MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 279-294

PSEUDORANDOM VECTOR GENERATION BY THE MULTIPLE-RECURSIVE MATRIX METHOD

HARALD NIEDERREITER

ABSTRACT. Pseudorandom vectors are of importance for parallelized simulation methods. In this paper we carry out an in-depth analysis of the multiple-recursive matrix method for the generation of uniform pseudorandom vectors which was introduced in an earlier paper of the author. We study, in particular, the periodicity properties, the lattice structure, and the behavior under the serial test for sequences of pseudorandom vectors generated by this method.

1. INTRODUCTION

A sequence of pseudorandom vectors is generated by a deterministic algorithm and should simulate, for practical computational purposes, a sequence of i.i.d. random vector variables with a given multivariate distribution. The widespread use of parallelized simulation methods has created a great demand for good algorithms for the generation of pseudorandom vectors (see [2, 3, 4]). This paper is devoted to *uniform pseudorandom vectors* where the target distribution is the uniform distribution on the k-dimensional unit cube $[0, 1]^k$ with $k \geq 2$. We are interested only in methods that directly generate pseudorandom vectors, and not in methods that build up pseudorandom vectors from suitable pseudorandom numbers.

A few such direct methods for the generation of uniform pseudorandom vectors have already been proposed in the literature. The *matrix method* is a natural analog of the classical linear congruential method for pseudorandom number generation; expository accounts of the matrix method can be found in L'Ecuyer [7, 8] and Niederreiter [16, Chapter 10]. An extension of the matrix method, the *multiple-recursive matrix method*, was recently introduced by the author [17] and will be the subject of the present paper. One of the advantages of the multiple-recursive matrix method is that it leads to larger periods than the matrix method. The general family of *nonlinear methods* was proposed by Niederreiter [15], and a brief discussion of these methods is presented in [16, Chapter 10]. The *inversive method* is a particularly attractive nonlinear method which was introduced by Niederreiter [14] and studied in detail in [18]. The inversive method can be viewed as an analog of the inversive congruential method for pseudorandom number generation due to Eichenauer and Lehn [5].

The aim of this paper is to carry out a detailed analysis of the multiple-recursive matrix method for the generation of uniform pseudorandom vectors.

Received by the editor December 7, 1993.
1991 *Mathematics Subject Classification*. Primary 11K45, 65C10; Secondary 11K38, 11T30.

As mentioned above, this method was introduced in [17], but the discussion in [17] was confined to elementary periodicity properties. Here we study now the finer structure of sequences of pseudorandom vectors generated by the multiple-recursive matrix method, such as the lattice structure and statistical (almost-) independence properties as measured by the serial test, and we introduce and analyze appropriate figures of merit. We will even be able to say more about periodicity properties.

We now recall the definition of the multiple-recursive matrix method from Niederreiter [17]. Let us first note that we always use F_r for the finite field with r elements, where r is a prime power. Now let p be a prime and let $k \geq 2$ and $m \geq 2$ be integers. As above, k is the dimension of the vectors to be generated. Let $A_0, A_1, \dots, A_{m-1}$ be $k \times k$ matrices over F_p, where A_0 is assumed to be nonsingular. We generate a sequence $\mathbf{z}_0, \mathbf{z}_1, \dots$ of row vectors from F_p^k by choosing initial vectors $\mathbf{z}_0, \mathbf{z}_1, \dots, \mathbf{z}_{m-1}$ that are not all $\mathbf{0}$ and using the mth-order vector recursion

$$\text{(1)} \qquad \mathbf{z}_{n+m} = \sum_{h=0}^{m-1} \mathbf{z}_{n+h} A_h \quad \text{for } n = 0, 1, \dots .$$

For the sake of easier reference, we call such a sequence $\mathbf{z}_0, \mathbf{z}_1, \dots$ an (mth-order) *recursive vector sequence* (in F_p^k). Now we identify F_p with the set $\{0, 1, \dots, p-1\}$ of integers and we derive a sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ of pseudorandom vectors by putting

$$\text{(2)} \qquad \mathbf{u}_n = \frac{1}{p}\mathbf{z}_n \in [0, 1)^k \quad \text{for } n = 0, 1, \dots .$$

The sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ defined by (1) and (2) is then a sequence of pseudorandom vectors generated by the multiple-recursive matrix method. In practice, p is taken to be large. We could of course have included the case $m = 1$, but this case corresponds to the matrix method with which we are not concerned here. The matrix method for the dimension km can be used to derive some elementary results on the multiple-recursive matrix method (see [17]), but not the more intricate results presented here.

We mention in passing that recursive vector sequences can also be used for pseudorandom number generation. This was already pointed out in [17], and an in-depth study of pseudorandom numbers produced from recursive vector sequences was carried out in [19]. Some results of the latter paper will also be useful in the present work. These pseudorandom number generators include various interesting generators as special cases, for instance the classical GFSR generators and the twisted GFSR generators recently introduced by Matsumoto and Kurita [10].

In §2 we review the known periodicity properties of sequences of pseudorandom vectors generated by the multiple-recursive matrix method, and we also employ concepts and results from [19] to gain further insight for the case of the maximum period. In §3 we establish the lattice structure of pseudorandom vectors generated by the multiple-recursive matrix method. The performance of these pseudorandom vectors under the serial test for statistical independence is investigated in §4, and general theoretical results for the full period as well as for parts of the period are proved. The theory of the serial test leads to the introduction and the analysis of appropriate figures of merit in §5. In §6 we discuss the practical implications of our results and we raise some open problems.

2. Periodicity properties

A recursive vector sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ generated by (1) is periodic, and from the fact that A_0 is nonsingular it follows that it is even purely periodic, i.e., that there is no preperiod. For a purely periodic sequence $a_0, a_1, \ldots$ of elements of an arbitrary set we write $\operatorname{per}(a_n)$ for its least period length. It is obvious from (2) that $\operatorname{per}(\mathbf{u}_n) = \operatorname{per}(\mathbf{z}_n)$, so that it suffices to study the periodicity properties of recursive vector sequences. It was already shown in [17] that for an mth-order recursive vector sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ in F_p^k we always have $\operatorname{per}(\mathbf{z}_n) \leq p^{km} - 1$. For practical implementations of the multiple-recursive matrix method the case $\operatorname{per}(\mathbf{z}_n) = p^{km} - 1$ of the maximum period is certainly of greatest interest. The following general criterion for the maximum period in terms of the matrices $A_0, A_1, \ldots, A_{m-1}$ in (1) was established in [17]. We denote by I_r the $r \times r$ identity matrix over F_p.

