Discrepancy of higher rank polynomial lattice point sets

Julia Greslehner and Friedrich Pillichshammer[*]

Abstract

Polynomial lattice point sets (PLPSs) (of rank 1) are special constructions of finite point sets which may have outstanding equidistribution properties. Such point sets are usually required as nodes in quasi-Monte Carlo rules. Any PLPS is a special instance of a (t,m,s)-net in base b as introduced by Niederreiter.

In this paper we generalize PLPSs of rank 1 to what we call then PLPSs of rank r and analyze their equidistribution properties in terms of the quality parameter t and the (weighted) star discrepancy. We show the existence of PLPSs of "good" quality with respect to these quality measures. In case of the (weighted) star discrepancy such PLPSs can be constructed component-by-component wise. All results are for PLPSs in prime power base b. Therefore, we also generalize results for PLPSs of rank 1 that were only known for prime bases so far.

1 Introduction

Quasi-Monte Carlo rules for multivariate-integration are equal weight quadrature rules which approximate the integral of a function over the unit-cube by the average of function evaluations over a well-chosen deterministic point set. On first sight this approach looks simple but the crux of this method is the choice of sample points. From the well-known Koksma-Hlawka inequality it is known that point sets chosen from the unit-cube having low star-discrepancy yield small integration errors, at least for functions with bounded variation in the sense of Hardy and Krause (see [1, 2, 5, 12]). For a point set $\mathcal{P} = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ consisting of N points in $[0,1)^s$, the *star-discrepancy* is defined by

$$D_N^*(\mathcal{P}) = \sup_J \left| \frac{1}{N} \sum_{k=0}^{N-1} \chi_J(\boldsymbol{x}_k) - \lambda_s(J) \right| ,$$

where the supremum is extended over all subintervals J of $[0,1)^s$ of the form $\prod_{i=1}^s [0,\alpha_i)$, χ_J denotes the characteristic function of J, and $\lambda_s(J)$ is the volume of J.

Currently the best constructions of finite point sets with low star-discrepancy are based on the concept of (t,m,s)-nets in base b as introduced by Niederreiter [10] (see also [1] or [12, Chapter 4] for a survey of this theory).

[*] The authors are partially supported by the Austrian Science Foundation (FWF), Project S9609, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory". The first author is also supported by the Austrian Science Foundation (FWF), Project P21943-N18.

Definition 1 ((t,m,s)-nets)**.** Let $b \geq 2$, $s \geq 1$ and $0 \leq t \leq m$ be integers. A point set $\mathcal{P}$ consisting of b^m points in $[0,1)^s$ forms a (t,m,s)-net in base b, if every subinterval of the form $J = \prod_{i=1}^s [a_i b^{-d_i}, (a_i+1)b^{-d_i})$ of $[0,1)^s$, with integers $d_i \geq 0$ and integers $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ and of volume b^{t-m}, contains exactly b^t points of $\mathcal{P}$.

A (t,m,s)-net in base b with $t \geq 1$ is called a *strict* (t,m,s)-net in base b if it is not a $(t-1,m,s)$-net in base b. Furthermore, a $(0,m,s)$-net in base b is called strict by definition.

Note that for any point set of b^m points there always exists a $t \in \{0,\ldots,m\}$ such that it is a (t,m,s)-net in base b, e.g., we can always choose $t = m$. On the other hand, a net with optimal quality parameter $t = 0$ can only exist if $s \leq b+1$. With regard to this fact, t is often called the *quality parameter* of the net. Smaller values of t imply lower values for the star-discrepancy for nets. This is reflected in Niederreiter's [10] bound

$$D_N^*(\mathcal{P}) = O_{s,b}\left(b^t \frac{(\log N)^{s-1}}{N}\right) \tag{1}$$

on the star-discrepancy of any (t,m,s)-net in base b, where $N = b^m$. For explicit bounds on the star-discrepancy of (t,m,s)-nets we refer to [1, 12].

Concrete constructions of (t,m,s)-nets are based on the digital construction scheme as introduced by Niederreiter [10] which we recall in the following. To avoid too many technical notions we restrict ourselves to digital nets defined over the finite field $\mathbb{F}_b$ of prime power order b. For a more general definition (over arbitrary finite, commutative rings) see for example [6, 7, 12].

