COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
60. SETS, GRAPHS AND NUMBERS, BUDAPEST (HUNGARY), 1991

Constructions of Low-Discrepancy Point Sets and Sequences

H. NIEDERREITER

1. Introduction

The discrepancy is a well-known measure for the irregularity of distribution of a finite point set or of an infinite sequence. We consider point sets and sequences in the standard setting of discrepancy theory, namely when their elements belong to an s-dimensional unit cube, and we put particular emphasis on the multidimensional case $s \geq 2$. The construction of point sets and sequences with small discrepancy is a classical problem of number theory which, not surprisingly, also has a certain combinatorial flavor. Furthermore, such constructions are of great interest for various areas in which discrepancy theory can be applied. We will briefly discuss such applications later on.

There have been major developments recently in the theory and the applications of discrepancy, for instance the initiation of a general theory of nets and (t, s)-sequences and new methods of constructing point sets and sequences with small discrepancy. Our aim in this paper is to survey those developments connected with constructions of point sets and sequences with small discrepancy and also to present some related new results. For the sake of background we also review classical constructions of point sets and sequences with small discrepancy.

Let P be the point set consisting of the N points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1} \in I^s := [0,1)^s, s \geq 1$. Here "point set" means the same as "multiset" in combinatorics, i.e., a set in which the multiplicity of elements is taken into account. For a subinterval J of I^s we define the counting function $A(J;P)$ as the number of integers n with $0 \leq n \leq N-1$ and $\mathbf{x}_n \in J$. Furthermore, we introduce the *remainder function*

$$R(J;P) = \frac{A(J;P)}{N} - \mathrm{Vol}(J).$$

For $\mathbf{t} = (t_1, \ldots, t_s) \in \bar{I}^s := [0,1]^s$ let $[\mathbf{0}, \mathbf{t})$ be the interval $\prod_{i=1}^{s} [0, t_i)$.

Definition 1. *The* (star) discrepancy *of the point set P is defined by*

$$D_N^* = D_N^*(P) = \sup_{\mathbf{t} \in \bar{I}^s} |R([\mathbf{0}, \mathbf{t}); P)|.$$

For a sequence S of elements of I^s we define $D_N^* = D_N^*(S)$ to be the (star) discrepancy of the point set consisting of the first N terms of S.

Informally, a point set P is called a *low-discrepancy point set* if $D_N^*(P)$ is small, where N is the given number of points in P. A sequence S is called a *low-discrepancy sequence* if $D_N^*(S)$ is small for all $N \geq 1$. In the s-dimensional case, "small" is usually interpreted to mean $O(N^{-1}(\log N)^s)$.

A rather well-known application of the discrepancy occurs in numerical integration. Detailed expositions of this application are available in the book of Hua and Wang [13] and in the survey articles of Niederreiter [19], [26]. An up-to-date account will be given in a forthcoming book of the author [30]. The discrepancy can also be applied to related problems in numerical analysis, such as the approximate solution of integral equations [13, Ch. 10] and the approximate solution of difficult integro-differential equations [16]. The discrepancy plays an important role in the theoretical analysis of the statistical properties of pseudorandom numbers generated by various number-theoretic methods; see [19] and the more recent papers [27], [29]. Interesting connections between discrepancy and the combinatorial theory of irregularities of partitions have been highlighted in the excellent survey article of Sós [37]; see also Beck [1] and the proceedings volume [10]. The recent solution of Tarski's circle-squaring problem by Laczkovich [15] depends on some remarkable and imaginative applications of discrepancy theory. Niederreiter and Schnorr [31] have employed the discrepancy in an

analysis of random bit and random function generators of cryptological significance. The L^2 discrepancy of a point set P, which is defined as the L^2 norm of $R([\mathbf{0},\mathbf{t});P)$ as a function of $\mathbf{t} \in \bar{I}^s$, is of crucial importance in the work of Woźniakowski [39] on the average-case complexity of multidimensional numerical integration for continuous functions.

2. Classical constructions

In the one-dimensional case it is easy to determine, for every given $N \geq 1$, the minimum value of $D_N^*(P)$ among all N-element point sets P. It suffices to apply a well-known explicit formula for the one-dimensional discrepancy $D_N^*(P)$ (see [14, p.91, Theorem 1.4]), from which it follows that the minimum value of $D_N^*(P)$ is $1/(2N)$ and that this minimum value is attained for $x_n = (2n+1)/(2N), n = 0, 1, \ldots, N-1$.

For sequences we have the phenomenon of *irregularities of distribution* which already appears in the one-dimensional case. As Schmidt [34] has shown, for any sequence S of elements of $[0,1)$ we have

$$D_N^*(S) \geq cN^{-1} \log N \quad \text{for infinitely many } N,$$

where $c > 0$ is an absolute constant. This result is best possible since $D_N^*(S) = O(N^{-1} \log N)$ can be achieved for several types of sequences S.

A classical example is given by the *van der Corput sequence* $x_n = \phi_2(n)$ for $n = 0, 1, \ldots$, where ϕ_2 is the radical-inverse function in base 2. In general, for an integer $b \geq 2$ let

$$n = \sum_{r=0}^{\infty} a_r(n) b^r \quad \text{for} \quad n \geq 0 \tag{1}$$

be the digit expansion of n in base b, where $a_r(n) \in Z_b := \{0, 1, \ldots, b-1\}$ for $r \geq 0$ and $a_r(n) = 0$ for all sufficiently large r. Then the radical-inverse function ϕ_b in base b is defined by

$$\phi_b(n) = \sum_{r=0}^{\infty} a_r(n) b^{-r-1} \quad \text{for} \quad n \geq 0.$$

The best bound for the discrepancy of the van der Corput sequence S is that of Béjian and Faure [4], namely

$$ND_N^*(S) \le \frac{\log N}{\log 8} + 1 \quad \text{for all} \quad N \ge 1.$$

The factor $1/(\log 8)$ is best possible. Even smaller discrepancies have been obtained by using generalized van der Corput sequences, but since our main interest is in the multidimensional case, we will not pursue this further.

Other one-dimensional low-discrepancy sequences arise from considering multiples of irrationals mod 1. For an irrational α let $S(\alpha)$ be the sequence $x_n = \{n\alpha\}$ for $n = 0, 1, \ldots$, where $\{u\}$ is the fractional part of the real number u. Let $\alpha = [a_0; a_1, a_2, \ldots]$ be the continued fraction expansion of α. If the partial quotients a_j satisfy $\sum_{j=1}^{m} a_j = O(m)$, then $D_N^*(S(\alpha)) = O(N^{-1} \log N)$. Detailed studies of the discrepancy of the sequences $S(\alpha)$ have been carried out in recent years by Dupain and Sós [8], Schoißengeier [35], and Sós [38], among others.

There are various ways of extending the definition of the van der Corput sequence to the multidimensional case $s \ge 2$. Historically, the first interesting extension was given by Halton [11]. In this construction we choose s pairwise relatively prime bases $b_1, \ldots, b_s$ and define the *Halton sequence*

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n)) \in I^s \quad \text{for} \quad n = 0, 1, \ldots.$$

This sequence S satisfies $D_N^*(S) = O(N^{-1}(\log N)^s)$, where the implied constant depends on $b_1, \ldots, b_s$. The choice of bases which minimizes the value of the implied constant is obtained by letting $b_1, \ldots, b_s$ be the first s primes. With this choice we have

$$D_N^*(S) \le A_s N^{-1} (\log N)^s + O(N^{-1} (\log N)^{s-1}) \quad \text{for} \quad N \ge 2, \qquad (2)$$

where the constant A_s depends only on s, but increases superexponentially as $s \to \infty$. An improved construction was given by Sobol' [36] who obtained sequences S satisfying (2) with smaller constants A_s which still increase superexponentially as $s \to \infty$. A breakthrough was achieved by Faure [9] who constructed sequences S satisfying (2) with constants A_s for which $\lim_{s \to \infty} A_s = 0$. The construction of Faure is a special case of a construction which will be described in Section 3.

The following general principle can be used to derive low-discrepancy point sets from low-discrepancy sequences. For $s \geq 2$ let S be the sequence of points $\mathbf{x}_0, \mathbf{x}_1, \ldots$ in I^{s-1}. For given $N \geq 1$ let P be the point set consisting of the N points

$$\left(\frac{n}{N}, \mathbf{x}_n\right) \in I^s \quad \text{for} \quad n = 0, 1, \ldots, N-1.$$

Then it is easily seen (see e.g. [24, Lemma 8.9]) that

$$ND_N^*(P) \leq \max_{1 \leq M \leq N} MD_M^*(S) + 1. \tag{3}$$

If this principle is applied to a Halton sequence, then we obtain the *Hammersley point set*

$$\mathbf{x}_n = \left(\frac{n}{N}, \phi_{b_1}(n), \ldots, \phi_{b_{s-1}}(n)\right) \in I^s \quad \text{for} \quad n = 0, 1, \ldots, N-1,$$

where the bases $b_1, \ldots, b_{s-1}$ are pairwise relatively prime. It follows from (2) and (3) that this point set P satisfies $D_N^*(P) = O(N^{-1}(\log N)^{s-1})$.