Lemma 1. *For an mth-order recursive vector sequence $\mathbf{z}_0, \mathbf{z}_1, \ldots$ in F_p^k we have $\operatorname{per}(\mathbf{z}_n) = p^{km} - 1$ if and only if the polynomial*

$$\det\left(x^m I_k - \sum_{h=0}^{m-1} x^h A_h\right)$$

of degree km is a primitive polynomial over F_p.

Recursive vector sequences with maximum period can be further characterized in terms of explicit formulas, and such formulas are also instrumental for the deeper analysis of these sequences. Throughout the rest of the paper we use the abbreviation $q = p^{km}$, and we write Tr for the trace function from the finite field F_q to its prime subfield F_p (see [9, Definition 2.22] for the definition of the trace). The following result from [19] characterizes recursive vector sequences with maximum period among *all* sequences in F_p^k.

Lemma 2. *Let*

$$\mathbf{z}_n = (z_n^{(1)}, \ldots, z_n^{(k)}) \in F_p^k \quad \text{for } n = 0, 1, \ldots$$

be an arbitrary sequence of elements of F_p^k. Then this sequence is an mth-order recursive vector sequence with $\operatorname{per}(\mathbf{z}_n) = p^{km} - 1$ if and only if

$$z_n^{(j)} = \operatorname{Tr}(\beta_j \sigma^n) \quad \text{for } 1 \leq j \leq k \text{ and } n \geq 0, \tag{3}$$

where σ is a primitive element of F_q with $q = p^{km}$ and the km elements $\beta_j \sigma^{i-1}$, $1 \leq i \leq m$, $1 \leq j \leq k$, of F_q form a basis of F_q over F_p.

For the moment, we consider an arbitrary field extension F/K and we note that F can be viewed as a vector space over K. For $\theta \in F$ and a K-linear subspace W of F we define $\theta W = \{\theta\mu : \mu \in W\}$, which is again a K-linear subspace of F. In the following definition we introduce subspaces of the vector space F over K that permit a special kind of direct-sum decomposition of F.

Definition 1. Let F/K be an arbitrary field extension and let $\sigma \in F$ with $\sigma \neq 0$. Then a K-linear subspace W of F is called *σ-splitting* if for some $m \geq 1$ we have

$$F = \bigoplus_{i=1}^{m} (\sigma^{i-1} W).$$

It is clear that if F/K is a finite extension and W is a σ-splitting K-linear subspace of F of dimension k, then $[F : K] = km$, where m is the integer in Definition 1. We now apply this concept to the extension F_q/F_p with $q = p^{km}$, and we can then rephrase the last condition in Lemma 2 in the form given in the lemma below.

Lemma 3. *Let $\sigma \in F_q$ with $\sigma \neq 0$, where $q = p^{km}$. Then the km elements $\beta_j \sigma^{i-1}$, $1 \leq i \leq m$, $1 \leq j \leq k$, of F_q form a basis of F_q over F_p if and only if $\beta_1, \dots, \beta_k$ form a basis of a σ-splitting F_p-linear subspace of F_q.*

Consequently, we can construct an mth-order recursive vector sequence $\mathbf{z}_0$, $\mathbf{z}_1, \dots$ in F_p^k with $\text{per}(\mathbf{z}_n) = p^{km} - 1$ if we start from an arbitrary primitive element σ of F_q and an arbitrary σ-splitting F_p-linear subspace W of F_q of dimension k and then define the sequence by (3), where $(\beta_1, \dots, \beta_k)$ is an ordered basis of W. To guarantee that this construction is always possible, it suffices to find examples of appropriate σ-splitting subspaces.

Lemma 4. *Let F/K be an arbitrary field extension and let E be an intermediate field such that F is a finite simple extension of E. Then for any nonzero $\sigma \in F$ with $F = E(\sigma)$ and any nonzero $\theta \in F$, the K-linear subspace θE of F is σ-splitting.*

Proof. If F has degree m over E and $F = E(\sigma)$, then the elements σ^{i-1}, $1 \leq i \leq m$, form a basis of F over E. Therefore, for a nonzero $\theta \in F$ and any $\alpha \in F$ we have

$$\theta^{-1}\alpha = \sum_{i=1}^{m} \mu_i \sigma^{i-1}$$

with suitable $\mu_i \in E$, and so

$$\alpha = \sum_{i=1}^{m} \sigma^{i-1} \theta \mu_i.$$

This means that F is the sum of the subspaces $\sigma^{i-1}\theta E$, $1 \leq i \leq m$. Using again the basis property of the elements σ^{i-1}, $1 \leq i \leq m$, we see that F is the direct sum of these subspaces. □

Theorem 1. *For any prime p and for any integers $k \geq 2$ and $m \geq 2$ there exists a sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ of k-dimensional pseudorandom vectors generated by (1) and (2) with $\text{per}(\mathbf{u}_n) = p^{km} - 1$.*

Proof. We recall that $\text{per}(\mathbf{u}_n) = \text{per}(\mathbf{z}_n)$, so that it suffices to prove the analogous result for mth-order recursive vector sequences in F_p^k. We choose a primitive element σ of F_q with $q = p^{km}$. Furthermore, we apply Lemma 4 to the extension F_q/F_p and the intermediate field $E = F_{p^k}$. Since $F_q = F_{p^k}(\sigma)$, we obtain that for any nonzero $\theta \in F_q$ the F_p-linear subspace θF_{p^k} of F_q

of dimension k is σ-splitting. Therefore, the construction described after Lemma 3 yields an mth-order recursive vector sequence $\mathbf{z}_0, \mathbf{z}_1, \dots$ in F_p^k with $\operatorname{per}(\mathbf{z}_n) = p^{km} - 1$. □

The result of Theorem 1 exhibits one of the significant advantages of the multiple-recursive matrix method over the matrix method, namely that for a given prime p and a given dimension k we can obtain arbitrarily large least period lengths by choosing higher-order vector recursions, whereas for the matrix method we can reach only the least period length $p^k - 1$ (see [16, Chapter 10]).

