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

FAST GENERATION OF LOW DISCREPANCY POINTS BASED ON FIBONACCI POLYNOMIALS

Shu Tezuka

IBM Research
Tokyo Research Laboratory
5-11 Sanbancho, Chiyoda-ku, Tokyo 102, Japan

Masanori Fushimi

Faculty of Engineering
University of Tokyo
7-3-1 Hongo, Bunkyou-ku, Tokyo 113, Japan

ABSTRACT

In this paper, we consider GFSR sequences with low discrepancies that are produced by a recurrence relation whose characteristic polynomial is a primitive pentanomial, whereby each term can be generated only by three bitwise exclusive-or operations. The use of pentanomials is motivated by the fact that there exists at least one pair of Fibonacci polynomials, which can be exploited to generate low-discrepancy GFSR sequences, for every degree less than 22, whereas this is not true for the trinomial case, and in most of practical applications we need the point sets of size around 2^{10} to 2^{20}. We give the table of the pentanomial GFSR sequences with low discrepancies which were found to be the best in the dimensions two to five for degrees less than 22. The paper also gives some results of the applications of these low discrepancy points to multiple integration problems.

1 INTRODUCTION

Low discrepancy points and sequences are known to be useful for numerical integration, simulation, and optimization. The most recent survey on this topic can be found in Niederreiter (1992). Fibonacci polynomials are closely related to the two-dimensional discrepancy of Tausworthe sequences, a typical class of shift register random numbers (Tausworthe 1965; Lewis and Payne 1973). For the digital multistep sequences, the special subclass of Tausworthe sequences, Mullen and Niederreiter (1987) obtained the figure of merit for the discrepancy of the sequences, and defined Fibonacci polynomials as giving the best figure of merit in the two-dimensions. Further, they conducted an exhaustive search for the Fibonacci polynomials based on their definition. Recently (Tezuka and Fushimi 1993), we generalized their definition based on linear congruential sequences in the field of formal Laurent series over $GF(2)$, which includes Tausworthe sequences as a subclass (Tezuka 1990). The merit of this generalization is that there are many Fibonacci polynomials which are primitive, while the original Fibonacci polynomials as defined in Mullen and Niederreiter (1987) are rarely primitive. This means that there are many possible choices of parameters for fast generation of low discrepancy points based on Fibonacci polynomials.

The paper is organized as follows. Section 2 overviews the discrepancy as well as Fibonacci polynomials and their related results. In Section 3, we conduct exhaustive search for the best GFSR generators with primitive pentanomials that quickly produce low discrepancy points based on Fibonacci polynomials. Finally, we discuss the applications of these point sets to multiple integration problems.

2 OVERVIEW

2.1 Discrepancy and Related Results

First, we recall the definition of discrepancy. For N points $X_0, X_1, ..., X_{N-1}$ in $I^k = [0,1)^k, k \geq 1$, and a subinterval $J = [0, u_i)^k, k \geq 1$, where $0 < u_i \leq 1$ for $1 \leq i \leq k$, we define the *discrepancy* as

$$D_N^{(k)} = \sup_J \left| \frac{A(J;N)}{N} - V(J) \right|,$$

where $A(J;N)$ is the number of $n, 0 \leq n < N$, with $X_n \in J$ and $V(J)$ is the volume of J, and the supremum is extended over all subintervals J. We call as a *low-discrepancy points* such a point set, $X_0, X_1, ..., X_{N-1}$, in I^k, that the discrepancy satisfies

$$D_N^{(k)} \leq C_k (\log N)^k / N,$$

where C_k is a constant only depending on the dimension k.

The use of low discrepancy points are justified by the Koksma-Hlawka theorem, which is presented as

follows:

$$E_N(f) \stackrel{\text{def}}{=} \left| \int_{I^k} f(x)dx - \frac{1}{N}\sum_{i=0}^{N-1} f(X_i) \right| \le V(f)D_N^{(k)}, \tag{1}$$

where $V(f)$ is the total bounded variation of f in the sense of Hardy-Krause, reflecting the regularity of f.

