ACTA ARITHMETICA
LXIII.1 (1993)

Nets obtained from rational functions over finite fields

by

Gerhard Larcher (Salzburg)

1. Introduction. For N points $x_1, x_2, \ldots, x_N$ in the s-dimensional unit-cube $I^s := [0,1)^s$ and for a subinterval J of I^s we put

$$D_N(J) := A_N(J) - V(J)N$$

where $A_N(J)$ is the number of n, $1 \le n \le N$, with $x_n \in J$, and $V(J)$ is the volume of J.

The *star-discrepancy* D_N^* of $x_1, \ldots, x_N$ is then defined by

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

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

In the theory of uniform distribution as well as in the theory of Monte Carlo methods for numerical integration, point sets with small star-discrepancy play a crucial role. It is known (Roth [10]) that for every s there is a $c_s > 0$ such that for every point set $x_1, \ldots, x_N$ in I^s we have

$$D_N^* > c_s \frac{(\log N)^{(s-1)/2}}{N}\,.$$

It is conjectured that even

$$D_N^* > c_s \frac{(\log N)^{s-1}}{N}$$

is always true. (This is trivial for $s = 1$ and was shown for $s = 2$ in [11].)

In this connection (especially for numerical integration) the notion of good lattice points plays an outstanding role. (See for example [1]–[3], [6].)

An s-tuple $\boldsymbol{g} := (g_1, \ldots, g_s) \in \mathbb{Z}^s$ will be called a *good lattice point modulo* $N \in \mathbb{N}$ if the point set

$$x_n := \left(\left\{ \frac{ng_1}{N} \right\}, \ldots, \left\{ \frac{ng_s}{N} \right\} \right), \qquad n = 1, \ldots, N\,,$$

has small discrepancy $D_N^*(\boldsymbol{g})$. ($\{\cdot\}$ denotes the fractional part.)

It is known that for every s there is a c_s such that for all $N \in \mathbb{N}$ there is a $\boldsymbol{g} \in \mathbb{Z}^s$ with

$$D_N^*(\boldsymbol{g}) < c_s \frac{(\log N)^s}{N} \quad \text{(see [6])}.$$

For dimension $s = 2$ this result was improved in [5] to

$$D_N^*(\boldsymbol{g}) < c_2 \frac{(\log N)(\log\log N)^2}{N}.$$

It is conjectured that for arbitrary dimension the result can be improved at least to the form

$$D_N^*(\boldsymbol{g}) < c_s \frac{(\log N)^{s-1}(\log\log N)^{k(s)}}{N}$$

with some $k(s)$.

In connection with the construction of nets and (t, s)-sequences (these are classes of low-discrepancy point sets and sequences, see [7] and [8]) Niederreiter [9] introduced a class of point sets which in some sense can be viewed as analogous to the point sets generated by good lattice points. In the following we give an inessentially simplified definition for essentially the same point set as in [9]:

Let q be a prime and $F_q \cong \mathbb{Z}_q$ be the field of q elements which we denote by $\{\overline{0}, \overline{1}, \ldots, \overline{q-1}\}$.

Let $F_q((x^{-1}))$ be the field of formal Laurent series L with

$$L = 0 \quad \text{or} \quad L = \sum_{k=w}^{\infty} t_k x^{-k}$$

with $t_k \in F_q$ and w an arbitrary integer with $t_w \neq 0$. We define the *fractional part* $\{L\}$ of L by

$$\{L\} := \sum_{k=\max(1,w)}^{\infty} t_k x^{-k}.$$

$F_q((x^{-1}))$ contains the field of rational functions over F_q as a subfield.

Let

$$\phi : B_q := \{0, 1, \ldots, q-1\} \ \rightarrow \ \{\overline{0}, \overline{1}, \ldots, \overline{q-1}\}$$

be defined by $\phi(i) := \bar{i}$ for all i and let

$$\Phi : B_q((x^{-1})) \ \rightarrow \ F_q((x^{-1}))$$

be the extension of ϕ to $B_q((x^{-1}))$.

Let $t \in \mathbb{N}$. Every integer n with $0 \le n < q^t$ can be uniquely represented in the form

$$n = \sum_{k=0}^{t-1} a_k q^k \quad \text{with } a_k \in B_q\,.$$

Let $n(x) \in F_q[x]$ be defined by $n(x) = \sum_{k=0}^{t-1} \overline{a}_k x^k$. Then it was shown in [9] that for every $f \in F_q[x]$ with $\deg(f) = t \ge 1$, there are $g_1, \dots, g_s \in F_q[x]$, $(g_i, f) = 1,\ i = 1, \dots, s,\ \deg(g_i) < t$, such that for the star-discrepancy D_N^* of the point set

$$x_n := \left(\Phi^{-1}\left\{ \frac{n(x)g_1(x)}{f(x)} \right\}\Big|_{x=q}, \dots, \Phi^{-1}\left\{ \frac{n(x)g_s(x)}{f(x)} \right\}\Big|_{x=q} \right), \qquad n = 0, \dots, q^t - 1 =: N - 1\,,$$

we have

$$D_N^* < c_s \frac{(\log N)^s}{N}\,.$$

(c_s depends only on s.)

