MATHEMATICS OF COMPUTATION
VOLUME 54, NUMBER 190
APRIL 1990, PAGES 737–748

FIGURES OF MERIT FOR DIGITAL MULTISTEP PSEUDORANDOM NUMBERS

DEBRA A. ANDRÉ, GARY L. MULLEN, AND HARALD NIEDERREITER

ABSTRACT. The statistical independence properties of s successive digital multistep pseudorandom numbers are governed by the figure of merit $\rho^{(s)}(f)$ which depends on s and the characteristic polynomial f of the recursion used in the generation procedure. We extend previous work for $s = 2$ and describe how to obtain large figures of merit for $s > 2$, thus arriving at digital multistep pseudorandom numbers with attractive statistical independence properties. Tables of figures of merit for $s = 3, 4, 5$ and degrees ≤ 32 are included.

I. INTRODUCTION

The well-known linear congruential method for the generation of uniform pseudorandom numbers in the interval [0, 1] is based on the one-step recursion

$$y_{n+1} \equiv by_n + c \mod M \quad \text{for } n = 0, 1, \ldots,$$

where the modulus M is a large integer, b is a suitably chosen integer coprime to M, c is an integer, and the y_n are integers with $0 \leq y_n < M$. A sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers is obtained by the scaling $x_n = y_n/M$. Since these pseudorandom numbers have some undesirable features, such as their lattice structure (see e.g. Knuth [2, Chapter 3]), other pseudorandom number generators have recently received increased attention.

The idea of using multistep recursions for pseudorandom number generation is usually attributed to Tausworthe [12] but can be traced back to the 1950's (see e.g. van Wijngaarden [13]). The generation of uniform pseudorandom numbers by k-step recursions with $k \geq 2$ proceeds as follows. First, we generate a sequence $y_0, y_1, \ldots$ of bits by the recursion

$$y_{n+k} \equiv b_{k-1}y_{n+k-1} + \cdots + b_0y_n \mod 2 \quad \text{for } n = 0, 1, \ldots, \tag{1}$$

where the b_i are fixed bits with $b_0 = 1$ and where the initial values $y_0, y_1, \ldots, y_{k-1}$ are not all 0. The sequence of y_n is periodic, and to maximize the length of its least period for given k, we assume from now on that the

Received January 12, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C10; Secondary 11T06, 11Y65.
The second author would like to thank the National Security Agency for partial support under grant agreement #MDA904-87-H-2023.

0025-5718/90 $1.00 + $.25 per page

characteristic polynomial

$$f(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0 \tag{2}$$

of the recursion (1), considered as a polynomial over the binary field F_2, is a primitive polynomial. We recall that a polynomial over F_2 of degree k is called *primitive* if its roots are generators of the cyclic group F_q^*, the multiplicative group of nonzero elements of the finite field F_q with $q = 2^k$ elements (compare with Lidl and Niederreiter [3, Chapter 3]).

The bits y_n generated by (1) are transformed into a sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers in [0, 1] by setting

$$x_n = \sum_{j=1}^{k} y_{kn+j-1}2^{-j} \quad \text{for } n = 0, 1, \ldots . \tag{3}$$

In other words, we obtain the numbers x_n by splitting up the sequence $y_0, y_1, \ldots$ into consecutive blocks of length k and then interpreting each block as the dyadic expansion of a number in $[0, 1)$ (more generally, one may take any block length m with $2 \leq m \leq k$, but we restrict the attention to the most common case $m = k$). The numbers x_n in (3) are called *digital k-step pseudorandom numbers.* We assume from now on that $\gcd(k, 2^k - 1) = 1$; then the sequence $x_0, x_1, \ldots$ is purely periodic and its least period length is $\tau = 2^k - 1$. For these and other elementary properties of digital k-step pseudorandom numbers we refer to Knuth [2, Chapter 3], Lidl and Niederreiter [3, Chapter 7], and Niederreiter [6]. We note that the construction of digital multistep pseudorandom numbers may be carried out in an arbitrary prime base p, but that the base $p = 2$ with which we work is the most convenient one for practical implementations.

