Proceedings of the 1992 Winter Simulation Conference
ed. J. J. Swain, D. Goldsman, R. C. Crain, and J. R. Wilson

NEW METHODS FOR PSEUDORANDOM NUMBER AND PSEUDORANDOM VECTOR GENERATION

Harald Niederreiter

Institute for Information Processing
Austrian Academy of Sciences
Sonnenfelsgasse 19
A–1010 Vienna, AUSTRIA

ABSTRACT

We present a brief survey of recent developments in uniform pseudorandom number generation, with an emphasis on nonlinear congruential methods, and we establish some new results on the explicit inversive congruential method. Related developments in the area of uniform pseudorandom vector generation are also mentioned.

1 INTRODUCTION

A crucial task in the application of simulation methods is the generation of random samples that simulate a sequence of i.i.d. random variables sufficiently well. In practice, random samples are generated by a deterministic algorithm, and in this case we speak of pseudorandom numbers. We concentrate on the important case where the target distribution is the uniform distribution on the interval $I = [0, 1]$, i.e., on the case of *uniform pseudorandom numbers.* An expository account of methods for nonuniform random variate generation can be found in the excellent book of Devroye (1986).

Classical methods for the generation of uniform pseudorandom numbers, such as the linear congruential method and shift-register methods, tend to produce pseudorandom numbers with too much intrinsic structure. Recent research has led to the design and the analysis of a family of alternative methods that show great promise. These methods will be at the center of our interest. Further recent work on uniform pseudorandom numbers is surveyed in the articles of James (1990), L'Ecuyer (1990), and Niederreiter (1991) and in the monograph of Niederreiter (1992). Among the interesting new contributions to this area that are not covered in the present paper because of space limitations, we point out in particular the add-and-carry generator of Marsaglia and Zaman (1991) and the work on various types of combined generators by Couture, L'Ecuyer, and Tezuka (1992) and L'Ecuyer and Tezuka (1991).

In Section 2 we briefly review the structural and statistical deficiencies of linear congruential and shift-register pseudorandom numbers. The family of nonlinear congruential methods, which includes the inversive congruential method and the explicit inversive congruential method, is discussed in Section 3, where one can also find some new results on explicit inversive congruential pseudorandom numbers. In Section 4 we turn to uniform pseudorandom vectors, and in Section 5 we draw some conclusions.

2 CLASSICAL METHODS AND THEIR DEFICIENCIES

2.1 Linear Congruential Method

In this method we choose a large integer M and then generate a sequence $y_0, y_1, \ldots$ of integers in $Z_M = \{0, 1, \ldots, M-1\}$ by the recursion

$$y_{n+1} \equiv a y_n + c \bmod M \text{ for } n \geq 0,$$

where a and c are suitable integers. The *linear congruential pseudorandom numbers (LCPRN)* $x_0, x_1, \ldots$ are obtained by the normalization $x_n = y_n/M$ for $n \geq 0$. The least period length $\mathrm{per}(x_n)$ of the sequence of x_n satisfies $\mathrm{per}(x_n) \leq M$, and conditions that guarantee $\mathrm{per}(x_n) = M$ are known.

A detailed description of the structural and statistical properties of LCPRN can be found in Chapter 3 of Knuth (1981). Since the deficiencies of the linear congruential method were already discussed at length in Section 7.3 of Niederreiter (1992), we repeat here only the salient points. A structural deficiency is the unfavorable lattice structure, which results from the fact that all points $\mathbf{y}_n = (y_n, y_{n+1}, \ldots, y_{n+s-1}) \in \mathbf{Z}^s$, $n = 0, 1, \ldots$, lie on a coarse grid or on a union of relatively few such grids (a grid is a shifted sublattice of the s-dimensional integer lattice $\mathbf{Z}^s$). To describe

an important statistical deficiency of LCPRN, we define for any N points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in I^s = [0,1]^s$ their *discrepancy* D_N by

$$D_N = \sup_J |K_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of I^s, $K_N(J)$ is N^{-1} times the number of $0 \le n \le N-1$ with $\mathbf{t}_n \in J$, and $V(J)$ denotes the volume of J. If $x_0, x_1, \ldots$ is a sequence of LCPRN and $s \ge 2$ is a given dimension, then we put $D_N^{(s)}$ for the discrepancy of the points

$$\begin{aligned} \mathbf{x}_n &= (x_n, x_{n+1}, \ldots, x_{n+s-1}) \\ &\in I^s, 0 \le n \le N-1. \end{aligned} \tag{1}$$

According to the law of the iterated logarithm for the discrepancy of random points in I^s, $D_N^{(s)}$ should have an order of magnitude between $N^{-1/2}$ and $N^{-1/2}(\log\log N)^{1/2}$, but e.g. for $N = \mathrm{per}(x_n)$ the order of magnitude of $D_N^{(s)}$ is significantly smaller for the average parameters in the linear congruential method.

