Math. J. Okayama Univ. 30 (1988), 93－119

THE SERIAL TEST FOR DIGITAL k-STEP PSEUDORANDOM NUMBERS

HARALD NIEDERREITER*)

1. Introduction

A widely used method for the generation of uniform pseudorandom numbers is the multiplicative congruential method of Lehmer [8], which is based on the one-step recursion

$$y_{n+1} \equiv a y_n \bmod M \text{ for } n = 0, 1, \ldots,$$

where the modulus M is a large integer, a is a suitably chosen integral multiplier, and the y_n are integers with $0 < y_n < M$. A sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers in the interval $[0, 1]$ is obtained by the normalization $x_n = y_n/M$. The statistical properties of these pseudorandom numbers have been studied extensively both from the theoretical and the empirical point of view (see Knuth [6, Ch. 3] and Niederreiter [13] for surveys). The use of general k-step recursions for pseudorandom number generation was proposed shortly after the appearance of Lehmer's paper (see e.g. van Wijngaarden [24]), and this idea received wider dissemination through an article of Tausworthe [23]. There is now a sizable literature on k-step pseudorandom number generators; see e.g. Arvillias and Maritsas [1], Fushimi [2], Fushimi and Tezuka [3], Kirkpatrick and Stoll [5], Peskun [22], and the references in Niederreiter [16].

The generation of uniform pseudorandom numbers by k-step recursions proceeds as follows. Let p be a prime number and generate a sequence $y_0, y_1, \ldots$ of integers with $0 \leq y_n < p$ by the recursion

$$(1) \qquad y_{n+k} \equiv a_{k-1} y_{n+k-1} + \cdots + a_0 y_n \bmod p \text{ for } n = 0, 1, \ldots,$$

where the a_i are constant integral coefficients with $a_0 \not\equiv 0 \bmod p$. We assume that not all initial values $y_0, y_1, \ldots, y_{k-1}$ are 0, for otherwise we would get the distinctly nonrandom situation where all $y_n = 0$. The sequence $y_0, y_1, \ldots$ is then transformed into a sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers in $[0, 1]$ by one of the following two methods. In the *normalization method* we choose p to be a large prime and set $x_n = y_n/p$ for $n = 0, 1, \ldots$.

*) The author gratefully acknowledges support for this research project by the Austrian Ministry for Science and Research.

In the *digital method* we let p be a small prime (usually $p = 2$), choose an integer m with $2 \leq m \leq k$, and set

$$x_n = \sum_{j=1}^{m} y_{mn+j-1} p^{-j} \text{ for } n = 0, 1, \ldots. \tag{2}$$

In other words, we obtain the numbers x_n by splitting up the sequence $y_0, y_1, \ldots$ into consecutive blocks of length m and then interpreting each block as the digit expansion in the base p of a number in $[0, 1]$. The numbers x_n will be called *digital k-step pseudorandom numbers*. The digital method has the advantage that we can work with a small modulus in the recursion (1), in contrast to the normalization method and also to Lehmer's method where one has to use large moduli.

For many numerical applications of uniform pseudorandom numbers, the most important properties are equidistribution in $[0, 1]$ and statistical independence of successive pseudorandom numbers. Equidistribution is tested by the uniformity test. The performance under the uniformity test was investigated in Niederreiter [11] for pseudorandom numbers generated by the normalization method and in Niederreiter [16] for digital k-step pseudorandom numbers. Statistical independence properties of pseudorandom numbers generated by the normalization method were studied in Niederreiter [14]. In the present paper we discuss statistical independence properties of digital k-step pseudorandom numbers. We note that some of the results of this paper were announced in [15].

A reliable test for the statistical independence of s successive pseudorandom numbers is the *s-dimensional serial test* (see Knuth [6, Ch. 3]). If $x_0, x_1, \ldots$ is a sequence of uniform pseudorandom numbers in $[0, 1]$ and $s \geq 2$ is given, then we introduce the s-tuples

$$\boldsymbol{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0, 1]^s \text{ for } n = 0, 1, \ldots. \tag{3}$$

The s-dimensional serial test amounts to considering the maximum deviation between the empirical distribution of the s-tuples $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}$ and the uniform distribution on $[0, 1]^s$, the latter distribution corresponding to the ideal case of statistical independence among s successors. In detail, we define the quantity

$$D_N^{(s)} = \sup_J |E_N(J) - V(J)| \text{ for } N \geq 1, \tag{4}$$

where $E_N(J)$ is N^{-1} times the number of terms among $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}$ falling

into the interval J, $V(J)$ denotes the volume of J, and the supremum is extended over all subintervals J of $[0,1]^s$ of the form

$$J = [0, t_1] \times \cdots \times [0, t_s].$$

The sequence $x_0, x_1, \ldots$ of pseudorandom numbers passes the s-dimensional serial test if $D_N^{(s)}$ is small for large N. In statistics the quantity in (4) corresponds to a multivariate Kolmogorov test, and in the theory of uniform distribution of sequences this quantity is called the *discrepancy*. Compare with Kuipers and Niederreiter [7, Ch. 2] and Niederreiter [13] for basic facts about the discrepancy. It should be noted that the discrepancy occurs in error bounds for quasi-Monte Carlo integration over the s-dimensional unit cube $[0,1]^s$ (see [13, 19]), so that the results of this paper have immediate applications to numerical integration. Furthermore, other statistical quantities can be bounded in terms of an appropriate $D_N^{(s)}$. For instance, for the serial correlation coefficient

$$\sigma_N = \frac{M[(x_n - M(x_n))(x_{n+1} - M(x_{n+1}))]}{M[(x_n - M(x_n))^2]^{1/2} M[(x_{n+1} - M(x_{n-1}))^2]^{1/2}},$$

with $M(u_n)$ denoting the mean value of the numbers $u_0, u_1, \ldots, u_{N-1}$, we have

$$|\sigma_N| < 73 D_N^{(2)}$$

by a result in [17].

In [16] we also considered digital k-step pseudorandom numbers obtained from overlapping blocks of y_n, so that instead of (2) we have

$$x_n = \sum_{j=1}^{m} y_{n+j-1} p^{-j} \quad \text{for } n = 0, 1, \ldots.$$

With respect to the uniformity test, these numbers show the same behavior as those defined by (2) (see [16]). However, the serial test is failed badly by these numbers. In fact, if we consider the corresponding s-tuples $\boldsymbol{x}_n$ defined as in (3), then it is seen immediately that none of these s-tuples falls into the interval

$$\left[0, \frac{1}{p^2}\right) \times \left[\frac{1}{p}, 1\right] \times [0,1]^{s-2}.$$

It follows easily (compare with the proof of Theorem 6.2) that $D_N^{(s)} \geq \frac{1}{2}(p-1)p^{-3}$ for all $s \geq 2$ and $N \geq 1$, and so the discrepancy is unacceptably large.

For this reason, we restrict the attention to the digital k-step pseudorandom numbers defined by (2).

We recall some elementary properties of the sequences $y_0, y_1, \ldots$ and $x_0, x_1, \ldots$ defined by (1) and (2), respectively (see Lidl and Niederreiter [10, Ch. 7] and Niederreiter [16]). First of all, both sequences are periodic, and if τ denotes the least period of the sequence of y_n, then the least period of the sequence of x_n is given by $\tau/\gcd(m, \tau)$. In order to achieve a large value of τ, we assume that the *characteristic polynomial of* (1), i.e. the polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0, \tag{5}$$

considered as a polynomial over the finite field $F_p = \mathbf{Z}/p\mathbf{Z}$, is irreducible over F_p. Then τ can be described as the order of any root of $f(x)$ in the group F_q^*, the multiplicative group of nonzero elements of the finite field F_q with $q = p^k$ elements. Therefore, the maximal value of τ is $\tau = p^k - 1$, and this can be achieved if we choose for $f(x)$ a *primitive polynomial* over F_p (compare with [9, Ch. 3]). We will always assume that $\gcd(m, \tau) = 1$, thus guaranteeing that the least period of the sequence of x_n is equal to τ. Because of the periodic nature of the x_n, it is only of interest to study $D_N^{(s)}$ for $1 \leq N \leq \tau$.

An important fact regarding the performance of digital k-step pseudorandom numbers under the s-dimensional serial test is the following. If the dimension s is small, concretely if $s \leq k/m$ with m denoting the block length, then the bounds for $D_N^{(s)}$ depend only on the least period τ and not on the specific nature of the polynomial $f(x)$ in (5). On the other hand, for $s > k/m$ the bounds for $D_N^{(s)}$ depend strongly on the concrete form of $f(x)$, so that this polynomial has to be chosen judiciously in order to guarantee good performance under the s-dimensional serial test. We shall distinguish these two cases as the *low-dimensional case* (i.e. $s \leq k/m$) and the *high-dimensional case* (i.e. $s > k/m$). The fact that good behavior can be expected in the low-dimensional case was already noted by Tausworthe [23] who showed a kind of equidistribution property of the points $\boldsymbol{x}_n$ in (3) provided that $f(x)$ is a primitive polynomial over F_p (see also [10, Ch. 7]).

