PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 8, August 2017, Pages 3297–3310
http://dx.doi.org/10.1090/proc/13490
Article electronically published on January 27, 2017

DIGITAL INVERSIVE VECTORS CAN ACHIEVE POLYNOMIAL TRACTABILITY FOR THE WEIGHTED STAR DISCREPANCY AND FOR MULTIVARIATE INTEGRATION

JOSEF DICK, DOMINGO GOMEZ-PEREZ, FRIEDRICH PILLICHSHAMMER, AND ARNE WINTERHOF

(Communicated by Walter Van Assche)

In memory of Joseph Frederick Traub (1932–2015)
and
Oscar Moreno de Ayala (1946–2015)

Abstract. We study high-dimensional numerical integration in the worst-case setting. The subject of tractability is concerned with the dependence of the worst-case integration error on the dimension. Roughly speaking, an integration problem is tractable if the worst-case error does not grow exponentially fast with the dimension. Many classical problems are known to be intractable. However, sometimes tractability can be shown. Often such proofs are based on randomly selected integration nodes. Of course, in applications, true random numbers are not available and hence one mimics them with pseudorandom number generators. This motivates us to propose the use of pseudorandom vectors as underlying integration nodes in order to achieve tractability. In particular, we consider digital inverse vectors and present two examples of problems, the weighted star discrepancy and integration of Hölder continuous, absolute convergent Fourier and cosine series, where the proposed method is successful.

1. Introduction

We study numerical integration of multivariate functions f defined on the s-dimensional unit cube by means of quasi-Monte Carlo (QMC) rules; i.e.,

$$I_s(f) := \int_{[0,1]^s} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x} \approx \frac{1}{N}\sum_{n=0}^{N-1} f(\boldsymbol{x}_n) =: Q_N(f),$$

where we assume that $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ are well chosen integration nodes from the unit cube and where Q_N is the QMC rule based on these nodes. General references for QMC integration are [5, 6, 15, 18].

Received by the editors December 21, 2015 and, in revised form, September 9, 2016.
2010 *Mathematics Subject Classification.* Primary 11K38, 11K45, 11T23, 65C05, 65C10.
Key words and phrases. Weighted star discrepancy, pseudorandom numbers, tractability, quasi-Monte Carlo.
The research of the first author was supported under the Australian Research Councils Discovery Projects funding scheme (project number DP150101770). The research of the second author was supported by the Ministerio de Economia y Competitividad research project MTM2014-55421-P. The third and fourth authors were supported by the Austrian Science Fund (FWF): Projects F5509-N26 (third author) and F5511-N26 (fourth author), respectively, which are part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

Usually, one studies integrands from a given Banach space $(\mathcal{F}, \|\cdot\|_{\mathcal{F}})$ of functions. As quality criterion, we consider the *worst-case error*

$$e(Q_N, \mathcal{F}) := \sup_{\substack{f \in \mathcal{F} \\ \|f\|_{\mathcal{F}} \leq 1}} |I_s(f) - Q_N(f)|.$$

For many function classes, the problem of QMC integration is well studied and one can achieve optimal asymptotic convergence rates for the worst-case error that are often of the form $O(N^{-1+\varepsilon})$ for some $\varepsilon > 0$ with some implicit dependence on the dimension s. Although this is the best possible convergence rate in N, the dependence on the dimension can be crucial if s is large. This question is the subject of tractability. Tractability means that we control the dependence of the worst-case error on the dimension.

Tractability. For the numerical integration problem in $\mathcal{F}$ the *Nth minimal worst-case error* is defined as

$$e(N, s) := \inf_{A_{N,s}} \sup_{\substack{f \in \mathcal{F} \\ \|f\|_{\mathcal{F}} \leq 1}} |I_s(f) - A_{N,s}(f)|,$$

where the infimum is extended over all integration rules (not necessarily QMC rules) that are based on N function evaluations $f(\boldsymbol{x}_n)$, $n = 0, 1, \ldots, N-1$. For $\varepsilon \in (0,1)$ the *information complexity* $N(\varepsilon, s)$ is then defined as the minimal number of function evaluations that are required in order to achieve a worst-case error of at most ε. In other words,[1]

$$N(\varepsilon, s) := \min\{N \in \mathbb{N} \ : \ e(N, s) \leq \varepsilon\}.$$

We say that we have:

- The *curse of dimensionality* if there exist positive numbers C, τ, and ε_0 such that
$$N(\varepsilon, s) \geq C(1+\tau)^s \quad \text{for all } \varepsilon \leq \varepsilon_0 \ \text{ and infinitely many } s \in \mathbb{N}.$$
- *Polynomial tractability* if there exist non-negative numbers C, τ_1, τ_2 such that
$$N(\varepsilon, s) \leq C s^{\tau_1} \varepsilon^{-\tau_2} \quad \text{for all } s \in \mathbb{N},\ \varepsilon \in (0,1).$$
- *Strong polynomial tractability* if there exist non-negative numbers C and τ such that
$$N(\varepsilon, s) \leq C \varepsilon^{-\tau} \quad \text{for all } s \in \mathbb{N},\ \varepsilon \in (0,1).$$

In addition to polynomial and strong polynomial tractability, there is also the refined notion of *weak tractability* that means that

$$\lim_{\varepsilon^{-1}+s \to \infty} \frac{\log N(\varepsilon, s)}{\varepsilon^{-1} + s} = 0.$$

Problems that are not weakly tractable (that is, the information complexity depends exponentially on ε^{-1} or s) are said to be *intractable*. There are even further more refined notions of tractability but those mentioned above are certainly the most important and most studied ones. For a detailed introduction into tractability theory we refer to the three volumes of Novak and Woźniakowski [20–22].

[1]Here, we speak about the absolute error criterion. Sometimes, one uses the so-called initial error $e(0, s) = \|I_s\|$ as a reference value and asks for the minimal N in order to reduce this minimal error by a factor of ε. In this case, one speaks about the normalized error criterion.

It is known that many multivariate problems defined over standard spaces of functions suffer from the curse of dimensionality. Examples include integration of Lipschitz functions, monotone functions, convex functions (see [11]), or smooth functions (see [9, 10]). A possible reason for this disadvantageous behavior may be found in the fact that for standard spaces all variables and groups of variables are equally important. As a way out, Sloan and Woźniakowski [24] suggested considering weighted spaces. This means that the importance of successive variables and groups of variables of function is monitored by corresponding weights. This often allows one to vanquish the curse of dimensionality and to obtain polynomial or even strong polynomial tractability, depending on the decay of the weights.

In some cases it is possible to construct QMC rules that achieve tractability in some sense. One example is (polynomial) lattice rules for integration in weighted Korobov spaces or Sobolev spaces. However, the point sets of these rules heavily depend on the chosen weights and can generally not be reused with different weights. A further disadvantage is, that there is in general no explicit construction for point sets that can achieve tractability error bounds and thus one relies on computer search algorithms (for example, the fast component-by-component constructions; see [5, 15] and the references therein).