2.2 Shift-Register Methods

Shift-register pseudorandom numbers (SRPRN) are generated from higher-order linear recurring sequences modulo 2 which are then transformed by various methods into uniform pseudorandom numbers, such as the digital multistep method and the GFSR method. It is an advantage of shift-register methods that they yield sequences with very long periods. Disadvantages of SRPRN are mentioned in Section 9.2 of Niederreiter (1992). If $x_0, x_1, \ldots$ is a sequence of SRPRN and the points $\mathbf{x}_n \in I^s, s \ge 2$, are defined as in (1), then these points have strong uniformity properties which are expressed e.g. by the "net property" established by Niederreiter (1987). These uniformity properties also lead to the phenomenon that the discrepancy of these points is, on the average, much smaller than it should be according to the law of the iterated logarithm for discrepancies. Thus, on the whole, SRPRN tend to have too regular a distribution in comparison with truly random numbers.

3 NONLINEAR CONGRUENTIAL METHODS

3.1 General Nonlinear Congruential Methods

To overcome the deficiencies of the linear congruential method, the general family of *nonlinear congruential methods* was introduced by Eichenauer, Grothe, and Lehn (1988). In these methods, a large prime modulus p is chosen and a sequence $y_0, y_1, \ldots$ of integers in Z_p is generated by the recursion

$$y_{n+1} \equiv f(y_n) \bmod p \text{ for } n \ge 0, \tag{2}$$

where the function f is selected in such a way that the sequence $y_0, y_1, \ldots$ is purely periodic with least period length $\mathrm{per}(y_n) = p$. Then *nonlinear congruential pseudorandom numbers (NCPRN)* are obtained by setting $x_n = y_n/p$ for $n \ge 0$, and we have $\mathrm{per}(x_n) = p$. If Z_p is identified with the finite field $F_p = \mathbf{Z}/p\mathbf{Z}$ of order p, then we may also describe the y_n by the uniquely determined polynomial $g \in F_p[x]$ such that $y_n = g(n)$ for all $n \in F_p$ and $1 \le d := \deg(g) \le p-2$. The case $d = 1$ yields a trivial generator, hence it is assumed that $2 \le d \le p-2$.

The number d plays a role in the description of structural and statistical properties of NCPRN. It has been shown that a sequence of NCPRN passes the s-dimensional lattice test if and only if $s \le d$. Furthermore, if $D_p^{(s)}$ denotes the discrepancy of the points $\mathbf{x}_n \in I^s, 0 \le n \le p-1$, in (1) obtained from NCPRN, then

$$D_p^{(s)} = O(dp^{-1/2}(\log p)^s) \text{ for } 2 \le s \le d,$$

and as a general bound this is essentially best possible. Note that this behavior of $D_p^{(s)}$ for NCPRN is in better accordance with the law of the iterated logarithm for discrepancies than for the classical methods. An expository account of the results above is given in Chapter 8 of Niederreiter (1992).

3.2 Inversive Congruential Method

The *inversive congruential method* is a special nonlinear congruential method that has received greater attention. The feedback function f in the recursion (2) is now taken to be a self-map f of F_p of the form $f(c) = a\bar{c} + b$ for all $c \in F_p$, where $a, b \in F_p$ are suitable constants and where $\bar{c} \in F_p$ is defined by $\bar{c} = c^{-1}$ if $c \ne 0$ and $\bar{c} = 0$ if $c = 0$. *Inversive congruential pseudorandom numbers (ICPRN)* are derived by putting $x_n = y_n/p$ for $n \ge 0$. This method was introduced by Eichenauer and Lehn (1986). A characterization of those $a, b \in F_p$ which yield $\mathrm{per}(x_n) = p$ was given by Flahive and Niederreiter (1992).