The paper is organized as follows. In Section 2 we collect some preparatory results. Then we establish upper bounds for $D_N^{(s)}$, in Section 3 for the low-dimensional case and in Section 4 for the high-dimensional case. In both cases we consider the behavior for the full period, i.e. for $N = \tau$, as well as for parts of the period, i.e. for $N < \tau$. Although most of the

research so far has been devoted to the performance over the full period, the performance for parts of the period is of great practical importance since in a typical Monte Carlo application one will only work with a segment of the period. The bounds in Section 4 depend in a rather complicated way on the characteristic polynomial $f(x)$, and so we elucidate this dependence by introducing a convenient integer (called the "figure of merit") that measures the suitability of $f(x)$. This is done in Section 5, where one can also find basic results on figures of merit. Section 6 contains lower bounds for $D_N^{(s)}$. In particular, for the high-dimensional case we show that $D_N^{(s)}$ can be bounded from below in terms of the figure of merit. This demonstrates that the upper bounds in Section 4 are in a sense best possible. In Section 7 we discuss the results from the viewpoint of practical pseudorandom number generation.

On the surface, there is a certain similarity between the results of this paper and the author's earlier results on the serial test for Lehmer's congruential pseudorandom numbers: compare with [12, 13, 18]. There is, however, a fundamental difference inasmuch as for Lehmer's method the way the bounds depend on the modulus M is essential, whereas for the digital method this is rather insignificant since one usually works with the fixed prime modulus $p = 2$. For digital k-step pseudorandom numbers, a more important entity besides k and the characteristic polynomial $f(x)$ turns out to be the block length m.

For the convenience of the reader we state again all the *standing hypotheses* of this paper: (i) the polynomial $f(x)$ in (5) is irreducible over F_p; (ii) the initial values $y_0, y_1, \ldots, y_{k-1}$ are not all 0; (iii) $2 \le m \le k$ and $\gcd(m, \tau) = 1$.

2. Preparatory results

We first recall an inequality for the discrepancy in terms of exponential sums. This inequality refers to the situation where the given points $\boldsymbol{w}_0, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{N-1}$ in $[0,1]^s$ are such that all their coordinates have digit expansions of fixed finite length m. Let $b \ge 2$ be an integer that serves as the base for the digit expansions and let $\boldsymbol{w}_n = (w_{n1}, \ldots, w_{ns})$ with

$$w_{ni} = \sum_{j=1}^{m} w_{ni}^{(j)} b^{-j} \text{ for } 0 \le n < N,\ 1 \le i \le s,$$

where the digits $w_{ni}^{(j)}$ are integers in the interval $[0, b-1]$. Let $C(b)$ be the set of all integers h with $-b/2 < h \le b/2$. For $H = (h_1, \ldots, h_m)$ with

$h_j \in C(b)$ for $1 \leq j \leq m$ we define

$$(6)\quad d(H) = d(h_1,\ldots,h_m) = \begin{cases} 0 & \text{if } H = (0,\ldots,0), \\ \text{largest index } d \text{ with } h_d \neq 0 & \text{if } H \neq (0,\ldots,0). \end{cases}$$

For $b = 2$ we set

$$(7)\qquad Q_2(H) = Q_2(h_1,\ldots,h_m) = 2^{-d(H)}$$

and for $b > 2$ we set

$$(8)\quad Q_b(H) = Q_b(h_1,\ldots,h_m) = \begin{cases} 1 & \text{if } H = (0,\ldots,0), \\ b^{-d}\left(\dfrac{1}{\sin \pi |h_d/b|} + \delta_d\right) & \text{if } H \neq (0,\ldots,0), \end{cases}$$

where $d = d(H)$ and where $\delta_d = 1$ if $d < m$, but $\delta_m = 0$. Now let $C_{ms}(b)$ be the set of ms-dimensional lattice points of the form

$$\boldsymbol{h} = (h_{ij}) = (h_{11},\ldots,h_{1m},\ldots,h_{s1},\ldots,h_{sm})$$

with $h_{ij} \in C(b)$ for $1 \leq i \leq s$, $1 \leq j \leq m$. For each such $\boldsymbol{h}$ we define the weight

$$(9)\qquad P_b(\boldsymbol{h}) = \prod_{i=1}^{s} Q_b(h_{i1},\ldots,h_{im}).$$

We note that in the case $b = 2$ this reduces to the expression

$$(10)\qquad P_2(\boldsymbol{h}) = 2^{-D(\boldsymbol{h})} \text{ with } D(\boldsymbol{h}) = \sum_{i=1}^{s} d(h_{i1},\ldots,h_{im}).$$

For integers h we use the complex exponential function $e_b(h) = e^{2\pi\sqrt{-1}\,h/b}$. The following result is a special case of [20, Satz 2] and can also be considered as a refinement of [15, Lemma 1] and a multidimensional version of [16, Lemma 1].

Lemma 2.1. *For the discrepancy $D_N^{(s)}$ of the points $\boldsymbol{w}_n$, $0 \leq n < N$, we have*

$$D_N^{(s)} \leq 1 - (1 - b^{-m})^s + \sum_{\boldsymbol{h} \neq 0} P_b(\boldsymbol{h}) \left| \frac{1}{N} \sum_{n=0}^{N-1} e_b\left(\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} w_{ni}^{(j)} \right) \right|$$

where the outer sum is extended over all nonzero lattice points $\boldsymbol{h} = (h_{ij}) \in C_{ms}(b)$.

Lemma 2.2. *For the weights $P_b(\boldsymbol{h})$ defined by (9) we have*

$$\sum_{\boldsymbol{h}\neq 0} P_b(\boldsymbol{h}) < \left(\frac{2}{\pi} m \log b + \frac{7}{5} m - \frac{m-1}{b}\right)^s - 1 \tag{11}$$

for $b > 2$, where the sum is extended over all nonzero lattice points $\boldsymbol{h} \in C_{ms}(b)$. In the case $b = 2$ we have

$$\sum_{\boldsymbol{h}\neq 0} P_2(\boldsymbol{h}) = \left(\frac{m}{2}+1\right)^s - 1. \tag{12}$$

Proof. For any $b \geq 2$ we have

$$\begin{aligned} \sum_{\boldsymbol{h}\neq 0} P_b(\boldsymbol{h}) &= \sum_{\substack{h_{ij}\in C(b) \\ 1\leq i\leq s, 1\leq j\leq m}} Q_b(h_{11},\ldots,h_{1m})\ldots Q_b(h_{s1},\ldots,h_{sm}) - 1 \\ &= \left(\sum_{h_1,\ldots,h_m \in C(b)} Q_b(h_1,\ldots,h_m)\right)^s - 1. \end{aligned} \tag{13}$$

To evaluate the last sum, we split it up according to the value of $d = d(h_1,\ldots,h_m)$ for nonzero lattice points $(h_1,\ldots,h_m)$. There are b^{d-1} such lattice points with a fixed nonzero value of h_d. Writing $C^*(b)$ for the set of nonzero elements of $C(b)$, we get for $b > 2$ by using (8),

$$\begin{aligned} \sum_{h_1,\ldots,h_m\in C(b)} Q_b(h_1,\ldots,h_m) &= 1 + \sum_{d=1}^{m} b^{d-1} b^{-d} \sum_{h\in C^*(b)} \left(\frac{1}{\sin \pi |h/b|} + \delta_d\right) \\ &= 1 + \frac{m}{b} \sum_{h\in C^*(b)} \frac{1}{\sin \pi |h/b|} + \frac{b-1}{b} \sum_{d=1}^{m} \delta_d \\ &= \frac{m}{b} \sum_{h\in C^*(b)} \frac{1}{\sin \pi |h/b|} + m - \frac{m-1}{b}. \end{aligned}$$

By [11, p. 574] we have

$$\sum_{h\in C^*(b)} \frac{1}{\sin \pi |h/b|} < \frac{2}{\pi} b \log b + \frac{2}{5} b,$$

and combining these results with (13) we obtain (11). In the case $b = 2$ we use (7) to get

$$\sum_{h_1,\ldots,h_m\in C(2)} Q_2(h_1,\ldots,h_m) = 1 + \sum_{d=1}^{m} 2^{d-1} 2^{-d} = \frac{m}{2} + 1,$$

and so (12) follows from (13).

We now collect some auxiliary results from the theory of finite fields. We refer to the books of Lidl and Niederreiter [9], [10] for the necessary

background on finite fields. The integers $y_0, y_1, \ldots$ as well as the coefficients a_i in (1) may be interpreted as elements of the finite field F_p. The recursion (1) becomes then the linear recurrence relation

$$y_{n+k} = a_{k-1}y_{n+k-1} + \cdots + a_0 y_n \text{ for } n = 0, 1, \ldots \tag{14}$$

over F_p. Set $q = p^k$ and let F_q be the finite field with q elements. Let Tr denote the trace function from F_q onto F_p, which is an F_p-linear mapping. Let $\alpha \in F_q$ be a fixed root of the characteristic polynomial $f(x)$ in (5). The following result is identical with Lemma 2 in [16].