From now on let b be a prime power and let $\mathbb{F}_b$ be the finite field of b elements. For a positive integer r let $\mathbb{Z}_r = \{0,\ldots,r-1\}$. Let $\varphi : \mathbb{Z}_b \to \mathbb{F}_b$ be a fixed bijection with $\varphi(0) = 0$. For $k = \kappa_0 + \kappa_1 b + \cdots + \kappa_{m-1} b^{m-1}$ with $\kappa_0, \ldots, \kappa_{m-1} \in \mathbb{Z}_b$ we define

$$\mathbf{k} := (\varphi(\kappa_0), \ldots, \varphi(\kappa_{m-1}))^\top. \tag{2}$$

Here $\boldsymbol{x}^\top$ means the transpose of the vector $\boldsymbol{x}$. (Later, the symbol $^\top$ is used not only for row vectors but also for any matrix. Hence in general, $A^\top$ means the transpose of a matrix A.) Furthermore, we often associate the integer k with the polynomial $k(x) = \varphi(\kappa_0) + \varphi(\kappa_1)x + \cdots + \varphi(\kappa_{m-1})x^{m-1} \in \mathbb{F}_b[x]$ and vice versa.

Definition 2 (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 $\mathbb{F}_b$. Now we construct b^m points in $[0,1)^s$: for $1 \leq i \leq s$ and for $k \in \mathbb{Z}_{b^m}$ multiply the matrix C_i by the vector $\mathbf{k}$, i.e.,

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

and set

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

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

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

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

The quality parameter t of a digital net over $\mathbb{F}_b$ depends only on the choice of generating matrices $C_1, \ldots, C_s$: let $\rho = \rho(C_1, \ldots, C_s)$ be the largest integer such that for any choice of $d_1, \ldots, d_s \in \mathbb{N}_0$, with $d_1 + \cdots + d_s = \rho$, the following holds:

the first d_1 row vectors of C_1 together with

the first d_2 row vectors of C_2 together with

$\vdots$

the first d_s row vectors of C_s,

(these are together ρ vectors in $\mathbb{F}_b^m$) are linearly independent over the finite field $\mathbb{F}_b$. We call ρ the *linear independence parameter* of the matrices $C_1, \ldots, C_s$.

The point set constructed by the digital method with the $m \times m$ matrices $C_1, \ldots, C_s$ over a finite field $\mathbb{F}_b$ is then a strict $(m - \rho, m, s)$-net in base b, where $\rho = \rho(C_1, \ldots, C_s)$ is the linear independence parameter; see [12, Theorem 4.28] or [1, Theorem 4.52].

In [11] Niederreiter introduced a special family of digital (t, m, s)-nets over $\mathbb{F}_b$. Those nets are obtained from rational functions over finite fields. Since the construction of those point sets has some similarities with the construction of ordinary lattice point sets, at least for prime bases b, they are nowadays known under the name "polynomial lattice point sets (PLPSs)" or, using a more general terminology, "polynomial lattice point sets of rank 1". PLPSs are very poplar node sets for quasi-Monte Carlo rules. Since their introduction a lot of theory concerning distribution properties and efficiency for quasi-Monte Carlo has been developed by a multitude of authors. For a recent overview we refer to [1, Chapter 10] or to [14].

In this paper we introduce a generalization of Niederreiter's construction which we call "PLPSs of rank r". The aim is then to develop some theory on PLPSs of rank r which generalizes the existing theory for the rank 1 case. From these results we deduce existence results and even constructions of point sets with good distribution properties with respect to the quality parameter t or the (weighted) star-discrepancy. Thereby we also generalize many known results from the rank 1 case in prime base b to the case of *prime power* bases.