For many simulation purposes the most desirable property of a sequence of uniform pseudorandom numbers is that of statistical independence of successive terms. In the case of digital multistep pseudorandom numbers, theoretical results on statistical independence properties are available and they will be described in detail in §2. The essential feature of these results is that in order to have any s successive digital k-step pseudorandom numbers close to statistical independence, the characteristic polynomial f in (2) has to be chosen carefully. The suitability of f is measured by the figure of merit $\rho^{(s)}(f)$ which will be defined in Definition 2 and depends on f and also on the prescribed value of s. The larger the figure of merit $\rho^{(s)}(f)$, the closer we are to statistical independence of any s successive digital k-step pseudorandom numbers. This leads to the computational problem of finding primitive polynomials f over F_2 with a large value of $\rho^{(s)}(f)$ for given $s \geq 2$. It is inherent in the nature of this problem that the required computational effort increases with s. The simplest case $s = 2$ was treated by Mullen and Niederreiter [4]. In the present paper we deal with larger values of s. In this way we arrive at concrete digital

multistep pseudorandom numbers with very attractive statistical independence properties.

2. Theoretical background

The statistical independence properties of a sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers in $[0, 1]$ can be analyzed as follows. For fixed $s \geq 2$ consider the points

$$X_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0, 1]^s \quad \text{for } n = 0, 1, \ldots . \tag{4}$$

In the ideal case where $x_0, x_1, \ldots$ is a sequence of uniformly distributed and independent random variables, the probability that X_n falls into a given interval $J \subseteq [0, 1]^s$ is equal to the volume $V(J)$ of J. Therefore, the statistical independence properties of the pseudorandom numbers x_n can be tested by comparing the actual distribution of the points X_n in (4) with this ideal case. The following definition from [9, §2] describes point sets for which the relative frequency of points in J is equal to $V(J)$ for a whole family of intervals J.

Definition 1. Let $0 \leq t \leq k$ be integers. A (t, k, s)-*net* (in base 2) is a set P of 2^k points in $[0, 1)^s$ with the following property: every interval $J \subseteq [0, 1)^s$ of the form

$$J = \prod_{i=1}^{s} [a_i 2^{-e_i}, (a_i + 1)2^{-e_i}) \tag{5}$$

with integers a_i and e_i and with $V(J) = 2^{t-k}$ contains exactly 2^t points of P.

It follows from Definition 1 that if P is a (t, k, s)-net and $J \subseteq [0, 1)^s$ is an interval of the form (5) with $V(J) \geq 2^{t-k}$, or a finite disjoint union of such intervals, then J contains exactly $2^k V(J)$ points of P. In particular, Definition 1 becomes stronger for smaller values of t. Further details and numerous results concerning (t, k, s)-nets can be found in Niederreiter [9].

If $x_0, x_1, \ldots$ is a sequence of digital k-step pseudorandom numbers, then consider the points X_n in (4) over the full period, i.e., for $0 \leq n \leq \tau - 1 = 2^k - 2$. According to Theorem A below, which is a special case of [9, Theorem 9.1], these points together with $\mathbf{0} = (0, \ldots, 0)$ form a (t, k, s)-net with a value of t that depends on the figure of merit $\rho^{(s)}(f)$ defined in Definition 2. We write again F_q for the finite field with $q = 2^k$ elements and note that F_q can be viewed as a vector space of dimension k over F_2.

Definition 2. For any $s \geq 2$ and any characteristic polynomial f of degree k, the *figure of merit* $\rho^{(s)}(f)$ is defined by

$$\rho^{(s)}(f) = \min \sum_{i=1}^{s} d_i,$$

where the minimum is extended over all s-tuples $(d_1, \ldots, d_s) \neq (0, \ldots, 0)$ of integers with $0 \leq d_i \leq k$ for $1 \leq i \leq s$ such that the elements $\alpha^{(i-1)k+j-1}$, $1 \leq j \leq d_i$, $1 \leq i \leq s$, are linearly dependent over F_2. Here α is a fixed root of f in F_q (the value of $\rho^{(s)}(f)$ does not depend on the specific choice of α, since f is assumed to be primitive, and hence irreducible over F_2).

Theorem A. *Let $x_0, x_1, \ldots$ be digital k-step pseudorandom numbers and let f be the characteristic polynomial. Then for any $s \geq 2$ the points $\mathbf{0}, X_0, X_1, \ldots, X_{\tau-1}$ form a (t, k, s)-net with $t = k + 1 - \rho^{(s)}(f)$.*

It is clear from Definition 2 that we always have $2 \leq \rho^{(s)}(f) \leq k + 1$. Since the property expressed in Theorem A is stronger the smaller the value of t, the desirable choices for f are those for which $\rho^{(s)}(f)$ is large.

