Proceedings of the 1990 Winter Simulation Conference
Osman Balci, Randall P. Sadowski, Richard E. Nance (eds.)

LATTICE STRUCTURE OF PSEUDORANDOM SEQUENCES FROM SHIFT-REGISTER GENERATORS

Shu Tezuka

IBM Research, Tokyo Research Laboratory
5-19, Sanbancho, Chiyoda-ku, Tokyo 102, Japan

ABSTRACT

In this paper, we develop a theory of the lattice structure of pseudorandom sequences from shift register generators, i.e., Tausworthe sequences and GFSR(Generalized Feedback Shift Register) sequences. First, we define an analog of linear congruential sequences in $GF\{2,x\}$, the field of all Laurent series over the Galois Field of two elements $GF(2)$, and show that this class of sequences contains as a subclass the Tausworthe sequence. We then derive a theorem that links the k-distribution of such sequences and the successive minima of the k-dimensional lattice over $GF\{2,x\}$ associated with the sequences, thereby leading to the geometric interpretation of the lattice structure in the k-dimensional unit space of these sequences. By generalizing this result, we define the successive minima for the point set of k-dimensional vectors each consisting of k consecutive terms of GFSR sequences, and show that GFSR sequences have a similar structure to that of Tausworthe sequences. Finally, we give an example of a simulation problem in which shift-register-type pseudorandom sequences yield useless results due to such lattice structures.

1. INTRODUCTION

Pseudorandom sequences from shift register generators have long been used for Monte Carlo simulations, since the sequences can be quickly generated in a computer. Two typical types of sequences are currently used: the Tausworthe sequence and the GFSR(Generalized Feedback Shift Register) sequence. Although a theory on the randomness, in particular the k-dimensional distribution(henceforth, k-distribution) of these sequences has just recently been developed [Fushimi 1988; Fushimi and Tezuka 1983; Niederreiter 1987, 1988; Tezuka 1987a, b, 1988], there still remains a major open problem: *What kind of structure underlies these sequences?* Some researchers [Fishman 1978; Marsaglia 1976; Ripley 1987] have suspected that these sequences have a structure similar to the lattice structure of linear congruential sequences discovered by Marsaglia[1968], and have pointed out some examples of irregular patterns in the two dimensional plot of the points produced from the consecutive terms of this type of sequence, for example, see Figure 1.

The objective of this paper is to give a solution to this long open problem in the field of random number generation for discrete-event simulations. The paper is organized as follows. Section 2 briefly overviews the definitions of pseudorandom sequences from shift register generators, i.e., Tausworthe sequences and GFSR sequences. In Section 3, first, we define an analog of linear congruential sequences in $GF\{2,x\}$, the field of all Laurent series over the Galois Field of two elements $GF(2)$, and show that it contains Tausworthe sequences as its special case. Then we give the key theorem that links the k-distribution of such sequences and the successive minima of the k-dimensional lattice over $GF\{2,x\}$ associated with the sequences, thereby leading to the geometric interpretation of the lattice structure of these sequences. In Section 4, on the basis of the results obtained in the foregoing sections, we define the 'successive minima' of the point set produced from the consecutive terms of GFSR sequences, and show that GFSR sequences have a similar structure to that of Tausworthe sequences. Section 5 discusses an example of a simulation problem for which these kinds of pseudorandom sequences produce completely useless results due to their intrinsic structure.

2. DESCRIPTION OF SHIFT-REGISTER-TYPE PSEUDORANDOM SEQUENCES

First, we introduce the definition of shift register sequences. A binary sequence $\{a_i\}$ is called a (p-th order) linear feedback shift register sequence if the sequence is generated by a linear recurrence relation

$$a_i \;=\; c_{p-1}a_{i-1} + \cdots + c_0 a_{i-p}, \quad (\text{mod } 2)$$

where c_i is 0 or 1, for $i = 0, ..., p-1$, and $\{a_i\}$ is a binary sequence. Note that $a_1, ..., a_p$ are initial values for the recurrence. The polynomial,

$$f(x) \;=\; x^p + c_{p-1}x^{p-1} + \cdots + c_1 x + c_0,$$

is called the characteristic polynomial of the shift register sequence. If the characteristic polynomial is chosen to be a primitive polynomial over $GF(2)$, then the period length of the sequence becomes $2^p - 1$, provided that the initial values are not all zero. Therefore, we assume hereafter that $f(x)$ is primitive and that the initial values are not all zero.

