ACTA ARITHMETICA
LXIII.4 (1993)

Kronecker-type sequences and nonarchimedean diophantine approximations

by

Gerhard Larcher (Salzburg) and Harald Niederreiter (Wien)

1. Introduction. A classical *Kronecker sequence* is a sequence of integer multiples of a point in $\mathbb{R}^s$ which are considered modulo 1. Thus, if $(\alpha_1, \ldots, \alpha_s) \in \mathbb{R}^s$, $s \geq 1$, then the corresponding Kronecker sequence is defined by

$$\mathbf{x}_n = (\{n\alpha_1\}, \ldots, \{n\alpha_s\}), \quad n = 0, 1, \ldots,$$

where $\{u\}$ is the fractional part of $u \in \mathbb{R}$. It is well known that the sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ is uniformly distributed in $\bar{I}^s = [0,1]^s$ if and only if $1, \alpha_1, \ldots, \alpha_s$ are linearly independent over $\mathbb{Q}$, and that the finer quantitative description of the distribution behavior of this sequence depends on the diophantine approximation character of the point $(\alpha_1, \ldots, \alpha_s)$; compare with [6].

In this paper we study sequences of points in $\bar{I}^s$ that are obtained by a construction reminiscent of that of classical Kronecker sequences, but which operates in a function field setting. This construction was introduced in Niederreiter [17, Chapter 4], and the resulting sequences have attractive distribution properties. The detailed investigation of these Kronecker-type sequences that we carry out in the present work leads to interesting connections with nonarchimedean diophantine approximations. The construction belongs to the framework of the theory of (t, m, s)-nets and (t, s)-sequences, which are point sets and sequences, respectively, with special uniformity properties.

We follow [17] in the notation and terminology. For a point set P consisting of N arbitrary points $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1}$ in $\bar{I}^s$ and for an arbitrary subset B of $\bar{I}^s$, let $A(B; P)$ be the number of n with $0 \leq n \leq N-1$ for which $\mathbf{y}_n \in B$. Let an integer $b \geq 2$ be fixed, and let λ_s denote the s-dimensional Lebesgue measure. A subinterval E of $I^s = [0,1)^s$ of the form

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

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ is called an *elementary interval in base* b.

DEFINITION 1. Let $0 \leq t \leq m$ be integers. A (t, m, s)-*net in base* b is a point set P of b^m points in I^s such that $A(E; P) = b^t$ for every elementary interval E in base b with $\lambda_s(E) = b^{t-m}$.

DEFINITION 2. Let $t \geq 0$ be an integer. A sequence $\mathbf{y}_0, \mathbf{y}_1, \ldots$ 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 $\mathbf{y}_n$ with $kb^m \leq n < (k+1)b^m$ is a (t, m, s)-net in base b.

Constructions of (t, m, s)-nets and (t, s)-sequences have been given by Faure [4], Niederreiter [12], [13], [14], [16], and Sobol' [21]. An expository account of these constructions can be found in [17, Chapter 4]. The Kronecker-type sequences that we investigate can be viewed as the sequence analogs of the point sets introduced and analyzed in Niederreiter [16] (see also Larcher [10] for further results on these point sets). These point sets are obtained from rational functions over finite fields and, as the recent calculations of Hansen, Mullen, and Niederreiter [5] have shown, possess excellent distribution properties if the parameters in the construction are chosen suitably; in particular, this family of point sets includes (t, m, s)-nets with relatively small values of t.

For an arbitrary prime power q, let F_q be the finite field of order q, let $F_q(z)$ be the rational function field over F_q, and let $\mathfrak{C}_q$ be the completion of $F_q(z)$ with respect to the unique infinite prime of $F_q(z)$. Every element L of $\mathfrak{C}_q$ has a unique expansion into a formal Laurent series

$$L = \sum_{k=w}^{\infty} u_k z^{-k} \tag{1}$$

with an integer w and all $u_k \in F_q$. The degree valuation ν on $\mathfrak{C}_q$ is defined by $\nu(L) = -\infty$ if $L = 0$ and $\nu(L) = -w$ if $L \neq 0$ and (1) is written in such a way that $u_w \neq 0$. If L is as in (1), then its *fractional part* is defined by

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

For a given dimension $s \geq 1$ the construction of Kronecker-type sequences in [17] can now be described as follows.

Let $Z_q = \{0, 1, \ldots, q-1\}$ be the set of digits in base q. For $r = 0, 1, \ldots$ we choose bijections $\psi_r : Z_q \to F_q$ with $\psi_r(0) = 0$, and for $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots$ we choose bijections $\eta_{ij} : F_q \to Z_q$. Furthermore, we choose

s elements $L_1, \ldots, L_s$ of $\mathfrak{C}_q$, say

$$L_i = \sum_{k=w_i}^{\infty} u_k^{(i)} z^{-k} \quad \text{for } 1 \le i \le s\,, \tag{2}$$

where we can assume that $w_i \le 1$ for $1 \le i \le s$. For $n = 0, 1, \ldots$ let

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

be the digit expansion of n in base q. For $n \ge 0$, $j \ge 1$, and $1 \le i \le s$ we put

$$y_{nj}^{(i)} = \eta_{ij} \Big(\sum_{r=0}^{m(n)} u_{r+j}^{(i)} \psi_r(a_r(n)) \Big) \in Z_q\,, \tag{3}$$

and for $n \ge 0$ and $1 \le i \le s$ we put

$$x_n^{(i)} = \sum_{j=1}^{\infty} y_{nj}^{(i)} q^{-j}\,. \tag{4}$$

We now define the sequence

$$\mathbf{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in \bar{I}^s \quad \text{for } n = 0, 1, \ldots \tag{5}$$

The results that we establish for the sequence (5) depend only on the choice of $L_1, \ldots, L_s$ in the above construction, and so we denote this sequence by $S(L_1, \ldots, L_s)$; thus, in this notation we suppress the dependence of the sequence on the chosen bijections ψ_r and η_{ij}.

