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

SOME LINEAR AND NONLINEAR METHODS FOR PSEUDORANDOM NUMBER GENERATION

Harald Niederreiter

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

ABSTRACT

Two principal classes of methods for the generation of uniform pseudorandom numbers can nowadays be distinguished, namely linear and nonlinear methods, and contributions to both types of methods are presented. A very general linear method, the multiple-recursive matrix method, was recently introduced and analyzed by the author. This method includes as special cases several classical methods, and also the twisted GFSR method. New theoretical results on the multiple-recursive matrix method are discussed. Among nonlinear methods, the digital inversive method recently introduced by Eichenauer-Herrmann and the author is highlighted. This method combines real and finite-field arithmetic and, in contrast to other inversive methods, allows a very fast implementation, while still retaining the advantages of inversive methods.

1 INTRODUCTION

Pseudorandom numbers are generated by a deterministic algorithm and should simulate a sequence of i.i.d. random variables sufficiently well. 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*. Recent reviews of the area of uniform pseudorandom number generation can be found in the books of Niederreiter (1992) and Tezuka (1995) and in the survey articles of L'Ecuyer (1994) and Niederreiter (1995c). We also touch upon *uniform pseudorandom vectors*, the parallelized versions of uniform pseudorandom numbers, which are needed in parallelized simulation methods.

Two principal classes of methods for uniform pseudorandom number generation can nowadays be distinguished, namely linear and nonlinear methods. Most classical methods, such as the linear congruential method and shift-register methods, are of the linear type. A very general linear method for uniform pseudorandom number generation, the *multiple-recursive matrix method*, was introduced in Niederreiter (1993) and further analyzed in Niederreiter (1995a). In Section 2 we briefly review this method and then present new theoretical results that improve on earlier theorems. We also explain how the multiple-recursive matrix method can be used for uniform pseudorandom vector generation and discuss results that go beyond those in Niederreiter (1995b) for uniform pseudorandom vectors. A very promising nonlinear method is the *digital inversive method* of Eichenauer-Herrmann and Niederreiter (1994) which is discussed in Section 3. Some conclusions are drawn in Section 4.

We recall the following concepts that form the basis of the *serial test* for uniform pseudorandom numbers and vectors; see Chapter 7 of Niederreiter (1992) for a full treatment of this test. For any N points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in I^s = [0,1]^s$ we define their (*star*) *discrepancy* D_N by

$$D_N = \sup_J |K_N(J) - V(J)|, \tag{1}$$

where the supremum is extended over all subintervals J of I^s with one vertex at the origin, $K_N(J)$ 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 M is a positive integer and the supremum in (1) is extended over all subintervals J of I^s of the form $J = \prod_{i=1}^{s} [a_i/M, b_i/M)$ with integers $0 \le a_i < b_i \le M$ for $1 \le i \le s$, then we arrive at the *discrete discrepancy* $E_{N,M}$ of the points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$.

We use the following notation: for a purely periodic sequence of arbitrary elements $u_n, n = 0, 1, \ldots$, we write $\mathrm{per}(u_n)$ for the least period length of the sequence.

2 MULTIPLE-RECURSIVE MATRIX METHOD

2.1 General Description

The multiple-recursive matrix method for the generation of uniform pseudorandom numbers and vectors was introduced in Niederreiter (1993) and proceeds by vector recursions. The following is a description of the method in a general framework. We choose integers $M \geq 2, k \geq 1$, and $m \geq 1$ as well as $m \times m$ matrices $A_0, A_1, \ldots, A_{k-1}$ with integer entries, and also an m-dimensional row vector $\mathbf{b}$ with integer components. Then we generate a sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ of m-dimensional row vectors with integer components from the set $\{0, 1, \ldots, M-1\}$ by selecting initial vectors $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{k-1}$ and using the kth-order vector recursion

$$\mathbf{z}_{n+k} \equiv \sum_{h=0}^{k-1} \mathbf{z}_{n+h} A_h + \mathbf{b} \bmod M \text{ for } n = 0, 1, \ldots.$$

