Discrepancy of hyperplane nets and cyclic nets

Friedrich Pillichshammer and Gottlieb Pirsic [⋆]

Institut für Finanzmathematik, Universität Linz, Altenbergerstraße 69, A-4040 Linz, Austria. E-mail: `friedrich.pillichshammer@jku.at`, `gpirsic@gmail.com`

Summary. Digital nets are very important representatives in the family of low-discrepancy point sets which are often used as underlying nodes for quasi-Monte Carlo integration rules. Here we consider a special sub-class of digital nets known as cyclic nets and, more general, hyperplane nets. We show the existence of such digital nets of good quality with respect to star discrepancy in the classical as well as weighted case and we present effective search algorithms based on a component-by-component construction.

1 Introduction

For a finite point set $\mathcal{P}$ consisting of N (not necessarily distinct) points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ in the s-dimensional unit-cube $[0,1)^s$ the *star discrepancy* is defined by

$$D_N^*(\mathcal{P}) = \sup_B \left| \frac{|\{0 \le n < N \,:\, \boldsymbol{x}_n \in B\}|}{N} - \lambda_s(B) \right| \tag{1}$$

where the supremum is extended over all subintervals B of $[0,1)^s$ of the form $B = \prod_{i=1}^s [0, b_i)$, $0 < b_i \le 1$ for all $1 \le i \le s$. This is a quantitative measure for the deviation of the empirical distribution of $\mathcal{P}$ from uniform distribution modulo one. The star discrepancy is also intimately connected with the error of a quasi-Monte Carlo (QMC) rule via the well-known Koksma-Hlawka inequality

$$\left| \int_{[0,1]^s} f(\boldsymbol{x}) \,\mathrm{d}\boldsymbol{x} - \frac{1}{N} \sum_{\boldsymbol{x} \in \mathcal{P}} f(\boldsymbol{x}) \right| \le D_N^*(\mathcal{P}) V(f), \tag{2}$$

where $V(f)$ denotes the variation of f in the sense of Hardy and Krause and $\mathcal{P}$ consists of N points in $[0,1)^s$. See [4, 8, 11] for further informations.

[⋆] The authors are supported by the Austrian Science Foundation (FWF), Project S9609, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

Apart from the above (classical) concept one often studies a "weighted version" of the star discrepancy. This concept has been introduced by Sloan and Woźniakowski [19] with the idea that different coordinates of integrands may have different influence on the quality of approximation of an integral by a QMC rule.

Let $\mathcal{D} = \{1, \ldots, s\}$ be the set of coordinate indices and let $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ denote a sequence of non-negative real numbers, the so-called "weights" associated to the coordinate directions $i = 1, 2, \ldots$. To avoid a trivial case, we will always assume that not all weights are 0. For $\emptyset \neq \mathfrak{u} \subseteq \mathcal{D}$ let $\gamma_{\mathfrak{u}} = \prod_{i \in \mathfrak{u}} \gamma_i$ be the weight associated to the coordinate directions given by $\mathfrak{u}$, let $|\mathfrak{u}|$ the cardinality of $\mathfrak{u}$, and for a vector $\boldsymbol{z} \in [0,1]^s$ or a subset $B \subseteq [0,1]^s$ let $\boldsymbol{z}(\mathfrak{u})$ or $B(\mathfrak{u})$ denote the projection of the vector or the subset to the components given by $\mathfrak{u}$. Hence $\boldsymbol{z}(\mathfrak{u}) \in [0,1]^{|\mathfrak{u}|}$ and $B(\mathfrak{u}) \subseteq [0,1]^{|\mathfrak{u}|}$.

For a point set $\mathcal{P}$ of N points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ in $[0,1)^s$ and given weights $\boldsymbol{\gamma}$, the *weighted star discrepancy* is defined by

$$D^*_{N,\boldsymbol{\gamma}}(\mathcal{P}) = \sup_{B} \max_{\emptyset \neq \mathfrak{u} \subseteq \mathcal{D}} \gamma_{\mathfrak{u}} \left| \frac{|\{0 \leq n < N \,:\, \boldsymbol{x}_n(\mathfrak{u}) \in B(\mathfrak{u})\}|}{N} - \lambda_{|\mathfrak{u}|}(B(\mathfrak{u})) \right|,$$

where the supremum is extended over all subintervals B of $[0,1)^s$ of the form $B = \prod_{i=1}^{s} [0, b_i)$, $0 < b_i \leq 1$ for all $1 \leq i \leq s$.

This is a generalization of the classical star discrepancy (1) which is recovered if we choose $\gamma_i = 1$ for all $i \geq 1$. Furthermore, the error bound (2) can also be generalized by replacing the star discrepancy with the weighted star discrepancy and the variation by a weighted version of the variation (see [19] for more details).

The best constructions of finite point sets with low star discrepancy are based on the concept of (t,m,s)-nets in base q. A detailed theory of (t,m,s)-nets was developed by Niederreiter [10] (see also [11, Chapter 4] and [14] for surveys of this theory). We refer to [11] and [14] for the definition of (t,m,s)-nets. The crucial fact is that (t,m,s)-nets in a base q provide sets of q^m points in the s-dimensional unit cube $[0,1)^s$ which are extremely well distributed if the quality parameter t is "small". Explicit constructions of (t,m,s)-nets are based on the digital construction scheme which we recall in the following.

From now on let q denote a prime-power, let $\mathbb{F}_q$ be the finite field of q elements and let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$, where 0 is the neutral element with respect to addition. For a positive integer r let $\mathbb{Z}_r = \{0, \ldots, r-1\}$. Let $\varphi : \mathbb{Z}_q \to \mathbb{F}_q$ be a fixed bijection with $\varphi(0) = 0$. We extend φ to integers in $\mathbb{Z}_{q^m}$ by setting

$$\varphi(k) := (\varphi(\kappa_0), \ldots, \varphi(\kappa_{m-1}))^\top \tag{3}$$

for $k = \kappa_0 + \kappa_1 q + \cdots + \kappa_{m-1} q^{m-1}$ with $\kappa_0, \ldots, \kappa_{m-1} \in \mathbb{Z}_q$. Here $\boldsymbol{x}^\top$ means the transpose of the vector $\boldsymbol{x}$.

