A LOWER BOUND ON A QUANTITY RELATED TO THE QUALITY OF POLYNOMIAL LATTICES

PETER KRITZER AND FRIEDRICH PILLICHSHAMMER

ABSTRACT. In this paper, we study a quantity R_b which is closely related to the quality of an important subclass of digital (t, m, s)-nets over a finite field $\mathbb{F}_b$, namely polynomial lattices. Niederreiter has shown by an averaging argument that there always exist generators of polynomial lattices for which R_b is small, establishing thereby the existence of polynomial lattices with particularly low star discrepancy. In this work, we show that this result is best possible, i.e., we prove that for all generators of polynomial lattices the quantity R_b cannot go below a certain threshold.

1. Introduction and Statement of the Result

In many applications, one is interested in approximating the value of an integral $I_s(F) := \int_{[0,1]^s} F(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}$ of a function $F : [0,1]^s \to \mathbb{R}$. One way of numerically approximating $I_s(F)$ is to employ a quasi-Monte Carlo (QMC) rule,

$$Q_{N,s}(F) := \frac{1}{N}\sum_{n=0}^{N-1} F(\boldsymbol{x}_n),$$

where $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}$ are deterministically chosen points in $[0,1)^s$. We refer to a collection of integration nodes as a "point set", by which we mean a multi-set, i.e., points may occur repeatedly. It is well known (see, e.g., [5, 18]) that point sets which are in some sense evenly distributed in the unit cube yield a low integration error when applying a QMC rule for approximating $I_s(F)$.

Naturally, an essential question in the theory of QMC methods is how the node set of a QMC integration rule should be chosen. One very prominent class of point sets are polynomial lattices, as proposed by Niederreiter in [17, 18]. These point sets are special cases of digital (t, m, s)-nets (see [5, 15, 18]).

Date: May 27, 2010.

2010 *Mathematics Subject Classification.* Primary 11K06; Secondary 11T06.

Key words and phrases. Polynomial lattices, star discrepancy, digital nets.

The authors gratefully acknowledge the support of the Austrian Science Fund (FWF) Project S9609, which is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

For the construction of a polynomial lattice, choose a prime b and let $\mathbb{F}_b$ be the finite field consisting of b elements. Furthermore let $\mathbb{F}_b[x]$ be the field of polynomials over $\mathbb{F}_b$, and let $\mathbb{F}_b((x^{-1}))$ be the field of formal Laurent series over $\mathbb{F}_b$, 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 $\mathbb{F}_b$. Note that the field of Laurent series contains the field of rational functions as a subfield. Given an integer $m \geq 1$, define a function $\chi_m : \mathbb{F}_b((x^{-1})) \to [0,1)$ by

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

Let, in the following, given a prime b and an integer $m \geq 1$,

$$G_{b,m} := \{a \in \mathbb{F}_b[x] \,:\, \deg(a) < m\}.$$

Given a prime b, an integer $m \geq 1$, and a dimension $s \geq 2$, we choose an $f \in \mathbb{F}_b[x]$ with $\deg(f) = m$ and s polynomials $g_1, \ldots, g_s \in \mathbb{F}_b[x]$ and define

$$\boldsymbol{x}_h := \left(\chi_m\left(\frac{h(x)g_1(x)}{f(x)}\right), \ldots, \chi_m\left(\frac{h(x)g_s(x)}{f(x)}\right)\right), \quad h \in G_{b,m}.$$

The point set consisting of the points $\boldsymbol{x}_h$, $h \in G_{b,m}$, is denoted by $P(\boldsymbol{g}, f)$, where $\boldsymbol{g} := (g_1, \ldots, g_s)$. Note that $|P(\boldsymbol{g}, f)| = |G_{b,m}| = b^m$. Due to the many analogies of such a point set to good lattice points (see, e.g, [18, 19]), a QMC rule using $P(\boldsymbol{g}, f)$ is called polynomial lattice rule, and $P(\boldsymbol{g}, f)$ is called polynomial lattice. Using a more general terminology, $P(\boldsymbol{g}, f)$ can also be called a polynomial lattice rule of rank 1, see, e.g., [13, 14]. The polynomial f in the construction of $P(\boldsymbol{g}, f)$ is referred to as the modulus, and the vector $\boldsymbol{g}$ is referred to as the generating vector of the polynomial lattice.

Furthermore, given two vectors of polynomials $\boldsymbol{u} = (u_1, \ldots, u_r)$, $\boldsymbol{v} = (v_1, \ldots, v_r) \in (\mathbb{F}_b[x])^r$, we define

$$\boldsymbol{u} \cdot \boldsymbol{v} := \sum_{i=1}^{r} u_i v_i.$$

When studying the quality of a QMC rule using a polynomial lattice $P(\boldsymbol{g}, f)$, one frequently considers (see [1]– [5], [11, 12, 18]) the quantity

$$R_b(\boldsymbol{g}, f) := \sum_{\substack{\boldsymbol{h} \in G_{b,m}^s \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 \pmod f}} r_b(\boldsymbol{h}),$$

where for $\boldsymbol{h} = (h_1, \ldots, h_s) \in G_{b,m}^s$ we put $r_b(\boldsymbol{h}) = r_b(h_1) \cdots r_b(h_s)$, and for $h \in G_{b,m}$ we put

$$r_b(h) = \begin{cases} 1 & \text{if } h = 0, \\ \frac{1}{b^{r+1} \sin(\pi \kappa_r / b)} & \text{if } h = \kappa_0 + \kappa_1 x + \cdots + \kappa_r x^r,\ \kappa_r \neq 0. \end{cases}$$

Note that slightly different versions of r_b are considered in some of the papers cited above.

