

## GENERALIZED $(t, s)$ -SEQUENCES, KRONECKER-TYPE SEQUENCES, AND DIOPHANTINE APPROXIMATIONS OF FORMAL LAURENT SERIES

GERHARD LARCHER AND HARALD NIEDERREITER

**ABSTRACT.** The theory of  $(t, s)$ -sequences leads to powerful constructions of low-discrepancy sequences in an  $s$ -dimensional unit cube. We generalize this theory in order to cover arbitrary sequences constructed by the digital method and, in particular, the Kronecker-type sequences introduced by the second author. We define diophantine approximation constants for formal Laurent series over finite fields and show their connection with the distribution properties of Kronecker-type sequences. The main results include probabilistic theorems on the distribution of sequences constructed by the digital method and on the diophantine approximation character of  $s$ -tuples of formal Laurent series over finite fields.

### 1. INTRODUCTION AND BASIC DEFINITIONS

The most effective constructions of low-discrepancy sequences in an  $s$ -dimensional unit cube are currently based on the notion of a  $(t, s)$ -sequence (see [16, Chapter 4]). A  $(t, s)$ -sequence satisfies strong uniformity properties within special finite segments of the sequence (see Definition 2 below for the details). Some constructions of  $(t, s)$ -sequences work with formal Laurent series, in particular a construction introduced in [16, Chapter 4] and studied further by the authors [8]. However, the full range of this construction goes well beyond the framework of  $(t, s)$ -sequences. Thus, to analyze the whole family of sequences obtained by this construction, which is one of the aims of the present paper, it is necessary to generalize the concept of a  $(t, s)$ -sequence in the way described in Definition 3 below. These generalized  $(t, s)$ -sequences should also be of interest in other contexts involving low-discrepancy sequences.

The construction mentioned above not only motivates the definition of generalized  $(t, s)$ -sequences, but it also leads to intriguing connections with the theory of diophantine approximations of formal Laurent series. Some of these connections were already pointed out in [8], but in the present paper we can go much further by introducing and analyzing new diophantine approximation constants for formal Laurent series (see Section 4).

We follow [16] in our basic notation and terminology. For a point set  $P$  consisting of  $N$  arbitrary points  $y_0, y_1, \dots, y_{N-1}$  in the half-open  $s$ -dimensional

---

Received by the editors March 9, 1994 and, in revised form, August 11, 1994.

1991 *Mathematics Subject Classification.* Primary 11J61, 11K38, 11K60.

*Key words and phrases.* Low-discrepancy sequences,  $(t, s)$ -sequences, diophantine approximations of formal Laurent series.

unit cube  $I^s = [0, 1]^s$ ,  $s \geq 1$ , and for an arbitrary subinterval  $J$  of  $I^s$ , let  $A(J; P)$  be the number of  $n$  with  $0 \leq n \leq N - 1$  for which  $y_n \in J$ . Let  $\lambda_s$  denote the  $s$ -dimensional Lebesgue measure.

**Definition 1.** Let  $b \geq 2$ ,  $s \geq 1$ , and  $0 \leq t \leq m$  be integers. Then a point set  $P$  consisting of  $b^m$  points of  $I^s$  forms a  $(t, m, s)$ -net in base  $b$  if  $A(J; P) = b^t$  for every subinterval  $J = \prod_{i=1}^s [a_i b^{-d_i}, (a_i + 1)b^{-d_i})$  of  $I^s$  with integers  $d_i \geq 0$  and  $0 \leq a_i < b^{d_i}$  for  $1 \leq i \leq s$  and with  $\lambda_s(J) = b^{t-m}$ . Furthermore, a  $(t, m, s)$ -net  $P$  in base  $b$  is a *strict*  $(t, m, s)$ -net in base  $b$  if  $P$  is not a  $(u, m, s)$ -net in base  $b$  for some  $u$  with  $0 \leq u < t$ .

**Definition 2.** Let  $b \geq 2$ ,  $s \geq 1$ , and  $t \geq 0$  be integers. Then a sequence  $y_0, y_1, \dots$  of points in  $I^s$  is a  $(t, s)$ -sequence in base  $b$  if for all integers  $k \geq 0$  and  $m > t$  the point set consisting of the  $y_n$  with  $kb^m \leq n < (k+1)b^m$  forms a  $(t, m, s)$ -net in base  $b$ . Furthermore, a  $(t, s)$ -sequence in base  $b$  is a *strict*  $(t, s)$ -sequence in base  $b$  if it is not a  $(u, s)$ -sequence in base  $b$  for some  $u$  with  $0 \leq u < t$ .

Clearly, the uniformity properties of  $(t, s)$ -sequences are the stronger the smaller the value of  $t$ . The “strict” variants in Definitions 1 and 2 have not been considered before. Constructions of  $(t, s)$ -sequences can be found in Faure [2], Niederreiter [10], [11], [12], [16, Chapter 4], Sobol’ [18], and Tezuka [19].

We now generalize Definition 2 by allowing the parameter  $t$  to vary with  $m$ . We write  $\mathbb{N}_0$  for the set of nonnegative integers.

**Definition 3.** Let  $b \geq 2$  and  $s \geq 1$  be integers and let  $T: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  be a function with  $T(m) \leq m$  for all  $m \in \mathbb{N}_0$ . Then a sequence  $y_0, y_1, \dots$  of points in  $I^s$  is a  $(T, s)$ -sequence in base  $b$  if for all  $k, m \in \mathbb{N}_0$  the point set consisting of the  $y_n$  with  $kb^m \leq n < (k+1)b^m$  forms a  $(T(m), m, s)$ -net in base  $b$ .

*Remark 1.* If  $T$  and  $U$  are functions as in Definition 3 with  $T(m) \leq U(m)$  for all  $m \in \mathbb{N}_0$ , then any  $(T, s)$ -sequence in base  $b$  is also a  $(U, s)$ -sequence in base  $b$ . In particular, if  $T$  is such that  $T(m) \leq t \in \mathbb{N}_0$  for all  $m \in \mathbb{N}_0$ , then any  $(T, s)$ -sequence in base  $b$  is a  $(t, s)$ -sequence in base  $b$ .

We note that since any function  $T$  in Definition 3 must satisfy  $T(0) = 0$ , we will often define  $T(m)$  only for  $m \geq 1$ . The following definition generalizes the second part of Definition 2.

**Definition 4.** Let  $b, s$ , and  $T$  be as in Definition 3. Then a  $(T, s)$ -sequence in base  $b$  is called a *strict*  $(T, s)$ -sequence in base  $b$  if it is not a  $(U, s)$ -sequence in base  $b$  for some function  $U: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  with  $U(m) \leq m$  for all  $m \in \mathbb{N}_0$  and  $U(m) < T(m)$  for at least one  $m \in \mathbb{N}_0$ .

We now present a brief overview of the paper. In Section 2 we establish bounds for the star discrepancy  $D_N^*(S)$  of a  $(T, s)$ -sequence  $S$ ; of particular interest are the cases in which  $D_N^*(S) = O(N^{-1}(\log N)^s)$ . The digital method of constructing low-discrepancy sequences is recalled in Section 3, and conditions under which sequences obtained by this method form  $(T, s)$ -sequences are given. We also prove probabilistic results on the average behavior of sequences constructed by the digital method. Various diophantine approximation constants for formal Laurent series over finite fields are introduced and analyzed in

Section 4. The sequences studied in [8] are then shown to be  $(T, s)$ -sequences in Section 5, with the function  $T$  depending on the diophantine approximation constants from Section 4.

## 2. THE STAR DISCREPANCY OF $(T, s)$ -SEQUENCES

We recall that for a point set  $P$  consisting of  $N$  points in  $I^s$  its *star discrepancy* is defined by

$$D_N^*(P) = \sup_J \left| \frac{A(J; P)}{N} - \lambda_s(J) \right|,$$

where the supremum is extended over all subintervals  $J$  of  $I^s$  with one vertex at the origin. For a sequence  $S$  of elements of  $I^s$ , we write  $D_N^*(S)$  for the star discrepancy of the first  $N$  terms of  $S$ .

As in [16, p. 56], we let  $\Delta_b(t, m, s)$  be a number for which

$$ND_N^*(P) \leq \Delta_b(t, m, s)$$

holds for any  $(t, m, s)$ -net  $P$  in base  $b$ , where  $N = b^m$ . Such upper bounds  $\Delta_b(t, m, s)$  are given in great detail in [10, Section 3], [16, Chapter 4]. In particular, we can take

$$(1) \quad \Delta_b(t, m, s) = O(b^t m^{s-1}) \quad \text{for } m \geq 1$$

with an implied constant depending only on  $b$  and  $s$ .

**Lemma 1.** For  $T: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  with  $T(m) \leq m$  for all  $m \in \mathbb{N}_0$  let  $S$  be a  $(T, s)$ -sequence in base  $b$ . Let  $N = \sum_{m=0}^k a_m b^m$  be the digit expansion of the positive integer  $N$  in base  $b$ . Then we have

$$ND_N^*(S) \leq \sum_{m=0}^k a_m \Delta_b(T(m), m, s).$$

*Proof.* This follows immediately from the definition of a  $(T, s)$ -sequence and from the fact that for the star discrepancy  $D_N^*(P)$  of the union  $P$  of two point sets  $P_1$  and  $P_2$  with star discrepancies  $D_L^*(P_1)$  and  $D_M^*(P_2)$ , respectively, and with  $L + M = N$  we have  $ND_N^*(P) \leq LD_L^*(P_1) + MD_M^*(P_2)$  (compare with [4, Chapter 2, Theorem 2.6]).  $\square$

The following bound for the star discrepancy of a  $(T, s)$ -sequence is sometimes sharper with respect to the implied constants, especially if no specific information on  $N$  is available.