Specifically, let

$$\mathbf{z}_n = \left(z_n^{(1)}, \ldots, z_n^{(m)}\right) \quad \text{for } n = 0, 1, \ldots.$$

Then a sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers is defined by

$$x_n = \sum_{j=1}^{m} z_n^{(j)} M^{-j} \in I \quad \text{for } n = 0, 1, \ldots. \qquad (2)$$

There is a considerable amount of flexibility in this method: we may either choose M to be a large modulus and m small, or we may take M to be a small modulus and m sufficiently large to obtain a small discretization.

The multiple-recursive matrix method includes as special cases the linear congruential method (take $k = m = 1$), the multiple-recursive congruential method, the GFSR method, and also the twisted GFSR method of Matsumoto and Kurita (1992). The multiple-recursive matrix method is not only an extension of earlier methods, but it also provides a general framework for studying many types of linear pseudorandom number generators.

If we want to use the multiple-recursive matrix method for uniform pseudorandom vector generation, then we generate the sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ of vectors from above with a large modulus M and we derive a sequence $\mathbf{u}_0, \mathbf{u}_1, \ldots$ of m-dimensional pseudorandom vectors by putting

$$\mathbf{u}_n = \frac{1}{M} \mathbf{z}_n \in I^m \quad \text{for } n = 0, 1, \ldots. \qquad (3)$$

With $k = 1$ we get the matrix method for pseudorandom vector generation as a special case.

It is an interesting mathematical problem to analyze the periodicity properties of a sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ generated by a kth-order vector recursion as above. We report here on the results of Niederreiter (1993, 1995a) that have been obtained for the case where the recursion is homogeneous, i.e., where $\mathbf{b} = \mathbf{0}$, and where the modulus M is a prime p. In this case we assume also that the matrix A_0 is nonsingular as a matrix over the finite field F_p of order p and that the initial vectors $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{k-1}$ are not all $\mathbf{0}$. Then the sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ is purely periodic with $\mathrm{per}(\mathbf{z}_n) \leq p^{km} - 1$. It is an important fact that the maximum possible period $\mathrm{per}(\mathbf{z}_n) = p^{km} - 1$ can be achieved by a suitable choice of parameters. It turns out that the sequences $\mathbf{z}_0, \mathbf{z}_1, \ldots$ with $\mathrm{per}(\mathbf{z}_n) = p^{km} - 1$ are determined by a primitive element σ of the finite field F_q of order $q = p^{km}$ and by an m-tuple $B = (\beta_1, \ldots, \beta_m) \in F_q^m$ with the property that the km elements $\beta_j \sigma^{i-1}, 1 \leq i \leq k, 1 \leq j \leq m$, are linearly independent over F_p; compare with Theorem 2 in Niederreiter (1995a). Let $\mathcal{B} = \mathcal{B}(\sigma)$ denote the set of all m-tuples B with this property. The lemma below is crucial for the following.

LEMMA 1. *The cardinality $|\mathcal{B}|$ of the set $\mathcal{B}$ satisfies*

$$|\mathcal{B}| \geq \frac{(p-2)q+1}{p-1} q^{m-1}.$$

2.2 Results on Pseudorandom Numbers

We restrict the attention to the case of the maximum possible period $\mathrm{per}(\mathbf{z}_n) = T := p^{km} - 1$. Let the pseudorandom numbers $x_0, x_1, \ldots$ be defined by (2) with $M = p$; then we also have $\mathrm{per}(x_n) = T$. For a given dimension $s \geq 1$ we consider the points

$$\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in I^s, n = 0, 1, \ldots. \qquad (4)$$

For $s \leq k$ the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{T-1}$ in the full period show an almost perfect equidistribution; see Corollary 3 in Niederreiter (1995a). For $s > k$ the distribution of these points can be described in terms of the *figure of merit* $r^{(s)}(B, \sigma)$ defined by Definition 4 in Niederreiter (1995a). The larger the figure of merit, the more uniform the distribution of these points, according to Theorem 5 in Niederreiter (1995a). The following existence theorem for large figures of merit, whose proof depends on Lemma 1, improves on Theorem 6 in Niederreiter (1995a).