Lemma 2.3. *Let the sequence $y_0, y_1, \ldots$ of elements of F_p satisfy (14), and suppose that not all initial values $y_0, y_1, \ldots, y_{k-1}$ are 0. Then there exists $\beta \in F_q^*$ such that*

$$y_n = \mathrm{Tr}(\beta\alpha^n) \text{ for } n = 0, 1, \ldots.$$

Next we consider character sums over the finite field F_q. We note that

$$\chi(\beta) = e_p(\mathrm{Tr}(\beta)) \text{ for all } \beta \in F_q \tag{15}$$

defines a character of the additive group of F_q. The following bounds are obtained from Lemma 4 and Lemma 5 in [16], respectively.

Lemma 2.4. *If λ is an element of F_q^* of order d, then for any $\theta \in F_q^*$ we have*

$$\left| \sum_{n=0}^{d-1} \chi(\theta\lambda^n) \right| \leq q^{1/2} - \frac{d}{1+q^{1/2}}.$$

Lemma 2.5. *If λ is an element of F_q^* of order d, then for any $\theta \in F_q^*$ we have*

$$\left| \sum_{n=0}^{N-1} \chi(\theta\lambda^n) \right| < q^{1/2}\left(\frac{2}{\pi}\log d + \frac{2}{5}\right) + \frac{Nq^{1/2}}{d} - \frac{N}{1+q^{1/2}} \text{ for all } N \geq 1.$$

3. The low-dimensional case

We consider the s-dimensional serial test for digital k-step pseudorandom numbers in the case $s \leq k/m$. We establish upper bounds for the discrepancy $D_N^{(s)}$ of the points $\boldsymbol{x}_n$ in (3), and we distinguish the case $N = \tau$ of the full period and the case $N < \tau$.

Theorem 3.1. *If $s \le k/m$, then for digital k-step pseudorandom numbers we have for $p > 2$*

$$D_\tau^{(s)} < 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{\tau}-\frac{1}{1+p^{k/2}}\right)\left(\left(\frac{2}{\pi}m\log p+\frac{7}{5}m-\frac{m-1}{p}\right)^s-1\right).$$

In the case $p = 2$ we have

$$D_\tau^{(s)} \le 1-(1-2^{-m})^s+\left(\frac{2^{k/2}}{\tau}-\frac{1}{1+2^{k/2}}\right)\left(\left(\frac{m}{2}+1\right)^s-1\right).$$

Proof. In the notation of Section 2 we have $\boldsymbol{w}_n = \boldsymbol{x}_n$, hence

$$w_{ni} = x_{n+i-1} \text{ for } 1 \le i \le s \text{ and } n \ge 0.$$

From (2) we get the digits of w_{ni} to the base $b = p$, namely

$$w_{ni}^{(j)} = y_{m(n+i-1)+j-1} \text{ for } 1 \le i \le s,\ 1 \le j \le m, \text{ and } n \ge 0.$$

We consider the exponential sums appearing in Lemma 2.1. Take a nonzero lattice point $\boldsymbol{h} = (h_{ij}) \in C_{ms}(p)$. Since the h_{ij} and $w_{ni}^{(j)}$ only matter mod p, we can view them as elements of F_p. Put

$$z_n = \sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij}w_{ni}^{(j)} = \sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij}y_{m(n+i-1)+j-1} \text{ for } n \ge 0.$$

Then by Lemma 2.3 we get with a suitable $\beta \in F_q^*$,

$$\begin{aligned} z_n &= \sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij}\,\mathrm{Tr}\left(\beta\alpha^{m(n+i-1)+j-1}\right) \\ &= \mathrm{Tr}\left(\beta\sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij}\alpha^{m(n+i-1)+j-1}\right) \\ &= \mathrm{Tr}\left(\beta\lambda^n\sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij}\alpha^{m(i-1)+j-1}\right) \end{aligned}$$

for all $n \ge 0$, where $\lambda = \alpha^m$. The double sum in the last expression is a linear combination of the powers $\alpha^0, \alpha^1, \ldots, \alpha^{ms-1}$ with coefficients in F_p that are not all 0. Now $f(x)$ is irreducible over F_p, so the powers $\alpha^0, \alpha^1, \ldots, \alpha^{k-1}$ are linearly independent over F_p, and since $ms \le k$ by hypothesis, it follows that

$$\sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij}\alpha^{m(i-1)+j-1} \ne 0.$$

Consequently, for some $\theta \in F_q^*$ we have

$$z_n = \mathrm{Tr}(\theta\lambda^n) \text{ for all } n \geq 0.$$

From (15) we obtain then

$$\sum_{n=0}^{\tau-1} e_p\left(\sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij} w_{ni}^{(j)}\right) = \sum_{n=0}^{\tau-1} e_p(z_n) = \sum_{n=0}^{\tau-1} \chi(\theta\lambda^n).$$

Since $\lambda = \alpha^m$ and $\gcd(m, \tau) = 1$, the order of λ in the group F_q^* is τ. Thus by Lemma 2.4,

$$\left|\frac{1}{\tau}\sum_{n=0}^{\tau-1} e_p\left(\sum_{i=1}^{s}\sum_{j=1}^{m} h_{ij} w_{ni}^{(j)}\right)\right| \leq \frac{q^{1/2}}{\tau} - \frac{1}{1+q^{1/2}}.$$

Recalling that $q = p^k$, we obtain from Lemma 2.1 with $b = p$

$$D_\tau^{(s)} \leq 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}\right)\sum_{\boldsymbol{h}\neq 0} P_p(\boldsymbol{h}).$$

The desired result follows now from Lemma 2.2.

In the special case where $s \leq k/m$ and the characteristic polynomial $f(x)$ is a primitive polynomial over F_p, we have the exact formula

$$D_\tau^{(s)} = 1-(1-p^{-m})^s \tag{16}$$

for all primes p according to [20, Satz 7].

Theorem 3.2. *If $s \leq k/m$, then for digital k-step pseudorandom numbers we have for $p > 2$*

$$D_N^{(s)} < 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{N}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}\right)\cdot$$
$$\cdot\left(\left(\frac{2}{\pi}m\log p + \frac{7}{5}m - \frac{m-1}{p}\right)^s - 1\right) \text{ for } 1 \leq N < \tau.$$

In the case $p = 2$ we have

$$D_N^{(s)} < 1-(1-2^{-m})^s + \left(\frac{2^{k/2}}{N}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{2^{k/2}}{\tau} - \frac{1}{1+2^{k/2}}\right)\cdot$$
$$\cdot\left(\left(\frac{m}{2}+1\right)^s - 1\right) \text{ for } 1 \leq N < \tau.$$

Proof. We proceed as in the proof of Theorem 3.1, but we use Lemma 2.5 instead of Lemma 2.4.

4. The high-dimensional case

We consider the s-dimensional serial test for digital k-step pseudorandom numbers in the case $s > k/m$. We establish upper bounds for the discrepancy $D_N^{(s)}$ of the points $\boldsymbol{x}_n$ in (3) for the cases $N = \tau$ and $N < \tau$. These bounds depend now also on the characteristic polynomial $f(x)$ in (5). We introduce the crucial quantity $R^{(s)}(f, p, m)$ which depends on the dimension s, the polynomial $f = f(x)$, the prime p, and the block length m. As in Section 2, let $C_{ms}(p)$ be the set of lattice points $\boldsymbol{h} = (h_{ij})$ with $h_{ij} \in C(p)$ for $1 \le i \le s$, $1 \le j \le m$. To each $\boldsymbol{h}$ we attach the weight $P_p(\boldsymbol{h})$ defined in (9). Furthermore, we associate with $\boldsymbol{h}$ the polynomial

$$g(\boldsymbol{h}) = \sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} x^{m(i-1)+j-1}, \tag{17}$$

viewed as a polynomial in x over the finite field F_p. Now we define

$$R^{(s)}(f, p, m) = \sum_{\substack{\boldsymbol{h} \neq 0 \\ f \mid g(\boldsymbol{h})}} P_p(\boldsymbol{h}), \tag{18}$$

where the sum is extended over all nonzero lattice points $\boldsymbol{h} \in C_{ms}(p)$ such that $g(\boldsymbol{h})$ is divisible by f in the polynomial ring $F_p[x]$. Note that the sum is nonempty since $g(\boldsymbol{h})$ runs through all polynomials over F_p of degree $< ms$ as $\boldsymbol{h}$ runs through $C_{ms}(p)$, and since f has degree $k < ms$.

