

Harald Niederreiter

Low-discrepancy point sets obtained by digital constructions over finite fields

Czechoslovak Mathematical Journal, Vol. 42 (1992), No. 1, 143–166

Persistent URL: <http://dml.cz/dmlcz/128322>

Terms of use:

© Institute of Mathematics AS CR, 1992

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

LOW-DISCREPANCY POINT SETS OBTAINED BY DIGITAL
CONSTRUCTIONS OVER FINITE FIELDS

HARALD NIEDERREITER, Vienna

(Received March 26, 1991)

Dedicated to the Memory of Theodor Schneider

1. INTRODUCTION

For N points $\mathbf{x}_1, \dots, \mathbf{x}_N$ in the s -dimensional half-open unit cube $I^s = [0, 1)^s$, $s \geq 1$, and for a subinterval J of I^s we put

$$D(J; N) = A(J; N) - V(J)N,$$

where $A(J; N)$ is the number of n , $1 \leq n \leq N$, with $\mathbf{x}_n \in J$ and $V(J)$ is the volume of J . Then the *star discrepancy* D_N^* of the points $\mathbf{x}_1, \dots, \mathbf{x}_N$ is defined by

$$D_N^* = \sup_J \left| \frac{D(J; N)}{N} \right|,$$

where the supremum is extended over all half-open subintervals $J = \prod_{i=1}^s [0, u_i)$ of I^s .

Point sets with small star discrepancy (or *low-discrepancy point sets*) are not only of number-theoretic interest, but they also play a crucial role in quasi-Monte Carlo methods for numerical integration (see [7, 11, 17]). The aim in the construction of low-discrepancy point sets is to obtain point sets in I^s for which the star discrepancy satisfies $D_N^* = O(N^{-1}(\log N)^{k(s)})$, where the implied constant and the exponent $k(s)$ depend only on the dimension s . The main interest is in constructions which achieve $k(s) \leq s$; see [11, 17] for surveys of such constructions. Since for $s = 1$ the point sets achieving the minimal star discrepancy $D_N^* = 1/(2N)$ are known (see [11, p. 972]), we concentrate on the multidimensional case $s \geq 2$.

The present paper deals with "digital constructions" for low-discrepancy point sets, i.e., constructions in which the coordinates of the points are given by digit expansions in a chosen base and every digit is obtained by a prescribed scheme.

A general family of such digital constructions was introduced in [16]. These constructions yield point sets with the special equidistribution property described in the following definition.

Definition 1. Let $0 \leq t \leq m$ and $b \geq 2$ be integers. A (t, m, s) -net in base b is a point set of b^m points in I^s such that $A(J; b^m) = b^t$ for every subinterval J of I^s of the form

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

with integers a_i and d_i and with $V(J) = b^{t-m}$.

Nets were first constructed by Sobol' [21] in base 2. A construction of Faure [5] yields $(0, m, s)$ -nets in prime bases $\geq s - 1$, and constructions of Niederreiter [16, 17] yield $(0, m, s)$ -nets in prime power bases $\geq s - 1$. A general construction principle for nets in arbitrary bases, which uses systems of linear equations over finite rings, was introduced in [16] and explicit constructions based on this principle were given in [18]. From results in [16, Sect. 3] we get for $s \geq 2$ that the star discrepancy of a (t, m, s) -net in an arbitrary base b satisfies

$$ND_N^* \leq B(s, b) b^t (\log N)^{s-1} + O(b^t (\log N)^{s-2}), \quad (1)$$

where $N = b^m$ and

$$B(s, b) = \begin{cases} \left(\frac{b-1}{2 \log b} \right)^{s-1} & \text{if either } s = 2 \text{ or } b = 2 \text{ and } s = 3, 4, \\ \frac{1}{(s-1)!} \left(\frac{\lfloor b/2 \rfloor}{\log b} \right)^{s-1} & \text{otherwise,} \end{cases} \quad (2)$$

and where the constant implied by the Landau symbol in (1) depends only on s and b . For fixed m, s , and b the discrepancy bound in (1) is an increasing function of t , hence t should be small to guarantee a small value of D_N^* .

In this paper we study constructions of nets in prime power bases. These constructions may be extended to arbitrary bases by proceeding in analogy with [18, Sect. 4]. Prime power bases are of particular interest because in this case one can take as the underlying finite ring a finite field. Section 2 contains a further study of the general construction principle introduced in [16]. A new type of upper bound for the star discrepancy of nets obtained by this construction is established, which leads to a determination of the average order of magnitude of the star discrepancy in this family of nets. Lower bounds for the star discrepancy of these nets are also established. In Section 3 we specialize the method in Section 2 to obtain a construction of nets based on rational functions over finite fields. The main result of Section 3 provides an existence theorem for low-discrepancy point sets within this special family of nets. We also discuss the connection between the construction in Section 3 and an earlier construction in [12].

2. A GENERAL FAMILY OF NETS

We first recall the general construction principle for nets in [16, Sect. 6], but we consider only the special case of a prime power base. Let q be an arbitrary prime power and let F_q be the finite field of order q . We write $B_q = \{0, 1, \dots, q-1\}$ for the set of digits in base q . For given integers $m \geq 1$ and $s \geq 2$ we choose the following:

- (i) bijections $\psi_r: B_q \rightarrow F_q$ for $0 \leq r \leq m-1$;
- (ii) bijections $\lambda_{ij}: F_q \rightarrow B_q$ for $1 \leq i \leq s$ and $1 \leq j \leq m$;
- (iii) elements $c_{jr}^{(i)} \in F_q$ for $1 \leq i \leq s, 1 \leq j \leq m$, and $0 \leq r \leq m-1$.

For $n = 1, 2, \dots, q^m$ let

$$n-1 = \sum_{r=0}^{m-1} a_r(n)q^r, \quad a_r(n) \in B_q,$$

be the representation of $n-1$ in base q . Put

$$x_n^{(i)} = \sum_{j=1}^m x_{nj}^{(i)} q^{-j} \quad \text{for } 1 \leq n \leq q^m \quad \text{and } 1 \leq i \leq s$$

with

$$x_{nj}^{(i)} = \lambda_{ij} \left(\sum_{r=0}^{m-1} c_{jr}^{(i)} \psi_r(a_r(n)) \right) \in B_q \quad \text{for } 1 \leq n \leq q^m, 1 \leq i \leq s, 1 \leq j \leq m.$$

Then define the point set

$$\mathbf{x}_n = \left(x_n^{(1)}, \dots, x_n^{(s)} \right) \in I^s \quad \text{for } 1 \leq n \leq q^m. \quad (3)$$

The following definition and lemma from [16, Sect. 6] are basic.

Definition 2. For the system C of vectors

$$\mathbf{c}_j^{(i)} = \left(c_{j0}^{(i)}, c_{j1}^{(i)}, \dots, c_{j,m-1}^{(i)} \right) \in F_q^m \quad \text{for } 1 \leq i \leq s \quad \text{and } 1 \leq j \leq m$$

we define

$$\varrho(C) = \min \sum_{i=1}^s d_i,$$

where the minimum is extended over all nonempty systems $\{\mathbf{c}_j^{(i)} : 1 \leq j \leq d_i, 1 \leq i \leq s\}$ with $0 \leq d_i \leq m$ for $1 \leq i \leq s$ that are linearly dependent over F_q .