Definition 1 (digital (t,m,s)-nets). Let $s \geq 1$ and $m \geq 1$ be integers. Let $C_1, \ldots, C_s$ be $m \times m$ matrices over $\mathbb{F}_q$. Now we construct q^m points in $[0,1)^s$: For $1 \leq i \leq s$ and for $k \in \mathbb{Z}_{q^m}$ multiply the matrix C_i by the vector $\varphi(k)$, i.e.,

$$C_i\varphi(k) =: (y_{i,1}(k), \ldots, y_{i,m}(k))^\top \in \mathbb{F}_q^m,$$

and set

$$x_{k,i} := \frac{\varphi^{-1}(y_{i,1}(k))}{q} + \cdots + \frac{\varphi^{-1}(y_{i,m}(k))}{q^m}.$$

If for some integer t with $0 \le t \le m$ the point set consisting of the points

$$\boldsymbol{x}_k = (x_{k,1}, \ldots, x_{k,s}) \quad \text{for} \quad k \in \mathbb{Z}_{q^m},$$

is a (t, m, s)-net in base q, then it is called a *digital (t, m, s)-net over* $\mathbb{F}_q$, or, in brief, a *digital net (over $\mathbb{F}_q$).* The C_i are called its *generating matrices.*

Many constructions of digital nets are inspired by a close connection between coding theory and the theory of digital nets (see, for example, Niederreiter [13] or [15]). The construction considered here has been introduced by Niederreiter [13] and it is an analogue to a special type of codes, namely to cyclic codes which are well known in coding theory. Later this construction has been generalized by Pirsic, Dick and Pillichshammer [18] to so-called hyperplane nets.

Definition 2 (hyperplane nets). Let integers $m \ge 1, s \ge 2$ and a prime-power q be given. Let $\mathbb{F}_{q^m}$ be a finite field with q^m elements and fix an element $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{F}_{q^m}^s$. Let $\mathcal{F}$ be the space of linear forms

$$\mathcal{F} := \{f(x_1, \ldots, x_s) = x_1\gamma_1 + \cdots + x_s\gamma_s \,:\, \gamma_1, \ldots, \gamma_s \in \mathbb{F}_{q^m}\} \subseteq \mathbb{F}_{q^m}[x_1, \ldots, x_s]$$

and consider the subset

$$\mathcal{F}_{\boldsymbol{\alpha}} := \{f \in \mathcal{F} \,:\, f(\alpha_1, \ldots, \alpha_s) = 0\}.$$

For each $1 \le i \le s$ choose an ordered basis $\mathcal{B}_i$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and define the mapping $\phi : \mathcal{F} \to \mathbb{F}_q^{ms}$ by

$$f = \sum_{i=1}^{s} \gamma_i x^{i-1} \in \mathcal{F} \mapsto (\gamma_{1,1}, \ldots, \gamma_{1,m}, \ldots, \gamma_{s,1}, \ldots, \gamma_{s,m}) \in \mathbb{F}_q^{ms},$$

where $(\gamma_{i,1}, \ldots, \gamma_{i,m})$ is the coordinate vector of γ_i with respect to the chosen basis $\mathcal{B}_i$.

We denote by $\mathcal{C}_\alpha$ the orthogonal subspace in $\mathbb{F}_q^{ms}$ of the image $\mathcal{N}_\alpha := \phi(\mathcal{P}_\alpha)$. Let

$$C_\alpha = (C_1^\top \cdots C_s^\top) \in \mathbb{F}_q^{m \times sm}$$

be a matrix whose row space is $\mathcal{C}_\alpha$. Then $C_1, \ldots, C_s$ are the generating matrices of a *hyperplane net over* $\mathbb{F}_q$ *with respect to* $\mathcal{B}_1, \ldots, \mathcal{B}_s$ and C_α is its overall generating matrix. This hyperplane net will be denoted by $\mathcal{P}_{\boldsymbol{\alpha}}$ and we say $\mathcal{P}_{\boldsymbol{\alpha}}$ is the hyperplane net associated to $\boldsymbol{\alpha}$. We shall from now on assume a fixed choice of bases $\mathcal{B}_1, \ldots, \mathcal{B}_s$ and will therefore not explicitly mention them anymore.

Remark 1. In Definition 2 above, if $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ is of the special form $\boldsymbol{\alpha} = \alpha^{(s)} := (1, \alpha, \alpha^2, \ldots, \alpha^{s-1})$ with some $\alpha \in \mathbb{F}_{q^m}$, then we obtain a *cyclic digital net* as introduced initially by Niederreiter [13]. This cyclic net will be denoted by $\mathcal{P}_{\alpha^{(s)}}$ and we say $\mathcal{P}_{\alpha^{(s)}}$ is the cyclic net associated to α.

For a concise representation of the generator matrices $C_1, \ldots, C_s$ of a hyperplane net in terms of $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ we refer to [18]. We remark here that polynomial lattice point sets can be considered as a (proper) sub-class of hyperplane nets. This has been shown in [17].

In this paper we investigate the (weighted) star discrepancy of hyperplane nets. We show by an average argument that there exist hyperplane nets and even cyclic nets with “low” (weighted) star discrepancy. Furthermore, such point sets can be constructed with a component-by-component algorithm. For the weighted star discrepancy, under certain conditions on the weights, it turns out that our discrepancy bounds do not depend on the dimension s. Such a behavior is known as strong tractability (see [19]). We remark here that similar results are already known for polynomial lattice point sets but only in *prime* bases q (see [1, 2]). However, we point out that our results are valid for the much more general class of hyperplane nets. Beside this, here we consider arbitrary prime-power bases q instead of prime base only as done so far ([1, 2, 3]). For cyclic nets we further show that they can be extended in the dimension s.

2 Prerequisites

Let $q = p^r$, p prime, $r \in \mathbb{N}_0$ and let $\mathbb{F}_q$ be the finite field with q elements. Let $\mathbb{Z}_q = \{0, 1, \ldots, q-1\} \subseteq \mathbb{Z}$ with ring operations modulo q and let $\varphi : \mathbb{Z}_q \to \mathbb{F}_q$ be a bijection such that $\varphi(0) = 0$, the neutral element of addition in $\mathbb{F}_q$. Moreover denote by ψ_1 the isomorphism of additive groups $\psi_1 : \mathbb{F}_q \to \mathbb{Z}_p^r$ and define $\eta := \psi_1 \circ \varphi$. For $1 \le i \le r$ denote by π_i the projection $\pi_i : \mathbb{Z}_p^r \to \mathbb{Z}_p$, $\pi_i(x_1, \ldots, x_r) = x_i$.