Theorem 4.1. *If $s > k/m$, then for digital k-step pseudorandom numbers we have for $p > 2$*

$$D_\tau^{(s)} < 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}\right)\left(\left(\frac{2}{\pi} m \log p + \frac{7}{5} m - \frac{m-1}{p}\right)^s - 1\right) + R^{(s)}(f, p, m).$$

In the case $p = 2$ we have

$$D_\tau^{(s)} < 1-(1-2^{-m})^s + \left(\frac{2^{k/2}}{\tau} - \frac{1}{1+2^{k/2}}\right)\left(\left(\frac{m}{2}+1\right)^s - 1\right) + R^{(s)}(f, 2, m).$$

Proof. We apply Lemma 2.1. As in the proof of Theorem 3.1, we have

$$w_{ni}^{(j)} = y_{m(n+i-1)+j-1} \text{ for } 1 \le i \le s,\ 1 \le j \le m, \text{ and } n \ge 0,$$

and for a nonzero lattice point $\boldsymbol{h} = (h_{ij}) \in C_{ms}(p)$ we get

$$z_n = \sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} w_{ni}^{(j)} = \mathrm{Tr}\left(\beta \lambda^n \sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} \alpha^{m(i-1)+j-1}\right)$$

for all $n \geq 0$. If

$$\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} \alpha^{m(i-1)+j-1} \neq 0,$$

then we proceed as in the proof of Theorem 3.1 and obtain

$$\left|\frac{1}{\tau} \sum_{n=0}^{\tau-1} e_p\left(\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} w_{ni}^{(j)}\right)\right| \leq \frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}.$$

If

$$\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} \alpha^{m(i-1)+j-1} = 0, \tag{19}$$

then $z_n = 0$ for all $n \geq 0$, and so

$$\frac{1}{\tau} \sum_{n=0}^{\tau-1} e_p\left(\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} w_{ni}^{(j)}\right) = 1.$$

Since α is a root of the irreducible polynomial f over F_p, the identity (19) holds if and only if f divides the polynomial $g(\boldsymbol{h})$ in (17). Combining these results, we obtain from Lemma 2.1,

$$\begin{aligned} D_\tau^{(s)} &\leq 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}\right) \sum_{\substack{\boldsymbol{h} \neq 0 \\ f \mid g(\boldsymbol{h})}} P_p(\boldsymbol{h}) + \sum_{\substack{\boldsymbol{h} \neq 0 \\ f \mid g(\boldsymbol{h})}} P_p(\boldsymbol{h}) \\ &< 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}\right) \sum_{\boldsymbol{h} \neq 0} P_p(\boldsymbol{h}) + R^{(s)}(f, p, m). \end{aligned}$$

The desired result follows now from Lemma 2.2.

Theorem 4.2. *If $s > k/m$, then for digital k-step pseudorandom numbers we have for $p > 2$*

$$\begin{aligned} D_N^{(s)} < 1-(1-p^{-m})^s + \left(\frac{p^{k/2}}{N}\left(\frac{2}{\pi} \log \tau + \frac{2}{5}\right) + \frac{p^{k/2}}{\tau} - \frac{1}{1+p^{k/2}}\right) \cdot \\ \cdot \left(\left(\frac{2}{\pi} m \log p + \frac{7}{5} m - \frac{m-1}{p}\right)^s - 1\right) + R^{(s)}(f, p, m) \end{aligned}$$

for $1 \leq N < \tau$. In the case $p = 2$ we have

$$D_N^{(s)} < 1-(1-2^{-m})^s + \left(\frac{2^{k/2}}{N}\left(\frac{2}{\pi}\log \tau+\frac{2}{5}\right)+\frac{2^{k/2}}{\tau}-\frac{1}{1+2^{k/2}}\right)\left(\left(\frac{m}{2}+1\right)^s-1\right) + R^{(s)}(f, 2, m) \text{ for } 1 \le N < \tau.$$

Proof. We proceed as in the proof of Theorem 4.1, but we use the bound in Lemma 2.5 instead of that in Lemma 2.4.

The usefulness of the bounds in Theorems 4.1 and 4.2 is clearly linked with the problem of how small we can make the quantity $R^{(s)}(f, p, m)$. We will prove that $R^{(s)}(f, p, m)$ does indeed attain small values with a suitable choice of f. We consider irreducible polynomials f over F_p of fixed degree $\deg(f) = k$ and yielding a fixed value τ for the least period of the sequence $y_0, y_1, \ldots$. We write $\tau = \operatorname{ord}(f)$, i.e. $\operatorname{ord}(f)$ is the order of any root of f in the group F_q^* with $q = p^k$. Since τ divides p^k-1, we must have $\gcd(p, \tau) = 1$. Furthermore, k is determined by the value of τ, namely k is the multiplicative order of p modulo τ according to [9, Theorem 3.5].

Theorem 4.3. *Let p be prime, let τ be a positive integer with $\gcd(p, \tau) = 1$, let k be the multiplicative order of p modulo τ, and let m and s be positive integers such that $ms > k$. Then there exists a monic irreducible polynomial f_0 over F_p with $\deg(f_0) = k$, $\operatorname{ord}(f_0) = \tau$, and*

$$R^{(s)}(f_0, p, m) < \frac{ms-1}{\phi(\tau)}\left(\left(\frac{2}{\pi}m\log p+\frac{7}{5}m-\frac{m-1}{p}\right)^s-1\right) \text{ if } p > 2,$$

$$R^{(s)}(f_0, 2, m) \le \frac{ms-1}{\phi(\tau)}\left(\left(\frac{m}{2}+1\right)^s-1\right) \text{ if } p = 2,$$

where ϕ is Euler's totient function.

Proof. We consider the mean value R of $R^{(s)}(f, p, m)$ with s, p, m fixed and f running through the set I of all monic irreducible polynomials over F_p with $\deg(f) = k$ and $\operatorname{ord}(f) = \tau$, where k and τ are fixed. Since I has $\phi(\tau)/k$ elements according to [9, Theorem 3.5], we get from (18),

$$R = \frac{k}{\phi(\tau)}\sum_{f\in I} R^{(s)}(f, p, m) = \frac{k}{\phi(\tau)}\sum_{f\in I}\sum_{\substack{h\neq 0\\ f\backslash g(h)}} P_p(\boldsymbol{h})$$

$$= \frac{k}{\phi(\tau)}\sum_{h\neq 0} P_p(\boldsymbol{h})\sum_{\substack{f\in I\\ f\backslash g(h)}} 1.$$

In the inner sum, $g(\boldsymbol{h})$ is a nonzero polynomial with $\deg(g(\boldsymbol{h})) \le ms-1$

by (17). Therefore $g(\boldsymbol{h})$ can be divisible by at most $(ms-1)/k$ distinct elements of I. Consequently,

$$R \leq \frac{ms-1}{\phi(\tau)} \sum_{\boldsymbol{h} \neq 0} P_p(\boldsymbol{h}).$$

We apply Lemma 2.2 to obtain the final bound for R, and then we note that there must exist an $f_0 \in I$ for which $R^{(s)}(f_0, p, m)$ does not exceed the mean value R.

We note that $\phi(\tau)$ is almost of the order of magnitude τ, since according to [4, Theorem 328] we have

$$\phi(\tau) > \frac{C\tau}{\log\log \tau} \tag{20}$$

with an absolute constant $C > 0$. Therefore, if f_0 is chosen as in Theorem 4.3, then $R^{(s)}(f_0, p, m)$ is usually smaller (and in the worst case only marginally larger) than the other terms in the bounds of Theorems 4.1 and 4.2.

5. Figures of merit

The important quantity $R^{(s)}(f, p, m)$ defined in (18) is rather inconvenient numerically since it is a sum of many and mostly very small numbers. Therefore we introduce a related positive integer, the figure of merit $\rho^{(s)}(f, p, m)$, which is easier to handle. Let f, as usual, be a monic irreducible polynomial over F_p of degree k, and let $ms > k$, so that we are in the high-dimensional case. For $\boldsymbol{h} = (h_{ij}) \in C_{ms}(p)$ we define

$$D(\boldsymbol{h}) = \sum_{i=1}^{s} d(h_{i1}, \ldots, h_{im}), \tag{21}$$

where we use the notation introduced in (6). The *figure of merit* is now given by

$$\rho^{(s)}(f, p, m) = \min_{\substack{\boldsymbol{h} \neq 0 \\ f \mid g(\boldsymbol{h})}} D(\boldsymbol{h}), \tag{22}$$

where the minimum is extended over all nonzero lattice points $\boldsymbol{h} \in C_{ms}(p)$ such that the polynomial $g(\boldsymbol{h})$ in (17) is divisible by f in the polynomial ring $F_p[x]$. It is clear that the figure of merit is a positive integer. We note the following upper bounds.

Lemma 5.1. *For $s > k/m$ we have $\rho^{(s)}(f, p, m) \leq k+1$ and $\rho^{(s)}(f, p, m)$*

$\leq D(\boldsymbol{h}_0)$, *where* $\boldsymbol{h}_0 \in C_{ms}(p)$ *is the lattice point for which* $g(\boldsymbol{h}_0) = f$.