A Tausworthe sequence $\{u_i\}$, a sequence of numbers in $[0,1)$, is constructed as follows [Bratley et al. 1987; Tausworthe 1965]:

$$u_i = \sum_{l=1}^{L} a_{is+l} 2^{-l},$$

where L is an integer, usually chosen to be the word size of a computer, and s is an integer $0 < s < 2^p - 1$ with $gcd(s, 2^p - 1) = 1$. Note that the digital multistep pseudorandom numbers over $GF(2)$ defined by Niederreiter[1988] are a special case of Tausworthe sequences, i.e., $0 < s = L \leq p$.

A GFSR sequence is defined as follows [Lewis and Payne 1973]:

$$u_i = \sum_{l=1}^{L} a_{j_l+i} 2^{-l}.$$

Note that $L \leq p$ (otherwise, a linear dependence relation appears between the column bits of u_i). Originally, Lewis and Payne set j_l to be $l \cdot d$, where d is a constant, and suggested that d should be greater than $100p$. In addition, they employed a primitive trinomial for the characteristic polynomial of $\{a_i\}$ in order to realize a fast generation scheme for the sequence in the following way: Let $f(x) = x^p + x^q + 1$. Then the sequence can be generated by the scheme

$$u_i = u_{i-q} \text{ .XOR. } u_{i-p}.$$

In this paper, we assume that $j_l, l = 1, ..., L$, are integers between 0 and $2^p - 1$ and that $f(x)$ is a primitive polynomial.

The matrix representation of GFSR sequences is very useful for the analysis to be carried out in Section 4. Let C be the companion matrix of the polynomial $f(x)$, namely,

$$C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \cdots & \cdots & \cdots & \\ & \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & \cdots & c_{p-1} & 1 \end{pmatrix},$$

and let α be a non-zero binary column vector. Then the GFSR sequence is written as follows:

$$G\alpha, GC\alpha, ..., GC^i\alpha, ...,$$

where G is a $L \times p$ matrix over $GF(2)$ whose i-th row vector, denoted by G_i, is uniquely determined by the equations

$$a_{j_l+i} = (G_l, C^{i-1}\alpha), \text{ for } i = 1, ..., p.$$

Here (α, β) means the inner-product of binary vectors α and β over $GF(2)$. Note that Tausworthe sequences can be written as a special case of GFSR sequences.

3. LATTICE STRUCTURE OF TAUSWORTHE SEQUENCES

3.1 Definition of Linear Congruential Generators in $GF\{2, x\}$

Here we define an analogous version of linear congruential sequences in $GF\{2, x\}$. This generator is formulated as follows: let σ be a mapping from $GF\{2, x\}$ to the real field defined as

$$\sigma\left(\sum_{i=-\infty}^{m} a_i x^i\right) = \sum_{i=-\infty}^{m} a_i 2^i,$$

where a_i is in $GF(2)$. Then a pseudorandom sequence $u_i, i = 1, 2, ...$, in [0,1) is given as

$$\begin{aligned} f_i(x) &= g(x)f_{i-1}(x) + h(x) \pmod{M(x)} \\ u_i &= \sigma(f_i(x)/M(x)), \end{aligned} \tag{1}$$

where $g(x), h(x), M(x)$ and $f_i(x)$ are polynomials in $GF\{2, x\}$. In practical situations, u_i is expressed approximately by its truncated value due to the word-size limitation.