**Lemma 2.** For  $T: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  with  $T(m) \leq m$  for all  $m \in \mathbb{N}_0$  let  $S$  be a  $(T, s)$ -sequence in base  $b$ . Given a positive integer  $N$ , let  $k \in \mathbb{N}_0$  be such that  $b^k \leq N < b^{k+1}$  and let  $r \in \mathbb{N}_0$  be maximal such that  $b^r$  divides  $N$ . Then we have

$$\begin{aligned} ND_N^*(S) &\leq \frac{b-1}{2} \sum_{m=r}^k \Delta_b(T(m), m, s) + \frac{1}{2} \Delta_b(T(r), r, s) \\ &\quad + \frac{1}{2} \Delta_b(T(k+1), k+1, s). \end{aligned}$$

*Proof.* The proof is carried out quite analogously to the proof of [10, Lemma 4.1] and by noting that now by definition we always have  $T(m) \leq m$ .  $\square$

By combining now Lemma 1 or Lemma 2 with the known detailed upper bounds  $\Delta_b(t, m, s)$ , we get upper bounds for the star discrepancy of  $(T, s)$ -sequences with explicit constants. Since in the general case we are mainly interested in the *order of magnitude* of the star discrepancy, we do not write down the implied constants, but rather use the bound in Theorem 1(i) below as a fundamental result. Furthermore, we give a condition on  $T$  under which the star discrepancy  $D_N^*(S)$  of a  $(T, s)$ -sequence  $S$  in base  $b$  has the possibly optimal order of magnitude, i.e.,  $D_N^*(S) = O(N^{-1}(\log N)^s)$ . Note that it is a classical conjecture in the theory of uniform distribution of sequences that for every dimension  $s$  there is a constant  $c_s > 0$  such that for any sequence  $S$  of elements of  $I^s$  we have

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

for infinitely many  $N$ . This conjecture has been proved in the case  $s = 1$  by Schmidt [17].

**Theorem 1.** For  $T: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  with  $T(m) \leq m$  for all  $m \in \mathbb{N}_0$  let  $S$  be a  $(T, s)$ -sequence in base  $b$ .

(i) Given an integer  $N \geq b$ , let the integer  $k$  be such that  $b^k \leq N < b^{k+1}$ . Then we have

$$ND_N^*(S) \leq B(b, s) \sum_{m=1}^k b^{T(m)} m^{s-1}$$

with a constant  $B(b, s)$  depending only on  $b$  and  $s$ .

(ii) If the sequence

$$\left( \frac{1}{k} \sum_{m=1}^k b^{T(m)} \right)_{k=1, 2, \dots}$$

is bounded, then we have

$$D_N^*(S) = O(N^{-1}(\log N)^s) \quad \text{for } N \geq 2.$$

*Proof.* (i) This follows immediately by combining Lemma 1 with the bound in (1).

(ii) This follows from part (i) and from  $k \log b \leq \log N$ .  $\square$

**Remark 2.** For a  $(t, s)$ -sequence in base  $b$  the sequence in Theorem 1(ii) is obviously bounded. There are of course also functions  $T$  which are not bounded by some  $t$ , but for which  $k^{-1} \sum_{m=1}^k b^{T(m)}$  is bounded.

**Remark 3.** It is easily seen that  $k^{-s} \sum_{m=1}^k b^{T(m)} m^{s-1}$  is bounded if and only if  $k^{-1} \sum_{m=1}^k b^{T(m)}$  is bounded. The sufficiency was already used in the proof of Theorem 1(ii) and the necessity follows by summation by parts.

### 3. SEQUENCES OBTAINED BY DIGITAL CONSTRUCTIONS

The main method for the construction of  $(t, m, s)$ -nets, of  $(t, s)$ -sequences, and in the following also of  $(T, s)$ -sequences is the method of digital constructions over finite commutative rings with identity, or in short the *digital method*. This method was introduced in [10, Section 6] and was further used e.g. in [11], [12], [14].

We follow [16, Chapter 4] in the description of the digital method for the construction of sequences. Let the integers  $s \geq 1$  and  $b \geq 2$  be given. We write  $Z_b = \{0, 1, \dots, b-1\}$  for the set of digits in base  $b$ . Then we choose the following:

- (i) a commutative ring  $R$  with identity and  $\text{card}(R) = b$ ;
- (ii) bijections  $\psi_r: Z_b \rightarrow R$  for  $r = 0, 1, \dots$ , with  $\psi_r(0) = 0$  for all sufficiently large  $r$ ;
- (iii) bijections  $\eta_{ij}: R \rightarrow Z_b$  for  $i = 1, 2, \dots, s$  and  $j = 1, 2, \dots$ ;
- (iv) elements  $c_{jr}^{(i)} \in R$  for  $1 \leq i \leq s$ ,  $j \geq 1$ , and  $r \geq 0$ .

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

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

be the digit expansion of  $n$  in base  $b$ , where  $a_r(n) \in Z_b$  for  $r \geq 0$  and  $a_r(n) = 0$  for all sufficiently large  $r$ . Then we define the sequence

$$(2) \quad \mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}) \in I^s \quad \text{for } n = 0, 1, \dots$$

by putting

$$x_n^{(i)} = \sum_{j=1}^{\infty} y_{nj}^{(i)} b^{-j} \quad \text{for } n \geq 0 \text{ and } 1 \leq i \leq s,$$

where

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

Here the following condition is assumed to hold:

- (v) for each  $n \geq 0$  and  $1 \leq i \leq s$ , we have  $y_{nj}^{(i)} < b-1$  for infinitely many  $j$ .
- This condition guarantees, in particular, that the points  $\mathbf{x}_n$  in (2) belong to  $I^s = [0, 1)^s$  and not just to  $[0, 1]^s$ . The sequences in (2) constructed by this method are called *digital sequences* constructed over  $R$ . In many cases of practical interest  $R$  is chosen to be a finite field.

**Remark 4.** Note that the above construction method can be symbolically illustrated by the following scheme. (Here we do not explicitly use the identification of the elements of  $R$  and  $Z_b$  by the bijections  $\psi_r$  and  $\eta_{ij}$ ; in most cases we actually have one fixed identification independent of  $i$ ,  $j$ , and  $r$ .) For  $1 \leq i \leq s$  let  $C_i$  be the infinite matrix over  $R$  with rows

$$\mathbf{c}_j^{(i)} = (c_{j0}^{(i)}, c_{j1}^{(i)}, \dots) \quad \text{for } j = 1, 2, \dots$$

Every  $n \geq 0$  with digit expansion  $n = \sum_{r=0}^{\infty} a_r(n) b^r$  in base  $b$  is identified with the infinite column vector

$$\mathbf{n} = \begin{pmatrix} a_0(n) \\ a_1(n) \\ \vdots \end{pmatrix}$$

over  $R$ . Then if

$$C_i \mathbf{n} = \begin{pmatrix} x_n^{(i)}(1) \\ x_n^{(i)}(2) \\ \vdots \end{pmatrix},$$

we set

$$x_n^{(i)} = \sum_{j=1}^{\infty} x_n^{(i)}(j) b^{-j} \quad \text{for } n \geq 0 \text{ and } 1 \leq i \leq s,$$

$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}) \quad \text{for } n \geq 0.$$

**Lemma 3.** *With the notation for the digital method above, suppose that the function  $\mathbf{T}: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  with  $\mathbf{T}(m) \leq m$  for all  $m \in \mathbb{N}_0$  satisfies the following property: for any integers  $m \geq 1$  and  $d_1, \dots, d_s \geq 0$  with  $\sum_{i=1}^s d_i = m - \mathbf{T}(m)$  and any  $f_j^{(i)} \in R$ ,  $1 \leq j \leq d_i$ ,  $1 \leq i \leq s$ , the system of linear equations*

$$\sum_{r=0}^{m-1} c_{jr}^{(i)} z_r = f_j^{(i)} \quad \text{for } 1 \leq j \leq d_i, 1 \leq i \leq s,$$

*in the unknowns  $z_0, \dots, z_{m-1}$  over  $R$  has exactly  $b^{\mathbf{T}(m)}$  solutions. Then the digital sequence  $\mathbf{x}_0, \mathbf{x}_1, \dots$  constructed over  $R$  is a  $(\mathbf{T}, s)$ -sequence in base  $b$ . If, in addition, for all  $m \geq 1$  there are  $d_1, \dots, d_s \geq 0$  with  $\sum_{i=1}^s d_i = m + 1 - \mathbf{T}(m)$  and  $f_j^{(i)} \in R$  such that the above system does not have exactly  $b^{\mathbf{T}(m)-1}$  solutions, then the sequence  $\mathbf{x}_0, \mathbf{x}_1, \dots$  is a strict  $(\mathbf{T}, s)$ -sequence in base  $b$ .*

*Proof.* The arguments in the proof of [16, Theorem 4.35] yield also the present more general result.  $\square$

If the base  $b$  is a prime power  $q$ , then we can take for  $R$  the finite field  $F_q$  of order  $q$ . We can then simplify Lemma 3 by using a notion from [16, Chapter 4] in a notation that suits our purpose.

**Definition 5.** For  $1 \leq i \leq s$  let  $C_i$  be an infinite matrix over the finite field  $F_q$  with rows

$$\mathbf{c}_j^{(i)} = (c_{j0}^{(i)}, c_{j1}^{(i)}, \dots) \quad \text{for } j = 1, 2, \dots$$

For an integer  $m \geq 1$  put

$$\mathbf{c}_j^{(i)}(m) = (c_{j0}^{(i)}, \dots, c_{j,m-1}^{(i)}) \in F_q^m \quad \text{for } j = 1, 2, \dots$$

Then we define  $\varrho_m(C_1, \dots, C_s)$  to be the largest integer  $d$  such that any system  $\{\mathbf{c}_j^{(i)}(m): 1 \leq j \leq d_i, 1 \leq i \leq s\}$  of vectors with  $0 \leq d_i \leq m$  for  $1 \leq i \leq s$  and  $\sum_{i=1}^s d_i = d$  is linearly independent over  $F_q$  (here the empty system is viewed as linearly independent).

