MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 202
APRIL 1993, PAGES 763–770

CALCULATION OF FIBONACCI POLYNOMIALS FOR GFSR SEQUENCES WITH LOW DISCREPANCIES

SHU TEZUKA AND MASANORI FUSHIMI

ABSTRACT. Fibonacci polynomials are defined in the context of the two-dimensional discrepancy of Tausworthe pseudorandom sequences as an analogue to Fibonacci numbers, which give the best figure of merit for the two-dimensional discrepancy of linear congruential sequences. We conduct an exhaustive search for the Fibonacci polynomials of degree less than 32 whose associated Tausworthe sequences can be easily implemented and very quickly generated.

1. INTRODUCTION

The major part of the theory of linear congruential sequences was developed in the 1960s and 70s. (The most comprehensive reference on this subject is the book by Knuth [4].) One of the most interesting results obtained in that period is the fact that the autocorrelation property of linear congruential sequences can be characterized by using the partial quotients in the continued fraction expansions associated with the linear congruential generators. To be specific, we have the best autocorrelation performance for the linear congruential sequences when their modulus and multiplier are selected as a consecutive pair of Fibonacci numbers. It is also known [12] that the autocorrelation can be bounded from above by the corresponding two-dimensional discrepancy. Borosh and Niederreiter [2] made an exhaustive search for good parameters in terms of this criterion.

For the digital multistep sequences, the special subclass of Tausworthe sequences, Mullen and Niederreiter [7] obtained the figure of merit for the discrepancy of the sequences, and defined Fibonacci polynomials based on the two-dimensional case of their results. Further, they conducted an exhaustive search for the Fibonacci polynomials based on their definition. Recently, Tausworthe sequences have been shown to be formulated as linear congruential sequences in terms of polynomial arithmetic modulo two [16]. This result has the important consequence that we can derive a systematized theory for Tausworthe sequences analogous to that of linear congruential sequences. For example, in the paper [18] Tezuka developed the theory on the lattice structure of Tausworthe sequences. Another consequence of the result is a more general definition of Fibonacci polynomials, which directly correspond to Fibonacci numbers and

Received by the editor June 26, 1991 and, in revised form, February 29, 1992.
1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 11T06, 11Y65.
Key words and phrases. Tausworthe sequences, Fibonacci polynomials, discrepancy, GFSR algorithms.

0025-5718/93 $1.00 + $.25 per page

linear congruential sequences. The merit of this generalization is that there are many Fibonacci polynomials which are primitive, while the original Fibonacci polynomials as defined in [7] are rarely primitive.

The objective of this paper is to provide the parameters of Tausworthe sequences with the following properties: (1) the parameters are best possible with respect to the two-dimensional discrepancy, and (2) the sequences can be generated very fast, i.e., one pseudorandom number is generated with one exclusive-or (XOR) operation. The paper is organized as follows. Section 2 briefly overviews the definition of Tausworthe sequences and defines Fibonacci polynomials based on the theorem for the two-dimensional discrepancy of the sequences. In §3, we describe an exhaustive search conducted for finding Fibonacci polynomials whose corresponding Tausworthe sequence can be generated by using the GFSR (Generalized Feedback Shift Register) algorithm [5]. Section 4 gives some comparisons with the generators obtained in André et al. [1].

2. Overview of Tausworthe sequences

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 $GF(2)$. Here we define linear congruential sequences in $GF\{2, x\}$. Let σ be a mapping from $GF\{2, x\}$ to the real field, defined by

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

Then a pseudorandom sequence u_n, $n = 1, 2, \ldots$, in [0,1) is defined by

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

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 index $-L$ to m, rather than from $-\infty$ to m.