THEOREM 1. *Let $p > 2, m \geq 2$, and $k < s \leq km$. Then for every primitive element $\sigma \in F_q$ there exists*

a $B \in \mathcal{B}$ *with*

$$r^{(s)}(B,\sigma) \geq \min(m, \lfloor km - \log_p \tfrac{p-1}{p-2} - (s-1)\log_p(m+1) \rfloor),$$

where $\lfloor u \rfloor$ *is the greatest integer* $\leq u$ *and* $\log_p$ *denotes the logarithm to the base* p.

For $s > k$ and $1 \leq N \leq T$ let $D_N^{(s)}$ denote the discrepancy of the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ from (4). The following result on the average order of magnitude of $D_N^{(s)}$ improves on Corollaries 4 and 6 in Niederreiter (1995a). The proof depends again on Lemma 1.

THEOREM 2. *Let* $p > 2, m \geq 2$, *and* $k < s \leq km$, *and let* σ *be a primitive element of* F_q. *Then for the corresponding sequences with* $\mathrm{per}(x_n) = T$ *we have on the average*

$$D_T^{(s)} = O\left(p^{-m} + p^{-km}(m \log p)^s\right)$$

and

$$D_N^{(s)} = O\left(p^{-m} + N^{-1} p^{km/2} (\log T)(m \log p)^s\right)$$

for $1 \leq N < T$ *with implied constants depending only on* s, *where the average is taken over all* $B \in \mathcal{B}$.

2.3 Results on Pseudorandom Vectors

Again, we consider only the case of the maximum possible period $\mathrm{per}(\mathbf{z}_n) = T = p^{km} - 1$. Let the m-dimensional pseudorandom vectors $\mathbf{u}_0, \mathbf{u}_1, \ldots$ be defined by (3) with $M = p$; then we also have $\mathrm{per}(\mathbf{u}_n) = T$. For a given dimension $s \geq 1$ we consider the points

$$\mathbf{v}_n = (\mathbf{u}_n, \mathbf{u}_{n+1}, \ldots, \mathbf{u}_{n+s-1}) \in I^{ms}, n = 0, 1, \ldots. \tag{5}$$

For $s \leq k$ the points $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{T-1}$ in the full period show an almost perfect equidistribution; see Theorem 3 in Niederreiter (1995b). For $s > k$ these points display a nontrivial lattice structure. Indeed, it was shown in Theorem 2 in Niederreiter (1995b) that

$$\{\mathbf{0}, \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{T-1}\} = L \cap [0,1)^{ms}$$

with an explicitly given ms-dimensional lattice L.

For $s > k$ there is a *figure of merit* $\varrho^{(s)}(B,\sigma)$ associated with the points in (5), according to Definition 3 in Niederreiter (1995b). In view of Theorem 8 and Corollaries 3 and 4 in Niederreiter (1995b), a larger figure of merit indicates a more uniform distribution of these points. The following existence theorem for large figures of merit, whose proof depends on Lemma 1, improves on Theorem 10 in Niederreiter (1995b).

THEOREM 3. *Let* $p > 2, m \geq 2$, *and* $k < s \leq km$. *Then there exists an effective constant* $d(m,s) > 0$ *depending only on* m *and* s *such that the following holds: if* $(p-2)p^{km} \geq d(m,s)(p-1)$, *then for every primitive element* $\sigma \in F_q$ *there exists a* $B \in \mathcal{B}$ *such that*

$$\varrho^{(s)}(B,\sigma) > \frac{2a}{(\log a)^{ms-1}} \text{ with } a = \frac{(p-2)p^{km}}{b(p-1)},$$

where $b > 0$ *is an effective absolute constant.*

Note that by Theorem 7 in Niederreiter (1995b) we always have $\varrho^{(s)}(B,\sigma) \leq 2p^{km}$. Thus, the figure of merit $\varrho^{(s)}(B,\sigma)$ given by Theorem 3 above has the best possible order of magnitude, up to logarithmic factors.