It is the aim of this paper to show that this estimate can be improved for the special (and most important for applications) case $f(x) = x^t$ in the following form:

THEOREM. *For every $t \in \mathbb{N}$ there are $g_1, \dots, g_s \in F_q[x]$, $g_1 = 1$, $(g_i, x) = 1$, $i = 1, \dots, s$, such that for the discrepancy D_N^* of the point set*

$$x_n := \left(\Phi^{-1}\left\{ \frac{n(x)g_1(x)}{x^t} \right\}\Big|_{x=q}, \dots, \Phi^{-1}\left\{ \frac{n(x)g_s(x)}{x^t} \right\}\Big|_{x=q} \right), \qquad n = 0, \dots, q^t - 1 =: N - 1\,,$$

we have

$$D_N^* < c \frac{(\log N)^{s-1}(\log\log N)}{N}\,,$$

with a constant c depending only on s and q.

(For the connection of these point sets with the theory of nets see [9].)

So in this "non-archimedean case" the analogue of the conjecture on classical good lattice points is true.

2. Proof of the Theorem. In the following, for simplicity, we always write i instead of $\bar{i}$ for all $\bar{i} \in F_q$. It will always be clear whether i is a digit or an element of F_q.

For the first coordinate of our point set we have

$$\Phi^{-1}\left\{ \frac{n(x)}{x^t} \right\}\Big|_{x=q} = \frac{n}{q^t}\,,$$

so by standard methods (see [4], Chapter 2.2) we have

$$ND_N^* \le \max_{1\le N_0<N} N_0 \overline{D}_{N_0}^*$$

where we denote by $\overline{D}_{N_0}^*$ the star-discrepancy of the $(s-1)$-dimensional point set

$$\left(\Phi^{-1}\left\{\frac{n(x)g_2(x)}{x^t}\right\}\Big|_{x=q}, \dots, \Phi^{-1}\left\{\frac{n(x)g_s(x)}{x^t}\right\}\Big|_{x=q}\right), \quad n=0,\dots,N_0-1\,.$$

For simplicity we now consider the quantity $\overline{D}_{N_0}^*$ for all $1 \le N_0 \le N = q^t$ for the sequence

$$x_n = \left(\Phi^{-1}\left\{\frac{n(x)g_1(x)}{x^t}\right\}\Big|_{x=q}, \dots, \Phi^{-1}\left\{\frac{n(x)g_s(x)}{x^t}\right\}\Big|_{x=q}\right), \quad n=0,\dots,N_0-1\,,$$

and show that there are always $g_1,\dots,g_s$, $(g_i,x)=1$, such that

$$\overline{D}_{N_0}^* < c_s \frac{(\log N)^s \log\log N}{N_0} \quad \text{for all } N_0\,.$$

Then the result follows.

Let

$$g_i(x) := \sum_{k=1}^{t} u_{i,k} x^{k-1}$$

and let $U^{(i)}$ be the $t\times t$ matrix $(u_{k,j}^{(i)})$, $k,j=1,\dots,t$, with $u_{k,j}^{(i)} := u_{i,t-k-j+2}$ (where $u_{k,j}^{(i)} := 0$ if $k+j-1>t$). Then, with $x_n := (x_n^{(1)},\dots,x_n^{(s)})$ and $n=\sum_{k=0}^{t-1} a_k q^k$, we have

$$x_n^{(i)} = \sum_{l=1}^{t} q^{-l}\Big(\sum_{k=0}^{t-1} u_{i,t-l-k+1}\Big) \quad (\text{with } u_{i,j}=0 \text{ for } j\le 0)\,.$$

(Here the inner sum is taken in F_q.) This fact can formally be denoted by

$$x_n^{(i)} \cong U^{(i)} \cdot (a_0,\dots,a_{t-1})^t\,.$$

Let now N_0, $1\le N_0\le N$, $N_0=\sum_{k=0}^{t_0-1} b_k q^k$, $b_i\in B_q$, $b_{t_0-1}\ne 0$ be given. For fixed m, $0\le m\le t_0-1$, and $b\in\{0,\dots,b_m-1\}$ we consider the subsequence (x_n) with

$$\sum_{k=m+1}^{t_0-1} b_k q^k + bq^m \le n < \sum_{k=m+1}^{t_0-1} b_k q^k + (b+1)q^m\,.$$

For such n we have

$$n = \sum_{k=0}^{m-1} a_k q^k + bq^m + \sum_{k=m+1}^{t_0-1} b_k q^k \quad \text{with } a_k \in B_q$$

and therefore

$$x_n^{(i)} = \sum_{l=1}^{t} q^{-l} \Big(\sum_{k=0}^{m-1} u_{i,t-l-k+1} a_k + A_l^{(i)} \Big)$$

with

$$A_l^{(i)} = \begin{cases} u_{i,t-m-l+1} b + \displaystyle\sum_{j=1}^{t_0-m-1} u_{i,t-m-l+1-j} b_{m+j} & \text{for } l = 1, \dots, t-m, \\ 0 & \text{for } l > t-m. \end{cases}$$