ICPRN pass the s-dimensional lattice test for all $s \le (p+1)/2$, and in the case $p \equiv 3 \bmod 4$ for all $s \le (p+3)/2$. A strong nonlinearity property of ICPRN was established by Eichenauer-Herrmann (1991); compare with Theorem 1 below for an analogous result for a related method. The discrepancy $D_p^{(s)}$ of the points $\mathbf{x}_n \in I^s, 0 \le n \le p-1$, in (1) obtained from ICPRN satisfies $D_p^{(s)} = O(p^{-1/2}(\log p)^s)$,

and $D_p^{(s)}$ is on the average at least of the order of magnitude $p^{-1/2}$ for all $s \geq 2$. This accords well with the law of the iterated logarithm for discrepancies. Detailed surveys of the inversive congruential method can be found in Eichenauer-Herrmann (1992a) and in Section 8.2 of Niederreiter (1992).

3.3 Explicit Inversive Congruential Method

A variant of the inversive congruential method with very attractive features was recently introduced by Eichenauer-Herrmann (1992b). In this *explicit inversive congruential method* we choose $a, b \in F_p$ with $a \neq 0$ and define

$$y_n = \overline{an+b} \quad \text{for } n \geq 0, \tag{3}$$

where $\overline{c} \in F_p$ is defined as in Section 3.2. Then *explicit inversive congruential pseudorandom numbers (EICPRN)* are obtained by setting $x_n = y_n/p$ for $n \geq 0$. This method may also be viewed as a nonlinear congruential method (2) with feedback function $f(c) = \overline{c+a}$ for $c \in F_p$. It is clear that the sequence $x_0, x_1, \ldots$ is purely periodic with $\mathrm{per}(x_n) = p$. Since the y_n are also given by $y_n = (an+b)^{p-2}$ for $n \geq 0$, we have $d = \deg(g) = p-2$, and so a sequence of EICPRN passes the s-dimensional lattice test exactly for all $s \leq p-2$, which is the optimal behavior under the lattice test.

We now establish an analog of the strong nonlinearity property of ICPRN shown by Eichenauer-Herrmann (1991). We consider the general framework of parallel streams of sequences of y_n generated by the formula (3). Thus, for $a_1, \ldots, a_s, b_1, \ldots, b_s \in F_p$ with $a_i \neq 0$ for $1 \leq i \leq s$ we put

$$y_n^{(i)} = \overline{a_i n + b_i} \quad \text{for } 1 \leq i \leq s \text{ and } n \geq 0. \tag{4}$$

Let F_p^s be the s-dimensional affine space over F_p.

THEOREM 1. *If $b_1\overline{a}_1, \ldots, b_s\overline{a}_s \in F_p$ are distinct, then every hyperplane in F_p^s contains at most s of the points $(y_n^{(1)}, \ldots, y_n^{(s)}) \in F_p^s, 0 \leq n \leq p-1$, with $y_n^{(1)} \ldots y_n^{(s)} \neq 0$. If the hyperplane passes through the origin of F_p^s, then it contains at most $s-1$ of these points.*

Proof. Let the hyperplane H in F_p^s be given by $\sum_{j=1}^s c_j z_j = c_0$ with $c_0, \ldots, c_s \in F_p$ and $(c_1, \ldots, c_s) \neq \mathbf{0}$. Let $W = F_p \setminus \{-b_1\overline{a}_1, \ldots, -b_s\overline{a}_s\}$. Then for $n \in W$ we have $(y_n^{(1)}, \ldots, y_n^{(s)}) \in H$ if and only if

$$\sum_{j=1}^{s} \frac{c_j}{a_j n + b_j} = c_0.$$

By clearing denominators, this is equivalent to

$$\sum_{j=1}^{s} c_j \prod_{\substack{i=1 \\ i \neq j}}^{s} (a_i n + b_i) = c_0 \prod_{i=1}^{s} (a_i n + b_i).$$