On the other hand, for those instances of problems that are tractable this property is often proved with probabilistic arguments. A particular example is the "inverse of star discrepancy problem" for which Heinrich, Novak, Wasilkowski, and Woźniakowski [12] showed with the help of random point sets that the star discrepancy is polynomially tractable (see also [1]). In [2] it is even shown that with very high probability (say 99%), a randomly selected point set satisfies the aforementioned bounds. However, if we generate a random point set on a computer using a pseudorandom number generator, this result does not apply since the pseudorandom numbers are deterministically constructed. Hence, a fundamental question is whether known pseudorandom generators can be used to generate point sets that satisfy discrepancy bounds which imply polynomial tractability.

In this paper we consider point sets generated by a certain pseudorandom number generator as candidates for point sets that achieve tractability for certain problems. First attempts in this direction have been made in [4, 8] where so-called p-sets are used (see also the survey [7]). We consider another choice of pseudorandom numbers obtained from explicit inversive pseudorandom number generators. We show that such point sets can be used to get tractability for two problems: namely, the weighted star discrepancy problem (Section 3) and integration of functions from a subclass of the Wiener algebra that has some additional smoothness properties (Section 4).

In the subsequent section we introduce the proposed pseudorandom vectors and prove two estimates on character sums from which we can derive discrepancy- and worst-case error bounds.

2. Explicit inversive vectors

Let $\mathbb{F}_q$ be the finite field of order $q = p^k$ with a prime p and an integer $k \geq 1$. Further, let $\{\beta_1, \ldots, \beta_k\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$.

From a finite vector set

$$\{\boldsymbol{z}_n = (z_{n,1}, z_{n,2}, \ldots, z_{n,s}) \in \mathbb{F}_q^s : n = 0, 1, \ldots, N-1\}$$

in $\mathbb{F}_q^s$ we derive a point set in the s-dimensional unit cube in the following way: if

$$\boldsymbol{z}_n = \boldsymbol{c}_n^{(1)}\beta_1 + \boldsymbol{c}_n^{(2)}\beta_2 + \cdots + \boldsymbol{c}_n^{(k)}\beta_k \tag{1}$$

with all $\boldsymbol{c}_n^{(j)} = (c_{n,1}^{(j)}, c_{n,2}^{(j)}, \ldots, c_{n,s}^{(j)}) \in \mathbb{F}_p^s$, then we define an s-dimensional *digital point set*

$$\mathcal{P}_s := \left\{ \boldsymbol{x}_n = \sum_{j=1}^{k} \boldsymbol{c}_n^{(j)} p^{-j} \in [0,1)^s : n = 0, 1, \ldots, N-1 \right\}. \tag{2}$$

The following point set is constructed by vectors where the projection on each component gives a sequence introduced in [19].

Definition 1 (Set of explicit inversive points of size q)**.** Put

$$\overline{z} = \begin{cases} z^{-1} & \text{if } z \in \mathbb{F}_q^*, \\ 0 & \text{if } z = 0. \end{cases}$$

For $1 \le s \le q$ we choose a subset $S \subseteq \mathbb{F}_q$ of cardinality s. We consider the vector set

$$\mathcal{S} = \{\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{q-1}\} = \{(\overline{u+v})_{v \in S} : u \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^s \tag{3}$$

of size q and derive $\mathcal{P}_s = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{q-1}\} \in [0,1)^s$ from $\mathcal{S}$ by (1) and (2). Note that here $N = |\mathcal{P}_s| = q$.

Our second point set was essentially introduced in [23] and is defined as follows.

Definition 2 (Set of explicit inversive points of period T)**.** Let $0 \ne \theta \in \mathbb{F}_q$ be an element of multiplicative order T (hence T is a divisor of $q-1$; i.e., $T|(q-1)$) and $S \subseteq \mathbb{F}_q$ be of cardinality $1 \le s \le q$. Then we define

$$\mathcal{S} := \{\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{T-1}\} = \{(\overline{\theta^n + v})_{v \in S} : n = 0, \ldots, T-1\} \subseteq \mathbb{F}_q^s \tag{4}$$

of size T and derive $\mathcal{P}_s = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{T-1}\} \in [0,1)^s$ from $\mathcal{S}$ by (1) and (2). We remark that in this case $N = |\mathcal{P}_s| = T$ and T divides $q-1$.

We introduce frequently used notation.

- For $s \in \mathbb{N}$ put $[s] := \{1, 2, \ldots, s\}$.
- For a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_s)$ and for a non-empty $\mathfrak{u} \subseteq [s]$, let $\boldsymbol{x}_{\mathfrak{u}}$ be the projection of $\boldsymbol{x}$ onto those components indexed by $\mathfrak{u}$; i.e., for $\mathfrak{u} = \{u_1, u_2, \ldots, u_w\}$ with $u_1 < u_2 < \cdots < u_w$ we have $\boldsymbol{x}_{\mathfrak{u}} = (x_{u_1}, x_{u_2}, \ldots, x_{u_w})$.
- ψ denotes the canonical additive character of $\mathbb{F}_q$ which is defined as $\psi(x) := \exp\left(\frac{2\pi \mathtt{i}}{p}\, \mathrm{Tr}(x)\right)$, where Tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\mathtt{i} = \sqrt{-1}$.
- For vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^s$ let $\boldsymbol{x} \cdot \boldsymbol{y} \in \mathbb{F}_q$ denote their standard inner product.

Now, we are ready to state the first character sum bound.

Lemma 3. *Let $\mathcal{S} = \{\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{q-1}\}$ be given by* (3) *and let $\emptyset \ne \mathfrak{u} \subseteq [s]$. Then we have*

$$\max_{\boldsymbol{w} \in \mathbb{F}_q^{|\mathfrak{u}|} \setminus \{\boldsymbol{0}\}} \left| \sum_{n=0}^{q-1} \psi(\boldsymbol{w} \cdot \boldsymbol{z}_{n,\mathfrak{u}}) \right| \le (2|\mathfrak{u}| - 2) q^{1/2} + |\mathfrak{u}| + 1,$$

where $\boldsymbol{z}_{n,\mathfrak{u}} \in \mathbb{F}_q^{|\mathfrak{u}|}$ is the projection of $\boldsymbol{z}_n$ onto the coordinates indexed by $\mathfrak{u}$.