There are obvious multidimensional analogs of the one-dimensional sequences $S(\alpha)$ introduced above, namely sequences which consist of the multiples of an irrational point mod 1. However, for these sequences it has not yet been possible to obtain a discrepancy of the order $O(N^{-1}(\log N)^s)$ in dimension $s \geq 2$. A more promising line of research has dealt with discrete versions of these sequences, i.e., point sets consisting of the multiples of a rational point mod 1. For $N \geq 2$ and $\mathbf{g} \in \mathbb{Z}^s$ such a point set P comprises the points $\mathbf{x}_n = \{(n/N)\mathbf{g}\}, n = 0, 1, \ldots, N-1$, where $\{\mathbf{u}\}$ is the fractional part of $\mathbf{u} \in \mathbb{R}^s$. It is known that for every $s \geq 2$ and $N \geq 2$ there exists a $\mathbf{g} \in \mathbb{Z}^s$ such that $D_N^*(P) = O(N^{-1}(\log N)^s)$. The best implied constants have been given in Niederreiter [20] for N prime and in Niederreiter [21] for general N. A generalization of these types of low-discrepancy point sets was studied by Niederreiter and Sloan [32].

It is a widely held belief that the orders of magnitude $N^{-1}(\log N)^{s-1}$ for the discrepancy of point sets and $N^{-1}(\log N)^s$ for the discrepancy of sequences in the s-dimensional case are best possible. As mentioned earlier, this has been established for $s = 1$. For $s = 2$ Schmidt [34] has shown that for any N-element point set P we have

$$D_N^*(P) \geq cN^{-1} \log N,$$

and more recently Beck [2] proved that for any sequence S we have

$$D_N^*(S) \geq cN^{-1}(\log N)(\log\log N)^{c'} \quad \text{for infinitely many } N,$$

where c and c' are positive absolute constants. The paper of Beck [2] also contains the result that for any N-element point set P in the case $s = 3$ we have

$$D_N^*(P) \geq cN^{-1}(\log N)(\log\log N)^{c'}.$$

For arbitrary s there are the classical lower bounds of Roth [33]: for any N-element point set P we have

$$D_N^*(P) \geq c_s N^{-1}(\log N)^{(s-1)/2}$$

and for any sequence S we have

$$D_N^*(S) \geq c_s N^{-1}(\log N)^{s/2} \quad \text{for infinitely many } N,$$

where the constant $c_s > 0$ depends only on s. Proofs of Roth's results can also be found in Kuipers and Niederreiter [14] and Beck and Chen [3].

3. Nets and (t, s)-sequences

In this section we describe a theory of point sets and sequences with a very regular distribution behavior. As our starting point we take the following special property of the van der Corput sequence $x_0, x_1, \ldots$. For fixed integers $k \geq 0$ and $m \geq 1$ consider the points x_n with $k2^m \leq n < (k+1)2^m$. We claim that every dyadic interval $[a2^{-m}, (a+1)2^{-m})$, where $a \in \mathbb{Z}$ and $0 \leq a < 2^m$, contains exactly one point x_n with $k2^m \leq n < (k+1)2^m$. To see this, just note that for $k2^m \leq n < (k+1)2^m$ the m least significant bits in the binary expansion of n can range freely, whereas the remaining leading bits are fixed; for $x_n = \phi_2(n)$ this means that its m leading bits after the "decimal point" can range freely, whereas the remaining bits are fixed.

This special distribution property of the van der Corput sequence motivates the following definitions. We fix the dimension $s \geq 1$ and an integer $b \geq 2$.

Definition 2. *An* elementary interval in base b *is a subinterval* J *of* I^s *of the form*

$$J = \prod_{i=1}^{s} [a_i b^{-d_i}, (a_i + 1) b^{-d_i})$$

with $a_i, d_i \in \mathbb{Z}$ *for* $1 \le i \le s$.

Definition 3. *Let* $0 \le t \le m$ *be integers. A* (t, m, s)-net in base b *is a point set* P *of* b^m *points in* I^s *such that* $A(J; P) = b^t$ *for every elementary interval* J *in base* b *with* $Vol(J) = b^{t-m}$.

Definition 4. *Let* $t \ge 0$ *be an integer. A sequence* $\mathbf{x}_0, \mathbf{x}_1, \ldots$ *of points in* I^s *is a* (t, s)-sequence in base b *if for all integers* $k \ge 0$ *and* $m > t$ *the point set consisting of the* $\mathbf{x}_n$ *with* $kb^m \le n < (k+1)b^m$ *is a* (t, m, s)-*net in base* b.

In this language, the van der Corput sequence is a $(0, 1)$-sequence in base 2. Definitions 3 and 4 were introduced by Sobol' [36] in the case $b = 2$; the general definitions were first given by Niederreiter [24]. Note that if P is a (t, m, s)-net in base b, then the remainder function satisfies $R(J; P) = 0$ for every elementary interval J in base b with $\mathrm{Vol}(J) = b^{t-m}$. More generally, it follows that if J is an elementary interval in base b with $\mathrm{Vol}(J) \ge b^{t-m}$, or a disjoint union of such intervals, then $R(J; P) = 0$ (observe that such sets J can be written as disjoint unions of elementary intervals in base b with volume b^{t-m}). This implies that any (t, m, s)-net in base b is also a (u, m, s)-net in base b for $t \le u \le m$ and that any (t, s)-sequence in base b is also a (u, s)-sequence in base b for $u \ge t$. Therefore, it is clear that smaller values of t mean stronger regularity properties.

Upper bounds for the discrepancy of nets and (t, s)-sequences have been established in Niederreiter [24]. These bounds are completely explicit, but for the sake of simplicity we give them here in an abbreviated form.

Theorem 1. *If* P *is a* (t, m, s)-*net in base* b *with* $s \ge 2$, *then*

$$D_N^*(P) \le B(s, b) b^t N^{-1} (\log N)^{s-1} + O(b^t N^{-1} (\log N)^{s-2}).$$

If either $s = 2$ *or* $b = 2, s = 3, 4$, *then*

$$B(s, b) = \left(\frac{b-1}{2 \log b} \right)^{s-1},$$

otherwise

$$B(s,b) = \frac{1}{(s-1)!}\left(\frac{\lfloor b/2 \rfloor}{\log b}\right)^{s-1}.$$

Theorem 2. *If S is a (t,s)-sequence in base b with $s \geq 2$, then*

$$D_N^*(S) \leq C(s,b)b^t N^{-1}(\log N)^s + O(b^t N^{-1}(\log N)^{s-1}) \text{ for } N \geq 2.$$

If either $s = 2$ or $b = 2, s = 3, 4$, then

$$C(s,b) = \frac{1}{s}\left(\frac{b-1}{2\log b}\right)^s,$$

otherwise

$$C(s,b) = \frac{1}{s!} \cdot \frac{b-1}{2\lfloor b/2 \rfloor}\left(\frac{\lfloor b/2 \rfloor}{\log b}\right)^s.$$

The fact that these upper bounds are increasing functions of t is in accordance with earlier remarks on the values of t. In the case of the least possible value $t = 0$ there are interesting connections with classical combinatorial problems. We first note that in the cases $m = 0, 1$ it is trivial to construct a $(0, m, s)$-net in base b. For $m = 0$ take one arbitrary point from I^s, and for $m = 1$ take the point set consisting of $(n/b, \ldots, n/b) \in I^s, n = 0, 1, \ldots, b-1$. For $m \geq 2$ it was shown in Niederreiter [24] that a $(0, m, s)$-net in base b can only exist if $s \leq M(b) + 2$, where $M(b)$ is the maximum cardinality of a set of mutually orthogonal latin squares of order b. Since $M(b) \leq b - 1$, we get in particular the necessary condition $s \leq b + 1$ for the existence of a $(0, m, s)$-net in base b with $m \geq 2$. The following curious result was also noted in [24]: there exists a finite projective plane of order b if and only if there exists a $(0, 2, b+1)$-net in base b. For sequences it was shown in [24] that a $(0, s)$-sequence in base b can only exist if $s \leq M(b) + 1$; in particular, we must have $s \leq b$.

A general principle for the construction of nets was introduced in [24]. Although this construction principle works for arbitrary bases, we now consider only the special case where the base is a prime power q. Let F_q be the finite field of order q and as before let $Z_q = \{0, 1, \ldots, q-1\} \subseteq \mathbb{Z}$. For given $m \geq 1$ and $s \geq 1$ we choose:

(i) bijections $\psi_r : Z_q \to F_q$ for $0 \leq r \leq m-1$;

(ii) bijections $\eta_{ij} : F_q \to Z_q$ for $1 \le i \le s, 1 \le j \le m$;

(iii) elements $c_{jr}^{(i)} \in F_q$ for $1 \le i \le s, 1 \le j \le m, 0 \le r \le m-1$.

