J$ of all the candidate vectors composed of J multipliers of the MCG's satisfy the maximum-period condition for the Wichmann–Hill method, and

(ii) that the period of the sequence of non-overlapping t-tuples from a maximum-period sequence by the Wichmann–Hill method is at least half of the maximum period, with few exceptions in the value of t.

Some of the principles of random-number generation in Section 3.6 of the second edition (1981) of the encyclopedic book by Donald E. Knuth (1969) implies (i) that serial correlations of a random-number sequence should not be large in absolute value, and (ii) that the overlapping or non-overlapping t-tuples of random numbers should form a good lattice, when they are viewed as points in the unit cube of t-dimensional space.

Efficiently evaluatable formulae for serial correlations of the sequence obtained by some types of MCG's are derived by Dieter and Ahrens (1971). In this paper, we shall see an efficiently evaluatable formula for serial correlations of the maximum-period sequences obtained by the Wichmann–Hill method.

The quality of the lattice structure of the points from an MCG sequence can be quantified by the spectral test originated by Coveyou and MacPherson (1967), which is the most meaningful test known so far, for assessment of the lattice structure of the MCG (Section 3.3.4 of Knuth 1969; Fishman and Moore 1986). The quality of the lattice structure of the points from a Wichmann–Hill sequence can be also quantified by the spectral test; there is an MCG equivalent to the Wichmann–Hill method (H. Zeisel 1986; L'Ecuyer and Tezuka 1991).

The author's recommendation on the Wichmann–Hill combination is to

(i) make the modulus of each of the component MCG's safe prime, and

(ii) chose the multipliers of the component MCG's so as to make (a) the period equal to the maximum, (b) the serial correlations of the maximum-period sequences small in absolute value, and (c) the lattice structure of the points from a maximum-period sequence good.

The rest of this paper is organized as follows. In Section 2, we first see the period for a prime-modulus MCG (PMMCG), which can be a component of the Wichmann–Hill method, second an efficiently evaluatable expression for serial correlations of a PMMCG sequence, and then how the quality of the MCG is quantified by the spectral test. In Section 3, we first investigate a necessary and sufficient set of efficiently verifiable conditions, for the period of a Wichmann–Hill sequence to be equal to its maximum, second examine an efficiently evaluatable expression for the serial correlations of the Wichmann–Hill sequences, and then consider how the quality of the Wichmann–Hill method is quantified by the spectral test. Finally in Section 4, we review the results of the paper.

2 THE PRIME-MODULUS MULTIPLICATIVE CONGRUENTIAL GENERATOR

An MCG (multiplicative congruential generator) is determined by three integers

m: the modulus, $m > 2$;
a: the multiplier, $0 < a < m$;
X_0: the initial value, $0 < X_0 < m$.

The case where $m = 2$ is excluded because of its triviality. The sequence $\{ X_n \mid n \geq 0 \}$ of integers in the range $[1, m-1]$ is obtained by the recursion

$$X_n = aX_{n-1} \bmod m \tag{1}$$

for each $n \geq 1$. The corresponding sequence $\{ U_n \mid n \geq 0 \}$ of numbers on the interval $(0, 1)$ is obtained by the normalization

$$U_n = X_n/m \tag{2}$$

for each $n \geq 0$.

We call an MCG whose modulus is a prime number (greater than two) a PMMCG (prime-modulus MCG). Wichmann and Hill's method combines two or more PMMCG's. The value of the modulus m of a PMMCG is usually chosen to be close to the largest integer representable on the computer. The value of the multiplier a affects the period, serial correlations, and lattice structure, of the sequence. The initial value X_0 may be arbitrary, as long as $0 < X_0 < m$.