For $s > k$ and $1 \leq N \leq T$ let $E_{N,p}^{(s)}$ denote the discrete discrepancy of the points $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{N-1}$ from (5). The following result on the average order of magnitude of $E_{N,p}^{(s)}$ improves on Corollaries 1 and 2 in Niederreiter (1995b). The proof depends again on Lemma 1.

THEOREM 4. *Let* $p > 2, m \geq 2$, *and* $k < s \leq km$, *and let* σ *be a primitive element of* F_q. *Then for the corresponding sequences with* $\mathrm{per}(\mathbf{u}_n) = T$ *we have on the average*

$$E_{T,p}^{(s)} = O\left(p^{-km}(\log p)^{ms}\right)$$

and

$$E_{N,p}^{(s)} = O\left(N^{-1} p^{km/2} (\log T)(\log p)^{ms}\right)$$

for $1 \leq N < T$ *with implied constants depending only on* m *and* s, *where the average is taken over all* $B \in \mathcal{B}$.

3 DIGITAL INVERSIVE METHOD

Inversive methods for the generation of uniform pseudorandom numbers rely on the operation of multiplicative inversion in modular arithmetic or in finite fields to create pseudorandomness. An expository account of such methods can be found in Chapter 8 of Niederreiter (1992), and an up-to-date survey is given in Niederreiter (1995c). Inversive methods lead to pseudorandom numbers with very attractive properties, but until recently these methods suffered from the disadvantage that the generation algorithms are relatively slow. Although pseudorandom number generation is usually not the bottleneck in calculations for simulation methods, it would still be desirable to find a faster inversive method. Such a method is now available in the form of the *digital inversive method* due to Eichenauer-Herrmann and Niederreiter (1994).

We select a precision $k \geq 1$ and let F_q be the finite field of order $q = 2^k$. We denote by F_q^* the multiplicative group of nonzero elements of F_q. For $\gamma \in F_q^*$ let $\bar{\gamma} = \gamma^{-1} \in F_q^*$ be the multiplicative inverse of γ in F_q^* and define $\bar{\gamma} = 0 \in F_q$ for $\gamma = 0 \in F_q$. Now we choose parameters $\alpha \in F_q^*$ and $\beta \in F_q$ and an initial value $\gamma_0 \in F_q$, and then we generate the sequence $\gamma_0, \gamma_1, \ldots$ of elements of F_q by the recursion

$$\gamma_{n+1} = \alpha\bar{\gamma}_n + \beta \quad \text{for } n = 0, 1, \ldots.$$

Next, we choose an ordered basis C of F_q over F_2 and we let

$$\mathbf{c}_n = \left(c_n^{(1)}, \ldots, c_n^{(k)}\right) \quad \text{for } n = 0, 1, \ldots$$

be the coordinate vector of $\gamma_n \in F_q$ relative to C. Note that the $c_n^{(j)}$ are bits. Now a sequence $x_0, x_1, \ldots$ of *digital inversive pseudorandom numbers* is defined by

$$x_n = \sum_{j=1}^{k} c_n^{(j)} 2^{-j} \in I \quad \text{for } n = 0, 1, \ldots. \tag{6}$$

This sequence is purely periodic, and we have $\mathrm{per}(x_n) = q$ if and only if $x^2 - \beta x - \alpha$ is a so-called IMP polynomial over F_q. We note that any primitive quadratic polynomial over F_q is an IMP polynomial over F_q.