For $n = 0, 1, \ldots, q^m - 1$ let

$$n = \sum_{r=0}^{m-1} a_r(n) q^r \quad \text{with all } a_r(n) \in Z_q.$$

Put

$$x_n^{(i)} = \sum_{j=1}^{m} y_{nj}^{(i)} q^{-j} \quad \text{for} \quad 0 \le n < q^m, 1 \le i \le s,$$

with

$$y_{nj}^{(i)} = \eta_{ij}\left(\sum_{r=0}^{m-1} c_{jr}^{(i)} \psi_r(a_r(n))\right) \in Z_q \text{ for } 0 \le n < q^m, 1 \le i \le s, 1 \le j \le m,$$

and define the point set

$$\mathbf{x}_n = \left(x_n^{(1)}, \ldots, x_n^{(s)}\right) \in I^s \quad \text{for} \quad 0 \le n < q^m. \tag{4}$$

We collect the elements $c_{jr}^{(i)} \in F_q$ into the system C of vectors

$$\mathbf{c}_j^{(i)} = \left(c_{j0}^{(i)}, \ldots, c_{j,m-1}^{(i)}\right) \in F_q^m \quad \text{for} \quad 1 \le i \le s, 1 \le j \le m.$$

Definition 5. *For the system* $C = \{\mathbf{c}_j^{(i)} : 1 \le i \le s, 1 \le j \le m\}$ *as above let* $\varrho(C)$ *be the largest positive integer* d *such that any system* $\{\mathbf{c}_j^{(i)} : 1 \le j \le d_i, 1 \le i \le s\}$ *with* $0 \le d_i \le m$ *for* $1 \le i \le s$ *and* $\sum_{i=1}^{s} d_i = d - 1$ *is linearly independent over* F_q *(here the empty system is viewed as linearly independent).*

We always have $1 \le \varrho(C) \le m + 1$. The following result was shown in [24, Theorem 6.10].

Lemma 1. *The point set* (4) *is a* (t, m, s)*-net in base* q *with* $t = m + 1 - \varrho(C)$.

From Lemma 1 and the general discrepancy bound in Theorem 1 it follows that if P is the point set (4) and $s \ge 2$, then

$$D_N^*(P) \le B(s, q) q^{1-\varrho(C)} (\log N)^{s-1} + O\left(q^{-\varrho(C)} (\log N)^{s-2}\right).$$

A lower bound is shown in [30], namely

$$D_N^*(P) \geq \frac{q-1}{3} q^{-\varrho(C)}.$$

These bounds demonstrate that $D_N^*(P)$ is small if and only if $\varrho(C)$ is large. A general study of how large one can make $\varrho(C)$ has been carried out in [28].

If q is prime, then F_q and Z_q can be identified and every bijection η_{ij} in (ii) above can be taken as the identity map. In this case there is another method of obtaining an upper bound for $D_N^*(P)$. We need some notation to describe this method. Put $C(q) = (-q/2, q/2] \cap \mathbb{Z}$. For $(h_1, \ldots, h_m) \in C(q)^m$ define $d(h_1, \ldots, h_m)$ to be the largest index d with $h_d \neq 0$, provided that $(h_1, \ldots, h_m) \neq (0, \ldots, 0)$, and put $d(0, \ldots, 0) = 0$. For $q = 2$ put

$$Q_q(h_1, \ldots, h_m) = 2^{-d(h_1, \ldots, h_m)},$$

and for $q > 2$ put

$$Q_q(h_1, \ldots, h_m) = \begin{cases} q^{-d}(\csc \frac{\pi}{q} |h_d| + \sigma(d, m)) & \text{if } (h_1, \ldots, h_m) \neq (0, \ldots, 0), \\ 1 & \text{if } (h_1, \ldots, h_m) = (0, \ldots, 0), \end{cases}$$

where $d = d(h_1, \ldots, h_m)$ and where $\sigma(d, m) = 1$ for $d < m$ and $\sigma(m, m) = 0$. Let $C(q)^{s \times m}$ be the set of all $s \times m$ matrices with entries in $C(q)$. For each $H = (h_{ij}) \in C(q)^{s \times m}$ we define

$$P_q(H) = \prod_{i=1}^{s} Q_q(h_{i1}, \ldots, h_{im}).$$

For the system $C = \{\mathbf{c}_j^{(i)} : 1 \leq i \leq m, 1 \leq j \leq s\}$ of vectors in Definition 5 we set

$$R(C) = \sum_H P_q(H),$$

the sum running over all nonzero $H = (h_{ij}) \in C(q)^{s \times m}$ with

$$\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} \mathbf{c}_j^{(i)} = \mathbf{0} \in F_q^m,$$

where the h_{ij} are viewed as elements of F_q. Then the following result is proved in [30].

Lemma 2. *If q is prime and every η_{ij} is the identity map, then the point set P given by (4) satisfies*

$$D_N^*(P) \le 1 - \left(1 - \frac{1}{N}\right)^s + R(C) \le \frac{s}{N} + R(C).$$

An important application of Lemma 2 is the following one. For a prime q and for integers $m \ge 1$ and $s \ge 2$ let

$$M_q(m,s) = \frac{1}{\mathrm{card}(\mathcal{C})} \sum_{C \in \mathcal{C}} R(C)$$

be the mean value of $R(C)$ over the set $\mathcal{C}$ of all choices for a system $C = \{\mathbf{c}_j^{(i)} \in F_q^m : 1 \le i \le s, 1 \le j \le m\}$. This mean value is calculated in [30], and the value is $O(N^{-1}(\log N)^s)$ with $N = q^m$. Thus, Lemma 2 implies that the construction of the point sets (4) yields on the average a point set P with $D_N^*(P) = O(N^{-1}(\log N)^s)$.

An analogous principle is available for the construction of (t,s)-sequences (see [24]). In the case of a prime power base q we let $s \ge 1$ be given and we choose:

(i) bijections $\psi_r : Z_q \to F_q$ for $r \ge 0$, with $\psi_r(0) = 0$ for all sufficiently large r;

(ii) bijections $\eta_{ij} : F_q \to Z_q$ for $1 \le i \le s$ and $j \ge 1$;

(iii) elements $c_{jr}^{(i)} \in F_q$ for $1 \le i \le s, j \ge 1, r \ge 0$.

For $n = 0, 1, \ldots$ let

$$n = \sum_{r=0}^{\infty} a_r(n) q^r$$

be the digit expansion in base q as in (1). Put

$$x_n^{(i)} = \sum_{j=1}^{\infty} y_{nj}^{(i)} q^{-j} \quad \text{for} \quad n \ge 0, 1 \le i \le s,$$

with

$$y_{nj}^{(i)} = \eta_{ij}\left(\sum_{r=0}^{\infty} c_{jr}^{(i)} \psi_r(a_r(n))\right) \in Z_q \quad \text{for} \quad n \ge 0, 1 \le i \le s, j \ge 1.$$

Note that the sum over r is a finite sum since $\psi_r(0) = 0$ and $a_r(n) = 0$ for all sufficiently large r. We now define the sequence

$$\mathbf{x}_n = \left(x_n^{(1)}, \ldots, x_n^{(s)}\right) \quad \text{for} \quad n = 0, 1, \ldots. \tag{5}$$

To guarantee that the points $\mathbf{x}_n$ belong to I^s (and not only to $\bar{I}^s$), and also for the analysis of the sequence (5), we need the following condition:
(iv) for each n and i we have $y_{nj}^{(i)} < q - 1$ for infinitely many j.

In [24] a stronger condition than (iv) was used, namely that $\eta_{ij}(0) = 0$ for $1 \le i \le s$ and all sufficiently large j and that for each i and r we have $c_{jr}^{(i)} = 0$ for all sufficiently large j. This stronger condition guarantees that for each n and i we have $y_{nj}^{(i)} = 0$ for all sufficiently large j, so that each $x_n^{(i)}$ is given by a finite digit expansion in base q. However, the proof of [24, Theorem 6.23] shows that condition (iv) suffices to establish the following result.

Lemma 3. *Let $t \ge 0$ be an integer. If for each integer $m > t$ the system $C^{(m)}$ given by*

$$\mathbf{c}_j^{(i)} = \left(c_{j0}^{(i)}, \ldots, c_{j,m-1}^{(i)}\right) \in F_q^m \quad \text{for} \quad 1 \le i \le s,\ 1 \le j \le m,$$

satisfies $\varrho(C^{(m)}) \ge m + 1 - t$, then the sequence (5) is a (t, s)-sequence in base q.

The problem of constructing (t, m, s)-nets and (t, s)-sequences in base q with a small value of t leads to combinatorial questions for vector spaces over F_q. These questions are connected with problems in algebraic coding theory (see [24], [28]). There are various approaches to these combinatorial questions, for instance by ad hoc constructions as in [24], by the theory of hyperderivatives as in [26], or by using formal Laurent series over F_q, with the latter being the most promising method.

The method of formal Laurent series was introduced in Niederreiter [25] to carry out the following construction of (t, s)-sequences in base q. To simplify the exposition, we consider only a special case of the construction in [25]. Let $F_q((x^{-1}))$ be the field of formal Laurent series over F_q in the variable x^{-1}, and note that $F_q((x^{-1}))$ contains the field of rational functions over F_q. For a given dimension $s \ge 2$ choose s pairwise relatively prime

polynomials $p_1, \ldots, p_s \in F_q[x]$ with $\deg(p_i) = e_i \geq 1$ for $1 \leq i \leq s$. For integers $j \geq 1$ and $u \geq 0$ we have the expansion

$$\frac{x^u}{p_i(x)^j} = \sum_{r=w}^{\infty} a^{(i)}(j,u,r)x^{-r-1}$$

in $F_q((x^{-1}))$, where the integer $w \leq 0$ may depend on i, j, and u. Then define

$$c_{jr}^{(i)} = a^{(i)}(Q+1,u,r) \in F_q \quad \text{for} \quad 1 \leq i \leq s, j \geq 1, r \geq 0,$$

where $j - 1 = Qe_i + u$ with $Q, u \in \mathbb{Z}$ and $0 \leq u < e_i$. It is clear that for each i and r we have $c_{jr}^{(i)} = 0$ for all sufficiently large j. If we assume that $\eta_{ij}(0) = 0$ for $1 \leq i \leq s$ and all sufficiently large j, then the condition (iv) above is satisfied, and so (5) yields a sequence of points in I^s. It was shown in [25] that this sequence is a (t,s)-sequence in base q with

