ハイパフォーマンス
コンピューティング 47－6
（1993．6．18）

Twisted GFSR 乱数のラティス構造について

手塚 集（日本アイビーエム東京基礎研究所）

概要

高精度モンテカルロ計算で現在広く用いられている乱数生成法にシフトレジスター系列に基づく方法がある。この方法は非常に長い周期の系列を効率的に生成できるという長所をもっている。この方法は詳しく分類すると、Tausworthe 法、GFSR 法、Twisted GFSR 法という 3 通りの方法に分けられる。ここでは、これらの方式により生成される乱数列すべてが有限体上の多項式演算に関するラティス構造を持つ事を示す。さらに、その事実が一様分布の解析に非常に役立つことも示す。最後に、Twisted GFSR 法による乱数列は、常に高次元における一様分布が非常に悪いことを証明する。

Lattice Structure of Twisted GFSR Random Numbers

Shu Tezuka (IBM Japan, Tokyo Research Laboratory)

ABSTRACT

Shift Register Random Numbers are widely used in High Precision Monte Carlo (HPMC) Calculations. There are three types of generators: Tausworthe generators, GFSR generators, and Twisted GFSR generators. We show that random numbers generated by these methods have lattice structure with respect to polynomial arithmetic over finite fields. We also show that Twisted GFSR random numbers are far from uniform distribution in higher dimensions than the degree of the recurrence relation.

1 Introduction

There are two types of shift-register random number sequences: Tausworthe sequences and GFSR sequences. Let $M(z) = z^r + a_{r-1}z^{r-1} + \cdots + a_0$ be a primitive polynomial of degree r over $GF(2)$, and L be the "word-size." A binary sequence $x_i, i = r, r+1, ...$ follows the recurrence relation $x_i = a_{r-1}x_{i-1} + \cdots + a_0 x_{i-r} \pmod 2$.

A Tausworthe sequence is thus defined as follows [7]:

$$u_i = \sum_{j=1}^{L} x_{di+j} 2^{-j}, \tag{1}$$

where d is a constant with $0 < d < 2^r - 1$, $\gcd(d, 2^r - 1) = 1$. The algorithm below (see [11]) generates a Tausworthe sequence whose characteristic polynomial is a primitive trinomial of the form $M(z) = z^r + z^s + 1$, $s < r/2$, and $0 < d \leq r - s$. Each term of the sequence $\{u_i\}$ is expressed by its leading $L = r$ bits in this algorithm. This can be implemented easily, in a "portable" language that supports shifting and XOR operations (such as C), if r [=L] is not larger than the computer's word-size.

An algorithm for implementing (1) when $0 < d \leq r - s$:

Step 0: A and B are r-bit words.
Step 1: B $\longleftarrow$ s bit left shift of A
Step 2: B $\longleftarrow$ A XOR B
Step 3: B $\longleftarrow$ $r - d$ bit right shift of B
Step 4: A $\longleftarrow$ d bit left shift of A
Step 5: A $\longleftarrow$ A XOR B
Step 6: Output A as the leading r bits of u_i, return to Step 1.

A slight modification of the above can be adapted for generating a Tausworthe sequence whose characteristic polynomial is a primitive trinomial of the form $M(z) = z^r + z^s + 1$, $s < r/2$, and $d = r$.

A GFSR sequence is originally defined as follows [4]:

$$u_i = \sum_{j=1}^{L} x_{dj+i} 2^{-j}. \tag{2}$$

Note that $L \leq r$ (otherwise, a linear dependence relation appears between the column bits of u_i). Lewis and Payne suggested that d should be greater than $100r$. In addition, they employed a primitive trinomial as the characteristic polynomial of $\{x_i\}$ in order to realize a fast generation scheme for the sequence in the following way: Let $M(z) = z^r + z^s + 1$. The sequence can then be generated by the scheme

$$u_i = u_{i-s} \text{ XOR } u_{i-r}. \tag{3}$$

The lagged Fibonacci with XOR is a more general version of the sequences in (2) with primitive characteristic trinomials,

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

where $j_l, l = 1, ..., L$, are integers between 0 and $2^r - 1$. However, the recurrence relation (3) can still be exploited in this case. Today, people call this general version with any primitive characteristic polynomials a GFSR sequence [6, 8].