**Lemma 4.** *Let  $S$  be an  $s$ -dimensional digital sequence constructed over the finite field  $F_q$  and let the infinite matrices  $C_1, \dots, C_s$  over  $F_q$  be as in Remark 4. Then  $S$  is a strict  $(\mathbf{T}, s)$ -sequence in base  $q$  with*

$$\mathbf{T}(m) = m - \varrho_m(C_1, \dots, C_s) \quad \text{for } m \geq 1.$$

*Proof.* This follows from Lemma 3, Definition 5, and elementary facts of linear algebra.  $\square$

In the following we will prove that digital sequences constructed over  $F_q$  show, on the average, a very good distribution behavior. For this purpose we use a natural measure on the class of all  $s$ -dimensional digital sequences constructed over  $F_q$ . First of all, we note that in view of Lemma 4 the distribution

properties of such a sequence depend only on the matrices  $C_1, \dots, C_s$ . Therefore, we identify the class of all  $s$ -dimensional digital sequences constructed over  $F_q$  with the set  $\mathcal{M}_s$  of all  $s$ -tuples  $(C_1, \dots, C_s)$  of infinite matrices over  $F_q$  (in the notation  $\mathcal{M}_s$  and in some of the following notation, we suppress the dependence on  $q$  for simplicity).

We define the probability measure  $\mu_s$  on  $\mathcal{M}_s$  as the product measure induced by a certain probability measure  $\mu$  on the set  $\mathcal{M}$  of all infinite matrices over  $F_q$ . We can view  $\mathcal{M}$  as the product of denumerably many copies of the sequence space  $F_q^\infty$  over  $F_q$ , and so we define  $\mu$  as the product measure induced by a certain probability measure  $\tilde{\mu}$  on  $F_q^\infty$ .

In view of later investigations of sequences defined via formal Laurent series, we use the following way of introducing the measure  $\tilde{\mu}$ . We identify each  $\mathbf{c} = (c_1, c_2, \dots) \in F_q^\infty$  with its generating function

$$\sum_{k=1}^{\infty} c_k z^{-k} \in F_q((z^{-1})),$$

where  $F_q((z^{-1}))$  is the field of formal Laurent series over  $F_q$  in the variable  $z^{-1}$ . In this way we have identified  $F_q^\infty$  with the set  $H_q$  of all generating functions. With the topology induced by the degree valuation (compare with Section 4) and with respect to addition,  $H_q$  is a compact abelian group, and we define  $\tilde{\mu}$  to be the unique Haar probability measure on  $H_q$ .

The probability measure  $\mu_s$  on  $\mathcal{M}_s$  is thus defined completely. We can now establish the following probabilistic result with respect to  $\mu_s$ . We write  $\mathbb{N}$  for the set of positive integers.

**Theorem 2.** *Let  $\mathbf{D}: \mathbb{N} \rightarrow [0, \infty)$  be such that*

$$\sum_{m=1}^{\infty} \frac{m^{s-1}}{q^{\mathbf{D}(m)}} < \infty.$$

*Then  $\mu_s$ -almost all  $s$ -dimensional digital sequences constructed over the finite field  $F_q$  are  $(\mathbf{T}, s)$ -sequences in base  $q$  with*

$$\mathbf{T}(m) \leq \mathbf{D}(m) + O(1) \quad \text{for all } m \geq 1,$$

*where the implied constant may depend on the sequence.*

*Proof.* We can assume w.l.o.g. that  $\mathbf{D}(m) \in \mathbb{N}_0$  for all  $m \in \mathbb{N}$ . Now we put

$$K_q(s, \mathbf{D}) = \sum_{m=1}^{\infty} \frac{m^{s-1}}{q^{\mathbf{D}(m)}}.$$

For  $M \in \mathbb{N}$  let  $\mathcal{M}_s(\mathbf{D}, M)$  be the set of all  $(C_1, \dots, C_s) \in \mathcal{M}_s$  with the following property: there are  $m \in \mathbb{N}$  and  $d_1, \dots, d_s \in \mathbb{N}_0$  with  $\sum_{i=1}^s d_i = m - \mathbf{D}(m) - M$  such that the vectors  $\mathbf{c}_j^{(i)}(m) \in F_q^m$ ,  $1 \leq j \leq d_i$ ,  $1 \leq i \leq s$ , are linearly dependent over  $F_q$ . Here the  $\mathbf{c}_j^{(i)}(m)$  are as in Definition 5. Then

$$\mu_s(\mathcal{M}_s(\mathbf{D}, M)) \leq \sum_{m=1}^{\infty} \sum_{\substack{d_1, \dots, d_s=0 \\ d_1 + \dots + d_s = m - \mathbf{D}(m) - M}} \sum_{\mathbf{h}} \mu_s(\mathcal{M}_s(\mathbf{h}, m, d_1, \dots, d_s)),$$

where the last sum is extended over all nonzero  $\mathbf{h} = (h_1^{(1)}, \dots, h_{d_1}^{(1)}, \dots, h_1^{(s)}, \dots, h_{d_s}^{(s)}) \in F_q^{m-\mathbf{D}(m)-M}$  and

$$\mathcal{M}_s(\mathbf{h}, m, d_1, \dots, d_s) := \left\{ (C_1, \dots, C_s) \in \mathcal{M}_s : \sum_{i=1}^s \sum_{j=1}^{d_i} h_j^{(i)} \mathbf{c}_j^{(i)}(m) = \mathbf{0} \right\}.$$

Because of  $\mathbf{h} \neq \mathbf{0}$ , the equation

$$\sum_{i=1}^s \sum_{j=1}^{d_i} h_j^{(i)} \mathbf{c}_j^{(i)}(m) = \mathbf{0}$$

determines one of the vectors  $\mathbf{c}_j^{(i)}(m)$  uniquely in terms of the others, and so this vector equation has exactly  $q^{m(m-\mathbf{D}(m)-M-1)}$  solutions. Therefore

$$\mu_s(\mathcal{M}_s(\mathbf{h}, m, d_1, \dots, d_s)) = q^{-m}.$$

It follows that

$$\begin{aligned} \mu_s(\mathcal{M}_s(\mathbf{D}, M)) &\leq \sum_{m=1}^{\infty} \sum_{\substack{d_1, \dots, d_s=0 \\ d_1 + \dots + d_s = m - \mathbf{D}(m) - M}}^{\infty} \sum_{\mathbf{h}} q^{-m} \\ &\leq \sum_{m=1}^{\infty} m^{s-1} q^{m-\mathbf{D}(m)-M} q^{-m} = q^{-M} K_q(s, \mathbf{D}). \end{aligned}$$

Since  $M$  can be chosen arbitrarily large, the result follows now from Lemma 4.  $\square$

*Remark 5.* Theorem 2 implies, for example, that given any  $\varepsilon > 0$ , we have

$$\mathbf{T}(m) \leq (s + \varepsilon) \log_q m + O(1) \quad \text{for all } m \geq 1$$

for  $\mu_s$ -almost all  $s$ -dimensional digital sequences constructed over  $F_q$ , where  $\log_q$  denotes the logarithm to the base  $q$ .

Using Theorem 1(i) and Remark 5, we get that for  $\mu_s$ -almost all  $s$ -dimensional digital sequences  $S$  constructed over  $F_q$  the star discrepancy satisfies

$$D_N^*(S) = O(N^{-1}(\log N)^{2s+\varepsilon})$$

for  $N \geq 2$  and for all  $\varepsilon > 0$ , with an implied constant depending only on  $q$ ,  $s$ ,  $\varepsilon$ , and  $S$ . At least for the case where  $q$  is prime, it may be possible to reduce this probabilistic discrepancy bound to  $O(N^{-1}(\log N)^s(\log \log N)^{2+\varepsilon})$ , by adapting an approach that was developed in [6] for the special class of digital sequences to be described in Section 5; however, this method involves enormous technical complications.

#### 4. DIOPHANTINE APPROXIMATIONS OF FORMAL LAURENT SERIES

Let  $F_q$  again be the finite field of order  $q$  and let  $F_q((z^{-1}))$  be the field of formal Laurent series over  $F_q$  in the variable  $z^{-1}$ . Every element  $L$  of  $F_q((z^{-1}))$  has the form

$$(3) \quad L = \sum_{k=w}^{\infty} u_k z^{-k}$$



with an integer  $w$  and all  $u_k \in F_q$ . The *degree valuation*  $\nu$  on  $F_q((z^{-1}))$  is defined by

$$\nu(L) = \begin{cases} -\min\{k: u_k \neq 0\} & \text{if } L \neq 0, \\ -\infty & \text{if } L = 0. \end{cases}$$

For nonzero polynomials  $Q \in F_q[z]$  we have then  $\nu(Q) = \deg(Q)$ , but for the zero polynomial we use the convention  $\deg(0) = -1$ . If  $L$  is as in (3), then its *fractional part*  $\text{Fr}(L)$  is given by

$$\text{Fr}(L) = \sum_{k=\max(1, w)}^{\infty} u_k z^{-k}.$$

We now introduce the following diophantine approximation constants.