3. Lattice structure

Pseudorandom vectors generated by the multiple-recursive matrix method possess an inherent lattice structure, just like linear congruential pseudorandom numbers (see Knuth [6, Chapter 3] and Ripley [20, Chapter 2]) and pseudorandom vectors generated by the matrix method (see Afflerbach and Grothe [1] and Niederreiter [16, Chapter 10]). We consider a sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ of k-dimensional pseudorandom vectors generated by (1) and (2) with $\operatorname{per}(\mathbf{u}_n) = p^{km} - 1 =: T$, i.e., with the maximum period for given p, k, and m. For a given dimension s we define the points

$$(4) \qquad \mathbf{v}_n = (\mathbf{u}_n, \mathbf{u}_{n+1}, \dots, \mathbf{u}_{n+s-1}) \in [0, 1)^{ks} \quad \text{for } n = 0, 1, \dots.$$

For $s \leq m$ we have an almost perfect equidistribution of the $\mathbf{v}_n$, $n = 0, 1, \dots, T-1$, as will be shown in Theorem 3. A nontrivial lattice structure arises for dimensions $s > m$.

We define the $k \times k$ matrices $A_h^{(j)}$ over F_p for $0 \leq h \leq m-1$ and $j \geq 0$ by setting the initial values

$$A_h^{(0)} = A_h \quad \text{for } 0 \leq h \leq m-1,$$

where the A_h are as in (1), and then using the following recursions for $j \geq 0$:

$$A_0^{(j+1)} = A_0 A_{m-1}^{(j)},$$

$$A_h^{(j+1)} = A_{h-1}^{(j)} + A_h A_{m-1}^{(j)} \quad \text{for } 1 \leq h \leq m-1.$$

For given $s > m$ we introduce the $km \times k(s-m)$ matrix

$$A^{(s)} = \begin{pmatrix} A_0^{(0)} & A_0^{(1)} & \cdots & A_0^{(s-m-1)} \\ A_1^{(0)} & A_1^{(1)} & \cdots & A_1^{(s-m-1)} \\ \vdots & \vdots & & \vdots \\ A_{m-1}^{(0)} & A_{m-1}^{(1)} & \cdots & A_{m-1}^{(s-m-1)} \end{pmatrix},$$

which we view as a matrix over $\mathbf{Z}$ by identifying F_p with the set $\{0, 1, \dots, p-1\}$ of integers. Then we define the $ks \times ks$ matrix

$$G^{(s)} = \begin{pmatrix} p^{-1}E_{km} & p^{-1}A^{(s)} \\ 0 & E_{k(s-m)} \end{pmatrix}$$

with rational entries, where E_r is the $r \times r$ identity matrix over $\mathbf{Z}$. Let $L^{(s)}$ be the lattice in $\mathbf{R}^{ks}$ with generator matrix $G^{(s)}$; that is, $L^{(s)}$ consists of all $\mathbf{Z}$-linear combinations of the row vectors of $G^{(s)}$.

Theorem 2. *Let* $\mathbf{u}_0, \mathbf{u}_1, \dots$ *be a sequence of* k*-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *If* $s > m$ *and the points* $\mathbf{v}_n$ *are given by* (4), *then we have*

$$\{\mathbf{0}, \mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{T-1}\} = L^{(s)} \cap [0, 1)^{ks},$$

where $L^{(s)}$ *is the lattice in* $\mathbf{R}^{ks}$ *with generator matrix* $G^{(s)}$.

Proof. We claim that for the row vectors $\mathbf{z}_n \in F_p^k$ we have

$$\mathbf{z}_{n+m+j} = \sum_{h=0}^{m-1} \mathbf{z}_{n+h} A_h^{(j)} \quad \text{for all } j \geq 0 \text{ and } n \geq 0. \tag{5}$$

This is proved by induction on j. For $j = 0$ this is just (1). If (5) is true for some $j \geq 0$, then by the induction hypothesis and (1) we get

$$\begin{aligned} \mathbf{z}_{n+m+j+1} &= \sum_{h=0}^{m-1} \mathbf{z}_{n+h+1} A_h^{(j)} = \sum_{h=0}^{m-2} \mathbf{z}_{n+h+1} A_h^{(j)} + \sum_{h=0}^{m-1} \mathbf{z}_{n+h} A_h A_{m-1}^{(j)} \\ &= \sum_{h=0}^{m-1} \mathbf{z}_{n+h} A_h^{(j+1)} \end{aligned}$$

for all $n \geq 0$, and so (5) is established. It follows that

$$\begin{aligned} \mathbf{v}_n &\equiv \frac{1}{p}(\mathbf{z}_n, \mathbf{z}_{n+1}, \dots, \mathbf{z}_{n+s-1}) \\ &\equiv (\mathbf{z}_n, \mathbf{z}_{n+1}, \dots, \mathbf{z}_{n+m-1}) \left(\frac{1}{p} E_{km} \; \frac{1}{p} A^{(s)} \right) \bmod \mathbf{Z}^{ks} \end{aligned}$$

for all $n \geq 0$. This shows that all $\mathbf{v}_n$, and also $\mathbf{0}$, belong to the lattice $L^{(s)}$; hence

$$\{\mathbf{0}, \mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{T-1}\} \subseteq L^{(s)} \cap [0, 1)^{ks}.$$

All standard basis vectors of $\mathbf{R}^{ks}$ lie in $L^{(s)}$, and so $\mathbf{Z}^{ks} \subseteq L^{(s)}$. Furthermore, $\det(L^{(s)}) := |\det(G^{(s)})| = p^{-km}$, and thus $L^{(s)} \cap [0, 1)^{ks}$ contains exactly p^{km} points by [16, Theorem 5.30]. On the other hand, the p^{km} points $\mathbf{0}, \mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{T-1}$ are distinct since $\operatorname{per}(\mathbf{u}_n) = T$, and so the desired result follows. □

We note that $\det(L^{(s)}) = p^{-km}$ is independent of s, so that pseudorandom vectors generated by the multiple-recursive matrix method have in a sense a "coarse" lattice structure, but the "coarseness" is much less pronounced than for the linear congruential method or the matrix method. The lattice $L^{(s)}$ can be used to assess the quality of the sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ of pseudorandom vectors. This is done by computing reduced bases, Beyer quotients, and other characteristics of $L^{(s)}$; we refer to completely analogous procedures for the linear congruential method (Ripley [20, Chapter 2]) and the matrix method (Afflerbach and Grothe [1]).

4. Performance under the serial test

The statistical independence of s successive pseudorandom vectors can be tested by the s-dimensional *serial test.* Given a sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ of k-

dimensional pseudorandom vectors, this test amounts to studying the distribution of the ks-dimensional points

$$(6) \qquad \mathbf{v}_n = (\mathbf{u}_n, \mathbf{u}_{n+1}, \dots, \mathbf{u}_{n+s-1}) \quad \text{for } n = 0, 1, \dots$$

in the unit cube $[0, 1]^{ks}$. We restrict attention to the case where $\mathbf{u}_0, \mathbf{u}_1, \dots$ is a sequence of k-dimensional pseudorandom vectors generated by (1) and (2) with $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. Note that then the points $\mathbf{v}_n$ are in the half-open unit cube $[0, 1)^{ks}$.