The considerations above are closely connected with the *s-dimensional serial test*, which is a standard test for the statistical independence of s successive uniform pseudorandom numbers (see Knuth [2, Chapter 3] and Niederreiter [5]). Let $x_0, x_1, \ldots$ be a sequence of uniform pseudorandom numbers in $[0, 1]$, and for given $s \geq 2$ define the points X_n by (4). Then define the *discrepancy*

$$D_N^{(s)} = \sup_J \left| \frac{1}{N} \#\{n < N : X_n \in J\} - V(J) \right| \quad \text{for } N \geq 1,$$

where the supremum is extended over all intervals $J = \prod_{i=1}^{s} [0, u_i) \subseteq [0, 1)^s$. The sequence $x_0, x_1, \ldots$ passes the s-dimensional serial test if $D_N^{(s)}$ is small for large N. For digital k-step pseudorandom numbers we have the following result on $D_N^{(s)}$ for the full period, i.e., for $N = \tau = 2^k - 1$; a similar result for $N < \tau$ is also known (see [10]).

Theorem B. *For digital k-step pseudorandom numbers and any $s \geq 2$, we have*

$$2^{-\rho-1} \leq D_\tau^{(s)} \leq \frac{\rho^{s-1}}{(s-1)!} 2^{-\rho+1} + O(\rho^{s-2} 2^{-\rho})$$

with $\rho = \rho^{(s)}(f)$, where the implied constant in the O-term is effective and depends only on s.

The lower bound in Theorem B is a special case of [7, Satz 10], and the upper bound is a special case of [9, Theorem 9.4]. Theorem B shows that in order to get a small discrepancy $D_\tau^{(s)}$, we have to choose f in such a way that $\rho^{(s)}(f)$ is large.

Thus, Theorems A and B lead to the same conclusion, namely that the suitability of a characteristic polynomial f can be measured by the figure of merit $\rho^{(s)}(f)$, and that $\rho^{(s)}(f)$ should be as large as possible. It is clear from Definition 2 that, as the notation suggests, $\rho^{(s)}(f)$ depends also on s. Characteristic polynomials f for which $\rho^{(s)}(f)$ is large for several values of s, such as

$s = 2, 3, 4, 5$, are of particular interest. It is easy to see that

$$\rho^{(s)}(f) \leq \rho^{(r)}(f) \quad \text{for } s \geq r, \tag{6}$$

hence if $\rho^{(s)}(f)$ is large for some s, it is necessarily large for all smaller values of s.

3. Computational results

In searching for primitive polynomials f of degree k with large figure of merit $\rho^{(s)}(f)$ for $s \geq 3$, we first require that such f be optimal characteristic polynomials for the $s = 2$ case as discussed in Mullen and Niederreiter [4]. To be more specific, if f is the characteristic polynomial of degree k as in (2), then the rational function $f(x)/x^k$ has a unique continued fraction expansion

$$\frac{f(x)}{x^k} = 1 + 1/(A_1 + 1/(A_2 + \cdots + 1/A_h)) =: [1, A_1, A_2, \ldots, A_h],$$

where A_i is a polynomial over F_2 with $\deg(A_i) \geq 1$ for $1 \leq i \leq h$. The partial quotients $A_1, A_2, \ldots, A_h$ can be calculated by the Euclidean algorithm. We put

$$L(f) = \max_{1 \leq i \leq h} \deg(A_i),$$

so that $L(f)$ is an integer with $1 \leq L(f) \leq k$. It was shown in Niederreiter [7, Satz 12] that

$$\rho^{(2)}(f) = k + 2 - L(f). \tag{7}$$

Hence, in order to make $\rho^{(2)}(f)$ as large as possible for a fixed k (i.e., to obtain an *optimal characteristic polynomial*), one would like to have $L(f) = 1$; however, it turns out that this is usually not feasible for the following reason.