2.1 The Period

2.1.1 The Period of the Sequence

The sequences $\{ X_n \mid n \geq 0 \}$ and $\{ U_n \mid n \geq 0 \}$ of a PMMCG, defined by (1) and (2), have the same period

$$\lambda \stackrel{\text{def}}{=} \min\{ l \geq 1 \mid X_{n+l} = X_n \text{ for each } n \geq 0 \}.$$

This is called the period for the PMMCG. When the modulus m is fixed, the multiplier a changes the period λ. The period λ is at most $m-1$, which is the maximum period for the PMMCG.

Later in Section 3.1.1, we shall see that it is not necessary that each of the PMMCG's composing the Wichmann–Hill method has its maximum period, for the Wichmann–Hill method to have its maximum period. Thus, we consider the period λ that need not reach the maximum.

Let α designate a primitive element modulo m. Each multiplier a can then be expressed in the form

$$a = \alpha^i \bmod m, \tag{3}$$

where i is a uniquely determined positive integer less than m. The period λ when a in (3) is used for the PMMCG is given by

$$\lambda = (m-1)/\gcd(i, m-1). \tag{4}$$

The greatest common divisor $\gcd(i, m-1)$ can be evaluated efficiently by Euclid's algorithm. Equation (4) states that λ is a divisor of $m-1$, and implies that the maximum period $m-1$ is attained if and only if $\gcd(i, m-1) = 1$.

Consider the case where m is a safe prime number, i.e., where the prime factorization of $m-1$ is expressed as $2 \cdot [(m-1)/2]$. If the exponent $i = m-1$ or $(m-1)/2$, then $\lambda = 1$ or 2, respectively; otherwise $\lambda = m-1$ for i odd and $\lambda = (m-1)/2$ for i even: Approximately half of all the candidate values for the multiplier of the MCG satisfy the maximum-period condition; besides, no multiplier except 1 and $m-1$ has its period less than half of the maximum (Marsaglia and Zaman 1994).

2.1.2 The Period of the Sequence of Non-Overlapping t-tuples

Factors of the maximum period of a random-number sequence are undesirable; they provide periodic subsequences of a maximum-period sequence (Marsaglia and Zaman 1994). The number of prime factors of the maximum period $m-1$ of a PMMCG with modulus m is minimized to be two, if the (prime) modulus m is safe prime. In this case, the period of the sequence of non-overlapping t-tuples from the maximum-period sequence by the PMMCG is equal to $m-1$, the maximum period, for t odd, or equal to $(m-1)/2$, half of the maximum period, for t even, unless t is divisible by $(m-1)/2$.

Consider an example where the modulus of a PMMCG for 32-bit computers is the greatest safe prime number 2147483579 less than 2^{31}. The maximum period for the PMMCG has the prime factorization $2 \cdot 1073741789$; the period of the sequence of non-overlapping t-tuples from the maximum-period sequence by the PMMCG is equal to the maximum period for t odd, or equal to half of the maximum period for t even, unless t is a multiple of 1073741789.

2.2 Serial Correlations

If the serial correlation (sometimes called the serial correlation coefficient)

$$c_s = \frac{(m-1)\sum_{n=0}^{m-2} U_n U_{n+s} - \left(\sum_{n=0}^{m-2} U_n^2\right)}{(m-1)\sum_{n=0}^{m-2} U_n^2 - \left(\sum_{n=0}^{m-2} U_n^2\right)}$$

at lag s of the maximum-period sequence $\{ U_n \mid n \geq 0 \}$ of random numbers obtained by an PMMCG is large in absolute value, then U_n and U_{n+s} are not to be regarded as independent. It is necessary to have serial correlations small in absolute value, though it is not sufficient (Section 3.3.3 of Knuth 1969; Section 7.2 of Niederreiter 1992).

The serial correlation c_1 at lag one can be calculated efficiently: The correlation at lag one has an expression (equation (4.12) of Dieter and Ahrens 1971) for it in terms of the Dedekind sum $\sigma(a, m)$:

$$c_1 = \frac{m\,\sigma(a, m)}{(m-2)(m-1)}.$$

The Dedekind sum $\sigma(a, m)$ can be computed efficiently by some methods (Dieter and Ahrens 1971; exercise 3.3.3–17 of the second edition (1981) of Knuth 1969). (For a definition of the Dedekind sum $\sigma(a, m)$, see Knuth's (1969) definition of a generalized Dedekind sum, with the integer c equal to zero.) Therefore, the correlation at lag one can be evaluated efficiently.