Let $\mathbb{F}_{q^m} = \mathbb{F}_q[\omega]$, such that $\{1, \omega, \ldots, \omega^{m-1}\}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. If we have the representation of $\alpha \in \mathbb{F}_{q^m}$ as $\alpha = \sum_{l=0}^{m-1} a_l \omega^l$, where $a_0, \ldots, a_{m-1} \in \mathbb{F}_q$, define

$$\psi(\alpha) := (a_0, \ldots, a_{m-1}) \in \mathbb{F}_q^m.$$

Furthermore, for $k = \sum_{l=0}^{m-1} \kappa_l q^l \in \mathbb{Z}_{q^m}$ let

$$\varphi'(k) := \sum_{l=0}^{m-1} \varphi(\kappa_l)\omega^l \quad \text{and} \quad \psi'(k) := \psi(\varphi'(k)).$$

We have the following commutative diagrams:

$$\begin{tikzcd}
\mathbb{Z}_q \arrow[r, "\varphi"] \arrow[dr, "\eta"'] & \mathbb{F}_q \arrow[d, "\psi_1"] & \\
& \mathbb{Z}_p^r \arrow[r, "\pi_i"] & \mathbb{Z}_p
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{Z}_{q^m} \arrow[r, "\varphi'"] \arrow[dr, "\psi'"'] & \mathbb{F}_{q^m} \arrow[d, "\psi"] \\
& \mathbb{F}_q^m
\end{tikzcd}$$

For $1 \leq i \leq s$ we define the permutations $\tau_i : \mathbb{Z}_{q^m} \to \mathbb{Z}_{q^m}$ by $\tau_i(k) = \psi'^{-1}(B_i\psi'(k))$, where $B_i = (\psi(b_{i,1}), \ldots, \psi(b_{i,m})))^{-1}$, and where the $b_{i,l}$ constitute the chosen basis $\mathcal{B}_i$.

Proposition 1. *Let $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$. For the star discrepancy of the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$ we have*

$$D_{q^m}^*(\mathcal{P}_{\boldsymbol{\alpha}}) \leq 1 - \left(1 - \frac{1}{q^m}\right)^s + 2R_q(\boldsymbol{\alpha}) \leq \frac{s}{q^m} + 2R_q(\boldsymbol{\alpha}), \tag{4}$$

where

$$R_q(\boldsymbol{\alpha}) = \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}_{q^m}^s \setminus \{\boldsymbol{0}\} \\ \sum_{j=1}^s \alpha_j \varphi'(\tau_j(k_j)) = 0}} r_q(\boldsymbol{k}),$$

where for $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{Z}_{q^m}^s$ we write $r_q(\boldsymbol{k}) = r_q(k_1) \cdots r_q(k_s)$ and for $k \in \mathbb{Z}_{q^m}$,

$$r_q(k) = \begin{cases} 1 & \text{if } k = 0, \\ \frac{C}{q^{r+1}} & \text{if } k = \kappa_0 + \kappa_1 q + \cdots + \kappa_r q^r,\ \kappa_r \neq 0. \end{cases}$$

Furthermore, $C := 1 + \max\limits_{1 \leq x < q} \max\limits_{1 \leq y < q} \left| \sum_{a=0}^{y-1} \prod_{i=1}^r \exp\left(2\pi \mathtt{i} \frac{(\pi_i \circ \eta)(x)(\pi_i \circ \eta)(a)}{p}\right) \right|$. (Note that $C = C(q) \leq q$.)

Proof. This result follows from [5, Theorem 1] in combination with [18, Corollary 2.12]. □

For the weighted star discrepancy $D_{N,\boldsymbol{\gamma}}^*$ of a point set $\mathcal{P}$ of N points in $[0,1)^s$ we find from the definition (or see [3]) that

$$D_{N,\boldsymbol{\gamma}}^*(\mathcal{P}) \leq \sum_{\emptyset \neq \mathfrak{u} \subseteq \mathcal{D}} \gamma_{\mathfrak{u}} D_N^*(\mathcal{P}(\mathfrak{u})),$$

where $\mathcal{P}(\mathfrak{u})$ denotes the projection of the point set $\mathcal{P}$ to the coordinates given by $\mathfrak{u}$. If we consider the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$, then (4) yields

$$D_{q^m}^*(\mathcal{P}_{\boldsymbol{\alpha}}(\mathfrak{u})) \leq 1 - \left(1 - \frac{1}{q^m}\right)^{|\mathfrak{u}|} + 2R_q(\boldsymbol{\alpha}_{\mathfrak{u}})$$

for $\mathfrak{u} \neq \emptyset$, where $\boldsymbol{\alpha}_{\mathfrak{u}} = (\alpha_j)_{j \in \mathfrak{u}} \in \mathbb{F}_{q^m}^{|\mathfrak{u}|}$. Hence for the weighted star discrepancy of the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$, we get

$$D^*_{q^m,\boldsymbol{\gamma}}(\mathcal{P}_{\boldsymbol{\alpha}}) \le \mathit{\Gamma}_{s,q^m,\boldsymbol{\gamma}} + 2\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha}), \tag{5}$$

where

$$\mathit{\Gamma}_{s,q^m,\boldsymbol{\gamma}} := \sum_{\emptyset \ne \mathfrak{u} \subseteq \mathcal{D}} \gamma_{\mathfrak{u}} \left(1 - \left(1 - \frac{1}{q^m}\right)^{|\mathfrak{u}|}\right) \quad \text{and} \quad \widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha}) := \sum_{\emptyset \ne \mathfrak{u} \subseteq \mathcal{D}} \gamma_{\mathfrak{u}} R_q(\boldsymbol{\alpha}_u).$$

Remark 2. It was proven by Joe [7] that if the sequence of weights $(\gamma_i)_{i\ge1}$ satisfies $\sum_{i=1}^\infty \gamma_i < \infty$, then, with $\mathit{\Lambda} := \sum_{i=1}^\infty \frac{\gamma_i}{1+\gamma_i}$, we have

$$\mathit{\Gamma}_{s,q^m,\boldsymbol{\gamma}} \le \frac{\max(1,\mathit{\Lambda})\mathrm{e}^{\sum_{i=1}^\infty \gamma_i}}{q^m} \quad \text{for all } m,s \ge 1.$$

In the following proposition we obtain a formula for $\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha})$.