As shown in Niederreiter [8], for every $k \geq 1$, there exists a unique polynomial f_k over F_2 of degree k with $f_k(0) \neq 0$ and $L(f_k) = 1$. Moreover, $f_k(x)$ is given by

$$f_k(x) = \sum_{j=0}^{d+1} x^{k - \lfloor k/2^j \rfloor},$$

where the integer d is defined by $2^d \leq k < 2^{d+1}$ and $\lfloor w \rfloor$ denotes the greatest integer $\leq w$. Unfortunately, as indicated in Mullen and Niederreiter [4], most of these polynomials are not even irreducible, let alone primitive (in fact, in the range $2 \leq k \leq 32$, the only primitive polynomials f_k are f_2, f_3, and f_{10}). Hence, most are not optimal characteristic polynomials for the $s = 2$ case.

Since there are so few primitive polynomials f with $L(f) = 1$, primitive polynomials with $L(f) = 2$ were also considered by Mullen and Niederreiter [4]. On the basis of calculations performed for [4], there appear to be, in general, a number of primitive polynomials f with $L(f) = 2$ for each degree k.

For each $k \leq 21$, an exhaustive search was conducted by machine (an IBM 3090/400 computer) to locate all primitive polynomials f of degree k over

TABLE 1
Primitive polynomials f with large $\rho^{(3)}(f)$ values

k	$\rho^{(3)}(f)$	f
3	3	0 1 3
4	4	0 3 4
5	5	0 1 2 3 5
*6	4	0 1 2 5 6
7	6	0 1 3 6 7
8	7	0 1 2 5 6 7 8
9	8	0 5 6 8 9
10	9	0 1 3 5 6 8 10
11	10	0 6 8 9 11
*12	11	0 2 5 7 9 10 12
13	11	0 1 2 5 6 7 8 10 11 12 13
14	12	0 1 2 3 9 12 14
15	13	0 1 6 7 8 9 13 14 15
16	14	0 1 2 3 4 6 7 9 11 14 16
17	15	0 2 4 5 6 11 12 14 15 16 17
*18	16	0 2 5 6 7 9 10 13 15 16 18
19	17	0 1 2 4 6 9 10 14 15 17 19
*20	18	0 1 2 4 9 11 12 15 17 18 20
*21	19	0 2 3 6 9 10 11 12 13 14 17 19 21
22	20	0 1 2 3 9 16 17 19 20 21 22
23	21	0 1 2 4 6 9 10 12 13 14 18 19 20 21 23
*24	21	0 1 2 3 4 5 6 9 10 11 12 14 15 16 17 20 21 22 24
25	22	0 1 2 3 4 5 6 9 12 13 14 15 17 19 20 21 22 24 25
26	23	0 1 2 3 4 5 6 7 9 12 14 15 16 19 22 24 26
27	24	0 1 2 3 4 5 6 7 11 13 14 15 18 19 23 26 27
28	25	0 1 2 3 4 5 6 7 8 9 13 14 17 18 23 24 25 26 28
29	26	0 1 3 4 11 16 18 20 23 25 27 28 29
*30	27	0 1 3 5 6 7 8 10 13 14 15 20 23 24 27 29 30
31	28	0 1 2 3 4 5 6 7 8 9 10 14 15 18 22 23 27 29 31
32	29	0 1 2 3 4 5 6 7 8 9 12 15 19 20 21 23 25 26 27 28 29 31 32

F_2 with $L(f) \leq 2$. For $22 \leq k \leq 32$, nonexhaustive collections of primitive polynomials of degree k with $L(f) \leq 2$ were obtained. By having $k \leq 32$, one can take full advantage of the precision of a 32-bit machine. While stopping at $k = 64$ would have been beneficial for 64-bit processors, the amount of calculation described below becomes excessive for k much greater than 32.

The following simplified version of an algorithm from Peterson and Weldon [11] was used to test a polynomial f of degree k over F_2 for primitivity. The residues of $x, x^2, x^4, \ldots, x^{2^{k-1}}$ are computed modulo $f(x)$. The product of these residues is calculated to obtain the residue of x^{2^k-1} modulo $f(x)$. If $x^{2^k-1} \not\equiv 1 \pmod{f(x)}$, then $f(x)$ is not primitive. If $x^{2^k-1} \equiv 1 \pmod{f(x)}$, we proceed as follows. The factorization of $2^k - 1$ is obtained from Brillhart, Lehmer, Selfridge, Tuckerman, and Wagstaff [1] and then for each prime factor r of $2^k - 1$, the residue of $x^{(2^k-1)/r}$ modulo $f(x)$ is calculated. If for at least one such r we have $x^{(2^k-1)/r} \equiv 1 \pmod{f(x)}$, then $f(x)$ is not primitive. If

