Low Discrepancy Polynomial Lattice Point Sets

Peter Kritzer and Friedrich Pillichshammer*

Abstract

Polynomial lattice point sets are polynomial versions of classical lattice point sets and among the most widely used classes of node sets in quasi-Monte Carlo integration algorithms. In this paper, we show the existence of s-dimensional polynomial lattice point sets with N points whose star discrepancy D_N^* satisfies a discrepancy bound of the type $ND_N^* \leq c(\log N)^{s-1} \log\log N$ (c a constant). This result is a substantial extension of an earlier result by Larcher.

Keywords: Polynomial lattice point sets, star discrepancy.

2010 Mathematics Subject Classification: 11K38, 11K06, 15A99.

1 Introduction and Statement of the Result

For a point set $\mathcal{P} = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ of $N \geq 1$ points in the s-dimensional unit cube $[0,1)^s$, the *star discrepancy* is defined by

$$D_N^*(\mathcal{P}) = \sup_B \left| \frac{A_N(B)}{N} - \lambda(B) \right|,$$

where the supremum is extended over all subintervals B of $[0,1)^s$ of the form $B = \prod_{i=1}^s [0, b_i)$, $0 < b_i \leq 1$, $A_N(B)$ denotes the number of n for which $\boldsymbol{x}_n \in B$, and λ is the Lebesgue measure. It should be noted that by "point set" we do not mean a set in the set-theoretic sense, but a collection of points where single points may occur repeatedly. For a finite or infinite sequence ω we denote by $D_N^*(\omega)$ the star discrepancy of the first N terms of ω.

The star discrepancy is a quantitative measure for the irregularity of distribution of $\mathcal{P}$, i.e., the deviation from perfect uniform distribution. Point sets with low star discrepancy are required as nodes of quasi-Monte Carlo algorithms for the integration of high dimensional functions; see the monographs [3, 8] for further information.

It is known that for any dimension s there exists a constant $c(s) > 0$, depending only on s, such that for any point set $\mathcal{P}$ consisting of N points in $[0,1)^s$ we have

$$D_N^*(\mathcal{P}) \geq c(s) \frac{(\log N)^{\kappa_s}}{N},$$

where $\kappa_2 = 1$ (see [1, 11]) and $\kappa_s \geq (s-1)/2$ for $s \geq 3$ which follows from a result of Roth [10]. For $s \geq 3$ the lower bound on κ_s has recently been improved to $\kappa_s \geq (s-1)/2 + \delta_s$ for some unknown $\delta_s \in (0, 1/2)$; see [2]. The exact value of κ_s for $s \geq 3$ is not known until now, but it is

*The authors gratefully acknowledge the support of the Austrian Science Fund (Projects P21943, P23389, and S9609).

conjectured that $\kappa_s = s - 1$. (Throughout the paper there will appear several constants c which are assumed to be different from occurence to occurrence. These constants may depend on the dimension s or on other quantities which are then indicated in parentheses.)

The currently most effective constructions of point sets with small star discrepancy are based on the concept of (t, m, s)-nets in a base b. For a definition of such nets see [3, 8]. In [7] (see also [3, 8]) Niederreiter introduced a special construction of such nets. These types of nets, which are based on rational functions over finite fields, are known as polynomial lattice point sets.

For the construction of a polynomial lattice point set, choose a prime q and let $\mathbb{F}_q$ be the finite field consisting of q elements. We identify $\mathbb{F}_q$ with $\mathbb{Z}_q := \{0, \ldots, q-1\}$ endowed with the usual arithmetic operations modulo q (addition and subtraction modulo q will be denoted by $\oplus$ and $\ominus$, respectively). Furthermore let $\mathbb{F}_q[x]$ be the field of polynomials over $\mathbb{F}_q$, and let $\mathbb{F}_q((x^{-1}))$ be the field of formal Laurent series over $\mathbb{F}_q$, with elements of the form $\sum_{l=z}^{\infty} t_l x^{-l}$, where z is an arbitrary integer and the t_l are arbitrary elements in $\mathbb{F}_q$. Note that the field of Laurent series contains the field of rational functions as a subfield. Given an integer $m \geq 1$, define a map $\phi_m : \mathbb{F}_q((x^{-1})) \to [0, 1)$ by

$$\phi_m\left(\sum_{l=z}^{\infty} t_l x^{-l}\right) := \sum_{l=\max(1,z)}^{m} t_l q^{-l}.$$

For $0 \leq n < q^m$ let $n = n_0 + n_1 q + \cdots + n_{m-1} q^{m-1}$, where $n_i \in \mathbb{Z}_q$, be the q-adic expansion of n. With each such n we associate the polynomial $n(x) = \sum_{r=0}^{m-1} n_r x^r \in \mathbb{F}_q[x]$.

Given a prime q, an integer $m \geq 1$, and a dimension $s \geq 1$, choose an $f \in \mathbb{F}_q[x]$ with $\deg(f) = m$ and s polynomials $g_1, \ldots, g_s \in \mathbb{F}_q[x]$ and define

$$\boldsymbol{x}_n := \left(\phi_m\left(\frac{n(x)g_1(x)}{f(x)}\right), \ldots, \phi_m\left(\frac{n(x)g_s(x)}{f(x)}\right)\right) \quad \text{for } 0 \leq n < q^m.$$

The point set $\mathcal{P}(\boldsymbol{g}, f) = \{\boldsymbol{x}_n : 0 \leq n < q^m\}$, where $\boldsymbol{g} := (g_1, \ldots, g_s)$, is called *polynomial lattice point set*.

For any $s \in \mathbb{N}$ and any prime number q there exists a $c(s, q) > 0$, depending only on s and q, with the following property: for any $f \in \mathbb{F}_q[x]$ with $\deg(f) = m$ there exist $\boldsymbol{g} \in \mathbb{F}_q[x]^s$ such that

$$D_N^*(\mathcal{P}(\boldsymbol{g}, f)) \leq c(s, q)\frac{(\log N)^s}{N}, \tag{1}$$

where $N = q^m$; see [3, 8]. Such $\boldsymbol{g}$ can be constructed by using the so-called component-by-component method (see [3]). There are even vectors $\boldsymbol{g}$ of the form $\boldsymbol{g} = (1, g, \ldots, g^{s-1}) \pmod f$ which satisfy an upper bound of the form (1) (see again [3]). However, it was shown in [4] that the method of proof used to show (1) does not allow an improvement of this upper bound with respect to the order of magnitude in the total number of points N.

In [9] Larcher showed the following improved existence result for the special case $f(x) = x^m$. There exists a $c(s, q) > 0$ with the property that for every $m \in \mathbb{N}$ there exists a vector $\boldsymbol{g} \in \mathbb{F}_q[x]^s$ such that

$$D_N^*(\mathcal{P}(\boldsymbol{g}, x^m)) \leq c(s, q)\frac{(\log N)^{s-1} \log\log N}{N},$$

where $N = q^m$.

It should also be noted that for $s = 2$ and $q = 2$ there is, for any $m \geq 1$, an explicit construction due to Niederreiter of a polynomial $g \in \mathbb{F}_2[x]$ which yields $D_N^*(\mathcal{P}((1, g), x^m)) \leq c(\log N)/N$, where $N = 2^m$ — combine the results from [8, p. 86–88] with [6, Theorem 2].

It is the aim of this paper to show a result corresponding to that of Larcher for all $f \in \mathbb{F}_q[x]$ with $\gcd(f, x) = 1$. To be more precise, we are going to show the following theorem.

Theorem 1 *Let $s \in \mathbb{N}$ and let q be a prime number. Then there exists a $c(s,q) > 0$, depending only on q and s, with the following property: for any polynomial $f \in \mathbb{F}_q[x]$ of degree m with $\gcd(f,x) = 1$ there exists a generating vector $\boldsymbol{g} = (g_1, \ldots, g_s) \in \mathbb{F}_q[x]^s$ of monic polynomials where $g_1 = 1$ and $\deg(g_i) < m$ for $2 \le i \le s$, such that, for the star discrepancy of the polynomial lattice point set $\mathcal{P}(\boldsymbol{g}, f)$, we have*

$$D_N^*(\mathcal{P}(\boldsymbol{g}, f)) \le c(s,q) \frac{(\log N)^{s-1} \log\log N}{N},$$

where $N = q^m$.

2 The Proof of Theorem 1

The proof of Theorem 1 is inspired by the proof of the corresponding result in [9]. Since many technical difficulties have to be overcome in the extension of Larcher's result to the one presented here, and in order to keep the paper self-contained, we provide a detailed outline of the proof.

Proof. Let $f(x) = x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_{m-1}x + a_m$. Furthermore, let $g_1 = 1$ and, for $2 \le i \le s$, let $g_i(x) = g_1^{(i)} x^{m-1} + g_2^{(i)} x^{m-2} + \cdots + g_{m-1}^{(i)} x + g_m^{(i)}$.

We interpret $\mathcal{P}(\boldsymbol{g}, f) = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{q^m-1}\}$ as a digital net over $\mathbb{F}_q$ with generating matrices $C^{(1)}, \ldots, C^{(s)}$. I.e., for $0 \le k < q^m$ with q-adic expansion $k = k_0 + k_1 q + \cdots + k_{m-1} q^{m-1}$ with digits $k_i \in \mathbb{Z}_q \cong \mathbb{F}_q$, set $\vec{k} := (k_0, \ldots, k_{m-1})^\top$. Then for $1 \le i \le s$ the i-th component $x_k^{(i)}$ of $\boldsymbol{x}_k$ is given by $x_k^{(i)} = x_{k,i,1} q^{-1} + \cdots + x_{k,i,m} q^{-m}$, where $(x_{k,i,1}, \ldots, x_{k,i,m})^\top = C^{(i)} \vec{k}$; see [3, Chapter 10]. Motivated by this construction, we will often write $x_k^{(i)} \cong C^{(i)} \vec{k}$.

According to what is outlined in [3, Section 10.1], the first generating matrix $C^{(1)}$ of the point set $\mathcal{P}(\boldsymbol{g}, f)$ is of the form (since $g_1 = 1$)

$$C^{(1)} = \begin{pmatrix} 0 & \ldots & 0 & 0 & 1 \\ 0 & \ldots & 0 & 1 & u_{m+1}^{(1)} \\ 0 & \ldots & 1 & u_{m+1}^{(1)} & u_{m+2}^{(1)} \\ \vdots & \iddots & \iddots & \vdots & \vdots \\ 1 & u_{m+1}^{(1)} & u_{m+2}^{(1)} & \ldots & u_{2m-1}^{(1)} \end{pmatrix},$$

where the $u_i^{(1)}$ are elements in $\mathbb{F}_q$, depending on f. Furthermore, the matrices $C^{(2)}, \ldots, C^{(s)}$ are Hankel matrices over $\mathbb{F}_q$, i.e., they are of the form

$$C^{(i)} = \begin{pmatrix} u_1^{(i)} & \ldots & \ldots & u_{m-1}^{(i)} & u_m^{(i)} \\ u_2^{(i)} & \ldots & \ldots & u_m^{(i)} & u_{m+1}^{(i)} \\ u_3^{(i)} & \ldots & \ldots & u_{m+1}^{(i)} & u_{m+2}^{(i)} \\ \vdots & \iddots & \iddots & \vdots & \vdots \\ u_m^{(i)} & u_{m+1}^{(i)} & u_{m+2}^{(i)} & \ldots & u_{2m-1}^{(i)} \end{pmatrix}, \quad i = 2, \ldots, s, \tag{2}$$

where the $u_j^{(i)}$ are again elements of $\mathbb{F}_q$, depending on g_i and f. (In fact, $u_l^{(i)}$ is the coefficient of x^{-l} in the Laurent series expansion of g_i/f; see [3, Section 10.1].)