Proposition 2. *We have*

$$\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha}) = \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^s_{q^m}\setminus\{\boldsymbol{0}\} \\ \sum_{j=1}^s \alpha_j \varphi'(\tau_j(k_j))=0}} \widetilde{r}_q(\boldsymbol{k},\boldsymbol{\gamma}),$$

where for $\boldsymbol{k} = (k_1,\ldots,k_s) \in \mathbb{Z}^s_{q^m}$ *we write* $\widetilde{r}_q(\boldsymbol{k},\boldsymbol{\gamma}) = \widetilde{r}_q(k_1,\gamma_1)\cdots\widetilde{r}_q(k_s,\gamma_s)$ *and for* $k \in \mathbb{Z}_{q^m}$,

$$\widetilde{r}_q(k,\gamma) = \begin{cases} 1+\gamma & \text{if } k = 0, \\ \gamma r_q(k) & \text{if } k \ne 0. \end{cases}$$

Proof. The proof of this result is nearly the same as that of [2, Proposition 3.2]. □

Proposition 2 shows that R_q and $\widetilde{R}_{q,\boldsymbol{\gamma}}$ only differ by the definitions of r_q and $\widetilde{r}_q$. For this reason we will provide the proofs of the forthcoming results only for the unweighted case. The proofs for the weighted case apply accordingly. In the Appendix (Proposition 3) it is shown how for $\boldsymbol{\alpha} \in \mathbb{F}^s_{q^m}$ one can compute $R_q(\boldsymbol{\alpha})$ and $\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha})$ at a cost of $O(sq^m)$ operations.

3 The Results

First we determine the average value of $R_q(\boldsymbol{\alpha})$ resp. $\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha})$ over all possible $\boldsymbol{\alpha} \in (\mathbb{F}^*_{q^m})^s$. We denote $c_q := C\frac{q-1}{q} \le q-1$ where C is as in Proposition 1.

Theorem 1. *We have*

$$\frac{1}{|\mathbb{F}^*_{q^m}|^s} \sum_{\boldsymbol{\alpha}\in(\mathbb{F}^*_{q^m})^s} R_q(\boldsymbol{\alpha}) = \frac{1}{q^m-1}\left((1+mc_q)^s - 1 - smc_q\right)$$

and

$$\frac{1}{|\mathbb{F}^*_{q^m}|^s} \sum_{\boldsymbol{\alpha}\in(\mathbb{F}^*_{q^m})^s} \widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha}) = \frac{1}{q^m-1} \sum_{\substack{\mathfrak{u}\subseteq\mathcal{D} \\ |\mathfrak{u}|\ge2}} \prod_{i\in\mathfrak{u}} (\gamma_i m c_q) \prod_{i\notin\mathfrak{u}} (1+\gamma_i)\,.$$

Proof. First observe that $|\mathbb{F}_{q^m}^*| = q^m - 1$. We have

$$\begin{aligned}\frac{1}{|\mathbb{F}_{q^m}^*|^s} \sum_{\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s} R_q(\boldsymbol{\alpha}) &= \frac{1}{(q^m-1)^s} \sum_{\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s} \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}_{q^m}^s \setminus \{\boldsymbol{0}\} \\ \sum_{j=1}^s \alpha_j \varphi'(\tau_j(k_j))=0}} r_q(\boldsymbol{k}) \\ &= \frac{1}{(q^m-1)^s} \sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}^s \setminus \{\boldsymbol{0}\}} r_q(\boldsymbol{k}) \sum_{\substack{\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s \\ \sum_{j=1}^s \alpha_j \varphi'(\tau_j(k_j))=0}} 1,\end{aligned}$$

where we inserted for $R_q(\boldsymbol{\alpha})$ and changed the order of summation. Note that the τ_j's are permutations and that $\tau_j(k) = 0$ if and only if $k = 0$.

If $\boldsymbol{k} \in \mathbb{Z}_{q^m}^s \setminus \{\boldsymbol{0}\}$ is of the form $\boldsymbol{k} = (0, \ldots, 0, k_i, 0, \ldots, 0)$ with $k_i \neq 0$, then there is no $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ such that $\alpha_1 \varphi'(\tau_1(k_1)) + \cdots + \alpha_s \varphi'(\tau_s(k_s)) = \alpha_i \varphi'(\tau_i(k_i)) = 0$, since $\mathbb{F}_{q^m}$ is an integral domain. Otherwise, the number of $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ which satisfy $\alpha_1 \varphi'(\tau_1(k_1)) + \cdots + \alpha_s \varphi'(\tau_s(k_s)) = 0$ is exactly $(q^m - 1)^{s-1}$. Therefore we have (note that $r_q(0) = 1$)

$$\frac{1}{|\mathbb{F}_{q^m}^*|^s} \sum_{\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s} R_q(\boldsymbol{\alpha}) = \frac{1}{q^m-1} \left(\sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}^s \setminus \{\boldsymbol{0}\}} r_q(\boldsymbol{k}) - \sum_{i=1}^s \sum_{k_i \in \mathbb{Z}_{q^m}^*} r_q(k_i) \right).$$

Now the result follows from

$$\sum_{k=0}^{q^m-1} r_q(k) = 1 + mc_q \tag{6}$$

which is easily verified. □

The following consequence of Theorem 1 gives an improvement of [16, Corollary 2].

Corollary 1. *Let $0 \leq \varepsilon < 1$. Then there are more than $\varepsilon |\mathbb{F}_{q^m}^*|^s$ vectors $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ such that*

$$D_{q^m}^*(\mathcal{P}_{\boldsymbol{\alpha}}) \leq \frac{s}{q^m} + \frac{2}{(1-\varepsilon)(q^m-1)} (1 + mc_q)^s$$

resp.

$$D_{\boldsymbol{\gamma}, q^m}^*(\mathcal{P}_{\boldsymbol{\alpha}}) \leq \Gamma_{s,q^m,\boldsymbol{\gamma}} + \frac{2}{(1-\varepsilon)(q^m-1)} \prod_{i=1}^s (1 + \gamma_i (1 + mc_q)).$$

Proof. Let $\delta > 0$, then we obtain from Theorem 1,

$$\begin{aligned}&\frac{1}{q^m-1} (1 + mc_q)^s \geq \frac{1}{|\mathbb{F}_{q^m}^*|^s} \sum_{\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s} R_q(\boldsymbol{\alpha}) \\ &> \frac{\delta}{q^m-1} (1 + mc_q)^s \frac{1}{|\mathbb{F}_{q^m}^*|^s} \left| \left\{ \boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s \,:\, R_q(\boldsymbol{\alpha}) > \frac{\delta}{q^m-1} (1 + mc_q)^s \right\} \right|.\end{aligned}$$

Hence

$$\left|\left\{\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s \ : \ R_q(\boldsymbol{\alpha}) \leq \frac{\delta}{q^m-1}\left(1+mc_q\right)^s\right\}\right| > |\mathbb{F}_{q^m}^*|^s\left(1-\frac{1}{\delta}\right),$$

and the result follows from Proposition 1 by substituting $\delta = (1-\varepsilon)^{-1}$. □

From the previous results it follows that there exists a sufficient large amount of vectors $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ which yield hyperplane nets of good quality with respect to (weighted) star discrepancy. As for polynomial lattices (see [1, 2]), such vectors can be found by computer search using a component-by-component construction. We state the algorithm for the star- and the weighted star discrepancy.