The paper is organized as follows: in Section 2 we introduce PLPSs of rank r over $\mathbb{F}_b$ where b is a prime power and we characterize the dual net of such nets. For prime bases b we show how this construction can be introduced independent from the theory of digital nets. In Section 3 we introduce a figure of merit for PLPSs of rank r and show how this is related to the quality parameter t. Based on this figure of merit we show the existence of PLPSs of rank r with reasonable low t-value. In Section 4 we analyze the (weighted) star discrepancy of PLPSs of rank r and we give a component-by-component construction of PLPSs with reasonable low (weighted) star discrepancy.

More notation. For a prime power b let $\mathbb{F}_b((x^{-1}))$ be the field of formal Laurent series over $\mathbb{F}_b$. Elements of $\mathbb{F}_b((x^{-1}))$ are formal Laurent series of the form $L = \sum_{l=w}^{\infty} t_l x^{-l}$, where w is an arbitrary integer and all $t_l \in \mathbb{F}_b$. Note that $\mathbb{F}_b((x^{-1}))$ contains the field of rational functions over $\mathbb{F}_b$ as a subfield. Further let $\mathbb{F}_b[x]$ be the set of all polynomials over $\mathbb{F}_b$. The *discrete exponential valuation* ν on $\mathbb{F}_b((x^{-1}))$ is defined by $\nu(L) = -w$ if

$L \neq 0$ and w is the least index with $t_w \neq 0$. For $L = 0$ we set $\nu(0) = -\infty$. Observe that we have $\nu(p) = \deg(p)$ for all nonzero polynomials $p \in \mathbb{F}_b[x]$.

For a polynomial $f \in \mathbb{F}_b[x]$ we will sometimes write $f(x)$ to indicate that it is a polynomial and similar for Laurent series $L \in \mathbb{F}_b((x^{-1}))$.

For a prime power b and $m \in \mathbb{N}$ we denote by $G_{b,m}$ the subset of $\mathbb{F}_b[x]$ consisting of all polynomials g with degree smaller than m, i.e.

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

where we use the convention $\deg(0) = -1$. Furthermore we define $G^*_{b,m} = G_{b,m} \setminus \{0\}$. Obviously we have $|G_{b,m}| = b^m$ and $|G^*_{b,m}| = b^m - 1$.

2 Definition of PLPSs of rank r

In this section we introduce PLPSs of rank r and characterize their dual nets.

Definition 3. Let b be a prime power and let $1 \leq r \leq s$ be integers. For $1 \leq i \leq r$ let $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,s}) \in \mathbb{F}_b[x]^s$, $f_i \in \mathbb{F}_b[x]$ with $m_i = \deg(f_i)$ and assume that

$$\frac{q_{i,j}}{f_i} = \sum_{k=w_{i,j}}^{\infty} u^{(i)}_{k,j} x^{-k} \in \mathbb{F}_b((x^{-1})).$$

Let $m = m_1 + \cdots + m_r$. For $1 \leq j \leq s$ define $C_j \in \mathbb{F}_b^{m \times m}$ by

$$C_j = \begin{pmatrix} u^{(1)}_{1,j} & u^{(1)}_{2,j} & \ldots & u^{(1)}_{m_1,j} & \ldots & u^{(r)}_{1,j} & u^{(r)}_{2,j} & \ldots & u^{(r)}_{m_r,j} \\ u^{(1)}_{2,j} & u^{(1)}_{3,j} & \ldots & u^{(1)}_{m_1+1,j} & \ldots & u^{(r)}_{2,j} & u^{(r)}_{3,j} & \ldots & u^{(r)}_{m_r+1,j} \\ \multicolumn{9}{c}{\dotfill} \\ u^{(1)}_{m,j} & u^{(1)}_{m+1,j} & \ldots & u^{(1)}_{m+m_1-1,j} & \ldots & u^{(r)}_{m,j} & u^{(r)}_{m+1,j} & \ldots & u^{(r)}_{m+m_r-1,j} \end{pmatrix},$$

i.e., $C_j = (C_j[k,\ell])_{k,\ell=1}^m$ and $C_j[k,\ell] = u^{(i)}_{k+\ell-(m_1+\cdots+m_{i-1}+1),j}$ whenever $m_1+\cdots+m_{i-1}+1 \leq \ell \leq m_1 + \cdots + m_i$ for $1 \leq i \leq r$ and $1 \leq k \leq m$.