Since $C^{(1)}$ is non-singular, we can find a non-singular matrix $\widetilde{C} = \widetilde{C}(C_1)$ such that

$$C^{(1)} \widetilde{C} = E_m := \begin{pmatrix} 0 & \ldots & 0 & 0 & 1 \\ 0 & \ldots & 0 & 1 & 0 \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ 0 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Note that, due to the special form of $C^{(1)}$, $\widetilde{C}$ is a non-singular right upper triangular matrix. We now write $D^{(i)} := C^{(i)}\widetilde{C}$ for $1 \le i \le s$. It is well known (see, e.g., [3, Lemma 4.61]) that if we multiply the generating matrices of a digital net by a non-singular matrix from the right, the net does not change except for the order of points. Hence we can say that $\mathcal{P}(\boldsymbol{g}, f)$, up to the order of points, is also generated by $D^{(1)}, D^{(2)}, \ldots, D^{(s)}$, where $D^{(1)} = E_m$. In order to keep an overview, we denote this re-ordered version of $\mathcal{P}(\boldsymbol{g}, f)$ by $\mathcal{R}(\boldsymbol{g}, f) = \{\boldsymbol{r}_0, \ldots, \boldsymbol{r}_{q^m-1}\}$ where $\boldsymbol{r}_k = (r_k^{(1)}, \ldots, r_k^{(s)})$ and $\boldsymbol{r}_k^{(i)} \cong D^{(i)}\vec{k}$. In particular, the points of $\mathcal{R}(\boldsymbol{g}, f)$ are of the form $\boldsymbol{r}_k = (\frac{k}{q^m}, r_k^{(2)}, \ldots, r_k^{(s)})$, for all $0 \le k < q^m$.

Now we use a result from [5] (see also [3, Lemma 3.45]) to obtain

$$ND_N^*(\mathcal{P}(\boldsymbol{g}, f)) = ND_N^*(\mathcal{R}(\boldsymbol{g}, f)) \le \max_{1 \le N_0 \le N} N_0 D_{N_0}^*((\widetilde{\boldsymbol{r}}_k)_{k=0}^{N-1}) + 1,$$

where $\widetilde{\boldsymbol{r}}_k$ is the projection of $\boldsymbol{r}_k$ onto its last $s-1$ components, i.e., $\widetilde{\boldsymbol{r}}_k = (r_k^{(2)}, \ldots, r_k^{(s)})$.

Theorem 1 now follows by applying Proposition 1 below to the sequence $(\widetilde{\boldsymbol{r}}_k)_{k=0}^{N-1}$. □

Proposition 1 *Let a polynomial $f \in \mathbb{F}_q[x]$ of degree m with $\gcd(f, x) = 1$ and a non-singular right upper triangular matrix $\widetilde{C}$ over $\mathbb{F}_q$ be given. Then there exists a polynomial lattice $\mathcal{P}(\boldsymbol{g}, f)$ with generating matrices $C^{(1)}, \ldots, C^{(s)}$ (which are obtained from $\boldsymbol{g}$ and f as usual by the algorithm outlined, e.g., in [3, Chapter 10]), such that the re-ordered point set $\mathcal{Q}(\boldsymbol{g}, f)$, generated by $D^{(1)}, \ldots, D^{(s)}$, where $D^{(i)} = C^{(i)}\widetilde{C}$, satisfies*

$$N_0 D_{N_0}^*(\mathcal{Q}(\boldsymbol{g}, f)) \le c(s, q)(\log N)^s \log\log N$$

for all $N_0 \in \{1, \ldots, N\}$, where $c(s, q) > 0$ is a constant depending only on s and q.

The proof of Proposition 1 requires several lemmas, which we shall formulate and discuss within the proof of the proposition.

Proof. Let $N_0 \in \{1, \ldots, N\}$. We are interested in studying the point set $\{\boldsymbol{y}_0, \ldots, \boldsymbol{y}_{N_0-1}\}$, where

$$\boldsymbol{y}_k = (y_k^{(1)}, \ldots, y_k^{(s)}) \ \text{ and } \ y_k^{(i)} \cong D^{(i)}\vec{k},$$

where $\vec{k}$ denotes the m-dimensional base q digit vector of k, $0 \le k \le N_0 - 1$. Let now $T : \{0, \ldots, q^m - 1\} \to \{0, \ldots, q^m - 1\}$ be the map that is defined by the matrix $\widetilde{C}$ via $\vec{T}(k) = \widetilde{C}\vec{k}$ where $\vec{T}(k)$ is the m-dimensional q-adic digit vector of $T(k)$. Then we can, equivalently, study the point set $\{\boldsymbol{x}_{T(0)}, \boldsymbol{x}_{T(1)}, \ldots, \boldsymbol{x}_{T(N_0-1)}\}$, where

$$\boldsymbol{x}_{T(k)} = (x_{T(k)}^{(1)}, \ldots, x_{T(k)}^{(s)}) \ \text{ and } \ x_{T(k)}^{(i)} \cong C^{(i)}\vec{T}(k).$$

Let

$$C^{(i)} = \begin{pmatrix} u_1^{(i)} & \cdots & \cdots & u_{m-1}^{(i)} & u_m^{(i)} \\ u_2^{(i)} & \cdots & \cdots & u_m^{(i)} & u_{m+1}^{(i)} \\ u_3^{(i)} & \cdots & \cdots & u_{m+1}^{(1)} & u_{m+2}^{(i)} \\ \vdots & \iddots & \iddots & \vdots & \vdots \\ u_m^{(i)} & u_{m+1}^{(i)} & u_{m+2}^{(i)} & \cdots & u_{2m-1}^{(i)} \end{pmatrix} = (c_{j,l}^{(i)})_{j,l=1}^{m},$$

where $c_{j,l}^{(i)} = u_{l+j-1}^{(i)}$.

For a given $r \in \{T(0), T(1), \ldots, T(N_0 - 1)\}$ with base q representation $r = \sum_{k=0}^{m-1} r_k q^k$ we have

$$x_r^{(i)} = \sum_{l=1}^{m} q^{-l} \bigoplus_{k=0}^{m-1} r_k u_{l+k}^{(i)},$$

where $\bigoplus$ denotes a sum modulo q.

We write

$$N_0 = \sum_{j=0}^{m_0-1} b_j q^j, \quad b_j \in \mathbb{Z}_q, \quad b_{m_0-1} \neq 0.$$

For fixed integers $0 \leq n < m_0$, and $0 \leq b < b_n$, we consider integers k belonging to the set

$$\mathcal{I}(n,b) := \left\{ k \in \mathbb{Z} : \sum_{j=n+1}^{m_0-1} b_j q^j + b q^n \leq k < \sum_{j=n+1}^{m_0-1} b_j q^j + (b+1) q^n \right\}. \tag{3}$$

For such k we have the q-adic expansion

$$k = \sum_{j=0}^{n-1} \alpha_j q^j + b q^n + \sum_{j=n+1}^{m_0-1} b_j q^j \tag{4}$$

with $\alpha_j \in \mathbb{Z}_q$, i.e., the m-dimensional base q digit vector is of the form

$$\vec{k} = (\alpha_0, \ldots, \alpha_{n-1}, b, b_{n+1}, \ldots, b_{m_0-1}, 0, 0, \ldots 0)^\top.$$

Since $\widetilde{C}$ is right upper triangular,

$$\widetilde{C}\vec{k} = \left(a_0, \ldots, a_{n-1}, b', b'_{n+1}, \ldots, b'_{m_0-1}, 0, 0, \ldots, 0\right)^\top \tag{5}$$

with $a_0, \ldots, a_{n-1} \in \mathbb{Z}_q$, and with certain fixed $b', b'_{n+1}, \ldots, b'_{m_0-1}$. (Note that, if $\alpha_0, \ldots, \alpha_{n-1}$ run through all possible values, then so do $a_0, \ldots, a_{n-1}$.) Hence we have

$$T(k) = \sum_{j=0}^{n-1} a_j q^j + b' q^n + \sum_{j=n+1}^{m_0-1} b'_j q^j, \tag{6}$$

and therefore

$$x^{(i)}_{T(k)} = \sum_{l=1}^{m} q^{-l} \left(\bigoplus_{j=0}^{n-1} a_j u^{(i)}_{l+j} \oplus A^{(i)}_l \right),$$

where

$$A^{(i)}_l = b' u^{(i)}_{l+n} \oplus \left(\bigoplus_{j=1}^{m_0-n-1} b'_{n+j} u^{(i)}_{l+n+j} \right).$$

For given, fixed $A^{(i)}_l$, we now consider the sequence $\widetilde{\boldsymbol{x}}_{T(k)} = (\widetilde{x}^{(1)}_{T(k)}, \ldots, \widetilde{x}^{(s)}_{T(k)})$ with

$$\widetilde{x}^{(i)}_{T(k)} = \sum_{l=1}^{n} q^{-l} \left(\bigoplus_{j=0}^{n-1} a_j u^{(i)}_{l+j} \oplus A^{(i)}_l \right), \tag{7}$$

where k is as in (4) with $\alpha_j \in \mathbb{Z}_q$ arbitrary, and where $a_0, \ldots, a_{n-1}$ are the first n components of $\widetilde{C}\vec{k}$ as given by (5) (i.e., each of the a_j runs through all elements of $\mathbb{Z}_q$ if we vary $\alpha_0, \ldots, \alpha_{m-1}$).

Let, for $1 \leq i \leq s$,

$$\widetilde{C}^{(i)}_1 := (c^{(i)}_{j,l})^n_{j,l=1}$$

be the left upper $n \times n$ submatrix of $C^{(i)}$, and let $\boldsymbol{c}^{(i)}_j$ be the j-th row of $\widetilde{C}^{(i)}_1$. Hence we can write (7) in the form

$$\widetilde{x}^{(i)}_{T(k)} \cong \widetilde{C}^{(i)}_1 (a_0, \ldots, a_{n-1})^\top \oplus (A^{(i)}_1, \ldots, A^{(i)}_n)^\top.$$

Let $h(1) \in \mathbb{N}_0$ be maximal such that $\boldsymbol{c}_1^{(1)}, \ldots, \boldsymbol{c}_{h(1)}^{(1)}$ are linearly independent over $\mathbb{F}_q$. If $p(1) \le h(1)$, then for all $d \in \mathbb{N}_0$, $0 \le d < q^{p(1)}$, there are exactly $q^{m-p(1)}$ integers k of the form (4) such that

$$\widetilde{x}_{T(k)}^{(1)} \in \left[\frac{d}{q^{p(1)}}, \frac{d+1}{q^{p(1)}}\right). \tag{8}$$

In the following lemma we characterize those $\widetilde{\boldsymbol{x}}_{T(k)}$ for which $\widetilde{x}_{T(k)}^{(1)}$ lies in an interval of the type displayed in (8). This characterization, though rather technical, will enable us to efficiently count points in certain intervals in order to derive discrepancy bounds.