For $c_0 \neq 0$ this is a polynomial equation of degree s for n which has at most s solutions. If $c_0 = 0$, then from the above we get the polynomial equation

$$\sum_{j=1}^{s} c_j \prod_{\substack{i=1 \\ i \neq j}}^{s} (a_i x + b_i) = 0.$$

The left-hand side has degree $\leq s-1$, thus it suffices to show that the left-hand side is not the zero polynomial. If this were the case, then by considering a fixed k with $c_k \neq 0$ and substituting $x = -b_k\overline{a}_k$ we would obtain

$$\begin{aligned} 0 &= c_k \prod_{\substack{i=1 \\ i \neq k}}^{s} (-a_i b_k \overline{a}_k + b_i) \\ &= c_k \prod_{\substack{i=1 \\ i \neq k}}^{s} a_i \prod_{\substack{i=1 \\ i \neq k}}^{s} (-b_k\overline{a}_k + b_i\overline{a}_i) \neq 0, \end{aligned}$$

a contradiction. □

Eichenauer-Herrmann (1992b) studied the discrepancy of the points

$$\mathbf{x}_n = (x_{n+n_1}, x_{n+n_2}, \ldots, x_{n+n_s}) \in I^s, 0 \leq n \leq p-1,$$

obtained from EICPRN, where $0 = n_1 < n_2 < \ldots < n_s < p$ are integers. We consider, more generally, parallel streams of EICPRN by letting the $y_n^{(i)}$ be as in (4) and putting $x_n^{(i)} = y_n^{(i)}/p$ for $1 \leq i \leq s$ and $n \geq 0$. For $1 \leq N \leq p$ let $D_N^{(s)}$ be the discrepancy of the points

$$\mathbf{v}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in I^s, 0 \leq n \leq N-1.$$

We first consider $N = p$, i.e., the case of the full period which is trivial for $s = 1$.

THEOREM 2. *If $b_1\overline{a}_1, \ldots, b_s\overline{a}_s \in F_p$ are distinct and $2 \leq s < p$, then for $p \geq 5$ we have*

$$D_p^{(s)} \leq 1 - (1-\frac{1}{p})^s + \left(\frac{2s-2}{p^{1/2}} + \frac{s+1}{p}\right) \cdot \left(\frac{4}{\pi^2}\log p + 1.38 + \frac{0.64}{p}\right)^s.$$

Proof. We use the general method and the notation in the proof of Theorem 8.7 in Niederreiter (1992). For $\mathbf{h} = (h_1, \ldots, h_s) \in C_s^*(p)$ put

$$E(\mathbf{h}) = \sum_{n \in F_p} \chi\left(\sum_{i=1}^{s} h_i y_n^{(i)}\right).$$

If W is as in the proof of Theorem 1, then

$$\begin{aligned} |E(\mathbf{h})| &\le s + |\sum_{n \in W} \chi\left(\sum_{i=1}^{s} h_i \overline{a_i n + b_i}\right)| \\ &= s + |\sum_{\substack{n \in F_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right)| \end{aligned}$$

with the rational function

$$\frac{Q(x)}{R(x)} = \sum_{i=1}^{s} \frac{h_i}{a_i x + b_i}.$$

It is easily seen that Q/R is not of the form $A^p - A$ with a rational function A over the algebraic closure of F_p. Thus, it follows from Theorem 2 in Moreno and Moreno (1991) that

$$|E(\mathbf{h})| \le (2s-2)p^{1/2} + s + 1. \tag{5}$$

Since this bound is independent of $\mathbf{h} \in C_s^*(p)$, we can apply Corollary 3.11 in Niederreiter (1992). For a prime modulus $p \ge 5$ the constants in this corollary can be slightly improved by going back to Cochrane(1987), and this yields the desired result. □

THEOREM 3. *If $b_1\overline{a}_1, \ldots, b_s\overline{a}_s \in F_p$ are distinct and $1 \le s < p$, then for $p \ge 5$ and $1 \le N < p$ we have*

$$\begin{aligned} D_N^{(s)} &< 1 - (1 - \frac{1}{p})^s \\ &+ \left(\frac{2s-2}{p^{1/2}} + \frac{s+1}{p}\right)\left(\frac{4}{\pi^2}\log p + 1.38 + \frac{0.64}{p}\right)^s \\ &+ \frac{s}{N}(2p^{1/2}+1)\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) \cdot \\ &\cdot \left(\frac{4}{\pi^2}\log p + 1.38 + \frac{0.64}{p}\right)^s. \end{aligned}$$