2.2 Fibonacci Polynomials and Discrepancy

Let $GF\{2,x\}$ denote the field of all Laurent series of the form $S(x) = \sum_{j=-\infty}^{m} s_j x^j$, with m an integer and s_j in $GF(2)$. The field $GF\{2,x\}$ contains the field of rational functions over $GF(2)$ as a subfield. Here we define an analogous version of linear congruential sequences in $GF\{2,x\}$. Let σ be a mapping from $GF\{2,x\}$ to the real field, defined as

$$\sigma(S(x)) = S(2).$$

Then a pseudorandom sequence u_n, $n = 1,2,...$, in [0,1) is defined as

$$\begin{aligned} f_n(x) &= (g(x)f_{n-1}(x) + h(x)) \bmod M(x) \\ u_n &= \sigma(f_n(x)/M(x)), \end{aligned} \tag{2}$$

where $g(x), h(x), M(x)$ and $f_n(x)$ are polynomials in $GF\{2,x\}$. In practical situations, u_n is expressed approximately by its truncated value, i.e. by summing from some constant $-L$ instead of $-\infty$.

The discrepancy of the sequences defined in (2) has been obtained (Niederreiter 1987a,c; Tezuka 1987, 1989). Here we define $\deg(0) = -1$.

Theorem 1 *Let*

$$\rho^{(k)} = \min \sum_{i=1}^{k} (\deg(h_i) + 1),$$

where the minimum is taken over all nonzero polynomial solutions $(h_1(x), ..., h_k(x))$ of the equation:

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

If the sequence defined in (2) has a period of $2^p - 1$, then the k-dimensional discrepancy of the sequence over the full period is given as

$$D_N^{(k)} \le C_k(\log N)^{k-1}/2^{\rho^{(k)}},$$

where $N = 2^p$ and C_k is a constant depending only on k.

Hence, the value of $\rho^{(k)}$ can be regarded as a figure of merit for the discrepancy of the sequences; that is to say, the larger $\rho^{(k)}$ is, the lower the discrepancy.

For the two-dimensional case, the next theorem (Tezuka 1988) links the continued fraction expansion of $g(x)/M(x)$ with the two-dimensional discrepancy.

Theorem 2 *Let the partial quotients in the continued fraction expansion of $g(x)/M(x)$ be $A_1(x)$, ..., $A_s(x)$, i.e.,*

$$\begin{aligned} & g(x)/M(x) \\ = \; & 1/(A_1(x) + 1/(A_2(x) + \cdots + 1/A_s(x))) \\ =: \; & [A_1(x), A_2(x), \cdots, A_s(x)]. \end{aligned}$$

Then we have

$$\rho^{(2)} = p + 2 - \max_{1\le i\le s}(\deg(A_i)).$$

Note that there exists a pair of polynomials $(g(x), M(x))$ for any degree of $M(x)$ such that the degrees of partial quotients in the continued fraction expansion of $g(x)/M(x)$ are all one.

Recently, we defined Fibonacci polynomials as follows (Tezuka and Fushimi 1993):

Definition **1** A pair of polynomials $(a(x), b(x))$ with $\deg(a) < \deg(b)$ is called a pair of Fibonacci polynomials if the partial quotients in the continued fraction of $a(x)/b(x)$ are all of degree one.

As pointed out in Niederreiter (1987b), on the average, every polynomial $b(x)$ has one $a(x)$ such that in the continued fraction expansion of $a(x)/b(x)$ the partial quotients are all of degree one. Mesirov and Sweet (1987) proved that there exist exactly two $a(x)$ for every irreducible $b(x)$, where $(a(x), b(x))$ is a pair of Fibonacci polynomials.

The following recurrence relation produces a sequence of Fibonacci polynomials, $F_i(x), i = 0,1,2,...$.

$$F_i(x) = A_i(x)F_{i-1}(x) + F_{i-2}(x), \quad i = 2,3,..., \tag{3}$$

where $F_0(x) = 1, F_1(x) = A_1(x)$, and $A_i(x), i = 1,2,...$, are arbitrary polynomials over $GF(2)$ of degree one, i.e., $A_i(x) = x$ or $x+1$. Thus, $(F_i(x), F_{i+1}(x))$ is a pair of Fibonacci polynomials.

Note that if in the equation (2), $g(x)$ satisfies the trinomial relation

$$g(x)^p + g(x)^q + 1 = 0 \bmod M(x), \tag{4}$$

$p > q$, and $h(x) \equiv 0$, then u_n follows the recurrence relation:

$$u_{n+p} = u_{n+q} \text{ XOR } u_n,$$

where XOR is the bitwise exclusive-or operation. If $x^p + x^q + 1$ is primitive, the period of $u_n, n = 1, 2, ...,$ becomes $2^p - 1$. Furthermore, the sequence $\{u_n\}$ can be quickly generated by the GFSR algorithm with a small amount of initialization cost required to calculate $u_1, ..., u_p$. In our previous paper (Tezuka and Fushimi 1993), we conducted an exhaustive search for the pairs of Fibonacci polynomials $(g(x), M(x))$ that satisfy the above recurrence relation and obtained the best pairs with respect to the two to five dimensional discrepancies for the degrees less than 32. However, it turned out that there exist no pairs $(g(x), M(x))$ satisfying the primitive trinomial relation (4) for the degrees $4, 6, 8,\ 9, 10, 11, 12,\ 13, 14, 16, 19,\ 21, 24, 26,\ 27, 29, 30$, and 32. This is practically unsatisfactory because in most of applications of low discrepancy points we need the point sets of size around 2^{10} through 2^{20}.