It is well known that low values of $R_b(\boldsymbol{g}, f)$ imply high quality of $P(\boldsymbol{g}, f)$ with respect to the performance of a QMC algorithm using $P(\boldsymbol{g}, f)$ as the underlying node set. In particular, the quantity $R_b(\boldsymbol{g}, f)$ is closely related to the so-called star discrepancy of $P(\boldsymbol{g}, f)$. The star discrepancy of a point set P of N points is defined as follows.

$$D_N^*(P) := \sup_{\substack{0 \le \alpha_i \le 1 \\ 1 \le i \le s}} \left| \frac{A_N\left([0, \alpha_1) \times \cdots \times [0, \alpha_s), P\right)}{N} - \alpha_1 \cdots \alpha_s \right|,$$

where $A_N(E, P)$ denotes the number of points of P lying in an interval $E \subseteq [0,1)^s$. Obviously, the star discrepancy of a point set provides a way of measuring to which extent the points are uniformly distributed in the unit cube. It was shown by Niederreiter ([18, p. 77]) that the star discrepancy D_N^* of a polynomial lattice $P(\boldsymbol{g}, f)$ with $N = b^m$ points in dimension s satisfies

$$D_N^*(P(\boldsymbol{g}, f)) \le \frac{s}{N} + R_b(\boldsymbol{g}, f), \tag{1.1}$$

hence low values of $R_b(\boldsymbol{g}, f)$ imply low star discrepancy. In particular, Theorem 4.43 in [18] states that for any prime b and dimension $s \ge 2$ there exists a number $C_{s,b} > 0$ such that for any $f \in \mathbb{F}_b[x]$ with $\deg(f) = m \ge 1$ there exists a vector $\boldsymbol{g}_0 \in G_{b,m}^s$ such that

$$R_b(\boldsymbol{g}_0, f) \le C_{s,b} \frac{m^s}{b^m}. \tag{1.2}$$

The result in (1.2) was obtained by averaging over all $\boldsymbol{g} \in G_{b,m}^s$. Together with (1.1) this establishes for any $N = b^m$ the existence of polynomial lattices $P(\boldsymbol{g}, f)$ of cardinality N and with star discrepancy

$$D_N^*(P(\boldsymbol{g}, f)) = O\left(\frac{(\log N)^s}{N}\right).$$

Constructions of such polynomial lattices using the component-by-component approach or generating vectors of so-called Korobov form can be found in [1, 3, 5].

In this paper, we are going to show that Niederreiter's result is essentially best possible, i.e., given f, there is no $\boldsymbol{g}$ with components different from zero such that the order of magnitude of $R_b(\boldsymbol{g}, f)$ with respect to the degree of

f is better than that given in (1.2). To be more precise, in Section 3 we are going to show the following theorem.

Theorem 1.1. *For any prime b and dimension $s \geq 2$ there exists a number $c_{s,b} > 0$ with the following property: for any $f \in \mathbb{F}_b[x]$ with $\deg(f) = m \geq 1$ and any $\boldsymbol{g} \in G_{b,m}^s$, $g_i \neq 0$, $1 \leq i \leq s$, we have*

$$R_b(\boldsymbol{g}, f) \geq c_{s,b} b^{\deg(\delta_s)} \frac{(m - \deg(\delta_s))^s}{b^m},$$

where $\delta_s := \gcd(g_1, \ldots, g_s, f)$.

We remark here that a corresponding result for classical integration lattices has been shown by Larcher [9] (for dimension $s = 2$) and [10] (for arbitrary dimensions $s \geq 2$).

2. Preliminaries

We use the convention $\deg(0) = -\infty$. Note that for any $h \in G_{b,m} \setminus \{0\}$ we have $r_b(h) \geq b^{-1-\deg(h)}$.

For $L \in \mathbb{F}_b((x^{-1}))$ we write $\lfloor L \rfloor$ for the polynomial part of L and $\{L\} := L - \lfloor L \rfloor$.

For the proof of Theorem 1.1 we use facts from the theory of continued fractions of formal Laurent series; see, for example, [18, Appendix B], or [7]. For the sake of completeness we recall the most important results.

Let $g, f \in \mathbb{F}_b[x]$ with $\deg(g) < \deg(f)$ and let $[0, A_1, A_2, \ldots, A_r]$ be the continued fraction expansion of g/f, $Q_1, \ldots, Q_r$, $Q_r = f$, the denominators of the convergents. Formally, we set $Q_{-1} = 0$ and $Q_0 = 1$. Furthermore, we denote by P_i the numerator of the i-th convergent to g/f. It is well known that $\deg(Q_1) < \deg(Q_2) < \cdots < \deg(Q_r)$, that $\deg(Q_i) \geq i$, and that

$$m = \deg(Q_r) = \sum_{i=1}^{r} \deg(A_i).$$

We define ν as the discrete exponential valuation on $\mathbb{F}_b((x^{-1}))$ defined by

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

Note that ν extends the degree function from $\mathbb{F}_b[x]$ to $\mathbb{F}_b((x^{-1}))$, in particular, $\nu(p) = \deg(p)$ for $p \in \mathbb{F}_b[x]$. Furthermore, for $p, q \in \mathbb{F}_b[x]$, $q \neq 0$, we have $\nu(p/q) = \deg(p) - \deg(q)$.