Proof. Note that the sums to be estimated are of the form

$$\Sigma_q := \sum_{n=0}^{q-1} \psi(\boldsymbol{w} \cdot \boldsymbol{z}_{n,\mathfrak{u}}) = \sum_{u \in \mathbb{F}_q} \psi\left(\sum_{i=1}^{|\mathfrak{u}|} w_i \overline{u + v_i}\right)$$

for some $(w_1, \ldots, w_{|\mathfrak{u}|}) \in \mathbb{F}_q^{|\mathfrak{u}|} \setminus \{\mathbf{0}\}$ and $(v_1, \ldots, v_{|\mathfrak{u}|}) \in \mathbb{F}_q^{|\mathfrak{u}|}$ with pairwise distinct coordinates $v_i \neq v_j$ if $i \neq j$.

We proceed as in the proof of [19, Theorem 1]. We have

$$|\Sigma_q| \leq |\mathfrak{u}| + \left| \sum_{\substack{u \in \mathbb{F}_q \\ g(u) \neq 0}} \psi\left(\frac{f(u)}{g(u)}\right) \right|,$$

where

$$f(x) = \sum_{i=1}^{|\mathfrak{u}|} w_i \prod_{\substack{j=1 \\ j \neq i}}^{|\mathfrak{u}|} (x + v_j)$$

and

$$g(x) = \prod_{j=1}^{|\mathfrak{u}|} (x + v_j).$$

Since at least one of the w_i is non-zero and the v_i are distinct, we have $f(-v_i) = w_i \prod_{j \neq i}(v_j - v_i) \neq 0$ and f is not the zero polynomial. Since $\deg(f) < \deg(g)$, by [19, Lemma 2], the rational function $\frac{f(x)}{g(x)}$ is not of the form $A^p - A$ where A is a rational function with coefficients in the algebraic closure of $\mathbb{F}_q$. This quite technical condition is equivalent to the fact that the terms in Σ_q are not all equal.

Hence, we can apply a bound of Moreno and Moreno [17, Theorem 2] (see also [19, Lemma 1]) and the result follows. □

For the second point set, which was essentially studied in [3, 26], we also give an analogous character sum bound.

Lemma 4. *Let $\{\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{T-1}\}$ be given by (4) have size T and let $\emptyset \neq \mathfrak{u} \subseteq [s]$. Then we have*

$$\max_{\boldsymbol{w} \in \mathbb{F}_q^{|\mathfrak{u}|} \setminus \{\mathbf{0}\}} \left| \sum_{n=0}^{T-1} \psi(\boldsymbol{w} \cdot \boldsymbol{z}_{n,\mathfrak{u}}) \right| \leq 2|\mathfrak{u}| q^{1/2} + |\mathfrak{u}|,$$

where $\boldsymbol{z}_{n,\mathfrak{u}} \in \mathbb{F}_q^{|\mathfrak{u}|}$ is the projection of $\boldsymbol{z}_n$ onto the coordinates indexed by $\mathfrak{u}$.

Proof. The proof is analogous to the proof of [26, Theorem 1]. □

3. The weighted star discrepancy

The *local discrepancy* $\Delta_{\mathcal{P}_s}$ of an N point set $\mathcal{P}_s$ in $[0,1)^s$ is defined as

$$\Delta_{\mathcal{P}_s}(\boldsymbol{\alpha}) := \frac{|\mathcal{P}_s \cap [\mathbf{0}, \boldsymbol{\alpha})|}{N} - \mathrm{Volume}([\mathbf{0}, \boldsymbol{\alpha}))$$

for all $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in [0,1]^s$. The *star discrepancy* is then the L_∞-norm of the local discrepancy,

$$D_N^*(\mathcal{P}_s) := \|\Delta_{\mathcal{P}_s}\|_{L_\infty}.$$

We consider the weighted star discrepancy. The study of weighted discrepancy has been initiated by Sloan and Woźniakowski [24] in 1998 in order to overcome the curse of dimensionality. Their basic idea was to introduce a set of weights $\boldsymbol{\gamma} = \{\gamma_{\mathfrak{u}} \;:\; \emptyset \neq \mathfrak{u} \subseteq [s]\}$ consisting of non-negative real numbers $\gamma_{\mathfrak{u}}$. A simple choice of weights are so-called product weights $\gamma_{\mathfrak{u}} = \prod_{j\in\mathfrak{u}} \gamma_j$ for weights in $(\gamma_j)_{j\geq 1}$. In this case, the weight γ_j is associated with the variable x_j.

Definition 5 (Weighted star discrepancy)**.** For a given weight set $\boldsymbol{\gamma}$ and for a point set $\mathcal{P}_s$ in $[0,1]^s$ the *weighted star discrepancy* is defined as

$$D^*_{N,\boldsymbol{\gamma}}(\mathcal{P}_s) := \max_{\emptyset\neq\mathfrak{u}\subseteq[s]} \gamma_{\mathfrak{u}} \sup_{\boldsymbol{\alpha}\in[0,1]^s} |\Delta_{\mathcal{P}_s}((\boldsymbol{\alpha}_{\mathfrak{u}}, \mathbf{1}))|,$$

where for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in [0,1]^s$ and for $\mathfrak{u} \subseteq [s]$ we put $(\boldsymbol{\alpha}_{\mathfrak{u}}, \mathbf{1}) = (y_1, \ldots, y_s)$ with

$$y_j = \begin{cases} \alpha_j & \text{if } j \in \mathfrak{u}, \\ 1 & \text{if } j \notin \mathfrak{u}. \end{cases}$$

Remark 6. Let $\mathcal{F}_1$ be the space of functions $f : [0,1]^s \to \mathbb{R}$ with finite norm

$$\|f\|_{\mathcal{F}_1} := |f(\mathbf{1})| + \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} \frac{1}{\gamma_{\mathfrak{u}}} \int_{[0,1]^{|\mathfrak{u}|}} \left| \frac{\partial^{|\mathfrak{u}|} f}{\partial \boldsymbol{x}_{\mathfrak{u}}}(\boldsymbol{x}_{\mathfrak{u}}, \mathbf{1}) \right| \mathrm{d}\boldsymbol{x}_{\mathfrak{u}},$$

where $\mathbf{1} = (1, 1, \ldots, 1)$. Then it was shown in [24, p. 12] that the weighted star discrepancy of a point set $\mathcal{P}_s$ is an upper bound for the worst-case error of the QMC rule Q_N based on $\mathcal{P}_s$; i.e.,

$$e(Q_N, \mathcal{F}_1) \leq D^*_{N,\boldsymbol{\gamma}}(\mathcal{P}_s).$$

It is well known that there is a close connection between discrepancy and character sums. In discrepancy theory such relations are known under the name *"Erdős-Turán-Koksma inequalities"*. One particular instance of an Erdős-Turán-Koksma inequality is given in the following lemma which is perfectly suited for our applications. Before stating the result, we introduce the following auxiliary function. For $q = p^k$, we define

$$\mathcal{T}(q, s) := \begin{cases} \left(\frac{k}{2} + 1\right)^s & \text{if } p = 2, \\ \left(\frac{2}{\pi} \log p + \frac{7}{5}\right)^s k^s & \text{if } p > 2. \end{cases} \tag{5}$$