Then, $C_1, \ldots, C_s$ are the generating matrices of a digital (t,m,s)-net over $\mathbb{F}_b$. The digital net obtained from the polynomials f_i and $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,s}) \in \mathbb{F}_b[x]^s$ for $1 \leq i \leq r$, without explicitly specifying the involved bijection $\varphi : \mathbb{Z}_b \to \mathbb{F}_b$, is denoted by $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$. We call $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ a *PLPS of rank r* (or short again *PLPS*) and a quasi-Monte Carlo rule using it is called a *polynomial lattice rule (of rank r)*.

Remark 4.

1. If we set $r = 1$ in the above definition then we obtain Niederreiter's definition of PLPSs from [11].

2. More general PLPSs of rank r, so-called polynomial integration lattices, can and have been introduced independently of net theory. See [8] for $b = 2$ and [9] for arbitrary base b. In [9, Section 5] it is shown how this notion can be interpreted as digital net at least for prime bases b.

For prime bases b there is an equivalent but more concise definition of PLPSs of rank r which makes the connection to ordinary lattice point sets obvious.

Let us for a moment assume that b is a prime. In this case we can identify $\mathbb{Z}_b$ and $\mathbb{F}_b$ and choose the involved bijection φ to be the identity. For $m \in \mathbb{N}$ let v_m be the map from $\mathbb{Z}_b((x^{-1}))$ to the interval $[0,1)$ defined by

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

Proposition 5. *Let b be a prime. Then we have that*

$$\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r) = v_m\left(\left\{\frac{h_1\boldsymbol{q}_1}{f_1} + \cdots + \frac{h_r\boldsymbol{q}_r}{f_r} : h_i \in \mathbb{Z}_b[x]/(f_i) \textit{ for all } 1 \le i \le r\right\}\right).$$

Proof: Assume that $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r) = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{b^m-1}\}$. Let $h_i = h_0^{(i)} + h_1^{(i)}x + \cdots + h_{m_i-1}^{(i)}x^{m_i-1}$ for $1 \le i \le r$, then for $1 \le j \le s$ we have

$$\begin{aligned}
v_m\left(\sum_{i=1}^{r} \frac{h_i(x)q_{i,j}(x)}{f_i(x)}\right) &= v_m\left(\sum_{i=1}^{r}\left(\sum_{l=w_{i,j}}^{\infty} u_{l,j}^{(i)}x^{-l}\right)\left(\sum_{k=0}^{m_i-1} h_k^{(i)}x^k\right)\right)\\
&= v_m\left(\sum_{i=1}^{r}\sum_{l=w_{i,j}}^{\infty}\sum_{k=0}^{m_i-1} u_{l,j}^{(i)}h_k^{(i)}x^{-(l-k)}\right)\\
&= v_m\left(\sum_{i=1}^{r}\sum_{t=w_{i,j}-m_i+1}^{\infty}\frac{1}{x^t}\sum_{k=0}^{m_i-1} u_{t+k,j}^{(i)}h_k^{(i)}\right)\\
&= v_m\left(\sum_{t=\min_i(w_{i,j}-m_i+1)}^{\infty}\frac{1}{x^t}\sum_{i=1}^{r}\sum_{k=0}^{m_i-1} u_{t+k,j}^{(i)}h_k^{(i)}\right)\\
&= \sum_{t=1}^{m} b^{-t}\sum_{i=1}^{r}\sum_{k=0}^{m_i-1} u_{t+k,j}^{(i)}h_k^{(i)},
\end{aligned}$$

where $\sum_{i=1}^{r}\sum_{k=0}^{m_i-1} u_{t+k,j}^{(i)}h_k^{(i)}$ is evaluated in $\mathbb{Z}_b$. We have

$$\sum_{k=0}^{m_i-1} u_{t+k,j}^{(i)}h_k^{(i)} = (u_{t,j}^{(i)}, \ldots u_{t+m_i-1,j}^{(i)}) \cdot \boldsymbol{h}_i,$$

where $\boldsymbol{h}_i = (h_0^{(i)}, \ldots h_{m_i-1}^{(i)})^\top \in \mathbb{Z}_b^{m_i}$. From this we get