It is known that (see, e.g., [18, p. 220], or [7, p. 11]), for $0 \leq i < r$,

$$\nu\left(\frac{g}{f} - \frac{P_i}{Q_i}\right) \;=\; -\deg(Q_i) - \deg(Q_{i+1})$$

$$= \quad -2\deg(Q_i) - \deg(A_{i+1}). \tag{2.1}$$

Furthermore, see again [7], for $0 \le i < r$ we have

$$\frac{g}{f} - \frac{P_i}{Q_i} = \frac{(-1)^i}{(R_{i+1}Q_i + Q_{i+1})Q_i},$$

where $R_i := [A_i; A_{i+1}, \ldots, A_r]$. Using the identity $Q_{i+1} = A_{i+1}Q_i + Q_{i-1}$, we obtain

$$\begin{aligned} \frac{g}{f} - \frac{P_i}{Q_i} &= \frac{(-1)^i}{R_{i+1}Q_i^2 + A_{i+1}Q_i^2 + Q_{i-1}Q_i} \\ &= \frac{1}{A_{i+1}Q_i^2} \frac{(-1)^i}{\frac{R_{i+1}}{A_{i+1}} + 1 + \frac{Q_{i-1}}{A_{i+1}Q_i}}. \end{aligned}$$

Since $\nu(l_1 l_2) = \nu(l_1) + \nu(l_2)$, for $l_1, l_2 \in \mathbb{F}_b((x^{-1}))$, it follows from (2.1) that

$$\nu\left(\frac{(-1)^i}{\frac{R_{i+1}}{A_{i+1}} + 1 + \frac{Q_{i-1}}{A_{i+1}Q_i}}\right) = 0,$$

such that we arrive at

$$\frac{g}{f} - \frac{P_i}{Q_i} = \frac{\theta_i}{A_{i+1}Q_i^2} \tag{2.2}$$

for $0 \le i < r$, with $\theta_i \neq 0$ and $\nu(\theta_i) = 0$.

3. The Proof of Theorem 1.1

We now give the proof of Theorem 1.1.

Proof. The proof is inspired by [10]. Note that it is sufficient to show Theorem 1.1 for the case $\deg(\delta_s) = 0$, since

$$R_b(\boldsymbol{g}, f) \ge \sum_{\substack{\boldsymbol{h} \in G_{b,m'}^s \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h}\cdot\boldsymbol{g}' \equiv 0 \pmod{f'}}} r_b(\boldsymbol{h}),$$

where $f' = f/\delta_s$, $\boldsymbol{g}' = \boldsymbol{g}/\delta_s$, and $m' = m - \deg(\delta_s)$.

Hence, we assume in the following that $\deg(\delta_s) = 0$. Furthermore, we are going to assume that m is large enough to satisfy the inequality $\log_b m < 2\log_b(m - 2s\log_b m)$. For the finitely many m not satisfying this condition, the theorem holds by choosing the constant $c_{s,b} > 0$ small enough.

Let $d_i := \gcd(g_i, f)$ for $1 \le i \le s$, and $g_i t_i \equiv d_i \pmod{f}$ such that $\deg(\gcd(t_i, f)) = 0$. We consider three cases:

(1) Suppose that $\deg(d_{i_0}) \ge s\log_b m$ for an $i_0 \in \{1, \ldots, s\}$. Then we have

$$R_b(\boldsymbol{g}, f) \ge \sum_{\substack{h_{i_0} \in (G_{b,m} \setminus \{0\}) \\ h_{i_0} g_{i_0} \equiv 0 \pmod{f}}} \frac{1}{b^{\deg(h_{i_0})+1}}.$$

However, $h_{i_0} g_{i_0} \equiv 0 \pmod f$ if and only if $h_{i_0} = l \frac{f}{d_{i_0}}$, where $0 \le \deg(l) < \deg(d_{i_0})$, so

$$R_b(\boldsymbol{g}, f) \ge \frac{1}{b} \sum_{\substack{l \in \mathbb{F}_b[x] \\ 0 \le \deg(l) < \deg(d_{i_0})}} \frac{b^{\deg(d_{i_0})}}{b^{\deg(l)+\deg(f)}} \ge \frac{b-1}{b} \frac{m^s}{b^m}.$$

Hence, we can assume $\deg(d_i) \le s \log_b m$ for all $i \in \{1, \ldots, s\}$ in the following.