The result is the following:

Lemma 7. *For $q = p^k$ and $\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{N-1} \in \mathbb{F}_q^s$, let $\mathcal{P}_s = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ be the N point set defined by* (1) *and* (2)*. Then we have*

$$D^*_N(\mathcal{P}_s) \leq \frac{s}{q} + \frac{\mathcal{T}(q,s)}{N} \max_{\boldsymbol{w}\in\mathbb{F}_q^s\setminus\{\mathbf{0}\}} \left| \sum_{n=0}^{N-1} \psi(\boldsymbol{w} \cdot \boldsymbol{z}_n) \right|,$$

where $\mathcal{T}(q, s)$ is defined as in (5)*.*

Proof. For a non-zero $s \times k$ matrix $H = (h_{ij})$ with entries $h_{ij} \in (-p/2, p/2] \cap \mathbb{Z}$, we define the exponential sum

$$\Sigma_N(H) := \sum_{n=0}^{N-1} \exp\left(\frac{2\pi \mathtt{i}}{p} \sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} c_{n,i}^{(j)} \right),$$

where the $c_{n,i}^{(j)} \in \mathbb{F}_p$ are defined by (1) and where $\mathtt{i} = \sqrt{-1}$. By a general discrepancy bound taken from [18, Theorem 3.12 and Lemma 3.13] we get

$$D_N^*(\mathcal{P}_s) \leq \frac{s}{q} + \frac{\mathcal{T}(q,s)}{N} \max_{H \neq 0} |\Sigma_N(H)|,$$

where the maximum is extended over all non-zero matrices H with entries h_{ij} in the set $(-p/2, p/2] \cap \mathbb{Z}$.

Let $\{\delta_1, \ldots, \delta_k\}$ be the dual basis of the given ordered basis $\{\beta_1, \ldots, \beta_k\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$; i.e.,

$$\operatorname{Tr}(\delta_j \beta_i) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

where Tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. For any basis, there exists a dual basis and this basis is unique; see [16, p. 55] for a proof. Then we have

$$c_{n,i}^{(j)} = \operatorname{Tr}(\delta_j z_{n,i}) \quad \text{for } 1 \leq j \leq k,\ 1 \leq i \leq s, \text{ and } n \in \mathbb{N}_0,$$

where $\boldsymbol{z}_n = (z_{n,1}, \ldots, z_{n,s})$. Therefore,

$$\begin{aligned} \Sigma_N(H) &= \sum_{n=0}^{N-1} \exp\left(\frac{2\pi\mathtt{i}}{p} \sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} \operatorname{Tr}(\delta_j z_{n,i})\right) \\ &= \sum_{n=0}^{N-1} \exp\left(\frac{2\pi\mathtt{i}}{p} \operatorname{Tr}\left(\sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} \delta_j z_{n,i}\right)\right) \\ &= \sum_{n=0}^{N-1} \psi\left(\sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} \delta_j z_{n,i}\right). \end{aligned}$$

Put

$$\boldsymbol{w} = (w_1, \ldots, w_s) \in \mathbb{F}_q^s \text{ with } w_i = \sum_{j=1}^{k} h_{ij} \delta_j \text{ for } i = 1, \ldots, s.$$

Since H is not the zero matrix and $\{\delta_1, \ldots, \delta_k\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, it follows that $\boldsymbol{w}$ is not the zero vector. This fact finishes the proof. □

Now we extend the star discrepancy estimate from Lemma 7 to the setting of weighted star discrepancy:

Lemma 8. *For $\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{N-1} \in \mathbb{F}_q^s$ let $\mathcal{P}_s = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ be the N point set defined by* (1) *and* (2). *Then we have*

$$D_{N,\boldsymbol{\gamma}}^*(\mathcal{P}_s) \leq \max_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} \left(\frac{|\mathfrak{u}|}{q} + \frac{\mathcal{T}(q,|\mathfrak{u}|)}{N} \max_{\boldsymbol{w} \in \mathbb{F}_q^{|\mathfrak{u}|} \setminus \{\boldsymbol{0}\}} \left| \sum_{n=0}^{N-1} \psi(\boldsymbol{w} \cdot \boldsymbol{z}_{n,\mathfrak{u}}) \right| \right),$$

where $\boldsymbol{z}_{n,\mathfrak{u}} \in \mathbb{F}_q^{|\mathfrak{u}|}$ is the projection of $\boldsymbol{z}_n$ onto the coordinates indexed by $\mathfrak{u}$.

Proof. The result follows immediately from Lemma 7 together with the fact that

$$D_{N,\boldsymbol{\gamma}}^*(\mathcal{P}_s) \leq \max_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} D_N^*(\mathcal{P}_{\mathfrak{u}}),$$

where $\mathcal{P}_{\mathfrak{u}}$ consists of the points from $\mathcal{P}_s$ projected onto the components whose indices belong to $\mathfrak{u}$. □

The previous lemma gives us our first main result.

Theorem 9. *For the point set $\mathcal{P}_s$ defined as in Definition* 1 *the following bound holds:*

$$D^*_{q,\boldsymbol{\gamma}}(\mathcal{P}_s) \leq \max_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} |\mathfrak{u}| \left(\frac{1}{q} + \frac{3\mathcal{T}(q, |\mathfrak{u}|)}{q^{1/2}} \right).$$

For the point set $\mathcal{P}_s$ defined as in Definition 2 *the following bound holds:*

$$D^*_{T,\boldsymbol{\gamma}}(\mathcal{P}_s) \leq \max_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} |\mathfrak{u}| \left(\frac{1}{q} + \frac{3\mathcal{T}(q, |\mathfrak{u}|) q^{1/2}}{T} \right).$$

Proof. The result follows from Lemma 8 and Lemmas 3 and 4. □

We point out that the discrepancy estimate from Theorem 9 holds for every choice of positive weights. Also, it is important to remark that point sets defined in Definition 2 are more flexible in terms of size. It is easy to check that for any prime p and T not divisible by p, there exists $q = p^k$, such that T divides $q - 1$. This k is the multiplicative order of p modulo T. Since the multiplicative group of $\mathbb{F}_q$ is cyclic, there is an element $\theta \in \mathbb{F}_q$ of order T.

Tractability. For a recent overview of results concerning tractability properties of the weighted star discrepancy we refer to [7, 8].

Important Remark 10. Unfortunately, the proof of [8, Theorem 3.2 (ii)] (also [7, Theorem 7(2)]) is not correct and hence this part of the theorem must be discarded. All other parts of these papers are correct.

We now restrict ourselves to product weights and present a condition on the weights for polynomial tractability.