Lemma 1 *For every $p(1) \le h(1)$ there exist*

(a) a column vector $\boldsymbol{\gamma}^{(1)} = (\underbrace{0, 0, \ldots\ldots\ldots, 0}_{p(1) \text{ components}}, \gamma_{p(1)+1}^{(1)}, \ldots, \gamma_n^{(1)})^\top$, with some $\gamma_i^{(1)} \in \mathbb{F}_q$,

(b) a non-singular matrix $V^{(1)} \in \mathbb{F}_q^{n \times n}$ (depending on $p(1)$ and on $\widetilde{C}_1^{(1)}$),

(c) and n-dimensional column vectors $\boldsymbol{v}_i^{(1)}$ over $\mathbb{F}_q$ (depending on $p(1)$, $\widetilde{C}_1^{(1)}$, and the $\widetilde{C}_1^{(i)}, A_l^{(i)}$), for $2 \le i \le s$,

such that for $d = \sum_{j=0}^{p(1)-1} d_j q^j$, $d_j \in \mathbb{Z}_q$, and for k with $\widetilde{x}_{T(k)}^{(1)} \in \left[\frac{d}{q^{p(1)}}, \frac{d+1}{q^{p(1)}}\right)$, we have

(1)

$$\widetilde{x}_{T(k)}^{(1)} \cong \widetilde{C}_1^{(1)} V^{(1)} (\boldsymbol{d}_1, \boldsymbol{\eta})^\top \oplus \boldsymbol{\gamma}^{(1)}$$

for some $\boldsymbol{\eta} \in \mathbb{F}_q^{n-p(1)}$,

(2) and

$$\widetilde{x}_{T(k)}^{(i)} \cong \widetilde{C}_1^{(i)} V^{(1)} (\boldsymbol{d}_1, \boldsymbol{\eta})^\top \oplus \boldsymbol{v}_i^{(1)} \quad \text{for } 2 \le i \le s,$$

where $\boldsymbol{\eta}$ is as in (1),

and where we write for short $\boldsymbol{d}_1 = (d_{p(1)-1}, \ldots, d_0)$.

Proof. Let $\boldsymbol{a} = (a_0, \ldots, a_{n-1})^\top$ be such that

$$\widetilde{C}_1^{(1)} \boldsymbol{a} = (\boldsymbol{d}_1, \boldsymbol{\xi})^\top \ominus \boldsymbol{A} \tag{9}$$

for some $\boldsymbol{\xi} \in \mathbb{F}_q^{n-p(1)}$, where $\boldsymbol{A} := (A_1^{(1)}, \ldots, A_{p(1)}^{(1)}, 0, \ldots, 0)^\top$. This is equivalent to the condition

$$\widetilde{x}_{T(k)}^{(1)} \in \left[\frac{d}{q^{p(1)}}, \frac{d+1}{q^{p(1)}}\right) \quad \text{when } T(k) \text{ is of the form (6).}$$

Note that we can restrict ourselves to considering only $(A_1^{(1)}, \ldots, A_{p(1)}^{(1)}, 0, \ldots, 0)^\top$ in (9), since $A_{p(1)+1}^{(1)}, \ldots, A_n^{(1)}$ can be absorbed by an appropriate choice of $\boldsymbol{\xi}$.

We arrange the columns of $\widetilde{C}_1^{(1)}$ and the vector $\boldsymbol{a}$ simultaneously into $U := (u_{j,l})_{j,l=1}^n$ and $\boldsymbol{a}' = (a'_0, \ldots, a'_{n-1})^\top$ in such a way that the system (9) does not change and that the left upper $p(1) \times p(1)$ sub-matrix $U_0 = (u_{j,l})_{j,l=1}^{p(1)}$ of U is non-singular. Then we can rewrite (9) as

$$U \boldsymbol{a}' = (\boldsymbol{d}_1, \boldsymbol{\xi})^\top \ominus \boldsymbol{A}. \tag{10}$$

Furthermore, we put $U_1 := (\ominus u_{j,l})_{j=1,l=p(1)+1}^{p(1),n}$. Then the vectors $\boldsymbol{a}'$ which satisfy (10) for some $\boldsymbol{\xi}$ are given by $\boldsymbol{a}' = (a'_0, \ldots, a'_{n-1})^\top$ with arbitrary $a'_{p(1)}, \ldots, a'_{n-1}$ and with

$$(U_0| \ominus U_1)\, \boldsymbol{a}' = \boldsymbol{d}_1^\top \ominus (A_1^{(1)}, \ldots, A_{p(1)}^{(1)})^\top,$$

which is equivalent to

$$U_0 \begin{pmatrix} a'_0 \\ \vdots \\ a'_{p(1)-1} \end{pmatrix} = \boldsymbol{d}_1^\top \oplus U_1 \begin{pmatrix} a'_{p(1)} \\ \vdots \\ a'_{n-1} \end{pmatrix} \ominus \begin{pmatrix} A_1^{(1)} \\ \vdots \\ A_{p(1)}^{(1)} \end{pmatrix},$$

which is again equivalent to

$$\begin{pmatrix} a'_0 \\ \vdots \\ a'_{p(1)-1} \end{pmatrix} = U_0^{-1} \left(\boldsymbol{d}_1^\top \oplus U_1 \begin{pmatrix} a'_{p(1)} \\ \vdots \\ a'_{n-1} \end{pmatrix} \right) \ominus U_0^{-1} \begin{pmatrix} A_1^{(1)} \\ \vdots \\ A_{p(1)}^{(1)} \end{pmatrix}.$$

We now write

$$G_1 := \left(\begin{array}{c|c} U_0^{-1} & \mathbf{0} \\ \hline \mathbf{0} & I_{n-p(1)} \end{array}\right) \quad \text{and} \quad G_2 := \left(\begin{array}{c|c} I_{p(1)} & U_1 \\ \hline \mathbf{0} & I_{n-p(1)} \end{array}\right),$$

with I_l denoting the $l \times l$ unit matrix and $\mathbf{0}$ a zero-matrix of suitable size. This means that

$$\boldsymbol{a}' = G_1 G_2 (\boldsymbol{d}_1, a'_{p(1)}, \ldots, a'_{n-1})^\top \ominus G_1 \boldsymbol{A}.$$

We now write

$$\widetilde{V} := G_1 G_2 = \left(\begin{array}{c|c} U_0^{-1} & U_0^{-1} U_1 \\ \hline \mathbf{0} & I_{n-p(1)} \end{array}\right) \text{ and } \widetilde{\boldsymbol{v}} := G_1 \boldsymbol{A},$$

which results in

$$\boldsymbol{a}' = \widetilde{V} (\boldsymbol{d}_1, a'_{p(1)}, \ldots, a'_{n-1})^\top \ominus \widetilde{\boldsymbol{v}}.$$

We now rearrange the rows of $\widetilde{V}$ and $\widetilde{\boldsymbol{v}}$ in the inverse way to the initial rearrangement of $\widetilde{C}_1^{(1)}$ and $\boldsymbol{a}$, and thereby obtain a non-singular matrix $V^{(1)}$ and a vector $\boldsymbol{v}$. Then

$$\boldsymbol{a} = V^{(1)} (\boldsymbol{d}_1, a'_{p(1)}, \ldots, a'_{n-1})^\top \ominus \boldsymbol{v}$$

satisfies

$$\widetilde{C}_1^{(1)} \boldsymbol{a} = (\boldsymbol{d}_1, \boldsymbol{\xi})^\top \ominus \boldsymbol{A}.$$

By the construction of $V^{(1)}$ and $\boldsymbol{a}'$ above, we have

$$\begin{aligned} \widetilde{x}_{T(k)}^{(1)} &\cong \widetilde{C}_1^{(1)} \boldsymbol{a} \oplus \boldsymbol{A} = U \boldsymbol{a}' \oplus \boldsymbol{A} \\ &= U \widetilde{V} (\boldsymbol{d}_1, a'_{p(1)}, \ldots, a'_{n-1})^\top \ominus U G_1 \boldsymbol{A} \oplus \boldsymbol{A} \\ &= \widetilde{C}_1^{(1)} V^{(1)} (\boldsymbol{d}_1, a'_{p(1)}, \ldots, a'_{n-1})^\top \oplus \boldsymbol{\gamma}^{(1)}, \end{aligned}$$

where $\boldsymbol{\gamma}^{(1)} = \boldsymbol{A} \ominus U G_1 \boldsymbol{A}$. Taking into account the construction of G_1 establishes the first assertion of the lemma by setting $\boldsymbol{\eta} = (a'_{p(1)}, \ldots, a'_{n-1})$.

Furthermore, for $i \geq 2$, we obtain by inserting

$$\widetilde{C}_1^{(i)} \boldsymbol{a} = \widetilde{C}_1^{(i)} V^{(1)} (\boldsymbol{d}_1, \boldsymbol{\eta})^\top \ominus \widetilde{C}_1^{(i)} \boldsymbol{v},$$

for some $\boldsymbol{\eta} \in \mathbb{Z}_q^{n-p(1)}$, such that

$$\widetilde{x}_{T(k)}^{(i)} \cong \widetilde{C}_1^{(i)} V^{(1)}(\boldsymbol{d}_1, \boldsymbol{\eta})^\top \ominus \widetilde{C}_1^{(i)} \boldsymbol{v} \oplus (A_1^{(i)}, \ldots, A_n^{(i)})^\top.$$

Hence, $V^{(1)}$ and

$$\boldsymbol{v}_i^{(1)} := \ominus \widetilde{C}_1^{(i)} \boldsymbol{v} \oplus (A_1^{(i)}, \ldots, A_n^{(i)})^\top$$

satisfy the second assertion of the lemma. □

Let now $\widetilde{C}_2^{(i)} := \widetilde{C}_1^{(i)} V^{(1)}$ for $i \geq 2$. Let

$$\widetilde{C}_2^{(i)} = (\overline{c}_{j,l}^{(i)})_{j,l=1}^{n},$$

let $\overline{\boldsymbol{c}}_j^{(i)}$ be the j-th row of $\widetilde{C}_2^{(i)}$ and let ${}^*\boldsymbol{c}_j^{(i)} := (\overline{c}_{j,p(1)+1}^{(i)}, \ldots, \overline{c}_{j,n}^{(i)})$ be the vector consisting of the last $n - p(1)$ components of the j-th row-vector of $\widetilde{C}_2^{(i)}$.

Choose $h(2) \in \mathbb{N}_0$ maximal such that ${}^*\boldsymbol{c}_1^{(2)}, \ldots, {}^*\boldsymbol{c}_{h(2)}^{(2)}$ are linearly independent over $\mathbb{F}_q$. Let $p(1) \leq h(1)$ and $p(2) \leq h(2)$. Then, for all $d(i) \in \mathbb{N}_0$, $0 \leq d(i) < q^{p(i)}$, $i = 1, 2$, there are exactly $q^{n-p(1)-p(2)}$ integers k of the form (4) such that

$$(\widetilde{x}_{T(k)}^{(1)}, \widetilde{x}_{T(k)}^{(2)}) \in \left[\frac{d^{(1)}}{q^{p(1)}}, \frac{d^{(1)}+1}{q^{p(1)}}\right) \times \left[\frac{d^{(2)}}{q^{p(2)}}, \frac{d^{(2)}+1}{q^{p(2)}}\right). \tag{11}$$

We now show the following lemma, which is the "extension" of Lemma 1 to dimension 2. I.e., we characterize those $\widetilde{\boldsymbol{x}}_{T(k)}$ for which $(\widetilde{x}_{T(k)}^{(1)}, \widetilde{x}_{T(k)}^{(2)})$ lies in an interval of the form displayed in (11).