We will show that a Tausworthe sequence is a special case of the above general class. Let $M(x) = x^p + c_1 x^{p-1} + \cdots + c_p$ be a primitive polynomial of degree p over $GF(2)$, $h(x) \equiv 0$, $g(x) = (x^s \bmod M(x))$, with $0 < s < 2^p - 1$, $\gcd(s, 2^p - 1) = 1$, $m = -1$, and L be the "word-size". Suppose $f_0(x)/M(x) = a_1 x^{-1} + a_2 x^{-2} + \cdots$. Then $M(x) \times (a_1 x^{-1} + a_2 x^{-2} + \cdots) = f_0(x)$, i.e., no fractional terms exist in the left-hand side. Hence, a_n, $n = p + 1, p + 2, \ldots$, satisfies the recurrence relation $a_n = c_1 a_{n-1} + \cdots + c_p a_{n-p} \pmod 2$ whose characteristic polynomial is $M(x)$. Therefore, the sequence is written, for $n = 1, 2, \ldots$, as

$$u_n = \sum_{j=1}^{L} a_{ns+j} 2^{-j}. \tag{2}$$

This sequence is identical with the Tausworthe sequence defined in [13]. Note that the digital multistep sequences defined by Niederreiter [12] are a special case of Tausworthe sequences, i.e., $2 \le s = L \le p$.

The discrepancy of Tausworthe sequences has been obtained in [9, 11, 14, 17]. The result can be rewritten as follows based on the formulation given above in (1). Here we define $\deg(0) = -1$.

Theorem 1. *Let*

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

where the minimum is taken over all nonzero polynomial solutions $(h_1(x), \ldots, h_k(x))$ *of the equation*

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

Then the k-dimensional discrepancy of the Tausworthe sequence over the full period satisfies

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

where $N = 2^p$.

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

Note that Theorem 1 also holds for the sequence defined by (1) if the period is $2^p - 1$, where p is the degree of $M(x)$ [9, 11, 14, 17].

2.1. **Definition of Fibonacci polynomials.** For the two-dimensional case, the next theorem [15] links the continued fraction expansion of $g(x)/M(x)$ to the two-dimensional discrepancy. The proof, which is almost the same as, but simpler than, that of the special case of $g(x) = x^p$ in [8], is included for the reader's convenience.

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

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

Then we have

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

Proof. Since $h_1 + h_2 g = 0 \pmod M$, there exists a polynomial l with degree $< p$ such that $h_1 = h_2 g + lM$. Then we have

$$\begin{aligned} \rho^{(2)} - 2 &= \min(\deg(h_1) + \deg(h_2)) \\ &= \min(\deg(h_2 g + lM) + \deg(h_2)) \\ &= \min(\deg(M) + \deg(l/h_2 + g/M) + 2\deg(h_2)) \\ &= p + \min(\deg(l/h_2 + g/M) + 2\deg(h_2)), \end{aligned}$$

where the minimum is taken over all l and h_2 with degree $< p$ except for $h_2 = 0$, and the degree of a rational function is defined to be the degree of the numerator minus the degree of the denominator. The continued fraction expansion of g/M is $[A_1, \ldots, A_s]$. For $i = 1, 2, \ldots, s$, the convergents are written as

$$\frac{P_i}{Q_i} = [A_1, \ldots, A_i].$$

The numerators P_i and denominators Q_i can be obtained by

$$P_{-1} = 1, \quad P_0 = 0, \quad P_i = A_i P_{i-1} + P_{i-2}, \qquad i = 1, \ldots, s,$$
$$Q_{-1} = 0, \quad Q_0 = 1, \quad Q_i = A_i Q_{i-1} + Q_{i-2}, \qquad i = 1, \ldots, s.$$

Here, $\deg(Q_r) = \sum_{j=1}^{r} \deg(A_j)$ and $\deg(Q_s) = \deg(M) = p$. If $\deg(Q_r) \leq \deg(h_2) < \deg(Q_{r+1})$ for some r, $0 \leq r < s$, then

$$\begin{aligned}
&\deg(l/h_2 + g/M) + 2\deg(h_2) \\
&\quad \geq \deg(P_r/Q_r + g/M) + 2\deg(Q_r) = -\deg(Q_r Q_{r+1}) + 2\deg(Q_r) \\
&\quad = -\deg(Q_r) - \deg(Q_{r+1}) + 2\deg(Q_r) \\
&\quad = \deg(Q_r) - \deg(Q_{r+1}) = -\deg(A_{r+1}).
\end{aligned}$$

The first inequality comes from the fact that the continued fraction gives the best approximation of g/M. Hence we obtain

$$\rho^{(2)} = p + 2 + \min_{0 \leq r < s} (-\deg(A_{r+1})). \quad \square$$

Note that there exists a pair of polynomials $(a(x), b(x))$ for any degree of $b(x)$ such that the degrees of partial quotients in the continued fraction expansion of $a(x)/b(x)$ are all one. Some properties of this kind of pair have recently been investigated in [6, 10].