Theorem 11. *Let $\mathcal{P}_s$ be the point set from Definition* 1 *or Definition* 2*. Assume that for an ordered sequence of weights $(\gamma_j)_{j \geq 1}$ with $\gamma_1 \geq \gamma_2 \geq \cdots > 0$, there is a $0 < \delta < 1/2$ such that*

$$\limsup_{j \to \infty} j\gamma_j < \frac{\delta}{3}. \tag{6}$$

Then there is a constant $c_{\boldsymbol{\gamma},\delta} > 0$, which depends only on $\boldsymbol{\gamma} = \{\prod_{j \in \mathfrak{u}} \gamma_j \ : \ \emptyset \neq \mathfrak{u} \subseteq [s]\}$ and δ but not on s, such that for all $1 \leq s \leq q$ we have

$$D^*_{q,\boldsymbol{\gamma}}(\mathcal{P}_s) \leq c_{\boldsymbol{\gamma},\delta} \frac{q^{1/2+\delta}}{N},$$

where q is a prime power, and $N = q \geq s$ for the point set from Definition 1 *and $q \geq s$ and $N | (q-1)$, where N is independent of s, for the point set from Definition* 2*. If $\limsup_{j \to \infty} j\gamma_j = 0$, then the result holds for all $\delta > 0$.*

Proof. We show the result for $p > 2$ and when the weights satisfy (6) only. The other cases are proven in a similar way. From Theorem 9, the fact that $r \leq 2^r$ for $r \geq 1$, and using the ordering of $\boldsymbol{\gamma}$ we have

$$\begin{aligned} D^*_{q,\boldsymbol{\gamma}}(\mathcal{P}_s) &\leq C^{(1)} \frac{q^{1/2}}{N} \max_{r=1,\ldots,s} r \prod_{j=1}^{r} \left(\gamma_j k \left(\frac{2}{\pi} \log p + \frac{7}{5} \right) \right) \\ &\leq C^{(1)} \frac{q^{1/2}}{N} \max_{r=1,\ldots,s} \prod_{j=1}^{r} \left(2\gamma_j k \left(\frac{2}{\pi} \log p + \frac{7}{5} \right) \right), \end{aligned}$$

where $C^{(1)}$ is an absolute positive constant. Notice that $2k(\frac{2}{\pi}\log p+\frac{7}{5})$ can also be bounded by $c\log q$ for some $0<c<3$. Now, let ℓ be the largest integer such that $c\gamma_\ell \log q > 1$. Then we have

$$D^*_{q,\boldsymbol{\gamma}}(\mathcal{P}_s) \le C^{(1)} \frac{q^{1/2}}{N} \prod_{j=1}^{\ell} (c\gamma_j \log q).$$

The condition $\limsup_{j\to\infty} j\gamma_j < \delta/3$ implies that there is an $L>0$ such that $j\gamma_j < \delta/3$ for all $j \ge L$. Without loss of generality we may assume that $\ell \ge L$. (Otherwise, if $\ell < L$, consider a new weight sequence $\boldsymbol{\gamma}' = (\gamma_j')_{j\ge 1}$ with $\gamma_j' = \gamma_j$ for all $j \in \{1,\ldots,\ell\} \cup \{L, L+1,\ldots\}$ and $\gamma_j' = \gamma_\ell$ for $j\in\{\ell+1,\ldots,L-1\}$, and hence $\gamma_j \le \gamma_j'$ for all $j\ge 1$.)

For $r \in \mathbb{N}$ let

$$c_r := \prod_{j=1}^{r} (c\gamma_j \log q),$$

so we have

$$\frac{c_\ell}{c_{\ell-1}} = c\gamma_\ell \log q < \frac{c\delta}{3\ell}\log q.$$

By the definition of ℓ we have $c_{\ell-1} < c_\ell$, hence

$$1 < \frac{c\delta}{3\ell}\log q,$$

which implies $\ell < c\delta(\log q)/3$ or $\ell \le \lfloor c\delta(\log q)/3\rfloor$.

Therefore, there is a constant $C^{(2)}_{\boldsymbol{\gamma}} > 0$ such that

$$\begin{aligned}\prod_{j=1}^{\ell}(c\gamma_j \log q) &= \prod_{j=1}^{L-1}(c\gamma_j \log q)\prod_{j=L}^{\ell}(c\gamma_j \log q)\\ &\le C^{(2)}_{\boldsymbol{\gamma}} (c\log q)^{L-1} \prod_{j=L}^{\lfloor c\delta(\log q)/3\rfloor} \frac{c\delta \log q}{3j}.\end{aligned}$$

Let $x := c\delta(\log q)/3$. Then

$$\begin{aligned}\prod_{j=1}^{\ell}(c\gamma_j \log q) &\le C^{(2)}_{\boldsymbol{\gamma}} \left(\frac{c\log q}{x}\right)^{L-1} ((L-1)!)\ \frac{x^{\lfloor x\rfloor}}{\lfloor x\rfloor !}\\ &\le C^{(2)}_{\boldsymbol{\gamma}} \left(\frac{3}{\delta}\right)^{L-1} ((L-1)!)\ \mathrm{e}^{x}\\ &= C^{(3)}_{\boldsymbol{\gamma},\delta}\ q^{c\delta/3}\\ &< C^{(3)}_{\boldsymbol{\gamma},\delta}\ q^{\delta},\end{aligned}$$

where $C^{(3)}_{\boldsymbol{\gamma},\delta} = C^{(2)}_{\boldsymbol{\gamma}} \left(\frac{3}{\delta}\right)^{L-1}((L-1)!)$ (note that L only depends on $\boldsymbol{\gamma}$). This implies

$$D^*_{q,\boldsymbol{\gamma}}(\mathcal{P}_s) \le C^{(1)} 3 C^{(3)}_{\boldsymbol{\gamma},\delta} \frac{q^{1/2+\delta}}{N}$$

and finishes the proof. □

Remark 12. Note that $\sum_{j=1}^{\infty}\gamma_j < \infty$ and the monotonicity relation $\gamma_1 \geq \gamma_2 \geq \cdots > 0$ imply $\limsup_{j\to\infty} j\gamma_j = 0$. To see this let $\varepsilon > 0$. From $\sum_{j=1}^{\infty}\gamma_j < \infty$ it follows with the Cauchy condensation test that also $\sum_{k=0}^{\infty} 2^k\gamma_{2^k} < \infty$. In particular, $2^k\gamma_{2^k} \to 0$ for $k \to \infty$. This means that $\gamma_{2^k} \leq \varepsilon/2^{k+1}$ for k large enough. Thus, for large enough j with $2^k \leq j < 2^{k+1}$ we obtain

$$\gamma_j \leq \gamma_{2^k} \leq \frac{\varepsilon}{2^{k+1}} < \frac{\varepsilon}{j}.$$

In particular, for j large enough we have $j\gamma_j < \varepsilon$. This implies that

$$\limsup_{j\to\infty} j\gamma_j = 0.$$

Of course, the converse is not true in general (for example, $\gamma_j = 1/(j\log j)$).