3 TABLES OF THE BEST GFSRS WITH PRIMITIVE PENTANOMIALS

In this paper, we consider the case where $g(x)$ satisfies the pentanomial relation

$$g(x)^p + g(x)^{q_1} + g(x)^{q_2} + g(x)^{q_3} + 1 = 0 \bmod M(x), \tag{5}$$

and $h(x) \equiv 0$, where $p > q_1 > q_2 > q_3 > 0$.

The strategy of the search is as follows: By using the recurrence (3), we generate all pairs $(F_{p-1}(x), F_p(x))$, and then for each pair, we check whether $F_{p-1}(x)^p + F_{p-1}(x)^{q_1} + F_{p-1}(x)^{q_2} + F_{p-1}(x)^{q_3} + 1 = 0 \pmod{F_p(x)}$, which comes from the condition (5), where $x^p + x^{q_1} + x^{q_2} + x^{q_3} + 1, p > q_1 > q_2 > q_3 > 0$, is a primitive polynomial. If the check is OK, then the obtained pair is regarded as $(g(x), M(x))$ for the sequence. The validity of this approach is the same as in Tezuka and Fushimi (1993).

In the range $3 \le p \le 21$, we found that for each degree p there exist pairs of Fibonacci polynomials which pass the above check. Then, the best pair is selected by using the criterion: The minimum l such that $\rho^{(k)} \ge p - k - l$ for all $3 \le k \le 5$ is calculated for the obtained generators, and then the generators giving the smallest l are selected for each degree. Among them, we chose the generator with the best figure of merit in dimensions 5 and 6. As a result, exactly one generator was obtained for every p except for $p = 12$, in which two generators exist. The corresponding polynomials $M(x)$ and $g(x)$ are given in Table 1, where we listed only the exponents of the nonzero terms of the polynomials. In this search, we omitted the pair for the reciprocal case, $x^p + x^{p-q_1} + x^{p-q_2} + x^{p-q_3} + 1$, which could be used as well. Also we omitted a pair $(g'(x), M'(x))$, which is obtained by the transformation $(g'(x), M'(x)) = (g(x+1), M(x+1))$.

In Table 2, we summarize the figures of merit in dimensions 2 through 6 for these generators. Since no efficient algorithm for calculation of figures of merit in higher dimensions than two is available at present, the brute force calculation, which is the same as the one in Andre et al. (1990) was done. Notice that for all $2 \le k \le 5$ we have $\rho^{(k)} \ge p - k + 1$ for $p \le 11$; $\rho^{(k)} \ge p - k$ for $p \le 15$; $\rho^{(k)} \ge p - k - 1$ for $p \le 21$.

Table 1: Pairs of Fibonacci Polynomials $(g(x), M(x))$ for the Best Pentanomial GFSR Generators G_{p,q_1,q_2,q_3} for $5 \le p \le 21$