In what follows, we show that Tausworthe sequences are a special case of the above general class. Let $M(x)$ be a primitive polynomial, $g(x) = x^s \pmod{M(x)}$ with $0 \leq s < 2^p - 1$, $h(x) = 0$, and L be the word-size. Then, for $i = 1, 2, ...$, the sequence is given as

$$u_i = \sum_{l=1}^{L} a_{is+l} 2^{-l},$$

where $\{a_i\}$ is a binary sequence generated by a linear recurrence relation whose characteristic polynomial is $M(x)$. Clearly, this is equivalent to the definition of Tausworthe sequences.

3.2 A Theorem on the K-distribution of Linear Congruential Sequences in $GF\{2, x\}$

In this subsection, we present a theorem that links the k-distribution of the sequences defined in (1) with the successive minima and reduced basis of a lattice in the vector space over $GF\{2, x\}$. The k-distribution of a sequence $\{u_i\}$ is concerned with the uniform distribution of the d-bit k-tuple $([u_i]_d, ..., [u_{i+k-1}]_d)$, where $[u_i]_d$ is the leading d bits of u_i.

Definition 1 *A sequence $\{u_i\}$ with period $2^p - 1$ is k-distributed with d-bit resolution if every d-bit k-tuple appears 2^{p-kd} times over the whole period, except for one d-bit k-tuple, which appears one time less.*

Consider the k-tuples $(f_i(x)/M(x), ..., f_{i+k-1}(x)/M(x)), i = 1, 2, ...$, produced by (1). These are expressed by the lattice $L_k + \lambda$, where the basis of L_k is given as

$$\begin{aligned} e_1 &= \frac{1}{M(x)}(1, g(x), g^2(x), ..., g^{k-1}(x)), \\ e_2 &= (0, 1, 0, ..., 0), \\ &\vdots \\ e_k &= (0, 0, 0, ..., 1), \end{aligned}$$

and $\lambda = \frac{h(x)}{M(x)}(0, 1, 1 + g(x), ...)$. Hereafter, we call L_k the lattice associated with a sequence defined in (1). Let L_k^* be the dual of L_k. Then the basis for L_k^* is given as

$$\begin{aligned} e_1^* &= (M(x), 0, 0, ..., 0), \\ e_2^* &= (g(x), 1, 0, ..., 0), \\ \vdots &\quad \vdots \\ e_k^* &= (g^{k-1}(x), 0, 0, ..., 1). \end{aligned}$$

Define the norm $|\alpha|$ of a vector $\alpha = (a_1, ..., a_k)$ as $\max\{deg(a_i) : 1 \leq i \leq k\}$. The notions of reduced basis and successive minima of a lattice L in a vector space over $GF\{2, x\}$ are defined as follows [Lenstra 1985]:

Definition 2 *For $1 \leq j \leq k$, a j-th successive minimum $|b_j|$ of L is recursively defined as the norm of a vector of a smallest norm in L that is linearly independent of $b_1, b_2, ..., b_{i-1}$ over $GF\{2, x\}$, and the basis $b_1, b_2, ..., b_k$ is called a reduced basis of L.*

We obtained the following theorem[Tezuka 1989]. (For the reader's convenience, the proof is added.)

Theorem 1 *A sequence with the maximum possible period $2^p - 1$ defined by (1) is k-distributed with d-bit resolution if and only if the k-th successive minimum of the lattice L_k is at most $-d$.*
Proof. From the theory of uniform distribution of sequences in $GF\{q, x\}$ [Kuipers and Niederreiter 1974], a sequence defined in (1) of length $2^p - 1$ is k-distributed with d bit resolution if and only if, for any nonzero $(s_1(x), ..., s_k(x))$ with $deg(s_i) < d$,

$$\begin{aligned} &\sum_{deg(n) < p} \Pi_{i=1}^{k} e\left(s_i(x)\frac{n(x)g^{i-1}(x)}{M(x)}\right) \\ = &\sum_{deg(n) < p} e\left(n(x)\frac{\sum_{i=1}^{k} g^{i-1}(x)s_i(x)}{M(x)}\right) \\ = &\ 0. \end{aligned}$$