Proof. Since $s > k/m$ implies $k+1 \leq ms$, there exist integers $d_1, \ldots, d_s$ with $0 \leq d_i \leq m$ for $1 \leq i \leq s$ and $\sum_{i=1}^{s} d_i = k+1$. Let α be a root of f in the finite field F_q with $q = p^k$ elements. Note that F_q can be considered as a vector space over F_p of dimension k, and so the $k+1$ elements $\alpha^{m(i-1)+j-1}$, $1 \leq j \leq d_i$, $1 \leq i \leq s$, are linearly dependent over F_p. Thus there exist coefficients $h_{ij} \in C(p)$, not all 0, such that

$$\sum_{i=1}^{s} \sum_{j=1}^{d_i} h_{ij} \alpha^{m(i-1)+j-1} = 0.$$

Since f is irreducible over F_p, it follows that f divides the polynomial

$$\sum_{i=1}^{s} \sum_{j=1}^{d_i} h_{ij} x^{m(i-1)+j-1}$$

in $F_p[x]$. By the definition (22) we get

$$\rho^{(s)}(f, p, m) \leq \sum_{i=1}^{s} d_i = k+1,$$

and so the first bound is shown. The second bound is trivial since $\boldsymbol{h}_0$ is one of the lattice points appearing in the minimum in (22).

From the argument in the proof of Lemma 5.1 it follows that $\rho^{(s)}(f, p, m) = k+1$ if and only if every system $\{\alpha^{m(i-1)+j-1} : 1 \leq j \leq d_i, 1 \leq i \leq s\}$ with $0 \leq d_i \leq m$ for $1 \leq i \leq s$ and $\sum_{i=1}^{s} d_i = k$ is linearly independent over F_p.

We show now that $R^{(s)}(f, p, m)$ can be bounded in terms of $\rho^{(s)}(f, p, m)$. For an integer $r \geq 0$ let $K(r)$ be the number of $(d_1, \ldots, d_s) \in \{0, 1, \ldots, m\}^s$ with $\sum_{i=1}^{s} d_i \leq r$.

Theorem 5.2. *If* $s > k/m$ *and if* $R = R^{(s)}(f, p, m)$ *is defined by* (18) *and* $\rho = \rho^{(s)}(f, p, m)$ *by* (22), *then we have*

$$R \leq (p-1)\left(\frac{1}{\sin(\pi/p)}+1\right)^s ((m+1)^s - K(\rho-1))p^{-\rho} \text{ for } p > 2,$$

$$R \leq ((m+1)^s - K(\rho-1))2^{-\rho} \text{ for } p = 2.$$

Proof. For $p > 2$ the definition of Q_ρ in (8) shows that

$$Q_p(h_1,\ldots,h_m) \le \left(\frac{1}{\sin(\pi/p)}+1\right)p^{-d(h_1,\ldots,h_m)}.$$

Thus for all $\boldsymbol{h} = (h_{ij}) \in C_{ms}(p)$ we have by (9),

$$P_p(\boldsymbol{h}) \le \left(\frac{1}{\sin(\pi/p)}+1\right)^s \prod_{i=1}^{s} p^{-d(h_{i1},\ldots,h_{im})} = \left(\frac{1}{\sin(\pi/p)}+1\right)^s p^{-D(\boldsymbol{h})}$$

with $D(\boldsymbol{h})$ as in (21). In the case $p = 2$ we have $P_2(\boldsymbol{h}) = 2^{-D(\boldsymbol{h})}$ by (10). Hence if we put

$$R_1 = R_1^{(s)}(f, p, m) = \sum_{\substack{\boldsymbol{h}\neq 0 \\ f\mid g(\boldsymbol{h})}} p^{-D(\boldsymbol{h})} \tag{23}$$

with the range of summation being the same as in (18), then we get

$$\begin{aligned} &R \le \left(\frac{1}{\sin(\pi/p)}+1\right)^s R_1 \text{ for } p > 2, \\ &R = R_1 \qquad\qquad\qquad \text{for } p = 2. \end{aligned} \tag{24}$$

It suffices therefore to find an upper bound for R_1. Splitting up the sum in (23) according to the value of $D(\boldsymbol{h})$, we can write

$$R_1 = \sum_{r=\rho}^{ms} M(r)p^{-r}, \tag{25}$$

where $M(r)$ is the number of $\boldsymbol{h} \in C_{ms}(p)$ (or equivalently $\boldsymbol{h} \in F_p^{ms}$) with $D(\boldsymbol{h}) = r$ such that f divides $g(\boldsymbol{h})$.

We determine now an upper bound for $M(r)$, where $\rho \le r \le ms$. Let $L(r)$ be the number of $\boldsymbol{d} = (d_1,\ldots,d_s) \in \{0,1,\ldots,m\}^s$ with $\sum_{i=1}^{s} d_i = r$. Fix such a $\boldsymbol{d}$, and let $e_1,\ldots,e_s$ be fixed integers with $0 \le e_i \le d_i$ for $1 \le i \le s$ and $\sum_{i=1}^{s} e_i = \rho-1$. We consider the number $N(\boldsymbol{d})$ of $\boldsymbol{h} = (h_{ij}) \in F_p^{ms}$ with $d(h_{i1},\ldots,h_{im}) = d_i$ for $1 \le i \le s$ and f dividing $g(\boldsymbol{h})$. By an argument in the proof of Lemma 5.1, the condition that f divides $g(\boldsymbol{h})$ is equivalent to

$$\sum_{i=1}^{s}\sum_{j=1}^{d_i} h_{ij}\alpha^{m(i-1)+j-1} = 0. \tag{26}$$

Furthermore, by the definition of ρ in (22) the $\rho-1$ elements $\alpha^{m(i-1)+j-1}$, $1 \le j \le e_i$, $1 \le i \le s$, are linearly independent over F_p. It follows that for those i with $e_i < d_i$ we can assign coefficients $h_{ij} \in F_p$, $e_i < j \le d_i$,

with $h_{id_i} \neq 0$ arbitrarily in (26), whereas for the remaining coefficients in (26) there is at most one choice. Therefore

$$N(\boldsymbol{d}) \leq \prod_{\substack{i=1 \\ e_i<d_i}}^{s} (p-1)p^{d_i-e_i-1} = p^{r-\rho+1} \prod_{\substack{i=1 \\ e_i<d_i}}^{s} \frac{p-1}{p} \leq (p-1)p^{r-\rho}.$$

Since there are $L(r)$ possibilities for $\boldsymbol{d}$, we get

$$M(r) \leq L(r)(p-1)p^{r-\rho}.$$

We go back to (25), use the fact that $|0, 1, \ldots, m|^s$ has $(m+1)^s$ elements, and get

$$\begin{aligned} R_1 \leq (p-1)p^{-\rho} \sum_{r=\rho}^{ms} L(r) &= (p-1)p^{-\rho}\left(\sum_{r=0}^{ms} L(r) - \sum_{r=0}^{\rho-1} L(r)\right) \\ &= (p-1)p^{-\rho}((m+1)^s - K(\rho-1)). \end{aligned}$$

Together with (24) this implies the result of the theorem.

In most cases it will suffice to work with an obvious consequence of Theorem 5.2, namely

$$\begin{aligned} &R^{(s)}(f, p, m) \leq (p-1)\left(\frac{1}{\sin(\pi/p)}+1\right)^s (m+1)^s p^{-\rho} && \text{for } p > 2, \\ &R^{(s)}(f, 2, m) \leq (m+1)^s 2^{-\rho} && \text{for } p = 2, \end{aligned} \tag{27}$$

where $\rho = \rho^{(s)}(f, p, m)$. An explicit formula for $K(r)$ can be given as follows. We use $[v]$ to denote the greatest integer $\leq v$.

Lemma 5.3. *For $0 \leq r \leq ms$ we have*

$$K(r) = \sum_{t=0}^{[r/(m+1)]} (-1)^t \binom{s}{t} \binom{s+r-t(m+1)}{s}.$$

Proof. From the definition of $K(r)$ it follows that $K(r)$ is equal to the coefficient of x^r in the real power series

$$(1+x+\cdots+x^m)^s(1+x+x^2+\cdots) = \frac{(1-x^{m+1})^s}{(1-x)^{s+1}}.$$

Now

$$\frac{1}{(1-x)^{s+1}} = \sum_{u=0}^{\infty} \binom{s+u}{s} x^u$$

and so $K(r)$ is equal to the coefficient of x^r in

$$\left(\sum_{t=0}^{s}(-1)^t\binom{s}{t}x^{t(m+1)}\right)\left(\sum_{u=0}^{\infty}\binom{s+u}{s}x^u\right).$$

This coefficient is easily seen to be given by the formula in the lemma.