Lemma 2 *For every $p(1) \leq h(1)$ and $p(2) \leq h(2)$ there exist*

(a) a column vector $\boldsymbol{\gamma}^{(2)} = (\underbrace{0, 0, \ldots\ldots\ldots, 0}_{p(2) \text{ components}}, \gamma_{p(2)+1}^{(2)}, \ldots, \gamma_n^{(2)})^\top$, with some $\gamma_i^{(2)} \in \mathbb{F}_q$,

(b) a non-singular matrix $V^{(2)} \in \mathbb{F}_q^{n \times n}$, depending on $p(2)$ and $\widetilde{C}_2^{(2)}$,

(c) and n-dimensional column vectors $\boldsymbol{v}_i^{(2)}$ over $\mathbb{F}_q$ (depending on $p(1), p(2)$, $\widetilde{C}_1^{(1)}, \widetilde{C}_2^{(2)}$, $\boldsymbol{v}_2^{(1)}$, and the $\widetilde{C}_2^{(i)}, A_l^{(i)}$), for $3 \leq i \leq s$,

such that for $d^{(i)} = \sum_{l=0}^{p(i)-1} d_l^{(i)} q^l$, $d_l^{(i)} \in \mathbb{Z}_q$ for $i = 1, 2$, and for k with

$$(\widetilde{x}_{T(k)}^{(1)}, \widetilde{x}_{T(k)}^{(2)}) \in \left[\frac{d^{(1)}}{q^{p(1)}}, \frac{d^{(1)}+1}{q^{p(1)}}\right) \times \left[\frac{d^{(2)}}{q^{p(2)}}, \frac{d^{(2)}+1}{q^{p(2)}}\right),$$

we have

(1)

$$\widetilde{x}_{T(k)}^{(1)} \cong \widetilde{C}_1^{(1)} V^{(1)}(\boldsymbol{d}_1, \boldsymbol{\eta})^\top \oplus \boldsymbol{\gamma}^{(1)}$$

for some $\boldsymbol{\eta} \in \mathbb{F}_q^{n-p(1)}$, as in Lemma 1, and where also $\boldsymbol{\gamma}^{(1)}$ is as in Lemma 1.

(2)

$$\widetilde{x}_{T(k)}^{(2)} \cong \widetilde{C}_2^{(2)} V^{(2)}(\boldsymbol{d}_1, \boldsymbol{d}_2, \boldsymbol{\xi})^\top \oplus \boldsymbol{\gamma}^{(2)}$$

for some $\boldsymbol{\xi} \in \mathbb{F}_q^{n-p(1)-p(2)}$,

(3) and

$$\widetilde{x}^{(i)}_{T(k)} \cong \widetilde{C}^{(i)}_2 V^{(2)}(\boldsymbol{d}_1, \boldsymbol{d}_2, \boldsymbol{\xi})^\top \oplus \boldsymbol{v}^{(2)}_i \quad \textit{for } 3 \le i \le s,$$

where $\boldsymbol{\xi}$ is as in (2),

and where we write for short $\boldsymbol{d}_1 = (d^{(1)}_{p(1)-1}, \ldots, d^{(1)}_0)$ and $\boldsymbol{d}_2 = (d^{(2)}_{p(2)-1}, \ldots, d^{(2)}_0)$.

Proof. Let $\widetilde{x}^{(1)}_{T(k)}$ be such that $\widetilde{x}^{(1)}_{T(k)} \in \left[\frac{d^{(1)}}{q^{p(1)}}, \frac{d^{(1)}+1}{q^{p(1)}}\right)$. Using Lemma 1, this means that $\widetilde{x}^{(1)}_{T(k)}$ is of the form as stated in Assertion (1), i.e.,

$$\widetilde{x}^{(1)}_{T(k)} \cong \widetilde{C}^{(1)}_1 V^{(1)}(\boldsymbol{d}_1, \boldsymbol{\eta})^\top \oplus \boldsymbol{\gamma}^{(1)}$$

for some $\boldsymbol{\eta} \in \mathbb{F}_q^{n-p(1)}$, so this assertion is shown. Furthermore, Lemma 1 implies

$$\widetilde{x}^{(2)}_{T(k)} \cong \widetilde{C}^{(2)}_1 V^{(1)}(\boldsymbol{d}_1, \boldsymbol{\eta})^\top \oplus \boldsymbol{v}^{(1)}_2 = \widetilde{C}^{(2)}_2 (\boldsymbol{d}_1, \boldsymbol{\eta})^\top \oplus \boldsymbol{v}^{(1)}_2.$$

We also require $\widetilde{x}^{(2)}_{T(k)} \in \left[\frac{d^{(2)}}{q^{p(2)}}, \frac{d^{(2)}+1}{q^{p(2)}}\right)$, i.e.,

$$\widetilde{C}^{(2)}_2 (\boldsymbol{d}_1, \boldsymbol{\eta})^\top = (\boldsymbol{d}_2, \boldsymbol{\rho})^\top \ominus \boldsymbol{v}^{(1)}_2, \tag{12}$$

for some $\boldsymbol{\rho} \in \mathbb{F}_q^{n-p(2)}$. We write ${}^*\boldsymbol{w}^{(2)}_j := (\overline{c}^{(2)}_{j,1}, \ldots, \overline{c}^{(2)}_{j,p(1)})$, so we can write

$$\widetilde{C}^{(2)}_2 = (W | C^{(*)}),$$

where

$$W = ({}^*\boldsymbol{w}^{(2)}_1, \ldots, {}^*\boldsymbol{w}^{(2)}_n)^\top \in \mathbb{F}_q^{n \times p(1)}, \text{ and } C^{(*)} = ({}^*\boldsymbol{c}^{(2)}_1, \ldots, {}^*\boldsymbol{c}^{(2)}_n)^\top \in \mathbb{F}_q^{n \times (n-p(1))}.$$

Hence we can rewrite (12) as

$$W\boldsymbol{d}_1^\top \oplus C^{(*)}\boldsymbol{\eta}^\top = (\boldsymbol{d}_2, \boldsymbol{\rho})^\top \ominus \boldsymbol{v}^{(1)}_2. \tag{13}$$

Now we rearrange the columns of $C^{(*)}$ and the components of $\boldsymbol{\eta}$ into $\overline{U} = (\overline{u}_{j,p(1)+l})^{n,n-p(1)}_{j=1,l=1}$ and $\overline{\boldsymbol{\xi}} = (\xi_{n-p(1)}, \ldots, \xi_1)$, such that the left-upper $p(2) \times p(2)$ sub-matrix

$$\overline{U}_0 := \begin{pmatrix} \overline{u}_{1,p(1)+1} & \cdots & \overline{u}_{1,p(1)+p(2)} \\ \vdots & & \vdots \\ \overline{u}_{p(2),p(1)+1} & \cdots & \overline{u}_{p(2),p(1)+p(2)} \end{pmatrix} \in \mathbb{F}_q^{p(2) \times p(2)}$$

of $\overline{U}$ is non-singular and the system (13) remains unchanged. So, (13) can be written as

$$W\boldsymbol{d}_1^\top \oplus \overline{U}\overline{\boldsymbol{\xi}}^\top = (\boldsymbol{d}_2, \boldsymbol{\rho})^\top \ominus \boldsymbol{v}^{(1)}_2, \tag{14}$$

where

$$\overline{U} = \left(\begin{array}{c|c} \overline{U}_0 & X \\ \hline Y & Z \end{array}\right),$$

with $X \in \mathbb{F}_q^{p(2) \times (n-p(1)-p(2))}$, $Y \in \mathbb{F}_q^{(n-p(2)) \times p(2)}$, and $Z \in \mathbb{F}_q^{(n-p(2)) \times (n-p(1)-p(2))}$. With this notation, we can rewrite (14) as

$$\begin{pmatrix} \overline{U}_0 \\ Y \end{pmatrix} (\xi_{n-p(1)}, \ldots, \xi_{n-p(1)-p(2)+1})^\top = (\boldsymbol{d}_2, \boldsymbol{\rho})^\top \ominus \boldsymbol{v}^{(1)}_2 \ominus W\boldsymbol{d}_1^\top \ominus \begin{pmatrix} X \\ Z \end{pmatrix} (\xi_{n-p(1)-p(2)}, \ldots, \xi_1)^\top.$$

Note that in the latter system we need not explicitly deal with the "lower" $n-p(2)$ components, since those can be absorbed by an appropriate choice of $\boldsymbol{\rho}$. Hence we consider

$$\overline{U}_0 \begin{pmatrix} \xi_{n-p(1)} \\ \vdots \\ \xi_{n-p(1)-p(2)+1} \end{pmatrix} = \boldsymbol{d}_2^\top \ominus {}^*\boldsymbol{v}_2^{(1)} \ominus \begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)} \end{pmatrix} \boldsymbol{d}_1^\top \ominus X \begin{pmatrix} \xi_{n-p(1)-p(2)} \\ \vdots \\ \xi_1 \end{pmatrix},$$

where ${}^*\boldsymbol{v}_2^{(1)}$ is the vector consisting of the first $p(2)$ components of $\boldsymbol{v}_2^{(1)}$. The latter equation is equivalent to

$$\begin{pmatrix} \xi_{n-p(1)} \\ \vdots \\ \xi_{n-p(1)-p(2)+1} \end{pmatrix} = \overline{U}_0^{-1}\boldsymbol{d}_2^\top \ominus \overline{U}_0^{-1}\,{}^*\boldsymbol{v}_2^{(1)} \ominus \overline{U}_0^{-1} \begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)} \end{pmatrix} \boldsymbol{d}_1^\top \ominus \overline{U}_0^{-1} X \begin{pmatrix} \xi_{n-p(1)-p(2)} \\ \vdots \\ \xi_1 \end{pmatrix}.$$

Let now

$$\overline{G}_1 = \left(\begin{array}{c|c} \overline{U}_0^{-1} & \mathbf{0} \\ \hline \mathbf{0} & I_{n-p(1)-p(2)} \end{array}\right) \in \mathbb{F}_q^{(n-p(1))\times(n-p(1))},$$

and

$$\overline{G}_2 = \left(\begin{array}{c|c} I_{p(2)} & \ominus X \\ \hline \mathbf{0} & I_{n-p(1)-p(2)} \end{array}\right) \in \mathbb{F}_q^{(n-p(1))\times(n-p(1))}.$$

Then we have

$$\overline{G}_1\overline{G}_2 = \left(\begin{array}{c|c} \overline{U}_0^{-1} & \ominus \overline{U}_0^{-1} X \\ \hline \mathbf{0} & I_{n-p(1)-p(2)} \end{array}\right). \tag{15}$$

According to what we outlined above, we can now write

$$\begin{aligned} \overline{\boldsymbol{\xi}}^\top &= \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} \boldsymbol{d}_2^\top \ominus \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} {}^*\boldsymbol{v}_2^{(1)} \ominus \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} \begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)} \end{pmatrix} \boldsymbol{d}_1^\top \oplus \begin{pmatrix} \ominus \overline{U}_0^{-1} X \\ \hline I_{n-p(1)-p(2)} \end{pmatrix} \begin{pmatrix} \xi_{n-p(1)-p(2)} \\ \vdots \\ \xi_1 \end{pmatrix} \\ &= \overline{G}_1\overline{G}_2 \begin{pmatrix} \boldsymbol{d}_2^\top \\ \boldsymbol{\xi}^\top \end{pmatrix} \ominus \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} {}^*\boldsymbol{v}_2^{(1)} \ominus \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} \begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)} \end{pmatrix} \boldsymbol{d}_1^\top, \end{aligned} \tag{16}$$

where $\boldsymbol{\xi} = (\xi_{n-p(1)-p(2)}, \ldots, \xi_1)$. Plugging into (14) yields

$$\begin{pmatrix} \boldsymbol{d}_2^\top \\ \boldsymbol{\rho}^\top \end{pmatrix} \ominus \boldsymbol{v}_2^{(1)} = W\boldsymbol{d}_1^\top \oplus \overline{UG}_1\overline{G}_2 \begin{pmatrix} \boldsymbol{d}_2^\top \\ \boldsymbol{\xi}^\top \end{pmatrix} \ominus \overline{U} \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} \begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)} \end{pmatrix} \boldsymbol{d}_1^\top \ominus \overline{U} \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} {}^*\boldsymbol{v}_2^{(1)}. \tag{17}$$