For given $A_l^{(i)}$ we now consider the sequence

$$\widetilde{x}_n := (\widetilde{x}_n^{(1)}, \dots, \widetilde{x}_n^{(s)})$$

with

$$\widetilde{x}_n^{(i)} := \sum_{l=1}^{m} q^{-l} \Big(\sum_{k=0}^{m-1} u_{i,t-l-k+1} a_k + A_l^{(i)} \Big), \quad n = 0, \dots, q^m - 1 .$$

Let $\widetilde{U}_1^{(i)}$ be the $m \times m$ matrix

$$\widetilde{U}_1^{(i)} := (u_{k,j}^{(i)}), \quad k, j = 1, \dots, m .$$

By $\mathfrak{v}_l^{(i)}$ we denote the lth row of $\widetilde{U}_1^{(i)}$. Let $h(1) \in \mathbb{N}_0$ be maximal such that $\mathfrak{v}_1^{(1)}, \dots, \mathfrak{v}_{h(1)}^{(1)}$ are linearly independent over F_q. If $p(1) \le h(1)$ then in every interval $[dq^{-p(1)}, (d+1)q^{-p(1)})$, $d \in \mathbb{N}_0$, $0 \le d < q^{p(1)}$, there are exactly $q^{m-p(1)}$ of the $\widetilde{x}_n^{(1)}$.

LEMMA 1. *For every $p := p(1)$ there are a regular $m \times m$ matrix $V := V^{(1)}$ (depending on $p(1)$ and on $\widetilde{U}_1^{(1)}$) and m-dimensional vectors $\mathfrak{c}_i$ (depending on $p(1)$, $\widetilde{U}_1^{(1)}$ and the $A_1^{(i)}$), $i = 2, \dots, s$, such that for all $d = \sum_{k=0}^{p-1} d_k q^k$, $d_k \in B_q$, and for all n with $\widetilde{x}_n^{(1)} \in [dq^{-p}, (d+1)q^{-p})$, we have*

$$\widetilde{x}_n^{(i)} \cong \widetilde{U}_1^{(i)} \cdot V \cdot (d_{p-1}, \dots, d_0, \xi_{m-p}, \dots, \xi_1)^t + \mathfrak{c}_i , \quad i = 2, \dots, s ,$$

with some $\xi_k \in B_q$.

Proof. Let $\mathfrak{a}' = (a'_0, \dots, a'_{m-1})^t$ be such that

$$U_1^{(1)} \mathfrak{a}' = (d_{p-1}, \dots, d_0, \xi_{m-p}, \dots, \xi_1)^t - (A_1^{(1)}, \dots, A_p^{(1)}, 0, \dots, 0)^t$$

for any ξ_i. We arrange the columns of $\widetilde{U}_1^{(1)}$ and the vector $\mathfrak{a}'$ into $U := (u_{j,k})$ and $\mathfrak{a} = (a_0, \dots, a_{m-1})^t$ in such a way that the system does not change and

the submatrix $U^0 := (u_{j,k}),\ j,k = 1,\dots,p$, is regular. Then the vectors $\mathfrak{a}$ which satisfy the above system for any ξ_i are given by $\mathfrak{a} = (a_0,\dots,a_{m-1})^t$ with arbitrary $a_p,\dots,a_{m-1}$ and with

$$(a_0,\dots,a_{p-1})^t = (U^0)^{-1}\cdot(d_{p-1} - A_1^{(1)} - u_{1,p+1}a_p - \dots - u_{1,m}a_{m-1},\dots \\ \dots, d_0 - A_p^{(1)} - u_{p,p+1}a_p - \dots - u_{p,m}a_{m-1})^t\,.$$

Let $U^1 := (-u_{j,k}),\ j = 1,\dots,p,\ k = p+1,\dots,m$ and let $\widetilde{V} := U(1)U(2)$ with

$$U(1) := \begin{pmatrix} (U^0)^{-1} & 0 \\ 0 & E_{m-p} \end{pmatrix} \quad \text{and} \quad U(2) := \begin{pmatrix} E_p & U^1 \\ 0 & E_{m-p} \end{pmatrix}$$

with E_k the $k\times k$ unit matrix. Then

$$\mathfrak{a} = U(1)U(2)(d_{p-1},\dots,d_0,a_p,\dots,a_{m-1}) - \widetilde{\mathfrak{c}}$$

with

$$\widetilde{\mathfrak{c}} = U(1)\cdot(A_1^{(1)},\dots,A_p^{(1)},0,\dots,0)^t\,.$$

We rearrange the rows of $\widetilde{V}$ and $\widetilde{\mathfrak{c}}$ in the inverse way to the initial rearrangement and get thereby a regular matrix V and a vector $\mathfrak{c}$. Then V and $\mathfrak{c}_i := -\widetilde{U}_1^{(i)}\mathfrak{c}$ satisfy the assertion of Lemma 1. ∎