We first consider the s-dimensional serial test for the full period. For dimensions $s \le m$ the exact distribution of the points $\mathbf{v}_n$ in (6) from the full period can be determined.

Theorem 3. *Let* $\mathbf{u}_0, \mathbf{u}_1, \dots$ *be a sequence of k-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *If* $s \le m$, *then among the points* $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{T-1}$ *in* (6) *every nonzero point in* $[0, 1)^{ks}$ *all of whose coordinates are rationals with fixed denominator* p *occurs with frequency* $p^{k(m-s)}$, *and the point* $\mathbf{0} \in [0, 1)^{ks}$ *occurs with frequency* $p^{k(m-s)} - 1$.

Proof. For $s = m$ this was shown in [17, Remark 8], and for $s < m$ this follows by projecting the points $\mathbf{v}_n$ for $s = m$ to $[0, 1)^{ks}$ and counting. □

Theorem 3 demonstrates that for $s \le m$ the points $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{T-1}$ show an almost perfect equidistribution. In general, the distribution properties of the points $\mathbf{v}_n$ are measured by the notion of discrete discrepancy which was introduced in [18] and is defined below for the special case that is of interest to us.

Definition 2. Let p be a prime and let $d \ge 1$ be an arbitrary dimension. Let $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ be N points in $[0, 1)^d$ with the property that all their coordinates are rationals with fixed denominator p. Then the *discrete discrepancy* $E_{N,p}$ of the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ is defined by

$$E_{N,p} = E_{N,p}(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}) = \max \left| \frac{A(J)}{N} - \operatorname{Vol}(J) \right|,$$

where the maximum is taken over all subintervals of $[0, 1)^d$ of the form $J = \prod_{i=1}^{d} [a_i/p, b_i/p)$ with integers $0 \le a_i < b_i \le p$ for $1 \le i \le d$ and where $A(J)$ is the number of integers n with $0 \le n \le N - 1$ and $\mathbf{x}_n \in J$.

Now let $\mathbf{u}_0, \mathbf{u}_1, \dots$ be as above a sequence of k-dimensional pseudorandom vectors generated by (1) and (2) with $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. As explained in [18], natural quantities for the s-dimensional serial test are the discrete discrepancies

$$(7) \qquad E_{N,p}^{(s)} := E_{N,p}(\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{N-1}) \quad \text{for } 1 \le N \le T,$$

where the points $\mathbf{v}_n$ are given by (6). A principal theme of this and the following section will be the provision of upper and lower bounds for these discrepancies.

We need the following notation. Let $C(p) = (-p/2, p/2] \cap \mathbf{Z}$, and for a dimension $d \ge 1$ let $C_d(p)$ be the set of points $(h_1, \dots, h_d)$ with $h_i \in C(p)$ for $1 \le i \le d$ and define $C_d^*(p) = C_d(p) \backslash \{\mathbf{0}\}$. For $h \in C(p)$ we put

$$r(h, p) = \begin{cases} p \sin \dfrac{\pi |h|}{p} & \text{if } h \ne 0, \\ 1 & \text{if } h = 0. \end{cases}$$

For $\mathbf{h} = (h_1, \dots, h_d) \in C_d(p)$ we define

$$r(\mathbf{h}, p) = \prod_{i=1}^{d} r(h_i, p).$$

We write $\mathbf{x} \cdot \mathbf{y}$ for the standard inner product of $\mathbf{x}, \mathbf{y} \in \mathbf{R}^d$.

By Lemmas 2 and 3, we can characterize the parameters for generating $\mathbf{u}_0, \mathbf{u}_1, \dots$ in the case $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$ by a primitive element σ of F_q and an ordered basis $B = (\beta_1, \dots, \beta_k)$ of a σ-splitting F_p-linear subspace of F_q with $q = p^{km}$. Now let $s \geq 1$ be a given dimension. We write $\mathbf{h} \in C^*_{ks}(p)$ in the form $\mathbf{h} = (\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_s)$, where $\mathbf{h}_i \in C_k(p)$ for $1 \leq i \leq s$ and not all $\mathbf{h}_i = \mathbf{0}$. Furthermore, let

$$\mathbf{h}_i = (h_{i1}, \dots, h_{ik}) \quad \text{for } 1 \leq i \leq s, \tag{8}$$

where all $h_{ij} \in C(p)$. We write $Z^{(s)}(B, \sigma)$ for the set of all $\mathbf{h} = (\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_s) \in C^*_{ks}(p)$ which satisfy

$$\sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} \beta_j \sigma^{i-1} = 0.$$

Then we define

$$R^{(s)}(B, \sigma) = \sum_{\mathbf{h} \in Z^{(s)}(B, \sigma)} \frac{1}{r(\mathbf{h}, p)}. \tag{9}$$

Now we have the following bound for the discrete discrepancy $E^{(s)}_{T,p}$ in (7).

Theorem 4. *Let* $\mathbf{u}_0, \mathbf{u}_1, \dots$ *be a sequence of k-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *Then for* $s \geq 1$ *we have*

$$E^{(s)}_{T,p} \leq \frac{1}{T} + \left(1 + \frac{1}{T}\right) R^{(s)}(B, \sigma).$$

Proof. Let the points $\mathbf{v}_0, \dots, \mathbf{v}_{T-1} \in [0, 1)^{ks}$ be as in (6) and put

$$E^{(s)}_{T+1,p} = E_{T+1,p}(\mathbf{v}_0, \dots, \mathbf{v}_{T-1}, \mathbf{0}).$$