The serial correlation c_s at lag $s \geq 2$ can be calculated efficiently by a method for evaluating a serial correlation at lag one; the lag-s correlation for the multiplier a is equal to the lag-one correlation for another multiplier $a^s \bmod m$.

2.3 Multidimensional Lattice Structure

As George Marsaglia (1968) has indicated, an MCG has a defect that, if overlapping t-tuples $(U_0, U_1, \ldots, U_{t-1})$, $(U_1, U_2, \ldots, U_t)$, $(U_2, U_3, \ldots, U_{t+1}), \ldots$ of random numbers obtained by the MCG are viewed as points in the unit cube of t-dimensional space, then all the points lie in a relatively small number of $(t-1)$-dimensional equidistant parallel hyperplanes. The set of all such points is called a lattice.

The spectral test quantifies the defect of an MCG. In the t-dimensional spectral test to an MCG with the modulus m and the multiplier a, we calculate the maximum distance $d_t(a, m)$ between adjacent hyperplanes, taken over all families of parallel hyperplanes that cover the points in t-dimensional space, and conclude that, the smaller the value of $d_t(a, m)$ is, the more uniformly distributed in t-dimensional space the points are.

Given m, we cannot find a value of a that will make $d_t(a, m)$ less than the right-hand member of the inequality

$$d_t(a, m) \geq d_t^*(m) \stackrel{\text{def}}{=} \gamma_t^{-1/2} m^{-1/t},$$

where γ_t is Hermite's constant (see equation (47) in Chapter 1 of Conway and Sloane 1988). Thus, in order to choose good values of a, we use the measure

$$M_T(a, m) = \min_{2 \leq t \leq T} d_t^*(m)/d_t(a, m)$$

suggested by Fishman and Moore (1986), which is the worst case of the normalized measures of the spectral tests in up-to-T-dimensional space. The value of the Fishman–Moore measure $M_T(a, m)$ lies in the interval $(0, 1]$, and the closer to 1 it is, the better the MCG is thought to be.

The exact value of γ_t when $t \leq 8$ is known, but the exact value when $t > 8$ is unknown, which means that we cannot calculate the exact value of $d_t^*(m)$ when $t > 8$; however, we can calculate a considerably tight lower bound on $d_t^*(m)$ when $8 < t \leq 24$, with the value of C. A. Rogers's (1958) upper bound on the maximum center density of lattice packing, which has been computed by John Leech (1967). (Page 20 of Conway and Sloane (1988) says that, the Rogers bound was the best known for $t \leq 42$ at the time of publication of the book; it seems to the authors that the state of mathematics on the topic has remained the same.)

The values of lower bounds on the maximum center density shown in table 1.2 of Conway and Sloane (1988) affirm that the lower bound on $d_t^*(m)$ when $8 < t \leq 24$ has a relative error less than 6.5%; hence, the bounds on $d_t^*(m)$'s lead to an estimator of (lower bound on) $M_T(a, m)$ whose relative error is also less than 6.5%, when $8 < T \leq 24$.

The spectral test was invented by Coveyou and MacPherson (1967). Their procedure for performing the test has been improved in Section 3.3.4 of the second edition (1981) of Knuth (1969). His procedure for performing the tests in up-to-T-dimensional space takes a time that grows superexponentially as T increases; therefore, when $T > 8$, it is quite slow. Faster procedures have been proposed by Fincke and Pohst (1985) and by Holger Grothe (1988); however, they are numerically unstable, when they are implemented unwarily (L'Ecuyer 1992). The authors wrote a Fortran-77 code for performing the spectral tests by Knuth's procedure, which is numerically stable.