The matrix representation of shift register sequences is very useful. Let C be the companion matrix of the polynomial $M(z) = z^r + a_{r-1}z^{r-1} + \cdots + a_1 z + a_0$, namely,

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & a_0 \\ 1 & 0 & 0 & \cdots & a_1 \\ & \cdots & \cdots & \cdots & \\ & \cdots & \cdots & \cdots & \\ 0 & \cdots & 1 & 0 & a_{r-2} \\ 0 & 0 & \cdots & 1 & a_{r-1} \end{pmatrix},$$

and let $\alpha = (x_0, ..., x_{r-1})$ be a non-zero binary vector. The general GFSR is then written as follows:

$$\alpha G, \alpha CG, ..., \alpha C^i G, ...,$$

where G is an $r \times L$ matrix over $GF(2)$ whose l-th column vector, denoted by $G_l, l = 1, ..., L$, is uniquely determined by the equations,

$$x_{j_l+i} =< G_l, \alpha C^{i-1} >, \text{ for } i = 1, ..., r.$$

Here $< \alpha, \beta >$ means the inner-product of the binary vectors α and β over $GF(2)$.

Twisted GFSR generators were recently defined by Matsumoto and Kurita [5]:

$$\mathbf{v}_i = \mathbf{v}_{i-s} \text{ XOR } \mathbf{v}_{i-r}A, \text{ for } i = r, r+1, ...,$$

where $\mathbf{v}_i$ is a sequence of vectors in $GF(2^w)$, A is a $w \times w$ matrix over GF(2), and $r > s$. In particular, they analyzed the following special case, which is very useful for quick generation of the sequences:

$$\mathbf{v}_i = \mathbf{v}_{i-s} \text{ XOR } \mathbf{v}_{i-r}C^T, \tag{4}$$

where $\mathbf{v}_i$ is a sequence of vectors in $GF(2^w)$, C is a $w \times w$ companion matrix, and $r > s$. In this paper, we call this special case as Twisted GFSR with companion matrices. The conversion from a binary vector $(v_0, ..., v_{w-1})$ into a random number between 0 and 1 is as follows:

$$u = \frac{1}{2^w} \sum_{i=0}^{w-1} v_i 2^i.$$

The parameters r, s, and C are chosen so that the maximum period of the sequence v_i becomes $2^{wr} - 1$. In their paper, some parameters of Twisted GFSR with maximum periods are listed.

One of the advantages of this scheme is that the size r of an array is the minimum necessary to produce the period length $2^{wr} - 1$ with respect to the word-size w. In this sense, the scheme can be viewed as an improved version of the lagged Fibonacci scheme with XOR, because the latter produces a period $2^r - 1$ of a sequence with an identically sized array of r w-bit words. Another important merit is the fast generation algorithm. Let $\mathbf{v}_i = (v_{i,0}, ..., v_{i,w-1})$ and $\mathbf{a} = (a_0, ..., a_{w-1})$. The algorithm is then:

$$\begin{aligned} \text{if } v_{i-r,w-1} = 0 \text{ then } \mathbf{v}_i &= \mathbf{v}_{i-s} \text{ XOR SR}(\mathbf{v}_{i-r}) \\ \text{else } \mathbf{v}_i &= \mathbf{v}_{i-s} \text{ XOR SR}(\mathbf{v}_{i-r}) \text{ XOR } \mathbf{a}, \end{aligned}$$

where SR is the one-bit right-shift operation.