Corollary 13. *With the notation and conditions as in Theorem* 11*, in particular, when* $\limsup_{j\to\infty} j\gamma_j < \delta/3$ *holds, the weighted star discrepancy (or, equivalently, integration in* $\mathcal{F}_1$*) is polynomially tractable.*

Proof. For $\varepsilon > 0$ let $M := \max\{\lceil (c_{\boldsymbol{\gamma},\delta}\varepsilon^{-1})^{2/(1-2\delta)}\rceil, s\}$. Let q be the smallest prime power that is greater than or equal to M. According to the Postulate of Bertrand we have $q < 2M$. Then we have $D^*_{q,\boldsymbol{\gamma}}(\mathcal{P}_s) \leq \varepsilon$ and hence the information complexity satisfies

$$N(\varepsilon, s) \leq q \leq 2M = 2\max\{\lceil (c_{\boldsymbol{\gamma},\delta}\varepsilon^{-1})^{2/(1-2\delta)}\rceil, s\}.$$

This means that we have polynomial tractability. □

For the proof of Corollary 13 it is enough to use the construction of Definition 1 with a prime q. However, from a practical point of view the construction of Definition 1 with any prime power q and the construction of Definition 2 provide more flexibility. In particular the case $q = 2^r$ can be efficiently implemented using (optimal) normal bases and the Itoh-Tsujii inversion algorithm; see [13] and [14, Chapter 3], respectively.

4. Integration of Hölder continuous, absolutely convergent Fourier series and cosine series

Absolutely convergent Fourier series. For $f \in L_2([0,1]^s)$ and $\boldsymbol{h} \in \mathbb{Z}^s$ we define the $\boldsymbol{h}$th Fourier coefficient of f as $\widehat{f}(\boldsymbol{h}) = \int_{[0,1]^s} f(\boldsymbol{x})\mathrm{e}^{-2\pi\mathrm{i}\boldsymbol{h}\cdot\boldsymbol{x}}\,\mathrm{d}\boldsymbol{x}$. Then we can associate with f its Fourier series

$$f(\boldsymbol{x}) \sim \sum_{\boldsymbol{h}\in\mathbb{Z}^s} \widehat{f}(\boldsymbol{h})\mathrm{e}^{2\pi\mathrm{i}\boldsymbol{h}\cdot\boldsymbol{x}}. \tag{7}$$

Let $\alpha \in (0,1]$ and $t \in [1,\infty]$. Similarly to [4], we consider the norm

$$\|f\|_{K_{\alpha,t}} = |f|_{H_{\alpha,t}} + \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} |\mathfrak{u}| \sum_{\boldsymbol{k}_{\mathfrak{u}}\in\mathbb{Z}_*^{|\mathfrak{u}|}} |\widehat{f}(\boldsymbol{k}_{\mathfrak{u}},\boldsymbol{0})|,$$

where $\mathbb{Z}_* = \mathbb{Z}\setminus\{0\}$ and where

$$|f|_{H_{\alpha,t}} = \sup_{\boldsymbol{x},\boldsymbol{h}:\boldsymbol{x}+\boldsymbol{h}\in[0,1]^s} \frac{|f(\boldsymbol{x}+\boldsymbol{h}) - f(\boldsymbol{x})|}{\|\boldsymbol{h}\|_t^{\alpha}},$$

is the Hölder semi-norm where $\|\cdot\|_t$ denotes the t-norm.

We define the following sub-class of the Wiener algebra:

$$K_{\alpha,t} := \{f \in L_2([0,1]^s) \ :\ f \text{ is one-periodic and } \|f\|_{K_{\alpha,t}} < \infty\}.$$

The choice of t will influence the dependence on the dimension of the worst-case error upper bound. As observed in [4], we remark that for any $f \in K_{\alpha,t}$ the Fourier series (7) of f converges to f at every point $\boldsymbol{x} \in [0,1]^s$. This follows directly from [25, Corollary 1.8, p. 249], using that f is continuous since it satisfies a Hölder condition; i.e., $|f|_{H_{\alpha,t}} < \infty$. More information on $K_{\alpha,t}$ can be found in [4].

Theorem 14. *Let $\mathcal{P}_s$ be the point set from Definition 1 with $k=1$, $N=q=p \geq s$ or the point set from Definition 2 with $k=1$, $q=p\geq s$, and $N|(p-1)$. Let Q_N be the QMC rule based on $\mathcal{P}_s$. Then, for $\alpha \in (0,1]$ and $t \in [1,\infty]$, we have*

$$e(Q_N, K_{\alpha,t}) \leq \max\left(\frac{3\sqrt{p}}{N}, \frac{s^{\alpha/t}}{N^\alpha}\right).$$

In particular, if $t=\infty$ and $N \geq s$, we can use the point set from Definition 1 to obtain

$$e(Q_N, K_{\alpha,\infty}) \leq \frac{3}{N^{\min(\alpha,1/2)}}.$$

Proof. For $f \in K_{\alpha,t}$ we have

$$\begin{aligned}
\left|\frac{1}{N}\sum_{n=0}^{N-1} f(\boldsymbol{x}_n) - \int_{[0,1]^s} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}\right| &= \left|\sum_{\boldsymbol{k}\in\mathbb{Z}^s\setminus\{\boldsymbol{0}\}} \widehat{f}(\boldsymbol{k}) \frac{1}{N}\sum_{n=0}^{N-1} \mathrm{e}^{2\pi\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{x}_n}\right| \\
\leq \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^s \\ N\nmid\boldsymbol{k}}} |\widehat{f}(\boldsymbol{k})| \frac{1}{N}\left|\sum_{n=0}^{N-1} \mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\boldsymbol{k}\cdot\boldsymbol{c}_n}\right| &+ \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^s\setminus\{\boldsymbol{0}\} \\ N|\boldsymbol{k}}} |\widehat{f}(\boldsymbol{k})| \\
= \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} \sum_{\substack{\boldsymbol{k}_\mathfrak{u}\in\mathbb{Z}_*^{|\mathfrak{u}|} \\ N\nmid\boldsymbol{k}_\mathfrak{u}}} |\widehat{f}((\boldsymbol{k}_\mathfrak{u},\boldsymbol{0}))| \frac{1}{N}\left|\sum_{n=0}^{N-1} \mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\boldsymbol{k}_\mathfrak{u}\cdot\boldsymbol{c}_{n,\mathfrak{u}}}\right| &+ \sum_{\boldsymbol{k}\in\mathbb{Z}^s\setminus\{\boldsymbol{0}\}} |\widehat{f}(N\boldsymbol{k})|,
\end{aligned}$$