(2) Suppose that one continued fraction coefficient A_{k_0} of a $\frac{g_{i_0} t_{j_0} d_{j_0}}{f}$, $i_0 \ne j_0$, $1 \le i_0, j_0 \le s$ satisfies $\deg(A_{k_0}) \ge s \log_b m$. Then we have

$$\begin{aligned}
R_b(\boldsymbol{g}, f) &\ge \sum_{\substack{(h_{i_0}, h_{j_0}) \in G_{b,m}^2 \setminus \{\mathbf{0}\} \\ h_{i_0} g_{i_0} + h_{j_0} g_{j_0} \equiv 0 \pmod f}} r_b(h_{i_0}) r_b(h_{j_0}) \\
&= \sum_{\substack{(h_{i_0}, h_{j_0}) \in G_{b,m}^2 \setminus \{\mathbf{0}\} \\ h_{i_0} g_{i_0} t_{j_0} + h_{j_0} g_{j_0} t_{j_0} \equiv 0 \pmod f}} r_b(h_{i_0}) r_b(h_{j_0}) \\
&= \sum_{\substack{(h_{i_0}, h_{j_0}) \in G_{b,m}^2 \setminus \{\mathbf{0}\} \\ h_{i_0} g_{i_0} t_{j_0} + h_{j_0} d_{j_0} \equiv 0 \pmod f}} r_b(h_{i_0}) r_b(h_{j_0}) \\
&\ge \sum_{\substack{(h_{i_0}, h_{j_0}) \in G_{b,m}^2 \setminus \{\mathbf{0}\} \\ h_{i_0} \equiv 0 \pmod{d_{j_0}} \\ h_{i_0} g_{i_0} t_{j_0} + h_{j_0} d_{j_0} \equiv 0 \pmod f}} r_b(h_{i_0}) r_b(h_{j_0}) \\
&\ge \sum_{\substack{(h_{i_0}, h_{j_0}) \in G_{b,m'}^2 \setminus \{\mathbf{0}\} \\ h_{i_0} g_{i_0} t_{j_0} + h_{j_0} \equiv 0 \pmod{f/d_{j_0}}}} \frac{r_b(h_{i_0}) r_b(h_{j_0})}{b^{\deg(d_{j_0})}},
\end{aligned}$$

where $m' := \deg(f/d_{j_0})$. Let now Q_k, $0 \le k \le r$, be the denominator of the k-th convergent of $\frac{g_{i_0} t_{j_0} d_{j_0}}{f}$, $Q_{-1} = 0$, $Q_0 = 1$, $Q_k = A_k Q_{k-1} + Q_{k-2}$ for $1 \le k \le r$.

Furthermore, let $h'_{i_0} := Q_{k_0-1}$, then there is a solution h'_{j_0} of $h'_{i_0} g_{i_0} t_{j_0} + h'_{j_0} \equiv 0 \pmod{f/d_{j_0}}$ such that

$$\begin{aligned}
\deg(h'_{j_0}) &= \deg(f/d_{j_0}) + \nu\left(\left\{\frac{Q_{k_0-1} g_{i_0} t_{j_0} d_{j_0}}{f}\right\}\right) \\
&= \deg(f/d_{j_0}) + \nu\left(\left\{Q_{k_0-1}\left(\frac{g_{i_0} t_{j_0} d_{j_0}}{f} - \frac{P_{k_0-1}}{Q_{k_0-1}}\right)\right\}\right) \\
&\le \deg(f/d_{j_0}) + \nu\left(Q_{k_0-1}\left(\frac{g_{i_0} t_{j_0} d_{j_0}}{f} - \frac{P_{k_0-1}}{Q_{k_0-1}}\right)\right) \\
&= \deg(f/d_{j_0}) - \deg(A_{k_0}) - \deg(Q_{k_0-1}),
\end{aligned}$$

where we used (2.1). Hence,

$$R_b(\boldsymbol{g}, f) \geq \frac{r(h'_{i_0})r(h'_{j_0})}{b^{\deg(d_{j_0})}} \geq \frac{1}{b^2}\frac{b^{\deg(A_{k_0})}}{b^{\deg(d_{j_0})}b^{\deg(f/d_{j_0})}} \geq \frac{1}{b^2}\frac{m^s}{b^m}.$$

So we can assume that the degrees of the continued fraction coefficients of $\frac{g_i t_j d_j}{f}$, $i \neq j$, $1 \leq i, j \leq s$, are smaller than $s \log_b m$.

(3) Suppose that $\deg(d_i) \leq s \log_b m$ for all $1 \leq i \leq s$ and that the degrees of the continued fraction coefficients of $\frac{g_i t_j d_j}{f}$, $i \neq j$, $1 \leq i, j \leq s$, are smaller than $s \log_b m$. In this case the result follows from the subsequent Lemma 3.1, so the result of the theorem is shown.

□

We now prove the following lemma which completes the proof of Theorem 1.1.

Lemma 3.1. *Let b be a prime, let $s \geq 2$, $\sigma \in \{2, \ldots, s\}$, and $\boldsymbol{g} = (g_1, \ldots, g_s) \in G_{b,m}^s$, $g_i \neq 0$, $1 \leq i \leq s$. Furthermore, define $d_i := \gcd(g_i, f)$ with $\deg(d_i) \leq s \log_b m$ for $1 \leq i \leq s$. Let $g_i t_i \equiv d_i \pmod f$ such that $\deg(\gcd(t_i, f)) = 0$, and assume that the degrees of the continued fraction coefficients of $\frac{g_i t_j d_j}{f}$, $i \neq j$, $1 \leq i, j \leq s$, are less than $s \log_b m$. Moreover, assume that m is large enough to satisfy the inequality $\log_b m < 2\log_b(m - 2s\log_b m)$. Then it is true that*

$$\widetilde{R}(\sigma, \boldsymbol{g}, f, w) := \sum_{\substack{\boldsymbol{h} \in G_{b,m}^{\sigma} \setminus \{\boldsymbol{0}\} \\ h_1 g_1 + \cdots + h_\sigma g_\sigma \equiv w \pmod f}} r_b(\boldsymbol{h}) \geq c(\sigma, s, b) b^{\deg(\delta_\sigma)} \frac{m^\sigma}{b^m},$$

for any $w \in \mathbb{F}_b[x]$ for which

$$\delta_\sigma := \gcd(g_1, \ldots, g_\sigma, f)$$

is a divisor of w. Here $c(\sigma, s, b) > 0$ is a constant depending only on σ, s, and b.