An equivalent and somewhat more convenient description of the sequence (5) can be given as follows. With every $n = 0, 1, \ldots$ we associate the polynomial

$$n(z) = \sum_{r=0}^{m(n)} \psi_r(a_r(n)) z^r \in F_q[z]\,, \tag{6}$$

and if $L \in \mathfrak{C}_q$ is as in (1), then we define

$$\eta^{(i)}(L) = \sum_{k=\max(1,w)}^{\infty} \eta_{ik}(u_k) q^{-k} \quad \text{for } 1 \le i \le s\,. \tag{7}$$

Using (2), (3), and (4) and a straightforward calculation, we see that

$$x_n^{(i)} = \eta^{(i)}(n(z) L_i(z)) \quad \text{for } n \ge 0 \text{ and } 1 \le i \le s\,.$$

Therefore the sequence $S(L_1, \ldots, L_s)$ is also described by

$$\mathbf{x}_n = (\eta^{(1)}(n(z) L_1(z)), \ldots, \eta^{(s)}(n(z) L_s(z))) \quad \text{for } n = 0, 1, \ldots \tag{8}$$

In Section 2 we prove a criterion for the uniform distribution in $\bar{I}^s$ of the sequence $S(L_1, \ldots, L_s)$ which is quite analogous to the criterion for a classical Kronecker sequence. In Section 3 we establish connections between the diophantine approximation character of the s-tuple $(L_1, \ldots, L_s)$ and bounds for the star discrepancy and the isotropic discrepancy of the sequence $S(L_1, \ldots, L_s)$. In low-dimensional cases there are relations with the theory of continued fractions for elements of $\mathfrak{C}_q$; these connections are explored in Section 4.

2. Criterion for uniform distribution. Recall that a sequence $\mathbf{y}_0, \mathbf{y}_1, \ldots$ of points in $\bar{I}^s$ is called *uniformly distributed* in $\bar{I}^s$ if

$$\lim_{N\to\infty} \frac{A(J; P_N)}{N} = \lambda_s(J) \tag{9}$$

holds for every subinterval J of $\bar{I}^s$, where P_N is the point set consisting of $\mathbf{y}_0$, $\mathbf{y}_1, \ldots, \mathbf{y}_{N-1}$.

We now investigate the sequence $S(L_1, \ldots, L_s)$ with regard to the property of uniform distribution in $\bar{I}^s$. An easy case arises if one of the L_i is a rational function over F_q. Then it follows immediately from the description (8) of $S(L_1, \ldots, L_s)$ that in the corresponding coordinate of the points $\mathbf{x}_n$ we can have only finitely many possible values, and so $S(L_1, \ldots, L_s)$ cannot be uniformly distributed in $\bar{I}^s$.

Thus, we can assume that $L_1, \ldots, L_s$ are irrational. We also impose the condition that for each $1 \le i \le s$ there exists a nonzero $c_i \in F_q$ such that $\eta_{ij}(c_i) = q - 1$ for all sufficiently large j. These conditions are *standing hypotheses* throughout the rest of the paper. According to [17, Lemma 4.47], these conditions imply that for each $n \ge 0$ and $1 \le i \le s$ we have $y_{nj}^{(i)} < q-1$ for infinitely many j. In particular, all points $\mathbf{x}_n$ of $S(L_1, \ldots, L_s)$ lie in I^s, and so it suffices to check (9) for all subintervals J of I^s.

THEOREM 1. *The sequence $S(L_1, \ldots, L_s)$ is uniformly distributed in $\bar{I}^s$ if and only if $1, L_1, \ldots, L_s$ are linearly independent over $F_q(z)$.*

Proof. We can write the L_i in the form

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

with $w \le 1$. Now $1, L_1, \ldots, L_s$ are linearly dependent over $F_q(z)$ if and only if there exist polynomials $g_1, \ldots, g_s \in F_q[z]$, not all 0, such that $\sum_{i=1}^{s} g_i L_i \in F_q[z]$. If we write

$$g_i = \sum_{k=0}^{m} g_k^{(i)} z^k \quad \text{for } 1 \le i \le s$$

and some $m \geq 0$, then the latter condition is equivalent to

$$\sum_{i=1}^{s} \sum_{k=0}^{m} g_k^{(i)} u_{r+k}^{(i)} = 0 \quad \text{for } r = 1, 2, \ldots$$

With

$$\mathbf{u}_k^{(i)} = (u_k^{(i)}, u_{k+1}^{(i)}, \ldots) \in F_q^{\infty} \quad \text{for } 1 \leq i \leq s \text{ and } k \geq 1$$

it follows that $1, L_1, \ldots, L_s$ are linearly dependent over $F_q(z)$ if and only if for some $m \geq 1$ the vectors $\mathbf{u}_k^{(i)}$, $1 \leq i \leq s$, $1 \leq k \leq m$, are linearly dependent over F_q.

Now let $1, L_1, \ldots, L_s$ be linearly dependent over $F_q(z)$. Then, without loss of generality, let $\mathbf{u}_k^{(i)}$, $1 \leq k \leq m_i$, $1 \leq i \leq s$, be linearly independent over F_q and $\mathbf{u}_k^{(i)}$, $1 \leq k \leq m_1 + 1$ for $i = 1$ and $1 \leq k \leq m_i$ for $2 \leq i \leq s$, be linearly dependent over F_q. Then for all $h \geq 0$ and all $a_0, \ldots, a_h \in Z_q$ the value

$$\mathbf{u}_{m_1+1}^{(1)} (\psi_0(a_0), \ldots, \psi_h(a_h), 0, 0, \ldots)^T$$

is uniquely determined by the values

$$\mathbf{u}_k^{(i)} (\psi_0(a_0), \ldots, \psi_h(a_h), 0, 0, \ldots)^T \quad \text{for } 1 \leq k \leq m_i, 1 \leq i \leq s\,.$$

Therefore, for example, in $q-1$ of the q intervals

$$[dq^{-m_1-1},\ (d+1)q^{-m_1-1}) \times \prod_{i=2}^{s} [0, q^{-m_i})\,, \qquad d = 0, 1, \ldots, q-1\,,$$

there never is a point of the sequence $S(L_1, \ldots, L_s)$, and so $S(L_1, \ldots, L_s)$ is not uniformly distributed in $\bar{I}^s$.