**Definition 6.** Let  $(L_1, \dots, L_s)$  be an  $s$ -tuple of elements of  $F_q((z^{-1}))$  for which  $1, L_1, \dots, L_s$  are linearly independent over the rational function field  $F_q(z)$ . Then we recursively define the integers  $d_h(L_1, \dots, L_s)$ ,  $h = 0, 1, \dots$ , by putting

$$d_0(L_1, \dots, L_s) = 1 - s,$$

$$d_{h+1}(L_1, \dots, L_s)$$

$$= \min \left\{ d > d_h(L_1, \dots, L_s) : \exists Q_1, \dots, Q_s \in F_q[z] \text{ with } \sum_{i=1}^s \deg(Q_i) = d \right. \\ \left. \text{such that } \nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) < \nu \left( \text{Fr} \left( \sum_{i=1}^s R_i L_i \right) \right) \right. \\ \left. \text{for all } R_1, \dots, R_s \in F_q[z] \text{ with } -s < \sum_{i=1}^s \deg(R_i) < d \right\} \\ \text{for } h = 0, 1, \dots$$

Furthermore, we define

$$v_h(L_1, \dots, L_s) = -\min \left\{ \nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) : Q_1, \dots, Q_s \in F_q[z] \right. \\ \left. \text{with } -s < \sum_{i=1}^s \deg(Q_i) < d_{h+1}(L_1, \dots, L_s) \right\} \\ \text{for } h = 0, 1, \dots$$

**Remark 6.** It is clear from Definition 6 that  $(d_h(L_1, \dots, L_s))_{h=0,1,\dots}$  is an increasing sequence of integers  $\geq 1-s$  and that  $(v_h(L_1, \dots, L_s))_{h=0,1,\dots}$  is an increasing sequence of positive integers.

**Remark 7.** In the case  $s = 1$ , i.e., when  $L_1$  is an irrational element of  $F_q((z^{-1}))$ , the numbers  $d_h(L_1)$  and  $v_h(L_1)$  can be expressed in terms of continued fraction parameters. In the standard notation for continued fractions, let

$$L_1 = [A_0; A_1, A_2, \dots]$$

be the continued fraction expansion of  $L_1$ , where the partial quotients  $A_h$ ,  $h = 0, 1, \dots$ , are polynomials over  $F_q$  with  $\deg(A_h) \geq 1$  for  $h \geq 1$ . By using well-known results on continued fractions (see e.g. [16, Appendix B]), we get then the formulas

$$d_h(L_1) = \sum_{i=1}^h \deg(A_i) \quad \text{for } h \geq 1,$$

$$v_h(L_1) = \sum_{i=1}^{h+1} \deg(A_i) \quad \text{for } h \geq 0.$$

**Lemma 5.** *If we also put  $v_{-1}(L_1, \dots, L_s) = 0$ , then*

$$v_h(L_1, \dots, L_s) \geq d_{h+1}(L_1, \dots, L_s) + s - 1 \quad \text{for } h \geq -1.$$

*Proof.* For  $h = -1$  this follows from the definitions, so we can assume  $h \geq 0$  from now on. We claim that for all integers  $N \geq 1 - s$  there exist  $Q_1, \dots, Q_s \in F_q[z]$  with  $-s < \sum_{i=1}^s \deg(Q_i) \leq N$  and

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) \leq -N - s.$$

Choosing then  $N = d_{h+1}(L_1, \dots, L_s) - 1$ , we get

$$-v_h(L_1, \dots, L_s) \leq -N - s = -d_{h+1}(L_1, \dots, L_s) + 1 - s,$$

and the result of the lemma follows.

The above claim can be deduced from the Minkowski linear forms theorem for formal Laurent series established by Mahler [9] (see also Eichler [1]). For the sake of completeness, we include a simple direct proof. For  $L$  as in (3) and  $l \in \mathbb{N}_0$  we put

$$\text{trunc}_l(L) := \sum_{k=\max(1, w)}^l u_k z^{-k}.$$

Now we choose integers  $g_1, \dots, g_s \geq -1$  with  $\sum_{i=1}^s g_i = N$ . Then there are  $q^{N+s}$   $s$ -tuples  $(P_1, \dots, P_s)$  of elements of  $F_q[z]$  with  $\deg(P_i) \leq g_i$  for  $1 \leq i \leq s$ . Consequently, there are two such  $s$ -tuples  $(P_1, \dots, P_s) \neq (R_1, \dots, R_s)$  with

$$\text{trunc}_{N+s-1} \left( \sum_{i=1}^s P_i L_i \right) = \text{trunc}_{N+s-1} \left( \sum_{i=1}^s R_i L_i \right).$$

With  $Q_i := P_i - R_i$  for  $1 \leq i \leq s$  we then get  $-s < \sum_{i=1}^s \deg(Q_i) \leq N$  and

$$\text{trunc}_{N+s-1} \left( \sum_{i=1}^s Q_i L_i \right) = 0,$$

so that

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) \leq -N - s. \quad \square$$

**Definition 7.** For an  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$  and for  $m \in \mathbb{N}_0$  we define  $e_m(L_1, \dots, L_s)$  to be the least integer  $d$  for which there exist  $Q_1, \dots, Q_s \in F_q[z]$  not all 0 with  $\sum_{i=1}^s \deg(Q_i) = d$  and

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) < -m.$$

**Lemma 6.** Let  $(L_1, \dots, L_s)$  be an  $s$ -tuple of elements of  $F_q((z^{-1}))$  for which  $1, L_1, \dots, L_s$  are linearly independent over  $F_q(z)$ . If again  $v_{-1}(L_1, \dots, L_s) = 0$ , then for  $h = 0, 1, \dots$  we have

$$e_m(L_1, \dots, L_s) = d_h(L_1, \dots, L_s) \quad \text{for } v_{h-1}(L_1, \dots, L_s) \leq m < v_h(L_1, \dots, L_s).$$

*Proof.* Fix  $h, m \in \mathbb{N}_0$  with  $v_{h-1}(L_1, \dots, L_s) \leq m < v_h(L_1, \dots, L_s)$ . By the definition of  $v_h(L_1, \dots, L_s)$  there exist  $Q_1, \dots, Q_s \in F_q[z]$  with  $-s < \sum_{i=1}^s \deg(Q_i) < d_{h+1}(L_1, \dots, L_s)$  such that

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) = -v_h(L_1, \dots, L_s).$$

We choose  $Q_1, \dots, Q_s$  such that  $\sum_{i=1}^s \deg(Q_i)$  is minimal. From

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) < -m$$

we conclude that

$$(4) \quad e_m(L_1, \dots, L_s) \leq \sum_{i=1}^s \deg(Q_i)$$

by Definition 7. If we had  $\sum_{i=1}^s \deg(Q_i) > d_h(L_1, \dots, L_s)$ , then it would follow from the definition of  $d_{h+1}(L_1, \dots, L_s)$  that there exist  $R_1, \dots, R_s \in F_q[z]$  with  $-s < \sum_{i=1}^s \deg(R_i) < \sum_{i=1}^s \deg(Q_i)$  such that

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s R_i L_i \right) \right) \leq \nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) = -v_h(L_1, \dots, L_s).$$

The definition of the last number would then imply that

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s R_i L_i \right) \right) = -v_h(L_1, \dots, L_s),$$

which is a contradiction to the minimality of  $\sum_{i=1}^s \deg(Q_i)$ . Thus  $\sum_{i=1}^s \deg(Q_i) \leq d_h(L_1, \dots, L_s)$ , and so (4) yields

$$e_m(L_1, \dots, L_s) \leq d_h(L_1, \dots, L_s).$$

For  $h = 0$  this already shows the result of the lemma, so we can assume  $h \geq 1$  in the rest of the proof. Take any  $P_1, \dots, P_s \in F_q[z]$  not all 0 with

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s P_i L_i \right) \right) < -m \leq -v_{h-1}(L_1, \dots, L_s).$$

Then by the definition of the last number  $\sum_{i=1}^s \deg(P_i) \geq d_h(L_1, \dots, L_s)$ , and so

$$e_m(L_1, \dots, L_s) \geq d_h(L_1, \dots, L_s)$$

in view of Definition 7.  $\square$

**Definition 8.** Let  $\tau: \{1-s, 2-s, \dots\} \rightarrow [1, \infty)$  be a function with  $\lim_{x \rightarrow \infty} \tau(x) = \infty$ . Then an  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$  is said to be of *type*  $\leq \tau$  if

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) \geq -\tau \left( \sum_{i=1}^s \deg(Q_i) \right)$$

for all  $Q_1, \dots, Q_s \in F_q[z]$  that are not all 0. If the function  $\tau$  is of the form  $\tau(x) = \beta x + \gamma$  for some real constants  $\beta \geq 1$  and  $\gamma$ , then  $(L_1, \dots, L_s)$  is said to be of *finite type*  $\leq \beta$ .