2 Linear Congruential Sequences with respect to Polynomial Arithmetic over Finite Fields

Here, we give a definition of linear congruential sequences with respect to polynomial arithmetic over $GF(q)$. Let $GF\{q,z\}$ denote the field of all Laurent series of the form $S(z) = \sum_{j=-\infty}^{m} c_j z^j$,where m is an integer, $c_j \in GF(q)$, and q is a power of prime p, i.e., $q = p^w$ (w is a positive integer). Here we define an analogous version of linear congruential sequences in $GF\{q,z\}$:

$$\begin{aligned} f_i(z) &= (g(z)f_{i-1}(z) + h(z)) \bmod M(z) \\ u_i(z) &= f_i(z)/M(z) = y_1^{(i)}z^{-1} + y_2^{(i)}z^{-2} + ..., \end{aligned} \tag{5}$$

where $g(z), h(z), M(z)$, and $f_i(z)$ are polynomials in $GF\{q,z\}$. We denote this generator by the triplet $G = (g,h,M)$ and call it an $LS(q)$ generator.

Consider the k-tuples $(f_i(z)/M(z), ..., f_{i+k-1}(z)/M(z))$, $i = 1,2,...$, produced by (5). These are expressed by the grid (shifted lattice) $\mathcal{L}_k + \lambda$, where $\mathcal{L}_k$ is a lattice with the basis

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

and $\lambda = (0, 1, 1+g(z), \ldots, 1+g(z)+\cdots+g^{k-2}(z))(h(z)/M(z))$. Hereafter, we call $\mathcal{L}_k$ the associated lattice to $G = (g,h,M)$.

Define the norm of a vector $\alpha = (a_1(z), ..., a_k(z))$, where each $a_i(z)$ is in $GF\{q,z\}$, as

$$|\alpha| = \max_{1 \le i \le k} \deg(a_i).$$

In this paper, the notions of reduced basis and successive minima of a lattice $\mathcal{L}_k$ in a vector space over $GF\{q,z\}$ follow Lenstra's definitions [3]:

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

Note that Lenstra gave an efficient algorithm that calculates the reduced basis in $GF\{q,z\}$ [3], and showed that it is much faster than the approach based on Gaussian elimination.

2.1 q is a prime

Let q be a prime p. Then we define σ as a mapping from $GF\{p,z\}$ to the real field as follows:

$$\sigma^{(p)}(S(z)) = S(p) = \sum_{j=-\infty}^{m} c_j p^j.$$

We use $\sigma_L^{(p)}$, the truncated version of $\sigma^{(p)}$:

$$\sigma_L^{(p)}(S(z)) = \sum_{j=-L}^{m} c_j p^j.$$

Hereafter, we denote the truncated $LS(q)$ sequences by $LS_L(q)$ sequences. In practical situations, L depends on the size of p such that $p^L \approx 2^{32}$. In the following discussions, we consider two cases: (i) p is small, i.e., $L > 1$ and (ii) p is large enough, i.e, $L = 1$. First, we deal with the former.

2.1.1 q is a small prime

For simplicity, we consider the case in which $q = p = 2$. Recently [10], Tausworthe sequences have been shown as a special case of the above general class.

Proposition 1 *Tausworthe sequences can be formulated as $LS_L(2)$ sequences from $G = (g, h, M)$ such that $M(z) = z^r + a_{r-1}z^{r-1} + \cdots + a_0$, $g(z)$ is primitive modulo $M(z)$, $h(z) \equiv 0$, and L is the "word-size," where $M(z)$ is a characteristic polynomial for a Tausworthe sequence, i.e, a primitive polynomial over $GF(2)$.*

Next, we consider a similar formulation for the original GFSR sequences defined in (2). The result implies that the original GFSR sequences contain Tausworthe sequences as a proper subclass.

Proposition 2 *The original GFSR sequences in (2) can be formulated as $LS_L(2)$ sequences from $G = (g, h, M)$ such that $M(z)$ is an irreducible polynomial of degree r over $GF(2)$, $g(z)$ is primitive modulo $M(z)$, $h(z) \equiv 0$, and L is the "word-size."*

Note that, in general, GFSR sequences cannot be written as $LS_L(2)$ sequences.