Lemma 1. *The point set (3) is a (t, m, s) -net in base q with $t = m + 1 - \varrho(C)$.*

If Lemma 1 is combined with (1) and (2), then we obtain the following upper bound for the star discrepancy D_N^* of the point set (3) with $N = q^m$:

$$D_N^* \leq B(s, q)q^{1-\varrho(C)}(\log N)^{s-1} + O(q^{-\varrho(C)}(\log N)^{s-2}), \quad (4)$$

where the constant implied by the Landau symbol depends only on s and q . The following results on the quantity $\varrho(C)$ were shown in [19]. First of all, there is a general upper bound of the form

$$\varrho(C) \leq \max(2, m + 1 - \lfloor k_q \log s \rfloor)$$

with a constant $k_q > 0$ depending only on q . On the other hand, there always exists a system C with

$$\varrho(C) \geq m + 1 - \sum_{i=1}^{s-1} (e_i - 1),$$

where e_1, \dots, e_{s-1} are the degrees of $s-1$ arbitrarily chosen distinct monic irreducible polynomials over F_q .

There is a trivial lower bound for the star discrepancy D_N^* with $N = q^m$ of the point set (3). Note that all coordinates of the points in (3) are rationals with denominator N . Let $0 < \varepsilon \leq N^{-1}$ and put $J_\varepsilon = [0, 1 - N^{-1} + \varepsilon]^s$. Then

$$D_N^* \geq N^{-1} |D(J_\varepsilon; N)| = 1 - \left(1 - \frac{1}{N} + \varepsilon\right)^s.$$

Letting $\varepsilon \rightarrow 0+$, we get the lower bound

$$D_N^* \geq 1 - \left(1 - \frac{1}{N}\right)^s. \quad (5)$$

A more important lower bound, which is a counterpart to the upper bound in (4), is given by the following result.

Theorem 1. *The star discrepancy D_N^* with $N = q^m$ of the point set (3) satisfies*

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

If the maps λ_{ij} are such that $\lambda_{ij}(0) = 0$ for $1 \leq i \leq s$ and $1 \leq j \leq m$, then

$$D_N^* \geq \frac{q-1}{2} q^{-\varrho(C)}.$$

Proof. If λ_{ij}^{-1} denotes the inverse map of λ_{ij} , then by construction we have

$$\sum_{r=0}^{m-1} c_{jr}^{(i)} \psi_r(a_r(n)) = \lambda_{ij}^{-1}(x_{nj}^{(i)}) \quad \text{for } 1 \leq n \leq q^m, 1 \leq i \leq s, 1 \leq j \leq m. \quad (6)$$

The definition of $\varrho(C)$ implies the existence of a nonzero s -tuple (d_1, \dots, d_s) of integers with $0 \leq d_i \leq m$ for $1 \leq i \leq s$ such that the system $\{c_j^{(i)} : 1 \leq j \leq d_i, 1 \leq i \leq s\}$ is linearly dependent over F_q and $\varrho(C) = \sum_{i=1}^s d_i$. Let w , $1 \leq w \leq s$, be the largest index for which $d_w \neq 0$. Since the system $\{c_j^{(i)} : 1 \leq j \leq d_i, 1 \leq i \leq w\}$ is linearly dependent over F_q , there exist elements $h_j^{(i)} \in F_q$, $1 \leq j \leq d_i, 1 \leq i \leq w$, not all 0 such that

$$\sum_{i=1}^w \sum_{j=1}^{d_i} h_j^{(i)} c_j^{(i)} = 0 \in F_q^m.$$

We have $h_{d_w}^{(w)} \neq 0$ by the definition of $\varrho(C)$. Comparing components we get

$$\sum_{i=1}^w \sum_{j=1}^{d_i} h_j^{(i)} c_{jr}^{(i)} = 0 \quad \text{for } 0 \leq r \leq m-1.$$

Together with (6) we obtain

$$\begin{aligned} \sum_{i=1}^w \sum_{j=1}^{d_i} h_j^{(i)} \lambda_{ij}^{-1}(x_{nj}^{(i)}) &= \sum_{i=1}^w \sum_{j=1}^{d_i} h_j^{(i)} \sum_{r=0}^{m-1} c_{jr}^{(i)} \psi_r(a_r(n)) \\ &= \sum_{r=0}^{m-1} \psi_r(a_r(n)) \sum_{i=1}^w \sum_{j=1}^{d_i} h_j^{(i)} c_{jr}^{(i)} = 0 \quad \text{for } 1 \leq n \leq q^m. \end{aligned} \quad (7)$$

Since $h_{d_w}^{(w)} \neq 0$, there exists a unique $b \in F_q$ with

$$\sum_{i=1}^{w-1} \sum_{j=1}^{d_i} h_j^{(i)} \lambda_{ij}^{-1}(0) + \sum_{j=1}^{d_w-1} h_j^{(w)} \lambda_{wj}^{-1}(0) + h_{d_w}^{(w)} b = 0. \quad (8)$$

Put $a = \lambda_{w d_w}(b) \in B_q$. Define the intervals

$$J_i = [0, q^{-d_i}) \quad \text{for } 1 \leq i < w,$$

$$J_w = \begin{cases} [(a+1)q^{-d_w}, q^{1-d_w}) & \text{if } a < \frac{1}{3}(q-1), \\ [0, aq^{-d_w}) & \text{if } a \geq \frac{1}{3}(q-1). \end{cases}$$

The subinterval J of I^s is then defined by

$$J = J_1 \times \dots \times J_w \times [0, 1)^{s-w}.$$

We claim that no point x_n in (3) belongs to J . Suppose on the contrary that $x_n \in J$ for some n with $1 \leq n \leq q^m$. Then $x_n^{(i)} \in J_i$ for $1 \leq i \leq w$. For $1 \leq i < w$ it follows from the definition of J_i that $x_n^{(i)} = 0$ for $1 \leq j \leq d_i$. For $i = w$ it follows from the definition of J_w that $x_n^{(w)} = 0$ for $1 \leq j < d_w$ and $x_{nd_w}^{(w)} \neq a$. Thus (7) implies

$$\sum_{i=1}^{w-1} \sum_{j=1}^{d_i} h_j^{(i)} \lambda_{ij}^{-1}(0) + \sum_{j=1}^{d_w-1} h_j^{(w)} \lambda_{wj}^{-1}(0) + h_{d_w}^{(w)} \lambda_{wd_w}^{-1}(x_{nd_w}^{(w)}) = 0.$$

In view of (8) this yields $\lambda_{wd_w}^{-1}(x_{nd_w}^{(w)}) = b$, hence $x_{nd_w}^{(w)} = \lambda_{wd_w}(b) = a$, a contradiction. Thus the claim is shown.