Let now $\widetilde{U}_2^{(i)} := \widetilde{U}_1^{(i)}V$. Let

$$\widetilde{U}_2^{(i)} := (v_{j,k}^{(i)})\,,\qquad j,k = 1,\dots,m\,,$$
$$\mathfrak{v}_j^{(i)} := (v_{j,1}^{(i)},\dots,v_{j,m}^{(i)}) \quad \text{and} \quad \overset{*}{\mathfrak{v}}_j^{(i)} := (v_{j,p(1)+1}^{(i)},\dots,v_{j,m}^{(i)})\,.$$

Let $h(2)\in\mathbb{N}_0$ be maximal such that $\overset{*}{\mathfrak{v}}_1^{(2)},\dots,\overset{*}{\mathfrak{v}}_{h(2)}^{(2)}$ are linearly independent over F_q. Let $p(2)\le h(2)$. Then for all $d(i)\in\mathbb{N}_0$, $0\le d(i) < q^{p(i)}$, $i=1,2$, there are exactly $q^{m-p(1)-p(2)}$ integers n with

$$\widetilde{x}_n^{(1)} \in [d^{(1)}q^{-p(1)}, (d^{(1)}+1)q^{-p(1)})\,,$$
$$\widetilde{x}_n^{(2)} \in [d^{(2)}q^{-p(2)}, (d^{(2)}+1)q^{-p(2)})\,.$$

Lemma 2. *For every $p(2)$ there is a regular $m\times m$ matrix $V^{(2)}$, depending on $p(2)$ and $\widetilde{U}_2^{(2)}$, such that for all*

$$d^{(i)} = \sum_{k=0}^{p(i)-1} d_k^{(i)}q^k\,,\qquad d_k^{(i)}\in B_q\,,\qquad i=1,2\,,$$

and for all n with

$$(\widetilde{x}_n^{(1)},\widetilde{x}_n^{(2)}) \in \prod_{i=1}^{2}[d^{(i)}q^{-p(i)}, (d^{(i)}+1)q^{-p(i)})$$

we have

$$\widetilde{x}_n^{(i)} \cong \widetilde{U}_2^{(i)} V^{(2)}(d_{p(1)-1}^{(1)}, \dots, d_0^{(1)}, d_{p(2)-1}^{(2)}, \dots, d_0^{(2)}, \xi_{m-p(1)-p(2)}, \dots, \xi_1)^t + \mathfrak{c}_i\,,$$

$i = 3, \dots, s$, *with some* $\xi_k \in B_q$.

P r o o f. $V^{(2)}$ must have the following two properties:

Let $\mathfrak{d}^{(i)} := (d_{p(i)-1}^{(i)}, \dots, d_0^{(i)})$. Then

(a) $\widetilde{U}_2^{(2)} V^{(2)}(\mathfrak{d}^{(1)}, \mathfrak{d}^{(2)}, \xi_{m-p(1)-p(2)}, \dots, \xi_1)^t = (\mathfrak{d}^{(2)}, \eta_{m-p(2)}, \dots, \eta_1)^t$ with arbitrary ξ_j, η_j;

(b) $V^{(2)}(\mathfrak{d}^{(1)}, \mathfrak{d}^{(2)}, \xi_{m-p(1)-p(2)}, \dots, \xi_1)^t = (\mathfrak{d}^{(1)}, \mathfrak{d}^{(2)}, \eta_{m-p(1)-p(2)}, \dots$ $\dots, \eta_1)^t$ with arbitrary ξ_j, η_j.

We arrange the columns of $\widetilde{U}_2^{(2)}$ so as to get a matrix $\overline{U} = (\overline{u}_{j,k})$ with $\overset{*}{u}_j := (\overline{u}_{j,p(1)+1}, \dots, \overline{u}_{j,p(1)+p(2)})$, $j = 1, \dots, p(2)$, linearly independent over F_q.

In the same way as in (a) we arrange the rows of $V^{(2)}$ so that the system remains unchanged. (Thereby we get a matrix which we denote by $\overline{V}$.) The first $p(1)$ rows of $V^{(2)}$ remain unchanged. We set

$$\overline{V} := \left(\begin{array}{c|c} E_{p(1)} & 0 \\ \hline A \;\vert\; B & C \end{array}\right)$$

with matrices A, B, C which will be determined later. Then condition (b) is satisfied.

Let

$$\overline{U} := \begin{pmatrix} \overline{\mathfrak{a}}_1 \\ \vdots \\ \overline{\mathfrak{a}}_m \end{pmatrix} \quad \text{and} \quad \overline{V} := (\overline{\mathfrak{v}}_1^t, \dots, \overline{\mathfrak{v}}_m^t)$$

with

$$\overline{\mathfrak{v}}_j := (\overline{v}_{1,j}, \dots, \overline{v}_{m,j})\,.$$

The $\overline{v}_{k,j}$, $k = 1, \dots, p(1)$, $j = 1, \dots, m$, are already fixed.