**Example.** We can construct  $s$ -tuples of finite type in the following way. Let  $A$  with  $F_q(z) \subseteq A \subseteq F_q((z^{-1}))$  be a Galois extension of  $F_q(z)$  of degree  $m \geq s+1$  and let  $E$  be the integral closure of  $F_q[z]$  in  $A$ . Take any  $L_1, \dots, L_s \in E$  for which  $1, L_1, \dots, L_s$  are linearly independent over  $F_q(z)$ . We claim that  $(L_1, \dots, L_s)$  is of finite type  $\leq m-1$ . For  $Q_1, \dots, Q_s \in F_q[z]$  not all 0 we have

$$\text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) = \sum_{i=1}^s Q_i L_i - P =: L$$

for some  $P \in F_q[z]$ . The linear independence condition implies that  $L \neq 0$ . Put  $G = \text{Gal}(A/F_q(z))$  and  $G^* = G \setminus \{\text{identity}\}$ . Then

$$N_A(L) := \prod_{\sigma \in G} \sigma(L) = L \prod_{\sigma \in G^*} \left( \sum_{i=1}^s Q_i \sigma(L_i) - P \right),$$

and so

$$(5) \quad \nu(N_A(L)) = \nu(L) + \sum_{\sigma \in G^*} \nu \left( \sum_{i=1}^s Q_i \sigma(L_i) - P \right).$$

Because of the nonarchimedean character of  $\nu$  we have

$$\nu(P) \leq \nu \left( \sum_{i=1}^s Q_i L_i \right) \leq \max_{1 \leq i \leq s} (\nu(Q_i) + \nu(L_i)),$$

and so for all  $\sigma \in G^*$ ,

$$\begin{aligned} \nu \left( \sum_{i=1}^s Q_i \sigma(L_i) - P \right) &\leq \max \left( \max_{1 \leq i \leq s} (\nu(Q_i) + \nu(\sigma(L_i))), \nu(P) \right) \\ &\leq \max_{1 \leq i \leq s} \nu(Q_i) + \gamma' = \max_{1 \leq i \leq s} \deg(Q_i) + \gamma' \end{aligned}$$

with

$$\gamma' = \max_{\substack{1 \leq i \leq s \\ \sigma \in G}} \nu(\sigma(L_i)).$$

From  $L_1, \dots, L_s \in E$  we get  $L \in E$ , and so  $N_A(L) \in F_q[z]$ . Furthermore,  $L \neq 0$  implies  $N_A(L) \neq 0$ . Therefore  $\nu(N_A(L)) \geq 0$ ; hence (5) yields

$$\begin{aligned} \nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) &\geq - \sum_{\sigma \in G^*} \nu \left( \sum_{i=1}^s Q_i \sigma(L_i) - P \right) \\ &\geq -(m-1) \max_{1 \leq i \leq s} \deg(Q_i) - (m-1)\gamma' \geq -(m-1) \sum_{i=1}^s \deg(Q_i) - \gamma \end{aligned}$$

for some real constant  $\gamma$ , and the claim is established. We remark that if  $m = s + 1$ , then the above argument shows that

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) \geq -s \max_{1 \leq i \leq s} \deg(Q_i) - s\gamma'$$

for all  $Q_1, \dots, Q_s \in F_q[z]$  that are not all 0, and so we also get an example of an  $s$ -tuple  $(L_1, \dots, L_s)$  that satisfies the hypothesis of [8, Theorem 3]. We note also that this example works not only over  $F_q$ , but also over an arbitrary field of constants.

**Lemma 7.** For an  $s$ -tuple  $(L_1, \dots, L_s)$  of type  $\leq \tau$  we have

$$(6) \quad e_m(L_1, \dots, L_s) \geq \tau^{-1}(m) \quad \text{for all } m \in \mathbb{N}_0,$$

where  $\tau^{-1}(m) := \min\{x \geq 1 - s : \tau(x) > m\}$ . If  $\tau$  is nondecreasing and attains only integer values, then the converse holds also.

*Proof.* By Definition 7, for given  $m \in \mathbb{N}_0$  there exist  $Q_1, \dots, Q_s \in F_q[z]$  not all 0 with  $\sum_{i=1}^s \deg(Q_i) = e_m(L_1, \dots, L_s)$  and

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) < -m.$$

On the other hand, we have

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) \geq -\tau(e_m(L_1, \dots, L_s))$$

by Definition 8. It follows that  $\tau(e_m(L_1, \dots, L_s)) > m$ ; hence we get (6).

For the converse we assume that (6) holds and that  $\tau$  is nondecreasing and attains only integer values. To prove that  $(L_1, \dots, L_s)$  is of type  $\leq \tau$ , we suppose that, on the contrary, there exist  $R_1, \dots, R_s \in F_q[z]$  not all 0 with

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s R_i L_i \right) \right) < -\tau \left( \sum_{i=1}^s \deg(R_i) \right).$$

Put  $d = \sum_{i=1}^s \deg(R_i)$  and  $m = \tau(d)$ ; then

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s R_i L_i \right) \right) < -m,$$

and so Definition 7 yields  $e_m(L_1, \dots, L_s) \leq d$ . In view of (6) we get  $\tau^{-1}(m) \leq d$ . Since  $\tau$  is nondecreasing, we obtain  $\tau(d) > m$ , a contradiction.  $\square$

Let us point out that a probabilistic result on the type of  $s$ -tuples  $(L_1, \dots, L_s)$  will be shown in Theorem 9 in the next section.

## 5. KRONECKER-TYPE SEQUENCES

We investigate a special class of  $s$ -dimensional digital sequences introduced in [16, Chapter 4] and studied further in [6], [8]. The construction of these sequences can be viewed as a function-field analog of the construction of classical  $s$ -dimensional Kronecker sequences, i.e., of sequences of integer multiples mod 1 of a point in  $\mathbb{R}^s$ , and so we use the name “Kronecker-type sequences” for these digital sequences. The main results of this section establish links between the distribution properties of Kronecker-type sequences and the diophantine approximation constants discussed in Section 4.

For our purposes, the most convenient definition of Kronecker-type sequences is the one given originally in [16, Chapter 4] since it fits into the framework of the construction of digital sequences in Section 3. An equivalent definition of Kronecker-type sequences, which shows the analogy with the construction of classical Kronecker sequences, is presented in [8].

Let  $F_q$  again be the finite field of order  $q$ , where  $q$  is an arbitrary prime power. For a given dimension  $s \geq 1$  we choose an  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$ , say

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

where we can assume that  $w_i \leq 1$  for  $1 \leq i \leq s$ . Then we use the construction of digital sequences in Section 3 with  $R = F_q$  and the elements

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

In other words, the matrices  $C_1, \dots, C_s$  in Remark 4 are now the infinite Hankel matrices

$$(7) \quad C_i := \begin{pmatrix} u_1^{(i)} & u_2^{(i)} & u_3^{(i)} & \dots \\ u_2^{(i)} & u_3^{(i)} & u_4^{(i)} & \dots \\ u_3^{(i)} & u_4^{(i)} & u_5^{(i)} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \quad \text{for } 1 \leq i \leq s.$$

We denote the resulting  $s$ -dimensional digital sequence constructed over  $F_q$  by  $S(L_1, \dots, L_s)$ . In this notation we suppress the dependence of the sequence on the chosen bijections  $\psi_r$  and  $\eta_{ij}$  since it will turn out that our results depend only on  $L_1, \dots, L_s$ . According to [16, Lemma 4.47], the following is a sufficient condition for the condition (v) in Section 3:  $L_1, \dots, L_s$  are irrational and for each  $1 \leq i \leq s$  there exists a nonzero  $c_i \in F_q$  such that  $\eta_{ij}(c_i) = q - 1$  for all sufficiently large  $j$ .

The case where  $L_1, \dots, L_s$  are rational corresponds to the construction of point sets in [14] which was further analyzed in [3], [5], [7], [15], [16, Chapter 4]. It was shown by the authors [8] that the sequence  $S(L_1, \dots, L_s)$  is uniformly distributed in  $I^s$  if and only if  $1, L_1, \dots, L_s$  are linearly independent over the rational function field  $F_q(z)$ , so this is clearly the case of main interest, although some results, such as Theorem 3 below, hold generally. In [8] one can

also find a sufficient condition for  $S(L_1, \dots, L_s)$  to be a  $(t, s)$ -sequence in base  $q$  for some  $t \in \mathbb{N}_0$ ; in the language of the present paper, this condition says that the  $s$ -tuple  $(L_1, \dots, L_s)$  is of finite type  $\leq 1$  (compare with Definition 8). A probabilistic result on the discrepancy of  $S(L_1, \dots, L_s)$  was proved by Larcher [6] in the special case where  $q$  is prime. The following general result shows the connection with notions introduced in Sections 1 and 4.

**Theorem 3.** *For every  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$  the sequence  $S(L_1, \dots, L_s)$  is a strict  $(\mathbf{T}, s)$ -sequence in base  $q$  with*

$$\mathbf{T}(m) = m - e_m(L_1, \dots, L_s) - s + 1 \quad \text{for all } m \in \mathbb{N}_0,$$

where  $e_m(L_1, \dots, L_s)$  is as in Definition 7.

*Proof.* In view of Lemma 4 it suffices to determine the numbers  $\varrho_m(C_1, \dots, C_s)$  for  $m \geq 1$ , where  $C_1, \dots, C_s$  are the matrices in (7). By Definition 5 we consider, for given  $m \geq 1$ , the vectors

$$\mathbf{u}_j^{(i)}(m) = (u_j^{(i)}, u_{j+1}^{(i)}, \dots, u_{j+m-1}^{(i)}) \in F_q^m \quad \text{for } 1 \leq i \leq s \text{ and } j \geq 1.$$

The definition of  $e_m(L_1, \dots, L_s)$  implies that there exist  $Q_1, \dots, Q_s \in F_q[z]$  not all 0 with  $\sum_{i=1}^s \deg(Q_i) = e_m(L_1, \dots, L_s)$  and

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s Q_i L_i \right) \right) < -m.$$