Now we consider two cases as in the definition of J_w . In the first case let $a < (q-1)/3$. Define subintervals I_1 and I_2 of I^s by

$$I_1 = J_1 \times \dots \times J_{w-1} \times [0, q^{1-d_w}) \times [0, 1)^{s-w},$$

$$I_2 = J_1 \times \dots \times J_{w-1} \times [0, (a+1)q^{-d_w}) \times [0, 1)^{s-w}.$$

Then I_1 is the disjoint union of J and I_2 . Since $A(J; N) = 0$, we get

$$V(J) = \frac{1}{N} |D(J; N)| \leq \frac{1}{N} |D(I_1; N)| + \frac{1}{N} |D(I_2; N)| \leq 2D_N^*.$$

Using $\varrho(C) = \sum_{i=1}^w d_i$ we obtain

$$D_N^* \geq \frac{1}{2} V(J) = \frac{1}{2} (q-a-1)q^{-d_1-\dots-d_w} = \frac{1}{2} (q-a-1)q^{-\varrho(C)} > \frac{q-1}{3} q^{-\varrho(C)}.$$

In the second case let $a \geq (q-1)/3$. Then from $A(J; N) = 0$ we get

$$D_N^* \geq \frac{1}{N} |D(J; N)| = V(J) = aq^{-d_1-\dots-d_w} = aq^{-\varrho(C)} \geq \frac{q-1}{3} q^{-\varrho(C)}.$$

Thus in both cases we have the first inequality in Theorem 1. If $\lambda_{ij}(0) = 0$ for $1 \leq i \leq s$ and $1 \leq j \leq m$, then from (8) we get $b = 0$, hence $a = 0$. Thus from the first case above we obtain

$$D_N^* \geq \frac{1}{2} (q-a-1)q^{-\varrho(C)} = \frac{q-1}{2} q^{-\varrho(C)},$$

and so the second inequality in Theorem 1 is shown. □

Remark 1. Since the proof of Theorem 1 is based on the construction of an interval J containing none of the points \mathbf{x}_n in (3), it follows that the lower bounds in Theorem 1 also hold for any point set consisting of the \mathbf{x}_n with n running through an arbitrary nonempty subset of $\{1, 2, \dots, q^m\}$.

Now let q be prime and put $C(q) = (-q/2, q/2] \cap \mathbf{Z}$, $C^*(q) = C(q) \setminus \{0\}$. For $(h_1, \dots, h_m) \in C(q)^m$ define $d(h_1, \dots, h_m)$ to be the largest index d with $h_d \neq 0$, provided that $(h_1, \dots, h_m) \neq (0, \dots, 0)$, and put $d(0, \dots, 0) = 0$. For $q = 2$ we put

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

and for $q > 2$ we put

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

where $d = d(h_1, \dots, h_m)$ and where $\sigma(d, m) = 1$ for $d < m$ and $\sigma(m, m) = 0$. Let $C(q)^{ms}$ be the set of ms -dimensional lattice points \mathbf{h} with coordinates indexed in the lexicographic form

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

where $h_{ij} \in C(q)$ for $1 \leq i \leq s, 1 \leq j \leq m$. For each such \mathbf{h} we define

$$P_q(\mathbf{h}) = \prod_{i=1}^s Q_q(h_{i1}, \dots, h_{im}).$$

For the system $C = (c_j^{(i)})$ of vectors in Definition 2 we set

$$R(C) = \sum_{\mathbf{h}} P_q(\mathbf{h}), \tag{9}$$

the sum running over all nonzero $\mathbf{h} = (h_{ij}) \in C(q)^{ms}$ with

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

where the h_{ij} are viewed as elements of F_q . Note that since we have assumed q to be prime, F_q and B_q can be identified.

Theorem 2. *If q is prime and every λ_{ij} is the identity map, then the star discrepancy D_N^* with $N = q^m$ of the point set (3) satisfies*

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

Proof. By the assumption on the λ_{ij} we have

$$x_{nj}^{(i)} = \sum_{r=0}^{m-1} c_{jr}^{(i)} \psi_r(a_r(n)) \quad \text{for } 1 \leq n \leq q^m, 1 \leq i \leq s, 1 \leq j \leq m.$$

We can now apply a general inequality for the star discrepancy in terms of exponential sums given in [13, Satz 2] (see also [15, Lemma 2]), which yields

$$D_N^* \leq 1 - \left(1 - \frac{1}{N}\right)^s + \sum_{\mathbf{h} \neq \mathbf{0}} P_q(\mathbf{h}) \left| \frac{1}{N} \sum_{n=1}^N e\left(\frac{1}{q} \sum_{i=1}^s \sum_{j=1}^m h_{ij} x_{nj}^{(i)}\right) \right|, \quad (10)$$

where the outer sum is over all nonzero $\mathbf{h} = (h_{ij}) \in C(q)^{ms}$ and where $e(u) = e^{2\pi\sqrt{-1}u}$ for real u . For fixed \mathbf{h} we have

$$\begin{aligned} \sum_{n=1}^N e\left(\frac{1}{q} \sum_{i=1}^s \sum_{j=1}^m h_{ij} x_{nj}^{(i)}\right) &= \sum_{b_0, \dots, b_{m-1} \in B_q} e\left(\frac{1}{q} \sum_{i=1}^s \sum_{j=1}^m h_{ij} \sum_{r=0}^{m-1} c_{jr}^{(i)} b_r\right) \\ &= \sum_{b_0, \dots, b_{m-1} \in B_q} e\left(\frac{1}{q} \sum_{r=0}^{m-1} b_r \sum_{i=1}^s \sum_{j=1}^m h_{ij} c_{jr}^{(i)}\right) \\ &= \prod_{r=0}^{m-1} \left(\sum_{b=0}^{q-1} e\left(\frac{b}{q} \sum_{i=1}^s \sum_{j=1}^m h_{ij} c_{jr}^{(i)}\right) \right). \end{aligned}$$

The last expression is equal to $q^m = N$ if

$$\sum_{i=1}^s \sum_{j=1}^m h_{ij} c_{jr}^{(i)} = 0 \in F_q \quad \text{for } 0 \leq r \leq m-1 \quad (11)$$

and equal to 0 otherwise, where the h_{ij} are viewed as elements of F_q . The condition (11) is equivalent to

$$\sum_{i=1}^s \sum_{j=1}^m h_{ij} c_j^{(i)} = 0 \in F_q^m.$$

The theorem now follows from (10) and the definition of $R(C)$ in (9). \square

Next we determine the average order of magnitude of the quantity $R(C)$ in (9). For a prime q and for integers $m \geq 1$ and $s \geq 2$ let

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

be the mean value of $R(C)$ extended over the set \mathcal{C} of all choices for a system $C = \{c_j^{(i)} \in F_q^m : 1 \leq i \leq s, 1 \leq j \leq m\}$.

Theorem 3. Let q be a prime, let $m \geq 1$ and $s \geq 2$ be integers, and put $N = q^m$. Then we have

$$M_q(m, s) = \frac{1}{N} \left(\frac{\log N}{\log 4} + 1 \right)^s - \frac{1}{N} \quad \text{if } q = 2,$$

$$M_q(m, s) = \frac{1}{N} \left(\frac{m}{q} \sum_{h \in C^*(q)} \csc \frac{\pi|h|}{q} + m - \frac{m-1}{q} \right)^s - \frac{1}{N}$$

$$< \frac{1}{N} \left(\left(\frac{2}{\pi} + \frac{7}{5 \log q} - \frac{1}{q \log q} \right) \log N + \frac{1}{q} \right)^s - \frac{1}{N} \quad \text{if } q > 2.$$