Let now $1, L_1, \ldots, L_s$ be linearly independent over $F_q(z)$. Take any $\varepsilon > 0$, and choose $m \geq 1$ such that $q^{-m} < \varepsilon$. The vectors $\mathbf{u}_k^{(i)}$, $1 \leq i \leq s$, $1 \leq k \leq m$, are linearly independent over F_q, and so for some integer $h \geq 1$ the vectors

$$\text{(10)} \qquad \mathbf{u}_k^{(i)}(h) = (u_k^{(i)}, u_{k+1}^{(i)}, \ldots, u_{k+h-1}^{(i)}) \in F_q^h\,, \qquad 1 \leq i \leq s, 1 \leq k \leq m\,,$$

are linearly independent over F_q. We consider the points $\mathbf{x}_n$ with $Bq^h \leq n < (B+1)q^h$, where $B \geq 0$ is an integer. Then

$$n = b_t q^t + \ldots + b_h q^h + a_{h-1} q^{h-1} + \ldots + a_0$$

with certain fixed $b_j \in Z_q$ and with $a_0, \ldots, a_{h-1}$ ranging freely over Z_q. For all $c_k^{(i)} \in F_q$, $1 \leq i \leq s$, $1 \leq k \leq m$, the system

$$\mathbf{u}_k^{(i)} \cdot (0, \ldots, 0, \psi_h(b_h), \ldots, \psi_t(b_t), 0, 0, \ldots)^T$$
$$+ \mathbf{u}_k^{(i)}(h) \cdot (\psi_0(a_0), \ldots, \psi_{h-1}(a_{h-1}))^T = c_k^{(i)}\,, \qquad 1 \leq i \leq s, 1 \leq k \leq m\,,$$

has exactly q^{h-ms} solutions $(a_0, \ldots, a_{h-1}) \in Z_q^h$.

We now consider a subinterval J' of I^s of the form

$$J' = \prod_{i=1}^{s} [D_i q^{-m}, \ (D_i + E_i) q^{-m})$$

with integers D_i, E_i satisfying $0 \le D_i < D_i + E_i \le q^m$ for $1 \le i \le s$. Let $Mq^h \le N < (M+1)q^h$ for some integer $M \ge 1$. Then of the points $\mathbf{x}_n$, $n = 0, 1, \ldots, N-1$, forming the point set P_N there are at least $Mq^h E_1 \ldots E_s q^{-ms}$ and at most $(M+1)q^h E_1 \ldots E_s q^{-ms}$ in J'. Therefore

$$\left| \frac{A(J'; P_N)}{N} - \lambda_s(J') \right| \le E_1 \ldots E_s q^{-ms} M^{-1} \le M^{-1} < \varepsilon$$

if N is large enough. Since for every subinterval J of I^s we can find subintervals J_1, J_2 of the above type with $J_1 \subseteq J \subseteq J_2$ and $\lambda_s(J_2 \backslash J_1) \le 2s\varepsilon$, it follows that $S(L_1, \ldots, L_s)$ is uniformly distributed in $\bar{I}^s$. ∎

3. Discrepancy bounds. For those sequences $S(L_1, \ldots, L_s)$ that are uniformly distributed in $\bar{I}^s$, we may ask for a more precise description of their distribution behavior by means of discrepancy bounds. Recall that for a point set P consisting of N points in $\bar{I}^s$ 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 over all subintervals J of $\bar{I}^s$ with one vertex at the origin, and its *isotropic discrepancy* is defined by

$$J_N(P) = \sup_C \left| \frac{A(C; P)}{N} - \lambda_s(C) \right|,$$

where the supremum is over all convex subsets C of $\bar{I}^s$. For a sequence S of elements of $\bar{I}^s$, we write $D_N^*(S)$ for the star discrepancy and $J_N(S)$ for the isotropic discrepancy of the first N terms of S.

For classical Kronecker sequences the star discrepancy has been very well studied (see e.g. [6, Chapter 2], [11]); recently their isotropic discrepancy was also investigated (see Larcher [8], [9]).

For these sequences it is known that if $(\alpha_1, \ldots, \alpha_s) \in \mathbb{R}^s$ is badly approximable in the sense that there exists a constant $c > 0$ such that for all $q_1, \ldots, q_s \in \mathbb{Z}$ (not all 0) we have

$$\left\| \sum_{i=1}^{s} q_i \alpha_i \right\| \ge c(\overline{q}_1 \ldots \overline{q}_s)^{-1},$$

where $\|u\|$ denotes the distance from $u \in \mathbb{R}$ to the nearest integer and $\overline{q} = \max(1, |q|)$, then the star discrepancy of the corresponding Kronecker sequence S satisfies

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

see [6, p. 132].

We now present an analog of this result (with an even better estimate for the star discrepancy) for the sequences $S(L_1, \ldots, L_s)$. We use the convention that for the zero polynomial we put $\deg(0) = -1$.

THEOREM 2. *If there is a constant $c \in \mathbb{Z}$ such that for all polynomials $Q_1, \ldots, Q_s \in F_q[z]$ (not all 0) we have*

$$\nu\Big(\operatorname{Fr}\Big(\sum_{i=1}^{s} Q_i L_i\Big)\Big) \geq -c - \sum_{i=1}^{s} \deg(Q_i)\,, \tag{11}$$

then the sequence $S(L_1, \ldots, L_s)$ is a (t,s)-sequence in base q with $t = c - s$. In particular, we have

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

with an implied constant depending only on c, q, and s.

Proof. For an integer $h \geq 1$ define the vectors $\mathbf{u}_k^{(i)}(h) \in F_q^h$ for $1 \leq i \leq s$ and $k \geq 1$ as in (10). Let $\varrho(h)$ be the largest integer m such that for any integers $m_1, \ldots, m_s \geq 0$ with $\sum_{i=1}^{s} m_i = m$ the system of vectors $\mathbf{u}_k^{(i)}(h)$, $1 \leq k \leq m_i$, $1 \leq i \leq s$, is linearly independent over F_q; here an empty system of vectors is viewed as linearly independent. For an integer $B \geq 0$ we consider the points $\mathbf{x}_n$ with $Bq^h \leq n < (B+1)q^h$. By arguments similar to those in the proof of Theorem 1, it is easily seen that these points form an $(h - \varrho(h), h, s)$-net in base q. We claim that $h - \varrho(h) \leq c - s$, where c is as in (11). By the definition of $\varrho(h)$, there exist integers $m_1, \ldots, m_s \geq 0$ with $\sum_{i=1}^{s} m_i = \varrho(h) + 1$ such that the vectors $\mathbf{u}_k^{(i)}(h)$, $1 \leq k \leq m_i$, $1 \leq i \leq s$, are linearly dependent over F_q. Then for some $c_k^{(i)} \in F_q$ we have

$$\sum_{i=1}^{s} \sum_{k=1}^{m_i} c_k^{(i)} \mathbf{u}_k^{(i)}(h) = \mathbf{0} \in F_q^h\,,$$

where $c_{m_i}^{(i)} \neq 0$ whenever $m_i \geq 1$. Hence with

$$Q_i(z) = \sum_{k=1}^{m_i} c_k^{(i)} z^{k-1} \in F_q[z] \quad \text{for } 1 \leq i \leq s$$

we obtain

$$\nu\Big(\operatorname{Fr}\Big(\sum_{i=1}^{s} Q_i L_i\Big)\Big) \leq -h - 1\,.$$