Here, we introduce the definition of Fibonacci polynomials.

Definition 1. A pair of polynomials $(a(x), b(x))$ with $\deg(a(x)) = \deg(b(x)) - 1$ 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.

Our definition can be viewed as a generalization of that of Mullen and Niederreiter [7], where a polynomial $a(x)$ of degree p is called a Fibonacci polynomial if the maximum degree of the partial quotients in the continued fraction expansion of $a(x)/x^p$ is one. The result in [6] claims that for each irreducible polynomial $b(x)$ there exist exactly two pairs of Fibonacci polynomials $(a(x), b(x))$.

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

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

where $F_0(x) = 1$, $F_1(x) = A_1(x)$, and $A_i(x)$, $i = 1, 2, \ldots$, 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.

2.2. **GFSR implementation of Tausworthe sequences.** Some subclass of Tausworthe sequences can be implemented by using the GFSR algorithm [3, 5, 19], which uses the following recurrence relation:

$$u_n = u_{n-p+q} \,\mathrm{XOR}\, u_{n-p}, \tag{4}$$

where XOR is the bit-wise exclusive-or operation. Since a Tausworthe sequence is given by (2), if the decimated sequence $\{a_{ns}: n = 1, 2, \ldots\}$ satisfies a recurrence relation whose characteristic polynomial is a primitive trinomial $x^p + x^q + 1$, $p > q$, then the Tausworthe sequence $\{u_n\}$ can be quickly generated by the GFSR algorithm with a small amount of initialization cost required to

calculate $u_1, \ldots, u_p$. Note that the recurrence relation (4) corresponds to the scheme (1) such that

$$g(x)^p + g(x)^q + 1 = 0 \pmod{M(x)}, \tag{5}$$

and $h(x) \equiv 0$.

3. Exhaustive search for the best generators

There are many pairs $(a(x), b(x))$ of Fibonacci polynomials for a given degree of $b(x)$. As pointed out in [10], 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. That is why we tabulate only the generators which can be implemented by the GFSR algorithm. 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 $(F_{p-1}(x))^p + (F_{p-1}(x))^q + 1 = 0 \pmod{F_p(x)}$, which comes from the condition (5), where $x^p + x^q + 1$, $p > q$, is a primitive polynomial. If the check passes, then the pair obtained is regarded as $(g(x), M(x))$ for the Tausworthe sequence. The validity of this approach is as follows: Since $x^p + x^q + 1$, $p > q$, is a primitive polynomial, the resulting sequence u_n, $n = 1, 2, \ldots$, has a period of $2^p - 1$, i.e., the sequence $f_n(x)/M(x)$, $n = 1, 2, \ldots$, is also of period $2^p - 1$. The fact that $f_n(x)$, $n = 1, 2, \ldots$, has a period of $2^p - 1$ implies that $M(x)$ is irreducible and $g(x)$ is a primitive root modulo $M(x)$ [16]. Strictly speaking, $M(x)$ should be primitive from the definition of a Tausworthe sequence in (2).

Table 1. The generators $G(p, q)$ resulting from the GFSR recurrence relation, $u_n = u_{n-p+q}$ XOR u_{n-p}

$G(3, 1): M$	0 1 3
g	2
$G(5, 2): M$	0 1 2 3 5
g	1 4
$G(7, 1): M$	0 1 2 4 5 6 7
g	2 5 6
$G(15, 1): M$	0 1 5 7 9 11 12 14 15
g	0 3 5 10 11 12 13 14
$G(17, 5): M$	0 4 5 6 11 14 15 16 17
g	7 9 12 15 16
$G(18, 7): M$	0 1 2 3 4 5 8 10 13 14 18
g	0 1 3 4 6 8 12 14 15 17
$G(20, 3): M$	0 2 4 6 10 12 13 14 15 16 20
g	1 3 4 5 6 7 9 10 16 17 19
$G(22, 1): M$	0 1 5 6 7 9 10 12 13 14 15 16 18 19 22
g	0 3 6 8 14 16 19 21
$G(23, 5): M$	0 1 4 5 7 8 9 11 13 14 16 17 18 19 20 21 23
g	1 3 6 7 8 9 11 18 22
$G(25, 3): M$	0 1 6 9 11 14 16 18 19 23 25
g	0 3 7 9 11 12 13 14 21 24
$G(28, 3): M$	0 1 3 4 5 8 9 10 11 12 15 20 21 22 23 24 26 27 28
g	0 1 2 3 4 5 6 7 9 10 11 12 13 14 15 16 17 18 19 21 22 24 26 27
$G(31, 13): M$	0 1 2 3 5 7 8 9 11 12 13 14 16 17 18 19 22 27 28 30 31
g	1 4 8 9 13 15 19 24 26 28 30