Set

$$\boldsymbol{\gamma}^{(2)} = \boldsymbol{v}_2^{(1)} \ominus \overline{U} \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} {}^*\boldsymbol{v}_2^{(1)} = \boldsymbol{v}_2^{(1)} \ominus \left(\begin{array}{c|c} \overline{U}_0 & X \\ \hline Y & Z \end{array}\right) \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} {}^*\boldsymbol{v}_2^{(1)} = \boldsymbol{v}_2^{(1)} \ominus \begin{pmatrix} {}^*\boldsymbol{v}_2^{(1)} \\ \hline Y\overline{U}_0^{-1}\,{}^*\boldsymbol{v}_2^{(1)} \end{pmatrix}$$

(hence $\boldsymbol{\gamma}^{(2)}$ is of the required form). So we can write (17) as

$$\begin{pmatrix} \boldsymbol{d}_2^\top \\ \boldsymbol{\rho}^\top \end{pmatrix} \ominus \boldsymbol{\gamma}^{(2)} = W\boldsymbol{d}_1^\top \oplus \overline{UG}_1\overline{G}_2 \begin{pmatrix} \boldsymbol{d}_2^\top \\ \boldsymbol{\xi}^\top \end{pmatrix} \ominus \overline{U} \begin{pmatrix} \overline{U}_0^{-1} \\ \hline \mathbf{0} \end{pmatrix} \begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)} \end{pmatrix} \boldsymbol{d}_1^\top. \tag{18}$$

We now would like to find a matrix $\overline{V} \in \mathbb{F}_q^{n\times n}$ such that the right hand side of (18) can be written as $\left(W|\overline{U}\right)\overline{V}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top$. To this end, let

$$\overline{V} := \left(\begin{array}{c|c} I_{p(1)} & \mathbf{0} \\ \hline A & \overline{G}_1\overline{G}_2 \end{array}\right),$$

with $A \in \mathbb{F}_q^{(n-p(1))\times p(1)}$, the precise form of which will be determined below. We then get

$$(W|\overline{U})\overline{V} = \left(W|\overline{U}\right)\left(\begin{array}{c|c} I_{p(1)} & \mathbf{0} \\ \hline A & \overline{G}_1\overline{G}_2 \end{array}\right) = \left(W \oplus \overline{U}A|\overline{U}\overline{G}_1\overline{G}_2\right).$$

So we obtain

$$(W|\overline{U})\overline{V}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top = W\boldsymbol{d}_1^\top \oplus \overline{U}\overline{G}_1\overline{G}_2\begin{pmatrix}\boldsymbol{d}_2^\top \\ \boldsymbol{\xi}^\top\end{pmatrix} \oplus \overline{U}A\boldsymbol{d}_1^\top.$$

If we now choose

$$A = \ominus\left(\begin{array}{c}\overline{U}_0^{-1} \\ \hline \mathbf{0}\end{array}\right)\begin{pmatrix} {}^*\boldsymbol{w}_1^{(2)} \\ \vdots \\ {}^*\boldsymbol{w}_{p(2)}^{(2)}\end{pmatrix},$$

then we see that we can indeed write (18) in the form

$$(\boldsymbol{d}_2,\boldsymbol{\rho})^\top \ominus \boldsymbol{\gamma}^{(2)} = \left(W|\overline{U}\right)\overline{V}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top.$$

Now we can arrange the columns of $\overline{U}$ and the rows of $\overline{V}$ in the inverse way to the initial rearrangement of $C^{(*)}$ and $\boldsymbol{\eta}$ such that

$$(\boldsymbol{d}_2,\boldsymbol{\rho})^\top = \widetilde{C}_2^{(2)}V^{(2)}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top \oplus \boldsymbol{\gamma}^{(2)}$$

for a certain matrix $V^{(2)}$. Consequently, for $i = 2$, we obtain

$$\widetilde{x}_{T(k)}^{(2)} \cong (\boldsymbol{d}_2,\boldsymbol{\rho})^\top = \widetilde{C}_2^{(2)}V^{(2)}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top \oplus \boldsymbol{\gamma}^{(2)}.$$

This proves Assertion (2).

Finally, let us prove Assertion (3). We know from Lemma 1 that we must have, due to the condition on $\widetilde{x}_{T(k)}^{(1)}$,

$$\widetilde{x}_{T(k)}^{(i)} \cong \widetilde{C}_2^{(i)}(\boldsymbol{d}_1,\boldsymbol{\eta})^\top \oplus \boldsymbol{v}_i^{(1)}$$

for $i \geq 3$. Furthermore, due to the condition on $\widetilde{x}_{T(k)}^{(2)}$, we know that $(\boldsymbol{d}_1,\boldsymbol{\eta})^\top$ must satisfy (13). Equivalently, the reordered version $\overline{\boldsymbol{\xi}}$ of $\boldsymbol{\eta}$ needs to satisfy (14). However, from our observations leading to Assertion (2), we know that $\overline{\boldsymbol{\xi}}$ needs to satisfy (16). From this, it is easy to see that

$$\begin{pmatrix}\boldsymbol{d}_1^\top \\ \overline{\boldsymbol{\xi}}^\top\end{pmatrix} = \overline{V}\begin{pmatrix}\boldsymbol{d}_1^\top \\ \boldsymbol{d}_2^\top \\ \boldsymbol{\xi}^\top\end{pmatrix} \ominus \left(\begin{array}{c}\mathbf{0} \\ \hline \left(\begin{array}{c}\overline{U}_0^{-1} \\ \hline \mathbf{0}\end{array}\right) {}^*\boldsymbol{v}_2^{(1)}\end{array}\right).$$

After performing the re-arrangement of the rows of this equation in the inverse way to the initial rearrangement of $\boldsymbol{\eta}$ we obtain

$$(\boldsymbol{d}_1,\boldsymbol{\eta})^\top = V^{(2)}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top \oplus \overline{\boldsymbol{v}}_i^{(2)},$$

where $\overline{\boldsymbol{v}}_i^{(2)}$ is some n-dimensional column vector. This finally yields

$$\begin{aligned}\widetilde{x}_{T(k)}^{(i)} &\cong \widetilde{C}_2^{(i)}(\boldsymbol{d}_1,\boldsymbol{\eta})^\top \oplus \boldsymbol{v}_i^{(1)} \\ &= \widetilde{C}_2^{(i)}V^{(2)}(\boldsymbol{d}_1,\boldsymbol{d}_2,\boldsymbol{\xi})^\top \oplus \widetilde{C}_2^{(i)}\overline{\boldsymbol{v}}_i^{(2)} \oplus \boldsymbol{v}_i^{(1)}.\end{aligned}$$

Setting $\boldsymbol{v}_i^{(2)} = \widetilde{C}_2^{(i)}\overline{\boldsymbol{v}}_i^{(2)} \oplus \boldsymbol{v}_i^{(1)}$ shows Assertion (3). □

Having shown Lemma 2, we now set $\widetilde{C}_3^{(i)} = \widetilde{C}_2^{(i)} V^{(2)}$ for $i \geq 3$. In particular, let

$$\widetilde{C}_3^{(3)} = (\overline{\overline{c}}_{j,l}^{(3)})_{j,l=1}^{n},$$

and ${}^*\overline{\overline{\boldsymbol{c}}}_j^{(3)} = (\overline{\overline{c}}_{j,p(1)+p(2)+1}^{(3)}, \ldots, \overline{\overline{c}}_{j,n}^{(3)})$.

Choose $h(3) \in \mathbb{N}_0$ maximal such that ${}^*\overline{\overline{\boldsymbol{c}}}_1^{(3)}, \ldots, {}^*\overline{\overline{\boldsymbol{c}}}_{h(3)}^{(3)}$ are linearly independent over $\mathbb{F}_q$.

In the same way as in Lemma 2, we construct for $p(3) \leq h(3)$ a non-singular matrix $V^{(3)}$, with analogous properties to $V^{(2)}$, and proceed as before.

In general, for any $w \in \{1, \ldots, s-1\}$, we have matrices $\widetilde{C}_w^{(i)}$ for $w \leq i \leq s$, integers $h(1), \ldots, h(w)$, and integers $p(1) \leq h(1), \ldots, p(w) \leq h(w)$, which are found in the same way as outlined for the special cases $w = 1, 2, 3$.

Furthermore, $\widetilde{C}_w^{(i)} = \widetilde{C}_{w-1}^{(i)} V^{(w-1)}$ for $w \geq 2$ and $i \geq w$, with non-singular matrices $V^{(j)}$ as above. In analogy to Lemmas 1 and 2, we then construct a non-singular $n \times n$-matrix $V^{(w)}$ and get

$$\widetilde{C}_{w+1}^{(i)} = \widetilde{C}_w^{(i)} V^{(w)} \quad \text{for} \quad i \geq w+1.$$

For $w \in \{1, \ldots, s-1\}$, we define $h(w+1) := h(p(1), \ldots, p(w))$, and for $w = 0$ we define $h(1) := h()$, each to be maximal such that with

$$\widetilde{C}_{w+1}^{(w+1)} = (z_{j,l})_{j,l=1}^{n}$$

we have that

$${}^*\boldsymbol{z}_j = (z_{j,p(1)+\cdots+p(w)+1}, \ldots, z_{j,n}) \quad \text{for} \quad 1 \leq j \leq h(w+1),$$

are linearly independent. Then for every $p(w+1) \leq h(w+1)$ and every $d(j)$, $0 \leq d(j) < q^{p(j)}$, $1 \leq j \leq w+1$, there are exactly $q^{n-(p(1)+\cdots+p(w+1))}$ integers k of the form (4) with

$$(\widetilde{x}_{T(k)}^{(1)}, \ldots, \widetilde{x}_{T(k)}^{(w+1)}) \in \prod_{j=1}^{w+1} \left[\frac{d(j)}{q^{p(j)}}, \frac{d(j)+1}{q^{p(j)}} \right). \tag{19}$$

This is no longer true if $p(w+1) > h(w+1)$. Due to (19), we see that this property is a property that is inherent to the sequence of the $\widetilde{\boldsymbol{x}}_{T(k)}$, and does not depend on the concrete form of the matrices $V^{(j)}$. The matrices $V^{(j)}$ are just a way of making this property "visible". Note that not all tuples $(p(1), \ldots, p(w))$ can occur (e.g., we always need $p(1) + \cdots + p(w) \leq m$).

A tuple $\boldsymbol{p} = (p(1), \ldots, p(w)) \in \mathbb{N}^w$ is called *admissible* if $p(i) \leq h(i)$ for all $1 \leq i \leq w$. Note that if a tuple $\boldsymbol{p} = (p(1), \ldots, p(w)) \in \mathbb{N}^w$ is admissible then we have $p(1) + \cdots + p(w) \leq m$. The empty tuple () for $w = 0$ will be called admissible by definition. For short we will in the following write $|\boldsymbol{p}| := p(1) + \cdots + p(w)$.

We now have the following lemma.

Lemma 3 *For the star discrepancy $D_{N_0}^*$ of the point set $(\boldsymbol{x}_{T(k)})_{k=0}^{N_0-1}$ we have*

$$N_0 D_{N_0}^* \leq sqm_0 + q^s \sum_{n=0}^{m_0-1} \sum_{w=0}^{s-1} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ \text{admissible}}} q^{n-(|\boldsymbol{p}|+h(w+1))}.$$

Proof. We show the result in two steps:

Step 1: For $0 \leq n < m_0$ and $0 \leq b < b_n$ we estimate the star discrepancy of the point set

$$\left\{ \widetilde{\boldsymbol{x}}_{T(k)} : \ k \in \mathcal{I}(n,b) \right\},$$

where the index set $\mathcal{I}(n,b)$ is as in (3).