Proof. First of all, assume that the bound in the lemma holds true for $\deg(\delta_\sigma) = 0$, then for the case that $\deg(\delta_\sigma) > 0$ we set $g'_i = g_i/\delta_\sigma$ for $1 \leq i \leq \sigma$, $w' = w/\delta_\sigma$, $f' = f/\delta_\sigma$, and $m' = m - \deg(\delta_\sigma)$. Since we assumed $\deg(d_i) \leq s \log_b m$, which implies $\deg(\delta_\sigma) \leq s \log_b m$, we then obtain

$$\begin{aligned} \sum_{\substack{\boldsymbol{h} \in G_{b,m}^{\sigma} \setminus \{\boldsymbol{0}\} \\ h_1 g_1 + \cdots + h_\sigma g_\sigma \equiv w \pmod f}} r_b(\boldsymbol{h}) &\geq \sum_{\substack{\boldsymbol{h} \in G_{b,m'}^{\sigma} \setminus \{\boldsymbol{0}\} \\ h_1 g'_1 + \cdots + h_\sigma g'_\sigma \equiv w' \pmod{f'}}} r_b(\boldsymbol{h}) \\ &\geq c(\sigma, s, b)\frac{(m')^\sigma}{b^{m'}} \end{aligned}$$

$$\begin{aligned} &\geq c(\sigma,s,b)b^{\deg(\delta_\sigma)}\frac{(m-s\log_b m)^\sigma}{b^m} \\ &\geq \widetilde{c}(\sigma,s,b)b^{\deg(\delta_\sigma)}\frac{m^\sigma}{b^m}, \end{aligned}$$

with another constant $\widetilde{c}(\sigma,s,b)>0$ depending only on σ, s, and b.

Hence there is no loss of generality in assuming in the following that $\deg(\delta_\sigma)=0$.

We are going to show the result of the lemma by induction on σ.

The case $\sigma=2$: Here, we study

$$\widetilde{R}(2,(g_1,g_2),f,w) := \sum_{\substack{\boldsymbol{h}\in G_{b,m}^2\setminus\{\mathbf{0}\}\\ h_1g_1+h_2g_2\equiv w \pmod f}} r_b(\boldsymbol{h}),$$

where we assume, without loss of generality, $\deg(\gcd(g_1,g_2,f))=0$, and set $d_i:=\gcd(g_i,f)$, $p:=f/d_2$.

Now, if $h_1g_1+h_2g_2\equiv w \pmod f$, then $h_2g_2\equiv w-h_1g_1 \pmod f$, and the latter equivalence can be solved if $w-h_1g_1\equiv 0 \pmod{d_2}$, which is fulfilled due to our assumptions. Hence there exist $a,l\in\mathbb{F}_b[x]$, $\deg(a)<\deg(d_2)$, such that $h_1=a+ld_2$ and $w-ag_1\equiv 0\pmod{d_2}$, so $h_2g_2\equiv w-g_1a-g_1ld_2 \pmod f$. Let now $v:=\frac{w-g_1a}{d_2}t_2$. With this notation, we have that $h_2\equiv v-g_1lt_2 \pmod p$, where p is defined as above.

Therefore, for every $l\in\mathbb{F}_b[x]$, there exists a solution

$$h_2 = p\left\{\frac{v}{p}-\frac{g_1lt_2}{p}\right\},$$

and we obtain

$$\begin{aligned} \widetilde{R}(2,(g_1,g_2),f,w) &\geq \frac{1}{b^2}\sum_{\substack{0\neq l\in\mathbb{F}_b[x]\\ \deg(l)<\deg(p)}} \frac{1}{b^{\deg(ld_2)}\max\left(1, b^{\deg\left(p\left\{\frac{v}{p}-\frac{g_1lt_2}{p}\right\}\right)}\right)} \\ &= \frac{1}{b^2}\frac{1}{b^{\deg(p)}}\frac{1}{b^{\deg(d_2)}}\sum_{\substack{0\neq l\in\mathbb{F}_b[x]\\ \deg(l)<\deg(p)}} \frac{1}{b^{\deg(l)}\max\left(\frac{1}{b^{\deg(p)}}, b^{\nu\left(\left\{\frac{v}{p}-\frac{g_1lt_2}{p}\right\}\right)}\right)}. \end{aligned}$$

Let now $G:=\frac{g_1t_2}{d_1}$ and $F:=\frac{p}{d_1}$, then $\gcd(G,F)=\frac{1}{d_1}\gcd(g_1t_2,p)=1$, and, due to our assumptions, G/F has continued fraction coefficients A_k with $\deg(A_k)<s\log_b m<2s\log_b(m-2s\log_b m)\leq 2s\log_b(\deg(F))$.