Following Tezuka and L'Ecuyer [11], Couture [1] obtained a theorem that links the k-dimensional distribution of $LS_L(2)$ sequences with the successive minima and reduced bases of a lattice in a vector space over $GF\{2, z\}$. Before going into details, we need to explain how to measure the k-dimensional uniformity of the sequences. An *equidissection* of the k-dimensional unit hypercube into $2^{k\ell}$ cubic cells is defined as the set of all cubic cells in $[0, 1)^k$ whose sides have a length of $2^{-\ell}$ and whose corners have coordinates that are all multiples of $2^{-\ell}$. That is,

$$S_k(\ell) = \left\{ [i_1 2^{-\ell}, (i_1 + 1)2^{-\ell}) \times \cdots \times [i_k 2^{-\ell}, (i_k + 1)2^{-\ell}) \mid 0 \le i_j < 2^\ell, 1 \le j \le k \right\}.$$

Thus we have the following theorem [1]:

Theorem 1 *For $1 \le i \le k$, let l_i be the i-th successive minimum of the lattice associated to $G = (g, 0, M)$, where $M(z)$ is an irreducible polynomial of degree r over $GF(2)$ and $g(z)$ is primitive modulo $M(z)$. Define the quantity $d(\ell)$ as follows:*

$$d(\ell) = \sum_{i=1}^{k} (-\ell - l_i)^+,$$

where $(t)^+ = t$ if $t > 0$, or 0 otherwise. Then we have Table 1, which gives the number of cells denoted by $\#_\ell(n)$ for all values of n for which it could be non-zero, where n is the number of lattice points in a cell.

According to Tezuka [8, 10], a pseudorandom sequence having a lattice structure in the vector space over $GF\{2, z\}$ is said to be k-distributed with ℓ-bit resolution when each cell of $S_k(\ell)$ contains the same number of lattice points. Now, the following result of Tezuka [10, Theorem 1] can be derived as a corollary of Theorem 1:

Table 1: Values of $\#_\ell(n)$ that could be non-zero for a given resolution ℓ

n	$\#_\ell(n)$
$2^{d(\ell)}$	$2^{r-d(\ell)}-1$
$2^{d(\ell)}-1$	1
0	$2^{\ell k}-2^{r-d(\ell)}$

Corollary 1 *A $LS_L(2)$ sequence from $G=(g,0,M)$ is k-distributed with resolution ℓ if and only if $l_k \leq -\ell$, where $M(z)$ is irreducible over $GF(2)$ and $g(z)$ is primitive modulo $M(z)$.*

We shall comment on this result in connection with the spectral test. Mahler's theorem says that the i-th successive minimum of the prime lattice is equal to the $(k-i)$-th successive minimum of the dual lattice. Hence, the norm of the shortest vector of the dual lattice is exactly equivalent to the resolution of the sequences. This result corresponds to the conventional spectral test for linear congruential sequences, where the length of the shortest vector of the dual lattice is equivalent to the reciprocal of the maximum distance of the hyperplanes in which the points fall. The discrepancy of simple Tausworthe sequences and general GFSR sequences has been analyzed in the last decade (see [6, 9, 12]).

2.2 q is a prime power

Now, we consider an analogous version of linear congruential sequences in $GF\{q,z\}$, where q is a prime power. For reasons of simplicity and practical importance, we henceforth restrict ourselves to the case in which $q=2^w$, where $w \approx 32$.

When q is large enough, the truncated linear congruential sequence in $GF\{q,z\}$ is given as follows: Let the truncated sequence $\tilde{u}_i(z), i=1,2,...,$ be defined as

$$\tilde{u}_i(z) = y_1^{(i)} z^{-1},$$

where $y_1^{(i)}$ is the coefficient of z^{-1} in the formal Laurent series $f_i(z)/M(z)$ in (5). Consider the case in which $M(z)=z^r-m_{r-1}z^{r-1}-\cdots-m_0$, $g(z)\equiv z$, and $h(z)\equiv 0$. If we use the polynomial representation of $GF(2^w)$ based on an irreducible polynomial $Q(t)=t^w+a_{w-1}t^{w-1}+\cdots+a_0$,, writing $y_i(t)$ for $y_1^{(i)}$, and $m_j(t)$ for m_j, $0\leq j<r$, then for the same reason as in the case of multiple recursive generators, the recurrence relation of $y_i(t)$ can be written as

$$y_i(t) = m_{r-1}(t)y_{i-1}(t)+\cdots+m_0(t)y_{i-r}(t) \pmod{Q(t)}. \tag{6}$$

Note that if $M(z)$ is primitive over $GF(2^w)$ the period of $y_i(t)$ becomes $2^{wr}-1$. Since Theorem 2 in Couture et al. [1] is valid for any lattice in the vector space over $GF\{2,z\}$, we have