For $1 \le j \le p(1)$ let $\overline{v}_{k,j}$, $k = p(1)+1, \dots, m$, be arbitrary with $\overline{\mathfrak{u}}_k \overline{\mathfrak{v}}_j^t = 0$ for all $k = 1, \dots, p(2)$. This is possible since the rank of each such system is $p(2) \le m - p(1)$.

For $p(1) + 1 \le j \le p(1) + p(2)$ let $\overline{v}_{p(1)+p(2)+1,j} = \dots = \overline{v}_{m,j} = 0$ and $\overline{v}_{l,j}$, $l = p(1) + 1, \dots, p(1) + p(2)$, be such that

$$\overline{\mathfrak{u}}_k \overline{\mathfrak{v}}_j^t = \begin{cases} 0 & \text{if } j \ne p(1) + k, \\ 1 & \text{if } j = p(1) + k, \end{cases}$$

for $k = 1, \dots, p(2)$. (Each such system has exactly one solution.)

Further, for $p(1)+p(2)+1 \le j \le m$ let $\overline{v}_{j,j} := 1$ and $\overline{v}_{l,j} := 0$ for $l = p(1)+p(2)+1, \dots, m$; $l \ne j$. Finally, $\overline{v}_{l,j}$ for $l = p(1)+1, \dots, p(1)+p(2)$ are determined by

$$\overline{\mathfrak{u}}_k \overline{\mathfrak{v}}_j^t = 0\,, \qquad k = 1, \dots, p(2)\,.$$

So $\overline{V}$ constructed in that way has the form

$$\overline{V} = \left(\begin{array}{c|cc} E_{p(1)} & 0 & \\ \hline & D & F \\ A & & \\ & 0 & E_{m-p(1)-p(2)} \end{array}\right)$$

with a regular $p(2) \times p(2)$ matrix D, so that $\overline{V}$ is regular. By rearranging the rows of $\overline{V}$ we get a regular matrix $V^{(2)}$ which satisfies (a) and (b). ∎

Again we set $\widetilde{U}_3^{(i)} := \widetilde{U}_2^{(i)} V^{(2)}$, $i = 3, \dots, s$, define $h(3)$ analogously to $h(2)$, take any $p(3) \le h(3)$ and construct in exactly the same way a matrix $V^{(3)}$ with the analogous properties to $V^{(2)}$ and proceed with this construction. In general, for any w, $0 \le w \le s-1$, we then have integers $p(1), \dots, p(w)$, matrices $\widetilde{U}_w^{(i)}$, $i = w, \dots, s$, where $\widetilde{U}_w^{(i)} = U_{w-1}^{(i)} M_{i,w}$ with a regular $m \times m$ matrix $M_{i,w}$, and we construct a regular $m \times m$ matrix $V^{(w)}$ and get $\widetilde{U}_{w+1}^{(i)} = \widetilde{U}_w^{(i)} V^{(w)}$, $i = w+1, \dots, s$.

We define $h(w+1) := h(p(1), \dots, p(w))$ to be maximal such that (with $\widetilde{U}_{w+1}^{(w+1)} := (z_{k,j})$)

$$\overset{*}{\mathfrak{z}}_k := (z_{k,p(1)+\dots+p(w)+1}, \dots, z_{k,m})\,, \qquad k = 1, \dots, h(w+1)\,,$$

are linearly independent over F_q. Then for every $p(w+1) \le h(w+1)$ and every $d(j)$, $0 \le d(j) < q^{p(j)}$, $j = 1, \dots, w+1$, there are exactly $q^{m-(p(1)+\dots+p(w+1))}$ integers n with

$$(x_n^{(1)}, \dots, x_n^{(w+1)}) \in \prod_{j=1}^{w+1} [d(j) q^{-p(j)}, (d(j)+1) q^{-p(j)})\,.$$

This is no longer true if $p(w+1) > h(w+1)$. So $h(w+1)$ depends only on the sequence $\widetilde{x}_n$ and on $p(1), \dots, p(w)$ but not on the special construction of the matrices $V^{(k)}$. Of course not all w-tuples $p(1), \dots, p(w)$ can occur in this construction. Those which can are called *admissible*. (For the case $w = 0$ we have to make the obvious adaptations in the notation.)

LEMMA 3. *For the discrepancy* $\overline{D}_{N_0}^* =: D$ *of the initial point set* x_n, $n = 1, \dots, N_0$, *we have*

$$N_0 D < q^s \Big(2st_0 + 2^s + q + \sum_{m=1}^{t_0-1} \sum_{w=0}^{s-1} \sum_{(p_1,\dots,p_w)} q^{m-(p_1+\dots+p_w)-h(p_1,\dots,p_w)} \Big)\,.$$

(*The last summation is over all w-tuples $p_1,\dots,p_w$ which are admissible with respect to m, and the quantity h of course also depends on m.*)