where $N|\boldsymbol{k}$ if all coordinates of $\boldsymbol{k}$ are divisible by N and $N \nmid \boldsymbol{k}$ otherwise. Now we apply Lemma 3 for the point set from Definition 1 to the first sum and [4, Lemma 1] to the second sum and obtain

$$\begin{aligned}
&\left|\frac{1}{N}\sum_{n=0}^{N-1} f(\boldsymbol{x}_n) - \int_{[0,1]^s} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}\right| \\
&\quad\leq \frac{3\sqrt{p}}{N}\sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} |\mathfrak{u}| \sum_{\substack{\boldsymbol{k}_\mathfrak{u}\in\mathbb{Z}_*^{|\mathfrak{u}|} \\ N\nmid\boldsymbol{k}_\mathfrak{u}}} |\widehat{f}((\boldsymbol{k}_\mathfrak{u},\boldsymbol{0}))| + \frac{s^{\alpha/t}}{N^\alpha}|f|_{H_{\alpha,t}} \\
&\quad\leq \max\left(\frac{3\sqrt{p}}{N}, \frac{s^{\alpha/t}}{N^\alpha}\right)\|f\|_{K_{\alpha,t}}.
\end{aligned}$$

For the point set from Definition 2 we use Lemma 4 instead of Lemma 3 to obtain the same bound. The result follows. ∎

Corollary 15. *Integration in $K_{\alpha,t}$ is polynomially tractable.*

Proof. The proof is similar to the one of Corollary 13. ∎

Absolutely convergent cosine series. So far we required that the functions be periodic. Now we show how we can get rid of this assumption. Let us consider cosine series instead of classical Fourier series.

The cosine system $\{\cos(k\pi x) \ : \ k \in \mathbb{N}_0\}$ forms a complete orthogonal basis of $L_2([0,1])$. To get an ONB we need to normalize it. Hence we define

$$\sigma_k(x) := \begin{cases} 1 & \text{if } k = 0, \\ \sqrt{2}\cos(k\pi x) & \text{if } k \in \mathbb{N}; \end{cases}$$

then the system

$$\{\sigma_k(x) \ : \ k \in \mathbb{N}_0\}$$

forms an ONB of $L_2([0,1])$. For $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$ and $\boldsymbol{x} = (x_1, \ldots, x_s) \in [0,1]^s$ define

$$\sigma_{\boldsymbol{k}}(\boldsymbol{x}) := \prod_{j=1}^{s} \sigma_{k_j}(x_j).$$

The $\sigma_{\boldsymbol{k}}$ with $\boldsymbol{k} \in \mathbb{N}_0^s$ constitute an ONB of $L_2([0,1]^s)$.

With an L_2-function g, we associate the cosine series

$$g(\boldsymbol{x}) \sim \sum_{\boldsymbol{k} \in \mathbb{N}_0^s} \widetilde{g}(\boldsymbol{k}) \sigma_{\boldsymbol{k}}(\boldsymbol{x})$$

with cosine coefficients $\widetilde{g}(\boldsymbol{k}) = \int_{[0,1]^s} g(\boldsymbol{x}) \sigma_{\boldsymbol{k}}(\boldsymbol{x}) \,\mathrm{d}\boldsymbol{x}$.

In order to apply the results for Fourier series to cosine series, we need the tent transformation $\phi : [0,1] \to [0,1]$ given by

$$\phi(x) := 1 - |2x - 1|.$$

For vectors $\boldsymbol{x}$ the tent transformed point $\phi(\boldsymbol{x})$ is understood component wise. The tent transformation is a Lebesgue measure preserving map and we have

$$\int_{[0,1]^s} g(\boldsymbol{x}) \,\mathrm{d}\boldsymbol{x} = \int_{[0,1]^s} g(\phi(\boldsymbol{x})) \,\mathrm{d}\boldsymbol{x}.$$

Define the norm

$$\|g\|_{C_{\alpha,t}} := 2^{\alpha} |g|_{H_{\alpha,t}} + \sum_{\emptyset \neq u \subseteq [s]} |\mathfrak{u}| 2^{|\mathfrak{u}|/2} \sum_{\boldsymbol{k}_{\mathfrak{u}} \in \mathbb{N}^{|\mathfrak{u}|}} |\widetilde{g}((\boldsymbol{k}_{\mathfrak{u}}, \boldsymbol{0}))|$$

and let

$$C_{\alpha,t} := \{g \in L_2([0,1]^s) \ : \ \|g\|_{C_{\alpha,t}} < \infty\}.$$

For $g \in L_2([0,1]^s)$ we have that the function $f = g \circ \phi$ is one-periodic and

$$\|f\|_{K_{\alpha,t}} = \|g\|_{C_{\alpha,t}}.$$

The cosine series of g converges pointwise and absolute to g for all points in $[0,1]^s$.

Now we consider integration of functions from $C_{\alpha,t}$:

For a point set $\mathcal{P}_s = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ let $\mathcal{Q} = \{\phi(\boldsymbol{x}_0), \ldots, \phi(\boldsymbol{x}_{N-1})\}$ be the tent transformed version of $\mathcal{P}_s$. Let Q_N be a QMC rule based on $\mathcal{P}_s$. Then we denote by Q_N^{ϕ} the QMC rule based on $\mathcal{Q}$.

As in [4, Proof of Theorem 2], we have that the worst-case errors in $K_{\alpha,t}$ and $C_{\alpha,t}$ coincide when we switch from a QMC rule to the tent transformed version of this rule, namely

$$e(Q_N, K_{\alpha,t}) = e(Q_N^{\phi}, C_{\alpha,t}).$$

With the help of this identity, we can transfer the results for periodic functions to not necessarily periodic ones.

Corollary 16. *Let $\mathcal{P}_s$ be the point set from Definition 1 with $k = 1$, $N = q = p \geq s$ or the point set from Definition 2 with $k = 1$, $q = p \geq s$, and $N|(p-1)$. Let Q_N^ϕ be the tent transformed version of the QMC rule based on $\mathcal{P}_s$. Then, for $\alpha \in (0,1]$ and $t \in [1,\infty]$, we have*

$$e(Q_N^\phi, C_{\alpha,t}) \leq \max\left(\frac{3\sqrt{p}}{N}, \frac{s^{\alpha/t}}{N^\alpha}\right).$$

In particular, if $t = \infty$ and $N \geq s$, we can use the point set from Definition 1 to obtain

$$e(Q_N^\phi, C_{\alpha,\infty}) \leq \frac{3}{N^{\min(\alpha,1/2)}}.$$

Corollary 17. *Integration in $C_{\alpha,t}$ is polynomially tractable.*

Acknowledgment

The authors would like to thank the two referees for their valuable comments that helped to improve the presentation of this paper.