Proof. Inserting the definition of $R(C)$ into the expression for $M_q(m, s)$ and interchanging the order of summation we get

$$M_q(m, s) = \frac{1}{\text{card}(C)} \sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}) \sum_C 1,$$

where the outer sum is over all nonzero $\mathbf{h} = (h_{ij}) \in C(q)^{ms}$ and the inner sum is over all $C = (c_j^{(i)}) \in \mathcal{C}$ for which

$$\sum_{i=1}^s \sum_{j=1}^m h_{ij} c_j^{(i)} = 0 \in F_q^m. \quad (12)$$

For a fixed nonzero $\mathbf{h} \in C(q)^{ms}$, the inner sum in the last expression for $M_q(m, s)$ represents the number of solutions $(c_j^{(i)}) \in \mathcal{C}$ of the vector equation (12). Since at least one h_{ij} is a nonzero element of F_q , we can choose $ms - 1$ vectors $c_j^{(i)} \in F_q^m$ arbitrarily, and the remaining vector is then uniquely determined by (12). Therefore the number of solutions of (12) is $q^{(ms-1)m}$. Since $\text{card}(C) = q^{m^2 s}$, it follows that

$$M_q(m, s) = q^{-m^2 s} q^{(ms-1)m} \sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}) = \frac{1}{N} \sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}).$$

If $q = 2$, then [15, Lemma 3] yields

$$\sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}) = \left(\frac{m}{2} + 1 \right)^s - 1 = \left(\frac{\log N}{\log 4} + 1 \right)^s - 1,$$

and the formula for $M_q(m, s)$ follows. If $q > 2$, then from the proof of [15, Lemma 3] we obtain

$$\sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}) = \left(\frac{m}{q} \sum_{h \in C^*(q)} \csc \frac{\pi|h|}{q} + m - \frac{m-1}{q} \right)^s - 1,$$

and the result of [15, Lemma 3] shows that

$$\sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}) < \left(\frac{2}{\pi} \log N + \frac{7}{5} m - \frac{m-1}{q} \right)^s - 1.$$

This yields the desired results for $q > 2$. □

Corollary 1. *If q is prime, every λ_{ij} is the identity map, and $m \geq 1$ and $s \geq 2$ are fixed, then the construction of the point sets (3) yields on the average a point set with star discrepancy $D_N^* = O(N^{-1}(\log N)^s)$, where $N = q^m$.*

Proof. This follows from Theorems 2 and 3. □

3. NETS OBTAINED FROM RATIONAL FUNCTIONS OVER FINITE FIELDS

We now specialize the construction in Section 2 by choosing the elements $c_{jr}^{(i)} \in F_q$ as the coefficients in the Laurent series expansions of certain rational functions over F_q . A different application of this device was already used in [18] for the construction of low-discrepancy sequences. Let $F_q((x^{-1}))$ be the field of formal Laurent series

$$L = \sum_{k=w}^{\infty} t_k x^{-k}$$

in the variable x^{-1} , where all $t_k \in F_q$ and w is an arbitrary integer. Define the discrete exponential valuation ν on $F_q((x^{-1}))$ as follows: for $L \neq 0$ put $\nu(L) = -w$ if w is the least index with $t_w \neq 0$, and for $L = 0$ put $\nu(L) = -\infty$. The field $F_q((x^{-1}))$ contains the field of rational functions over F_q as a subfield.

Let $f \in F_q[x]$ with $\deg(f) = m \geq 1$ and let $g_1, \dots, g_s \in F_q[x]$ with $\deg(g_i) < m$ for $1 \leq i \leq s$, where $s \geq 2$. Consider the expansions

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

Then define

$$c_{jr}^{(i)} = u_{r+j}^{(i)} \quad \text{for } 1 \leq i \leq s, 1 \leq j \leq m, 0 \leq r \leq m-1. \quad (13)$$

With this special choice of the $c_{jr}^{(i)}$ we use the construction at the beginning of Section 2 and obtain the point set

$$\mathbf{x}_n = \left(x_n^{(1)}, \dots, x_n^{(s)} \right) \in I^s \quad \text{for } 1 \leq n \leq q^m. \quad (14)$$

We write $\mathbf{g} = (g_1, \dots, g_s) \in F_q[x]^s$ for the s -tuple of polynomials g_1, \dots, g_s . For an arbitrary $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ we define the "inner product"

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

We use the convention $\deg(0) = -1$.

Definition 3. If f and g are as above, then we define

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

where the minimum is extended over all nonzero $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \leq i \leq s$ and $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$.

Note the similarity of this definition with that of the figure of merit in the theory of good lattice points (see [11, p. 986]). For this reason we may call $\varrho(g, f)$ the *figure of merit* of $\mathbf{g} \pmod{f}$.

Lemma 2. If C is the system of vectors

$$c_j^{(i)} = (c_{j0}^{(i)}, c_{j1}^{(i)}, \dots, c_{j,m-1}^{(i)}) \in F_q^m \quad \text{for } 1 \leq i \leq s \quad \text{and } 1 \leq j \leq m,$$

where the $c_{jr}^{(i)}$ are given by (13), then $\varrho(C) = \varrho(g, f)$.

Proof. We first show that for $h_{ij} \in F_q, 1 \leq i \leq s, 1 \leq j \leq m$, we have

$$\sum_{i=1}^s \sum_{j=1}^m h_{ij} c_j^{(i)} = 0 \in F_q^m \tag{15}$$

if and only if $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$, where $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with

$$h_i(x) = \sum_{j=1}^m h_{ij} x^{j-1} \in F_q[x] \quad \text{for } 1 \leq i \leq s. \tag{16}$$

By comparing components, (15) is equivalent to

$$\sum_{i=1}^s \sum_{j=1}^m h_{ij} u_{r+j}^{(i)} = 0 \quad \text{for } 0 \leq r \leq m-1. \tag{17}$$

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

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

Thus for $r \geq 0$ the coefficient of x^{-r-1} in $h_i g_i / f$ is $\sum_{j=1}^m h_{ij} u_{r+j}^{(i)}$. Therefore the condition (17) is equivalent to the following: for $0 \leq r \leq m-1$ the coefficient of x^{-r-1} in $\sum_{i=1}^s h_i g_i / f$ is 0. This means that

$$\sum_{i=1}^s \frac{h_i g_i}{f} = f_1 + L,$$

where $f_1 \in F_q[x]$ and $L \in F_q((x^{-1}))$ with $\nu(L) < -m$. The last identity is equivalent to

$$\mathbf{h} \cdot \mathbf{g} - f_1 f = Lf.$$

On the left-hand side we have a polynomial over F_q , whereas on the right-hand side we have $\nu(Lf) < 0$ since $\nu(f) = \deg(f) = m$. This is only possible if $Lf = 0$, i.e., if $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$. Hence the claim that (15) is equivalent to $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$ is established.

Now let the nonzero s -tuple (d_1, \dots, d_s) of integers with $0 \leq d_i \leq m$ for $1 \leq i \leq s$ be such that the system $\{c_j^{(i)} : 1 \leq j \leq d_i, 1 \leq i \leq s\}$ is linearly dependent over F_q . Then there exist $h_{ij} \in F_q, 1 \leq j \leq d_i, 1 \leq i \leq s$, not all 0 such that

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

and by putting $h_{ij} = 0$ for $d_i < j \leq m, 1 \leq i \leq s$, we get an identity of the form (15). By what we have already shown, it follows that $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$, where $\mathbf{h} = (h_1, \dots, h_s) \neq 0$ with the polynomials h_i in (16). Hence from Definition 3 we obtain

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

thus $\varrho(\mathbf{g}, f) \leq \varrho(C)$ by Definition 2. On the other hand, if for a nonzero $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \leq i \leq s$ we have $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$, then with the elements $h_{ij} \in F_q, 1 \leq i \leq s, 1 \leq j \leq m$, determined by (16) we get (15). Thus the system $\{c_j^{(i)} : 1 \leq j \leq \deg(h_i) + 1, 1 \leq i \leq s\}$ is linearly dependent over F_q , and from this we deduce $\varrho(\mathbf{g}, f) \geq \varrho(C)$. \square

Remark 2. From Lemma 2 and [16, Proposition 6.9] we obtain that we always have $1 \leq \varrho(\mathbf{g}, f) \leq m + 1$. Therefore the condition $\deg(h_i) < m$ for $1 \leq i \leq s$ in Definition 3 may be omitted.