TABLE 2
Primitive polynomials f with large $\rho^{(4)}(f)$ values

k	$\rho^{(3)}(f)$	$\rho^{(4)}(f)$	f
3	3	3	0 1 3
4	4	3	0 3 4
5	5	5	0 1 2 3 5
*6	4	4	0 1 2 5 6
7	6	6	0 1 3 6 7
8	7	5	0 1 2 5 6 7 8
9	8	6	0 5 6 8 9
10	8	8	0 2 3 7 8 9 10
11	10	9	0 6 8 9 11
*12	10	9	0 1 3 8 9 11 12
13	11	11	0 1 2 5 6 7 8 10 11 12 13
14	11	11	0 2 3 4 6 10 11 12 14
15	12	12	0 1 4 5 6 10 11 13 15
16	14	12	0 1 2 3 4 6 7 9 11 14 16
17	15	14	0 5 8 12 13 16 17
*18	15	14	0 1 2 4 5 7 12 15 16 17 18
19	16	16	0 1 2 4 6 7 10 13 14 15 16 18 19
*20	17	16	0 1 2 4 5 6 7 9 10 14 16 19 20
*21	19	17	0 1 3 4 5 6 8 10 14 16 17 20 21
22	19	18	0 1 3 12 13 15 16 17 18 20 22
23	19	19	0 1 2 5 6 7 9 10 11 12 13 16 17 19 20 21 23
*24	21	20	0 1 3 5 6 7 8 10 12 15 18 20 22 23 24
25	22	20	0 1 2 3 4 5 6 9 12 13 14 15 17 19 20 21 22 24 25
26	21	21	0 1 2 3 4 5 6 7 12 16 17 22 23 25 26
27	23	22	0 1 2 3 4 5 6 7 10 12 14 15 17 19 20 21 25 26 27
28	23	23	0 1 2 3 4 5 6 7 8 9 11 14 15 16 18 19 20 22 23 26 28
29	24	24	0 1 3 5 6 7 10 13 14 17 19 21 26 28 29
*30	25	25	0 1 2 3 4 5 6 7 8 11 13 17 18 23 24 26 28 29 30
31	26	26	0 1 2 3 4 5 6 7 8 9 11 12 13 14 17 18 21 22 24 27 28 30 31
32	27	27	0 1 2 3 4 5 6 7 8 12 14 16 19 20 21 22 24 27 28 30 32

$x^{(2^k-1)/r} \not\equiv 1 \pmod{f(x)}$ for all such r, then $f(x)$ is a primitive polynomial of degree k over F_2.

Having obtained exhaustive collections of primitive polynomials f with $L(f) \leq 2$ for each $k \leq 21$, and extensive collections of such polynomials for $22 \leq k \leq 32$, we then attempted to locate among those primitive polynomials of a given degree k, polynomials f with the property that for a fixed $3 \leq s \leq 5$, the figure of merit $\rho^{(s)}(f)$ is large. Note that by (6), $\rho^{(s)}(f)$ can be large for some $s \geq 3$ only if $\rho^{(2)}(f)$ is large, i.e., if $L(f)$ is small (see (7)).

To calculate the figure of merit $\rho^{(s)}(f)$ for a given primitive polynomial f of degree k, we proceeded as follows. Let α be a root of $f(x)$. For a fixed $3 \leq s \leq 5$ begin with $d = k$, and find all choices of $(d_1, \ldots, d_s) \neq (0, \ldots, 0)$ so that $\sum_{i=1}^{s} d_i = d$, where the d_i are integers with $0 \leq d_i \leq k$ for $1 \leq i \leq s$. If for all such choices of $(d_1, \ldots, d_s)$ the systems