On the other hand,

$$\nu\Big(\operatorname{Fr}\Big(\sum_{i=1}^{s} Q_i L_i\Big)\Big) \geq -c - \sum_{i=1}^{s} \deg(Q_i)$$

by (11). Now

$$\sum_{i=1}^{s} \deg(Q_i) = \varrho(h) + 1 - s\,,$$

so that indeed $h - \varrho(h) \leq c - s$. This shows that $S(L_1, \ldots, L_s)$ is a (t,s)-sequence in base q with $t = c - s$. The discrepancy bound follows then from Theorems 4.2 and 4.3 in [12]. ∎

An s-tuple $(L_1, \ldots, L_s) \in \mathfrak{C}_q^s$ satisfying (11) may be called "badly approximable". For $s = 1$, an irrational $L_1 \in \mathfrak{C}_q$ is badly approximable if and only if the degrees of the partial quotients in the continued fraction expansion of L_1 are bounded; compare with Section 4 for these continued fractions. For $s \geq 2$, Armitage [1], [2] claimed to have constructed badly approximable s-tuples of elements of $\mathfrak{C}_q$, but this claim was disproved by Taussat [22]. The question whether there exist badly approximable s-tuples of elements of $\mathfrak{C}_q$ for $s \geq 2$ is still open, as is the corresponding question for s-tuples of reals.

For the isotropic discrepancy we get a result quite analogous to that for classical Kronecker sequences (compare with [8]).

THEOREM 3. *Let $s \geq 2$ and suppose that there is a constant $c > 0$ such that for all polynomials $Q_1, \ldots, Q_s \in F_q[z]$ (not all 0) we have*

$$\nu\Big(\operatorname{Fr}\Big(\sum_{i=1}^{s} Q_i L_i\Big)\Big) \geq -c - s \max_{1\leq i\leq s} \deg(Q_i)\,.$$

Then the isotropic discrepancy of the sequence $S(L_1, \ldots, L_s)$ satisfies

$$J_N(S(L_1, \ldots, L_s)) = O(N^{-1/s})$$

with an implied constant depending only on c, q, and s.

Proof. As in the proof of Theorem 2, we again consider, for arbitrary integers $B \geq 0$ and $h \geq 1$, the point set $P(B,h)$ consisting of the $\mathbf{x}_n$ with $Bq^h \leq n < (B+1)q^h$. If the integers $m_1, \ldots, m_s \geq 0$ are such that the vectors $\mathbf{u}_k^{(i)}(h)$, $1 \leq k \leq m_i$, $1 \leq i \leq s$, are linearly dependent over F_q and if the polynomials $Q_1, \ldots, Q_s \in F_q[z]$ are obtained as in the proof of Theorem 2 from a linear dependence relation, then we have

$$-c - s \max_{1\leq i\leq s} \deg(Q_i) \leq \nu\Big(\operatorname{Fr}\Big(\sum_{i=1}^{s} Q_i L_i\Big)\Big) \leq -h - 1\,.$$

Consequently,

$$\max_{1\le i\le s} m_i \ge \frac{h+1-c}{s} + 1 \,.$$

Let $H = \lceil (h+1-c)/s \rceil$ and let h be so large that $H \ge 0$. Then the $\mathbf{u}_k^{(i)}(h)$, $1 \le k \le H$, $1 \le i \le s$, are linearly independent over F_q, and so in every elementary interval E in base q of the form

$$E = \prod_{i=1}^{s} [a_i q^{-H}, (a_i+1) q^{-H})$$

there are exactly q^{h-sH} points of the point set $P(B,h)$.

Now we can proceed by standard methods; see equation (1.15) and the last paragraph of the proof of Theorem 1.6 in [6, Chapter 2], as well as [7] for a more general method. Since the intervals E have diameter $s^{1/2} q^{-H}$, this yields that the isotropic discrepancy $J(B,h)$ of $P(B,h)$ satisfies

$$q^h J(B,h) \le C_0(s) q^h q^{-H} \le C_0(c,q,s) q^{h(1-1/s)} \,,$$

where $C_j(\ldots)$ denotes a positive constant depending only on the data listed between the parentheses. By adjusting the constant, we see that the last bound for $q^h J(B,h)$ holds also for the finitely many h that have been excluded before. Now let

$$N = \sum_{r=0}^{m} b_r q^r \ge 1 \qquad \text{with all } b_r \in Z_q \,.$$

Then we obtain

$$N J_N(S(L_1,\ldots,L_s)) \le C_1(c,q,s) \sum_{r=0}^{m} b_r q^{r(1-1/s)} \le C_2(c,q,s) N^{1-1/s} \,,$$

and the desired result follows. ∎

4. Connections with continued fractions. For classical Kronecker sequences it is well known that the star discrepancy of one-dimensional sequences and of associated two-dimensional point sets can be bounded quite precisely in terms of continued fraction parameters; see [6, Chapter 2], [11] and the more recent work of Schoißengeier [20]. We show that analogous results can be established for our Kronecker-type sequences.

Note that every $L \in \mathfrak{C}_q$ has a unique continued fraction expansion

$$L = A_0 + \cfrac{1}{A_1 + \cfrac{1}{A_2 + \ddots}} =: [A_0; A_1, A_2, \ldots] \,,$$

where $A_h \in F_q[z]$ for all $h \ge 0$ and $\deg(A_h) \ge 1$ for all $h \ge 1$. The expansion is finite for rational L and infinite for irrational L. For $h \ge 0$ the *h-th convergent* P_h/Q_h of L is defined by

$$P_h/Q_h = [A_0; A_1, \ldots, A_h], \quad \text{where } P_h, Q_h \in F_q[z] \text{ and } \gcd(P_h, Q_h) = 1\,.$$

For rational L there are only finitely many convergents.