Thus, the coefficients of  $z^{-k}$ ,  $1 \leq k \leq m$ , in  $\sum_{i=1}^s Q_i L_i$  are 0. Let

$$Q_i = \sum_{j=1}^{d_i+1} q_j^{(i)} z^{j-1}$$

with  $d_i = \deg(Q_i)$  for  $1 \leq i \leq s$ ; recall that  $\deg(0) = -1$ . Then, by working out the coefficients of  $Q_i L_i$ , we get

$$\sum_{i=1}^s \sum_{j=1}^{d_i+1} q_j^{(i)} u_{j+k-1}^{(i)} = 0 \quad \text{for } 1 \leq k \leq m,$$

and so the vectors  $\mathbf{u}_j^{(i)}(m)$ ,  $1 \leq j \leq d_i + 1$ ,  $1 \leq i \leq s$ , are linearly dependent over  $F_q$ . Therefore  $\sum_{i=1}^s (d_i + 1) \geq \varrho_m(C_1, \dots, C_s) + 1$  by Definition 5; hence

$$e_m(L_1, \dots, L_s) \geq \varrho_m(C_1, \dots, C_s) - s + 1.$$

Now let  $g_1, \dots, g_s \in \mathbb{N}_0$  be such that  $\sum_{i=1}^s g_i = \varrho_m(C_1, \dots, C_s) + 1$  and such that the vectors  $\mathbf{u}_j^{(i)}(m)$ ,  $1 \leq j \leq g_i$ ,  $1 \leq i \leq s$ , are linearly dependent over  $F_q$ . Then there exist  $r_j^{(i)} \in F_q$ ,  $1 \leq j \leq g_i$ ,  $1 \leq i \leq s$ , not all 0 with

$$\sum_{i=1}^s \sum_{j=1}^{g_i} r_j^{(i)} u_{j+k-1}^{(i)} = 0 \quad \text{for } 1 \leq k \leq m.$$

Then with

$$R_i := \sum_{j=1}^{g_i} r_j^{(i)} z^{j-1} \in F_q[z] \quad \text{for } 1 \leq i \leq s$$

we have

$$\nu \left( \text{Fr} \left( \sum_{i=1}^s R_i L_i \right) \right) < -m,$$

and therefore

$$e_m(L_1, \dots, L_s) \leq \sum_{i=1}^s (g_i - 1) = \varrho_m(C_1, \dots, C_s) - s + 1.$$

Thus we have shown

$$\varrho_m(C_1, \dots, C_s) = e_m(L_1, \dots, L_s) + s - 1 \quad \text{for } m \geq 1.$$

Lemma 4 implies that  $S(L_1, \dots, L_s)$  is a strict  $(\mathbf{T}, s)$ -sequence in base  $q$  with

$$\mathbf{T}(m) = m - e_m(L_1, \dots, L_s) - s + 1 \quad \text{for } m \geq 1.$$

Note that this formula for  $\mathbf{T}(m)$  holds also for  $m = 0$  since  $e_0(L_1, \dots, L_s) = 1 - s$ .  $\square$

We now establish connections between  $S(L_1, \dots, L_s)$  and the diophantine approximation constants introduced in Definition 6.

**Theorem 4.** *Let  $(L_1, \dots, L_s)$  be an  $s$ -tuple of elements of  $F_q((z^{-1}))$  for which  $1, L_1, \dots, L_s$  are linearly independent over  $F_q(z)$ .*

(i) *For a constant  $t \in \mathbb{N}_0$ ,  $S(L_1, \dots, L_s)$  is a  $(t, s)$ -sequence in base  $q$  if and only if*

$$(8) \quad v_h(L_1, \dots, L_s) - d_h(L_1, \dots, L_s) \leq s + t \quad \text{for all } h \geq 0.$$

*In particular,  $S(L_1, \dots, L_s)$  is a  $(t, s)$ -sequence in base  $q$  for some  $t \in \mathbb{N}_0$  if and only if  $v_h(L_1, \dots, L_s) - d_h(L_1, \dots, L_s)$  is bounded.*

(ii)  *$S(L_1, \dots, L_s)$  is a  $(0, s)$ -sequence in base  $q$  if and only if*

$$v_h(L_1, \dots, L_s) = h + 1 \quad \text{for all } h \geq 0.$$

*Proof.* (i) By Theorem 3 and Lemma 6,  $S(L_1, \dots, L_s)$  is a  $(\mathbf{T}, s)$ -sequence in base  $q$  with

$$\begin{aligned} \mathbf{T}(m) &= m - e_m(L_1, \dots, L_s) - s + 1 = m - d_h(L_1, \dots, L_s) - s + 1 \\ &\leq v_h(L_1, \dots, L_s) - d_h(L_1, \dots, L_s) - s \end{aligned}$$

for  $v_{h-1}(L_1, \dots, L_s) \leq m < v_h(L_1, \dots, L_s)$  and  $h \geq 0$ . Thus, if (8) holds, then  $S(L_1, \dots, L_s)$  is a  $(t, s)$ -sequence in base  $q$ . Furthermore, we have

$$\mathbf{T}(v_h(L_1, \dots, L_s) - 1) = v_h(L_1, \dots, L_s) - d_h(L_1, \dots, L_s) - s \quad \text{for all } h \geq 0,$$

and so from the strictness property in Theorem 3, if  $S(L_1, \dots, L_s)$  is a  $(t, s)$ -sequence in base  $q$ , then (8) must be satisfied.

(ii) If  $S(L_1, \dots, L_s)$  is a  $(0, s)$ -sequence in base  $q$ , then (8) holds with  $t = 0$ . By combining this inequality with Lemma 5, we get

$$d_{h+1}(L_1, \dots, L_s) - d_h(L_1, \dots, L_s) \leq 1 \quad \text{for all } h \geq 0.$$

By using again (8) with  $t = 0$ , we obtain

$$v_h(L_1, \dots, L_s) \leq d_h(L_1, \dots, L_s) + s \leq h + 1 \quad \text{for all } h \geq 0.$$



In view of Remark 6, this shows that  $v_h(L_1, \dots, L_s) = h + 1$  for all  $h \geq 0$ . Conversely, if  $v_h(L_1, \dots, L_s) = h + 1$  for all  $h \geq 0$ , then (8) trivially holds with  $t = 0$ , and so  $S(L_1, \dots, L_s)$  is a  $(0, s)$ -sequence in base  $q$ .  $\square$

**Corollary 1.** Let  $L_1 \in F_q((z^{-1}))$  be irrational with continued fraction expansion

$$L_1 = [A_0; A_1, A_2, \dots].$$

Then  $S(L_1)$  is a  $(t, 1)$ -sequence in base  $q$  if and only if  $\deg(A_h) \leq t + 1$  for all  $h \geq 1$ .

*Proof.* This follows from Theorem 4(i) and the formulas in Remark 7.  $\square$

Next we show that the distribution properties of  $S(L_1, \dots, L_s)$  can also be expressed in terms of the notion of type introduced in Definition 8.

**Theorem 5.** If the  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$  is of type  $\leq \tau$ , then  $S(L_1, \dots, L_s)$  is a  $(T, s)$ -sequence in base  $q$  with

$$T(m) = m - \tau^{-1}(m) - s + 1 \quad \text{for all } m \in \mathbb{N}_0,$$

where the inverse function  $\tau^{-1}$  of  $\tau$  is defined as in Lemma 7.

*Proof.* This follows by combining Lemma 7 and Theorem 3.  $\square$

**Theorem 6.** For real  $\beta \geq 1$ , an  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$  is of finite type  $\leq \beta$  if and only if  $S(L_1, \dots, L_s)$  is a  $(T, s)$ -sequence in base  $q$  with

$$(9) \quad T(m) \leq \frac{\beta - 1}{\beta} m + O(1) \quad \text{for all } m \in \mathbb{N}_0.$$

*Proof.* If  $(L_1, \dots, L_s)$  is of finite type  $\leq \beta$ , then in the notation of Lemma 7 we have for the corresponding function  $\tau$ ,

$$\tau^{-1}(m) \geq \frac{m}{\beta} + O(1) \quad \text{for all } m \in \mathbb{N}_0.$$

Thus, it follows from Theorem 5 that  $S(L_1, \dots, L_s)$  is a  $(T, s)$ -sequence in base  $q$  with  $T$  satisfying (9). Conversely, suppose that  $S(L_1, \dots, L_s)$  is a  $(T, s)$ -sequence in base  $q$  with  $T$  as in (9). From the strictness property in Theorem 3 we infer that

$$T(m) \geq m - e_m(L_1, \dots, L_s) - s + 1 \quad \text{for all } m \in \mathbb{N}_0,$$

and so

$$e_m(L_1, \dots, L_s) \geq \frac{m}{\beta} + \gamma \quad \text{for all } m \in \mathbb{N}_0,$$

where we can assume that the constant  $\gamma$  satisfies  $\gamma \leq 1 - s$ . Now choose the function

$$\tau(x) = \lfloor \beta(x - \gamma) \rfloor + 1 \quad \text{for integers } x \geq 1 - s.$$

Then  $\tau$  is nondecreasing with  $\tau(1 - s) \geq 1$ . Furthermore, for all  $m \in \mathbb{N}_0$  we have

$$\tau(e_m(L_1, \dots, L_s)) \geq \left\lfloor \beta \left( \frac{m}{\beta} + \gamma - \gamma \right) \right\rfloor + 1 > m;$$

hence  $e_m(L_1, \dots, L_s) \geq \tau^{-1}(m)$ . The second part of Lemma 7 shows now that  $(L_1, \dots, L_s)$  is of type  $\leq \tau$  and so of finite type  $\leq \beta$ .  $\square$

**Corollary 2.** *If the  $s$ -tuple  $(L_1, \dots, L_s)$  of elements of  $F_q((z^{-1}))$  is of finite type  $\leq \beta$ , then the star discrepancy of the first  $N \geq 2$  terms of the sequence  $S(L_1, \dots, L_s)$  satisfies*

$$D_N^*(S(L_1, \dots, L_s)) = \begin{cases} O(N^{-1/\beta}(\log N)^{s-1}) & \text{if } \beta > 1, \\ O(N^{-1}(\log N)^s) & \text{if } \beta = 1, \end{cases}$$

where in both cases the implied constant depends only on  $q, s, \beta$ , and  $(L_1, \dots, L_s)$ .