In Theorem 4.3 we have shown that there always exists a polynomial f_0 with a small value of $R^{(s)}(f_0, p, m)$. In view of Theorem 5.2, an analogous result for figures of merit should demonstrate the existence of an f_0 with a large value of $\rho^{(s)}(f_0, p, m)$. We prove such a theorem under the same conditions as in Theorem 4.3.

Theorem 5.4. *Let p be prime, let τ be a positive integer with $\gcd(p, \tau) = 1$, let k be the multiplicative order of p modulo τ, and let m and s be positive integers such that $ms > k$. Then there exists a monic irreducible polynomial f_0 over F_p with $\deg(f_0) = k$, $\operatorname{ord}(f_0) = \tau$, and*

$$\rho^{(s)}(f_0, p, m) \geq \left[\log_p \frac{(m+1)(p-1)\phi(\tau)}{(ms-1)(m+1-mp^{-1})^s}\right],$$

where $\log_p$ denotes the logarithm to the base p.

Proof. Put

$$t = \left[\log_p \frac{(m+1)(p-1)\phi(\tau)}{(ms-1)(m+1-mp^{-1})^s}\right] - 1. \tag{28}$$

If $t \leq 0$, then there is nothing to prove, so we can assume $t \geq 1$. For an integer $r \geq 1$ let $B(r)$ be the number of $\boldsymbol{h} \in C_{ms}(p)$ with $D(\boldsymbol{h}) = r$, where $D(\boldsymbol{h})$ is given in (21). If $(d_1, \ldots, d_s) \in \{0, 1, \ldots, m\}^s$ with $\sum_{i=1}^{s} d_i = r$, then the number of $\boldsymbol{h} = (h_{ij}) \in C_{ms}(p)$ with $d(h_{i1}, \ldots, h_{im}) = d_i$ for $1 \leq i \leq s$ is equal to

$$\prod_{\substack{i=1\\ d_i>0}}^{s}(p-1)p^{d_i-1} = p^r \prod_{\substack{i=1\\ d_i>0}}^{s}\frac{p-1}{p}.$$

Therefore $B(r)p^{-r}$ is equal to the coefficient of x^r in the real polynomial

$$\left(1+\frac{p-1}{p}x+\frac{p-1}{p}x^2+\cdots+\frac{p-1}{p}x^m\right)^s = \left(\frac{1}{p}+\frac{p-1}{p}(1+x+x^2+\cdots+x^m)\right)^s$$
$$= p^{-s}\left(1+(p-1)\frac{x^{m+1}-1}{x-1}\right)^s = p^{-s}\sum_{j=0}^{s}\binom{s}{j}(p-1)^j\left(\frac{x^{m+1}-1}{x-1}\right)^j.$$

For $j = 0$ the coefficient of x^r in $((x^{m+1}-1)/(x-1))^j$ is 0 and for $j \geq 1$ it is equal to the number of $(d_1, \ldots, d_j) \in \{0, 1, \ldots, m\}^j$ with $\sum_{i=1}^{j} d_i = r$. Since this number is obviously at most $(m+1)^{j-1}$, we obtain

$$B(r)p^{-r} \leq p^{-s}\sum_{j=1}^{s}\binom{s}{j}(p-1)^j(m+1)^{j-1} < \frac{1}{m+1}\left(m+1-\frac{m}{p}\right)^s.$$

If $E(t)$ is the number of nonzero $\boldsymbol{h} \in C_{ms}(p)$ with $D(\boldsymbol{h}) \leq t$, then

$$\begin{aligned} E(t) &= \sum_{r=1}^{t} B(r) < \frac{1}{m+1}\left(m+1-\frac{m}{p}\right)^s \sum_{r=1}^{t} p^r \\ &< \frac{1}{(m+1)(p-1)}\left(m+1-\frac{m}{p}\right)^s p^{t+1}. \end{aligned}$$

Now let $A_k(t)$ be the number of monic irreducible polynomials f over F_p with $\deg(f) = k$ and with the property that f divides $g(\boldsymbol{h})$ for some nonzero $\boldsymbol{h} \in C_{ms}(p)$ with $D(\boldsymbol{h}) \leq t$. Since each such $g(\boldsymbol{h})$ in (17) has degree $\leq ms-1$, it is divisible by at most $(ms-1)/k$ polynomials f, hence

$$A_k(t) \leq \frac{ms-1}{k}E(t) < \frac{ms-1}{(m+1)(p-1)k}\left(m+1-\frac{m}{p}\right)^s p^{t+1}.$$

From the definition of t in (28) it follows that

$$A_k(t) < \frac{\phi(\tau)}{k}. \tag{29}$$

By [9, Theorem 3.5], $\phi(\tau)/k$ is the total number of monic irreducible polynomials f over F_p with $\deg(f) = k$ and $\operatorname{ord}(f) = \tau$. Thus (29) implies that there exists a monic irreducible polynomial f_0 over F_p with $\deg(f_0) = k$ and $\operatorname{ord}(f_0) = \tau$ which is not counted by the counting function $A_k(t)$. In other words, f_0 divides no polynomial $g(\boldsymbol{h})$ with a nonzero $\boldsymbol{h} \in C_{ms}(p)$ and $D(\boldsymbol{h}) \leq t$. From the definition of the figure of merit in (22) we obtain then

$$\rho^{(s)}(f_0, p, m) \geq t+1,$$

and this is the result of the theorem.

6. Lower bounds

We first establish a universal lower bound for $D_N^{(s)}$ that can be viewed as the discretization error of digital k-step pseudorandom numbers. An anal-

ogous lower bound was already noted in [16, Sec. 5] for the uniformity test.

Theorem 6.1. *For digital k-step pseudorandom numbers we have*

$$D_N^{(s)} \geq 1-(1-p^{-m})^s \text{ for all } s \geq 2 \text{ and } N \geq 1.$$

Proof. We note that all the digital k-step pseudorandom numbers x_n given by (2) are rational numbers in $[0, 1)$ with denominator p^m. It follows that all the points $\boldsymbol{x}_n$ in (3) belong to the interval

$$J = [0, 1-p^{-m}]^s.$$

In the notation of (4) we have then $E_N(J) = 1$ for all $N \geq 1$ and $V(J) = (1-p^{-m})^s$, and so the desired lower bound follows immediately from (4).

Since this lower bound results from the fact that all x_n are rationals with a fixed denominator, we may interpret it as the *discretization error*. It is of interest to note that $1-(1-p^{-m})^s$ occurs also as a term in all the upper bounds for $D_N^{(s)}$ in Sections 3 and 4.

For the high-dimensional case, the results in Sections 4 and 5 show that $D_N^{(s)}$ can be bounded from above in terms of the figure of merit. We prove now that $D_N^{(s)}$ can also be bounded from below in a similar manner.

Theorem 6.2. *If $s > k/m$, then for digital k-step pseudorandom numbers we have*

$$D_N^{(s)} \geq \frac{p-1}{2} p^{-\rho} \text{ for all } N \geq 1,$$

where $\rho = \rho^{(s)}(f, p, m)$.

Proof. By the definition of ρ in (22) there exists a nonzero $\boldsymbol{h} = (h_{ij}) \in C_{ms}(p)$ such that $D(\boldsymbol{h}) = \rho$ and f divides

$$g(\boldsymbol{h}) = \sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} x^{m(i-1)+j-1} \in F_p[x].$$

Let r with $1 \leq r \leq s$ be the largest integer for which $(h_{r1}, \ldots, h_{rm}) \neq (0, \ldots, 0)$. Put $d_i = d(h_{i1}, \ldots, h_{im})$ for $1 \leq i \leq r$, then

$$D(\boldsymbol{h}) = \sum_{i=1}^{r} d_i$$

and

$$g(\boldsymbol{h}) = \sum_{i=1}^{r} \sum_{j=1}^{d_i} h_{ij} x^{m(i-1)+j-1}.$$

Now $y_0, y_1, \ldots$, considered as a sequence of elements of F_p, has the irreducible polynomial f over F_p as a characteristic polynomial, and not all initial values of the sequence are 0. Hence [9, Theorem 8.50] implies that f is the minimal polynomial of the sequence. Since f divides $g(\boldsymbol{h})$, it follows from [9, Theorem 8.42] that $g(\boldsymbol{h})$ is also a characteristic polynomial of the sequence. Therefore

$$\sum_{i=1}^{r} \sum_{j=1}^{d_i} h_{ij} y_{n+m(i-1)+j-1} = 0 \text{ for all } n \geq 0,$$

and replacing n by mn we get

$$\sum_{i=1}^{r} \sum_{j=1}^{d_i} h_{ij} y_{m(n+i-1)+j-1} = 0 \text{ for all } n \geq 0, \tag{30}$$

where this identity holds in F_p. Choose a small $\varepsilon > 0$ and define the intervals

$$I_i = [0,\ p^{-d_i} - \varepsilon] \text{ for } 1 \leq i < r,$$
$$I_r = (p^{-d_r},\ p^{-d_{r+1}} - \varepsilon].$$