$G_{5,3,2,1}$	M : 0 3 5
	g : 1 4
$G_{6,5,2,1}$	M : 0 1 6
	g : 0 1 2 3 5
$G_{7,5,3,1}$	M : 0 1 2 5 7
	g : 1 3 6
$G_{8,6,5,1}$	M : 0 1 2 3 6 7 8
	g : 0 1 3 6 7
$G_{9,4,3,1}$	M : 0 3 4 5 6 7 9
	g : 0 1 3 5 8
$G_{10,5,2,1}$	M : 0 2 3 5 7 9 10
	g : 1 4 6 7 8 9
$G_{11,8,3,2}$	M : 0 2 3 5 8 10 11
	g : 1 4 5 7 8 9 10
$G_{12,4,2,1}$	M : 0 1 4 7 8 10 12
	g : 0 4 6 11
$G_{12,9,3,2}$	M : 0 3 4 5 6 8 12
	g : 3 4 5 8 9 11
$G_{13,6,5,2}$	M : 0 2 4 7 10 11 13
	g : 0 1 2 3 7 8 9 12
$G_{14,12,2,1}$	M : 0 3 5 6 8 9 11 13 14
	g : 1 3 11 12 13
$G_{15,8,6,5}$	M : 0 1 8 9 11 13 15
	g : 0 5 8 10 11 14
$G_{16,12,10,3}$	M : 0 1 2 8 13 15 16
	g : 0 1 3 5 9 13 14 15
$G_{17,10,7,6}$	M : 0 3 6 8 11 12 17
	g : 3 4 6 7 8 9 10 12 13 14 16
$G_{18,10,8,5}$	M : 0 1 2 3 4 10 11 12 13 15 18
	g : 1 4 7 9 11 12 14 15 17
$G_{19,12,10,4}$	M : 0 1 2 6 7 10 12 13 14 15 16 18 19
	g : 2 3 8 10 11 14 15 16 17 18
$G_{20,11,6,1}$	M : 0 1 2 5 7 9 11 13 14 15 17 19 20
	g : 0 1 3 8 9 11 17 18 19
$G_{21,17,8,3}$	M : 0 2 4 5 6 7 8 10 16 20 21
	g : 1 8 10 13 14 18 19 20

Table 2: Figures of Merit in k Dimensions, $k = 2, ..., 6$, for the Resulting Generators

	$\rho^{(2)}$	$\rho^{(3)}$	$\rho^{(4)}$	$\rho^{(5)}$	$\rho^{(6)}$
$G_{5,3,2,1}$	6	4	4	4	3
$G_{6,5,2,1}$	7	5	3	3	3
$G_{7,5,3,1}$	8	6	6	5	4
$G_{8,6,5,1}$	9	6	5	5	5
$G_{9,4,3,1}$	10	8	6	6	6
$G_{10,5,2,1}$	11	8	8	7	6
$G_{11,8,3,2}$	12	9	8	8	8
$G_{12,4,2,1}$	13	9	9	8	7
$G_{12,9,3,2}$	13	9	9	8	7
$G_{13,6,5,2}$	14	10	10	9	9
$G_{14,12,2,1}$	15	11	10	9	8
$G_{15,8,6,5}$	16	12	11	11	9
$G_{16,12,10,3}$	17	12	12	11	11
$G_{17,10,7,6}$	18	14	13	12	12
$G_{18,10,8,5}$	19	15	13	13	11
$G_{19,12,10,4}$	20	16	14	14	12
$G_{20,11,6,1}$	21	16	15	14	12
$G_{21,17,8,3}$	22	18	16	15	12

4 EXPERIMENTAL RESULTS

Low-discrepancy points are mainly used to construct a set of nodes (sampling points) for multi-dimensional numerical integration, where the speed of generating nodes is very important. Our generator is quite attractive from this point of view, because it can generate one random number by three XOR operations and a normalization because $u_n, n = 1, 2, ...,$ satisfy

$$u_{n+p} = u_{n+q_1} \text{ XOR } u_{n+q_2} \text{ XOR } u_{n+q_3} \text{ XOR } u_n.$$

Here $u_1, ..., u_p$ are initial values calculated by the equation (2) using $(g(x), M(x))$ in Table 1.

We applied four of our generators, $G_{11,8,3,2}$, $G_{14,12,2,1}$, $G_{17,10,7,6}$, and $G_{20,11,6,1}$, to the following five multiple integration problems:

(i) $f_1 = \exp(-\sum_{k=1}^{5} x_k)$,

(ii) $f_2 = x_1x_2x_3x_4x_5 \exp(\sum_{k=1}^{5} x_k^2)$,

(iii) $f_3 = \exp(-\sum_{k=1}^{5} x_k) \sin(-\sum_{k=1}^{5} x_k)$,

(iv) $f_4 = \sqrt{1 + \sum_{k=1}^{5} x_k}$,

(v) $f_5 = 1 + x_1 + 2x_1x_2^2 + 3x_1x_2^2x_3^3 + 4x_1x_2^2x_3^3x_4^4 + 5x_1x_2^2x_3^3x_4^4x_5^5$.

In Table 3, we give initial values $U_n = [2^p u_n], n = 1, ..., p$, for the four generators. Table 4 shows the relative error $E_N(f_i)/I(f_i), i = 1, ..., 5$, where $I(f_i) = \int_{I^5} f_i(x)dx$. Here, we let X_0 be the origin and let $X_n = (u_n, ..., u_{n+4})$ for $n = 1, ..., 2^p - 1$. Observe that the results are almost of order $1/N$.