$$v_m\left(\frac{h_1(x)\boldsymbol{q}_1(x)}{f_1(x)} + \cdots + \frac{h_r(x)\boldsymbol{q}_r(x)}{f_r(x)}\right) = \boldsymbol{x}_h,$$

with $h = h_0^{(1)} + \cdots + h_{m_1-1}^{(1)}b^{m_1-1} + \cdots + h_0^{(r)}b^{m_1+\cdots m_{r-1}} + \cdots + h_{m_r-1}^{(r)}b^{m_1+\cdots+m_r-1}$ in b-adic representation. □

Now we return to the general case. From now on let b be a prime power again. The following lemma for the case $r = 1$ was shown by Niederreiter in [11, Proof of Lemma 2].

Lemma 6. *Let b be a prime power and let $C_1, \ldots, C_s$ be the generating matrices of a PLPS $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ as given in Definition 3. Then for $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{Z}_{b^m}^s$ we have that*

$$C_1^\top \mathbf{k}_1 + \cdots C_s^\top \mathbf{k}_s = \mathbf{0} \tag{3}$$

where $\mathbf{0}$ is the zero vector in $\mathbb{F}_b^m$ and $\mathbf{k}_i$ as in (2), if and only if

$$\boldsymbol{k}(x) \cdot \boldsymbol{q}_i(x) \equiv 0 \pmod{f_i(x)} \quad \textit{for all } 1 \le i \le r,$$

where in the last expression $\boldsymbol{k}(x) = (k_1(x), \ldots, k_s(x))$ is the vector of polynomials associated with $\boldsymbol{k} = (k_1, \ldots, k_s)$.

Proof: For $1 \le j \le s$ and $1 \le i \le r$ assume that $\frac{q_{i,j}}{f_i} = \sum_{l=w_{i,j}}^\infty u_{l,j}^{(i)} x^{-l} \in \mathbb{F}_b((x^{-1}))$. For $k_j = \kappa_{0,j} + \kappa_{1,j} b + \cdots + \kappa_{m-1,j} b^{m-1}$ we then have

$$\begin{aligned}
\frac{k_j(x) q_{i,j}(x)}{f_i(x)} &= \left(\sum_{h=0}^{m-1} \varphi(\kappa_{h,j}) x^h \right) \left(\sum_{l=w_{i,j}}^{\infty} u_{l,j}^{(i)} x^{-l} \right) \\
&= \sum_{h=0}^{m-1} \varphi(\kappa_{h,j}) \sum_{l=w_{i,j}}^{\infty} u_{l,j}^{(i)} x^{h-l} \\
&= \sum_{h=0}^{m-1} \varphi(\kappa_{h,j}) \sum_{l=w_{i,j}-h}^{\infty} u_{l+h,j}^{(i)} x^{-l}
\end{aligned}$$

and hence, for $l \in \mathbb{N}$, the coefficient of x^{-l} in $\frac{k_j(x) q_{i,j}(x)}{f_i(x)}$ is $\sum_{h=0}^{m-1} \varphi(\kappa_{h,j}) u_{l+h,j}^{(i)}$. Summing up, we obtain that for $l \in \mathbb{N}$ the coefficient of x^{-l} in $\frac{\boldsymbol{k}(x) \cdot \boldsymbol{q}_i(x)}{f_i(x)}$ is given by

$$\sum_{j=1}^{s} \sum_{h=0}^{m-1} \varphi(\kappa_{h,j}) u_{l+h,j}^{(i)}.$$

However condition (3) is equivalent to

$$\sum_{j=1}^{s} \sum_{h=0}^{m-1} \varphi(\kappa_{h,j}) u_{l+h,j}^{(i)} = 0 \in \mathbb{F}_b$$

for all $1 \le i \le r$ and all $1 \le l \le m_i$. Therefore we obtain for any $1 \le i \le r$