$$t = \sum_{i=1}^{s}(e_i - 1).$$

For fixed s and q the minimum value of t is obtained by letting $p_1, \ldots, p_s$ be the "first s" monic irreducible polynomials over F_q, i.e., the first s terms of a sequence in which all monic irreducible polynomials over F_q are listed according to nondecreasing degrees. With this choice of $p_1, \ldots, p_s$ we get

$$T_q(s) = \sum_{i=1}^{s}(\deg(p_i) - 1)$$

as the minimum value of t. Now consider the discrepancy bound in Theorem 2. For fixed s the minimum value of the leading coefficient $C(s,b)b^t$ obtained by the present construction is given by

$$C_s = \min_q C(s,q)q^{T_q(s)},$$

where the minimum is extended over all prime powers q. This yields, for example, $C_2 = 0.26\ldots, C_3 = 0.12\ldots, C_{10} = 0.0004\ldots$, and a value of C_{19} close to 10^{-8}. Asymptotically we have

$$\overline{\lim_{s\to\infty}} \frac{\log C_s}{s \log\log s} \leq -1.$$

Thus $C_s \to 0$ at a superexponential rate as $s \to \infty$. This construction gives the best low-discrepancy sequences, and by the principle in (3) also the best low-discrepancy point sets, that are currently known.

An interesting special case of the construction above arises if $s \leq q$. Then we can choose $p_i(x) = x - b_i$ with distinct $b_i \in F_q, 1 \leq i \leq s$. Thus $T_q(s) = 0$ and

$$c_{jr}^{(i)} = a^{(i)}(j, 0, r) \quad \text{for} \quad 1 \leq i \leq s, j \geq 1, r \geq 0.$$

Furthermore,

$$\frac{1}{p_i(x)^j} = \frac{1}{x^j (1 - b_i x^{-1})^j} = x^{-j} \sum_{r=0}^{\infty} \binom{r+j-1}{j-1} b_i^r x^{-r}$$
$$= \sum_{r=j-1}^{\infty} \binom{r}{j-1} b_i^{r-j+1} x^{-r-1},$$

and so

$$c_{jr}^{(i)} = 0 \quad \text{for} \quad r < j-1,$$
$$c_{jr}^{(i)} = \binom{r}{j-1} b_i^{r-j+1} \quad \text{for} \quad r \geq j-1.$$

This choice of the $c_{jr}^{(i)}$ yields the $(0, s)$-sequences in base q constructed in Niederreiter [24], and if we specialize further to q being a prime, then this yields the sequences constructed in Faure [9]. Note that if we want $(0, s)$-sequences in base q, then the condition $s \leq q$ is best possible since we mentioned earlier in this section that $s \leq q$ is a necessary condition for the existence of a $(0, s)$-sequence in base q.

4. Some new constructions

The method of formal Laurent series can be used for further constructions of nets and (t, s)-sequences. First we present a construction of nets, the origins of which go back to the author's paper [20]. For a given dimension $s \geq 2$

let $f \in F_q[x]$ with $\deg(f) = m \geq 1$ and let $g_1, \ldots, g_s \in F_q[x]$. Consider the expansions

$$\frac{g_i(x)}{f(x)} = \sum_{k=w_i}^{\infty} u_k^{(i)} x^{-k} \in F_q((x^{-1})) \quad \text{for} \quad 1 \leq i \leq s,$$

where $w_i \leq 1$ for $1 \leq i \leq s$. Then define

$$c_{jr}^{(i)} = u_{r+j}^{(i)} \in F_q \quad \text{for} \quad 1 \leq i \leq s, 1 \leq j \leq m, 0 \leq r \leq m-1. \tag{6}$$

With this choice of the elements $c_{jr}^{(i)}$ we then apply the general principle for the construction of nets described in Section 3. This yields the point set (4) consisting of q^m points in I^s. We denote this point set by $P(\mathbf{g}, f)$, where we write $\mathbf{g} = (g_1, \ldots, g_s) \in F_q[x]^s$ for the s-tuple of polynomials $g_1, \ldots, g_s$. For an arbitrary $\mathbf{h} = (h_1, \ldots, h_s) \in F_q[x]^s$ we define the "inner product"

$$\mathbf{h} \cdot \mathbf{g} = \sum_{i=1}^{s} h_i g_i.$$

Let ν be the discrete exponential valuation on $F_q((x^{-1}))$ which extends the degree function on $F_q[x]$.

Lemma 4. *Let*

$$\mathbf{c}_j^{(i)} = \left(c_{j0}^{(i)}, \ldots, c_{j,m-1}^{(i)}\right) \in F_q^m \text{ for } 1 \leq i \leq s, 1 \leq j \leq m,$$

where the $c_{jr}^{(i)}$ *are given by* (6). *Then for* $h_{ij} \in F_q, 1 \leq i \leq s, 1 \leq j \leq m$, *we have*

$$\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} \mathbf{c}_j^{(i)} = \mathbf{0} \in F_q^m \tag{7}$$

if and only if $f | \mathbf{h} \cdot \mathbf{g}$, *where* $\mathbf{h} = (h_1, \ldots, h_s) \in F_q[x]^s$ *with*

$$h_i(x) = \sum_{j=1}^{m} h_{ij} x^{j-1} \in F_q[x] \text{ for } 1 \leq i \leq s. \tag{8}$$

Proof. By comparing components, we see that (7) is equivalent to

$$\sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} u_{r+j}^{(i)} = 0 \quad \text{for} \quad 0 \leq r \leq m-1. \tag{9}$$

For $1 \le i \le s$ we have

$$\frac{h_i(x)g_i(x)}{f(x)} = \left(\sum_{j=1}^{m} h_{ij}x^{j-1}\right)\left(\sum_{k=w_i}^{\infty} u_k^{(i)}x^{-k}\right) = \sum_{j=1}^{m}\sum_{k=w_i}^{\infty} h_{ij}u_k^{(i)}x^{-k+j-1}$$
$$= \sum_{j=1}^{m} h_{ij} \sum_{r=w_i-j}^{\infty} u_{r+j}^{(i)}x^{-r-1}.$$

Thus for $r \ge 0$ the coefficient of x^{-r-1} in h_ig_i/f is $\sum_{j=1}^{m} h_{ij}u_{r+j}^{(i)}$. Therefore, the condition (9) is equivalent to the following: for $0 \le r \le m-1$ the coefficient of x^{-r-1} in $\sum_{i=1}^{s} h_ig_i/f$ is 0. This means that

$$\frac{1}{f}\mathbf{h}\cdot\mathbf{g} = p + L,$$

where $p \in F_q[x]$ and $L \in F_q((x^{-1}))$ with $\nu(L) < -m$. The last identity is equivalent to

$$\mathbf{h}\cdot\mathbf{g} - pf = Lf.$$

On the left-hand side we have a polynomial over F_q, whereas on the right-hand side we have $\nu(Lf) < 0$ since $\nu(f) = \deg(f) = m$. This is only possible if $Lf = 0$, i.e., if $f|\mathbf{h}\cdot\mathbf{g}$. ■

Corollary 1. *If C is the system of vectors $\mathbf{c}_j^{(i)}$ in Lemma 4 and $\varrho(C)$ is as in Definition 5, then*

$$\varrho(C) = \varrho(\mathbf{g}, f) := \min \sum_{i=1}^{s}(\deg(h_i) + 1),$$

where the minimum is extended over all nonzero $\mathbf{h} = (h_1, \ldots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \le i \le s$ and $f|\mathbf{h}\cdot\mathbf{g}$, where we use the convention $\deg(0) = -1$.

Theorem 3. *The point set $P(\mathbf{g}, f)$ is a (t, m, s)-net in base q with $t = m + 1 - \varrho(\mathbf{g}, f)$.*

Proof. This follows from Lemma 1 and Corollary 1. ■

From Theorems 1 and 3 we obtain the discrepancy bound

$$D_N^*(P(\mathbf{g}, f)) \le B(s, q)q^{1-\varrho(\mathbf{g},f)}(\log N)^{s-1} + O(q^{-\varrho(\mathbf{g},f)}(\log N)^{s-2}).$$

Another discrepancy bound is obtained from Lemma 2 in the case where q is prime and every η_{ij} is the identity map. If $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \le i \le s$, then we can use (8) and the fact that $C(q)$ forms a complete residue system mod q to identify $\mathbf{h}$ with $H = (h_{ij}) \in C(q)^{s \times m}$, and we put $P_q(\mathbf{h}) = P_q(H)$. In analogy with the definition of $R(C)$ we then set

$$R(\mathbf{g}, f) = \sum_{\mathbf{h}} P_q(\mathbf{h}), \tag{10}$$

where the sum is over all nonzero $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \le i \le s$ and $f | \mathbf{h} \cdot \mathbf{g}$. It follows from Lemma 4 that $R(\mathbf{g}, f) = R(C)$, where C is the system of vectors $\mathbf{c}_j^{(i)}$ in Lemma 4. Thus Lemma 2 shows that

$$D_N^*(P(\mathbf{g}, f)) \le 1 - \left(1 - \frac{1}{N}\right)^s + R(\mathbf{g}, f) \le \frac{s}{N} + R(\mathbf{g}, f), \tag{11}$$

provided that q is prime and every η_{ij} is the identity map.