We first consider two-dimensional point sets that are essentially equivalent to the two-dimensional version of the point sets constructed by Niederreiter [16] (compare also with [18]). For an integer $v \geq 1$ we define the truncated versions $\eta_v^{(i)}$ of the maps $\eta^{(i)}$ introduced in (7); if $L \in \mathfrak{C}_q$ is as in (1), then we put

$$\eta_v^{(i)}(L) = \sum_{k=\max(1,w)}^{v} \eta_{ik}(u_k) q^{-k} \quad \text{for } 1 \leq i \leq s\,. \tag{12}$$

Now choose f, g_1, $g_2 \in F_q[z]$ with $1 \leq \deg(f) = m \leq v$ and $\gcd(f, g_i) = 1$ for $i = 1, 2$. Then the point set $P(g_1, g_2; f)$ consists of the q^m points

$$\mathbf{x}_n = \left(\eta_v^{(1)}\left(\frac{n(z)g_1(z)}{f(z)}\right), \eta_v^{(2)}\left(\frac{n(z)g_2(z)}{f(z)}\right)\right) \in I^2 \quad \text{for } n = 0, 1, \ldots, q^m - 1\,. \tag{13}$$

If n runs through the set $\{0, 1, \ldots, q^m - 1\}$ of integers, then $n(z)$ defined by (6) runs through the set of all polynomials over F_q of degree less than m. Furthermore, $\eta_v^{(i)}(L)$ depends only on the fractional part of L, and so the point set $P(g_1, g_2; f)$ is identical with $P(1, g_1^* g_2; f)$, where $g_1^* \in F_q[z]$ is such that $g_1 g_1^* \equiv 1 \bmod f$. Therefore, it suffices to consider point sets $P(1, g; f)$ with $g \in F_q[z]$ and $\gcd(f, g) = 1$.

For the proof of Theorem 4 below, we need the following auxiliary result.

LEMMA 1. *Let* f, $g \in F_q[z]$ *with* $\deg(f) = m \geq 1$ *and* $\gcd(f, g) = 1$, *let* P_h/Q_h, $0 \leq h \leq H$, *be all convergents of* g/f, *and put* $d_h = \deg(Q_h)$ *for* $0 \leq h \leq H$. *Let* g/f *have the Laurent series expansion*

$$\frac{g(z)}{f(z)} = \sum_{k=w}^{\infty} v_k z^{-k}\,,$$

where we can assume $w \leq 1$. *For integers* l, $k \geq 1$ *put*

$$\mathbf{v}_l(k) = (v_l, v_{l+1}, \ldots, v_{l+k-1}) \in F_q^k\,,$$

and let $t = t(k)$ *be maximal such that* $\mathbf{v}_1(k), \ldots, \mathbf{v}_t(k)$ *are linearly independent over* F_q (*where an empty system of vectors is viewed as linearly independent*); *we set* $t(0) = 0$. *Then for* $0 \leq h \leq H-1$ *we have* $t(k) = d_h$ *for* $d_h \leq k \leq d_{h+1} - 1$, *and for* $k \geq d_H = m$ *we have* $t(k) = d_H = m$.

Proof. For $0 \leq h \leq H - 1$ we have

$$\nu\left(\mathrm{Fr}\left(Q_h \frac{g}{f}\right)\right) = -d_{h+1}\,, \tag{14}$$

and for all $Q \in F_q[z]$ with $d_h \le \deg(Q) < d_{h+1}$ we have

$$\nu\left(\mathrm{Fr}\left(Q\frac{g}{f}\right)\right) \ge \nu\left(\mathrm{Fr}\left(Q_h\frac{g}{f}\right)\right); \tag{15}$$

see e.g. [17, Appendix B] for these two results. Then for $0 \le h \le H-1$ the vectors $\mathbf{v}_1(d_{h+1}-1), \ldots, \mathbf{v}_{d_h+1}(d_{h+1}-1)$ are linearly dependent over F_q. For if

$$Q_h(z) = \sum_{r=0}^{d_h} q_r z^r,$$

then it follows from (14) that

$$\sum_{r=0}^{d_h} q_r \mathbf{v}_{r+1}(d_{h+1}-1) = \mathbf{0}.$$

Similarly, for $k \ge d_H$ the vectors $\mathbf{v}_1(k), \ldots, \mathbf{v}_{d_H+1}(k)$ are linearly dependent over F_q since $\mathrm{Fr}\left(Q_H\frac{g}{f}\right) = 0$.

Furthermore, for $0 \le h \le H-1$ the vectors $\mathbf{v}_1(d_{h+1}), \ldots, \mathbf{v}_{d_{h+1}}(d_{h+1})$ are linearly independent over F_q. For if we had

$$\sum_{r=0}^{d_{h+1}-1} p_r \mathbf{v}_{r+1}(d_{h+1}) = \mathbf{0}$$

with $P(z) = \sum_{r=0}^{d_{h+1}-1} p_r z^r$ not the zero polynomial, then we get

$$\nu\left(\mathrm{Fr}\left(P\frac{g}{f}\right)\right) < -d_{h+1}.$$

Since $0 \le \deg(P) < d_{h+1}$, there exists a unique j with $0 \le j \le h$ such that $d_j \le \deg(P) < d_{j+1}$. Then

$$\nu\left(\mathrm{Fr}\left(P\frac{g}{f}\right)\right) < -d_{j+1} = \nu\left(\mathrm{Fr}\left(Q_j\frac{g}{f}\right)\right),$$

which is a contradiction to (15). The result of the lemma follows now immediately. ∎

THEOREM 4. *If f, $g \in F_q[z]$, $1 \le \deg(f) = m \le v$, $\gcd(f,g) = 1$, and*

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

is the continued fraction expansion of g/f, then the star discrepancy of the two-dimensional point set $P(1,g;f)$ satisfies

$$q^m D^*_{q^m}(P(1,g;f)) \le 1 + \frac{1}{4}\sum_{h=1}^{H} q^{\deg(A_h)}(1+q^{-\deg(A_h)})^2.$$

Proof. The Laurent series expansion of $1/f$ has the form

$$\frac{1}{f(z)} = \sum_{k=m}^{\infty} u_k z^{-k} \quad \text{with } u_m \neq 0\,.$$

Let $0 < \alpha$, $\beta \le 1$ with digit expansions

$$\alpha = \sum_{k=1}^{m} \alpha_k q^{-k}\,, \qquad \beta = \sum_{k=1}^{\infty} \beta_k q^{-k}\,,$$

where all α_k, $\beta_k \in Z_q$, except in the case $\alpha = 1$ where we allow $\alpha_m = q$; also $\beta_k < q-1$ for infinitely many k, except in the case $\beta = 1$ where $\beta_k = q-1$ for all k.