$$\frac{\boldsymbol{k}(x) \cdot \boldsymbol{q}_i(x)}{f_i(x)} = g_i(x) + L_i(x)$$

for some $g_i(x) \in \mathbb{F}_b[x]$ and $L_i(x) \in \mathbb{F}_b((x^{-1}))$ of the form $\sum_{k=m_i+1}^\infty \alpha_k x^{-k}$, i.e. for the discrete exponential valuation of $L_i(x)$ we have $\nu(L_i) < -m_i$. Equivalently, we have

$$\boldsymbol{k}(x) \cdot \boldsymbol{q}_i(x) - g_i(x) f_i(x) = L_i(x) f_i(x).$$

On the left hand side, we have a polynomial over $\mathbb{F}_b$, whereas on the right hand side we have a Laurent series $L_i(x) f_i(x)$ with $\nu(L_i(x) f_i(x)) < 0$ since $\deg(f_i(x)) = m_i$. This is only possible if $L_i(x) f_i(x) = 0$ which means that $\boldsymbol{k}(x) \cdot \boldsymbol{q}_i(x) - g_i(x) f_i(x) = 0$ or equivalently $\boldsymbol{k}(x) \cdot \boldsymbol{q}_i(x) \equiv 0 \pmod{f_i(x)}$. □

Now Lemma 6 motivates the following definition:

Definition 7. The *dual net* of a PLPS $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ with $f_i \in \mathbb{F}_b[x]$, $\deg(f_i) = m_i$ and $\boldsymbol{q}_i \in \mathbb{F}_b[x]^s$ is given by

$$\mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r) := \{\boldsymbol{k} \in G_{b,m}^s \, : \, \boldsymbol{k} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i} \text{ for all } 1 \leq i \leq r\}.$$

Furthermore, let $\mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)' := \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r) \setminus \{\boldsymbol{0}\}$.

3 The quality parameter of PLPSs

For the determination of the quality parameter of PLPSs it is convenient to introduce the following figure of merit:

Definition 8. The *figure of merit* $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r)$ is defined as

$$\rho((\boldsymbol{q}_i, f_i)_{i=1}^r) := s - 1 + \min \sum_{j=1}^s \deg(h_j),$$

where the minimum is extended over all $(h_1, \ldots, h_s) \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)'$.

Theorem 9. *The PLPS $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ is a strict (t, m, s)-net over $\mathbb{F}_b$ with $t = m - \rho((\boldsymbol{q}_i, f_i)_{i=1}^r)$.*

Proof: It suffices to show that we have $\rho(C_1, \ldots, C_s) = \rho((\boldsymbol{q}_i, f_i)_{i=1}^r)$, where $\rho(C_1, \ldots, C_s)$ is the linear independence parameter. Let $\varphi : \{0, \ldots, b-1\} \to \mathbb{F}_b$ with $\varphi(0) = 0$ be the bijection used in the construction of the digital net $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$.

According to the definition of $\rho(C_1, \ldots, C_s)$ there are $d_1, \ldots, d_s \in \mathbb{N}_0$ with $d_1 + \cdots + d_s = \rho(C_1, \ldots, C_s) + 1$ such that the system consisting of the union of the first d_j row vectors $\mathbf{c}_1^{(j)}, \ldots \mathbf{c}_{d_j}^{(j)}$ of the matrix C_j, where $j = 1, \ldots, s$, is linearly dependent over $\mathbb{F}_b$. That is, there exist $\kappa_{j,h} \in \mathbb{Z}_b$ for $0 \leq h < d_j$, $1 \leq j \leq s$, not all zero, such that

$$\sum_{j=1}^s \sum_{h=0}^{d_j - 1} \varphi(\kappa_{j,h}) \mathbf{c}_{h+1}^{(j)} = \mathbf{0} \in \mathbb{F}_b^m.$$