The subinterval I of $[0, 1]^s$ is then defined by

$$I = I_1 \times \cdots \times I_r \times [0, 1]^{s-r}.$$

We claim that no point $\boldsymbol{x}_n$ in (3) belongs to I. Suppose that for some $n \geq 0$ we had

$$\boldsymbol{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in I.$$

Then from (2),

$$x_{n+i-1} = \sum_{j=1}^{m} y_{m(n+i-1)+j-1} p^{-j} \in I_i \text{ for } 1 \leq i \leq r.$$

For $1 \leq i < r$ it follows from the definition of I_i that

$$y_{m(n+i-1)+j-1} = 0 \text{ for } 1 \leq j \leq d_i.$$

For $i = r$ it follows from the definition of I_r that

$$y_{m(n+r-1)+j-1} = 0 \text{ for } 1 \leq j < d_r,$$
$$y_{m(n+r-1)+j-1} \neq 0 \text{ for } j = d_r.$$

These facts yield a contradiction to (30) since $h_{rd_r} \neq 0$. Thus, indeed, no point $\boldsymbol{x}_n$ belongs to I. Therefore we have $E_N(I) = 0$ for all $N \geq 1$ in the notation of (4). Now we define subintervals J_1 and J_2 of $[0, 1]^s$ by

$$J_1 = I_1 \times \cdots \times I_{r-1} \times [0, p^{-d_r+1} - \varepsilon] \times [0, 1]^{s-r},$$
$$J_2 = I_1 \times \cdots \times I_{r-1} \times [0, p^{-d_r}] \times [0, 1]^{s-r}.$$

Then J_1 is the disjoint union of I and J_2, thus

$$V(J_1) = V(I) + V(J_2),$$
$$E_N(J_1) = E_N(I) + E_N(J_2) \text{ for all } N \geq 1.$$

Hence

$$V(I) = |E_N(I) - V(I)| = |(E_N(J_1) - V(J_1)) - (E_N(J_2) - V(J_2))|$$
$$\leq |E_N(J_1) - V(J_1)| + |E_N(J_2) - V(J_2)| \leq 2D_N^{(s)}$$

by (4), and so

$$D_N^{(s)} \geq \frac{1}{2} V(I) = \frac{1}{2}(p^{-d_r+1} - p^{-d_r} - \varepsilon) \prod_{i=1}^{r-1} (p^{-d_i} - \varepsilon).$$

Letting $\varepsilon \to 0+$, we get

$$D_N^{(s)} \geq \frac{p-1}{2} \prod_{i=1}^{r} p^{-d_i} = \frac{p-1}{2} p^{-D(\boldsymbol{h})},$$

and since $D(\boldsymbol{h}) = \rho$, the proof is complete.

7. Discussion

In the context of studying the performance of digital k-step pseudorandom numbers x_n under the uniformity test, it was noted in [16] that the statistical quality of the x_n improves as the value τ of the least period of the sequence of x_n increases. This is also borne out by our Theorem 3.1 in which the upper bound for $D_\tau^{(s)}$ is a decreasing function of τ. As we have mentioned in Section 1, the maximal value of τ for given p and k is $\tau = p^k - 1$. This corresponds to choosing for the characteristic polynomial f a primitive polynomial over F_p. In the following discussion of our results we will concentrate on this case, and we will also take $N = \tau$, i.e. we consider the full period.

We remark that if $\tau = p^k - 1$, then for an expression which appears in the upper bounds in Theorems 3.1 and 4.1 we have

$$\frac{p^{k/2}}{\tau} - \frac{1}{1 + p^{k/2}} = \frac{1}{\tau}.$$

We use the symbol $\ll$ to denote an inequality in which constant factors depending only on s and p are suppressed.

For $s \leq k/m$ and $\tau = p^k - 1$ we have the exact formula

$$D_\tau^{(s)} = 1 - (1 - p^{-m})^s$$

according to (16). The discrepancy in the low-dimensional case is thus given by the discretization error and its order of magnitude is p^{-m}.

We turn now to the high-dimensional case $s > k/m$. We take again $\tau = p^k - 1$. If $\rho = \rho^{(s)}(f, p, m)$ is the figure of merit, then using $m \leq k$ we obtain

$$p^{-m} + p^{-\rho} \ll D_\tau^{(s)} \ll p^{-m} + \tau^{-1}(\log \tau)^s + p^{-\rho}(\log \tau)^s,$$

where the lower bound stems from Theorems 6.1 and 6.2 and the upper bound results from combining Theorem 4.1 with (27). Since $\rho \leq k+1$ by Lemma 5.1, we can further simplify to get

$$p^{-m} + p^{-\rho} \ll D_\tau^{(s)} \ll p^{-m} + p^{-\rho}(\log \tau)^s. \tag{31}$$

This demonstrates that if f is restricted to be a primitive polynomial over F_p of degree k, then *the dependence of the order of magnitude of $D_\tau^{(s)}$ on f is controlled by the figure of merit ρ.* The performance of digital k-step pseudorandom numbers under the s-dimensional serial test will improve as ρ increases. An interesting special case occurs if we choose $m = k$, for then (31) reduces to

$$p^{-\rho} \ll D_\tau^{(s)} \ll p^{-\rho}(\log \tau)^s,$$

so that the order of magnitude of $D_\tau^{(s)}$ is, up to a logarithmic factor, given by $p^{-\rho}$. The exponent s of the logarithmic factor can be improved to $s-1$ by a different method; see [21, Theorem 9.4].

To show that digital k-step pseudorandom numbers can yield very small values of $D_\tau^{(s)}$ even for $s > k/m$, we choose again $m = k$ and combine Theorems 4.1 and 4.3. We arrive then at the statement that with a suitable primitive polynomial f_0 over F_p of degree k we can obtain

$$D_\tau^{(s)} \ll \tau^{-1}(\log \tau)^s + \phi(\tau)^{-1}(\log \tau)^{s+1}.$$

Since $\phi(\tau) \leq \tau$, this reduces to

$$D_\tau^{(s)} \ll \phi(\tau)^{-1}(\log \tau)^{s+1}. \tag{32}$$

In order to get a bound not involving Euler's totient function, one may use (20) to obtain

$$D_\tau^{(s)} \ll \tau^{-1}(\log \tau)^{s+1} \log\log \tau. \tag{33}$$

Therefore, *digital k-step pseudorandom numbers pass the s-dimensional serial test for arbitrarily large s provided that the parameters in the generation process are chosen suitably.*

Note that if $\tau = p^k-1$, then the choice $m = k$ is not always possible since in view of our standing hypothesis $\gcd(m, \tau) = 1$ we must have $\gcd(k, p^k-1) = 1$. An easy way of satisfying the latter condition is to let k be a prime not dividing $p-1$, for then $p^k-1 \equiv p-1 \not\equiv 0 \bmod k$. More generally, we can take any k with prime factor decomposition $k = q_1^{e_1}\cdots q_r^{e_r}$ such that for every prime factor $q_i \neq p$ the multiplicative order of p modulo q_i does not divide $k/q_i^{e_i}$. For if this condition is satisfied and we have nevertheless $\gcd(k, p^k-1) > 1$, then some prime factor $q_i \neq p$ divides p^k-1. But then

$$1 \equiv p^k \equiv (p^{q_i^{e_i}})^{k/q_i^{e_i}} \equiv p^{k/q_i^{e_i}} \bmod q_i,$$

hence the multiplicative order of p modulo q_i divides $k/q_i^{e_i}$, a contradiction. In the case $p = 2$, an interesting possibility of satisfying $\gcd(k, 2^k-1) = 1$ is to choose k in such a way that 2^k-1 is a Mersenne prime. This has some additional advantages. First of all, we have then $\phi(\tau) = \tau-1$ since $\tau = 2^k-1$ is prime, and so (32) reduces to

$$D_\tau^{(s)} \ll \tau^{-1}(\log \tau)^{s+1}.$$

Thus the factor $\log\log \tau$ in (33) can be dropped in this case. Furthermore, if 2^k-1 is prime, then any irreducible polynomial f over F_2 of degree k is automatically primitive, since the facts that $\operatorname{ord}(f) > 1$ and $\operatorname{ord}(f)$ divides 2^k-1 imply $\operatorname{ord}(f) = 2^k-1$. In the range of interest for pseudorandom number generation, values of k with 2^k-1 prime are given by $k = 19, 31, 61$, and 89.