Theorem 4. *The point set (14) is a (t, m, s) -net in base q with $t = m + 1 - \varrho(\mathbf{g}, f)$.*

Proof. This follows from Lemmas 1 and 2. \square

Theorem 4 and (1) yield the following upper bound for the star discrepancy D_N^* of the point set (14) with $N = q^m$:

$$D_N^* \leq B(s, q) q^{1 - \varrho(\mathbf{g}, f)} (\log N)^{s-1} + O\left(q^{-\varrho(\mathbf{g}, f)} (\log N)^{s-2}\right), \quad (18)$$

where $B(s, q)$ is given by (2) and where the constant implied by the Landau symbol depends only on s and q . Lower bounds for D_N^* are obtained from (5) and Theorem 1, where in the latter we can use $\varrho(C) = \varrho(\mathbf{g}, f)$. These results for D_N^* demonstrate

that in order to obtain a low-discrepancy point set from the construction of the point sets (14), we have to choose f and g in such a way that the figure of merit $\varrho(g, f)$ is large. Large values of $\varrho(g, f)$ have already been determined in certain special cases since this figure of merit occurs also in the context of pseudorandom number generation. We refer to [1,9] for such calculations, which deal e.g. with g of the form $g = (1, x^m, x^{2m}, \dots, x^{(s-1)m})$ with each entry reduced mod f .

Another upper bound for the star discrepancy of the point sets (14) can be obtained in the case where q is prime and every λ_{ij} is the identity map, namely by specializing Theorem 2. If $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \leq i \leq s$, then we can use (16) and the fact that $C(q)$ forms a complete residue system mod q to identify \mathbf{h} with an ms -tuple $\mathbf{h}^* = (h_{ij}) \in C(q)^{ms}$, and we put $P_q(\mathbf{h}) = P_q(\mathbf{h}^*)$. In analogy with (9) we then define

$$R(g, f) = \sum_{\mathbf{h}} P_q(\mathbf{h}), \quad (19)$$

where the sum is over all nonzero $\mathbf{h} = (h_1, \dots, h_s) \in F_q[x]^s$ with $\deg(h_i) < m$ for $1 \leq i \leq s$ and $\mathbf{h} \cdot g \equiv 0 \pmod{f}$.

Theorem 5. *If q is prime and every λ_{ij} is the identity map, then the star discrepancy D_N^* with $N = q^m$ of the point set (14) satisfies*

$$D_N^* \leq 1 - \left(1 - \frac{1}{N}\right)^s + R(g, f).$$

Proof. If C is as in Lemma 2, then we have shown in the proof of this lemma that (15) holds if and only if $\mathbf{h} \cdot g \equiv 0 \pmod{f}$. Therefore $R(C) = R(g, f)$, and so the desired result follows from Theorem 2. \square

In the main result of this section we will show that in the special case considered in Theorem 5, the construction of the point sets (14) yields on the average a low-discrepancy point set. For $s \geq 2$ and $f \in F_q[x]$ with q prime and $\deg(f) = m \geq 1$ put

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

Let

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

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

[8, Lemma 3.69] we have

$$\Phi_q(f) = q^m \prod_{k=1}^r (1 - q^{-n_k}), \quad (20)$$

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

The proof of the following theorem depends on the theory of arithmetic functions on $F_q[x]$ as developed by Carlitz [3] and on the theory of characters of $F_q((x^{-1}))$ as developed by Carlitz [4] and Hayes [6]. In the sequel, an *arithmetic function* is a real-valued function on the multiplicative semigroup S_q of monic polynomials over F_q . An arithmetic function H is called *multiplicative* (resp. *additive*) if $H(gh) = H(g)H(h)$ (resp. $H(gh) = H(g) + H(h)$) for all $g, h \in S_q$ with $\gcd(g, h) = 1$. We write $\sum_{v \bmod f}$ for a sum over all $v \in F_q[x]$ with $\deg(v) < \deg(f)$, and we write $\sum_{v \bmod f}^*$ if the additional condition $\gcd(v, f) = 1$ is imposed. Furthermore, $\sum_{d|f}$ denotes a sum over all $d \in S_q$ dividing f .

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

$$\sum_{v \bmod f} X_q\left(\frac{vg}{f}\right) = \begin{cases} q^{\deg(f)} & \text{if } g \equiv 0 \pmod{f}, \\ 0 & \text{if } g \not\equiv 0 \pmod{f}. \end{cases} \quad (21)$$

See e.g. Car [2, p. 8] for this formula.

Theorem 6. *Let q be a prime, let $s \geq 2$ be an integer, let $f \in F_q[x]$ with $\deg(f) = m \geq 1$, and put $N = q^m$. Then we have*

$$M_s(f) \leq \frac{1}{N} \left(\frac{\log N}{\log 4} + 1 \right)^s - \frac{1}{N} \quad \text{if } q = 2,$$

$$M_s(f) < \frac{1}{N} \left(\left(\frac{2}{\pi} + \frac{7}{5 \log q} - \frac{1}{q \log q} \right) \log N + \frac{1}{q} \right)^s + \frac{(q-1)s}{qN} \left(1 + \frac{q-1}{q \Phi_q(f)} \right)^{s-1}$$

if $q > 2$.

Proof. We can assume w.l.o.g. that f is monic. Inserting the definition of $R(g, f)$ in (19) into the expression for $M_s(f)$ and interchanging the order of summation we get

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

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

$$M_s(f) = \frac{1}{\Phi_q(f)^s} \sum_{\mathbf{h}} A(\mathbf{h}) P_q(\mathbf{h}) - 1, \quad (22)$$

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

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

by (21). By the definition of $P_q(\mathbf{h})$ we can write

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

where we use (16) to identify h_i with $(h_{i1}, \dots, h_{im}) \in C(q)^m$ and we define $Q_q(h_i)$ to be the quantity $Q_q(h_{i1}, \dots, h_{im})$ in Section 2. Then we get

$$\begin{aligned} \sum_{\mathbf{h}} A(\mathbf{h}) P_q(\mathbf{h}) &= \frac{1}{N} \sum_{v \bmod f} \sum_{\mathbf{h}} \sum_{\mathbf{g} \in G_s(f)} X_q \left(\frac{v}{f} \mathbf{h} \cdot \mathbf{g} \right) P_q(\mathbf{h}) \\ &= \frac{1}{N} \sum_{v \bmod f} \sum_{h_1 \bmod f} \dots \sum_{h_s \bmod f} \sum_{g_1 \bmod f}^* \dots \sum_{g_s \bmod f}^* X_q \left(\frac{v}{f} h_1 g_1 \right) \dots \\ &\quad \times X_q \left(\frac{v}{f} h_s g_s \right) Q_q(h_1) \dots Q_q(h_s) \\ &= \frac{1}{N} \sum_{v \bmod f} Y_q(v, f)^s \end{aligned}$$

with

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

Now

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

thus

$$\sum_{\mathbf{h}} A(\mathbf{h}) P_q(\mathbf{h}) = \frac{1}{N} \Phi_q(f)^s \left(\sum_{h \bmod f} Q_q(h) \right)^s + \frac{1}{N} \sum_{\substack{v \bmod f \\ v \neq 0}} Y_q(v, f)^s. \quad (23)$$