Here $e(\alpha)$ denotes the character of α in $GF\{2, x\}$ defined as

$$e(\alpha) = (-1)^{a_1},$$

where a_1 is the coefficient of x^{-1} in the expression for α. Let l be the norm of a nonzero shortest vector of the lattice L_k^*. Then, from the definition of L_k^*, l is given as the minimum norm of the nonzero solutions of

$$\sum_{i=1}^{k} g^{i-1}(x)s_i(x) = 0 \pmod{M(x)}.$$

This is equivalent to the following: for any nonzero $(s_1(x), ..., s_k(x))$ with $deg(s_i) < d \leq l$,

$$\sum_{i=1}^{k} g^{i-1}(x)s_i(x) \neq 0 \pmod{M(x)}.$$

Recall Mahler's[1941] theorem that $|\beta_i| + |\alpha_{k-i+1}| = 0$, for $i = 1, ..., k$, where $\alpha_1, ..., \alpha_k$ and $\beta_1, ..., \beta_k$ are reduced bases of a lattice in a vector space over $GF\{2, x\}$ and of its dual, respectively. From this theorem it follows that $-l$ is equal to the k-th successive minimum of the lattice L_k. Thus the proof is complete.□

Lenstra[1985] presented a basis reduction algorithm in $GF\{q, x\}$ that runs in time polynomial in the size of data and the dimensions. Since this algorithm works with respect to the maximum norm of a vector over $GF\{q, x\}$, it can be applied to examining the k-distribution of the sequences defined in (1).

3.3 Geometric Interpretation of Theorem 1

For brevity, we consider the two-dimensional case. Let $S(l)$ be an equidissection of the two-dimensional unit space defined as

$$S(l) = \{J(l,i,j) | 0 \leq i,j < 2^l\},$$

where $J(l,i,j)$ is a subinterval $[i2^{-l},(i+1)2^{-l}) \times [j2^{-l},(j+1)2^{-l})$, for $0 \leq i,j < 2^l$. Let α_1,α_2 be the reduced basis of the lattice L_2. Since $|\alpha_1| \leq |\alpha_2|$, each cell of the equidissection $S(-|\alpha_2|-1)$ contains $2^{p+2|\alpha_2|}$ quadrilaterals, each consisting of four lattice points P_1, P_2, P_3, P_4 specified as $P_2 = P_1 \oplus \sigma(\alpha_1)$, $P_3 = P_1 \oplus \sigma(\alpha_2)$, $P_4 = P_1 \oplus \sigma(\alpha_1) \oplus \sigma(\alpha_2)$, where $\oplus$ is the bit-wise exclusive-or operation of the corresponding coordinates and $\sigma(\alpha)$ means a point $(\sigma(\alpha_x),\sigma(\alpha_y))$ for a vector $\alpha = (\alpha_x, \alpha_y)$. Theorem 1 claims that every cell of the equidissection $S(-|\alpha_2|)$ contains an equal number of points, namely, $2^{p+2|\alpha_2|}$, and that the point set cannot be evenly distributed into smaller cells of the equidissections $S(k)$ for $k > -|\alpha_2|$.

Figure 1 shows the point set produced by the Tausworthe sequence, $u_i = \sum_{j=1}^{6} a_{4i+j}2^{-j}$, where $\{a_i\}$ follows the recurrence relation $a_i = a_{i-5} + a_{i-6} \pmod 2$, and Figure 2 gives an example of the equidissection $S(2)$ of the unit space. As is easily seen, each cell of $S(1)$ contains four quadrilaterals consisting of 16 points in the point set, and each cell of the equidissection $S(2)$ contains four points. Furthermore, none of the equidissections $S(k), k > 2$, can evenly divide the point set. Here, $\alpha_1 = (.0001, .000011)$ and $\alpha_2 = (.000001, .01)$ in the binary representation.