We have seen that in the case $s > k/m$ it is important that we choose a characteristic polynomial f which is not only primitive, but also yields a large value of $\rho^{(s)}(f, p, m)$. We emphasize that the figure of merit depends strongly on the dimension s. This means, in particular, that if we consider "optimal" polynomials, i.e. primitive polynomials f for which $\rho^{(s)}(f, p, m)$ is maximal for given s, p, m, and k, then these optimal polynomials will depend on s. There is, however, a simple principle which guarantees that if f is optimal for some dimension s, then its figure of merit is large (though not necessarily maximal) for all smaller dimensions. In fact, for dimensions $s, t > k/m$ it follows easily from the definition of the figure of merit that

(34) $$\rho^{(t)}(f, p, m) \geq \rho^{(s)}(f, p, m) \text{ whenever } t \leq s.$$

This principle can be used as follows in the numerical practice: if a digital k-step pseudorandom number generator is needed for several purposes, it suffices to choose it in such a way that it satisfies the most stringent statistical independence condition desired in these applications (or equivalently, that it passes the s-dimensional serial test for the largest value of s that is needed). Viewed from a different angle, the inequality (34) says that if a sequence of digital k-step pseudorandom numbers fails the serial test for a certain dimension $t > k/m$(i.e., if $\rho^{(t)}(f, p, m)$ is small), then it will fail the serial test for all higher dimensions s. In this form the statement is of course intuitively obvious.

In the important special case $m = k$ the condition $s > k/m$ reduces to $s \geq 2$. In view of the discussion above, it is clear that if we want digital k-step pseudorandom numbers with good statistical independence properties, then the pseudorandom numbers must first of all pass the 2-dimensional serial test. In the case where $s = 2$ and $m = k$, there is an explicit formula for the figure of merit which facilitates its calculation considerably. This formula was shown in [20, Satz 12] and it says that

(35) $$\rho^{(2)}(f, p, k) = k+2-L(f),$$

where $L(f)$ is the maximum degree of the partial quotients in the continued fraction expansion of the rational function $f(x)/x^k$ over F_p. As is well known, the partial quotients in the continued fraction expansion can be calculated by the Euclidean algorithm.

We further illustrate the importance of figures of merit by considering an example of Knuth [6, Sec. 3.2.2] from the viewpoint of our theory. As a warning signal against an unreflected use of the digital method, Knuth constructs the example $p = 2$, $m = k = 35$, and $f(x) = x^{35}+x^2+1 \in F_2[x]$. Then f is primitive over F_2, hence $\tau = 2^{35}-1$, and the condition $\gcd(m, \tau) = \gcd(35, 2^{35}-1) = 1$ is satisfied. It is pointed out by Knuth that this particular generator fails the 2-dimensional serial test badly. This can also be seen immediately from our results, since the second part of Lemma 5.1 shows that $\rho^{(2)}(f, 2, 35) \leq D(\boldsymbol{h}_0) = 4$. In fact, it is easy to see that no polynomial $g(\boldsymbol{h})$ with $1 \leq D(\boldsymbol{h}) \leq 3$ is a multiple of f, and so $\rho^{(2)}(f, 2, 35) = 4$. This value is of course much too small. On the other hand, if we apply Theorem 5.4 with the parameters $p = 2$, $\tau = 2^{35}-1$, $m = k = 35$, and $s = 2$, then we can guarantee the existence of a primitive polynomial f_0 over F_2

of degree 35 with

$$\rho^{(2)}(f_0, 2, 35) \geq \left[\log_2 \frac{48\phi(2^{35}-1)}{31487}\right].$$

Since

$$\phi(2^{35}-1) = \phi(31 \cdot 71 \cdot 127 \cdot 122921) = 30 \cdot 70 \cdot 126 \cdot 122920,$$

this yields $\rho^{(2)}(f_0, 2, 35) \geq 25$. An explicit choice for f_0 is given by the primitive polynomial

$$f_0(x) = x^{35}+x^{34}+x^{32}+x^{28}+x^{27}+x^{18}+1 \in F_2[x],$$

for which we have $\rho^{(2)}(f_0, 2, 35) = 35$ by (35) since $L(f_0) = 2$. Thus there is a choice of f_0 such that the corresponding digital k-step pseudorandom numbers show an excellent behavior under the 2-dimensional serial test. The situation is thus quite similar to the one for the multiplicative congruential method where one has to choose the multiplier "correctly" in order to get good statistical properties; compare with the discussions in Knuth [6, Ch. 3] and Niederreiter [13].

Finally, we remark that if the parameters are well chosen in the digital method, then it is definitely superior to the normalization method mentioned in Section 1. Indeed, we have seen in (33) that for any s, p, and k a suitable choice of parameters yields digital k-step pseudorandom numbers with $\tau = p^k - 1$ and a discrepancy $D_\tau^{(s)}$ of order of magnitude at most $\tau^{-1}(\log \tau)^{s+1} \log\log \tau$. On the other hand, it was shown in Niederreiter [14] that for the normalization method we have a universal lower bound for $D_\tau^{(s)}$ of the order of magnitude p^{-1}, which is $\tau^{-1/k}$ in terms of τ and thus much larger than the upper bound attainable for the digital method.

References

[1] A. C. Arvillias and D. G. Maritsas : Partitioning the period of a class of m-sequences and application to pseudorandom number generation, J. Assoc. Comput. Mach. 25 (1978), 675–686.

[2] M. Fushimi : Increasing the orders of equidistribution of the leading bits of the Tausworthe sequence, Inform. Process. Lett. 16 (1983), 189–192.

[3] M. Fushimi and S. Tezuka : The k-distribution of the generalized feedback shift register pseudorandom numbers, Comm. Assoc. Comput. Mach. 26 (1983), 516–523.

[4] G. H. Hardy and E. M. Wright : An Introduction to the Theory of Numbers, 4th ed., Clarendon Press, Oxford, 1960.

[5] S. Kirkpatrick and E. P. Stoll : A very fast shift-register sequence random number generator, J. Comput. Physics 40 (1981), 517–526.

[6] D. E. KNUTH : The Art of Computer Programming, Vol. 2 : Seminumerical Algorithms, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

[7] L. KUIPERS and H. NIEDERREITER : Uniform Distribution of Sequences, Wiley-Interscience, New York, 1974.

[8] D. H. LEHMER : Mathematical methods in large-scale computing units, Proc. 2nd Symp. on Large-Scale Digital Calculating Machinery (Cambridge, Mass., 1949), 141−146, Harvard Univ. Press, Cambridge, Mass., 1951.

[9] R. LIDL and H. NIEDERREITER : Finite Fields, Encyclopedia of Math. and Its Appl., Vol. 20, Addison-Wesley, Reading, Mass., 1983.

[10] R. LIDL and H. NIEDERREITER : Introduction to Finite Fields and Their Applications, Cambridge Univ. Press, Cambridge, 1986.

[11] H. NIEDERREITER : On the distribution of pseudorandom numbers generated by the linear congruential method. III, Math. Comp. 30 (1976), 571−597.

[12] H. NIEDERREITER : Pseudorandom numbers and optimal coefficients, Advances in Math. 26 (1977), 99−181.

[13] H. NIEDERREITER : Quasi-Monte Carlo methods and pseudorandom numbers, Bull. Amer. Math. Soc. 84 (1978), 957−1041.

[14] H. NIEDERREITER : Statistical tests for Tausworthe pseudorandom numbers, Probability and Statistical Inference (W. Grossmann *et al.*, eds.), 265−274, Reidel, Dordrecht, 1982.

[15] H. NIEDERREITER : Applications des corps finis aux nombres pseudo-aléatoires, Sém. Théorie des Nombres 1982−1983, Exp. 38, Univ. de Bordeaux I, Talence, 1983.

[16] H. NIEDERREITER : The performance of k-step pseudorandom number generators under the uniformity test, SIAM J. Sci. Statist. Computing 5 (1984), 798−810.

[17] H. NIEDERREITER : Number-theoretic problems in pseudorandom number generation, Proc. Symp. on Applications of Number Theory to Numerical Analysis (Kyoto, 1984), 18−28, Lecture Notes No. 537, Research Inst. of Math. Sciences, Kyoto Univ., 1984.

[18] H. NIEDERREITER : The serial test for pseudorandom numbers generated by the linear congruential method, Numer. Math. 46 (1985), 51−68.

[19] H. NIEDERREITER : Multidimensional numerical integration using pseudorandom numbers, Math. Programming Study 27 (1986), 17−38.

[20] H. NIEDERREITER : Pseudozufallszahlen und die Theorie der Gleichverteilung, Sitzungsber. Österr. Akad. Wiss. Math.-Naturwiss. Kl. 195 (1986), 109−138.

[21] H. NIEDERREITER : Point sets and sequences with small discrepancy, Monatsh. Math. 104 (1987), 273−337.

[22] P. H. PESKUN : Theoretical tests for choosing the parameters of the general mixed linear congruential pseudorandom number generator, J. Statist. Comput. Simulation 11 (1980), 281−305.

[23] R. C. TAUSWORTHE : Random numbers generated by linear recurrence modulo two, Math. Comp. 19 (1965), 201−209.

[24] A. VAN WIJNGAARDEN : Mathematics and computing, Proc. Symp. on Automatic Digital Computation (London, 1954), 125−129, H. M. Stationery Office, London, 1954.

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

(*Received March 20, 1987*)