Algorithm 2 *Given a prime-power q, a sequence of ordered bases $(\mathcal{B}_i)_{i\geq 1}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ (and a sequence $\boldsymbol{\gamma} = (\gamma_i)_{i\geq 1}$ of weights).*

1. *Choose $\alpha_1 = 1$, the one element in $\mathbb{F}_{q^m}$.*
2. *For $d > 1$, assume we have already constructed $\alpha_1, \ldots, \alpha_{d-1}$. Then find $\alpha_d \in \mathbb{F}_{q^m}^*$ which minimizes $R_q(\alpha_1, \ldots, \alpha_{d-1}, \alpha_d)$ (or alternatively $\widetilde{R}_{q,\boldsymbol{\gamma}}(\alpha_1, \ldots, \alpha_{d-1}, \alpha_d)$ in the weighted case) as a function of α_d.*

The cost of the algorithm is of $O(s^2 q^{2m})$ operations. In the following theorem we show that Algorithm 2 is guaranteed to find a good vector $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$.

Theorem 3. *Let q be prime-power, $m \geq 1$ and $\boldsymbol{\gamma} = (\gamma_i)_{i\geq 1}$ be a sequence of weights. Suppose $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in (\mathbb{F}_{q^m}^*)^s$ is constructed according to Algorithm 2 using R_q (resp. $\widetilde{R}_{q,\boldsymbol{\gamma}}$). Then for all $d = 1, 2, \ldots, s$ we have*

$$D_{q^m}^*(\mathcal{P}_{\boldsymbol{\alpha}}) \leq \frac{s}{q^m} + \frac{2}{q^m-1}\left(1+mc_q\right)^s,$$

resp.

$$D_{q^m,\boldsymbol{\gamma}}^*(\mathcal{P}_{\boldsymbol{\alpha}}) \leq \mathit{\Gamma}_{s,q^m,\boldsymbol{\gamma}} + \frac{2}{q^m-1}\prod_{i=1}^{s}\left(1+\gamma_i\left(1+mc_q\right)\right).$$

Proof. By Proposition 1 it is enough to show that

$$R_q((\alpha_1, \ldots, \alpha_d)) \leq \frac{1}{q^m-1}\left(1+mc_q\right)^d \quad \text{for all} \quad d = 1, \ldots, s. \tag{7}$$

Since $\varphi'(\tau_1(k)) = 0$ if and only if $k = 0$ it follows that $R_q(1) = 0$ and (7) is true for $d = 1$. Suppose now that for some $1 \leq d < s$ we have already constructed $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in (\mathbb{F}_{q^m}^*)^d$ such that $R_q(\boldsymbol{\alpha}) \leq \frac{1}{q^m-1}\left(1+mc_q\right)^d$. Then we have

$$\begin{aligned}R_q((\boldsymbol{\alpha}, \alpha_{d+1})) &= \sum_{\substack{(\boldsymbol{k}, k_{d+1}) \in \mathbb{Z}_{q^m}^{d+1} \setminus \{\mathbf{0}\} \\ \sum_{j=1}^{d+1} \alpha_j \varphi'(\tau_j(k_j)) = 0}} \prod_{i=1}^{d+1} r_q(k_i) \\ &= \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}_{q^m}^d \setminus \{\mathbf{0}\} \\ \sum_{j=1}^{d} \alpha_j \varphi'(\tau_j(k_j)) = 0}} \prod_{i=1}^{d} r_q(k_i) + \theta(\alpha_{d+1}) = R_q(\boldsymbol{\alpha}) + \theta(\alpha_{d+1}),\end{aligned}$$

where

$$\theta(\alpha_{d+1}) = \sum_{k_{d+1} \in \mathbb{Z}_{q^m}^*} \left(r_q(k_{d+1}) \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}_{q^m}^d \\ \sum_{j=1}^{d} \alpha_j \varphi'(\tau_j(k_j)) = -\alpha_{d+1} \varphi'(\tau_{d+1}(k_{d+1}))}} \prod_{i=1}^{d} r_q(k_i) \right).$$

Since α_{d+1} is a minimizer of $R_q((\boldsymbol{\alpha}, \cdot))$ it follows that α_{d+1} is also a minimizer of $\theta(\cdot)$ and hence we obtain

$$\begin{aligned}\theta(\alpha_{d+1}) &\le \frac{1}{q^m - 1} \sum_{z \in \mathbb{F}_{q^m}^*} \theta(z) \\ &= \frac{1}{q^m - 1} \sum_{z \in \mathbb{F}_{q^m}^*} \sum_{k_{d+1} \in \mathbb{Z}_{q^m}^*} r_q(k_{d+1}) \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}_{q^m}^d \\ \sum_{j=1}^{d} \alpha_j \varphi'(\tau_j(k_j)) = -z \varphi'(\tau_{d+1}(k_{d+1}))}} \prod_{i=1}^{d} r_q(k_i) \\ &= \frac{1}{q^m - 1} \sum_{k_{d+1} \in \mathbb{Z}_{q^m}^*} r_q(k_{d+1}) \sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}^d} \prod_{i=1}^{d} r_q(k_i) \sum_{\substack{z \in \mathbb{F}_{q^m}^* \\ z \varphi'(\tau_{d+1}(k_{d+1})) = -\sum_{j=1}^{d} \alpha_j \varphi'(\tau_j(k_j))}} 1.\end{aligned}$$

The equation $z\varphi'(\tau_{d+1}(k_{d+1})) = -(\alpha_1\varphi'(\tau_1(k_1)) + \cdots + \alpha_d\varphi'(\tau_d(k_d)))$ has exactly one solution $z \in \mathbb{F}_{q^m}^*$ if $\alpha_1\varphi'(\tau_1(k_1)) + \cdots + \alpha_d\varphi'(\tau_d(k_d)) \neq 0$ and no solution if $\alpha_1\varphi'(\tau_1(k_1)) + \cdots + \alpha_d\varphi'(\tau_d(k_d)) = 0$. Therefore we obtain

$$\begin{aligned}\theta(\alpha_{d+1}) &\le \frac{1}{q^m - 1} \sum_{k_{d+1} \in \mathbb{Z}_{q^m}^*} r_q(k_{d+1}) \sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}^d} \prod_{i=1}^{d} r_q(k_i) \\ &= \frac{1}{q^m - 1} (1 + mc_q)^d \sum_{k_{d+1} \in \mathbb{Z}_{q^m}^*} r_q(k_{d+1}).\end{aligned}$$