Table 3: Initial Values for the Four Generators, Where $U_n = [2^p u_n]$

	$G_{11,8,3,2}$	$G_{14,12,2,1}$	$G_{17,10,7,6}$	$G_{20,11,6,1}$
U_1	1024	8192	65536	524288
U_2	757	5187	48304	853599
U_3	1333	2362	92158	956150
U_4	1355	14008	78013	591590
U_5	273	1957	127464	529024
U_6	1922	10841	5901	675699
U_7	808	10642	123275	281973
U_8	1123	10183	118759	239640
U_9	8	6497	68460	54439
U_{10}	1296	4790	87052	257100
U_{11}	157	10522	41304	127295
U_{12}	—	12502	79116	997588
U_{13}	—	15564	27543	795733
U_{14}	—	15715	105387	804259
U_{15}	—	—	50485	199720
U_{16}	—	—	109032	525368
U_{17}	—	—	67451	48081
U_{18}	—	—	—	876740
U_{19}	—	—	—	206167
U_{20}	—	—	—	375723

REFERENCES

Andre, D. A., G. L. Mullen, and H. Niederreiter. 1990. Figures of merit for digital multistep pseudorandom numbers, *Mathematics of Computation* **54**: 737-748.

Fushimi, M. 1989. An equivalence relation between Tausworthe and GFSR sequences and applications, *Applied Mathematics Letters* **2**: 135-137.

Lewis, T. G. and W. H. Payne. 1973. Generalized feedback shift register pseudorandom number algorithm, *Journal of the ACM* **20**: 456-468.

Mesirov, J. P. and M. M. Sweet. 1987. Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2, *Journal of Number Theory* **27**: 144-148.

Mullen, G. L. and H. Niederreiter. 1987. Optimal characteristic polynomials for digital multistep pseudorandom numbers, *Computing* **39**: 155-163.

Niederreiter, H. 1987a. A statistical analysis of generalized feedback shift register pseudorandom number generators, *SIAM Journal on Scientific and Statistical Computation* **8**: 1035-1051.

Niederreiter, H. 1987b. Rational functions with par-

Table 4: Relative Errors of Multiple Integrations Based on the Four Generators ($N = 2^p$)

p	(i)	(ii)	(iii)	(iv)	(v)	$1/N$
11	1.62E-3	1.39E-2	4.22E-4	1.82E-4	5.70E-4	4.88E-4
14	2.01E-4	2.48E-4	9.58E-5	2.27E-5	1.14E-4	6.10E-5
17	1.95E-5	5.83E-5	2.79E-5	2.78E-6	8.50E-6	7.62E-6
20	2.51E-6	5.35E-5	2.95E-6	3.46E-7	1.34E-6	9.53E-7

tial quotients of small degree in their continued fraction expansion, *Monatshefte für Mathematik* **103**: 269-288.

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

Niederreiter, H. 1992. *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conference Series in Applied Mathematics No. 63, SIAM.

Tausworthe, R. C. 1965. Random numbers generated by linear recurrence modulo two, *Mathematics of Computation* **19**: 201-209.

Tezuka, S. 1987. On the discrepancy of GFSR pseudorandom numbers, *Journal of the ACM* **34** : 939-949.

Tezuka, S. 1988. On Fibonacci polynomials, *Proceedings of the IPSJ Meeting on Algorithms* **3-7**, IPSJ (in Japanese).

Tezuka, S. 1989. Low-discrepancy point sets based on a lattice in $GF\{2, x\}^k$, *Proceedings of the IPSJ Meeting on Numerical Analysis* **31-1**, IPSJ.

Tezuka, S. 1990. Lattice structure of pseudorandom sequences from shift register generators. In *Proceedings of the 1990 Winter Simulation Conference*, eds. O. Balci, R. P. Sadowski, and R. E. Nance, 266-269. Institute of Electrical and Electronics Engineers, New Orleans, Louisiana.

Tezuka, S., and M. Fushimi. 1993. Calculation of Fibonacci polynomials for GFSR sequences with low discrepancies, to appear in *Mathematics of Computation*.

AUTHOR BIOGRAPHIES

SHU TEZUKA is an advisory researcher at IBM Research, Tokyo Research Laboratory. His research interests are random number generation, quasi-Monte Carlo methods, global optimization, and stochastic simulation. He is a member of ACM, IEEE, SIAM, an editor of IPSJ, and a councilor of SITA.

MASANORI FUSHIMI is a Professor in the Department of Mathematical Engineering and Information Physics at the University of Tokyo. His research interests include statistical computations, random number generation, and numerical analysis. He is a council member of the Operations Research Society of Japan.