$$\{\alpha^{(i-1)k+j-1} | 1 \leq j \leq d_i, \ 1 \leq i \leq s\}$$

TABLE 3
Primitive polynomials f with large $\rho^{(5)}(f)$ values

k	$\rho^{(3)}(f)$	$\rho^{(4)}(f)$	$\rho^{(5)}(f)$	f
3	3	3	3	0 1 3
4	4	3	3	0 3 4
5	5	5	4	0 1 2 3 5
*6	4	4	4	0 1 2 5 6
7	6	6	5	0 1 3 6 7
8	7	5	5	0 1 2 5 6 7 8
9	8	6	6	0 5 6 8 9
10	7	7	7	0 5 7 8 10
11	8	8	8	0 1 5 7 9 10 11
*12	10	9	8	0 1 3 8 9 11 12
13	11	11	9	0 1 2 5 6 7 8 10 11 12 13
14	12	10	10	0 1 2 3 9 12 14
15	12	12	11	0 1 4 5 6 10 11 13 15
16	13	12	12	0 3 4 7 10 12 14 15 16
17	14	13	12	0 6 9 13 14 15 17
*18	14	14	13	0 1 3 6 7 12 15 17 18
19	15	15	14	0 1 4 6 8 9 12 15 16 18 19
*20	17	15	15	0 5 7 13 14 16 18 19 20
*21	17	17	16	0 1 3 4 5 6 9 12 14 16 17 19 21
22	17	17	17	0 1 4 5 6 10 11 14 18 20 22
23	19	19	17	0 1 2 5 6 7 9 10 11 12 13 16 17 19 20 21 23
*24	21	19	18	0 1 2 3 4 5 6 9 10 11 12 14 15 16 17 20 21 22 24
25	21	19	19	0 1 2 3 4 5 7 12 18 21 23 24 25
26	21	21	20	0 1 2 3 4 5 6 7 12 16 17 22 23 25 26
27	21	21	20	0 1 2 3 4 5 6 7 8 13 16 17 19 20 22 25 27
28	24	21	21	0 1 2 3 4 5 6 7 8 9 12 17 18 21 22 23 24 26 28
29	25	23	22	0 1 3 4 10 11 13 17 18 19 21 22 24 25 26 28 29
*30	26	23	23	0 1 3 5 6 7 9 10 11 12 13 17 19 20 22 24 27 29 30
31	25	25	24	0 16 20 26 27 29 31
32	26	26	25	0 1 2 3 4 5 6 7 8 9 11 12 21 22 24 26 27 28 30 31 32

are linearly independent over F_2, then $\rho^{(s)}(f) = d + 1$. Otherwise, if at least one of the systems is linearly dependent over F_2, then d is decremented by one and the procedure is repeated.

Unfortunately, for $s > 2$ no formula for $\rho^{(s)}(f)$ analogous to (7) for $\rho^{(2)}(f)$ is known. For $k \leq 21$, an exhaustive search was made over all primitive polynomials f of degree k with $L(f) \leq 2$. For each of these polynomials f, $\rho^{(s)}(f)$ was calculated for each $3 \leq s \leq 5$. It was found that, for each $3 \leq s \leq 5$ and each $k \leq 21$, there exists at least one primitive polynomial f of degree k with $L(f) \leq 2$ and $\rho^{(s)}(f) \geq k - s$. There are however cases where there is no polynomial f of degree k with $\rho^{(s)}(f) \geq k - s + 1$. For example, if $k = 20$ and $s = 4$, there does not exist a primitive polynomial f of degree 20 with $L(f) \leq 2$ and $\rho^{(4)}(f) \geq 17$. Hence, we see that in general, if f has degree k, the best possible value for $\rho^{(s)}(f)$ is $k - s$. Thus, we have some justification for the following concept.

For a fixed $3 \leq s \leq 5$, a polynomial f of degree k is said to be *s-optimal* if it