*Proof.* This follows from Theorem 1(i) and Theorem 6.  $\square$

**Theorem 7.** *Let  $(L_1, \dots, L_s)$  be an  $s$ -tuple of elements of  $F_q((z^{-1}))$  for which  $1, L_1, \dots, L_s$  are linearly independent over  $F_q(z)$ . Put  $d_h = d_h(L_1, \dots, L_s)$  and  $v_h = v_h(L_1, \dots, L_s)$  for  $h \geq 0$ , and let the function  $T$  be such that  $S(L_1, \dots, L_s)$  is a strict  $(T, s)$ -sequence in base  $q$ .*

(i)  $\sum_{m=0}^k q^{T(m)} = O(k)$  if and only if  $\sum_{h=0}^j q^{v_h - d_h} = O(j)$ .

(ii) If  $\sum_{h=0}^j q^{v_h - d_h} = O(j)$ , then

$$D_N^*(S(L_1, \dots, L_s)) = O(N^{-1}(\log N)^s) \quad \text{for } N \geq 2.$$

*Proof.* (i) If we put  $v_{-1} = 0$ , then by Theorem 3 and Lemma 6 we have for  $h \geq 0$ ,

$$T(m) = m - d_h - s + 1 \quad \text{for } v_{h-1} \leq m < v_h.$$

Thus, for  $v_j \leq k < v_{j+1}$ ,  $j \geq 0$ , we obtain

$$(10) \quad \sum_{m=0}^k q^{T(m)} = q^{1-s} \sum_{h=0}^j q^{-d_h} \sum_{m=v_{h-1}}^{v_h-1} q^m + q^{-d_{j+1}-s+1} \sum_{m=v_j}^k q^m.$$

Now we suppose that there exists a constant  $M$  such that

$$\sum_{h=0}^j q^{v_h - d_h} \leq Mj \quad \text{for all } j \geq 1.$$

Then from (10) we get

$$\begin{aligned} \sum_{m=0}^k q^{T(m)} &< \frac{q^{1-s}}{q-1} \sum_{h=0}^j q^{v_h - d_h} + \frac{q^{2-s}}{q-1} q^{k-d_{j+1}} \\ &< \frac{q^{2-s}}{q-1} \sum_{h=0}^{j+1} q^{v_h - d_h} \leq \frac{q^{2-s}}{q-1} M(j+1). \end{aligned}$$

By Remark 6 we have  $v_j \geq j+1$ ; hence

$$\sum_{m=0}^k q^{T(m)} < \frac{q^{2-s}}{q-1} M v_j \leq \frac{q^{2-s}}{q-1} M k,$$

so that one direction is shown. For the converse we assume that there exists a constant  $M_1$  such that

$$\sum_{m=0}^k q^{T(m)} \leq M_1 k \quad \text{for all } k \geq 1.$$

Now we apply (10) with  $k = v_j$ ,  $j \geq 0$ , to obtain

$$(11) \quad \sum_{m=0}^{v_j} q^{T(m)} > q^{-s} \sum_{h=0}^j q^{v_h - d_h} \geq q^{-1} \sum_{h=0}^j q^{v_h - v_{h-1}},$$

where we used Lemma 5 in the second inequality. The arithmetic-geometric means inequality then yields

$$\sum_{m=0}^{v_j} q^{T(m)} > q^{-1} (j+1) \left( \prod_{h=0}^j q^{v_h - v_{h-1}} \right)^{1/(j+1)} = q^{-1} (j+1) q^{v_j/(j+1)}.$$

It follows that

$$\frac{q^{v_j/(j+1)}}{v_j/(j+1)} < \frac{q}{v_j} \sum_{m=0}^{v_j} q^{T(m)} \leq q M_1 \quad \text{for all } j \geq 0.$$

Therefore, the sequence  $(v_j/(j+1))_{j=0,1,\dots}$  is bounded, say  $v_j \leq M_2(j+1)$  for all  $j \geq 0$  with a suitable constant  $M_2$ . Thus, from the first inequality in (11) we get

$$\sum_{h=0}^j q^{v_h - d_h} < q^s \sum_{m=0}^{v_j} q^{T(m)} \leq q^s M_1 v_j \leq q^s M_1 M_2 (j+1)$$

for all  $j \geq 0$ , and so the converse is proved.

(ii) This follows from part (i) and Theorem 1(ii).  $\square$

**Remark 8.** In view of Remark 3, the first condition in Theorem 7(i) can also be replaced by  $\sum_{m=1}^k q^{T(m)} m^{s-1} = O(k^s)$ .

**Remark 9.** For  $s = 1$  the formulas in Remark 7 show that the condition  $\sum_{h=0}^j q^{v_h - d_h} = O(j)$  in Theorem 7 is equivalent to  $\sum_{h=1}^j q^{\deg(A_h)} = O(j)$ , where  $L_1 = [A_0; A_1, A_2, \dots]$  is the continued fraction expansion of the irrational element  $L_1$  of  $F_q((z^{-1}))$ . Therefore, if  $\sum_{h=1}^j q^{\deg(A_h)} = O(j)$ , then  $D_N^*(S(L_1)) = O(N^{-1} \log N)$  for  $N \geq 2$  (this can also be deduced from [8, Theorem 5]). In the case of classical Kronecker sequences in dimension  $s = 1$  there is an analogous result, but in this case the converse holds as well. It is an open question whether the converse holds also for the sequences  $S(L_1)$ .

We now establish an analog of Theorem 2 for sequences of the type  $S(L_1, \dots, L_s)$ . Since these sequences form a set of  $\mu_s$ -measure 0, we have to use another measure. We use the same notation as in Section 3; in particular, we write

$$H_q = \{L \in F_q((z^{-1})) : \nu(L) < 0\}.$$

Furthermore, we note that the sequence  $S(L_1, \dots, L_s)$  and its distribution properties depend only on the fractional parts of  $L_1, \dots, L_s$ . Therefore, we can assume that  $(L_1, \dots, L_s) \in H_q^s$ .

We now let  $\tilde{\mu}$  again be the unique Haar probability measure on  $H_q$ , and we denote by  $\tilde{\mu}_s$  the product measure on  $H_q^s$  induced by  $\tilde{\mu}$ .

**Theorem 8.** Let  $D: \mathbb{N} \rightarrow [0, \infty)$  be such that

$$\sum_{m=1}^{\infty} \frac{m^{s-1}}{q^{D(m)}} < \infty.$$

Then for  $\tilde{\mu}_s$ -almost all  $(L_1, \dots, L_s) \in H_q^s$  the sequence  $S(L_1, \dots, L_s)$  is a  $(\mathbf{T}, s)$ -sequence in base  $q$  with

$$\mathbf{T}(m) \leq \mathbf{D}(m) + O(1) \quad \text{for all } m \geq 1,$$

where the implied constant may depend on  $(L_1, \dots, L_s)$ .

*Proof.* The arguments for the proof of this theorem are quite analogous to those for the proof of Theorem 2. Instead of  $\mathcal{M}_s(\mathbf{D}, M)$  in the proof of Theorem 2 we use here  $\widetilde{\mathcal{M}}_s(\mathbf{D}, M)$ , where the matrices in the  $s$ -tuples  $(C_1, \dots, C_s)$  are restricted to the  $C_i$  of the special form (7). Similarly,  $\widetilde{\mathcal{M}}_s(\mathbf{h}, m, d_1, \dots, d_s)$  is defined in analogy with  $\mathcal{M}_s(\mathbf{h}, m, d_1, \dots, d_s)$ . The system of equations

$$\sum_{i=1}^s \sum_{j=1}^{d_i} h_j^{(i)} \mathbf{c}_j^{(i)}(m) = \mathbf{0}$$

is now a system in the  $(m-1)s + m - \mathbf{D}(m) - M$  variables  $u_1^{(i)}, \dots, u_{m+d_i-1}^{(i)}$ ,  $1 \leq i \leq s$ , of the form

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

The rank of this system is  $m$ , and therefore

$$\tilde{\mu}_s(\widetilde{\mathcal{M}}_s(\mathbf{h}, m, d_1, \dots, d_s)) = q^{-m}.$$

The result of the theorem follows then as in the proof of Theorem 2.  $\square$

**Theorem 9.** For every  $\varepsilon > 0$ ,  $\tilde{\mu}_s$ -almost all  $s$ -tuples  $(L_1, \dots, L_s) \in H_q^s$  are of type  $\leq \tau$  with

$$\tau(x) = x + (s + \varepsilon) \log_q(x + s) + O(1) \quad \text{for } x \geq 1 - s,$$

where  $\log_q$  denotes the logarithm to the base  $q$  and the implied constant depends only on  $q, s, \varepsilon$ , and  $(L_1, \dots, L_s)$ . In particular,  $\tilde{\mu}_s$ -almost all  $(L_1, \dots, L_s) \in H_q^s$  are of finite type  $\leq 1 + \varepsilon$  for all  $\varepsilon > 0$ .