Let μ_q be the M“obius function on S_q (see [3] and [8, p. 145]) and note that μ_q is multiplicative. Let us abbreviate $\gcd(g, f)$ by (g, f) in this proof. Then for fixed

$v \in F_q[x]$ with $0 \leq \deg(v) < m$ we get

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

where in the last step we changed d into f/d . Applying (21) to the innermost sum we obtain

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

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

$$Y_q(v, f) = \sum_{d|f} \mu_q\left(\frac{f}{d}\right) q^{\deg(d)} E_q\left(\frac{d}{(d, v)}, f\right), \quad (24)$$

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

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

If $a = f$, then

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

Now let $a \neq f$, then

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

For $q = 2$ we have

$$\begin{aligned}
 \sum_{\substack{b \bmod f/a \\ b \neq 0}} Q_q(ab) &= \sum_{\substack{b \bmod f/a \\ b \neq 0}} 2^{-\deg(ab)-1} = 2^{-\deg(a)-1} \sum_{k=0}^{\deg(f/a)-1} 2^{-k} 2^k \\
 &= \deg\left(\frac{f}{a}\right) 2^{-\deg(a)-1}.
 \end{aligned}$$

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

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

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

$$\begin{aligned} \sum_{\substack{b \bmod f/a \\ b \neq 0}} Q_q(ab) &= \sum_{\substack{b \bmod f/a \\ b \neq 0}} q^{-\deg(ab)-1} \left(\csc \frac{\pi}{q} |\operatorname{sgn}(b)| + \sigma(\deg(b), \deg\left(\frac{f}{a}\right) - 1) \right) \\ &= q^{-\deg(a)-1} \sum_{k=0}^{\deg(f/a)-1} q^{-k} q^k \sum_{z \in C^*(q)} \left(\csc \frac{\pi|z|}{q} + \sigma(k, \deg\left(\frac{f}{a}\right) - 1) \right) \\ &= \deg\left(\frac{f}{a}\right) q^{-\deg(a)-1} \sum_{z \in C^*(q)} \csc \frac{\pi|z|}{q} + (q-1) \left(\deg\left(\frac{f}{a}\right) - 1 \right) q^{-\deg(a)-1} \\ &= T_q \deg\left(\frac{f}{a}\right) q^{-\deg(a)} - \varepsilon_q q^{-\deg(a)} \end{aligned}$$

with

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

$$\varepsilon_q = \frac{q-1}{q} \quad \text{for } q > 2.$$

The case $q = 2$ is also covered by the formula above if we put $T_2 = \frac{1}{2}$ and $\varepsilon_2 = 0$. To include the case $a = f$, we put

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

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

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

Applying this formula with $a = d/(d, v)$ in (24), we obtain

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

thus

$$Y_q(v, f) = \Phi_q(f) + (mT_q - \varepsilon_q)H_q^{(1)}(v, f) - T_q H_q^{(2)}(v, f) + H_q^{(3)}(v, f) \quad (25)$$

with

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

In the rest of the proof p will always stand for a monic irreducible polynomial over F_q . For a nonzero $v \in F_q[x]$ let $e_p(v)$ be the largest nonnegative integer such that $p^{e_p(v)}$ divides v . Now we consider $H_q^{(1)}(v, f)$ for a fixed $v \neq 0$. Since $q^{\deg((d, v))}$ is a multiplicative function of d , it follows that $H_q^{(1)}(v, f)$ is a multiplicative function of f . For any integer $k \geq 1$ we have

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

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

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

by (20). By multiplicativity we obtain

$$H_q^{(1)}(v, f) = \begin{cases} \Phi_q(f) & \text{if } v \equiv 0 \pmod{f}, \\ 0 & \text{if } v \not\equiv 0 \pmod{f}. \end{cases} \quad (26)$$

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

$$H_q^{(2)}(v, f) = \sum_{p|f} H_q^{(2)}(v, p^{e_p(f)}) H_q^{(1)}(v, f/p^{e_p(f)}). \quad (27)$$

For any integer $k \geq 1$ we have

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

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

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

By (26) and (27) we get

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

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

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

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

Now we consider $H_q^{(3)}(v, f)$. Note that $\varepsilon_q(d/(d, v), f) \neq 0$ only if $q > 2$ and $d/(d, v) = f$. But since d divides f , we have $d/(d, v) = f$ if and only if $d = f$ and $(f, v) = 1$. Thus if $q > 2$ and $(f, v) = 1$, then $H_q^{(3)}(v, f) = (q - 1)/q$. In all other cases we have $H_q^{(3)}(v, f) = 0$. Now we go back to (25) and use the formulas for $H_q^{(k)}(v, f)$, $k = 1, 2$, established above. For $v \in F_q[x]$ with $0 \leq \deg(v) < m$ we have $H_q^{(1)}(v, f) = 0$ by (26), therefore

$$Y_q(v, f) = \Phi_q(f) - T_q \deg(p)q^{e_p(v)\deg(p)}\Phi_q\left(f/p^{e_p(f)}\right) + H_q^{(3)}(v, f)$$

if there exists a unique p with $e_p(v) < e_p(f)$, and otherwise

$$Y_q(v, f) = \Phi_q(f) + H_q^{(3)}(v, f).$$

Thus we always have

$$Y_q(v, f) \leq \Phi_q(f) + H_q^{(3)}(v, f). \quad (28)$$

Next we will prove that

$$Y_q(v, f) \geq 0. \quad (29)$$

The only case where (29) is not immediate is when there exists a unique p with $e_p(v) < e_p(f)$. In this case it will suffice to show that

$$T_q \deg(p)q^{e_p(v)\deg(p)}\Phi_q\left(f/p^{e_p(f)}\right) \leq \Phi_q(f),$$

or equivalently that

$$T_q \deg(p)q^{e_p(v)\deg(p)} \leq \frac{\Phi_q(f)}{\Phi_q\left(f/p^{e_p(f)}\right)} = q^{e_p(f)\deg(p)}\left(1 - q^{-\deg(p)}\right),$$

where the last identity follows from (20). Since $e_p(v) < e_p(f)$, it will be enough to show that

$$T_q \deg(p) \leq q^{\deg(p)} (1 - q^{-\deg(p)}) = q^{\deg(p)} - 1. \quad (30)$$

If $q = 2$, then $T_q = \frac{1}{2}$, and so (30) is trivial. If $q > 2$, then

$$T_q = \frac{1}{q} \left(q - 1 + \sum_{z \in C^*(q)} \csc \frac{\pi|z|}{q} \right) < \frac{2}{\pi} \log q + \frac{7}{5} - \frac{1}{q}$$

by an inequality in [10, p. 574]. Furthermore, by induction on k we obtain

$$q^k > \left(\frac{2}{\pi} \log q + \frac{7}{5} - \frac{1}{q} \right) k + 1 \quad \text{for } k \geq 1,$$

hence (30) follows for $q > 2$. Thus (29) is established.