We are now going to show the following inequality. For every $a\in\mathbb{F}_b((x^{-1}))$, $\nu(a)<0$, and for a constant $c(s,b)>0$ it is true that

$$\Sigma := \sum_{\substack{0\neq l\in\mathbb{F}_b[x]\\ \deg(l)<\deg(F)}} \frac{1}{b^{\deg(l)}\max\left(\frac{1}{b^{\deg(F)}}, b^{\nu\left(\left\{a-l\frac{G}{F}\right\}\right)}\right)} \geq c(s,b)(\deg(F))^2. \tag{3.1}$$

Let $Q_0,Q_1,\ldots,Q_r$, $Q_0=1$, $Q_{-1}=0$, $Q_r=F$, be the denominators of the convergents to G/F, with $Q_i=A_iQ_{i-1}+Q_{i-2}$ for $1\leq i\leq r$, $\deg(A_i)<$

$s \log_b m$. Then we have, as shown in (2.2),

$$\frac{G}{F} - \frac{P_i}{Q_i} = \frac{\theta_i}{A_{i+1}Q_i^2}, \text{ where } \nu(\theta_i) \le 0.$$

Furthermore,

$$\begin{aligned}\Sigma &= \sum_{y=0}^{\deg(F)-1} \sum_{\substack{l \in \mathbb{F}_b[x] \\ \deg(l)=y}} \frac{1}{b^{\deg(l)} \max\left(\frac{1}{b^{\deg(F)}}, b^{\nu(\{a-l\frac{G}{F}\})}\right)} \\ &\ge \sum_{i=0}^{r-1} \sum_{z_1=0}^{\deg(A_{i+1})-1} \sum_{z_2 \in \{-\infty,0,1,2,\ldots,\deg(Q_i)-1\}} S(i,z_1,z_2),\end{aligned}$$

where

$$S(i,z_1,z_2) := \sum_{\substack{l=\kappa Q_i+\lambda \\ \deg(\kappa)=z_1 \\ \deg(\lambda)=z_2}} \frac{1}{b^{\deg(l)} \max\left(\frac{1}{b^{\deg(F)}}, b^{\nu(\{a-l\frac{G}{F}\})}\right)}.$$

We have

$$\begin{aligned}b^{\deg(l)} \max\left(\frac{1}{b^{\deg(F)}}, b^{\nu(\{a-l\frac{G}{F}\})}\right) &= b^{z_1} b^{\deg(Q_i)} b^{\max\left(-\deg(F), \nu\left(\{a-l\frac{G}{F}\}\right)\right)} \\ &= b^{z_1} b^{\max\left(\deg(Q_i)-\deg(F), \deg(Q_i)+\nu\left(\{a-l\frac{G}{F}\}\right)\right)}.\end{aligned}$$

Now, on the one hand, for $0 \le i < r$ we have

$$\deg(Q_i) - \deg(F) \le -1,$$

and, on the other hand, for $0 \le i < r$ and $l = \kappa Q_i + \lambda$ we have

$$\begin{aligned}&\deg(Q_i) + \nu\left(\left\{a - l\frac{G}{F}\right\}\right) = \\ &= \deg(Q_i) + \nu\left(\left\{a - (\kappa Q_i+\lambda)\left(\frac{G}{F} - \frac{P_i}{Q_i} + \frac{P_i}{Q_i}\right)\right\}\right) \\ &= \deg(Q_i) + \nu\left(\left\{a - (\kappa Q_i+\lambda)\left(\frac{\theta_i}{A_{i+1}Q_i^2} + \frac{P_i}{Q_i}\right)\right\}\right) \\ &= \deg(Q_i) + \nu\left(\left\{a - \frac{\lambda P_i}{Q_i} - \frac{(\kappa Q_i+\lambda)\theta_i}{A_{i+1}Q_i^2}\right\}\right) \\ &= \deg(Q_i) + \nu\left(\left\{\frac{\lfloor aQ_i \rfloor + \{aQ_i\} - \lambda P_i}{Q_i} - \frac{(\kappa Q_i+\lambda)\theta_i}{A_{i+1}Q_i^2}\right\}\right) \\ &= \deg(Q_i) + \nu\left(\left\{\frac{k(\lambda) + \{aQ_i\}}{Q_i} - \frac{(\kappa Q_i+\lambda)\theta_i}{A_{i+1}Q_i^2}\right\}\right) \\ &= \deg(Q_i) + \nu\left(\frac{k(\lambda) + \{aQ_i\}}{Q_i} - \frac{(\kappa Q_i+\lambda)\theta_i}{A_{i+1}Q_i^2}\right) \\ &= \nu\left(Q_i\left(\frac{k(\lambda) + \{aQ_i\}}{Q_i} - \frac{(\kappa Q_i+\lambda)\theta_i}{A_{i+1}Q_i^2}\right)\right)\end{aligned}$$

$$\begin{aligned} &= \nu\left(k(\lambda) + \{aQ_i\} - \frac{(\kappa Q_i + \lambda)\theta_i}{A_{i+1}Q_i}\right) \\ &\leq \deg(k(\lambda)) + 1. \end{aligned}$$

where $k(\lambda) := \lfloor aQ_i \rfloor - \lambda P_i \pmod{Q_i}$.