For $i \in \{1,\dots,s\}$, let $\beta^{(i)} := \sum_{l=1}^{\infty} \beta_l^{(i)} q^{-l}$, and $B := \prod_{i=1}^{s} [0, \beta^{(i)})$.

Let now

$$\Theta := \bigcup_{\substack{(p(1),\dots,p(s)) \\ \text{admissible}}} \bigcup_{\substack{b_{p(i)}^{(i)}=0 \\ i=1,\dots,s}}^{\beta_{p(i)}^{(i)}-1} \prod_{i=1}^{s} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j} + \frac{b_{p(i)}^{(i)}}{q^{p(i)}}, \sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j} + \frac{b_{p(i)}^{(i)}+1}{q^{p(i)}} \right).$$

Note that this is a disjoint union, and, furthermore, that $\Theta \subseteq B$.

Moreover, define

$$\begin{aligned} \Lambda \;:=\; & \bigcup_{w=0}^{s-1} \bigcup_{\substack{(p(1),\dots,p(w)) \\ \text{admissible}}} \bigcup_{\substack{b_{p(i)}^{(i)}=0 \\ i=1,\dots,w}}^{\beta_{p(i)}^{(i)}-1} \left(\prod_{i=1}^{w} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j} + \frac{b_{p(i)}^{(i)}}{q^{p(i)}}, \sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j} + \frac{b_{p(i)}^{(i)}+1}{q^{p(i)}} \right) \times \right. \\ & \left. \times \left[\sum_{j=1}^{h(w+1)} \frac{\beta_j^{(w+1)}}{q^j}, \sum_{j=1}^{h(w+1)} \frac{\beta_j^{(w+1)}}{q^j} + \frac{1}{q^{h(w+1)}} \right) \times [0,1)^{s-w-1} \right). \end{aligned}$$

We are now going to show that $B \subseteq \Theta \cup \Lambda$ by induction on s. For $s=1$, we have

$$\begin{aligned} \Theta \cup \Lambda \;=\; & \bigcup_{\substack{p(1) \\ \text{admissible}}} \bigcup_{b_{p(1)}^{(1)}=0}^{\beta_{p(1)}^{(1)}-1} \left[\sum_{j=1}^{p(1)-1} \frac{\beta_j^{(1)}}{q^j} + \frac{b_{p(1)}^{(1)}}{q^{p(1)}}, \sum_{j=1}^{p(1)-1} \frac{\beta_j^{(1)}}{q^j} + \frac{b_{p(1)}^{(1)}+1}{q^{p(1)}} \right) \\ & \cup \left[\sum_{j=1}^{h(1)} \frac{\beta_j^{(1)}}{q^j}, \sum_{j=1}^{h(1)} \frac{\beta_j^{(1)}}{q^j} + \frac{1}{q^{h(1)}} \right) \\ =\; & \bigcup_{\substack{p(1) \\ \text{admissible}}} \left[\sum_{j=1}^{p(1)-1} \frac{\beta_j^{(1)}}{q^j}, \sum_{j=1}^{p(1)} \frac{\beta_j^{(1)}}{q^j} \right) \cup \left[\sum_{j=1}^{h(1)} \frac{\beta_j^{(1)}}{q^j}, \sum_{j=1}^{h(1)} \frac{\beta_j^{(1)}}{q^j} + \frac{1}{q^{h(1)}} \right) \\ =\; & \left[0, \sum_{j=1}^{h(1)} \frac{\beta_j^{(1)}}{q^j} + \frac{1}{q^{h(1)}} \right) \\ \supseteq\; & [0, \beta^{(1)}), \end{aligned}$$

which is the result for $s=1$.

Assume now that we have already shown the result for $s-1$. In the induction step, we would like to show the result for s. Let

$$B := \prod_{i=1}^{s-1} [0, \beta^{(i)}) \times [0, \beta^{(s)}).$$

By the induction assumption,

$$\prod_{i=1}^{s-1} [0, \beta^{(i)}) \subseteq \bigcup_{\substack{(p(1),\dots,p(s-1)) \\ \text{admissible}}} \prod_{i=1}^{s-1} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j}, \sum_{j=1}^{p(i)} \frac{\beta_j^{(i)}}{q^j} \right)$$

$$\cup \bigcup_{w=0}^{s-2} \bigcup_{\substack{(p(1),\ldots,p(w)) \\ \text{admissible}}} \bigcup_{\substack{b_{p(i)}^{(i)}=0 \\ i=1,\ldots,w}}^{\beta_{p(i)}^{(i)}-1} \left(\prod_{i=1}^{w} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j} + \frac{b_{p(i)}^{(i)}}{q^{p(i)}}, \sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j} + \frac{b_{p(i)}^{(i)}+1}{q^{p(i)}} \right) \times \right.$$
$$\left. \times \left[\sum_{j=1}^{h(w+1)} \frac{\beta_j^{(w+1)}}{q^j}, \sum_{j=1}^{h(w+1)} \frac{\beta_j^{(w+1)}}{q^j} + \frac{1}{q^{h(w+1)}} \right) \times [0,1)^{s-w-2} \right).$$

We extend each of the $(s-1)$-dimensional intervals K on the right-hand side above to an s-dimensional interval K' such that B is contained in the union of these extensions.

If K is of the form

$$\prod_{i=1}^{s-1} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j}, \sum_{j=1}^{p(i)} \frac{\beta_j^{(i)}}{q^j} \right)$$

for some admissible $(p(1), \ldots, p(s-1))$, then we take

$$K' = \prod_{i=1}^{s-1} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j}, \sum_{j=1}^{p(i)} \frac{\beta_j^{(i)}}{q^j} \right) \times \left(\bigcup_{l=1}^{h(s)} \left[\sum_{j=1}^{l-1} \frac{\beta_j^{(s)}}{q^j}, \sum_{j=1}^{l} \frac{\beta_j^{(s)}}{q^j} \right) \cup \left[\sum_{j=1}^{h(s)} \frac{\beta_j^{(s)}}{q^j}, \sum_{j=1}^{h(s)} \frac{\beta_j^{(s)}}{q^j} + \frac{1}{b^{h(s)}} \right) \right).$$

The remaining intervals K are just extended by $[0,1)$. So, by inserting, we obtain

$$\begin{aligned} B \;\subseteq\; & \bigcup_{\substack{(p(1),\ldots,p(s-1)) \\ \text{admissible}}} \left(\prod_{i=1}^{s-1} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j}, \sum_{j=1}^{p(i)} \frac{\beta_j^{(i)}}{q^j} \right) \times \bigcup_{l=1}^{h(s)} \left[\sum_{j=1}^{l-1} \frac{\beta_j^{(s)}}{q^j}, \sum_{j=1}^{l} \frac{\beta_j^{(s)}}{q^j} \right) \right) \cup \\ & \cup \bigcup_{\substack{(p(1),\ldots,p(s-1)) \\ \text{admissible}}} \left(\prod_{i=1}^{s-1} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j}, \sum_{j=1}^{p(i)} \frac{\beta_j^{(i)}}{q^j} \right) \times \left[\sum_{j=1}^{h(s)} \frac{\beta_j^{(s)}}{q^j}, \sum_{j=1}^{h(s)} \frac{\beta_j^{(s)}}{q^j} + \frac{1}{b^{h(s)}} \right) \right) \cup \\ & \cup \bigcup_{w=0}^{s-2} \bigcup_{\substack{(p(1),\ldots,p(w)) \\ \text{admissible}}} \left(\prod_{i=1}^{w} \left[\sum_{j=1}^{p(i)-1} \frac{\beta_j^{(i)}}{q^j}, \sum_{j=1}^{p(i)} \frac{\beta_j^{(i)}}{q^j} \right) \times \right. \\ & \left. \times \left[\sum_{j=1}^{h(w+1)} \frac{\beta_j^{(w+1)}}{q^j}, \sum_{j=1}^{h(w+1)} \frac{\beta_j^{(w+1)}}{q^j} + \frac{1}{q^{h(w+1)}} \right) \times [0,1)^{s-w-1} \right) \\ = \;& \Theta \cup \Lambda. \end{aligned}$$

and the induction is finished.

For fixed $0 \le n \le m_0 - 1$ and $0 \le b \le b_n - 1$ and an interval $B \subseteq [0,1)^s$ as above, let $A(B)$ be the number of points $\widetilde{\boldsymbol{x}}_{T(k)}$, with $k \in \mathcal{I}(n,b)$, in B. Since the union in the definition of Θ is extended over all admissible tuples $\boldsymbol{p} = (p(1), \ldots, p(s))$, it follows that each of the s-dimensional intervals contains exactly $q^{n-|\boldsymbol{p}|}$ elements $\widetilde{\boldsymbol{x}}_{T(k)}$. Hence it follows that

$$A(\Theta) - q^n \lambda(\Theta) = 0.$$

Furthermore, by the same argument,

$$q^n \lambda(\Lambda) = A(\Lambda) = \sum_{w=0}^{s-1} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ \text{admissible}}} \sum_{\substack{b_{p(i)}^{(i)}=0 \\ i=1,\ldots,w}}^{\beta_{p(i)}^{(i)}-1} q^{n-(|\boldsymbol{p}|+h(w+1))}.$$

Since $\Theta \subseteq B \subseteq \Theta \cup \Lambda$, it follows easily that

$$|A(B) - q^n\lambda(B)| \le \max\{A(\Lambda), q^n\lambda(\Lambda)\} \le \sum_{w=0}^{s-1} \sum_{\substack{\boldsymbol{p}\in\mathbb{N}^w \\ \text{admissible}}} q^w q^{n-(|\boldsymbol{p}|+h(w+1))}.$$

¿From this it follows that, for $0 \le n < m_0$ and $0 \le b < b_n$,

$$q^n D^*_{q^n}\left(\left\{\widetilde{\boldsymbol{x}}_{T(k)} : \ k \in \mathcal{I}(n,b)\right\}\right) \le \sum_{w=0}^{s-1} \sum_{\substack{\boldsymbol{p}\in\mathbb{N}^w \\ \text{admissible}}} q^w q^{n-(|\boldsymbol{p}|+h(w+1))}.$$

Step 2: Since $N_0 = b_0 + b_1 q + \cdots + b_{m_0-1}q^{m_0-1}$, where $b_j \in \mathbb{Z}_q$ and $b_{m_0-1} \neq 0$, we can write

$$(\boldsymbol{x}_{T(k)})_{k=0}^{N_0-1} = \bigcup_{n=0}^{m_0-1} \bigcup_{b=0}^{b_n-1} \left\{\boldsymbol{x}_{T(k)} : \ k \in \mathcal{I}(n,b)\right\}.$$

Since $|\widetilde{x}^{(i)}_{T(k)} - x^{(i)}_{T(k)}| \le q^{-n}$ for $1 \le i \le s$ and $k \in \mathcal{I}(n,b)$, with $0 \le n < m_0$ and $0 \le b \le b_n - 1$, we can apply [3, Proposition 3.15], and obtain

$$\left|q^n D^*_{q^n}\left(\left\{\widetilde{\boldsymbol{x}}_{T(k)} : \ k \in \mathcal{I}(n,b)\right\}\right) - q^n D^*_{q^n}\left(\left\{\boldsymbol{x}_{T(k)} : \ k \in \mathcal{I}(n,b)\right\}\right)\right| \le s.$$

