MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 182
APRIL 1988, PAGES 531-533

On Optimal GFSR Pseudorandom Number Generators

By Shu Tezuka

Abstract. It is shown that in t (≥ 4) dimensions no optimal GFSR generators exist.

1. Introduction. The binary representation of p-bit GFSR pseudorandom numbers is defined [1], [2] as follows, for given $j_1, j_2, \ldots, j_p$,

$$Xi = a_{j_1+i-1} a_{j_2+i-1} \cdots a_{j_p+i-1} \quad \text{for } i = 1, 2, 3, \ldots,$$

where $\{Xi\}$ is a sequence of p-bit integers and $\{a_i\}$ is an M-sequence with period length $2^p - 1$ whose characteristic polynomial is

$$f(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_{p-2} D^{p-2} + c_{p-1} D^{p-1} + D^p \pmod 2.$$

Here, the initial values $(a_1, a_2, \ldots, a_p) \neq (0, 0, \ldots, 0)$.

The GFSR sequences can be expressed by using the companion matrix of M-sequences. Denote the companion matrix by C,

$$C = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ & & \cdots\cdots & \cdots & \cdots & \\ & & \cdots\cdots & \cdots & \cdots & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & c_{p-1} & c_{p-2} & \cdots & c_2 & c_1 \end{bmatrix}.$$

Let* $\alpha = (a_1, a_2, \ldots, a_p)^t$, $\beta = (a_{j_1}, a_{j_2}, \ldots, a_{j_p})^t$. Then there exists a matrix G such that $\beta = G\alpha$. Hence, a p-bit GFSR sequence can be expressed as follows,

$$G\alpha,\ GC\alpha,\ GC^2\alpha, \ldots, GC^i\alpha, \ldots.$$

Assume that G is nonsingular. Then the above sequence is

$$\beta,\ T\beta,\ T^2\beta, \ldots, T^i\beta, \ldots,$$

where $T = GCG^{-1}$.

Received October 7, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C05, 65C10.
Key words and phrases. M-sequence, GFSR algorithm, quasi-Monte Carlo methods, discrepancy, random numbers.

*x^t is the transpose of a vector or a matrix x.

©1988 American Mathematical Society
0025-5718/88 $1.00 + $.25 per page

2. Discrepancy of GFSR Sequences. Recently, the t-dimensional discrepancy of GFSR sequences has been obtained in [3]. Let $r(L_1, L_2, \ldots, L_t)$ be the rank of the following set of row vectors,

$$\{T^{i_j} \mid j = 1, 2, \ldots, L_i \text{ for } i = 1, 2, \ldots, t\},$$

where T^{i_j} is the jth row vector of T^i and $L_i \geq 0$ for $1 \leq i \leq t$. Let $r\min$ be the minimum of $r(L_1, L_2, \ldots, L_t)$ such that $r(L_1, L_2, \ldots, L_t)$ is not full. Note that $r\min \leq p$. Then we have obtained the following theorem.

THEOREM D. *The t-dimensional discrepancy of GFSR sequences with period $2^p - 1$ is*

$$D_N^{(t)} = O((\log M)^t C\max),$$

where $M = 2^p$, $N = 2^p - 1$ and $C\max = 2^{-r\min}$.

3. Optimal GFSR Generators in High Dimensions. We have defined the optimal generators for GFSR sequences in [3]. The definition is as follows.

Definition. When $r\min = p$, we call the GFSR generator 'optimal', where p is the degree of the primitive polynomial.

Example. The following generator G1 is an optimal GFSR generator with $f(D) = D^7 + D^4 + 1$:

$$\mathrm{G1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

The purpose of this paper is to prove the following theorem. Here we consider the case of t $(\leq p)$ dimensions.

THEOREM. *In t (≥ 4) dimensions, no optimal GFSR generators exist.*

Proof. Consider the following linear equation,

$$\sum_{i=1}^{t} \sum_{j=1}^{L_i} T^{i_j} w_{ij} = (0, 0, \ldots, 0), \tag{3.1}$$

where w_{ij} is over GF(2).

Note that the above equation has a nonzero solution if and only if the T^{i_j}'s are linearly dependent. The solution of (3.1) is said to be in a class $(L_1, L_2, \ldots, L_t)$ if $w_{i,L_i} = 1$ for all $1 \leq i \leq t$.

Denote by $C(L_1, L_2, \ldots, L_t)$ the number of nonzero solutions of (3.1) in a class $(L_1, L_2, \ldots, L_t)$. By using the principle of inclusion and exclusion, for $L_i \geq 1$, $i = 1, 2, \ldots, t$, we have

$$C(L_1, L_2, \ldots, L_t) = \sum_{i=0}^{t} (-1)^i \sum_{0 < j_1 < j_2 < \cdots < j_i \leq t} 2^{\sum_{k=1}^{t} L_k - i - \rho(j_1, j_2, \ldots, j_i)},$$

where $\rho(j_1, j_2, \ldots, j_i)$ is equal to $r(f_1, f_2, \ldots, f_t)$ with

$$\begin{aligned} f_n &= L_n - 1 \quad \text{for } n = j_1, j_2, \ldots, j_i, \\ &= L_n \qquad\quad \text{otherwise,} \end{aligned}$$

and where $0 < j_1 < j_2 < \cdots < j_i \leq t$ and $n = 1, 2, \ldots, t$.

Assume that $r\min = p$ in t dimensions. Consider a class $(L_1, L_2, \ldots, L_t)$ such that $\sum_{i=1}^{t} L_i = p + 2$ with $L_i \geq 1$. Then

$$\begin{aligned} C(L_1, L_2, \ldots, L_t) &= 2^{p+2-p} - {}_tC_1 2^{p+1-p} + \sum_{i=2}^{t} (-1)^i {}_tC_i \\ &= 4 - 2t + t - 1 = 3 - t \geq 0. \end{aligned}$$

Therefore, t must be smaller than 4. □

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

1. M. FUSHIMI & S. TEZUKA, "The k-distribution of Generalized Feedback Shift Register pseudorandom numbers," *Comm. ACM*, v. 26, 1983, pp. 516–523.

2. T. G. LEWIS & W. H. PAYNE, "Generalized Feedback Shift Register pseudorandom number algorithms," *J. Assoc. Comput. Mach.*, v. 20, 1973, pp. 456–468.

3. S. TEZUKA, "On the discrepancy of GFSR pseudorandom numbers," *J. Assoc. Comput. Mach.*, v. 34, 1987.