*Proof.* For a fixed  $\varepsilon > 0$  we put

$$\mathbf{D}(m) = \left(s + \frac{\varepsilon}{2}\right) \log_q m \quad \text{for } m \in \mathbb{N}.$$

Then Theorem 8 implies that for  $\tilde{\mu}_s$ -almost all  $(L_1, \dots, L_s) \in H_q^s$  the sequence  $S(L_1, \dots, L_s)$  is a  $(\mathbf{T}, s)$ -sequence in base  $q$  with

$$\mathbf{T}(m) \leq \mathbf{D}(m) + O(1) \quad \text{for all } m \in \mathbb{N}.$$

Now we fix such an  $s$ -tuple  $(L_1, \dots, L_s)$  and we note that the strictness property in Theorem 3 yields

$$\mathbf{T}(m) \geq m - e_m(L_1, \dots, L_s) - s + 1 \quad \text{for all } m \in \mathbb{N}_0.$$

Therefore

$$(12) \quad e_m(L_1, \dots, L_s) \geq m - \mathbf{D}(m) + \gamma \quad \text{for all } m \in \mathbb{N}$$

with a suitable constant  $\gamma$ . Now we put

$$\tau_1(x) = x + \lfloor (s + \varepsilon) \log_q(x + s) \rfloor + \gamma_1 \quad \text{for } x \geq 1 - s,$$

where the integer  $\gamma_1 \geq s$  is determined later. We note that  $\tau_1$  is nondecreasing with  $\tau_1(1-s) \geq 1$ . Next let  $m \in \mathbb{N}$  be so large that

$$(13) \quad m - \mathbf{D}(m) + \gamma \geq 1 - s.$$

Then using (12) we obtain

$$\begin{aligned} \tau_1(e_m(L_1, \dots, L_s)) &\geq \tau_1(m - \mathbf{D}(m) + \gamma) \\ &= m - \left(s + \frac{\varepsilon}{2}\right) \log_q m + \gamma + \lfloor (s + \varepsilon) \log_q(m - \mathbf{D}(m) + \gamma + s) \rfloor + \gamma_1 > m \end{aligned}$$

for all  $m \in \mathbb{N}$  satisfying (13), if  $\gamma_1$  is chosen sufficiently large. For the remaining  $m \in \mathbb{N}_0$  we have

$$\tau_1(e_m(L_1, \dots, L_s)) > m$$

if  $\gamma_1$  is sufficiently large. Thus, with a suitable choice of  $\gamma_1$  we get

$$\tau_1(e_m(L_1, \dots, L_s)) > m \quad \text{for all } m \in \mathbb{N}_0,$$

and so

$$e_m(L_1, \dots, L_s) \geq \tau_1^{-1}(m) \quad \text{for all } m \in \mathbb{N}_0.$$

Therefore, the second part of Lemma 7 shows that  $(L_1, \dots, L_s)$  is of type  $\leq \tau_1$ , and the desired result follows.  $\square$

If we choose the function  $\mathbf{D}$  as in the proof of Theorem 9, then we obtain from Theorem 1(i) and Theorem 8 that for  $\tilde{\mu}_s$ -almost all  $(L_1, \dots, L_s) \in H_q^s$  the star discrepancy of the sequence  $S(L_1, \dots, L_s)$  satisfies

$$D_N^*(S(L_1, \dots, L_s)) = O(N^{-1}(\log N)^{2s+\varepsilon})$$

for  $N \geq 2$  and for all  $\varepsilon > 0$ , where the implied constant depends only on  $q$ ,  $s$ ,  $\varepsilon$ , and  $(L_1, \dots, L_s)$ . For  $s = 1$  a sharper result was shown in [8, Theorem 6]. In the case where  $q$  is prime and  $s \geq 2$  is arbitrary, Larcher [6] has proved by a completely different method that this probabilistic discrepancy bound can be reduced to  $O(N^{-1}(\log N)^s(\log \log N)^{2+\varepsilon})$ .

Finally, we prove a probabilistic result on the growth rate of  $v_h(L_1, \dots, L_s) - d_h(L_1, \dots, L_s)$ . This is a generalization of probabilistic results on the growth rate of the degrees of the partial quotients in the continued fraction expansion of a single formal Laurent series  $L_1$  (compare with [13]).

**Theorem 10.** *For  $\tilde{\mu}_s$ -almost all  $s$ -tuples  $(L_1, \dots, L_s) \in H_q^s$  we have for all  $\varepsilon > 0$  that*

$$v_h(L_1, \dots, L_s) - d_h(L_1, \dots, L_s) \leq (s + \varepsilon) \log_q h + O(1) \quad \text{for } h \geq 1,$$

where the implied constant depends only on  $q$ ,  $s$ ,  $\varepsilon$ , and  $(L_1, \dots, L_s)$ .

*Proof.* We first fix  $\varepsilon > 0$  and choose the function  $\mathbf{D}$  as in the proof of Theorem 9. Then for  $\tilde{\mu}_s$ -almost all  $(L_1, \dots, L_s) \in H_q^s$  we have the inequality (12). We fix such an  $s$ -tuple  $(L_1, \dots, L_s)$ , and for  $h \geq 0$  we use the abbreviations  $d_h = d_h(L_1, \dots, L_s)$  and  $v_h = v_h(L_1, \dots, L_s)$ . Now for  $h \geq 1$  we put  $m = v_h - 1$  in (12), and together with Lemma 6 this yields

$$d_h \geq v_h - 1 - \mathbf{D}(v_h - 1) + \gamma.$$

Consequently we get

$$(14) \quad v_h - d_h \leq \mathbf{D}(v_h) + \gamma_1 \quad \text{for all } h \geq 1$$

with some constant  $\gamma_1$ . Setting  $v_{-1} = 0$ , we deduce  $v_h - d_h \geq v_h - v_{h-1}$  for  $h \geq 0$  from Lemma 5, and so

$$\begin{aligned} v_h &\leq \sum_{j=0}^h (v_j - d_j) \leq \sum_{j=1}^h (\mathbf{D}(v_j) + \gamma_1) + O(1) \\ &\leq h\mathbf{D}(v_h) + O(h) = O(h \log v_h) \end{aligned}$$

for  $h \geq 1$ . Now we put

$$\delta = \frac{\varepsilon/2}{s + \varepsilon}.$$

Then  $v_h = O(hv_h^\delta)$ ; hence

$$v_h \leq \gamma_2 h^{1/(1-\delta)} \quad \text{for all } h \geq 1$$

with a suitable constant  $\gamma_2$ . It follows then from (14) that

$$\begin{aligned} v_h - d_h &\leq \left(s + \frac{\varepsilon}{2}\right) \log_q v_h + O(1) \leq \left(s + \frac{\varepsilon}{2}\right) \log_q (\gamma_2 h^{1/(1-\delta)}) + O(1) \\ &= (s + \varepsilon) \log_q h + O(1) \end{aligned}$$

for all  $h \geq 1$ . By letting  $\varepsilon$  run through a sequence converging to 0 through positive values, we get the final result.  $\square$

*Remark 10.* If we put  $s = 1$  in Theorem 10 and combine the result with the formulas in Remark 7, then we obtain that for  $\tilde{\mu}$ -almost all  $L_1 \in H_q$  we have

$$\deg(A_h) \leq (1 + \varepsilon) \log_q h + O(1)$$

for all  $h \geq 1$  and  $\varepsilon > 0$ , where the implied constant depends only on  $q$ ,  $\varepsilon$ , and  $L_1$ . This result should be compared with [13, Theorem 6].

## REFERENCES

1. M. Eichler, *Ein Satz über Linearformen in Polynombereichen*, Arch. Math. **10** (1959), 81–84.
2. H. Faure, *Discrepance de suites associées à un système de numération (en dimension  $s$ )*, Acta Arith. **41** (1982), 337–351.
3. T. Hansen, G. L. Mullen, and H. Niederreiter, *Good parameters for a class of node sets in quasi-Monte Carlo integration*, Math. Comp. **61** (1993), 225–234.
4. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley, New York, 1974.
5. G. Larcher, *Nets obtained from rational functions over finite fields*, Acta Arith. **63** (1993), 1–13.
6. ———, *On the distribution of an analog to classical Kronecker sequences*, J. Number Theory (to appear).
7. G. Larcher, A. Lauß, H. Niederreiter, and W. Ch. Schmid, *Optimal polynomials for  $(t, m, s)$ -nets and numerical integration of multivariate Walsh series*, SIAM J. Numer. Anal. (to appear).
8. G. Larcher and H. Niederreiter, *Kronecker-type sequences and nonarchimedean diophantine approximations*, Acta Arith. **63** (1993), 379–396.
9. K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series*, Ann. of Math. (2) **42** (1941), 488–522.
10. H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273–337.
11. ———, *Quasi-Monte Carlo methods for multidimensional numerical integration*, Numerical Integration III (H. Braß and G. Hämmerlin, eds.), Internat. Ser. Numer. Math., vol. 85, Birkhäuser, Basel, 1988, pp. 157–171.

12. ———, *Low-discrepancy and low-dispersion sequences*, J. Number Theory **30** (1988), 51–70.
13. ———, *The probabilistic theory of linear complexity*, Advances in Cryptology—EURO-CRYPT '88, (C. G. Günther) Lecture Notes in Computer Sci., vol. 330, Springer, Berlin, 1988, pp. 191–209.
14. ———, *Low-discrepancy point sets obtained by digital constructions over finite fields*, Czechoslovak Math. J. **42** (1992), 143–166.
15. ———, *Constructions of low-discrepancy point sets and sequences*, Sets, Graphs, and Numbers (Budapest, 1991), Colloq. Math. Soc. János Bolyai, vol. 60, North-Holland, Amsterdam, 1992, pp. 529–559.
16. ———, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992.
17. W. M. Schmidt, *Irregularities of distribution*. VII, Acta Arith. **21** (1972), 45–50.
18. I. M. Sobol', *The distribution of points in a cube and the approximate evaluation of integrals*, Zh. Vychisl. Mat. i Mat. Fiz. **7** (1967), 784–802. (Russian)
19. S. Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Modeling and Computer Simulation **3** (1993), 99–107.

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT SALZBURG, HELLBRUNNERSTRASSE 34, A-5020 SALZBURG, AUSTRIA

INSTITUT FÜR INFORMATIONSVERARBEITUNG, ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN, SONNENFELSGASSE 19, A-1010 WIEN, AUSTRIA  
E-mail address: nied@qiinfo.oeaw.ac.at