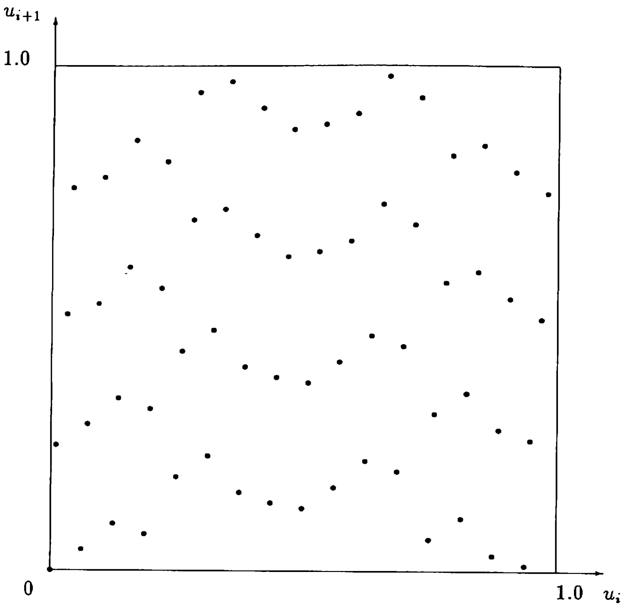

Figure 1. A set of two-dimensional points, $(u_i, u_{i+1}), i = 1, ..., 63$, produced by the Tausworthe sequence, $u_i = \sum_{j=1}^{6} a_{4i+j}2^{-j}$, where $\{a_i\}$ follows the recurrence relation $a_i = a_{i-5} + a_{i-6} \pmod 2$

4. LATTICE STRUCTURE OF GFSR SEQUENCES

In this section, we show that the result obtained in the preceding section can be extended to GFSR sequences. First, we define the successive minima of the point set produced by the consecutive terms of GFSR sequences. Let $L(m_1, ..., m_k)$ be the set of row vectors, $\{G_iC^{j-1} | 1 \leq i \leq m_j, 1 \leq j \leq k\}$.

Definition 3 *The first successive minimum l_1 is defined as the smallest l such that $L(l+1, ..., l+1)$ is not of full rank. The j-th successive minimum l_j is defined as the smallest $l > l_{j-1}$, if any, over all permutations $(m_1, ..., m_k)$ of $(l_1, ..., l_{j-1}, l+1, ..., l+1)$ such that $L(m_1, ..., m_k)$ is not of full rank; otherwise $l_j = l_{j-1}$.*

We can then show that the above definition is a natural extension of the successive minima of the dual lattice associated with Tausworthe sequences. The following theorem describes it:

Theorem 2 *The successive minima of the dual lattice associated with a Tausworthe sequence are identical with those of the GFSR sequence that is defined as a sequence of the leading p bits of each term of the Tausworthe sequence.*

Proof. This follows from the fact that p-bit Tausworthe sequences constitute a subclass of GFSR sequences. □

Note that the theorem on the k-distribution of GFSR sequences obtained in [Fushimi and Tezuka 1983; Tezuka 1987a] can be restated in terms of the successive minima defined above.

Proposition 1 *A necessary and sufficient condition for GFSR sequences to be k-distributed with l bit resolution is that $l_1 \geq l$.*

We should notice the following difference of the successive minima defined above from the original ones:

Proposition 2 *For GFSR sequences, we have $l_1 + \cdots + l_k \leq p$, whereas the equality always holds for Tausworthe sequences.*

The above considerations lead us to the conclusion that GFSR sequences also have a lattice structure similar to that of Tausworthe sequences. For GFSR sequences, the basis vectors corresponding to the successive minima are defined as follows: Denote $L = l_1 + \cdots + l_k - k$, let A be a $L \times p$ binary matrix, and define the i-th row vector of A as G_mC^h, where $m = i -$