Then by [18, Lemma 1], and by setting $\mathbf{v}_T = \mathbf{0}$, we get

$$E^{(s)}_{T+1,p} \leq \sum_{\mathbf{h} \in C^*_{ks}(p)} \frac{1}{r(\mathbf{h}, p)} \left| \frac{1}{T+1} \sum_{n=0}^{T} e(\mathbf{h} \cdot \mathbf{v}_n) \right|, \tag{10}$$

where $e(t) = e^{2\pi\sqrt{-1}t}$ for real t. For fixed $\mathbf{h} \in C^*_{ks}(p)$ consider

$$S(\mathbf{h}) := \sum_{n=0}^{T} e(\mathbf{h} \cdot \mathbf{v}_n).$$

As above, we write $\mathbf{h} = (\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_s)$ with $\mathbf{h}_i \in C_k(p)$ for $1 \leq i \leq s$. Then

$$\begin{aligned} S(\mathbf{h}) &= 1 + \sum_{n=0}^{T-1} e(\mathbf{h} \cdot \mathbf{v}_n) = 1 + \sum_{n=0}^{T-1} e\left(\sum_{i=1}^{s} \mathbf{h}_i \cdot \mathbf{u}_{n+i-1}\right) \\ &= 1 + \sum_{n=0}^{T-1} e\left(\frac{1}{p} \sum_{i=1}^{s} \mathbf{h}_i \cdot \mathbf{z}_{n+i-1}\right). \end{aligned}$$

By writing each $\mathbf{h}_i$ as in (8) and using (3), we get

$$\begin{aligned} S(\mathbf{h}) &= 1 + \sum_{n=0}^{T-1} e\left(\frac{1}{p}\sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\operatorname{Tr}(\beta_j\sigma^{n+i-1})\right) \\ &= 1 + \sum_{n=0}^{T-1} e\left(\frac{1}{p}\operatorname{Tr}\left(\sigma^n \sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\beta_j\sigma^{i-1}\right)\right), \end{aligned}$$

where Tr is the trace function from F_q to F_p with $q = p^{km}$. We note that $\chi(\alpha) = e(\frac{1}{p}\operatorname{Tr}(\alpha))$ for $\alpha \in F_q$ defines the canonical additive character of F_q (compare with [9, p. 190]). Since σ is a primitive element of F_q, the powers σ^n, $0 \le n \le T-1$, run through the set F_q^* of nonzero elements of F_q, and so

$$\begin{aligned} S(\mathbf{h}) &= 1 + \sum_{\gamma\in F_q^*} \chi\left(\gamma \sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\beta_j\sigma^{i-1}\right) \\ &= \sum_{\gamma\in F_q} \chi\left(\gamma \sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\beta_j\sigma^{i-1}\right). \end{aligned}$$

From the orthogonality relations for additive characters [9, p. 192], we obtain that $S(\mathbf{h}) = q = T+1$ if $\mathbf{h} \in Z^{(s)}(B, \sigma)$ and $S(\mathbf{h}) = 0$ otherwise. In view of (10) and the definition of $R^{(s)}(B, \sigma)$ in (9) we then get

$$E_{T+1,p}^{(s)} \le R^{(s)}(B, \sigma).$$

Since $E_{T,p}^{(s)}$ is the discrete discrepancy of the point set that is obtained from the point set $\mathbf{v}_0, \dots, \mathbf{v}_{T-1}, \mathbf{0}$ by deleting $\mathbf{0}$, it is easy to see (compare with the proof of [16, Theorem 7.3]) that

$$TE_{T,p}^{(s)} \le 1 + (T+1)E_{T+1,p}^{(s)},$$

which implies the result of the theorem. □

Note that $R^{(s)}(B, \sigma) = 0$ for $s \le m$ since the sum in (9) is then empty on account of the basis property in Lemma 2. Now we consider the discrete discrepancies $E_{N,p}^{(s)}$ in (7) for $1 \le N < T$, i.e., for parts of the period.

Theorem 5. *Let $\mathbf{u}_0, \mathbf{u}_1, \dots$ be a sequence of k-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *Then for $s \ge 1$ and $1 \le N < T$ we have*

$$E_{N,p}^{(s)} < \left(\frac{p^{km/2}}{N}\left(\frac{4}{\pi^2}\log T + 0.41 + \frac{0.61}{T}\right) + \frac{1}{T}\right)\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^{ks} + R^{(s)}(B, \sigma).$$

Proof. We basically follow the method in the proof of Theorem 4. First of all, by [18, Lemma 1] we get

$$E_{N,p}^{(s)} \le \sum_{\mathbf{h}\in C_{ks}^*(p)} \frac{1}{r(\mathbf{h}, p)}\left|\frac{1}{N}\sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{v}_n)\right|. \tag{11}$$

For fixed $\mathbf{h} \in C_{ks}^*(p)$ we obtain

$$\begin{aligned} S_N(\mathbf{h}) &:= \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{v}_n) = \sum_{n=0}^{N-1} e\left(\frac{1}{p}\operatorname{Tr}\left(\sigma^n \sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\beta_j\sigma^{i-1}\right)\right) \\ &= \sum_{n=0}^{N-1} \chi\left(\sigma^n \sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\beta_j\sigma^{i-1}\right). \end{aligned}$$

Thus, if $\mathbf{h} \in Z^{(s)}(B, \sigma)$, then $S_N(\mathbf{h}) = N$. If $\mathbf{h} \notin Z^{(s)}(B, \sigma)$, then by [13, Lemma 3] and the fact that σ is a primitive element of F_q we have

$$|S_N(\mathbf{h})| < p^{km/2}\left(\frac{4}{\pi^2}\log T + 0.41 + \frac{0.61}{T}\right) + \frac{N}{T}.$$

By combining this information with (11), we deduce that

$$E_{N,p}^{(s)} \le R^{(s)}(B, \sigma) + \left(\frac{p^{km/2}}{N}\left(\frac{4}{\pi^2}\log T + 0.41 + \frac{0.61}{T}\right) + \frac{1}{T}\right) \sum_{\mathbf{h}\in C_{ks}^*(p)} \frac{1}{r(\mathbf{h}, p)}.$$

It remains to note that

$$\sum_{\mathbf{h}\in C_{ks}^*(p)} \frac{1}{r(\mathbf{h}, p)} < \left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^{ks} \tag{12}$$

by [11, Lemma 2.3]. □

The following result provides information on how small we can make the quantity $R^{(s)}(B, \sigma)$ defined in (9). Since $R^{(s)}(B, \sigma) = 0$ for $s \le m$, we can assume $s > m$.