We abbreviate (13) by $\mathbf{x}_n = (x_n^{(1)}, x_n^{(2)})$, and we consider the set of all $n \in \{0, 1, \ldots, q^m - 1\}$ with $0 \le x_n^{(1)} < \alpha$. This set can also be described as the set of all $n = \sum_{r=0}^{m-1} a_r q^r$, $a_r \in Z_q$, for which for some integer j with $1 \le j \le m$ the following condition B_j holds:

$$\eta_{1r}(u_m \psi_{m-r}(a_{m-r}) + \ldots + u_{m+r-1}\psi_{m-1}(a_{m-1})) = \alpha_r \qquad \text{for } r = 1, 2, \ldots, j-1$$

and

$$\eta_{1j}(u_m \psi_{m-j}(a_{m-j}) + \ldots + u_{m+j-1}\psi_{m-1}(a_{m-1})) = a \qquad \text{for some integer } a \text{ with } 0 \le a < \alpha_j\,.$$

For $0 \le h \le H-1$ let M_h be the set of all $n \in \{0, 1, \ldots, q^m - 1\}$ for which one of the conditions B_j with

(16) $\quad m - d_{h+1} + 1 \le j \le m - d_h \quad$ where the d_h are as in Lemma 1,

is satisfied. For every such j and fixed $a \in \{0, 1, \ldots, \alpha_j - 1\}$, by the condition B_j the digits $a_{m-j}, \ldots, a_{m-1}$ are uniquely determined since $u_m \neq 0$, whereas the digits $a_0, \ldots, a_{m-j-1}$ are free.

For every j satisfying (16) we have $t(m-j) = d_h$ according to Lemma 1. By the definition of $t(m-j)$ in Lemma 1, for any such j, any $a \in \{0, 1, \ldots, \alpha_j - 1\}$, and any $b \in \{0, 1, \ldots, q^{d_h} - 1\}$, there are exactly q^{m-j-d_h} integers n, $0 \le n < q^m$, which satisfy the condition B_j with last digit a and such that

$$x_n^{(2)} \in [bq^{-d_h}, (b+1)q^{-d_h})\,.$$

The number of $n \in M_h$ with $x_n^{(2)} < \sum_{k=1}^{d_h} \beta_k q^{-k}$ is thus given by

$$\sum_{j=m-d_{h+1}+1}^{m-d_h} \Big(\sum_{k=1}^{d_h} \beta_k q^{d_h - k}\Big) q^{m-j-d_h} \alpha_j = q^m \Big(\sum_{k=1}^{d_h} \beta_k q^{-k}\Big) \sum_{j=m-d_{h+1}+1}^{m-d_h} \alpha_j q^{-j}.$$

For $0 \le h \le H-1$ and a subinterval K of $[0,1)$ we let $N_h(K)$ be the number of $n \in M_h$ with $x_n^{(2)} \in K$. Then with

$$\alpha^{(h)} = \sum_{j=m-d_{h+1}+1}^{m-d_h} \alpha_j q^{-j} \quad \text{for } 0 \le h \le H-1$$

the result above can be written in the form

$$N_h\Big(\Big[0, \sum_{k=1}^{d_h} \beta_k q^{-k}\Big)\Big) = q^m \alpha^{(h)} \sum_{k=1}^{d_h} \beta_k q^{-k} . \tag{17}$$

We abbreviate the point set $P(1,g;f)$ by P. Then with $J = [0,\alpha) \times [0,\beta)$ and $K_h = [\sum_{k=1}^{d_h} \beta_k q^{-k}, \beta)$ for $0 \le h \le H-1$ we have

$$\begin{aligned} A(J;P) &= \sum_{h=0}^{H-1} N_h([0,\beta)) = \sum_{h=0}^{H-1} N_h\Big(\Big[0, \sum_{k=1}^{d_h} \beta_k q^{-k}\Big)\Big) + \sum_{h=0}^{H-1} N_h(K_h) \\ &= q^m \sum_{h=0}^{H-1} \alpha^{(h)} \sum_{k=1}^{d_h} \beta_k q^{-k} + \sum_{h=0}^{H-1} N_h(K_h) . \end{aligned}$$

Consequently,

$$\begin{aligned} A(J;P) - q^m \alpha\beta &= A(J;P) - q^m \beta \sum_{h=0}^{H-1} \alpha^{(h)} \\ &= q^m \sum_{h=0}^{H-1} \alpha^{(h)} \Big(\sum_{k=1}^{d_h} \beta_k q^{-k} - \beta \Big) + \sum_{h=0}^{H-1} N_h(K_h) , \end{aligned}$$

and so

$$A(J;P) - q^m \alpha\beta = \sum_{h=0}^{H-1} (N_h(K_h) - q^m \alpha^{(h)} \lambda_1(K_h)) . \tag{18}$$

For $0 \le h \le H-1$ put

$$G_h = \Big[\sum_{k=1}^{d_h} \beta_k q^{-k}, \sum_{k=1}^{d_h} \beta_k q^{-k} + q^{-d_h} \Big) .$$

Then it follows from (17) that

$$N_h(G_h) = q^{m-d_h} \alpha^{(h)} .$$

For any fixed choice of $a_{d_{h+1}}, \ldots, a_{m-1} \in Z_q$ and for every $a \in \{0,1,\ldots,q^{d_{h+1}}-1\}$, we deduce from Lemma 1 that there is exactly one $n \in \{0,1,\ldots,q^m-1\}$ having the given digits $a_{d_{h+1}}, \ldots, a_{m-1}$ and such that $x_n^{(2)} \in [aq^{-d_{h+1}}, (a+1)q^{-d_{h+1}})$.

For given $0 \leq h \leq H-1$ we now want to derive an upper bound for

$$R_h := N_h(K_h) - q^m \alpha^{(h)} \lambda_1(K_h)\,.$$

We note that $K_h \subseteq G_h$. Clearly, $N_h(K_h)$ attains the largest value if the points $x_n^{(2)}$ counted by $N_h(G_h)$ are as close as possible to the left-hand endpoint of G_h, that is, for every $b = 0, 1, \ldots, q^{m-d_h}\alpha^{(h)} - 1$ there is exactly one point $x_n^{(2)}$ counted by $N_h(G_h)$ in the interval

$$\Big[\sum_{k=1}^{d_h} \beta_k q^{-k} + bq^{-d_{h+1}}, \sum_{k=1}^{d_h} \beta_k q^{-k} + (b+1)q^{-d_{h+1}}\Big)\,.$$

Also, if $N_h(K_h) = c$, then in order that all these c counted points $x_n^{(2)}$ can be in K_h, we must have

$$\beta > \sum_{k=1}^{d_h} \beta_k q^{-k} + (c-1)q^{-d_{h+1}}\,.$$

Thus we get

$$R_h < c(1-\gamma_h) + \gamma_h \quad \text{with} \quad \gamma_h = q^{m-d_{h+1}}\alpha^{(h)}\,.$$