3 THE WICHMANN–HILL METHOD

Consider J PMMCG's with different (prime) moduli $m^{(1)}, m^{(2)}, \ldots, m^{(J)}$. For the jth PMMCG, let $a^{(j)}$ and $X_n^{(j)}$ denote the multiplier and the nth random integer, respectively, and let $\delta^{(j)}$ be a (nonzero) integer with $\gcd(m^{(j)}, |\delta^{(j)}|) = 1$. The Wichmann–Hill method combines the PMMCG's. Their sequence $\{ W_n \mid n \geq 0 \}$ of numbers on the interval $(0, 1)$ is obtained by the formula

$$W_n = \left(\sum_{j=1}^{J} \delta^{(j)} X_n^{(j)} / m^{(j)} \right) \bmod 1$$
$$= \left(\sum_{j=1}^{J} \delta^{(j)} U_n^{(j)} \right) \bmod 1$$

for each $n \geq 0$. Here $U_n^{(j)}$ is the random number on the interval $(0, 1)$ obtained by the jth PMMCG.

3.1 The Period

3.1.1 The Period of the Sequence

Let $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(J)}$ denote the periods for the PMMCG's constituting the Wichmann–Hill method. The period μ for the Wichmann–Hill method is equal to the least common multiple $\mathrm{lcm}(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(J)})$ of $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(J)}$ (cf. lemma Q in Section 3.2.1.2 of Knuth 1969).

Since $\lambda^{(j)}$ is a divisor of $m^{(j)} - 1$, an even number (Section 2), it is true that $\mathrm{lcm}(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(J)})$, which is equal to the period μ, is a divisor of $(m^{(1)} - 1)(m^{(2)} - 1) \ldots (m^{(J)} - 1)/2^{J-1}$; this is the maximum period. The period μ is equal to the maximum, if and

only if

$$\text{lcm}(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(J)}) = \\ = (m^{(1)}-1)(m^{(2)}-1)\ldots(m^{(J)}-1)/2^{J-1}. \quad (5)$$

Whether the moduli $\lambda^{(1)}$, $\lambda^{(2)}$, ..., $\lambda^{(J)}$ of the component PMMCG's satisfy condition (5) or not can be verified efficiently, without calculation of $\text{lcm}(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(J)})$, for condition (5) holds if and only if the following three conditions are satisfied simultaneously.

(i) $\gcd(m^{(j_1)} - 1, m^{(j_2)} - 1) = 2$ for each pair of j_1 and j_2 with $j_1 < j_2$;

(ii) $\lambda^{(j)} = m^{(j)} - 1$ for some j;

(iii) if $(m^{(j)} - 1)/2$ is odd, then $\lambda^{(j)} \geq (m^{(j)} - 1)/2$, otherwise $\lambda^{(j)} = m^{(j)} - 1$, for each j.

Condition (i) guarantees that $(m^{(1)} - 1)/2$, $(m^{(2)} - 1)/2, \ldots$, $(m^{(J)} - 1)/2$ are relatively prime in pairs; it is related to the choice of the moduli $m^{(1)}$, $m^{(2)}$, ..., $m^{(J)}$. Condition (ii) guarantees that at least one of the PMMCG's has its maximum period; it is related to the choice of the multipliers $a^{(1)}$, $a^{(2)}$, ..., $a^{(J)}$. Condition (iii) allows us a possibility of attaining the maximum period for the Wichmann–Hill method by combining PMMCG's, with not each of them having its maximum period; it is related to the choice of both the moduli and the multipliers.

Consider the case where $m^{(1)}$, $m^{(2)}, \ldots, m^{(J)}$ are safe prime numbers. Condition (i) is always satisfied. Whether condition (ii) is satisfied or not can be easily verified, and condition (iii) is satisfied, unless we use a terrible multiplier $a^{(j)} = 1$ or $m^{(j)} - 1$ (see Section 2.1). Approximately $1 - 1/2^J$ of all the candidate vectors composed of J multipliers of the MCG's satisfy the maximum-period condition for the Wichmann–Hill method.