Now let $q = 2$ and use (23), (28), and (29) as well as $H_2^{(3)}(v, f) = 0$ to obtain

$$\begin{aligned} \sum_{\mathbf{h}} A(\mathbf{h})P_q(\mathbf{h}) &\leq \frac{1}{N} \Phi_q(f)^s \left(\sum_{h \bmod f} Q_q(h) \right)^s + \frac{1}{N} \sum_{\substack{v \bmod f \\ v \neq 0}} \Phi_q(f)^s \\ &= \frac{1}{N} \Phi_q(f)^s \left(\frac{m}{2} + 1 \right)^s + \Phi_q(f)^s \left(1 - \frac{1}{N} \right), \end{aligned}$$

where in the last step we applied [15, Lemma 3]. Together with (22) this yields

$$M_s(f) \leq \frac{1}{N} \left(\frac{m}{2} + 1 \right)^s - \frac{1}{N},$$

which is the result of the theorem for $q = 2$.

For $q > 2$ we use (23), (28), and (29) as well as the formula for $H_q^{(3)}(v, f)$ to obtain

$$\begin{aligned} \sum_{\mathbf{h}} A(\mathbf{h})P_q(\mathbf{h}) &\leq \\ &\leq \frac{1}{N} \Phi_q(f)^s \left(\sum_{h \bmod f} Q_q(h) \right)^s + \frac{1}{N} \sum_{v \bmod f}^* \left(\Phi_q(f) + \frac{q-1}{q} \right)^s \\ &\quad + \frac{1}{N} \sum_{\substack{v \bmod f \\ v \neq 0, (f, v) \neq 1}} \Phi_q(f)^s \\ &= \frac{1}{N} \Phi_q(f)^s \left(\sum_{h \bmod f} Q_q(h) \right)^s \\ &\quad + \frac{1}{N} \Phi_q(f) \left(\Phi_q(f) + \frac{q-1}{q} \right)^s + \frac{1}{N} (N-1 - \Phi_q(f)) \Phi_q(f)^s \\ &= \frac{1}{N} \Phi_q(f)^s \left(\sum_{h \bmod f} Q_q(h) \right)^s + \frac{1}{N} \Phi_q(f) \left(\left(\Phi_q(f) + \frac{q-1}{q} \right)^s - \Phi_q(f)^s \right) \\ &\quad + \left(1 - \frac{1}{N} \right) \Phi_q(f)^s. \end{aligned}$$

Together with (22) this yields

$$M_s(f) \leq \frac{1}{N} \left(\sum_{h \bmod f} Q_q(h) \right)^s + \frac{1}{N} \Phi_q(f) \left(\left(1 + \frac{q-1}{q\Phi_q(f)} \right)^s - 1 \right) - \frac{1}{N}$$

$$< \frac{1}{N} \left(\frac{2}{\pi} m \log q + \frac{7}{5} m - \frac{m-1}{q} \right)^s + \frac{(q-1)s}{qN} \left(1 + \frac{q-1}{q\Phi_q(f)} \right)^{s-1},$$

where in the last step we applied [15, Lemma 3] and the mean-value theorem. This is the result of the theorem for $q > 2$. \square

Corollary 2. *If q is prime, every λ_{ij} is the identity map, and $s \geq 2$ and $f \in F_q[x]$ with $\deg(f) = m \geq 1$ are fixed, then the construction of the point sets (14) yields on the average a point set with star discrepancy $D_N^* = O(N^{-1}(\log N)^s)$, where $N = q^m$.*

Proof. This follows from Theorems 5 and 6. \square

Remark 3. In the special case where f is irreducible over F_q , q prime, a result of the same type as Theorem 6 can be shown in a much easier fashion. Put $m = \deg(f)$ and let

$$G'_s(f) = \{ \mathbf{g} = (g_1, \dots, g_s) \in F_q[x]^s : \deg(g_i) < m \text{ for } 1 \leq i \leq s \},$$

$$M'_s(f) = \frac{1}{\text{card}(G'_s(f))} \sum_{\mathbf{g} \in G'_s(f)} R(\mathbf{g}, f).$$

Then $\text{card}(G'_s(f)) = q^{ms}$, and in the same way as in the beginning of the proof of Theorem 6 we obtain

$$M'_s(f) = q^{-ms} \sum_{\mathbf{h} \neq 0} A'(\mathbf{h}) P_q(\mathbf{h}),$$

where $A'(\mathbf{h})$ is the number of $\mathbf{g} \in G'_s(f)$ with $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$. For every \mathbf{h} in the range of summation we have $A'(\mathbf{h}) = q^{m(s-1)}$, since $s-1$ entries of \mathbf{g} can be prescribed arbitrarily and the remaining entry is uniquely determined because of the irreducibility of f . Thus with $N = q^m$ we obtain

$$M'_s(f) = \frac{1}{N} \sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}),$$

and so [15, Lemma 3] yields

$$M'_s(f) = \frac{1}{N} \left(\frac{\log N}{\log 4} + 1 \right)^s - \frac{1}{N} \quad \text{if } q = 2,$$

$$M'_s(f) < \frac{1}{N} \left(\left(\frac{2}{\pi} + \frac{7}{5 \log q} - \frac{1}{q \log q} \right) \log N + \frac{1}{q} \right)^s - \frac{1}{N} \quad \text{if } q > 2.$$

This special case, with $q = 2$, was also considered by Tezuka [22], but compare with Remark 5 below.

Remark 4. If q is prime and f is irreducible over F_q , then the average of $R(\mathbf{g}, f)$ over a much smaller set than $G'_s(f)$ already yields a bound comparable to that in Remark 3. Put again $m = \deg(f)$ and let $K_s(f)$ be the set of all \mathbf{g} of the form $\mathbf{g} = (1, g, g^2, \dots, g^{s-1})$ with each entry reduced mod f , where g runs through all polynomials over F_q of degree $< m$. Let

$$L_s(f) = \frac{1}{\text{card}(K_s(f))} \sum_{\mathbf{g} \in K_s(f)} R(\mathbf{g}, f).$$

Since $\text{card}(K_s(f)) = q^m$, we obtain

$$L_s(f) = q^{-m} \sum_{\mathbf{h} \neq 0} A_1(\mathbf{h}) P_q(\mathbf{h}),$$

where $A_1(\mathbf{h})$ is the number of $\mathbf{g} \in K_s(f)$ with $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$. For every \mathbf{h} in the range of summation, $\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$ can be viewed as a nonzero polynomial equation for g of degree $\leq s-1$ in the field $F_q[x]/(f)$, and so $A_1(\mathbf{h}) \leq s-1$. Thus with $N = q^m$ we obtain

$$L_s(f) \leq \frac{s-1}{N} \sum_{\mathbf{h} \neq 0} P_q(\mathbf{h}) = (s-1)M'_s(f),$$

and so the results on $M'_s(f)$ in Remark 3 yield

$$L_s(f) \leq \frac{s-1}{N} \left(\frac{\log N}{\log 4} + 1 \right)^s - \frac{s-1}{N} \quad \text{if } q = 2,$$

$$L_s(f) < \frac{s-1}{N} \left(\left(\frac{2}{\pi} + \frac{7}{5 \log q} - \frac{1}{q \log q} \right) \log N + \frac{1}{q} \right)^s - \frac{s-1}{N} \quad \text{if } q > 2.$$