Since $\gamma_h \leq 1$, this upper bound is maximal if c is maximal, that is, $c = q^{m-d_h}\alpha^{(h)}$. Therefore

$$R_h < q^{d_{h+1}-d_h}(\gamma_h - \gamma_h^2) + \gamma_h \leq \tfrac{1}{4} q^{d_{h+1}-d_h}(1 + q^{d_h - d_{h+1}})^2\,.$$

Quite analogously it is shown that

$$R_h > -\tfrac{1}{4} q^{d_{h+1}-d_h}(1 + q^{d_h - d_{h+1}})^2\,.$$

Together with (18) this yields

$$|A(J;P) - q^m \alpha\beta| < \frac{1}{4}\sum_{h=1}^{H} q^{\deg(A_h)}(1 + q^{-\deg(A_h)})^2\,.$$

For arbitrary $0 < \alpha$, $\beta \leq 1$ and $J = [0,\alpha) \times [0,\beta)$ we obtain

$$|A(J;P) - q^m \alpha\beta| < 1 + \frac{1}{4}\sum_{h=1}^{H} q^{\deg(A_h)}(1 + q^{-\deg(A_h)})^2$$

and the result of the theorem is established. ∎

If $K \geq 1$ is such that $\deg(A_h) \leq K$ for $1 \leq h \leq H$, then it follows from Theorem 4 that with $N = q^m$ we have

$$D_N^*(P(1,g;f)) = O(N^{-1}\log N)$$

with an implied constant depending only on K and q. Note that $N^{-1}\log N$ is the least order of magnitude of the star discrepancy of any N points in $\bar{I}^2$, according to a well-known result of Schmidt [19].

We now establish a discrepancy bound for a one-dimensional Kronecker-type sequence $S(L_1)$ with an irrational $L_1 \in \mathfrak{C}_q$ in terms of continued fraction parameters.

THEOREM 5. *Let $L_1 = [A_0; A_1, A_2, \ldots]$ be the continued fraction expansion of an irrational $L_1 \in \mathfrak{C}_q$ and put*

$$d_H = \deg(Q_H) = \sum_{h=1}^{H} \deg(A_h) \quad \textit{for } H \geq 0\,,$$

where the Q_H are the denominators of the convergents of L_1. Then for all integers N with $q^{d_{H-1}} < N \leq q^{d_H}$, $H \geq 1$, we have

$$N D_N^*(S(L_1)) \leq \frac{q+1}{q} + \frac{1}{4} \sum_{h=1}^{H} q^{\deg(A_h)} (1 + q^{-\deg(A_h)})^2 \,.$$

Proof. For $H \geq 1$ let P_H/Q_H be the Hth convergent of L_1. Then

$$\nu\left(L_1 - \frac{P_H}{Q_H}\right) = -d_H - d_{H+1} \tag{19}$$

by [17, Appendix B]. According to (8), the terms x_n of $S(L_1)$ are given by

$$x_n = \eta^{(1)}(n(z) L_1(z)) \quad \text{for } n = 0, 1, \ldots$$

For $n = 0, 1, \ldots, q^{d_H} - 1$ we have $\deg(n(z)) \leq d_H - 1$ by (6), and so it follows from (19) that for these n we have

$$\left| x_n - \eta^{(1)}_{d_{H+1}}\left(\frac{n(z) P_H(z)}{Q_H(z)}\right)\right| \leq q^{-d_{H+1}} \leq q^{-d_H - 1} \tag{20}$$

with the notation of (12). Now we consider the two-dimensional point set

$$\left(\frac{n}{q^{d_H}}, \eta^{(1)}_{d_{H+1}}\left(\frac{n(z) P_H(z)}{Q_H(z)}\right)\right), \quad n = 0, 1, \ldots, q^{d_H} - 1\,.$$

We can use almost exactly the same arguments as in the proof of Theorem 4. Then for the star discrepancy D^* of this point set we obtain

$$q^{d_H} D^* \leq 1 + \frac{1}{4} \sum_{h=1}^{H} q^{\deg(A_h)} (1 + q^{-\deg(A_h)})^2 \,.$$

Now by standard methods (compare with [6, pp. 105–106]) and by the inequality (20) it is easy to see that

$$N D_N^*(S(L_1)) \leq \frac{1}{q} + q^{d_H} D^* \quad \text{for } 1 \leq N \leq q^{d_H}\,,$$

and the desired result follows. ∎

If the irrational $L_1 \in \mathfrak{C}_q$ has bounded partial quotients, i.e., if there exists a $K \geq 1$ such that $\deg(A_h) \leq K$ for all $h \geq 1$, then it follows from

Theorem 5 that $D_N^*(S(L_1)) = O(N^{-1} \log N)$ for all $N \geq 2$, with an implied constant depending only on K and q. The lower bound of Schmidt [19] for the star discrepancy of arbitrary one-dimensional sequences shows that the order of magnitude $N^{-1} \log N$ is best possible.

For $q = 2$ the irrationals $L_1 \in \mathfrak{C}_2$ with $\nu(L_1) < 0$ and $\deg(A_h) = 1$ for all $h \geq 1$ have been characterized in terms of their Laurent series expansion by Baum and Sweet [3]; namely, $L_1 \in \mathfrak{C}_2$ satisfies these properties if and only if

$$L_1 = \sum_{k=1}^{\infty} u_k z^{-k}$$

with $u_1 = 1$ and $u_{2k+1} = u_{2k} + u_k$ for all $k \geq 1$.

We now show how to derive from Theorem 5 a metric result on the behavior of $D_N^*(S(L_1))$ for almost all L_1. This result is quite analogous to the corresponding metric theorem for one-dimensional classical Kronecker sequences (compare with [6, p. 128]). Since the sequence $S(L_1)$ depends only on the fractional part of L_1, it suffices to consider $L_1 \in \mathfrak{C}_q$ with $\nu(L_1) < 0$; let $\mathcal{M}_q$ be the set of all such L_1. With the topology induced by ν and with respect to addition, $\mathcal{M}_q$ is a compact abelian group, and so it has a unique Haar probability measure μ_q.