Theorem 6. *Let $m < s \le km$. Furthermore, let σ be a primitive element of F_q with $q = p^{km}$, let W be a σ-splitting F_p-linear subspace of F_q of dimension k, and let $\mathscr{B}$ be the set of all ordered bases of W. Then for the mean value*

$$R := \frac{1}{\operatorname{card}(\mathscr{B})} \sum_{B\in\mathscr{B}} R^{(s)}(B, \sigma)$$

of $R^{(s)}(B, \sigma)$ over $\mathscr{B}$ we have

$$R < \frac{p}{p-1}p^{-k}\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^{ks}.$$

Proof. From (9) we get

$$R = \frac{1}{\operatorname{card}(\mathscr{B})} \sum_{B\in\mathscr{B}} \sum_{\mathbf{h}\in Z^{(s)}(B,\sigma)} \frac{1}{r(\mathbf{h}, p)} = \frac{1}{\operatorname{card}(\mathscr{B})} \sum_{\mathbf{h}\in C_{ks}^*(p)} \frac{1}{r(\mathbf{h}, p)} \sum_{\substack{B\in\mathscr{B} \\ \mathbf{h}\in Z^{(s)}(B,\sigma)}} 1.$$

If we fix an $\mathbf{h} \in C_{ks}^*(p)$ and write it in the same way as prior to (9), then the inner sum above is equal to the number of $B = (\beta_1, \dots, \beta_k) \in \mathscr{B}$ with

$$\sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\beta_j\sigma^{i-1} = 0.$$

If we put $\alpha_j = \sum_{i=1}^{s} h_{ij}\sigma^{i-1}$ for $1 \le j \le k$, then this condition can be written as

$$\sum_{j=1}^{k} \alpha_j \beta_j = 0.$$

Since $s \le km$, the powers σ^{i-1}, $1 \le i \le s$, are linearly independent over F_p, and so $\alpha_j \ne 0$ for at least one j with $1 \le j \le k$. It follows that

$$\sum_{\substack{B \in \mathscr{B} \\ \mathbf{h} \in Z^{(s)}(B,\sigma)}} 1 \le \prod_{l=0}^{k-2} (p^k - p^l).$$

Since

$$\operatorname{card}(\mathscr{B}) = \prod_{l=0}^{k-1} (p^k - p^l),$$

we obtain

$$R \le \frac{1}{p^k - p^{k-1}} \sum_{\mathbf{h} \in C_{ks}^*(p)} \frac{1}{r(\mathbf{h}, p)} < \frac{p}{p-1} p^{-k} \left(\frac{2}{\pi} \log p + \frac{7}{5} \right)^{ks},$$

where we applied (12) in the last step. □

Corollary 1. *Let $m < s \le km$, let σ be a primitive element of F_q with $q = p^{km}$, and let W be a σ-splitting F_p-linear subspace of F_q of dimension k. Then for the corresponding sequences $\mathbf{u}_0, \mathbf{u}_1, \dots$ with $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$ we have on the average*

$$E_{T,p}^{(s)} = O(p^{-k} (\log p)^{ks})$$

with an implied constant depending only on k and s, where the average is taken over all ordered bases of W.

Proof. This follows from Theorems 4 and 6. □

Corollary 2. *Let $m < s \le km$ and let σ and W be as in Corollary 1. Then for the corresponding sequences $\mathbf{u}_0, \mathbf{u}_1, \dots$ with $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$ we have on the average*

$$E_{N,p}^{(s)} = O(p^{-k} (\log p)^{ks} + N^{-1} p^{km/2} (\log T)(\log p)^{ks})$$

for $1 \le N < T$ with an implied constant depending only on k and s, where the average is taken over all ordered bases of W.

Proof. This follows from Theorems 5 and 6. □

5. Figures of merit

In analogy with the theory for the matrix method (see [13]), we introduce a "figure of merit" which is a positive integer assessing the suitability of parameters in the multiple-recursive matrix method. We again restrict attention to the case where $\mathbf{u}_0, \mathbf{u}_1, \dots$ is a sequence of k-dimensional pseudorandom vectors generated by (1) and (2) with $\operatorname{per}(\mathbf{u}_n) = p^{km} - 1$. As we have seen in Lemmas

2 and 3, the sequence can then be described in terms of a primitive element σ of F_q and an ordered basis $B = (\beta_1, \dots, \beta_k)$ of a σ-splitting F_p-linear subspace of F_q with $q = p^{km}$. We define the subset $Z^{(s)}(B, \sigma)$ of $C^*_{ks}(p)$ as in §4. Furthermore, we put $r(h) = \max(1, |h|)$ for $h \in \mathbf{Z}$, and for a dimension $d \geq 1$ we define

$$r(\mathbf{h}) = \prod_{i=1}^{d} r(h_i) \quad \text{for } \mathbf{h} = (h_1, \dots, h_d) \in \mathbf{Z}^d.$$

Definition 3. Let σ be a primitive element of F_q with $q = p^{km}$ and let B be an ordered basis of a σ-splitting F_p-linear subspace of F_q of dimension k. Then for $s > m$ we define the *figure of merit*

$$\varrho^{(s)}(B, \sigma) = \min_{\mathbf{h} \in Z^{(s)}(B, \sigma)} r(2\mathbf{h}).$$

Theorem 7. *For any σ and B as in Definition* 3 *and for any $s > m$ we have*

$$2 \leq \varrho^{(s)}(B, \sigma) \leq 2p^{km}.$$

Proof. The lower bound is trivial. To prove the upper bound, let $B = (\beta_1, \dots, \beta_k)$ and note that $\beta_j \sigma^{i-1}$, $1 \leq i \leq m$, $1 \leq j \leq k$, form a basis of F_q over F_p by the definition of a σ-splitting F_p-linear subspace of F_q. Thus,

$$\beta_1 \sigma^m = \sum_{i=1}^{m} \sum_{j=1}^{k} b_{ij} \beta_j \sigma^{i-1}$$

with suitable $b_{ij} \in F_p$. We can rewrite this identity in the form

$$\sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} \beta_j \sigma^{i-1} = 0,$$

where each integer h_{ij} is reduced modulo p so that it lies in $(-p/2, p/2]$. Then the corresponding $\mathbf{h} \in C^*_{ks}(p)$ belongs to $Z^{(s)}(B, \sigma)$ and satisfies $r(2\mathbf{h}) \leq 2p^{km}$. □

It is an important fact that the quantity $R^{(s)}(B, \sigma)$ defined in (9) can be bounded in terms of the figure of merit $\varrho^{(s)}(B, \sigma)$.