Theorem 2 *For multiple recursive generators in (6) with maximum period $2^{wr}-1$, their point distribution is also given in Table 1 with r replaced by wr, where, for $1\leq i\leq k$, l_i is the i-th successive minimum of the associated lattice.*

Let $y_i(t)=\sum_{j=0}^{w-1} v_{i,j}t^j$, where $\mathbf{v}_i=(v_{i,0},...,v_{i,w-1})$ is defined in (4). Since the multiplication by t modulo $Q(t)$ is equivalent to the multiplication by C^T in (4), where C is the companion matrix corresponding to $Q(t)$, we obtain

Proposition 3 *Twisted GFSR sequences with companion matrices can be formulated as $LS_L(q)$ sequences from $G=(g,h,M)$, where $q=2^w$, $g(z)\equiv z$, $h(z)\equiv 0$, $M(z)$ is primitive over $GF(2^w)$,*

and $L = 1$, in other words, as multiple recursive sequences with respect to polynomial arithmetic modulo two, which is of the form

$$\begin{aligned} y_i(t) &= y_{i-s}(t) + t y_{i-r}(t) \pmod{Q(t)}, \\ u_i(t) &= y_i(t)/t^w. \end{aligned}$$

In Table 2, we give the lattice structure of one of the Twisted GFSRs proposed in [5], where $Q(t) = t^{31} + t^{29} + t^{28} + t^{26} + t^{25} + t^{24} + t^{23} + t^{20} + t^{19} + t^{16} + t^{15} + t^{13} + t^{12} + t^{11} + t^{10} + t^8 + t^6 + t^5 + t^3 + t + 1$, $s = 2$, and $r = 13$. The period is $2^{403} - 1$, so equidistribution is guaranteed up to 13 dimensions. We investigated the lattice structure in dimensions 14 to 30.

Table 2: The successive minima in dimensions 14 to 30 for the Twisted GFSR with a period of $2^{403} - 1$

dim	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$-l_1$	31	31	31	31	31	31	31	31	31	31	31	31	30	30	30	30	30
$-l_2$	31	31	31	31	31	31	31	31	31	31	31	30	30	30	30	30	30
$-l_3$	31	31	31	31	31	31	31	31	31	31	30	30	30	30	30	30	30
$-l_4$	31	31	31	31	31	31	31	31	31	30	30	30	30	30	30	30	30
$-l_5$	31	31	31	31	31	31	31	31	30	30	30	30	30	30	30	30	30
$-l_6$	31	31	31	31	31	31	31	30	30	30	30	30	30	30	30	30	30
$-l_7$	31	31	31	31	31	31	30	30	30	30	30	30	30	30	30	30	30
$-l_8$	31	31	31	31	31	30	30	30	30	30	30	30	30	30	30	30	30
$-l_9$	31	31	31	31	30	30	30	30	30	30	30	30	30	30	30	30	30
$-l_{10}$	31	31	31	30	30	30	30	30	30	30	30	30	30	30	30	30	29
$-l_{11}$	31	31	30	30	30	30	30	30	30	30	30	30	30	30	30	29	29
$-l_{12}$	31	30	30	30	30	30	30	30	30	30	30	30	30	30	29	29	29
$-l_{13}$	30	30	30	30	30	30	30	30	30	30	30	30	30	29	29	29	29
$-l_{14}$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$-l_{15}$	-	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$-l_{16}$	-	-	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$-l_{17}$	-	-	-	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$-l_{18}$	-	-	-	-	1	1	1	1	1	1	1	1	1	1	1	1	1
$-l_{19}$	-	-	-	-	-	1	1	1	1	1	1	1	1	1	1	1	1
$-l_{20}$	-	-	-	-	-	-	1	1	1	1	1	1	1	1	1	1	1
$-l_{21}$	-	-	-	-	-	-	-	1	1	1	1	1	1	1	1	1	1
$-l_{22}$	-	-	-	-	-	-	-	-	1	1	1	1	1	1	1	1	1
$-l_{23}$	-	-	-	-	-	-	-	-	-	1	1	1	1	1	1	1	1
$-l_{24}$	-	-	-	-	-	-	-	-	-	-	1	1	1	1	1	1	1
$-l_{25}$	-	-	-	-	-	-	-	-	-	-	-	1	1	1	1	1	1
$-l_{26}$	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1	1	1
$-l_{27}$	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1	1
$-l_{28}$	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1
$-l_{29}$	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1
$-l_{30}$	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1