Therefore, by using the so-called triangle inequality for the discrepancy (see [3, Proposition 3.16] or [5, p. 115, Theorem 2.6]), for the star discrepancy $D^*_{N_0}$ of $(\boldsymbol{x}_{T(k)})_{k=0}^{N_0-1}$ we get

$$\begin{aligned} N_0 D^*_{N_0} &\le \sum_{n=0}^{m_0-1} \sum_{b=0}^{b_n-1} q^n D^*_{q^n}\left(\left\{\boldsymbol{x}_{T(k)} : \ k \in \mathcal{I}(n,b)\right\}\right) \\ &\le \sum_{n=0}^{m_0-1} \sum_{b=0}^{b_n-1} \left(s + q^n D^*_{q^n}\left(\left\{\widetilde{\boldsymbol{x}}_{T(k)} : \ k \in \mathcal{I}(n,b)\right\}\right)\right) \\ &\le sqm_0 + q^s \sum_{n=0}^{m_0-1} \sum_{w=0}^{s-1} \sum_{\substack{\boldsymbol{p}\in\mathbb{N}^w \\ \text{admissible}}} q^{n-(|\boldsymbol{p}|+h(w+1))}. \end{aligned}$$

□

Let now $\epsilon \in \mathbb{N}_0$ and $r \in \mathbb{N}_0$ be fixed. Let $n \le m$ and let $\boldsymbol{p} = (p(1), \ldots, p(r-1)) \in \mathbb{N}^{r-1}$ be admissible with respect to n, which means with respect to the $n \times n$ matrices $\widetilde{C}_i^{(i)}$ for $1 \le i < r$. Let $\widetilde{C}_r^{(r)} := (z_{j,l})_{j,l=1}^m$ be the matrix that is constructed with respect to these parameters according to the algorithm outlined above. Again, let

$${}^*\boldsymbol{z}_j := (z_{j,|\boldsymbol{p}|+1}, \ldots, z_{j,n}).$$

Note that these definitions only depend on the choice of $g_1, \ldots, g_r$ and f, but not on $g_{r+1}, \ldots, g_s$.

We now define $\mathcal{M}_r$, $1 \le r \le s$, as the set of all $(g_1, \ldots, g_r) \in \mathbb{F}_q[x]^r$ such that there exists an $n \le m$, and $\boldsymbol{p} = (p(1), \ldots, p(r-1))$ admissible with respect to n, such that ${}^*\boldsymbol{z}_j$, $1 \le j \le n - |\boldsymbol{p}| - \epsilon$, are linearly dependent over $\mathbb{F}_q$. In this definition, ${}^*\boldsymbol{z}_j$, $j = 1, \ldots, n - |\boldsymbol{p}| - \epsilon$, are viewed to be linearly independent if $n - |\boldsymbol{p}| - \epsilon \le 0$. I.e.,

$$\begin{aligned} \mathcal{M}_r = \{&(g_1, \ldots, g_r) \in \mathbb{F}_q[x]^r : \exists n \le m \text{ and } \boldsymbol{p} \in \mathbb{N}^{r-1} \text{ admissible with respect to } n \\ &\text{such that } {}^*\boldsymbol{z}_1, \ldots, {}^*\boldsymbol{z}_{n-|\boldsymbol{p}|-\epsilon} \text{ are linearly dependent over } \mathbb{F}_q\}. \end{aligned}$$

We now have the following lemma.

Lemma 4 *For $1 \le r \le s$ we have $|\mathcal{M}_r| \le c'_s q^{rm-\epsilon} m^r$, where $c'_s > 0$ depends only on s.*

Proof. We have

$$|\mathcal{M}_r| \le \sum_{n=1}^{m} \sum_{\substack{\boldsymbol{p} \text{ admissible} \\ \text{with respect to } n}} \sum_{\boldsymbol{\lambda} \in \mathbb{F}_q^{n-|\boldsymbol{p}|-\epsilon} \setminus \{\mathbf{0}\}} |\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)|,$$

where $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_{n-|\boldsymbol{p}|-\epsilon})$ and

$$|\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \;:=\; \Big\{ (g_1, \ldots, g_r) \in \mathbb{F}_q[x]^r \,:\, \boldsymbol{p} \in \mathbb{N}^{r-1} \text{ admissible with respect to } n \text{ and } \sum_{j=1}^{n-|\boldsymbol{p}|-\epsilon} \lambda_j \, {}^*\boldsymbol{z}_j = \mathbf{0} \Big\}.$$

We have $\widetilde{C}_r^{(r)} = \widetilde{C}_1^{(r)} M$ with a non-singular $n \times n$ matrix M. Let

$$\widetilde{C}_r^{(r)} = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_n)^\top \text{ and } \widetilde{C}_1^{(r)} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)^\top,$$

with

$$\boldsymbol{u}_j = (u_{j,1}, \ldots, u_{j,n}) = (u_j^{(r)}, u_{j+1}^{(r)}, \ldots, u_{j+n-1}^{(r)}),$$

where the $u_l^{(r)} \in \mathbb{F}_q$ depend on g_r and f according to (2). Furthermore, let

$$M = (\boldsymbol{\sigma}_1 | \ldots | \boldsymbol{\sigma}_n), \text{ with } \boldsymbol{\sigma}_j = (\sigma_{1,j}, \ldots, \sigma_{n,j})^\top \text{ for } 1 \le j \le n.$$

Then the system

$$\sum_{j=1}^{n-|\boldsymbol{p}|-\epsilon} \lambda_j \, {}^*\boldsymbol{z}_j = \mathbf{0} \tag{20}$$

is equivalent to

$$\sum_{j=1}^{n} \xi_j \sigma_{j,|\boldsymbol{p}|+l} = 0 \;\text{ for }\; 1 \le l \le n - |\boldsymbol{p}|, \tag{21}$$

where $\xi_j := \sum_{k=1}^{n-|\boldsymbol{p}|-\epsilon} \lambda_k u_{j+k-1}^{(r)} \in \mathbb{F}_q$ for $1 \le j \le n$.

We consider two cases:

CASE (a): Suppose first that $2n - |\boldsymbol{p}| - \epsilon - 1 \le m$. The linear system (21) in the variables $\xi_1, \ldots, \xi_n$ has rank $n - |\boldsymbol{p}|$ since M is non-singular. For each of the $q^{|\boldsymbol{p}|}$ solutions $(\xi_1, \ldots, \xi_n)$ of (21) we consider the system

$$\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = \underbrace{\begin{pmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} & 0 & 0 & \ldots & 0 \\ 0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} & 0 \\ 0 & 0 & \ldots & 0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} \end{pmatrix}}_{=:L \in \mathbb{F}_q^{n \times (2n-|\boldsymbol{p}|-\epsilon-1)}} \begin{pmatrix} u_1^{(r)} \\ \vdots \\ u_{2n-|\boldsymbol{p}|-\epsilon-1}^{(r)} \end{pmatrix} \tag{22}$$

Since at least one of the λ_j is different from zero, the matrix L has rank n. Therefore, we have $q^{n-|\boldsymbol{p}|-\epsilon-1}$ solutions to (22) for each $(\xi_1, \ldots, \xi_n)$. Hence, the initial system (21) has

$q^{n-|\boldsymbol{p}|-\epsilon-1}q^{|\boldsymbol{p}|} = q^{n-\epsilon-1}$ solutions. Note, furthermore, that we can choose $g_1, \ldots, g_{r-1}$ arbitrarily, for which we have no more than $q^{(r-1)m}$ possibilities. Since not necessarily each solution $(u_1^{(r)}, \ldots, u_{2n-|\boldsymbol{p}|-\epsilon-1}^{(r)})$ of (22) can be represented by an appropriate $g_r \in \mathbb{F}_q[x]$, we obtain

$$|\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \leq q^{(r-1)m} q^{n-\epsilon-1}.$$

Using the assumption $2n - |\boldsymbol{p}| - \epsilon - 1 \leq m$, we obtain

$$|\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \leq q^{rm+|\boldsymbol{p}|-n}.$$

Consequently,

$$\sum_{\boldsymbol{\lambda} \in \mathbb{F}_q^{n-|\boldsymbol{p}|-\epsilon} \setminus \{\mathbf{0}\}} |\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \leq q^{rm-\epsilon}.$$

We now consider the second case.

CASE (b): Assume that $2n - |\boldsymbol{p}| - \epsilon - 1 > m$. Again, we have $q^{|\boldsymbol{p}|}$ solutions $(\xi_1, \ldots, \xi_n)$ to the system (21). Again, we would like to have

$$\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = \underbrace{\begin{pmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} & 0 & 0 & \ldots & 0 \\ 0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} & 0 \\ 0 & 0 & \ldots & 0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-|\boldsymbol{p}|-\epsilon} \end{pmatrix}}_{=:L \in \mathbb{F}_q^{n \times (2n-|\boldsymbol{p}|-\epsilon-1)}} \begin{pmatrix} u_1^{(r)} \\ \vdots \\ u_{2n-|\boldsymbol{p}|-\epsilon-1}^{(r)} \end{pmatrix} \tag{23}$$

Note that, due to the construction of the matrices C_i (cf. [3, Proposition 10.4]), the $u_l^{(r)}$ also need to satisfy the system

$$\begin{pmatrix} g_1^{(r)} \\ \vdots \\ g_m^{(r)} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ a_1 & 1 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ a_2 & a_1 & 1 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ a_m & a_{m-1} & \ldots & a_1 & 1 & 0 & \ldots & \ldots & 0 \\ 0 & a_m & a_{m-1} & \ldots & a_1 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_m & a_{m-1} & \ldots & a_1 & 1 & 0 \\ 0 & \ldots & 0 & 0 & a_m & a_{m-1} & \ldots & a_1 & 1 \end{pmatrix} \begin{pmatrix} u_1^{(r)} \\ \vdots \\ \\ \vdots \\ u_{2m-1}^{(r)} \end{pmatrix}. \tag{24}$$

Combining (23) and the last $m-1$ rows of (24), we obtain, as a necessary condition on $u_1^{(r)}, \ldots, u_{2n-|\boldsymbol{p}|-\epsilon-1}^{(r)}$,

$$\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \left(\frac{L}{A}\right) \begin{pmatrix} u_1^{(r)} \\ \vdots \\ u_{2n-|\boldsymbol{p}|-\epsilon-1}^{(r)} \end{pmatrix}, \tag{25}$$

where $A \in \mathbb{F}_q^{(m-1)\times(2n-|\boldsymbol{p}|-\epsilon-1)}$ is the matrix

$$\begin{pmatrix} a_m & a_{m-1} & \dots & \dots & a_1 & 1 & 0 & 0 & \dots & 0 \\ 0 & a_m & a_{m-1} & \dots & \dots & a_1 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_m & a_{m-1} & \dots & \dots & a_1 & 1 & 0 \\ 0 & \dots & \dots & 0 & a_m & a_{m-1} & \dots & \dots & a_1 & 1 \\ 0 & \dots & \dots & \dots & 0 & a_m & a_{m-1} & \dots & \dots & a_1 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & \dots & 0 & 0 & a_m & \dots & a_{2m-2n+|\boldsymbol{p}|+\epsilon} \end{pmatrix}.$$

Note that $a_m \neq 0$ since $\gcd(f, x) = 1$. For short, we write

$$Z := \begin{pmatrix} L \\ \hline A \end{pmatrix} \in \mathbb{F}_q^{(n+m-1)\times(2n-|\boldsymbol{p}|-\epsilon-1)}.$$

We would now like to estimate the rank of Z. To this end, let

$$i_0 := \max\left\{i \in \{1, \dots, n-|\boldsymbol{p}|-\epsilon\} : \lambda_i \neq 0\right\}.$$

We distinguish two sub-cases.