Theorem 8. *For any σ and B as in Definition* 3 *and for any $s > m$ we have*

$$\frac{(2/\pi)^{ks}}{\varrho^{(s)}(B, \sigma)} \leq R^{(s)}(B, \sigma) < \frac{(2\log 2p)^{ks} + 3(2\log 2p)^{ks-1}}{(\log 2)^{ks-1} \varrho^{(s)}(B, \sigma)}.$$

Proof. A comparison of the definitions shows that

$$r(h, p) \leq \frac{\pi}{2} r(2h) \quad \text{for all } h \in C(p),$$

and so

$$r(\mathbf{h}, p) \leq \left(\frac{\pi}{2}\right)^{ks} r(2\mathbf{h}) \quad \text{for all } \mathbf{h} \in C_{ks}(p).$$

By Definition 3 there exists an $\mathbf{h}_0 \in Z^{(s)}(B, \sigma)$ with $r(2\mathbf{h}_0) = \varrho^{(s)}(B, \sigma)$. Then

$$R^{(s)}(B, \sigma) \geq \frac{1}{r(\mathbf{h}_0, p)} \geq \frac{(2/\pi)^{ks}}{r(2\mathbf{h}_0)} = \frac{(2/\pi)^{ks}}{\varrho^{(s)}(B, \sigma)},$$

which is the lower bound in the theorem. To prove the upper bound, we proceed as in the proof of [12, Theorem 5.2], but we replace the dimension s there by ks and the integer m by the prime p. The crucial (but simple) fact that needs to be used in the key steps of the argument (which go back to [11, pp. 117–118]) is the following: if $\mathbf{h}, \mathbf{h}' \in Z^{(s)}(B, \sigma)$, then $\mathbf{h} - \mathbf{h}'$ is congruent mod p to an element of $Z^{(s)}(B, \sigma)$. □

Corollary 3. *Let* $\mathbf{u}_0, \mathbf{u}_1, \ldots$ *be a sequence of k-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *Then for* $s > m$ *we have*

$$E_{T,p}^{(s)} \leq \frac{c_1(\log p)^{ks}}{\varrho^{(s)}(B, \sigma)},$$

where the constant $c_1 > 0$ *depends only on* k *and* s.

Proof. This follows from Theorem 4 and the upper bounds in Theorems 7 and 8. □

Corollary 4. *Let* $\mathbf{u}_0, \mathbf{u}_1, \ldots$ *be a sequence of k-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *Then for* $s > m$ *and* $1 \leq N < T$ *we have*

$$E_{N,p}^{(s)} \leq \frac{c_2}{N} p^{km/2} (\log T)(\log p)^{ks} + \frac{c_3(\log p)^{ks}}{\varrho^{(s)}(B, \sigma)},$$

where the constants $c_2 > 0$ *and* $c_3 > 0$ *depend only on* k *and* s.

Proof. This follows from Theorem 5 and the upper bound in Theorem 8. □

Corollaries 3 and 4 provide upper bounds for the discrete discrepancies $E_{N,p}^{(s)}$, $1 \leq N \leq T$, in terms of the figure of merit $\varrho^{(s)}(B, \sigma)$. In the following we establish a lower bound for these discrete discrepancies in terms of $\varrho^{(s)}(B, \sigma)$.

Theorem 9. *Let* $\mathbf{u}_0, \mathbf{u}_1, \ldots$ *be a sequence of k-dimensional pseudorandom vectors generated by* (1) *and* (2) *with* $\operatorname{per}(\mathbf{u}_n) = T = p^{km} - 1$. *Then for* $s > m$ *and* $1 \leq N \leq T$ *we have*

$$E_{N,p}^{(s)} \geq \frac{\pi}{2(\pi + \frac{1}{2})^{ks} \varrho^{(s)}(B, \sigma)}.$$

Proof. By [18, Lemma 3] we have

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{v}_n) \right| \leq \frac{2}{\pi} \left(\prod_{i=1}^{ks} (2\pi |h_i| + 1) - 1 \right) N E_{N,p}^{(s)}$$

for any $\mathbf{h} = (h_1, \ldots, h_{ks}) \in \mathbf{Z}^{ks}$ for which not all coordinates are divisible by p, where $e(t) = e^{2\pi\sqrt{-1}t}$ for real t. Now

$$2\pi|h| + 1 \leq \left(\pi + \tfrac{1}{2}\right) r(2h)$$

for all integers h, and so

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{v}_n) \right| \leq \frac{2}{\pi} \left(\pi + \tfrac{1}{2}\right)^{ks} r(2\mathbf{h}) N E_{N,p}^{(s)}. \tag{13}$$

By Definition 3 there exists an $\mathbf{h}_0 \in Z^{(s)}(B, \sigma)$ with $r(2\mathbf{h}_0) = \varrho^{(s)}(B, \sigma)$. The proof of Theorem 5 shows that

$$\sum_{n=0}^{N-1} e(\mathbf{h}_0 \cdot \mathbf{v}_n) = N,$$

and together with (13) this yields the desired result. □

The bounds in Corollaries 3 and 4 and Theorem 9 demonstrate that $\varrho^{(s)}(B, \sigma)$ has to be large to guarantee small discrete discrepancies. The following result shows how large we can make the figure of merit.

Theorem 10. *Let $m < s \leq km$. Then there exists an effective constant $d(k, s) > 0$ depending only on k and s such that the following holds: if $p^{k-1}(p-1) \geq d(k, s)$, then for every primitive element σ of F_q with $q = p^{km}$ and every σ-splitting F_p-linear subspace W of F_q of dimension k there exists an ordered basis B of W such that*

$$\varrho^{(s)}(B, \sigma) > \frac{2a}{(\log a)^{ks-1}} \quad \textit{with } a = \frac{p^{k-1}(p-1)}{2b},$$

where $b > 0$ is an effective absolute constant.

Proof. In addition to k, m, and s we fix σ and W and let $\mathscr{B}$ be the set of all ordered bases of W. For real $t > 2$ let $Q(t)$ be the number of $B \in \mathscr{B}$ with $\varrho^{(s)}(B, \sigma) \leq t$, i.e., such that there exists an $\mathbf{h} \in Z^{(s)}(B, \sigma)$ with $r(2\mathbf{h}) \leq t$. In the proof of Theorem 6 we have shown that for a fixed $\mathbf{h} \in C_{ks}^*(p)$ the number of $B \in \mathscr{B}$ with $\mathbf{h} \in Z^{(s)}(B, \sigma)$ is at most $\prod_{l=0}^{k-2}(p^k - p^l)$. It follows that

$$Q(t) \leq G_{ks}(t) \prod_{l=0}^{k-2}(p^k - p^l), \tag{14}$$

where $G_{ks}(t)$ is the number of nonzero $\mathbf{h} \in \mathbf{Z}^{ks}$ with $r(2\mathbf{h}) \leq t$. Furthermore, by [13, equation (16)] we have

$$G_{ks}(t) \leq bt\left(\log \frac{t}{2}\right)^{ks-1} \quad \text{for } t \geq 2e^4 \tag{15}$$

with an effective absolute constant $b > 0$. Since $\lim_{u \to \infty} u/(\log u)^{ks-1} = \infty$, there exists $c(k, s) > 0$ such that

$$\frac{u}{(\log u)^{ks-1}} \geq e^4 \quad \text{for all } u \geq c(k, s). \tag{16}$$