As shown in the table, the lattice structure is bad in all of these dimensions. For example, in $k = 14$ the number of empty cells, $2^{\ell k} - 2^{wr-d(\ell)}$, becomes $0, 2^{27}, 2^{42} - 2^{40}, ...$, for $\ell = 1, 2, 3, 4, ...$ This means that even the most significant two bits of each term in the vectors $(\mathbf{v}_i, ..., \mathbf{v}_{i+14})$, $i = 1, 2, ...,$ from this Twisted GFSR sequence are not equally distributed.

This phenomenon can be explained as follows: Let $\mathbf{v}_i = (v_{i,0}, ..., v_{i,w-1})$. In general, for any Twisted GFSR sequence there exists the following linear dependency relation:

$$v_{ij} = v_{i-s,j} + v_{i-r,j-1} + a_j v_{i-r,w-1} \pmod 2$$

for $1 \leq j \leq w-1$, and

$$v_{i0} = v_{i-s,0} + v_{i-r,w-1} \pmod 2,$$

for $j = 0$, since $Q(t)$ is an irreducible polynomial, i.e., $a_0 = 1$, where a_j is the coefficient of t^j in $Q(t)$. Note that the case of $j = w-1$ means that there exists a linear dependency relation in the leading two bits of the consecutive $k(> r)$ vectors of $\mathbf{v}_i, i = 1, 2, \ldots$. Thus, we obtain

Theorem 3 *For any $k > r$, all Twisted GFSR sequences with companion matrices are k-distributed with at most one bit resolution.*

References

[1] R. Couture, P. L'Ecuyer, and S. Tezuka, *On the Distribution of k-dimensional Vectors for Simple and Combined Tausworthe Sequences,* to appear in Math. Comp. (April, 1993).

[2] D.E. Knuth, *The Art of Computer Programming: Vol. 2, Seminumerical Algorithms*, 2nd ed., Addison-Wesley, 1981.

[3] A.K. Lenstra, *Factoring Multivariate Polynomials over Finite Fields,* J. Comput. Syst. Sci., 30, (1985), 235-248.

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

[5] M. Matsumoto and Y. Kurita, *Twisted GFSR Generators*, to appear in ACM Trans. Modeling and Computer Simulation (1993).

[6] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conference Series in Applied Math., no. 63, SIAM, (1992).

[7] R.C. Tausworthe, *Random Numbers Generated by Linear Recurrence Modulo Two,* Math. Comp., 19, (1965), 201-209.

[8] S. Tezuka, *Walsh-Spectral Test for GFSR Pseudorandom Number Generators,* Comm. ACM., 30, (1987), 731-735.

[9] S. Tezuka, *On the Discrepancy of GFSR Pseudorandom Numbers,* J. ACM., 34, (1987), 939-949.

[10] S. Tezuka, *Lattice Structure of Pseudorandom Sequences from Shift Register Generators,* Proc. of the 1990 Winter Simulation Conference, IEEE Press, (1990), 266-269.

[11] S. Tezuka and P. L'Ecuyer, *Efficient and Portable Combined Tausworthe Random Number Generators,* ACM Trans. Modeling and Computer Simulation, 1 (1991), 99-112.

[12] S. Tezuka and M. Fushimi, *Calculation of Fibonacci Polynomials for GFSR Sequences with Low Discrepancies*, to appear in Math. Comp. (April, 1993).