In the case $s = 2$ there is a connection between the figure of merit $\varrho(\mathbf{g}, f)$ and continued fractions for rational functions over F_q , where q is again an arbitrary prime power. Let $\mathbf{g} = (g_1, g_2) \in F_q[x]^2$ with $\deg(g_i) < m = \deg(f)$ and $\gcd(g_i, f) = 1$ for $i = 1, 2$. Then the condition $\mathbf{h} \cdot \mathbf{g} = h_1 g_1 + h_2 g_2 \equiv 0 \pmod{f}$ in Definition 3 is equivalent to $h_1 + h_2 g_1^* g_2 \equiv 0 \pmod{f}$, where $g_1^* \in F_q[x]$ with $g_1 g_1^* \equiv 1 \pmod{f}$. Thus it suffices to consider the figure of merit for pairs \mathbf{g} of the form $\mathbf{g} = (1, g)$ with $g \in F_q[x]$, $\deg(g) < m$, and $\gcd(g, f) = 1$. Let

$$\frac{g}{f} = [A_1, A_2, \dots, A_u]$$

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

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

Then we have

$$\varrho(\mathbf{g}, f) = m + 2 - K\left(\frac{g}{f}\right), \quad (31)$$

which is shown in exactly the same way as the special case considered in [13, Satz 12]. Thus the desirable $\mathbf{g} = (1, g)$ are those with small $K(g/f)$. The quantity $K(g/f)$ was studied in detail in [14]. It is clear that for any $m \geq 1$ we can obtain a rational function g/f with $K(g/f) = 1$ and $\deg(f) = m$, by choosing partial quotients A_1, \dots, A_m with $\deg(A_r) = 1$ for $1 \leq r \leq m$. Then from (31) we get $\varrho(\mathbf{g}, f) = m + 1$ for $\mathbf{g} = (1, g)$, which is the maximum possible value of the figure of merit by Remark 2. With this choice of \mathbf{g} and f we obtain a two-dimensional point set with $D_N^* = O(N^{-1} \log N)$ according to (18), where $N = q^m$. Note that by the general lower bound of Schmidt [20] this is the smallest order of magnitude which can be achieved by the star discrepancy of a two-dimensional point set.

For the efficient implementation of the point sets (14) we can use similar principles as in [18, Sect. 6]. For fixed i the sequence $u_1^{(i)}, u_2^{(i)}, \dots$ is a linear recurring sequence with characteristic polynomial f . Therefore the elements $c_{j_r}^{(i)}$ in (13) can be calculated by linear recurrence relations. The calculation of the $c_{j_r}^{(i)}$ is even easier if we choose $f(x) = x^m$. To simplify the construction, the bijections ψ_r in Section 2 may all be chosen to be the same map, and the same can be done for the bijections λ_{ij} in Section 2. If q is prime, then all these bijections can be taken to be the identity map.

Remark 5. If f is irreducible over F_q , then the $c_{j_r}^{(i)}$ in (13) can also be represented as follows. As noted above, the sequence $u_1^{(i)}, u_2^{(i)}, \dots$ is a linear recurring sequence with characteristic polynomial f . Thus it follows from [8, Theorem 8.24] that there exist elements $\theta_i, 1 \leq i \leq s$, in the extension field F_N of order $N = q^m$ such that

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

where Tr is the trace function from F_N to F_q and where σ is a root of f in F_N . Hence (13) attains the form

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

Consequently, if q is prime, f is irreducible over F_q , and the bijections ψ_r and λ_{ij} are identity maps, then the construction of the point sets (14) is a special case of the construction in [12, p. 161], where in the latter construction we take $\beta_{ij} = \theta_i \sigma^{j-1} \in F_N$ for $1 \leq i \leq s, 1 \leq j \leq m$. In particular, the recent construction of low-discrepancy point sets by Tezuka [22], which works with $q = 2$, is a special case of the construction in [12, p. 161].

References

- [1] *D. A. André, G. L. Mullen, and H. Niederreiter*: Figures of merit for digital multistep pseudorandom numbers, *Math. Comp.* **54** (1990), 737–748.
- [2] *M. Car*: Sommes de carrés dans $F_q[X]$, *Dissertationes Math.* **215** (1983).
- [3] *L. Carlitz*: The arithmetic of polynomials in a Galois field, *Amer. J. Math.* **54** (1932), 39–50.
- [4] *L. Carlitz*: The singular series for sums of squares of polynomials, *Duke Math. J.* **14** (1947), 1105–1120.
- [5] *H. Faure*: Discrépance de suites associées à un système de numération (en dimension s), *Acta Arith.* **41** (1982), 337–351.
- [6] *D. R. Hayes*: The expression of a polynomial as a sum of three irreducibles, *Acta Arith.* **11** (1966), 461–488.
- [7] *L. K. Hua and Y. Wang*: *Applications of Number Theory to Numerical Analysis*, Springer, Berlin.
- [8] *R. Lidl and H. Niederreiter*: *Finite Fields*, Addison-Wesley, Reading, MA, 1983.
- [9] *G. L. Mullen and H. Niederreiter*: Optimal characteristic polynomials for digital multistep pseudorandom numbers, *Computing* **39** (1987), 155–163.
- [10] *H. Niederreiter*: On the distribution of pseudorandom numbers generated by the linear congruential method. III, *Math. Comp.* **30** (1976), 571–597.
- [11] *H. Niederreiter*: Quasi-Monte Carlo methods and pseudo-random numbers, *Bull. Amer. Math. Soc.* **84** (1978), 957–1041.
- [12] *H. Niederreiter*: Low-discrepancy point sets, *Monatsh. Math.* **102** (1986), 155–167.
- [13] *H. Niederreiter*: Pseudozufallszahlen und die Theorie der Gleichverteilung, *Sitzungsber. Oesterr. Akad. Wiss. Math.-Naturwiss. Kl. Abt. II* **195** (1986), 109–138.
- [14] *H. Niederreiter*: Rational functions with partial quotients of small degree in their continued fraction expansion, *Monatsh. Math.* **103** (1987), 269–288.
- [15] *H. Niederreiter*: A statistical analysis of generalized feedback shift register pseudorandom number generators, *SIAM J. Sci. Statist. Computing* **8** (1987), 1035–1051.
- [16] *H. Niederreiter*: Point sets and sequences with small discrepancy, *Monatsh. Math.* **104** (1987), 273–337.
- [17] *H. Niederreiter*: Quasi-Monte Carlo methods for multidimensional numerical integration, *Numerical Integration III (Oberwolfach 1987)*, *Internat. Series of Numer. Math.*, Vol. 85, Birkhäuser, Basel, 1988, pp. 157–171.
- [18] *H. Niederreiter*: Low-discrepancy and low-dispersion sequences, *J. Number Theory* **30** (1988), 51–70.
- [19] *H. Niederreiter*: A combinatorial problem for vector spaces over finite fields, *Discrete Math.*, to appear.
- [20] *W. M. Schmidt*: Irregularities of distribution. VII, *Acta Arith.* **21** (1972), 45–50.
- [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] *S. Tezuka*: A new family of low-discrepancy point sets, *Tech. Report RT-0031*, IBM Japan, Tokyo, 1990.

Author's address: Austrian Academy of Sciences, Institute for Information Processing, Sonnenfelsgasse 19, A-1010 Vienna, Austria.