TABLE 2. Figures of merit in k dimensions, $k = 2, \ldots, 6$, for the resulting generators

	$\rho^{(2)}$	$\rho^{(3)}$	$\rho^{(4)}$	$\rho^{(5)}$	$\rho^{(6)}$
$G(3, 1)$	4	3	3	3	3
$G(5, 2)$	6	4	4	4	3
$G(7, 1)$	8	5	5	5	5
$G(15, 1)$	16	12	11	7	7
$G(17, 5)$	18	14	12	11	7
$G(18, 7)$	19	14	13	12	11
$G(20, 3)$	21	14	14	12	12
$G(22, 1)$	23	17	17	15	13
$G(23, 5)$	24	16	15	15	15
$G(25, 3)$	26	20	19	17	15
$G(28, 3)$	29	24	23	18	18
$G(31, 13)$	32	24	24	22	19

However, we deal with a more general case where $M(x)$ is irreducible and the condition (5) is satisfied, because our objective is to find the pair $(g(x), M(x))$ which can be implemented by the recurrence relation (4).

In the range $3 \leq p \leq 32$, we found that there exist pairs of Fibonacci polynomials which pass the above check only for $p = 3, 5, 7, 15, 17, 18, 20, 22, 23, 25, 28,$ and 31. For each degree, the best pair is selected by using the criterion: The minimum l such that $\rho^{(k)} \geq p - k - l$ for all $3 \leq k \leq 5$ is calculated for the generators obtained, and then the generator giving the smallest l is selected for each degree. As a result, twelve generators are obtained in total. The corresponding polynomials $M(x)$ and $g(x)$ are given in Table 1, where we list only the exponents of the nonzero terms of the polynomials. Note that the $M(x)$'s for $G(20, 3)$ and $G(22, 1)$ are irreducible but not primitive. Here we omitted the pair for the reciprocal case, $x^p + x^{p-q} + 1$, 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 the calculation of figures of merit in higher dimensions than two is available at present, a brute force calculation, which is the same as the one in André et al. [1], was used.

4. COMPARISON AND DISCUSSION

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 integer random number by one bit-wise exclusive-or (XOR) operation, and we need one division (by 2^p) for normalization. On the other hand, the digital multistep pseudorandom number generator obtained by Mullen and Niederreiter [7] and André et al. [1] needs $m(:=$ #(nonzero terms of $M(x)) - 2)$ XOR operations to compute *one bit* of an integer random number, so that we need $m \times p$ XOR operations followed by some shifts and additions to get an integer random number.

Comparing the figures of merit in Table 2 with those of the universally optimal generators in [1], their generators are slightly better in dimensions three

TABLE 3. The generators G_i, $i = 1, \ldots, 4$, resulting from the GFSR recurrence relation $u_n = u_{n-31+q}$ XOR u_{n-31}, where $q = 3, 6,$ or 13

G_1	M	0 2 4 8 10 12 13 16 20 21 22 26 28 30 31
$q = 3$	g	1 5 9 13 14 17 20 21 23 24 27 28 30
G_2	M	0 3 4 8 10 15 16 19 25 28 29 30 31
$q = 6$	g	0 1 3 5 6 9 10 15 16 17 18 19 20 21 22 26 27 29 30
G_3	M	0 3 5 6 7 8 12 13 15 16 18 19 20 23 24 25 26 27 29 30 31
$q = 6$	g	1 3 8 9 10 11 12 13 14 22 23 30
G_4	M	0 1 2 3 5 7 8 9 11 12 13 14 16 17 18 19 22 27 28 30 31
$q = 13$	g	1 4 8 9 13 15 19 24 26 28 30