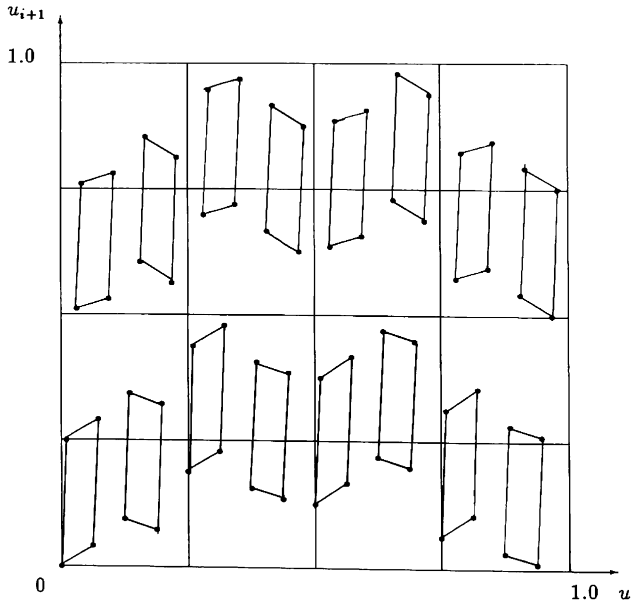

Figure 2. Sixteen quadrilaterals from the same point set as in Figure 1 divided by the equidissection $S(2)$

$\sum_{j=1}^{h-1}(l_j - 1)$ if $\sum_{j=1}^{h-1}(l_j - 1) < i \leq \sum_{j=1}^{h}(l_j - 1)$ for $1 \leq h \leq k$. Assume $l_1 + \cdots + l_k = p$, and denote the linearly independent nonzero solutions of the linear equation $Ax = 0$ by $x_1, ..., x_k$ such that the successive minimum l_i corresponds to the norm of the k-dimensional vector defined as $(GCx_i, ..., GC^k x_i)$, for $i = 1, ..., k$. These k-dimensional vectors can be regarded as the basis vectors for the lattice associated with GFSR sequences. Note that when $l_1 + \cdots + l_k < p$, multiple vectors correspond to each of the successive minima.

Consider, for example, the two-dimensional case. Since C is the companion matrix of a primitive polynomial, we can put one of nonzero solutions as $x_1 = C^{s_1} x_0$, where x_0 is a fixed nonzero binary vector and s_1 is a properly chosen integer. A point $(GC^l x_0, GC^{l+1} x_0)$ from a GFSR sequence has as one of its neighbors $(GC^l x_0, GC^{l+1} x_0) + (GCx_1, GC^2 x_1) = (G(C^{l-1} + C^{s_1})Cx_0, G(C^{l-1} + C^{s_1})C^2 x_0) = (G(C^d)Cx_0, G(C^d)C^2 x_0)$, where d is uniquely determined because the characteristic polynomial of C is primitive. Since the point $(GC^{d+1} x_0, GC^{d+2} x_0)$ is a different point from the same GFSR sequence, it becomes clear that GFSR sequences have a similar structure to that of Tausworthe sequences.

5. DISCUSSION

From the results obtained in the foregoing sections, we can show that in the following simulation problem shift-register-type pseudorandom sequences produce completely useless results because of their lattice structure. Consider a problem of distributing n points $P_i, i = 1, ..., n$, randomly in the k-dimensional unit space. Define the *distance* of two points as $d(P_i, P_j) = \max_{1 \leq l \leq k} |X_{il} \text{ .XOR. } X_{jl}|$, where $P_i = (X_{i1}, ..., X_{ik})$ and $|X|$ is defined to be i if $2^i \leq X < 2^{i+1}$. If the point set is uniformly and independently distributed in the k-dimensional unit space, then the minimum distance $d_n = \min_{1 \leq i \neq j \leq n} d(P_i, P_j)$ has the following distribution for small t:

$$\begin{aligned} Pr(d_n < t) &= 1 - Pr(d_n \geq t) \\ &= 1 - Pr(d_{n-1} \geq t) \times (Pr(d_2 \geq t))^{n-1} \\ &= 1 - \prod_{i=1}^{n-1} (1 - 2^{kt})^i \\ &\approx 1 - \prod_{i=1}^{n-1} (1 - i2^{kt}) \\ &\approx 1 - exp(-(\frac{n(n-1)2^{kt}}{2})(1 + \frac{(2n-1)2^{kt}}{6})). \end{aligned}$$