Put $d(k, s) = 2bc(k, s)$, let a be as in the theorem, and set

$$t_0 = \frac{2a}{(\log a)^{ks-1}}.$$

Now assume that $p^{k-1}(p-1) \geq d(k, s)$. Then $a \geq c(k, s)$, thus (16) implies $t_0 \geq 2e^4$, and so (15) yields

$$\begin{aligned} G_{ks}(t_0) &\leq bt_0\left(\log \frac{t_0}{2}\right)^{ks-1} = \frac{2ab}{(\log a)^{ks-1}}\left(\log \frac{a}{(\log a)^{ks-1}}\right)^{ks-1} \\ &< 2ab = p^{k-1}(p-1), \end{aligned}$$

since (16) shows that $a \geq c(k, s) > e$. Then (14) yields

$$Q(t_0) < \prod_{l=0}^{k-1} (p^k - p^l).$$

Since the number on the right-hand side is the cardinality of $\mathscr{B}$, it follows that there exists a $B \in \mathscr{B}$ not counted by $Q(t_0)$, and so for this B we have $\varrho^{(s)}(B, \sigma) > t_0$. □

6. Discussion

The multiple-recursive matrix method generates k-dimensional pseudorandom vectors $\mathbf{u}_0, \mathbf{u}_1, \ldots$ by an mth-order vector recursion in F_p^k. It extends the matrix method for pseudorandom vector generation, which corresponds to the case $m = 1$. For any p, k, and m we can achieve least period length $\operatorname{per}(\mathbf{u}_n) = p^{km} - 1$ by a suitable choice of parameters in the multiple-recursive matrix method, and explicit criteria can be given for this choice of parameters (see §2). For fixed p and k we can thus obtain arbitrarily large least period lengths by choosing sufficiently large values of m.

For dimensions $s > m$ the nontrivial lattice structure inherent in pseudorandom vectors generated by the multiple-recursive matrix method is described in Theorem 2. In this connection, it would be of interest to carry out computational work on the assessment of the lattices $L^{(s)}$ in Theorem 2. Analogous work for the linear congruential method and the matrix method is mentioned in §3.

The results of our analysis of the serial test for the case $\operatorname{per}(\mathbf{u}_n) = p^{km} - 1$ can be summarized as follows. For dimensions $s \leq m$ the corresponding s-tuples $\mathbf{v}_n$ of successive pseudorandom vectors are almost equidistributed over the full period. For dimensions $s > m$ the order of magnitude of the discrete discrepancy of these s-tuples is controlled by the figure of merit $\varrho^{(s)}(B, \sigma)$, with large values of $\varrho^{(s)}(B, \sigma)$ corresponding to small values of the discrete discrepancy. If $m < s \leq km$, then with a suitable choice of an ordered basis B of a given σ-splitting F_p-linear subspace W of F_q (with $q = p^{km}$) of dimension k, a good performance under the s-dimensional serial test can be guaranteed. In this context we point out an interesting open problem, namely that of determining, say for a primitive element σ of F_q, the total number of σ-splitting F_p-linear subspaces of F_q of given dimension k. A related task is that of studying the average performance under the serial test if one averages over all these subspaces W.

Future research on the multiple-recursive matrix method will also have to deal with figures of merit from the computational point of view. It would be useful to develop efficient algorithms for the calculation of figures of merit and to search for concrete parameters possessing a large figure of merit.

Bibliography

1. L. Afflerbach and H. Grothe, *The lattice structure of pseudo-random vectors generated by matrix generators*, J. Comput. Appl. Math. **23** (1988), 127–131.

2. S. L. Anderson, *Random number generators on vector supercomputers and other advanced architectures*, SIAM Rev. **32** (1990), 221–251.

3. V. C. Bhavsar and J. R. Isaac, *Design and analysis of parallel Monte Carlo algorithms*, SIAM J. Sci. Statist. Comput. **8** (1987), s73–s95.

4. W. F. Eddy, *Random number generators for parallel processors*, J. Comput. Appl. Math. **31** (1990), 63–71.

5. J. Eichenauer and J. Lehn, *A non-linear congruential pseudo random number generator*, Statist. Papers **27** (1986), 315–326.

6. D. E. Knuth, *The art of computer programming*, Vol. 2: *Seminumerical algorithms*, 2nd ed., Addison-Wesley, Reading, MA, 1981.

7. P. L'Ecuyer, *Random numbers for simulation*, Comm. ACM **33** (1990), no. 10, 85–97.

8. ——, *Uniform random number generation*, Ann. Oper. Res. (to appear).

9. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge University Press, Cambridge.)

10. M. Matsumoto and Y. Kurita, *Twisted GFSR generators*, ACM Trans. Modeling Comput. Simulation **2** (1992), 179–194.

11. H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Adv. Math. **26** (1977), 99–181.

12. ——, *The serial test for pseudo-random numbers generated by the linear congruential method*, Numer. Math. **46** (1985), 51–68.

13. ——, *Statistical independence properties of pseudorandom vectors produced by matrix generators*, J. Comput. Appl. Math. **31** (1990), 139–151.

14. ——, *Finite fields and their applications*, Contributions to General Algebra (Vienna, 1990), vol. 7, Teubner, Stuttgart, 1991, pp. 251–264.

15. ——, *Nonlinear methods for pseudorandom number and vector generation*, Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. Math. Systems, vol. 374, Springer, Berlin, 1992, pp. 145–153.

16. ——, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992.

17. ——, *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. **192** (1993), 301–328.

18. ——, *Pseudorandom vector generation by the inversive method*, ACM Trans. Modeling Comput. Simulation (to appear).

19. ——, *The multiple-recursive matrix method for pseudorandom number generation*, Finite Fields Appl. (to appear).

20. B. D. Ripley, *Stochastic simulation*, Wiley, New York, 1987.

Institute for Information Processing, Austrian Academy of Sciences, Sonnenfelsgasse 19, A-1010 Vienna, Austria
E-mail address: nied@qiinfo.oeaw.ac.at