TABLE 4. Figures of merit in k dimensions, $k = 2, \ldots, 6$, for the resulting generators

	$\rho^{(2)}$	$\rho^{(3)}$	$\rho^{(4)}$	$\rho^{(5)}$	$\rho^{(6)}$
G_1	32	23	23	22	20
G_2	32	24	22	20	20
G_3	32	25	25	20	20
G_4	32	24	24	22	19

five for any degree. However, all the generators in Table 1 are the best in terms of the two-dimensional discrepancy, while all the generators listed in André et al. are not. Tables 3 and 4 show all generators of degree 31 which we found. In comparison with the universally optimal generator of degree 31, whose figures of merits are 31, 25, 25, 24, and 20 in the dimensions two to six, respectively, the generator G_3 is almost comparable.

ACKNOWLEDGMENT

The authors are grateful to the referee for his valuable comments on the first draft of the manuscript.

BIBLIOGRAPHY

1. D. A. André, G. L. Mullen, and H. Niederreiter, *Figures of merit for digital multistep pseudorandom numbers*, Math. Comp. **54** (1990), 737-748.
2. I. Borosh and H. Niederreiter, *Optimal multipliers for pseudorandom number generation by the linear congruential method*, BIT **23** (1983), 65-74.
3. M. Fushimi, *An equivalence relation between Tausworthe and GFSR sequences and applications*, Applied Math. Lett. **2** (1989), 135-137.
4. D. E. Knuth, *The art of computer programming*: Vol. 2, *Seminumerical algorithms*, 2nd ed., Addison-Wesley, Reading, MA, 1981.
5. T. G. Lewis and W. H. Payne, *Generalized feedback shift register pseudorandom number algorithm*, J. Assoc. Comput. Mach. **20** (1973), 456-468.
6. J. P. Mesirov and M. M. Sweet, *Continued fraction expansions of rational expressions with irreducible denominators in characteristic* 2, J. Number Theory **27** (1987), 144-148.
7. G. L. Mullen and H. Niederreiter, *Optimal characteristic polynomials for digital multistep pseudorandom numbers*, Computing **39** (1987), 155-163.
8. H. Niederreiter, *Pseudozufallszahlen und die Theorie der Gleichverteilung*, Sitzungsber. Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **195** (1986), 109-138.
9. ——, *A statistical analysis of generalized feedback shift register pseudorandom number generators*, SIAM J. Sci. Statist. Comput. **8** (1987), 1035-1051.

10. ____, *Rational functions with partial quotients of small degree in their continued fraction expansion*, Monatsh. Math. **103** (1987), 269-288.
11. ____, *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273-337.
12. ____, *The serial test for digital k-step pseudorandom numbers*, Math. J. Okayama Univ. **30** (1988), 93-119.
13. R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two*, Math. Comp. **19** (1965), 201-209.
14. S. Tezuka, *On the discrepancy of GFSR pseudorandom numbers*, J. Assoc. Comput. Mach. **34** (1987), 939-949.
15. ____, *On Fibonacci polynomials*, Proc. of the IPSJ meeting on Algorithms, 3-7, Information Processing Soc. Japan, 1988. (in Japanese).
16. ____, *Random number generation based on polynomial arithmetic modulo two*, IBM TRL Research Report, RT-0017 (Oct. 1989).
17. ____, *Low-discrepancy point sets based on a lattice in* $GF\{2, x\}^k$, Proc. of the IPSJ meeting on Numerical Analysis, 31-1, Information Processing Soc. Japan, 1989.
18. ____, *Lattice structure of pseudorandom sequences from shift register generators*, Proceedings of the Winter Simulation Conference '90 (O. Balci, R. P. Sadowski, and R. E. Nance, eds.), IEEE Press, 1990, pp. 266-269.
19. J. P. R. Tootill, W. D. Robinson, and D. J. Eagle, *An asymptotically random Tausworthe sequence*, J. Assoc. Comput. Mach. **20** (1973), 469-481.

IBM Research, Tokyo Research Laboratory, 5-11 Sanbancho, Chiyoda-ku, Tokyo 102, Japan
E-mail address: tezuka@trlvm.vnet.ibm.com

Faculty of Engineering, University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo 113, Japan
E-mail address: fushimi@misojiro.t.u-tokyo.ac.jp