TABLE 4
Universally optimal primitive polynomials

k	$\rho^{(3)}(f)$	$\rho^{(4)}(f)$	$\rho^{(5)}(f)$	f
3	3	3	3	0 1 3
4	4	3	3	0 3 4
5	5	5	4	0 1 2 3 5
*6	4	4	4	0 1 2 5 6
7	6	6	5	0 1 3 6 7
8	7	5	5	0 1 2 5 6 7 8
9	8	6	6	0 5 6 8 9
10	8	8	6	0 2 3 7 8 9 10
11	10	9	7	0 6 8 9 11
*12	10	9	8	0 1 3 8 9 11 12
13	11	11	9	0 1 2 5 6 7 8 10 11 12 13
14	12	10	10	0 1 2 3 9 12 14
15	12	12	11	0 1 4 5 6 10 11 13 15
16	13	12	12	0 3 4 7 10 12 14 15 16
17	14	13	12	0 6 9 13 14 15 17
*18	14	14	13	0 1 3 6 7 12 15 17 18
19	15	15	14	0 1 4 6 8 9 12 15 16 18 19
*20	17	15	15	0 5 7 13 14 16 18 19 20
*21	17	17	16	0 1 3 4 5 6 9 12 14 16 17 19 21
22	18	18	16	0 1 2 5 6 8 9 11 13 14 16 17 18 20 22
23	19	19	17	0 1 2 5 6 7 9 10 11 12 13 16 17 19 20 21 23
*24	21	19	18	0 1 2 3 4 5 6 9 10 11 12 14 15 16 17 20 21 22 24
25	21	19	19	0 1 2 3 4 5 7 12 18 21 23 24 25
26	21	21	20	0 1 2 3 4 5 6 7 12 16 17 22 23 25 26
27	23	21	19	0 1 2 3 4 5 6 7 8 12 17 23 24 26 27
28	24	22	20	0 1 2 3 4 5 6 7 8 9 11 12 13 15 18 19 24 27 28
29	25	23	22	0 1 3 4 10 11 13 17 18 19 21 22 24 25 26 28 29
*30	26	23	23	0 1 3 5 6 7 9 10 11 12 13 17 19 20 22 24 27 29 30
31	25	25	24	0 16 20 26 27 29 31
32	26	26	25	0 1 2 3 4 5 6 7 8 9 11 12 21 22 24 26 27 28 30 31 32

is primitive and satisfies $L(f) \leq 2$ and $\rho^{(s)}(f) \geq k - s$. Because of the amount of computation required to determine whether a polynomial of degree k is s-optimal for $k > 21$, only a small fraction of the total number of primitive polynomials f with $L(f) \leq 2$ was tested.

In Tables 1–4, if $f(x) = \sum_{i=0}^{k} b_i x^i$, we have listed only the exponents of the terms for which $b_i \neq 0$, and hence $b_i = 1$. Thus, for example, the polynomial $1 + x + x^3$ is listed as 0 1 3. We have indicated with an asterisk those degrees k for which $\gcd(k, 2^k - 1) > 1$.

Tables 1, 2, and 3 list the primitive polynomials f of degree k, $3 \leq k \leq 32$, with $L(f) \leq 2$ that have the largest $\rho^{(s)}(f)$ value for $s = 3, 4$, and 5, respectively, out of all the polynomials tested. From Table 1 it can be seen that there exists a 3-optimal polynomial of degree k for all $k \leq 32$. Table 2 gives 4-optimal polynomials up to degree 24, while Table 3 gives 5-optimal polynomials up to degree 22. In Tables 2 and 3 we have also listed for the given polynomial f the values of $\rho^{(r)}(f)$ for $3 \leq r < s$. Of course, from (6)

it is clear that $\rho^{(r)}(f) \geq \rho^{(s)}(f)$. Moreover, in each of the three tables, for any polynomial f of degree k we have $\rho^{(2)}(f) = k$.

4. Universally optimal characteristic polynomials

From a practitioner's point of view, it would be convenient to have, for each degree, a single polynomial f that is s-optimal for all $2 \leq s \leq 5$. Since such polynomials in general do not exist, one would like to consider the question of whether there exists, for each degree k, a primitive polynomial f of degree k with $L(f) \leq 2$ having large $\rho^{(s)}(f)$ values for all $2 \leq s \leq 5$. Such polynomials will be considered to be *universally optimal*.

Table 4 contains a list of universally optimal polynomials. Notice that for

$$\begin{aligned} k &\leq 13, \quad \rho^{(s)}(f) \geq k - s + 1, \\ k &\leq 17, \quad \rho^{(s)}(f) \geq k - s, \\ k &\leq 24, \quad \rho^{(s)}(f) \geq k - s - 1, \\ k &\leq 26, \quad \rho^{(s)}(f) \geq k - s - 2, \\ k &\leq 32, \quad \rho^{(s)}(f) \geq k - s - 3 \end{aligned}$$

for all $2 \leq s \leq 5$.