On the basis of (11) we will prove that the point sets $P(\mathbf{g}, f)$ are on the average low-discrepancy point sets. For $s \ge 2$ and $f \in F_q[x]$ with q prime and $\deg(f) = m \ge 1$ put

$$G_s(f) = \{\mathbf{g} = (g_1, \dots, g_s) \in F_q[x]^s : \gcd(g_i, f) = 1 \quad \text{and} \quad \deg(g_i) < m \quad \text{for} \quad 1 \le i \le s\}.$$

Let

$$M_s(f) = \frac{1}{\operatorname{card}(G_s(f))} \sum_{\mathbf{g} \in G_s(f)} R(\mathbf{g}, f)$$

be the mean value of $R(\mathbf{g}, f)$ extended over the set $G_s(f)$. Note that $\operatorname{card}(G_s(f)) = \Phi_q(f)^s$, where Φ_q is the analog of Euler's totient function for the ring $F_q[x]$. By a formula in [17, Lemma 3.69] we have

$$\Phi_q(f) = q^m \prod_{k=1}^{r} \left(1 - q^{-n_k}\right), \tag{12}$$

where $n_1, \dots, n_r$ are the degrees of the distinct monic irreducible polynomials over F_q dividing f.

The proof of the following theorem depends on the theory of arithmetic functions on $F_q[x]$ as developed by Carlitz [6] and on the theory of characters of $F_q((x^{-1}))$ as developed by Carlitz [7] and Hayes [12]. In the sequel, an *arithmetic function* is a real-valued function on the multiplicative semigroup

S_q of monic polynomials over F_q. An arithmetic function E is called *multiplicative* (resp. *additive*) if $E(gh) = E(g)E(h)$ (resp. $E(gh) = E(g)+E(h)$) for all $g, h \in S_q$ with $\gcd(g,h) = 1$. We write $\sum_{v \bmod f}$ for a sum over all $v \in F_q[x]$ with $\deg(v) < \deg(f)$, and we write $\sum^*_{v \bmod f}$ if the additional condition $\gcd(v,f) = 1$ is imposed. Furthermore, $\sum_{d|f}$ denotes a sum over all $d \in S_q$ dividing f.

Let χ be a fixed nontrivial additive character of F_q. For $L \in F_q((x^{-1}))$ put $X_q(L) = \chi(t_1)$, where t_1 is the coefficient of x^{-1} in the expression for L. Then X_q is an additive character of $F_q((x^{-1}))$ which is trivial on $F_q[x]$. Consequently, $X_q(\cdot/f)$ is a nontrivial additive character of the residue class ring $F_q[x]/(f)$. For $g \in F_q[x]$ the orthogonality relations for characters yield

$$\sum_{v \bmod f} X_q\left(\frac{vg}{f}\right) = \begin{cases} q^{\deg(f)} & \text{if } f|g, \\ 0 & \text{if } f \nmid g. \end{cases} \tag{13}$$

See e.g. Car [5, p.8] for this formula. We put $C^*(q) = C(q) \setminus \{0\}$.

Theorem 4. *Let q be a prime, let $s \geq 2$ be an integer, let $f \in F_q[x]$ with $\deg(f) = m \geq 1$, and put $N = q^m$. Then*

$$M_s(f) = \frac{1}{N}(c_q \log N + d_q)^s - c_q s \frac{\log N}{N} + O\left(\frac{(\log\log N)^2}{N}\right),$$

where the implied constant depends only on q and s and where $d_2 = 1$, $d_q = 1/q$ for $q > 2$, $c_2 = 1/\log 4$, and

$$c_q = \frac{1}{q \log q}\left(q - 1 + \sum_{z \in C^*(q)} \csc\frac{\pi|z|}{q}\right) \text{ for } q > 2.$$

Proof. We can assume w.l.o.g. that f is monic. Inserting the definition of $R(\mathbf{g}, f)$ in (10) into the expression for $M_s(f)$ and interchanging the order of summation, we get

$$M_s(f) = \frac{1}{\Phi_q(f)^s} \sum_{\mathbf{h} \neq \mathbf{0}} A(\mathbf{h}) P_q(\mathbf{h}),$$

where the sum is over all nonzero $\mathbf{h} = (h_1, \ldots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \le i \le s$ and where $A(\mathbf{h})$ is the number of $\mathbf{g} \in G_s(f)$ with $f | \mathbf{h} \cdot \mathbf{g}$. Since $A(\mathbf{0}) = \Phi_q(f)^s$ and $P_q(\mathbf{0}) = 1$, we can write

$$M_s(f) = \frac{1}{\Phi_q(f)^s} \sum_{\mathbf{h}} A(\mathbf{h}) P_q(\mathbf{h}) - 1, \tag{14}$$

where the sum is over all $\mathbf{h} = (h_1, \ldots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \le i \le s$. For any such $\mathbf{h}$ we have

$$A(\mathbf{h}) = \sum_{\mathbf{g} \in G_s(f)} q^{-m} \sum_{v \bmod f} X_q\left(\frac{v}{f} \mathbf{h} \cdot \mathbf{g}\right)$$

by (13). By the definition of $P_q(\mathbf{h})$ we can write

$$P_q(\mathbf{h}) = \prod_{i=1}^{s} Q_q(h_i),$$

where we use (8) to identify h_i with $(h_{i1}, \ldots, h_{im}) \in C(q)^m$ and we define $Q_q(h_i)$ to be the quantity $Q_q(h_{i1}, \ldots, h_{im})$ in Section 3. Then we get

$$\sum_{\mathbf{h}} A(\mathbf{h}) P_q(\mathbf{h}) = \frac{1}{N} \sum_{v \bmod f} \sum_{\mathbf{h}} \sum_{\mathbf{g} \in G_s(f)} X_q\left(\frac{v}{f} \mathbf{h} \cdot \mathbf{g}\right) P_q(\mathbf{h})$$

$$= \frac{1}{N} \sum_{v \bmod f} \sum_{h_1 \bmod f} \cdots \sum_{h_s \bmod f} \sum_{g_1 \bmod f}^{*} \cdots \sum_{g_s \bmod f}^{*} X_q\left(\frac{v}{f} h_1 g_1\right) \ldots X_q\left(\frac{v}{f} h_s g_s\right)$$

$$Q_q(h_1) \ldots Q_q(h_s)$$

$$= \frac{1}{N} \sum_{v \bmod f} Y_q(v, f)^s$$

with

$$Y_q(v, f) = \sum_{h \bmod f} \sum_{g \bmod f}^{*} X_q\left(\frac{v}{f} hg\right) Q_q(h).$$

Now

$$Y_q(0, f) = \Phi_q(f) \sum_{h \bmod f} Q_q(h),$$

thus

$$\sum_{\mathbf{h}} A(\mathbf{h})P_q(\mathbf{h}) = \frac{1}{N}\Phi_q(f)^s \left(\sum_{h \bmod f} Q_q(h) \right)^s + \frac{1}{N} \sum_{\substack{v \bmod f \\ v \neq 0}} Y_q(v,f)^s. \quad (15)$$

Let μ_q be the Möbius function on S_q (see [6] and [17, p. 145]) and note that μ_q is multiplicative. We abbreviate $\gcd(g,f)$ by (g,f) in this proof. Then for fixed $v \in F_q[x]$ with $0 \leq \deg(v) < m$ we get

$$\begin{aligned} Y_q(v,f) &= \sum_{h \bmod f} Q_q(h) \sum_{g \bmod f} X_q\left(\frac{v}{f}hg\right) \sum_{d|(g,f)} \mu_q(d) \\ &= \sum_{h \bmod f} Q_q(h) \sum_{d|f} \mu_q(d) \sum_{\substack{g \bmod f \\ d|g}} X_q\left(\frac{v}{f}hg\right) \\ &= \sum_{h \bmod f} Q_q(h) \sum_{d|f} \mu_q(d) \sum_{a \bmod f/d} X_q\left(\frac{v}{f}had\right) \\ &= \sum_{h \bmod f} Q_q(h) \sum_{d|f} \mu_q\left(\frac{f}{d}\right) \sum_{a \bmod d} X_q\left(\frac{v}{d}ha\right), \end{aligned}$$

where in the last step we changed d into f/d. Applying (13) to the innermost sum, we obtain

$$\begin{aligned} Y_q(v,f) &= \sum_{h \bmod f} Q_q(h) \sum_{\substack{d|f \\ d|vh}} \mu_q\left(\frac{f}{d}\right) q^{\deg(d)} \\ &= \sum_{d|f} \mu_q\left(\frac{f}{d}\right) q^{\deg(d)} \sum_{\substack{h \bmod f \\ d|vh}} Q_q(h). \end{aligned}$$