Now we obtain

$$\begin{aligned}R_q((\boldsymbol{\alpha}, \alpha_{d+1})) &\le R_q(\boldsymbol{\alpha}) + \frac{1}{q^m - 1} (1 + mc_q)^d \sum_{k_{d+1} \in \mathbb{Z}_{q^m}^*} r_q(k_{d+1}) \\ &\le \frac{1}{q^m - 1} (1 + mc_q)^d \sum_{k_{d+1} \in \mathbb{Z}_{q^m}} r_q(k_{d+1}) = \frac{1}{q^m - 1} (1 + mc_q)^{d+1}\end{aligned}$$

where we have used Eq. (6). Now (7) follows by induction on d. □

The following result follows from Theorem 3 and can be proved in the same way as [3, Corollary 8].

Corollary 2. *Let q be a prime-power, $s \geq 2$, $m \geq 1$ and $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ be a sequence of weights. If $\sum_{i=1}^{\infty} \gamma_i < \infty$, then for any $\delta > 0$ there exists a $\widetilde{c}_{q,\boldsymbol{\gamma},\delta} > 0$, independent of s and m, such that the weighted star discrepancy of the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$ where $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ is constructed according to Algorithm 2 using $\widetilde{R}_{q,\boldsymbol{\gamma}}$ satisfies*

$$D_{q^m,\boldsymbol{\gamma}}^*(\mathcal{P}_{\boldsymbol{\alpha}}) \leq \frac{\widetilde{c}_{q,\boldsymbol{\gamma},\delta}}{q^{m(1-\delta)}}. \tag{8}$$

Let $N \in \mathbb{N}$ have q-adic expansion $N = \nu_1 q^{m_1} + \cdots + \nu_r q^{m_r}$ with digits $1 \leq \nu_i < q$ for $1 \leq i \leq r$. For each $1 \leq i \leq r$ construct a vector $\boldsymbol{\alpha}_i \in \mathbb{F}_{q^{m_i}}^s$ according to Algorithm 2 and let $\mathcal{P}_{N,s}$ be the superposition of ν_i copies of the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}_i}$ for all $1 \leq i \leq r$. Hence $\mathcal{P}_{N,s}$ contains N elements in $[0,1)^s$. We point out that for any N, s the point set $\mathcal{P}_{N,s}$ can be constructed explicitly. Using Corollary 2 and the same arguments as used in the proof of [6, Theorem 3] we obtain the following result.

Corollary 3. *Let $N, s \in \mathbb{N}$ and assume that $\sum_{i=1}^{\infty} \gamma_i < \infty$. Then for the weighted star discrepancy of the point set $\mathcal{P}_{N,s} \subseteq [0,1)^s$ of cardinality N constructed above, for any $\delta > 0$ we have*

$$D_{N,\boldsymbol{\gamma}}^*(\mathcal{P}_{N,s}) \leq \frac{C_{q,\delta,\boldsymbol{\gamma}}}{N^{1-\delta}},$$

where $C_{q,\delta,\boldsymbol{\gamma}} > 0$ is independent of s and N. Hence the weighted star discrepancy of $\mathcal{P}_{N,s}$ achieves a strongly tractability bound with ε-exponent equal to 1.

Obviously we can restrict the search space for $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ when we search for cyclic nets only. The subsequent theorem, which improves the second part of [16, Corollary 2], shows that there is a sufficient large amount of good α's in $\mathbb{F}_{q^m}$. The cost of a full search for the best $\alpha \in \mathbb{F}_{q^m}$ is of $O(sq^{2m})$ operations.

Theorem 4. *Let q be a prime-power, $s \geq 2$, $m \geq 1$ and $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ be a sequence of weights. For $0 \leq \varepsilon < 1$ there are more than $\varepsilon|\mathbb{F}_{q^m}^*|$ elements $\alpha \in \mathbb{F}_{q^m}^*$ such that*

$$D_{q^m}^*(\mathcal{P}_{\alpha^{(s)}}) \leq \frac{s}{q^m} + \frac{2(s-1)}{(1-\varepsilon)(q^m-1)}\left(1+mc_q\right)^s,$$

resp.

$$D_{q^m,\boldsymbol{\gamma}}^*(\mathcal{P}_{\alpha^{(s)}}) \leq \mathit{\Gamma}_{s,q^m,\boldsymbol{\gamma}} + \frac{2(s-1)}{(1-\varepsilon)(q^m-1)} \prod_{i=1}^{s} \left(1+\gamma_i\left(1+mc_q\right)\right).$$

Proof. We have

$$\begin{aligned}\frac{1}{q^m-1}\sum_{\alpha\in\mathbb{F}_{q^m}^*} R_q(\alpha^{(s)}) &= \frac{1}{q^m-1}\sum_{z\in\mathbb{F}_{q^m}^*}\ \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}_{q^m}^s\setminus\{\boldsymbol{0}\}\\ \sum_{j=1}^s z^{j-1}\varphi'(\tau_j(k_j))=0}}\ \prod_{i=1}^s r_q(k_i)\\ &= \frac{1}{q^m-1}\sum_{\boldsymbol{k}\in\mathbb{Z}_{q^m}^s\setminus\{\boldsymbol{0}\}}\ \prod_{i=1}^s r_q(k_i) \sum_{\substack{z\in\mathbb{F}_{q^m}^*\\ \sum_{j=1}^s z^{j-1}\varphi'(\tau_j(k_j))=0}} 1.\end{aligned}$$

As the polynomial $\sum_{j=1}^s z^{j-1}\varphi'(\tau_j(k_j))$ over the finite field $\mathbb{F}_{q^m}$ of degree at most $s-1$ has at most $s-1$ zeros $z\in\mathbb{F}_{q^m}^*$ we obtain

$$\frac{1}{q^m-1}\sum_{\alpha\in\mathbb{F}_{q^m}^*} R_q(\alpha^{(s)}) \le \frac{s-1}{q^m-1}\sum_{\boldsymbol{k}\in\mathbb{Z}_{q^m}^s}\prod_{i=1}^s r_q(k_i) = \frac{s-1}{q^m-1}(1+mc_q)^s. \quad (9)$$

For the rest of the proof one just has to follow the proof of Corollary 1. □

There even exists an α such that $\mathcal{P}_{\alpha^{(s)}}$ is of low star discrepancy for arbitrary dimensions $s\ge 1$. One says that $\mathcal{P}_{\alpha^{(s)}}$ is *extensible in the dimension s.* In the special case of polynomial lattices this was shown by Niederreiter [12, Theorem 9].