It should be pointed out that for $k \leq 21$ these results are best possible, so that for example, if $k = 14$, there does not exist a universally optimal characteristic polynomial f of degree 14 with $\rho^{(s)}(f) \geq 14 - s + 1$ for all $2 \leq s \leq 5$.

5. Conclusions

Our computational results show that for every $2 \leq s \leq 5$ and every $k \leq 32$ there exist digital k-step pseudorandom numbers such that any s successive pseudorandom numbers are statistically almost independent. In fact, for every $k \leq 32$ we have determined a primitive characteristic polynomial of degree k such that the generated pseudorandom numbers pass the s-dimensional serial test for all $2 \leq s \leq 5$ (see §4). It is to be expected that similar characteristic polynomials can also be found for larger values of k. For the case $s = 2$, suitable characteristic polynomials are available for all $k \leq 64$ by the calculations in [4]. For general s and k we have the following special case of a theorem of Niederreiter [10]: for any $s \geq 2$ and $k \geq 2$ there exists a primitive polynomial f over F_2 of degree k such that

$$\rho^{(s)}(f) \geq \log_2(C_s \phi(2^k - 1) k^{-s}),$$

where $\log_2$ is the logarithm to the base 2, the constant $C_s > 0$ depends only on s, and ϕ is Euler's totient function. It follows that for such an f the figure of merit $\rho^{(s)}(f)$ has a lower bound that is essentially of the form $k - s \log_2 k$. However, the proof of the result above is nonconstructive.

For the pseudorandom numbers obtained from our tables, the points X_n in (4) show a very even distribution over $[0, 1]^s$. For instance, if we consider the pseudorandom numbers generated by the characteristic polynomial listed in Table 1 for $k = 32$, then the points $\mathbf{0}, X_0, X_1, \ldots, X_{\tau-1}$ in $[0, 1)^3$ form a $(4, 32, 3)$-net according to Theorem A. This means that every subinterval of $[0, 1)^3$ of the form (5) with volume 2^{-28} contains exactly 16 points of this point set. Such strong uniformity properties are not known for comparable linear congruential pseudorandom numbers with modulus $M = 2^{32}$. Digital multistep pseudorandom numbers have another advantage over linear congruential pseudorandom numbers, namely, that they are generated by binary arithmetic as opposed to modular arithmetic with a very large modulus. Therefore, digital multistep pseudorandom numbers offer a viable alternative to linear congruential pseudorandom numbers when ease of generation and strong uniformity properties are desired.

Acknowledgment

The authors would like to thank the PSU Computation Center for use of its facilities. Special thanks are due Gerald McKenna for use of his finite field software package.

Bibliography

1. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, 2nd ed., Contemporary Math., Vol. 22, Amer. Math. Soc., Providence, R.I., 1988.
2. D. E. Knuth, *The art of computer programming*, Vol. 2: *Seminumerical algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.
3. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, Cambridge, 1986.
4. G. L. Mullen and H. Niederreiter, *Optimal characteristic polynomials for digital multistep pseudorandom numbers*, Computing **39** (1987), 155–163.
5. H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.
6. ——, *The performance of k-step pseudorandom number generators under the uniformity test*, SIAM J. Sci. Statist. Comput. **5** (1984), 798–810.
7. ——, *Pseudozufallszahlen und die Theorie der Gleichverteilung*, Sitzungsber. Österr. Akad. Wiss. Math.-Natur. Kl. Abt. II **195** (1986), 109–138.
8. ——, *Rational functions with partial quotients of small degree in their continued fraction expansion*, Monatsh. Math. **103** (1987), 269–288.
9. ——, *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273–337.
10. ——, *The serial test for digital k-step pseudorandom numbers*, Math. J. Okayama Univ. **30** (1988), 93–119.
11. W. W. Peterson and E. J. Weldon, Jr., *Error-correcting codes*, 2nd ed., M.I.T. Press, Cambridge, Mass., 1972.
12. R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two*, Math. Comp. **19** (1965), 201–209.

13. A. van Wijngaarden, *Mathematics and computing*, in Proc. Sympos. on Automatic Digital Computation (London, 1954), H. M. Stationery Office, London, 1954, pp. 125–129.

DEPARTMENT OF COMPUTER SCIENCE, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802

INSTITUTE FOR INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, DR.-IGNAZ-SEIPEL-PLATZ 2, A-1010 VIENNA, AUSTRIA