In other words, the probability of d_n being small for large n is non-negligible. Nevertheless, when the k-consecutive terms from a shift-register pseudorandom sequence with period $2^p - 1$ constitute the k-dimensional points, the distance d_n is always no smaller than $-\lceil p/k \rceil$, assuming that their k-distribution is good(i.e.,$l_1 + \cdots + l_k = p$ and $l_k = \lceil p/k \rceil$). For instance, if $p = 30$ and $k = 5$, then $d_n \geq -6$, for any $n \geq 1$, in the case of the points from shift register generators with good k-distribution, whereas $Pr(d_n < -6) \approx 1$, for $n \geq 50000$, in the case of genuinely random points. Therefore, we can say that the use of shift-register-type pseudorandom sequences with medium-sized period lengths should be avoided in this kind of simulation problem.

REFERENCES

Bratley, P., B.L. Fox, and L.E. Schrage (1987), *A Guide to Simulation*, Second Edition, Springer-Verlag, New York, NY.

Fishman, G.S. (1978), *Principles of Discrete Event Simulation*, Wiley, New York, NY.

Fushimi, M. (1988), "Designing a Uniform Random Number Generator Whose Subsequences are K-distributed," *SIAM Journal on Computing, 17*, 89-99.

Fushimi, M. and S. Tezuka (1983), " The K-distribution of Generalized Feedback Shift Register Pseudorandom Numbers," *Communications of the ACM, 26*, 516-523.

Knuth, D.E. (1981), *The Art of Computer Programming: Vol. 2, Seminumerical Algorithms*, Second Edition, Addison-Wesley, Reading, MA.

Kuipers, L. and H. Niederreiter (1974), *Uniform Distribution of Sequences*, Wiley, New York, NY.

Lenstra, A.K. (1985), "Factoring Multivariate Polynomials over Finite Fields," *Journal of Computer and System Sciences, 30*, 235-248.

Lewis, T.G. and W.H. Payne (1973), "Generalized Feedback Shift Register Pseudorandom Number Algorithms," *Journal of the ACM, 20*, 456-468.

Mahler, K. (1941), "An Analogue to Minkowski's Geometry of Numbers in a Field of Series," *Annals of Mathematics, 42*, 488-522.

Marsaglia, G. (1968), "Random Numbers Fall Mainly in the Planes," *Proceedings of National Academy of Sciences USA, 61*, 25-28.

Marsaglia, G. (1976), "Random Number Generator," In *Encyclopedia of Computer Science*, A. Ralston and C.L. Meek, Eds. Petrocelli/Charter, New York, NY, 1192-1197.

Niederreiter, H. (1987), "A Statistical Analysis of Generalized Feedback Shift Register Pseudorandom Number Generators,"*SIAM Journal on Scientific and Statistical Computing, 8*, 1035-1051.

Niederreiter, H. (1988), "The Serial Test for Digital K-step Pseudorandom Numbers," *Mathematical Journal of Okayama University, 30*, 93-119.

Ripley, B.D. (1987), *Stochastic Simulation*, Wiley, New York, NY.

Tausworthe, R.C. (1965), "Random Numbers Generated by Linear Recurrence Modulo Two", *Mathematics of Computation, 19*, 201-209.

Tezuka, S. (1987a), "Walsh-Spectral Test for GFSR Pseudorandom Number Generators", *Communications of the ACM, 30*, 731-735.

Tezuka, S. (1987b), "On the Discrepancy of GFSR Pseudorandom Numbers," *Journal of the ACM, 34*, 939-949.

Tezuka, S. (1988), "On Optimal GFSR Pseudorandom Number Generators," *Mathematics of Computation, 50*, 531-533.

Tezuka, S. (1989), "Random Number Generation Based on Polynomial Arithmetic Modulo Two," Research Report RT0017, IBM Research, Tokyo Research Laboratory, Tokyo.