3.1.2 The Period of the Sequence of Non-Overlapping t-tuples

The number of prime factors of the maximum period $(m^{(1)} - 1)(m^{(2)} - 1)\ldots(m^{(J)} - 1)/2^{J-1}$ of the Wichmann–Hill method is minimized to be $J + 1$, if each of the (prime) moduli $\lambda^{(1)}$, $\lambda^{(2)}, \ldots$, $\lambda^{(J)}$ of the PMMCG's composing the Wichmann–Hill method is safe prime, i.e., if $(m^{(1)} - 1)/2$, $(m^{(2)} - 1)/2$, ... $(m^{(J)} - 1)/2$ are prime numbers. In this case, the period of the sequence of non-overlapping t-tuples from a maximum-period sequence by the Wichmann–Hill method is equal to $(m^{(1)}-1)(m^{(2)}-1)\ldots(m^{(J)}-1)/2^{J-1}$, the maximum period, for t odd, or equal to $(m^{(1)} - 1)(m^{(2)} - 1)\ldots(m^{(J)} - 1)/2^J$, half of the maximum period, for t even, if t is divisible by none of $(m^{(1)} - 1)/2$, $(m^{(2)} - 1)/2, \ldots$, or $(m^{(J)} - 1)/2$.

Consider an example where two PMMCG's for 32-bit computers are combined. When the two moduli $m^{(1)}$ and $m^{(2)}$ are the two greatest safe prime numbers 2147483579 and 2147483123 less than 2^{31}, the maximum period for the Wichmann–Hill method has the prime factorization $2 \cdot 1073741561 \cdot 1073741789$; the period of the sequence of non-overlapping t-tuples from a maximum-period sequence by the Wichmann–Hill method is equal to the maximum period for t odd, or to half of the maximum period for t even, if t is neither a multiple of 1073741561 nor a multiple of 1073741789.

3.2 Serial Correlations

The Wichmann–Hill method possesses 2^{J-1} different maximum-period sequences. When the modulus $m^{(j)}$ and the multiplier $a^{(j)}$ of the jth component PMMCG are fixed for each j, choice of the initial values $X_0^{(1)}$, $X_0^{(2)}, \ldots$, $X_0^{(J)}$ determines the realized sequence. A maximum-period sequence obtained by the Wichmann–Hill method might as well be regarded as a random sample from a population with size 2^{J-1}, under a natural assumption that the initial value $X_0^{(j)}$ of the jth component is chosen at random for each j. When all the 2^{J-1} samples, i.e., all the 2^{J-1} maximum-period sequences, are collectively taken into account, their serial correlation e_1 at lag one has an expression for it in terms of $2^J - 1$ Dedekind sums:

$$e_1 = \\ = \frac{\displaystyle\sum_{i=0}^{J-1} \sum_{1 \leq j_1 < j_2 < \cdots < j_{J-i} \leq J} (-1)^i \sigma\left(a, \prod_{k=1}^{J-i} m^{(j_k)}\right)}{\left(4\displaystyle\prod_{j=1}^{J}(1 + 1/m^{(j)}) - 3 - 6/m\right)\displaystyle\prod_{j=1}^{J}(m^{(j)} - 1)},$$

where $m = \prod_{j=1}^{J} m^{(j)}$ and $a = \{a^{(1)}[m/m^{(1)}]^{m^{(1)}-1} + a^{(2)}[m/m^{(2)}]^{m^{(2)}-1} + \cdots + a^{(J)}[m/m^{(J)}]^{m^{(J)}-1}\} \bmod m$; notice that a and m are the multiplier and the modulus, respectively, of the MCG equivalent to the Wichmann–Hill method (Section 3.3). The Dedekind sums can be calculated efficiently (Section 2.2). Accordingly, the correlation e_1 at lag one can be evaluated efficiently.