Consequently,

$$b^{\deg(l)} \max\left(\frac{1}{b^{\deg(F)}}, b^{\nu(\{a - l\frac{G}{F}\})}\right) \leq b^{z_1} b^{\phi(\lambda)},$$

where

$$\phi(\lambda) := \begin{cases} \deg(Q_i) - \deg(F) & \text{if } k(\lambda) = 0, \\ \deg(k(\lambda)) + 1 & \text{otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned} \Sigma &\geq \sum_{i=0}^{r-1} \sum_{z_1=0}^{\deg(A_{i+1})-1} \frac{1}{b^{z_1}} \sum_{z_2 \in \{-\infty,0,1,2,\ldots,\deg(Q_i)-1\}} \sum_{\substack{\kappa \in \mathbb{F}_b[x] \\ \deg(\kappa)=z_1}} \sum_{\substack{\lambda \in \mathbb{F}_b[x] \\ \deg(\lambda)=z_2}} \frac{1}{b^{\phi(\lambda)}}. \\ &= (b-1)\sum_{i=0}^{r-1} \deg(A_{i+1}) \sum_{\substack{\lambda \in \mathbb{F}_b[x] \\ \deg(\lambda)<\deg(Q_i)}} \frac{1}{b^{\phi(\lambda)}} \\ &= (b-1)\sum_{i=0}^{r-1} \deg(A_{i+1}) \left(\frac{1}{b^{\deg(Q_i)-\deg(F)}} + \sum_{\substack{\lambda \in \mathbb{F}_b[x] \\ k(\lambda) \neq 0 \\ \deg(\lambda)<\deg(Q_i)}} \frac{1}{b^{\deg(k(\lambda))+1}} \right). \end{aligned}$$

Now as λ runs through all polynomials in $\mathbb{F}_b[x]$ with degree less than $\deg(Q_i)$, so does $k(\lambda)$.

$$\begin{aligned} \Sigma &\geq (b-1)\sum_{i=0}^{r-1} \deg(A_{i+1}) \sum_{z=0}^{\deg(Q_i)-1} \frac{1}{b^{z+1}} \sum_{\substack{\lambda \in \mathbb{F}_b[x] \\ \deg(\lambda)=z}} 1 \\ &= \frac{(b-1)^2}{b} \sum_{i=0}^{r-1} \deg(A_{i+1}) \deg(Q_i). \end{aligned}$$

For the latter expression,

$$\sum_{i=0}^{r-1} \deg(A_{i+1}) \deg(Q_i) = \sum_{i=0}^{r-1} \deg(A_{i+1}) \sum_{j=1}^{i} \deg(A_j).$$

Note that

$$\begin{aligned} \sum_{i=0}^{r-1} \deg(A_{i+1}) \sum_{j=1}^{i} \deg(A_j) &= \sum_{i=1}^{r} \deg(A_i) \sum_{j=1}^{i-1} \deg(A_j) \\ &= \sum_{j=1}^{r} \deg(A_j) \sum_{i=j+1}^{r} \deg(A_i). \end{aligned}$$

Hence,

$$\begin{aligned} 2\sum_{i=1}^{r}\deg(A_i)\sum_{j=1}^{i-1}\deg(A_j) &= \sum_{i=1}^{r}\deg(A_i)\sum_{j=1}^{r}\deg(A_j)-\sum_{i=1}^{r}\deg(A_i)^2 \\ &= (\deg(F))^2-\sum_{i=1}^{r}\deg(A_i)^2. \end{aligned}$$

However, from the assumption on $\deg(A_i)$ we obtain $\deg(A_i)\le 2s\log_b(\deg(F))$, hence the latter expression is bounded from below by

$$(\deg(F))^2-\deg(F)(2s\log_b(\deg(F))^2,$$

and (3.1) is shown.

However, (3.1) implies

$$\begin{aligned} \widetilde{R}(2,(g_1,g_2),f,w) &\ge \frac{1}{b^2}\frac{1}{b^{\deg(p)}}\frac{1}{b^{\deg(d_2)}}c(s,b)(\deg(F))^2 \\ &\ge \frac{1}{b^2}\frac{1}{b^{\deg(p)}}\frac{1}{b^{\deg(d_2)}}c(s,b)(m-2s\log_b m)^2 \\ &= \frac{1}{b^2}\frac{1}{b^{\deg(f)-\deg(d_2)}}\frac{1}{b^{\deg(d_2)}}c(s,b)(m-2s\log_b m)^2 \\ &\ge c'(s,b)\frac{m^2}{b^m}, \end{aligned}$$

with $c'(s,b)>0$ another constant depending only on s and b. Hence we have shown the result of the lemma for $\sigma=2$.

Induction step $\sigma-1\to\sigma$**:** The condition $h_1g_1+\cdots+h_\sigma g_\sigma\equiv w\pmod f$ is equivalent to

$$h_1g_1+\cdots+h_{\sigma-1}g_{\sigma-1}\equiv w-h_\sigma g_\sigma \pmod f.$$

The latter congruence has a solution if and only if $\delta_{\sigma-1}:=\gcd(g_1,\ldots,g_{\sigma-1},f)$ is a divisor of $w-h_\sigma g_\sigma$, i.e.,

$$h_\sigma g_\sigma\equiv w\pmod{\delta_{\sigma-1}}.$$

Now, since $\deg(\gcd(\delta_{\sigma-1},g_\sigma))=\deg(\delta_\sigma)=0$, there exists an $a\in\mathbb{F}_b[x]$, $\deg(a)<\deg(\delta_{\sigma-1})$, such that