CASE (b.1): Suppose first that $1 \leq i_0 \leq m-n+1$. Then we have

$$\operatorname{rank}(Z) \geq n + 2n - |\boldsymbol{p}| - \epsilon - m - 1,$$

which implies that the number of solutions of (25) is at most q^{m-n}. The same arguments as in Case (a) yield

$$|\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \leq q^{|\boldsymbol{p}|} q^{(r-1)m} q^{m-n} = q^{rm+|\boldsymbol{p}|-n}.$$

Consequently,

$$\sum_{\substack{\boldsymbol{\lambda} \in \mathbb{F}_q^{n-|\boldsymbol{p}|-\epsilon} \setminus \{\mathbf{0}\} \\ i_0 \leq m-n+1}} |\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \leq q^{rm+|\boldsymbol{p}|-n} q^{n-|\boldsymbol{p}|-\epsilon} = q^{rm-\epsilon}.$$

CASE (b.2): Let us now suppose $i_0 = m-n+\tau+1$, with $1 \leq \tau \leq 2n-m-|\boldsymbol{p}|-\epsilon-1$. It then follows that

$$\rho := \operatorname{rank}(Z) \geq 3n - m - \tau - |\boldsymbol{p}| - \epsilon - 1,$$

because the first n rows together with the rows $n+\tau+1, n+\tau+2, \dots, 3n-m-|\boldsymbol{p}|-\epsilon-1$ of Z are linearly independent over $\mathbb{F}_q$. On the other hand, we also know that

$$\rho \geq m - 1,$$

as the last $m-1$ rows of Z are certainly linearly independent (recall that $a_m \neq 0$). Since $3n-m-\tau-|\boldsymbol{p}|-\epsilon-1 \geq m-1$ if and only if $3n-2m-|\boldsymbol{p}|-\epsilon \geq \tau$ we get

$$\rho \geq \begin{cases} 3n-m-\tau-|\boldsymbol{p}|-\epsilon-1 & \text{if } \tau \leq 3n-2m-|\boldsymbol{p}|-\epsilon, \\ m-1 & \text{otherwise.} \end{cases}$$

The number of solutions of (25) is $q^{2n-|\boldsymbol{p}|-\epsilon-1-\rho}$, so

$$|\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, n)| \leq q^{2n-|\boldsymbol{p}|-\epsilon-1-\rho} q^{|\boldsymbol{p}|+(r-1)m} = q^{2n-\epsilon-1+(r-1)m-\rho}.$$

Hence,

$$\begin{aligned}\sum_{\substack{\boldsymbol{\lambda}\in\mathbb{F}_q^{n-|\boldsymbol{p}|-\epsilon}\setminus\{\mathbf{0}\}\\ i_0>m-n+1}} |\mathcal{M}(\boldsymbol{\lambda},\boldsymbol{p},n)| &\leq \sum_{\tau=1}^{3n-2m-|\boldsymbol{p}|-\epsilon} q^{2n-\epsilon-1+(r-1)m-(3n-m-\tau-|\boldsymbol{p}|-\epsilon-1)} \\ &\quad + \sum_{\tau=3n-2m-|\boldsymbol{p}|-\epsilon+1}^{2n-m-|\boldsymbol{p}|-\epsilon-1} q^{2n-\epsilon-1+(r-1)m-(m-1)} \\ &= q^{rm-n+|\boldsymbol{p}|} \sum_{\tau=1}^{3n-2m-|\boldsymbol{p}|-\epsilon} q^{\tau} + q^{(r-1)m-\epsilon+n}q^{n-m}(m-n-1).\end{aligned}$$

However, note that, due to our assumption for Case (b), we have $m-n-1 < 2n-|\boldsymbol{p}|-\epsilon-1-n-1 \leq n$. Furthermore, $q^{n-m} \leq 1$ and consequently,

$$\begin{aligned}\sum_{\substack{\boldsymbol{\lambda}\in\mathbb{F}_q^{n-|\boldsymbol{p}|-\epsilon}\setminus\{\mathbf{0}\}\\ i_0>m-n+1}} |\mathcal{M}(\boldsymbol{\lambda},\boldsymbol{p},n)| &\leq q^{rm-n+|\boldsymbol{p}|} \sum_{\tau=1}^{3n-2m-|\boldsymbol{p}|-\epsilon} q^{\tau} + nq^{(r-1)m-\epsilon+n} \\ &\leq q^{rm-n+|\boldsymbol{p}|}q^{3n-2m-|\boldsymbol{p}|-\epsilon+1} + nq^{(r-1)m-\epsilon+n} \\ &\leq q^{rm-\epsilon+1} + nq^{(r-1)m-\epsilon+n}.\end{aligned}$$

Putting Case (a) and Case (b) together, we obtain

$$|\mathcal{M}_r| \leq \sum_{n=1}^{m} \sum_{\substack{\boldsymbol{p}\\ |\boldsymbol{p}|\leq n}} (nq^{n+(r-1)m-\epsilon} + 2qq^{rm-\epsilon})$$

which yields, after some algebra, the desired result. □

We now outline the last step in the proof of Proposition 1.

Let again $\epsilon \in \mathbb{N}_0$. We define a sequence of sets of polynomials $H_0, H_1, \ldots, H_{s-1}$ with $H_{r-1} \subseteq \mathbb{F}_q[x]^r$ consisting of $(g_1, \ldots, g_r)$ with the following properties:

- $g_1, \ldots, g_r$ are monic and $\deg(g_i) < m$ for all $1 \leq i \leq r$,
- for all $j < r$ we have $(g_1, \ldots, g_j) \in H_{j-1}$.
- for all $n \leq m$ and all $(p(1), \ldots, p(r-1))$ which are admissible with respect to $(g_1, \ldots, g_r)$ and n, the vectors ${}^*\boldsymbol{z}_1, \ldots, {}^*\boldsymbol{z}_{n-|\boldsymbol{p}|-\epsilon}$, stemming from the matrix $\widetilde{C}_r^{(r)}$ as outlined in the definition of the set $\mathcal{M}_r$, are linearly independent over $\mathbb{F}_q$.

Let now $H := H_{s-1}$ and choose $\epsilon = \epsilon(m,s) = \left\lceil \frac{\log(2sc_s'm^sq^s)}{\log q} \right\rceil$, with c_s' as in Lemma 4 and $\lceil x \rceil$ denoting the smallest integer larger than or equal to a real x. This choice of c_s' yields

$$c_s'm^sq^{-\epsilon} < \frac{1}{2s}q^{-s},$$

and therefore

$$|\mathcal{M}_r| \leq \frac{1}{2s}q^{r(m-1)}$$

for all $1 \leq r \leq s$.

We then have

$$|H_0| \geq q^{m-1} - \frac{1}{2s} q^{m-1} = q^{m-1} \left(1 - \frac{1}{2s}\right),$$

and

$$|H_1| \geq q^{m-1} \left(1 - \frac{1}{2s}\right) q^{m-1} - \frac{1}{2s} q^{2(m-1)} = q^{2(m-1)} \left(1 - \frac{2}{2s}\right).$$

Inductively, we obtain,

$$|H| \geq \frac{q^{s(m-1)}}{2}.$$

We now would like to take the average over all elements in H of a sum that serves as an upper bound on the crucial sum in Lemma 3. To this end, we consider the term

$$\Sigma = \frac{1}{|H|} \sum_{\boldsymbol{g} \in H} \sum_{n=0}^{m-1} \sum_{w=0}^{s-1} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ \text{admissible}}} q^{n-(|\boldsymbol{p}|+h(w+1))},$$

where the innermost sum is over all $\boldsymbol{p} = (p(1), \ldots, p(w))$ admissible with respect to n and $\boldsymbol{g} = (g_1, \ldots, g_s) \in H$. In the following we shall write, for short, h instead of $h(w+1)$.

We now have

$$\begin{aligned}
\Sigma &\leq \frac{1}{|H|} \sum_{n=0}^{m-1} \sum_{w=0}^{s-1} q^{m(s-w-1)} \sum_{(g_1,\ldots,g_{w+1}) \in H_w} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ \text{admissible}}} q^{n-|\boldsymbol{p}|-h} \\
&\leq 2q^s \sum_{n=0}^{m-1} \sum_{w=0}^{s-1} q^{-m(w+1)} \sum_{(g_1,\ldots,g_{w+1}) \in H_w} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ \text{admissible}}} q^{n-|\boldsymbol{p}|-h} \\
&\leq 2q^{s+1} \sum_{n=0}^{m-1} \sum_{w=0}^{s-1} q^{-m(w+1)} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ |\boldsymbol{p}| \leq n}} \sum_{i=n-|\boldsymbol{p}|-\epsilon}^{n-|p|} q^{n-|p|-i} \sum_{\boldsymbol{\lambda} \in \mathbb{F}_q^i \setminus \{\boldsymbol{0}\}} \Gamma(w, \boldsymbol{p}, \boldsymbol{\lambda}), \qquad (26)
\end{aligned}$$

where $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_i)$ and $\Gamma(w, \boldsymbol{p}, \boldsymbol{\lambda})$ denotes the number of $(g_1, \ldots, g_{w+1}) \in H_w$ for which $\boldsymbol{p}$ is admissible and $\lambda_1 \, {}^*\boldsymbol{z}_1 + \cdots + \lambda_i \, {}^*\boldsymbol{z}_i = 0$. For estimating the innermost sum in (26), we can use exactly the same method as we used in the proof of Lemma 4 for estimating the sums of $|\mathcal{M}(\lambda, \boldsymbol{p}, n)|$. We then obtain

$$\Sigma \leq 2q^{s+1} \sum_{n=0}^{m-1} \sum_{w=0}^{s-1} q^{-m(w+1))} \sum_{\substack{\boldsymbol{p} \in \mathbb{N}^w \\ |\boldsymbol{p}| \leq n}} \sum_{i=n-|\boldsymbol{p}|-\epsilon}^{n-|p|} q^{n-|p|-i} (nq^{wm+i+|\boldsymbol{p}|} + 2qq^{(w+1)m+i+|\boldsymbol{p}|-n}).$$

Again, a few basic estimates show that the latter expression is of order ϵm^s with implied constants only depending on q and s. Since $\epsilon = \epsilon(m, s) = O(\log m)$ with implied constant depending only on s and q we obtain

$$\Sigma \leq c(s, q) (\log N)^s \log \log N,$$

where $N = q^m$, which, using Lemma 3, finally yields the result of Proposition 1. □

References

[1] R. Béjian: Minoration de la discrépance d'une suite quelconque sur T. Acta Arith. **41**: 185–202, 1982. (in French)

[2] D. Bilyk, M. T. Lacey and A. Vagharshakyan: On the small ball inequality in all dimensions. J. Funct. Anal. **254**: 2470–2502, 2008.

[3] J. Dick and F. Pillichshammer: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press. Cambridge, 2010.

[4] P. Kritzer and F. Pillichshammer: A lower bound on a quantity related to the quality of polynomial lattices. To appear in Funct. Approx. Comment. Math., 2011.

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

[6] H. Niederreiter: Rational functions with partial quotients of small degree in their continued fraction expansion. Monatsh. Math. **103**: 269–288, 1987.

[7] H. Niederreiter: Low-discrepancy point sets obtained by digital constructions over finite fields. Czechoslovak Math. J. **42**: 143–166, 1992.

[8] H. Niederreiter: *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[9] G. Larcher: Nets obtained from rational functions over finite fields. Acta Arith. **63**: 1–13, 1993.

[10] K. F. Roth: On irregularities of distribution. Mathematika **1**: 73–79, 1954.

[11] W. M. Schmidt: Irregularities of distribution VII. Acta Arith. **21**: 45–50, 1972.

Authors' address:
Institut für Finanzmathematik, Universität Linz, Altenbergerstr. 69, 4040 Linz, Austria
E-mail: {peter.kritzer,friedrich.pillichshammer}@jku.at