P r o o f. For $i=1,\dots,s$ let $\beta^{(i)} := \sum_{k=1}^{\infty} \beta_k^{(i)} q^{-k}$. Let $B := \prod_{i=1}^{s} [0,\beta^{(i)})$ and for any $C \subset I^s$ let $A(C)$ be the number of $\widetilde{x}_n$, $n=0,\dots,q^m-1$, in C. Let

$$\Theta := \bigcup_{\substack{(p_1,\dots,p_s)\\ \text{admissible}}} \bigcup_{\substack{b_{p_i}^{(i)}=0\\ i=1,\dots,s}}^{\beta_{p_i}^{(i)}-1} \Big(\prod_{i=1}^{s} \Big[\sum_{k=1}^{p_i-1} \beta_k^{(i)} q^{-k} + b_{p_i}^{(i)} q^{-p_i}\,, \sum_{k=1}^{p_i-1} \beta_k^{(i)} q^{-k} + (b_{p_i}^{(i)}+1) q^{-p_i} \Big) \Big)\,.$$

(This is a disjoint union.) Then

$$\Theta \subset B \subset \Theta \cup \Lambda$$

where

$$\Lambda := \bigcup_{w=0}^{s-1} \bigcup_{\substack{(p_1,\dots,p_w)\\ \text{admissible}}} \bigcup_{\substack{b_{p_i}^{(i)}=0\\ i=1,\dots,w}}^{\beta_{p_i}^{(i)}-1} \Big(\prod_{i=1}^{w} \Big[\sum_{k=1}^{p_i-1} \beta_k^{(i)} q^{-k} + b_{p_i}^{(i)} q^{-p_i}\,, \sum_{k=1}^{p_i-1} \beta_k^{(i)} q^{-k} + (b_{p_i}^{(i)}+1) q^{-p_i} \Big)$$
$$\times \Big[\sum_{k=1}^{h(p_1,\dots,p_w)} \beta_k^{(w+1)} q^{-k}\,, \sum_{k=1}^{h(p_1,\dots,p_w)} \beta_k^{(w+1)} q^{-k} + q^{-h(p_1,\dots,p_w)} \Big) \times [0,1)^{s-w-1} \Big)\,.$$

We have

$$A(\Theta) - q^m V(\Theta) = 0\,.$$

For every interval in the definition of Λ the quantity A equals $q^{m-(p_1+\dots+p_w+h(p_1,\dots,p_w))}$, and the volume of these intervals is equal to $q^{-(p_1+\dots+p_w+h(p_1,\dots,p_w))}$. Therefore

$$|A(B) - q^m V(B)| \le \sum_{w=0}^{s-1} \sum_{\substack{(p_1,\dots,p_w)\\ \text{admissible}}} q^w q^{m-(p_1+\dots+p_w+h(p_1,\dots,p_w))}\,.$$

Since $\max_{i=1,\dots,s} |x_n^{(i)} - \widetilde{x}_n^{(i)}| \le q^{-m}$, the result follows by standard methods. ∎

Let now $c \in \mathbb{N}_0$ and $r \in \mathbb{N}$ be fixed. Let $m \le t$ and $(p(1),\dots,p(r-1))$ be admissible with respect to m. Let $\widetilde{U}_r^{(r)} := (z_{k,j})$ be the new constructed matrix with respect to these parameters. Again let $\overset{*}{\mathfrak{z}}_k := (z_{k,p(1)+\dots+p(r-1)+1},\dots$

$\dots, z_{k,m})$ and let $\overline{p} := p(1) + \dots + p(r-1)$. These definitions depend only on $g_1, \dots, g_r$ and not on $g_{r+1}, \dots, g_s$.

We define

$$\mathcal{M} := \{(g_1, \dots, g_r) \in (F_q[x])^r \mid \text{there exist } m \le t \text{ and } \boldsymbol{p} := (p(1), \dots, p(r-1)) \text{ admissible such that } \overset{*}{\mathfrak{z}}_k, \; k = 1, \dots, m - \overline{p} - c, \text{ are linearly dependent over } F_q\}.$$

(In this definition $\overset{*}{\mathfrak{z}}_k$, $k = 1, \dots, m - \overline{p} - c$, are viewed to be linearly independent if $m - \overline{p} - c \le 0$.)

LEMMA 4. *$|\mathcal{M}|$, the number of elements in $\mathcal{M}$, always satisfies*

$$|\mathcal{M}| \le c'_s q^{rt-c} t^r,$$

with a certain constant c'_s depending only on s.

Proof. We have (with $p := \overline{p}$)

$$|\mathcal{M}| \le \sum_{m=1}^{t} \sum_{\mathsf{p} \text{ admissible}} \sum |\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, m)|$$

where the last sum is taken over all $\boldsymbol{\lambda} := (\lambda_1, \dots, \lambda_{m-\bar{p}-c}) \in (F_q)^{m-\bar{p}-c} \setminus \{(0, \dots, 0)\}$ and where

$$\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, m) := \Big\{(g_1, \dots, g_r) \in (F_q[x])^r : \boldsymbol{p} \text{ is admissible and } \sum_{k=1}^{m-\bar{p}-c} \lambda_k \overset{*}{\mathfrak{z}}_k = 0\Big\}.$$

We have $\widetilde{U}_r^{(r)} = \widetilde{U}_1^{(r)} M$ with a regular $m \times m$ matrix M.