Proof. We proceed as in the proof of Theorem 2. For $\mathbf{h} = (h_1, \ldots, h_s) \in C_s^*(p)$ put

$$E_N(\mathbf{h}) = \sum_{n=0}^{N-1} \chi(w_n)$$

with $w_n = \sum_{i=1}^{s} h_i y_n^{(i)}$ for $n \ge 0$. Then

$$E_N(\mathbf{h}) = \sum_{n=0}^{p-1} \chi(w_n) \sum_{t=0}^{N-1} \frac{1}{p} \sum_{u=0}^{p-1} \chi(u(n-t))$$

since the sum over t is 1 for $0 \le n \le N-1$ and 0 for $N \le n \le p-1$. By rearranging terms, we get

$$\begin{aligned} |E_N(\mathbf{h})| \le \frac{N}{p}|E(\mathbf{h})| &+ \frac{1}{p}\sum_{u=1}^{p-1}|\sum_{t=0}^{N-1}\chi(ut)| \\ &\cdot |\sum_{n \in F_p}\chi(w_n + un)|. \end{aligned} \tag{6}$$

For $1 \le u \le p-1$ we have

$$\begin{aligned} |\sum_{n \in F_p}\chi(w_n + un)| &\le s \\ &+ \left|\sum_{\substack{n \in F_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)} + un\right)\right| \end{aligned}$$

with $Q(x)/R(x)$ as in the proof of Theorem 2. Again, it is easily checked that $Q(x)/R(x) + ux$ is not of the form $A^p - A$ with a rational function A over the algebraic closure of F_p, and so it follows from Theorem 2 in Moreno and Moreno (1991) that

$$|\sum_{n \in F_p}\chi(w_n + un)| \le s(2p^{1/2}+1).$$

From Cochrane (1987) we obtain

$$\begin{aligned} &\sum_{u=1}^{p-1}|\sum_{t=0}^{N-1}\chi(ut)| \\ &= \sum_{u=1}^{p-1}|\frac{\sin(\pi uN/p)}{\sin(\pi u/p)}| < \frac{4}{\pi^2}p\log p + (0.38)p + 0.64. \end{aligned}$$

Together with (5) and (6) this yields

$$\begin{aligned} |E_N(\mathbf{h})| &< \frac{N}{p}\left((2s-2)p^{1/2} + s + 1\right) \\ &+ s(2p^{1/2}+1)(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}), \end{aligned}$$

and the proof is completed by invoking Corollary 3.11 in Niederreiter (1992). □

The bounds in Theorems 2 and 3 have the form $D_p^{(s)} = O(p^{-1/2}(\log p)^s)$ and $D_N^{(s)} = O(N^{-1}p^{1/2}(\log p)^{s+1})$, respectively, with absolute implied constants. These bounds show that, under the condition that $b_1\overline{a}_1, \ldots, b_s\overline{a}_s$ are distinct, the corresponding parallel streams of EICPRN are statistically almost independent.

4 PSEUDORANDOM VECTOR GENERATION

4.1 Matrix Method

The trend towards parallelization in simulation methods has led to the necessity of developing algorithms for pseudorandom vector generation. We again restrict the attention to the uniform case, i.e., to the task of generating k-dimensional pseudorandom vectors which simulate a sequence of i.i.d. random vectors with the uniform distribution on I^k as the common distribution function. Only a few methods for uniform pseudorandom vector generation have been developed so far.

The *matrix method* can be viewed as an extension of the linear congruential method. We choose a large prime p and generate a sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ of k-dimensional row vectors with components in F_p by starting from an initial vector $\mathbf{z}_0 \neq \mathbf{0}$ and using the recursion

$$\mathbf{z}_{n+1} \equiv \mathbf{z}_n A \bmod p \text{ for } n \geq 0,$$

where A is a nonsingular $k \times k$ matrix over F_p. Then uniform pseudorandom vectors are obtained by putting $\mathbf{u}_n = p^{-1}\mathbf{z}_n \in I^k$ for $n \geq 0$. We always have $\mathrm{per}(\mathbf{u}_n) \leq p^k - 1$, and a criterion is known which guarantees that $\mathrm{per}(\mathbf{u}_n) = p^k - 1$. The state of our knowledge about the matrix method is summarized in Section 10.1 of Niederreiter (1992). It should not come as a surprise that the pseudorandom vectors generated by this method display the same deficiencies as LCPRN, e.g. the unfavorable lattice structure and too much regularity in their distribution.