THEOREM 6. *Let G be a positive nondecreasing function on $[1, \infty)$ such that $\sum_{d=1}^{\infty} G(d)^{-1} < \infty$. Then μ_q-almost everywhere we have*

$$D_N^*(S(L_1)) = O(N^{-1}(\log N) G(C(L_1) \log\log N)) \quad \textit{for } N \geq 3\,,$$

with an implied constant depending only on G, q, and L_1 and with a constant $C(L_1) > 0$ depending only on L_1.

Proof. Since there are only countably many rational functions over F_q, the set of rational $L_1 \in \mathcal{M}_q$ has μ_q-measure 0 and can be neglected. Let P_q be the set of all polynomials over F_q of positive degree and consider the function g on P_q defined by

$$g(p) = G(\deg(p))^{-1} q^{\deg(p)} \quad \text{for all } p \in P_q\,.$$

Then

$$\sum_{p \in P_q} g(p) q^{-2\deg(p)} = \sum_{p \in P_q} G(\deg(p))^{-1} q^{-\deg(p)} = \sum_{d=1}^{\infty} G(d)^{-1} q^{-d} (q-1) q^d =: C(G, q) < \infty\,,$$

and so it follows from [15, Theorem 3] that

$$\lim_{H \to \infty} \frac{1}{H} \sum_{h=1}^{H} G(\deg(A_h))^{-1} q^{\deg(A_h)} = C(G, q) \quad \mu_q\text{-a.e.}$$

Consequently, we have

$$\sum_{h=1}^{H} G(\deg(A_h))^{-1} q^{\deg(A_h)} = O(H) \qquad \mu_q\text{-a.e.} \tag{21}$$

with an implied constant depending only on G, q, and L_1.

Furthermore, from [15, Theorem 6] it follows that μ_q-a.e. we have

$$\deg(A_h) = O(\log(h+1)) \qquad \text{for all } h \geq 1$$

with an implied constant depending only on L_1. Thus,

$$\max_{1\leq h\leq H} G(\deg(A_h)) \leq G(C_1(L_1)\log(H+1)) \qquad \mu_q\text{-a.e.} \tag{22}$$

By combining (21) and (22), we obtain

$$\begin{aligned} \sum_{h=1}^{H} q^{\deg(A_h)} &\leq \big(\max_{1\leq h\leq H} G(\deg(A_h))\big) \sum_{h=1}^{H} G(\deg(A_h))^{-1} q^{\deg(A_h)} \\ &= O(HG(C_1(L_1)\log(H+1))) \qquad \mu_q\text{-a.e.} \end{aligned} \tag{23}$$

with an implied constant depending only on G, q, and L_1.

For $N \geq 3$ we determine $H(N)$ by the condition in Theorem 5, i.e., by

$$q^{d_{H(N)-1}} < N \leq q^{d_{H(N)}}\,.$$

This condition is equivalent to

$$\frac{1}{H(N)} \sum_{h=1}^{H(N)-1} \deg(A_h) < \frac{\log N}{H(N)\log q} \leq \frac{1}{H(N)} \sum_{h=1}^{H(N)} \deg(A_h)\,,$$

hence by applying [15, Corollary 1] we obtain

$$H(N) = O(\log N) \qquad \mu_q\text{-a.e.}$$

with an implied constant depending only on L_1. In view of Theorem 5 and (23), this yields the desired result. ∎

Corollary 1. *For every $\varepsilon > 0$ we have μ_q-almost everywhere*

$$D_N^*(S(L_1)) = O(N^{-1}(\log N)(\log\log N)^{1+\varepsilon}) \qquad \textit{for } N \geq 3\,,$$

with an implied constant depending only on ε, q, and L_1.

References

[1] J. V. Armitage, *An analogue of a problem of Littlewood*, Mathematika 16 (1969), 101–105.

[2] —, *Corrigendum and addendum: An analogue of a problem of Littlewood*, ibid. 17 (1970), 173–178.

[3] L. E. Baum and M. M. Sweet, *Badly approximable power series in characteristic 2*, Ann. of Math. 105 (1977), 573–580.

[4] H. Faure, *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. 41 (1982), 337–351.
[5] T. Hansen, G. L. Mullen and H. Niederreiter, *Good parameters for a class of node sets in quasi-Monte Carlo integration*, Math. Comp., to appear.
[6] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York 1974.
[7] G. Larcher, *Über die isotrope Diskrepanz von Folgen*, Arch. Math. (Basel) 46 (1986), 240–249.
[8] —, *On the distribution of s-dimensional Kronecker-sequences*, Acta Arith. 51 (1988), 335–347.
[9] —, *On the distribution of the multiples of an s-tupel of real numbers*, J. Number Theory 31 (1989), 367–372.
[10] —, *Nets obtained from rational functions over finite fields*, this volume, 1–13.
[11] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. 84 (1978), 957–1041.
[12] —, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.
[13] —, *Quasi-Monte Carlo methods for multidimensional numerical integration*, in: Numerical Integration III, H. Braß and G. Hämmerlin (eds.), Internat. Ser. Numer. Math. 85, Birkhäuser, Basel 1988, 157–171.
[14] —, *Low-discrepancy and low-dispersion sequences*, J. Number Theory 30 (1988), 51–70.
[15] —, *The probabilistic theory of linear complexity*, in: Advances in Cryptology—EUROCRYPT'88, C. G. Günther (ed.), Lecture Notes in Comput. Sci. 330, Springer, Berlin 1988, 191–209.
[16] —, *Low-discrepancy point sets obtained by digital constructions over finite fields*, Czechoslovak Math. J. 42 (1992), 143–166.
[17] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia 1992.
[18] —, *Finite fields, pseudorandom numbers, and quasirandom points*, in: Proc. Internat. Conf. on Finite Fields (Las Vegas 1991), Dekker, New York 1992, 375–394.
[19] W. M. Schmidt, *Irregularities of distribution, VII*, Acta Arith. 21 (1972), 45–50.
[20] J. Schoißengeier, *On the discrepancy of $(n\alpha)$*, ibid. 44 (1984), 241–279.
[21] 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 (in Russian).
[22] Y. Taussat, *Approximation diophantienne dans un corps de séries formelles*, Thèse, Université de Bordeaux, 1986.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT SALZBURG
HELLBRUNNERSTRASSE 34
A-5020 SALZBURG
ÖSTERREICH

INSTITUT FÜR INFORMATIONSVERARBEITUNG
ÖSTERR. AKADEMIE DER WISSENSCHAFTEN
SONNENFELSGASSE 19
A-1010 WIEN
ÖSTERREICH
E-mail: NIED@QIINFO.OEAW.AC.AT

Received on 9.11.1992 (2320)