This method can be implemented in a fast manner because of an efficient algorithm due to Itoh and Tsujii (1988) for the calculation of multiplicative inverses in F_q. For $\gamma \in F_q^*$ we have

$$\gamma^{-1} = \gamma^{q-2} = \left(\gamma^{2^{k-1}-1}\right)^2,$$

and so it suffices to describe how to compute powers of the form γ^{2^m-1}. The idea is to reduce the calculation of γ^{2^m-1} to that of $\gamma^{2^{\lfloor m/2 \rfloor}-1}$. This is achieved by the identities

$$\gamma^{2^m-1} = \left(\gamma^{2^{m/2}-1}\right)^{2^{m/2}} \gamma^{2^{m/2}-1} \text{ for even } m,$$

$$\gamma^{2^m-1} = \left(\gamma^{2^{(m-1)/2}-1}\right)^{2^{(m+1)/2}} \left(\gamma^{2^{(m-1)/2}-1}\right)^2 \gamma$$

for odd m.

Note that the second of these identities was not printed correctly in Eichenauer-Herrmann and Niederreiter (1994). This paper provides further details on the implementation of the digital inversive method.

If the pseudorandom numbers $x_0, x_1, \ldots$ are as in (6), then the discrepancy $D_q^{(s)}$ of the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{q-1}$ given by (4) satisfies

$$D_q^{(s)} = O\left(k^s q^{-1/2}\right) \quad \text{for } s \geq 2$$

with an absolute implied constant. On the other hand, for a positive fraction of the possible parameters, $D_q^{(s)}$ is at least of the order of magnitude $q^{-1/2}$ for $s \geq 2$. These results of Eichenauer-Herrmann and Niederreiter (1994) demonstrate that digital inversive pseudorandom numbers show a satisfactory behavior under the s-dimensional serial test.

4 CONCLUSIONS

The results in Section 2 indicate that there are choices of m-tuples $B \in \mathcal{B}$ such that the corresponding pseudorandom numbers and vectors generated by the multiple-recursive matrix method have strong statistical independence properties, in the sense of a very uniform s-tuple distribution. The discussion in Section 3 shows that there is an inversive method which can be implemented in a fast manner, namely the digital inversive method. The digital inversive method shares the attractive properties of inversive methods with regard to the serial test. In particular, parameters in the digital inversive method that guarantee the maximum possible period q also guarantee a good performance under the serial test.

REFERENCES

Eichenauer-Herrmann, J., and H. Niederreiter. 1994. Digital inversive pseudorandom numbers. *ACM Transactions on Modeling and Computer Simulation* 4: 339–349.

Itoh, T., and S. Tsujii. 1988. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. *Information and Computation* 78: 171–177.

L'Ecuyer, P. 1994. Uniform random number generation. *Annals of Operations Research* 53: 77–120.

Matsumoto, M., and Y. Kurita. 1992. Twisted GFSR generators. *ACM Transactions on Modeling and Computer Simulation* 2: 179–194.

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

Niederreiter, H. 1993. Factorization of polynomials and some linear-algebra problems over finite fields. *Linear Algebra and Its Applications* 192: 301–328.

Niederreiter, H. 1995a. The multiple-recursive matrix method for pseudorandom number generation. *Finite Fields and Their Applications* 1: 3–30.

Niederreiter, H. 1995b. Pseudorandom vector generation by the multiple-recursive matrix method. *Mathematics of Computation* 64: 279–294.

Niederreiter, H. 1995c. New developments in uniform pseudorandom number and vector generation. In

Monte Carlo and quasi-Monte Carlo methods in scientific computing, ed. H. Niederreiter and P.J.-S. Shiue. Berlin: Springer-Verlag, to appear.

Tezuka, S. 1995. *Uniform random numbers: theory and practice*. Norwell, MA: Kluwer Academic Publishers.

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*, *Acta Arithmetica*, and *Applicable Algebra*. His research interests are random number generation, numerical analysis, information theory, number theory, and applied algebra.