Corollary 4. *Let q be a prime-power, $m\ge 1$, $(\mathcal{B}_i)_{i\ge 1}$ a sequence of ordered bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $\boldsymbol{\gamma}=(\gamma_i)_{i\ge 1}$ be a sequence of weights. Then for $c>\sum_{s=1}^\infty \frac{1}{s(\log(s+1))^2}$ there exists an element $\alpha\in\mathbb{F}_{q^m}^*$ such that for all $s\ge 1$ we have*

$$D_{q^m}^*(\mathcal{P}_{\alpha^{(s)}}) \le \frac{s}{q^m} + \frac{2cs(s-1)(\log(s+1))^2}{q^m-1}(1+mc_q)^s$$

resp.

$$D_{q^m,\boldsymbol{\gamma}}^*(\mathcal{P}_{\alpha^{(s)}}) \le \mathit{\Gamma}_{s,q^m,\boldsymbol{\gamma}} + \frac{2cs(s-1)(\log(s+1))^2}{q^m-1}\prod_{i=1}^s\left(1+\gamma_i\left(1+mc_q\right)\right).$$

In fact, in both cases for arbitrary small $\varepsilon>0$ we can get at least $(1-\varepsilon)(q^m-1)$ such elements α by choosing $c>0$ large enough.

Proof. The proof uses arguments from [12]. Let

$$E_s := \left\{\alpha\in\mathbb{F}_{q^m}^*\ :\ R_q(\alpha^{(s)}) > \frac{cs(s-1)(\log(s+1))^2}{q^m-1}(1+mc_q)^s\right\}$$

where the constant $c>0$ is chosen such that $c>\sum_{s=1}^\infty\frac{1}{s(\log(s+1))^2}$. Using (9) we obtain for any $s\ge 1$,

$$(s-1)(1+mc_q)^s \geq \sum_{\alpha \in \mathbb{F}_{q^m}^*} R_q(\alpha^{(s)}) \geq |E_s| \frac{cs(s-1)(\log(s+1))^2}{q^m-1}(1+mc_q)^s$$

and hence $|E_s| \leq \frac{q^m-1}{cs(\log(s+1))^2}$. For $E := \bigcup_{s \geq 1} E_s$ we hence obtain

$$|E| \leq \sum_{s=1}^{\infty} |E_s| \leq \frac{q^m-1}{c} \sum_{s=1}^{\infty} \frac{1}{s(\log(s+1))^2} < q^m - 1 = |\mathbb{F}_{q^m}^*|.$$

Especially, there exists an element $\alpha \in \mathbb{F}_{q^m}^* \setminus E$ and for this element we have

$$R_q(\alpha^{(s)}) \leq \frac{cs(s-1)(\log(s+1))^2}{q^m-1}(1+mc_q)^s \quad \text{for all} \quad s \geq 1.$$

Now the result follows from Proposition 1. □

Appendix: Calculation of R_q and $\widetilde{R}_{q,\gamma}$

We will give an explicit form of the quantities R_q and $\widetilde{R}_{q,\gamma}$ which can be computed efficiently. For this computation we will employ Walsh function which we briefly recall in the following (notations are defined as in Section 2).

Definition 3 (Walsh functions). Let $q = p^r$ with a prime p and a positive integer r, let $k \in \mathbb{N}_0$ with base q representation $k = \kappa_0 + \kappa_1 q + \cdots + \kappa_{m-1} q^{m-1}$ where $\kappa_l \in \mathbb{Z}_q$ and let $x \in [0,1)$ with base q representation $x = x_1/q + x_2/q^2 + \cdots$. Then the k-th Walsh function over the finite field $\mathbb{F}_q$ with respect to the bijection φ is defined by

$${}_{\mathbb{F}_q,\varphi}\mathrm{wal}_k(x) := \prod_{l=0}^{m-1} \prod_{i=1}^{r} \exp\left(2\pi \mathtt{i} \frac{(\pi_i \circ \eta)(\kappa_l)(\pi_i \circ \eta)(x_l)}{p}\right).$$

For convenience we will in the rest of the paper omit the subscript and simply write wal_k if there is no ambiguity.

Multivariate Walsh functions are defined by multiplication of the univariate components, i.e., for $\boldsymbol{x} = (x_1, \ldots, x_s) \in [0,1)^s$, $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$ where $s > 1$, we set

$$\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}) = \prod_{j=1}^{s} \mathrm{wal}_{k_j}(x_j).$$

Specifically we will need the following lemma that gives an important indicator function.

Lemma 1. *Let $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ and let $\mathcal{P}_{\boldsymbol{\alpha}}$ be the hyperplane net associated to $\boldsymbol{\alpha}$. Then for any $\boldsymbol{k} \in \mathbb{Z}_{q^m}^s$ we have*

$$\frac{1}{q^m} \sum_{\boldsymbol{x} \in \mathcal{P}_{\alpha}} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}) = \begin{cases} 1 & \textit{if } \alpha_1 \varphi'(\tau_1(k_1)) + \cdots + \alpha_s \varphi'(\tau_s(k_s)) = 0, \\ 0 & \textit{else.} \end{cases}$$

For a proof of this result see [18, Corollary 2.12].

Proposition 3. *Let $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$ and let $\mathcal{P}_{\boldsymbol{\alpha}}$ be the associated hyperplane net. Then for the quantities $R_q(\boldsymbol{\alpha})$ and $\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha})$ we get the formulas*

$$R_q(\boldsymbol{\alpha}) = -1 + \frac{1}{q^m} \sum_{\boldsymbol{x} \in \mathcal{P}_{\boldsymbol{\alpha}}} \prod_{i=1}^{s} \left(1 + C\left(\frac{q-1}{q} m_0(x_i) - 1\right)\right),$$

$$\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha}) = -\prod_{i=1}^{s}(1+\gamma_i) + \frac{1}{q^m} \sum_{\boldsymbol{x} \in \mathcal{P}_{\boldsymbol{\alpha}}} \prod_{i=1}^{s} \left(1 + \gamma_i + \gamma_i C\left(\frac{q-1}{q} m_0(x_i) - 1\right)\right),$$

with C as in the definition of r_q in Proposition 1 and for $x \in q^{-m}\mathbb{Z}_{q^m} \setminus \{0\}$, $m_0(x) := \max\{l \le m : x < q^{-(l-1)}\} = \lceil -\log_q x \rceil$ and $m_0(0) := m + q/(q-1)$. Hence $R_q(\boldsymbol{\alpha})$ and $\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha})$ can be computed at a cost of $O(sq^m)$ operations.