Let

$$\widetilde{U}_r^{(r)} := \begin{pmatrix} \mathfrak{z}_1 \\ \vdots \\ \mathfrak{z}_m \end{pmatrix} \quad \text{and} \quad \widetilde{U}_1^{(r)} := \begin{pmatrix} \mathfrak{u}_1 \\ \vdots \\ \mathfrak{u}_m \end{pmatrix}$$

with $\mathfrak{u}_j := (u_{j,1}, \dots, u_{j,m}) = (v_j, \dots, v_{j+m-1})$ if $g_r(x) = v_1 x^{t-1} + \dots + v_t$ ($v_k := 0$ if $k > t$), and $M := (\sigma_1, \dots, \sigma_m)$ with $\sigma_j = (\sigma_{1,j}, \dots, \sigma_{m,j})^t$.

Then the system $\sum_{k=1}^{m-\bar{p}-c} \lambda_k \overset{*}{\mathfrak{z}}_k = 0$ is equivalent to

$$\sum_{k=1}^{m} \xi_k \sigma_{k,\bar{p}+l} = 0, \qquad l = 1, \dots, m - \overline{p},$$

where $\xi_k := \sum_{j=1}^{m-\bar{p}-c} \lambda_j v_{k+j-1}$, $k = 1, \dots, m$.

We consider two cases.

(a) $2m-\overline{p}-c-1 \le t$. The above system in the variables ξ_k has rank $m-\overline{p}$ since M is regular. For each of the q^p solutions $(\xi_1,\dots,\xi_m)$ the system

$$\xi_k = \sum_{j=1}^{m-\bar{p}-c} \lambda_j v_{k+j-1}\,, \qquad k=1,\dots,m\,,$$

in $v_1,\dots,v_{2m-\bar{p}-c-1}$ has rank m. Therefore we have q^{m-c-1} solutions $(v_1,\dots,v_{2m-\bar{p}-c-1})$ for the initial system. Hence $g_1,\dots,g_{r-1}$ may be taken arbitrarily, $|\mathcal{M}(\boldsymbol{\lambda},\boldsymbol{p},m)| = q^{rt-m+\bar{p}}$ and consequently

$$\sum |\mathcal{M}(\boldsymbol{\lambda},\boldsymbol{p},m)| \le q^{rt-c}\,.$$

(b) $2m-\overline{p}-c-1 > t$. In this case (for any of the q^p solutions $\xi_1,\dots,\xi_m$ of $\sum_{k=1}^m \xi_k \sigma_{k,\bar{p}+l}=0,\ l=1,\dots,m-\overline{p}$) the system

$$\xi_k = \sum_{j=1}^{m-\bar{p}-c} \lambda_j v_{k+j-1}\,, \qquad k=1,\dots,m\,,$$

in the variables $v_1,\dots,v_t$ may have rank less than m.

If $\lambda_l \neq 0$ for at least one l with $1 \le l \le t-m+1$, then the system has rank m.

If there is a τ with $1 \le \tau \le 2m-t-\overline{p}-c-1$ such that $\lambda_1=\lambda_2=\dots$ $\dots=\lambda_{t-m+\tau}=0$, $\lambda_{t-m+\tau+1}\neq 0$, then the system has rank $m-\tau$. We have

$$|\mathcal{M}(\boldsymbol{\lambda},\boldsymbol{p},m)| \le \begin{cases} q^{rt-m+\bar{p}} & \text{in the first case,} \\ q^{rt-m+\bar{p}+\tau} & \text{in the second case,} \end{cases}$$

and therefore in case (b),

$$\begin{aligned}\sum |\mathcal{M}(\boldsymbol{\lambda},\boldsymbol{p},m)| &\le q^{rt-c} + \sum_{\tau=1}^{2m-t-\bar{p}-c-1} q^{2m-p-c-t-\tau} q^{rt-m+p+\tau} \\ &\le m q^{m+(r-1)t-c} + q^{rt-c}\,.\end{aligned}$$

So

$$|\mathcal{M}| \le \sum_{m=1}^{t} \sum_{\substack{\mathsf{p} \\ \bar{p}\le m}} (m q^{m+(r-1)t-c} + q^{rt-c})$$

and the assertion follows.

Now we finish the proof of the theorem. For given c as above we define a sequence $G_0,\dots,G_{s-1}$ with $G_{r-1} \subseteq (F_q[x])^r$ and with the following properties:

(i) If $(g_1,\dots,g_r) \in G_{r-1}$ then $(g_i,x)=1$ for all i.
(ii) For all $j<r$ we have $(g_1,\dots,g_j) \in G_{j-1}$.

(iii) For all $m \le t$ and all $(p(1), \ldots, p(r-1))$ which are admissible with respect to $(g_1, \ldots, g_r) \in G_{r-1}$ and m, the vectors $\overset{*}{\mathfrak{z}}_1, \ldots, \overset{*}{\mathfrak{z}}_{m-\bar{p}-c}$ are linearly independent.