The serial correlation e_s at lag $s \geq 2$ can be calculated by an efficient method for evaluating a serial correlation at lag one; the lag-s correlation for the multiplier a of the MCG equivalent to the

Wichmann–Hill method is equal to the lag-one correlation for another multiplier $a^s \bmod m$.

3.3 Multidimensional Lattice Structure

As L'Ecuyer and Tezuka (1991) have pointed out, the Wichmann–Hill method is equivalent to an MCG: The sequence $\{ W_n \mid n \geq 0 \}$ obtained by the Wichmann–Hill method is identical to a sequence of numbers on the interval $(0, 1)$ obtained by an MCG with its modulus equal to $\prod_{j=1}^{J} m^{(j)}$, multiplier equal to $\{a^{(1)}[(\prod_{j=1}^{J} m^{(j)})/m^{(1)}]^{m^{(1)}-1} + a^{(2)}[(\prod_{j=1}^{J} m^{(j)})/m^{(2)}]^{m^{(2)}-1} + \cdots + a^{(J)}[(\prod_{j=1}^{J} m^{(j)})/m^{(J)}]^{m^{(J)}-1}\} \bmod \prod_{j=1}^{J} m^{(j)}$, and initial value equal to $W_0 \prod_{j=1}^{J} m^{(j)}$. The equivalence of the Wichmann–Hill method to the MCG enables the quality of the t-dimensional structure of points $(W_0, W_1, \ldots, W_{t-1})$, $(W_1, W_2, \ldots, W_t)$, $(W_2, W_3, \ldots, W_{t+1})$, ...obtained by the Wichmann–Hill method to be quantified by the spectral test to the MCG.

4 CONCLUSIONS

The maximum period of a random-number sequence obtained by the Wichmann–Hill method is achieved if and only if conditions (i), (ii), and (iii) in Section 3.1.1 hold simultaneously. Whether each of the three conditions holds or not can be ascertained efficiently. When the modulus of each of the component PMMCG's is safe prime,

(i) condition (i) in Section 3.1.1 will be always satisfied,

(ii) conditions (ii) and (iii) in Section 3.1.1 will be more easily verifiable, and

(iii) the period of the sequence of non-overlapping t-tuples from a maximum-period sequence by the Wichmann–Hill method will be at least half of the maximum period, with few uncommon exceptions explained in Section 3.1.2.

The serial correlation at lag one of the maximum-period sequences obtained by the Wichmann–Hill method has the expression given in Section 3.2. The expression can be evaluated efficiently. An efficient method of calculating the expression for the serial correlation at lag one is applicable to efficient evaluation of the serial correlation at lag $s \geq 2$.

The quality of the lattice structure of the points from a Wichmann–Hill sequence can be quantified by the Fishman–Moore measure for the spectral tests to the MCG equivalent to the Wichmann–Hill method (Section 3.3). The Fishman–Moore measure can be

(i) computed exactly for the tests in up-to-8-or-lower-dimensional space, and

(ii) estimated with relative error less than 6.5% for the tests in up-to-24-or-lower-dimensional space,

as stated in Section 2.3.

The author's recommendation on finding a Wichmann–Hill combination to be considered a reliable source of random numbers is to

(i) make the modulus of each of the component PMMCG's safe prime, and

(ii) chose the multipliers of the components so as to make (a) the period equal to the maximum, (b) the serial correlations of the maximum-period sequences small in absolute value, and (c) the lattice structure of the points from a maximum-period sequence good.

(Some numerical examples shall be presented at the conference.)

ACKNOWLEDGMENTS

In the last class of a course in stochastic simulation, Professor Pierre L'Ecuyer of the University of Montreal, Canada, distributed copies of a draft of his survey paper entitled "Uniform Random Number Generation," which was published in the *Annals of Operations Research* 53:77–120 (1994), expounded principles of the subject matter, and gave an introduction to some state-of-the-art results, when he served the fall semester as a Visiting Professor, under the Toshiba Chair, in the Graduate School of Science and Engineering at Waseda University, Japan, three years ago; the attendants included the authors. The lecture offered a goodly guide in study of the subject.