Now $d|vh$ if and only if $d/(d,v)$ divides h, thus

$$Y_q(v,f) = \sum_{d|f} \mu_q\left(\frac{f}{d}\right) q^{\deg(d)} E_q\left(\frac{d}{(d,v)}, f\right), \quad (16)$$

where for an $a \in S_q$ dividing f we put

$$E_q(a,f) = \sum_{\substack{h \bmod f \\ a|h}} Q_q(h).$$

If $a = f$, then

$$E_q(a, f) = Q_q(0) = 1.$$

Now let $a \neq f$, then

$$E_q(a, f) = 1 + \sum_{\substack{b \bmod f/a \\ b \neq 0}} Q_q(ab).$$

For $q = 2$ we have

$$\sum_{\substack{b \bmod f/a \\ b \neq 0}} Q_q(ab) = \sum_{\substack{b \bmod f/a \\ b \neq 0}} 2^{-\deg(ab)-1} = 2^{-\deg(a)-1} \sum_{k=0}^{\deg(f/a)-1} 2^{-k} 2^k$$

$$= \deg\left(\frac{f}{a}\right) 2^{-\deg(a)-1}.$$

For $q > 2$ and for $h \in F_q[x]$ with $0 \leq \deg(h) < m$ we have

$$Q_q(h) = q^{-\deg(h)-1} \left(\csc\frac{\pi}{q}|\mathrm{sgn}(h)| + \sigma(\deg(h)+1, m)\right),$$

where $\mathrm{sgn}(h)$ is the leading coefficient of h, viewed as an element of $C^*(q)$. Since a is monic, we get

$$\sum_{\substack{b \bmod f/a \\ b \neq 0}} Q_q(ab) =$$

$$= \sum_{\substack{b \bmod f/a \\ b \neq 0}} q^{-\deg(ab)-1} \left(\csc\frac{\pi}{q}|\mathrm{sgn}(b)| + \sigma\left(\deg(b), \deg\left(\frac{f}{a}\right) - 1\right)\right)$$

$$= q^{-\deg(a)-1} \sum_{k=0}^{\deg(f/a)-1} q^{-k} q^k \sum_{z \in C^*(q)} \left(\csc\frac{\pi|z|}{q} + \sigma\left(k, \deg\left(\frac{f}{a}\right) - 1\right)\right)$$

$$= \deg\left(\frac{f}{a}\right) q^{-\deg(a)-1} \sum_{z \in C^*(q)} \csc\frac{\pi|z|}{q}$$

$$+ (q-1)\left(\deg\left(\frac{f}{a}\right) - 1\right) q^{-\deg(a)-1}$$

$$= T_q \deg\left(\frac{f}{a}\right) q^{-\deg(a)} - \varepsilon_q q^{-\deg(a)},$$

where we put $T_q = c_q \log q$ for all q and $\varepsilon_q = (q-1)/q$ for $q > 2$. The case $q = 2$ is also covered by this formula if we put $\varepsilon_2 = 0$. To include the case $a = f$, we put

$$\delta_q(a,f) = \begin{cases} \varepsilon_q & \text{if } a = f, \\ 0 & \text{if } a \neq f. \end{cases}$$

Then for all $a \in S_q$ dividing f we have

$$\begin{aligned} E_q(a,f) &= 1 + T_q \deg\left(\frac{f}{a}\right) q^{-\deg(a)} - (\varepsilon_q - \delta_q(a,f)) q^{-\deg(a)} \\ &= 1 + (mT_q - \varepsilon_q + \delta_q(a,f)) q^{-\deg(a)} - T_q \deg(a) q^{-\deg(a)}. \end{aligned} \tag{17}$$

Applying this formula with $a = d/(d,v)$ in (16), we obtain

$$\begin{aligned} Y_q(v,f) = \sum_{d \mid f} \mu_q\left(\frac{f}{d}\right) \cdot \\ \cdot \left(q^{\deg(d)} + \left(mT_q - \varepsilon_q + \delta_q\left(\frac{d}{(d,v)}, f\right)\right) q^{\deg((d,v))} \right. \\ \left. - T_q \deg\left(\frac{d}{(d,v)}\right) q^{\deg((d,v))} \right), \end{aligned}$$

thus

$$Y_q(v,f) = \Phi_q(f) + (c_q \log N - \varepsilon_q) H_q^{(1)}(v,f) - T_q H_q^{(2)}(v,f) + H_q^{(3)}(v,f) \tag{18}$$

with

$$\begin{aligned} H_q^{(1)}(v,f) &= \sum_{d \mid f} \mu_q\left(\frac{f}{d}\right) q^{\deg((d,v))}, \\ H_q^{(2)}(v,f) &= \sum_{d \mid f} \mu_q\left(\frac{f}{d}\right) \deg\left(\frac{d}{(d,v)}\right) q^{\deg((d,v))}, \\ H_q^{(3)}(v,f) &= \sum_{d \mid f} \mu_q\left(\frac{f}{d}\right) \delta_q\left(\frac{d}{(d,v)}, f\right) q^{\deg((d,v))}. \end{aligned}$$

In the rest of the proof p will always stand for a monic irreducible polynomial over F_q. For a nonzero $v \in F_q[x]$ let $e_p(v)$ be the largest nonnegative integer such that $p^{e_p(v)}$ divides v. Now we consider $H_q^{(1)}(v,f)$ for a fixed $v \neq 0$.

Since $q^{\deg((d,v))}$ is a multiplicative function of d, it follows that $H_q^{(1)}(v,f)$ is a multiplicative function of f. For any integer $k \geq 1$ we have

$$H_q^{(1)}(v,p^k) = q^{\deg((p^k,v))} - q^{\deg((p^{k-1},v))}.$$

Hence, if $e_p(v) < k$, then $H_q^{(1)}(v,p^k) = 0$. If $e_p(v) \geq k$, then

$$H_q^{(1)}(v,p^k) = q^{\deg(p^k)} - q^{\deg(p^{k-1})} = \Phi_q(p^k)$$

by (12). By multiplicativity we obtain

$$H_q^{(1)}(v,f) = \begin{cases} \Phi_q(f) & \text{if } f|v, \\ 0 & \text{if } f \nmid v. \end{cases} \tag{19}$$

Next we consider $H_q^{(2)}(v,f)$ for a fixed $v \neq 0$. Since $\deg(d/(d,v))$ is an additive and $q^{\deg((d,v))}$ a multiplicative function of d, it follows by induction on the number of distinct polynomials p dividing f that

$$H_q^{(2)}(v,f) = \sum_{p|f} H_q^{(2)}(v,p^{e_p(f)}) H_q^{(1)}(v,f/p^{e_p(f)}). \tag{20}$$

For any integer $k \geq 1$ we have

$$H_q^{(2)}(v,p^k) = \deg\left(\frac{p^k}{(p^k,v)}\right) q^{\deg((p^k,v))} - \deg\left(\frac{p^{k-1}}{(p^{k-1},v)}\right) q^{\deg((p^{k-1},v))}.$$

Hence, if $e_p(v) \geq k$, then $H_q^{(2)}(v,p^k) = 0$. If $e_p(v) < k$, then

$$H_q^{(2)}(v,p^k) = \deg(p) q^{e_p(v)\deg(p)}.$$

By (19) and (20) we get

$$H_q^{(2)}(v,f) = \sum_p \deg(p) q^{e_p(v)\deg(p)} \Phi_q\left(f/p^{e_p(f)}\right),$$

where the sum is over all p satisfying the following two conditions: (i) $e_p(v) < e_p(f)$; (ii) $f/p^{e_p(f)}$ divides v. Note that (ii) means $e_{p_1}(f) \leq e_{p_1}(v)$ for all monic irreducible polynomials p_1 over F_q with $p_1 \neq p$. Thus (i) and (ii) hold simultaneously if and only if there exists a unique p with $e_p(v) < e_p(f)$. If this condition is satisfied, then with this p we have

$$H_q^{(2)}(v,f) = \deg(p) q^{e_p(v)\deg(p)} \Phi_q(f/p^{e_p(f)}),$$

whereas $H_q^{(2)}(v,f) = 0$ otherwise.

Now we consider $H_q^{(3)}(v,f)$. Note that $\delta_q(d/(d,v),f) \neq 0$ only if $q > 2$ and $d/(d,v) = f$. But since d divides f, we have $d/(d,v) = f$ if and only if $d = f$ and $(f,v) = 1$. Thus if $q > 2$ and $(f,v) = 1$, then $H_q^{(3)}(v,f) = (q-1)/q$. In all other cases we have $H_q^{(3)}(v,f) = 0$.

For $v \in F_q[x]$ with $0 \leq \deg(v) < m$ we have $H_q^{(1)}(v,f) = 0$ by (19), and so in view of (18) and the formula for $H_q^{(3)}(v,f)$ we get

$$Y_q(v,f) = \Phi_q(f) - T_q H_q^{(2)}(v,f) + O(1)$$

with an absolute implied constant. We combine this with (14) and (15) to obtain

$$M_s(f) = \frac{1}{N} E_q(1,f)^s + \frac{1}{N} \sum_{\substack{v \bmod f \\ v \neq 0}} \left(1 - T_q J_q(v,f) + O\left(\frac{1}{\Phi_q(f)}\right)\right)^s - 1,$$

where $J_q(v,f) = H_q^{(2)}(v,f)/\Phi_q(f)$. The formula for $H_q^{(2)}(v,f)$ shows that $J_q(v,f) = O(1)$, hence

$$M_s(f) = \frac{1}{N} E_q(1,f)^s + \frac{1}{N} \sum_{i=1}^{s} \binom{s}{i} (-T_q)^i \sum_{\substack{v \bmod f \\ v \neq 0}} J_q(v,f)^i + O\left(\frac{1}{\Phi_q(f)}\right) \tag{21}$$

with an implied constant depending only on q and s.