Let

$$G := G_{s-1} \quad \text{and} \quad c = \left\lceil \frac{\log(2sc_s' t^s q^s)}{\log q} \right\rceil$$

(with c_s' as in Lemma 4 and $\lceil \cdot \rceil$ denoting the next larger integer). Then

$$c_s' t^s q^{-c} < \frac{1}{2s} q^{-s}$$

and therefore

$$|\mathcal{M}| \le \frac{1}{2s} q^{r(t-1)} \quad \text{for every } r\,.$$

Then

$$|G_0| \ge q^{t-1}\left(1 - \frac{1}{2s}\right),$$
$$|G_1| \ge q^{t-1}\left(1 - \frac{1}{2s}\right) q^{t-1} - \frac{1}{2s} q^{2(t-1)} = q^{2(t-1)}\left(1 - \frac{2}{2s}\right)$$

and going on in this way we get $|G| \ge q^{s(t-1)}/2$.

Now we consider

$$\Sigma := \frac{1}{|G|} \sum_{(g_1,\ldots,g_s)\in G} \sum_{m=1}^{t-1} \sum_{w=0}^{s-1} \sum_{\mathsf{p}} q^{m-\bar{p}-h(\mathsf{p},m,\mathsf{g})}$$

where the last sum is over all $\boldsymbol{p} = (p(1), \ldots, p(w))$ admissible with respect to m and $g_1, \ldots, g_s$. We have

$$\begin{aligned}
\Sigma &\le \frac{1}{|G|} \sum_{m=1}^{t-1} \sum_{w=0}^{s-1} q^{t(s-w-1)} \sum_{(g_1,\ldots,g_{w+1})\in G_w} \sum_{\mathsf{p}} q^{m-\bar{p}-h} \\
&\le 2q^s \sum_m \sum_w q^{-t(w+1)} \sum_{(g_1,\ldots,g_{w+1})} \sum_{\mathsf{p}} q^{m-\bar{p}-h} \\
&\le 2q^{s+1} \sum_m \sum_w q^{-t(w+1)} \sum_{\substack{(p(1),\ldots,p(w)) \\ \bar{p}\le m}} \sum_{i=m-\bar{p}-c}^{m-\bar{p}} q^{m-\bar{p}-i} \\
&\qquad\qquad \times \sum_{(\lambda_1,\ldots,\lambda_i)\in(F_q)^i\setminus\{(0,\ldots,0)\}} \sum_{\mathsf{g}} 1
\end{aligned}$$

where the last sum is over all $(g_1, \ldots, g_{w+1}) \in G_w$ for which $\boldsymbol{p}$ is admissible and $\lambda_1 \overset{*}{\mathfrak{z}}_1 + \ldots + \lambda_i \overset{*}{\mathfrak{z}}_i = 0$.

By the estimate for $\sum |\mathcal{M}(\boldsymbol{\lambda}, \boldsymbol{p}, m)|$ in the proof of Lemma 4 with $m - \overline{p} - c = i$ and $r = w + 1$ we get

$$\begin{aligned}\Sigma &\le 2q^{s+1} \sum_{m=1}^{t-1} \sum_{w=0}^{s-1} q^{-(w+1)t} \\ &\qquad \times \sum_{\substack{\mathsf{p} \\ \bar{p} \le m}} \sum_{i=m-\bar{p}-c}^{m-\bar{p}} q^{m-\bar{p}-i}(mq^{wt+i+\bar{p}} + q^{(w+1)t+i+\bar{p}-m}) \\ &\le c'' c t^s \le \widetilde{c}(\log N)^s (\log\log N)\end{aligned}$$

(here c'' is again a constant depending only on s and on q) and by Lemma 3 the result follows.

References

[1] E. Hlawka, *Zur angenäherten Berechnung mehrfacher Integrale*, Monatsh. Math. 66 (1962), 140–151.

[2] N. M. Korobov, *The approximate computation on multiple integrals*, Dokl. Akad. Nauk SSSR 124 (1959), 1207–1210 (in Russian).

[3] —, *Number-theoretical Methods in Approximate Analysis*, Fizmatgiz, Moscow 1963 (in Russian).

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

[5] G. Larcher, *On the distribution of sequences connected with good lattice points*, Monatsh. Math. 101 (1986), 135–150.

[6] H. Niederreiter, *Existence of good lattice points in the sense of Hlawka*, ibid. 86 (1978), 203–219.

[7] —, *Point sets and sequences with small discrepancy*, ibid. 104 (1987), 273–337.

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

[9] —, *Low-discrepancy point sets obtained by digital constructions over finite fields*, Czechoslovak Math. J. 42 (1992), 143–166.

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

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

INSTITUT FÜR MATHEMATIK
HELLBRUNNERSTRASSE 34
A-5020 SALZBURG
AUSTRIA

Received on 24.7.1991
and in revised form on 20.5.1992 and 17.7.1992 (2159)