References

[1] Christoph Aistleitner, *Covering numbers, dyadic chaining and discrepancy*, J. Complexity **27** (2011), no. 6, 531–540, DOI 10.1016/j.jco.2011.03.001. MR2846704

[2] Christoph Aistleitner and Markus Hofer, *Probabilistic discrepancy bound for Monte Carlo point sets*, Math. Comp. **83** (2014), no. 287, 1373–1381, DOI 10.1090/S0025-5718-2013-02773-1. MR3167462

[3] Zhixiong Chen, *Finite binary sequences constructed by explicit inversive methods*, Finite Fields Appl. **14** (2008), no. 3, 579–592, DOI 10.1016/j.ffa.2007.08.002. MR2435049

[4] Josef Dick, *Numerical integration of Hölder continuous, absolutely convergent Fourier, Fourier cosine, and Walsh series*, J. Approx. Theory **183** (2014), 14–30, DOI 10.1016/j.jat.2014.03.015. MR3209579

[5] Josef Dick, Frances Y. Kuo, and Ian H. Sloan, *High-dimensional integration: the quasi-Monte Carlo way*, Acta Numer. **22** (2013), 133–288. MR3038697

[6] Josef Dick and Friedrich Pillichshammer, *Digital nets and sequences*, Cambridge University Press, Cambridge, 2010. Discrepancy theory and quasi-Monte Carlo integration. MR2683394

[7] Josef Dick and Friedrich Pillichshammer, *The inverse of the star-discrepancy problem and the generation of pseudo-random numbers*, Sequences and their applications—SETA 2014, Lecture Notes in Comput. Sci., vol. 8865, Springer, Cham, 2014, pp. 173–184, DOI 10.1007/978-3-319-12325-7_15. MR3297330

[8] Josef Dick and Friedrich Pillichshammer, *The weighted star discrepancy of Korobov's p-sets*, Proc. Amer. Math. Soc. **143** (2015), no. 12, 5043–5057, DOI 10.1090/proc/12636. MR3411125

[9] A. Hinrichs, E. Novak, M. Ullrich, and H. Woźniakowski, *The curse of dimensionality for numerical integration of smooth functions*, Math. Comp. **83** (2014), no. 290, 2853–2863, DOI 10.1090/S0025-5718-2014-02855-X. MR3246812

[10] Aicke Hinrichs, Erich Novak, Mario Ullrich, and Henryk Woźniakowski, *The curse of dimensionality for numerical integration of smooth functions II*, J. Complexity **30** (2014), no. 2, 117–143, DOI 10.1016/j.jco.2013.10.007. MR3166524

[11] Aicke Hinrichs, Erich Novak, and Henryk Woźniakowski, *The curse of dimensionality for the class of monotone functions and for the class of convex functions*, J. Approx. Theory **163** (2011), no. 8, 955–965, DOI 10.1016/j.jat.2011.02.009. MR2832759

[12] Stefan Heinrich, Erich Novak, Grzegorz W. Wasilkowski, and Henryk Woźniakowski, *The inverse of the star-discrepancy depends linearly on the dimension*, Acta Arith. **96** (2001), no. 3, 279–302, DOI 10.4064/aa96-3-7. MR1814282

[13] Toshiya Itoh and Shigeo Tsujii, *A fast algorithm for computing multiplicative inverses in* GF(2^m) *using normal bases*, Inform. and Comput. **78** (1988), no. 3, 171–177, DOI 10.1016/0890-5401(88)90024-7. MR959807

[14] Dieter Jungnickel, *Finite fields*, Bibliographisches Institut, Mannheim, 1993. Structure and arithmetics. MR1238714

[15] Gunther Leobacher and Friedrich Pillichshammer, *Introduction to quasi-Monte Carlo integration and applications*, Compact Textbook in Mathematics, Birkhäuser/Springer, Cham, 2014. MR3289176

[16] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, 1st ed., Cambridge University Press, Cambridge, 1994. MR1294139

[17] Carlos J. Moreno and Oscar Moreno, *Exponential sums and Goppa codes. I*, Proc. Amer. Math. Soc. **111** (1991), no. 2, 523–531, DOI 10.2307/2048345. MR1028291

[18] Harald Niederreiter, *Random number generation and quasi-Monte Carlo methods*, CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 63, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992. MR1172997

[19] Harald Niederreiter and Arne Winterhof, *Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators*, Acta Arith. **93** (2000), no. 4, 387–399. MR1759483

[20] Erich Novak and Henryk Woźniakowski, *Tractability of multivariate problems. Vol. 1: Linear information*, EMS Tracts in Mathematics, vol. 6, European Mathematical Society (EMS), Zürich, 2008. MR2455266

[21] Erich Novak and Henryk Woźniakowski, *Tractability of multivariate problems. Volume II: Standard information for functionals*, EMS Tracts in Mathematics, vol. 12, European Mathematical Society (EMS), Zürich, 2010. MR2676032

[22] Erich Novak and Henryk Woźniakowski, *Tractability of multivariate problems. Volume III: Standard information for operators*, EMS Tracts in Mathematics, vol. 18, European Mathematical Society (EMS), Zürich, 2012. MR2987170

[23] Wilfried Meidl and Arne Winterhof, *On the linear complexity profile of some new explicit inversive pseudorandom numbers*, J. Complexity **20** (2004), no. 2-3, 350–355, DOI 10.1016/j.jco.2003.08.017. MR2067436

[24] Ian H. Sloan and Henryk Woźniakowski, *When are quasi-Monte Carlo algorithms efficient for high-dimensional integrals?*, J. Complexity **14** (1998), no. 1, 1–33, DOI 10.1006/jcom.1997.0463. MR1617765

[25] Elias M. Stein and Guido Weiss, *Introduction to Fourier analysis on Euclidean spaces*, Princeton University Press, Princeton, N.J., 1971. Princeton Mathematical Series, No. 32. MR0304972

[26] Arne Winterhof, *On the distribution of some new explicit inversive pseudorandom numbers and vectors*, Monte Carlo and quasi-Monte Carlo methods 2004, Springer, Berlin, 2006, pp. 487–499, DOI 10.1007/3-540-31186-6_30. MR2208727

School of Mathematics and Statistics, The University of New South Wales, Sydney NSW 2052, Australia
E-mail address: josef.dick@unsw.edu.au

Faculty of Sciences, University of Cantabria, E-39071 Santander, Spain
E-mail address: domingo.gomez@unican.es

Department for Financial Mathematics and Applied Number Theory, Johannes Kepler University Linz, Altenbergerstr. 69, 4040 Linz, Austria
E-mail address: friedrich.pillichshammer@jku.at

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria
E-mail address: arne.winterhof@oeaw.ac.at