We now consider the sum over v in (21) for $1 \leq i \leq s$. From the formula for $H_q^{(2)}(v,f)$ we obtain

$$J_q(v,f) = \frac{\deg(p)}{\Phi_q\left(p^{e_p(f)-e_p(v)}\right)}$$

if there exists a unique p with $e_p(v) < e_p(f)$, and $J_q(v,f) = 0$ otherwise. We put

$$H_i(f) = \sum_{\substack{v \bmod f \\ v \neq 0}} J_q(v,f)^i \quad \text{for} \quad 1 \leq i \leq s.$$

Let $g, h \in S_q$ with $(g,h) = 1$ and let $v \in F_q[x]$ with $0 \leq \deg(v) < \deg(gh)$ be such that there exists a unique p with $e_p(v) < e_p(gh)$. Since then $e_p(gh) > 0$, p divides exactly one of g and h, and so the sum $H_i(gh)$ can be split up into two subsums according to these two cases. If $p|g$, say, then $v = v_1 h$ with

$v_1 \in F_q[x], 0 \le \deg(v_1) < \deg(g)$, and $J_q(v, gh) = J_q(v_1 h, gh) = J_q(v_1, g)$. From this it is easily seen that $H_i(gh) = H_i(g) + H_i(h)$, hence H_i is additive. For an integer $e \ge 1$ and any p we have

$$H_i(p^e) = \deg(p)^i \sum_{k=0}^{e-1} \sum_{\substack{v \bmod p^e \\ e_p(v)=k}} \Phi_q(p^{e-k})^{-i}.$$

For $0 \le k \le e-1$ the number of $v \in F_q[x]$ with $0 \le \deg(v) < \deg(p^e)$ and $e_p(v) = k$ is equal to $\Phi_q(p^{e-k})$, and so

$$H_i(p^e) = \deg(p)^i \sum_{k=1}^{e} \Phi_q(p^k)^{1-i}. \tag{22}$$

For $i = 1$ this yields $H_1(p^e) = \deg(p)e = \deg(p^e)$, thus $H_1(f) = \deg(f) = m$ by additivity. For $i = 2$ we get

$$\begin{aligned} H_2(p^e) &= \deg(p)^2 \sum_{k=1}^{e} q^{-k\deg(p)} \left(1 - q^{-\deg(p)}\right)^{-1} \\ &\le 2\deg(p)^2 \sum_{k=1}^{e} q^{-k\deg(p)} < 4\deg(p)^2 q^{-\deg(p)}, \end{aligned}$$

and so by additivity

$$H_2(f) < 4 \sum_{p|f} \deg(p)^2 q^{-\deg(p)}.$$

Let n be the number of distinct monic irreducible polynomials over F_q dividing f and let $p_1, \ldots, p_n$ be the "first n" monic irreducible polynomials over F_q. Then

$$H_2(f) < 4 \sum_{j=1}^{n} \deg(p_j)^2 q^{-\deg(p_j)} + O(1) \le 4 \sum_{r=1}^{D(n)} r^2 q^{-r} I_q(r) + O(1),$$

where $D(n) = \deg(p_n)$ and $I_q(r)$ is the number of monic irreducible polynomials over F_q of degree r. Since $I_q(r) \le q^r/r$ for $r \ge 1$ by [17, Corollary 3.21], it follows that

$$H_2(f) < 4 \sum_{r=1}^{D(n)} r + O(1) = O(D(n)^2). \tag{23}$$

On the other hand, we have

$$m = \deg(f) \geq \sum_{j=1}^{n} \deg(p_j) \geq (D(n)-1)I_q(D(n)-1).$$

From [17, Exercise 3.27] we obtain $I_q(r) \geq cq^r/r$ for $r \geq 1$ with an absolute constant $c > 0$. Thus, if $D(n) \geq 2$, then $m \geq cq^{D(n)-1}$, hence $D(n) = O(1 + \log m)$, and this holds trivially if $D(n) = 1$. Combining this with (23), we obtain

$$H_2(f) = O((\log\log N)^2). \tag{24}$$

For $i \geq 3$ it follows from (22) that

$$H_i(p^e) \leq \deg(p)^i \sum_{k=1}^{e} \Phi_q\left(p^k\right)^{-2} = \deg(p)^i \sum_{k=1}^{e} q^{-2k\deg(p)} \left(1 - q^{-\deg(p)}\right)^{-2}$$
$$< 2\deg(p)^i \left(q^{\deg(p)} - 1\right)^{-2},$$

and so by additivity

$$H_i(f) < 2 \sum_{\substack{g \in S_q \\ \deg(g) \geq 1}} \deg(g)^i \left(q^{\deg(g)} - 1\right)^{-2} = 2\sum_{k=1}^{\infty} k^i (q^k - 1)^{-2} q^k$$
$$\leq 4\sum_{k=1}^{\infty} k^i \left(q^k - 1\right)^{-1} = O(1).$$

Now we use this information as well as (24) and $H_1(f) = m$ in the formula (21). This yields

$$M_s(f) = \frac{1}{N} E_q(1,f)^s - c_q s \frac{\log N}{N} + O\left(\frac{(\log\log N)^2}{N}\right) + O\left(\frac{1}{\Phi_q(f)}\right).$$

By (17) we have $E_q(1,f) = mT_q + d_q = c_q \log N + d_q$, and [5, Proposition VI.11] yields $\Phi_q(f)^{-1} = O(N^{-1}\log\log(N+1))$. Hence the desired result follows. ■

It follows from (11) and Theorem 4 that if q is prime, every η_{ij} is the identity map, and $s \geq 2$ and $f \in F_q[x]$ with $\deg(f) = m \geq 1$ are fixed, then as $\mathbf{g}$ runs through $G_s(f)$ we get on the average $D_N^*(P(\mathbf{g}, f)) =$

$O(N^{-1}(\log N)^s)$. We note that for the number c_q in Theorem 4 we have the bound

$$c_q < \frac{2}{\pi} + \frac{7}{5\log q} - \frac{1}{q\log q} \quad \text{for} \quad q > 2$$

by [18, p. 574].

If f is irreducible over F_q, then the $c_{jr}^{(i)}$ in (6) can also be represented as follows. Note first that the sequence $u_1^{(i)}, u_2^{(i)}, \ldots$ is a linear recurring sequence with characteristic polynomial f. Thus it follows from [17, Theorem 8.24] that there exist elements $\theta_i, 1 \le i \le s$, in the extension field F_N of order $N = q^m$ such that

$$u_k^{(i)} = \mathrm{Tr}(\theta_i \sigma^{k-1}) \quad \text{for} \quad 1 \le i \le s \quad \text{and} \quad k \ge 1,$$

where Tr is the trace function from F_N to F_q and where σ is a root of f in F_N. Hence (6) attains the form

$$c_{jr}^{(i)} = \mathrm{Tr}(\theta_i \sigma^{r+j-1}) \quad \text{for} \quad 1 \le i \le s, 1 \le j \le m, 0 \le r \le m-1.$$

Consequently, if q is prime, f is irreducible over F_q, and the bijections ψ_r and η_{ij} are identity maps, then the construction of the point sets $P(\mathbf{g}, f)$ is a special case of the construction in [20, p. 161], where in the latter construction we take $\beta_{ij} = \theta_i \sigma^{j-1} \in F_N$ for $1 \le i \le s, 1 \le j \le m$.

In the case $s = 2$ there is a connection between the quantity $\varrho(\mathbf{g}, f)$ in Corollary 1 and continued fractions for rational functions over F_q, where q is again an arbitrary prime power. Let $\mathbf{g} = (g_1, g_2) \in F_q[x]^2$ with $\gcd(g_i, f) = 1$ for $i = 1, 2$. Then the condition $\mathbf{h} \cdot \mathbf{g} = h_1 g_1 + h_2 g_2 \equiv 0 \bmod f$ in Corollary 1 is equivalent to $h_1 + h_2 g_1^* g_2 \equiv 0 \bmod f$, where $g_1^* \in F_q[x]$ with $g_1 g_1^* \equiv 1 \bmod f$. Thus it suffices to consider the quantity $\varrho(\mathbf{g}, f)$ for pairs $\mathbf{g}$ of the form $\mathbf{g} = (1, g)$ with $g \in F_q[x]$ and $\gcd(g, f) = 1$. Let

$$\frac{g}{f} = [A_0; A_1, A_2, \ldots, A_u]$$

be the continued fraction expansion of the rational function g/f, with partial quotients $A_r \in F_q[x]$ satisfying $\deg(A_r) \ge 1$ for $1 \le r \le u$. Put

$$K\left(\frac{g}{f}\right) = \max_{1 \le r \le u} \deg(A_r).$$

Then we have

$$\varrho(\mathbf{g}, f) = m + 2 - K\left(\frac{g}{f}\right), \tag{25}$$

which is shown in exactly the same way as the special case considered in [22, Satz 12]. Thus the desirable $\mathbf{g} = (1, g)$ are those with small $K(g/f)$. The quantity $K(g/f)$ was studied in detail in [23]. It is clear that for any $m \geq 1$ we can obtain a reduced rational function g/f with $K(g/f) = 1$ and $\deg(f) = m$, by choosing partial quotients with $\deg(A_r) = 1$ for $1 \leq r \leq m$. Then from (25) we get $\varrho(\mathbf{g}, f) = m + 1$ for $\mathbf{g} = (1, g)$. With this choice of $\mathbf{g}$ and f we obtain a two-dimensional point set $P(\mathbf{g}, f)$ with $D_N^*(P(\mathbf{g}, f)) = O(N^{-1} \log N)$ according to the discrepancy bound stated after Theorem 3. By a lower bound stated in Section 2 this is the smallest order of magnitude which can be achieved by the discrepancy of a two-dimensional point set.