$$w-ag_\sigma\equiv 0\pmod{\delta_{\sigma-1}},$$

and so

$$h_\sigma=a+l\delta_{\sigma-1}.$$

Hence we have, using the induction assumption,

$$\begin{aligned} &\widetilde{R}(\sigma,\boldsymbol{g},f,w) \\ &\ge \sum_{\substack{l\in\mathbb{F}_b[x]\\ \deg(l)<m-\deg(\delta_{\sigma-1})}}\frac{1}{b^{\deg(a+l\delta_{\sigma-1})}}\sum_{\substack{\boldsymbol{h}\in G_{b,m}^{\sigma-1}\setminus\{\boldsymbol{0}\}\\ h_1g_1+\cdots+h_{\sigma-1}g_{\sigma-1}\equiv w-(a+l\delta_{\sigma-1})g_\sigma \pmod f}} r_b(\boldsymbol{h}) \end{aligned}$$

$$\geq \quad c(\sigma-1,s,b)b^{\deg(\delta_{\sigma-1})}\frac{m^{\sigma-1}}{b^m} \sum_{\substack{l\in\mathbb{F}_b[x]\\ \deg(l)<m-\deg(\delta_{\sigma-1})}} \frac{1}{b^{\deg(a+l\delta_{\sigma-1})}}.$$

Now, for the latter sum we have

$$\begin{aligned}\sum_{\substack{l\in\mathbb{F}_b[x]\\ \deg(l)<m-\deg(\delta_{\sigma-1})}} \frac{1}{b^{\deg(a+l\delta_{\sigma-1})}} &\geq \frac{1}{b^{\deg(a)}}+\frac{1}{b^{\deg(\delta_{\sigma-1})}} \sum_{\substack{l\in\mathbb{F}_b[x]\\ 0\leq\deg(l)<m-\deg(\delta_{\sigma-1})}} \frac{1}{b^{\deg(l)}}\\ &\geq \frac{1}{b^{\deg(\delta_{\sigma-1})}}(m-\deg(\delta_{\sigma-1}))\\ &\geq \frac{1}{b^{\deg(\delta_{\sigma-1})}}c''(s,b)m,\end{aligned}$$

where $c''(s,b) > 0$ is another constant depending only on s and b, and where we made use of the assumption that $\deg(\delta_{\sigma-1}) \leq s\log_b m$. The result follows. □

References

[1] J. Dick, P. Kritzer, G. Leobacher, F. Pillichshammer, *Constructions of general polynomial lattice rules based on the weighted star discrepancy*, Finite Fields Appl. 13 (2007), 1045–1070.

[2] J. Dick, F.Y. Kuo, F. Pillichshammer, I.H. Sloan, *Construction algorithms for polynomial lattice rules for multivariate integration*, Math. Comp. 74 (2005), 1895–1921.

[3] J. Dick, G. Leobacher, F. Pillichshammer, *Construction algorithms for digital nets with small weighted star discrepancy*. SIAM J. Numer. Anal. 43 (2005), 76–95.

[4] J. Dick, F. Pillichshammer, *Multivariate integration in weighted Hilbert spaces based on Walsh functions and weighted Sobolev spaces*, J. Complexity 21 (2005), 149–195.

[5] J. Dick, F. Pillichshammer, *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, 2010 (to appear).

[6] M. Drmota, R.F. Tichy, *Sequences, Discrepancies and Applications*, Springer, Berlin, 1997.

[7] M. Fuchs, *Kettenbrüche im Körper der formalen Laurentreihen und Anwendungen*, Master thesis, Vienna University of Technology, 2000 (available at http://dmg.tuwien.ac.at/drmota/ (state: May 27, 2010)).

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

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

[10] G. Larcher, *A best lower bound for good lattice points*, Monatsh. Math. 104 (1987), 45–51.

[11] G. Larcher, *Digital point sets: analysis and applications*, in: Random and Quasi-Random Point Sets, P. Hellekalek and G. Larcher (eds.), Lecture Notes in Statistics Vol. 138, Springer, New York, 1998, 167–222.

[12] G. Larcher, A. Lauss, H. Niederreiter, W.Ch. Schmid, *Optimal polynomials for (t, m, s)-nets and numerical integration of multivariate Walsh series*, SIAM J. Numer. Anal. 33 (1996), 2239–2253.

[13] P. L'Ecuyer, *Polynomial integration lattices*, in: Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer, Berlin, 2004, 73–98.

[14] C. Lemieux, P. L'Ecuyer, *Randomized polynomial lattice rules for multivariate integration and simulation*, SIAM J. Sci. Comput. 24 (2003), 1768–1789.

[15] H. Niederreiter, *Point sets and sequences with small star discrepancy.* Monatsh. Math. 104 (1987), 273–337.

[16] H. Niederreiter, *Sequences with almost perfect linear complexity profile*, in: Advances in Cryptology—EUROCRYPT '87, D. Chaum and W.L. Price (eds.), Lecture Notes in Computer Science Vol. 304, Springer, Berlin, 1988, 37–51.

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

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

[19] I.H. Sloan, S. Joe, *Lattice methods for multiple integration*, Oxford University Press, Oxford, 1994.

Fachbereich Mathematik, University of Salzburg, Hellbrunnerstr. 34, 5020 Salzburg, Austria

E-mail address: peter.kritzer@gmail.com

Institut für Finanzmathematik, University of Linz, Altenbergerstr. 69, 4040 Linz, Austria

E-mail address: friedrich.pillichshammer@jku.at