Proof. We set $\lambda(\boldsymbol{k}) := \alpha_1 \varphi'(\tau_1(k_1)) + \cdots + \alpha_s \varphi'(\tau_s(k_s))$. By definition we have

$$1 + R_q(\boldsymbol{\alpha}) = \sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}^s, \lambda(\boldsymbol{k})=0} \prod_{i=1}^{s} r_q(k_i).$$

Using Lemma 1 we can let the sum range over all $\boldsymbol{k} \in \mathbb{Z}_{q^m}^s$. We get

$$\begin{aligned} 1 + R_q(\boldsymbol{\alpha}) &= \sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}} \frac{1}{q^m} \sum_{\boldsymbol{x} \in \mathcal{P}_{\alpha}} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}) \prod_{i=1}^{s} r_q(k_i) \\ &= \frac{1}{q^m} \sum_{\boldsymbol{x} \in \mathcal{P}_{\boldsymbol{\alpha}}} \sum_{\boldsymbol{k} \in \mathbb{Z}_{q^m}^s} \prod_{i=1}^{s} r_q(k_i) \mathrm{wal}_{k_i}(x_i) \\ &= \frac{1}{q^m} \sum_{\boldsymbol{x} \in \mathcal{P}_{\boldsymbol{\alpha}}} \prod_{i=1}^{s} \left(1 + \sum_{k \in \mathbb{Z}_{q^m} \setminus \{0\}} r_q(k) \mathrm{wal}_k(x_i)\right). \end{aligned} \tag{10}$$

Since $r_q(k)$ depends only on the "digit length" of k we get for $x \in [0,1)$, by [9, Lemma 4] (note that it is enough to consider $x \in q^{-m}\mathbb{Z}_{q^m}$ only)

$$\begin{aligned} \sum_{k \in \mathbb{Z}_{q^m} \setminus \{0\}} r_q(k) \mathrm{wal}_k(x) &= \sum_{l=1}^{m} \frac{C}{q^l} \sum_{k=q^{l-1}}^{q^l - 1} \mathrm{wal}_k(x) \\ &= \sum_{l=1}^{m} \frac{C}{q^l} q^{l-1} \times \begin{cases} q-1 & \text{if } x < q^{-l}, \\ -1 & \text{if } q^{-l} \le x < q^{-(l-1)}, \\ 0 & \text{else}, \end{cases} \\ &= \frac{C}{q}\Big((q-1)\big(m_0(x) - 1\big) - 1\Big), \end{aligned}$$

where for $x \in q^{-m}\mathbb{Z}_{q^m}$ the quantity $m_0(x)$ is defined in Proposition 3. Inserting the formula into (10) gives the claimed result for $R_q(\boldsymbol{\alpha})$.

The derivation of the weighted case from the unweighted one can be carried out as in [2]. □

References

1. Dick, J., Kritzer, P., Leobacher, G. and Pillichshammer, F.: Constructions of general polynomial lattice rules based on the weighted star discrepancy. Finite Fields Appl. **13**: 1045–1070, 2007.
2. Dick, J., Leobacher, G. and Pillichshammer, F.: Construction algorithms for digital nets with low weighted star discrepancy. SIAM J. Numer. Anal. **43**: 76–95, 2005.
3. Dick, J., Niederreiter, H. and Pillichshammer, F.: Weighted star discrepancy of digital nets in prime bases. In *Monte Carlo and quasi-Monte Carlo methods 2004*, pages 77–96. Springer, Berlin, 2006.
4. Drmota, M. and Tichy, R.F.: *Sequences, Discrepancies and Applications.* Lecture Notes in Mathematics 1651, Springer, Berlin, 1997.
5. Grozdanov, V.S. and Stoilova, S.S.: The inequality of Erdős-Turan-Koksma: Walsh and Haar functions over finite groups. Math. Balkanica (N.S.) **19**: 349–366, 2005.
6. Hinrichs, A., Pillichshammer, F. and Schmid, W. Ch.: Tractability properties of the weighted star discrepancy. J. Complexity **24**: 134–143, 2008.
7. Joe, S.: Construction of good rank-1 lattice rules based on the weighted star discrepancy. In *Monte Carlo and quasi-Monte Carlo methods 2004*, pages 181–196. Springer, Berlin, 2006.
8. Kuipers, L. and Niederreiter, H.: *Uniform Distribution of Sequences.* John Wiley, New York, 1974.
9. Larcher, G. and Pirsic, G.: Base change problems for generalized Walsh series and multivariate numerical integration. Pacific J. Math. **189**, no. 1: 75–105, 1999.
10. Niederreiter, H.: Point Sets and Sequences with Small Discrepancy. Monatsh. Math. **104**: 273–337 1987.
11. Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods. No. 63 in CBMS-NSF Series in Applied Mathematics. SIAM, Philadelphia, 1992.
12. Niederreiter, H.: The existence of good extensible polynomial lattice rules. Monatsh. Math. **139**: 295–307, 2003.
13. Niederreiter, H.: Digital nets and coding theory. In *Coding, Cryptography and Combinatorics*, pages 247–257. Birkhäuser, Basel, 2004.
14. Niederreiter, H.: Constructions of (t, m, s)-nets and (t, s)-sequences. Finite Fields Appl. **11**: 578–600, 2005.
15. Niederreiter, H.: Nets, (t, s)-sequences and codes. In *Monte Carlo and quasi-Monte Carlo methods 2006*, pages 83–100. Springer, Berlin, 2008.
16. Pillichshammer, F. and Pirsic, G.: The quality parameter of cyclic nets and hyperplane nets. Submitted 2008.
17. Pirsic, G.: A small taxonomy of integration node sets. Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **214** (2005): 133–140, 2006.
18. Pirsic, G., Dick, J. and Pillichshammer, F.: Cyclic digital nets, hyperplane nets, and multivariate integration in Sobolev spaces. SIAM J. Numer. Anal. **44**: 385–411, 2006.
19. Sloan, I.H., Woźniakowski, H.: When are quasi-Monte Carlo algorithms efficient for high dimensional integrals? J. Complexity **14**: 1–33, 1998.