A construction analogous to that of the point sets $P(\mathbf{g}, f)$ can also be applied to sequences. For this purpose, let $s \geq 1$ be a given dimension and choose irrational $L_1, \ldots, L_s \in F_q((x^{-1}))$, i.e., none of the formal Laurent series $L_i, 1 \leq i \leq s$, should be the expansion of a rational function over F_q. Let

$$L_i = \sum_{k=w_i}^{\infty} u_k^{(i)} x^{-k} \quad \text{for} \quad 1 \leq i \leq s,$$

where $w_i \leq 1$ for $1 \leq i \leq s$. Then define

$$c_{jr}^{(i)} = u_{r+j}^{(i)} \in F_q \quad \text{for} \quad 1 \leq i \leq s, j \geq 1, r \geq 0. \tag{26}$$

With this choice of the elements $c_{jr}^{(i)}$ we then apply the general principle for the construction of sequences described in Section 3. It remains to guarantee that the condition (iv) in Section 3 holds, i.e., that for each n and i we have $y_{nj}^{(i)} < q - 1$ for infinitely many j. The following is a sufficient condition for (iv) to hold. Here η_{ij}^{-1} denotes the inverse map of the bijection η_{ij}.

Lemma 5. *If the bijections η_{ij} are such that $\eta_{ij}^{-1}(q-1)$ is independent of j and $\neq 0$ for all sufficiently large j, then for each n and i we have $y_{nj}^{(i)} < q-1$ for infinitely many j.*

Proof. Suppose that for some n and i we had $y_{nj}^{(i)} = q-1$ for all sufficiently large j. Since for a suitable integer $R(n) \geq 0$ we have $\psi_r(a_r(n)) = 0$ for all

$r > R(n)$, it follows from (26) and the definition of the $y_{nj}^{(i)}$ that

$$\sum_{r=0}^{R(n)} u_{r+j}^{(i)} \psi_r(a_r(n)) = \eta_{ij}^{-1}(q-1) \quad \text{for all sufficiently large } j.$$

By hypothesis there exists a nonzero $m_i \in F_q$ such that $\eta_{ij}^{-1}(q-1) = m_i$ for all sufficiently large j. Thus, with a suitable integer $j_0 \geq 1$ we have

$$\sum_{r=0}^{R(n)} \psi_r(a_r(n)) u_{r+j}^{(i)} = m_i \quad \text{for all} \quad j \geq j_0.$$

Hence, if we put $v_k = u_{k+j_0}^{(i)}$ for $k \geq 0$, then the sequence $v_0, v_1, \ldots$ of elements of F_q satisfies a nontrivial linear recurrence relation and is thus ultimately periodic (see [17, Theorem 8.7]). Consequently, the sequence $u_1^{(i)}, u_2^{(i)}, \ldots$ is ultimately periodic, and so L_i is rational, a contradiction. ■

By analogy with Lemma 4 it is clear that the distribution properties of the sequence constructed from $L_1, \ldots, L_s$ are intimately connected with the simultaneous diophantine approximation character of the elements $L_1, \ldots, L_s$ of the field $F_q((x^{-1}))$, where polynomials over F_q play of course the role of the integers in classical diophantine approximation. These connections will be further explored in later work.

References

[1] J. Beck, Irregularities of distribution and combinatorics, in: *Surveys in Combinatorics 1985,* London Math. Soc. Lecture Note Series, **103**, Cambridge Univ. Press, Cambridge, 1985, 25–46.

[2] J. Beck, A two-dimensional van Aardenne–Ehrenfest theorem in irregularities of distribution, *Compositio Math.* **72**(1989), 269–339.

[3] J. Beck and W. W. L. Chen, *Irregularities of Distribution,* Cambridge Univ. Press, Cambridge, 1987.

[4] R. Béjian and H. Faure, Discrépance de la suite de van der Corput, *C. R. Acad. Sci. Paris Sér. A* **285**(1977), 313–316.

[5] M. Car, Sommes de carrés dans $F_q[X]$, *Dissertationes Math.* **215**(1983).

[6] L. Carlitz, The arithmetic of polynomials in a Galois field, *Amer. J. Math.* **54**(1932), 39-50.

[7] L. Carlitz, The singular series for sums of squares of polynomials, *Duke Math. J.* **14**(1947), 1105-1120.

[8] Y. Dupain and V.T. Sós, On the discrepancy of $(n\alpha)$ sequences, in: *Topics in Classical Number Theory,* (ed.: G. Halász), Colloq. Math. Soc. János Bolyai, **34**, North-Holland, Amsterdam, 1984, 355-387.

[9] H. Faure, Discrépance de suites associées à un système de numération (en dimension s), *Acta Arith.* **41**(1982), 337-351.

[10] G. Halász and V.T. Sós (eds.), *Irregularities of Partitions,* Springer, Berlin, 1989.

[11] J. H. Halton, On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals, *Numer. Math.* **2**(1960), 84–90; Berichtigung, *ibid.* **2**(1960), 196.

[12] D. R. Hayes, The expression of a polynomial as a sum of three irreducibles, *Acta Arith.* **11**(1966), 461-488.

[13] L. K. Hua and Y. Wang, *Applications of Number Theory to Numerical Analysis,* Springer, Berlin, 1981.

[14] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences,* Wiley, New York, 1974.

[15] M. Laczkovich, Equidecomposability and discrepancy; a solution of Tarski's circle-squaring problem, *J. reine angew. Math.* **404**(1990), 77–117.

[16] C. Lécot, Low discrepancy sequences for solving the Boltzmann equation, *J. Comput. Appl. Math.* **25**(1989), 237–249.

[17] R. Lidl and H. Niederreiter, *Finite Fields,* Addison-Wesley, Reading, MA, 1983.

[18] H. Niederreiter, On the distribution of pseudorandom numbers generated by the linear congruential method. III, *Math. Comp.* **30**(1976), 571-597.

[19] H. Niederreiter, Quasi-Monte Carlo methods and pseudo-random numbers, *Bull. Amer. Math. Soc.* **84**(1978), 957-1041.

[20] H. Niederreiter, Low-discrepancy point sets, *Monatsh. Math.* **102**(1986), 155-167.

[21] H. Niederreiter, Multidimensional numerical integration using pseudorandom numbers, in: *Stochastic Programming 84 Part I,* (eds.: A. Prékopa and R.J.-B. Wets), Math. Programming Study, **27**, North-Holland, Amsterdam, 1986, 17–38.

[22] H. Niederreiter, Pseudozufallszahlen und die Theorie der Gleichverteilung, *Sitzungsber. Österr. Akad. Wiss. Math.-Naturwiss. Kl. Abt. II* **195**(1986), 109-138.

[23] H. Niederreiter, Rational functions with partial quotients of small degree in their continued fraction expansion, *Monatsh. Math.* **103**(1987), 269-288.

[24] H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* **104**(1987), 273-337.

[25] H. Niederreiter, Low-discrepancy and low-dispersion sequences, *J. Number Theory* **30**(1988), 51–70.

[26] H. Niederreiter, Quasi-Monte Carlo methods for multidimensional numerical integration, in: *Numerical Integration III* (Oberwolfach, 1987), Internat. Series of Numer. Math., **85**, Birkhäuser, Basel, 1988, 157-171.

[27] H. Niederreiter, Pseudorandom numbers generated from shift register sequences, in: *Number-Theoretic Analysis,* (eds.: E. Hlawka and R. F. Tichy), Lecture Notes in Math., **1452**, Springer, Berlin, 1990, 165–177.

[28] H. Niederreiter, A combinatorial problem for vector spaces over finite fields, *Discrete Math.* to appear.

[29] H. Niederreiter, Recent trends in random number and random vector generation, *Ann. Operations Research* **31**(1991), 323–345.

[30] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods,* SIAM, Philadelphia, to appear.

[31] H. Niederreiter and C. P. Schnorr, Local randomness in polynomial random number and random function generators, *preprint,* Univ. of Frankfurt, 1991.

[32] H. Niederreiter and I. H. Sloan, Lattice rules for multiple integration and discrepancy, *Math. Comp.* **54**(1990), 303–312.

[33] K. F. Roth, On irregularities of distribution, *Mathematika* **1**(1954), 73–79.

[34] W. M. Schmidt, Irregularities of distribution, VII, *Acta Arith.* **21**(1972), 45-50.

[35] J. Schoißengeier, On the discrepancy of $(n\alpha)$, *Acta Arith.* **44**(1984), 241–279.

[36] I. M. Sobol', The distribution of points in a cube and the approximate evaluation of integrals (Russian), *Zh. Vychisl. Mat. i Mat. Fiz.* **7**(1967), 784-802.

[37] V. T. Sós, Irregularities of partitions: Ramsey theory, uniform distribution, in: *Surveys in Combinatorics* (ed.: E. K. Lloyd), London Math. Soc. Lecture Note Series, **82**, Cambridge Univ. Press, Cambridge, 1983, 201–246.

[38] V. T. Sós, On strong irregularities of the distribution of $\{n\alpha\}$ sequences, in: *Studies in Pure Mathematics (To the Memory of Paul Turán)*, Birkhäuser, Basel, 1983, 685–700.

[39] H. Woźniakowski, Average case complexity of multivariate integration, *Bull. Amer. Math. Soc.* **24**(1991), 185–194.

Harald Niederreiter

Institute for Information Processing
Austrian Academy of Sciences
Sonnenfelsgasse 19
A–1010 Vienna
Austria