4.2 Inversive Method

The *inversive method* is an extension of the inversive congruential method. For a given dimension $k \geq 2$ we choose again a large prime p and we let F_q be the finite field of order $q = p^k$. For $\gamma \in F_q$ we define $\overline{\gamma} \in F_q$ by $\overline{\gamma} = \gamma^{-1}$ if $\gamma \neq 0$ and $\overline{\gamma} = 0$ if $\gamma = 0$. Then we generate a sequence $\gamma_0, \gamma_1, \ldots$ of elements of F_q by the recursion

$$\gamma_{n+1} = \alpha\overline{\gamma}_n + \beta \text{ for } n \geq 0,$$

where $\alpha, \beta \in F_q$ are suitable constants. If $\{\beta_1, \ldots, \beta_k\}$ is a basis of F_q over F_p and Tr denotes the trace from F_q to F_p, then we derive uniform pseudorandom vectors by setting

$$\mathbf{u}_n = \frac{1}{p}(\mathrm{Tr}(\beta_1\gamma_n), \ldots, \mathrm{Tr}(\beta_k\gamma_n)) \in I^k \text{ for } n \geq 0.$$

By an appropriate choice of $\alpha, \beta \in F_q$ we can achieve $\mathrm{per}(\mathbf{u}_n) = q$. The known properties of these pseudorandom vectors are discussed in Section 10.2 of Niederreiter (1992). As is to be expected, there are similarities with the properties of ICPRN.

5 CONCLUSIONS

For uniform pseudorandom number generation, the explicit inversive congruential method looks like a very promising method. It leads to optimal nonlinearity properties, desirable statistical independence properties, and no coarse lattice structure. Furthermore, we can easily generate with this method a large number of parallel streams of pseudorandom numbers that are almost statistically independent; the corresponding problem has not been solved for LCPRN. In the area of uniform pseudorandom vector generation, further studies have to be carried out to provide a sound assessment, but on a preliminary basis the inversive method seems preferable to the matrix method.

REFERENCES

Cochrane, T. 1987. On a trigonometric inequality of Vinogradov. *Journal of Number Theory* 27:9–16.

Couture, R., P. L'Ecuyer, and S. Tezuka. 1992. On the distribution of k-dimensional vectors for simple and combined Tausworthe sequences. *Mathematics of Computation*, to appear.

Devroye, L. 1986. *Non-uniform random variate generation.* New York: Springer.

Eichenauer, J., H. Grothe, and J. Lehn. 1988. Marsaglia's lattice test and non-linear congruential pseudo random number generators. *Metrika* 35: 241–250.

Eichenauer, J., and J. Lehn. 1986. A non-linear congruential pseudo random number generator. *Statistical Papers* 27: 315–326.

Eichenauer-Herrmann, J. 1991. Inversive congruential pseudorandom numbers avoid the planes. *Mathematics of Computation* 56: 297–301.

Eichenauer-Herrmann, J. 1992a. Inversive congruential pseudorandom numbers: a tutorial. *International Statistical Review*, to appear.

Eichenauer-Herrmann, J. 1992b. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Mathematics of Computation*, to appear.

Flahive, M., and H. Niederreiter. 1992. On inversive congruential generators for pseudorandom numbers. In *Proceedings of the International Con-*

ference on Finite Fields (Las Vegas, 1991), to appear.

James, F. 1990. A review of pseudorandom number generators. *Computer Physics Communications* 60: 329–344.

Knuth, D.E. 1981. *The art of computer programming*, vol. 2: *Seminumerical algorithms*. 2nd ed. Reading, MA: Addison-Wesley.

L'Ecuyer, P. 1990. Random numbers for simulation. *Communications of the ACM* 33: no. 10, 85–97.

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

Marsaglia, G., and A. Zaman. 1991. A new class of random number generators. *Annals of Applied Probability* 1: 462–480.

Moreno, C.J., and O. Moreno. 1991. Exponential sums and Goppa codes: I. *Proceedings of the American Mathematical Society* 111: 523–531.

Niederreiter, H. 1987. Point sets and sequences with small discrepancy. *Monatshefte für Mathematik* 104: 273–337.

Niederreiter, H. 1991. Recent trends in random number and random vector generation. *Annals of Operations Research* 31: 323–345.

Niederreiter, H. 1992. *Random number generation and quasi-Monte Carlo methods*. Philadelphia: SIAM.

AUTHOR BIOGRAPHY

HARALD NIEDERREITER is the Director of the Institute for Information Processing at the Austrian Academy of Sciences in Vienna. He is on the editorial board of several journals, including *Mathematics of Computation*, *ACM Transactions on Modeling and Computer Simulation*, and *Applicable Algebra*. His research interests are random number generation, numerical analysis, information theory, number theory, and applied algebra.