The authors are deeply indebted to the two referees; one referee's generous encouragement of the authors and elaborate indication of their typographic errors, together with the other referee's recommendation that the paper be shortened, have contributed substantially to the final draft.

REFERENCES

Bratley, P., B. L. Fox, and L. E. Schrage. 1987. *A guide to simulation.* 2d ed. New York: Springer-Verlag.

Conway, J. H., and N. J. A. Sloane. 1988. *Sphere packings, lattices and groups.* New York: Springer-Verlag.

Coveyou, R. R., and R. D. MacPherson. 1967. Fourier analysis of uniform random number generators. *Journal of the Association for Computing Machinery* 14:100–119.

Dieter, U., and J. Ahrens. 1971. An exact determination of serial correlations of pseudo-random numbers. *Numerische Mathematik* 17:101–123.

Fincke, U., and M. Pohst. 1985. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation* 44:463–471.

Fishman, G. S., and L. R. Moore III. 1986. An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. *SIAM Journal on Scientific and Statistical Computing* (Society for Industrial and Applied Mathematics) 7:24–45.

Grothe, H. 1988. Matrixgeneratoren zur Erzeugung gleichverteilter Pseudozufallsvektoren. Doctoral dissertation, Technische Hochschule Darmstadt, Germany. [Cited by L'Ecuyer (1992).]

Knuth, D. E. 1969. *The art of computer programming.* Volume 2: *Seminumerical algorithms.* Reading, Massachusetts: Addison-Wesley. 2d ed., 1981.

L'Ecuyer, P. 1992. Testing random number generators. In *Proceedings of the 1992 Winter Simulation Conference*, ed. J. J. Swain, D. Goldsman, R. C. Crain, and J. R. Wilson, 305–313. Institute of Electrical and Electronics Engineers, Piscataway, New Jersey.

L'Ecuyer, P., and S. Tezuka. 1991. Structural properties for two classes of combined random number generators. *Mathematics of Computation* 57:735–746.

Leech, J. 1967. Notes on sphere packings. *Canadian Journal of Mathematics* 19:251–267.

Marsaglia, G. 1968. Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences of the United States of America* 61:25–28.

Marsaglia, G., and A. Zaman. 1994. Some portable very-long-period random number generators. *Computers in Physics* 8:117–121.

Niederreiter, H. 1992. *Random number generation and quasi-Monte Carlo methods.* Philadelphia, Pennsylvania: Society for Industrial and Applied Mathematics.

Rogers, C. A. 1958. The packing of equal spheres. *Proceedings of the London Mathematical Society*, series 3, 8:609–620.

Wichmann, B. A., and I. D. Hill. 1982. Algorithm AS 183: An efficient and portable pseudo-random number generator. *Applied Statistics* 31:188–190. Corrected in the same journal 33:123.

Zeisel, H. 1986. A remark on "Algorithm AS 183: An efficient and portable pseudo-random number generator." *Applied Statistics* 35:89.

AUTHOR BIOGRAPHIES

MUNETAKA SAKAMOTO is a graduate student enrolled in a doctoral course of the Department of Industrial Engineering and Management at Waseda University, Shinjuku, Tokyo. He received his M. Eng. degree from Waseda University. His research interests are in the areas of random-number generation and statistical analysis. Mr. Sakamoto is a member of the Operations Research Society of Japan.

SUSUMU MORITO is a Professor in the Department of Industrial Engineering and Management at Waseda University, Shinjuku, Tokyo. He received his Ph. D. degree from Case Western Reserve University, Cleveland, Ohio. His research interests are in the areas of discrete-event simulation, scheduling, and optimization, with great emphasis on their applications in manufacturing. Dr. Morito serves as the secretary of the Special Interest Group on Discrete-Event Simulation, at the Operations Research Society of Japan (ORSJ). He is a member of ACM and of INFORMS, as well as of ORSJ.