Putting $\kappa_{j,h} = 0$ for $d_j \leq h \leq m-1$, $1 \leq j \leq s$, and $k_j = \kappa_{j,0} + \kappa_{j,1} b + \cdots + \kappa_{j,m-1} b^{m-1}$ and correspondingly $\mathbf{k}_j = (\varphi(\kappa_{j,0}), \ldots, \varphi(\kappa_{j,m-1}))^\top \in (\mathbb{F}_b^m)^\top$ for $1 \leq j \leq s$ we obtain

$$C_1^\top \mathbf{k}_1 + \cdots + C_s^\top \mathbf{k}_s = \mathbf{0}.$$

By Lemma 6 this is equivalent to $\boldsymbol{k} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i}$, $1 \leq i \leq r$, for $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{F}_b[x]^s \setminus \{0\}$, where $k_j(x) = \varphi(\kappa_{j,0}) + \varphi(\kappa_{j,1})x + \cdots + \varphi(\kappa_{j,m-1})x^{m-1} \in \mathbb{F}_b[x]$. Hence from the definition of $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r)$ we obtain

$$\begin{aligned}\rho((\boldsymbol{q}_i, f_i)_{i=1}^r) &= s - 1 + \min \sum_{j=1}^s \deg(h_j) \leq s - 1 + \sum_{j=1}^s \deg(k_j) \\ &\leq s - 1 + \sum_{j=1}^s (d_j - 1) = \rho(C_1, \ldots, C_s).\end{aligned}$$

On the other hand, from the definition of $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r)$ we find that there exists a nonzero $\boldsymbol{k} = (k_1, \ldots, k_s) \in G_{b,m}^s$ for all $1 \leq j \leq s$ and $\boldsymbol{k} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i}$ such that $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r) = s-1+\sum_{j=1}^s \deg(k_j)$. Again from Lemma 6 we obtain $C_1^\top \mathbf{k}_1 + \cdots + C_s^\top \mathbf{k}_s = \mathbf{0}$, where the vector $\mathbf{k}_j$ over $\mathbb{F}_b$ is determined by the coefficients of the polynomials k_j for $1 \leq j \leq s$. For $1 \leq j \leq s$ let $d_j = \deg(k_j)+1$. Then the system consisting of the union of the first d_j row vectors of C_j, where $j = 1, \ldots, s$, is linearly dependent over $\mathbb{F}_b$ and hence

$$\begin{aligned}\rho(C_1, \ldots, C_s) &\leq -1 + \sum_{j=1}^s d_j = -1 + \sum_{j=1}^s (\deg(k_j)+1) = s-1+\sum_{j=1}^s \deg(k_j) \\ &= s-1+\min \sum_{j=1}^s \deg(h_j) = \rho((\boldsymbol{q}_i, f_i)_{i=1}^r).\end{aligned}$$

□

Remark 10. Let $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,s}) \in \mathbb{F}_b[x]^s$ with $\gcd(q_{i,1}, f_i) = 1$. Then the condition $\boldsymbol{k} \cdot \boldsymbol{q}_i = k_1 q_{i,1} + \cdots + k_s q_{i,s} \equiv 0 \pmod{f_i}$ in Definition 8 of the figure of merit $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r)$ is equivalent to $k_1 + k_2 q_{i,1}^* q_{i,2} + \cdots + k_s q_{i,1}^* q_{i,s} \equiv 0 \pmod{f_i}$, where $q_{i,1}^* \in \mathbb{F}_b[x]$ is such that $q_{i,1}^* q_{i,1} \equiv 1 \pmod{f_i}$ ($q_{i,1}^*$ always exists as long as $\gcd(q_{i,1}, f_i) = 1$). Therefore the figure of merit is the same for $\boldsymbol{q}_i$ and for $(1, q_{i,1}^* q_{i,2}, \ldots, q_{i,1}^* q_{i,s})$ and hence it suffices to consider the figure of merit for vectors $\boldsymbol{q}_i$ of the form $\boldsymbol{q}_i = (1, q_{i,2}, \ldots, q_{i,s}) \in \mathbb{F}_b[x]^s$ only.
We will also consider vectors $\boldsymbol{q}_i$ of the special form $\boldsymbol{q}_i = (1, q_i, q_i^2, \ldots, q_i^{s-1}) \pmod{f_i}$. Such vectors are called Korobov vectors.

Lemma 11. *For a prime power b, $s \in \mathbb{N}$, $\rho \in \mathbb{Z}$, the number of $(h_1, \ldots, h_s) \in \mathbb{F}_b[x]^s$ with $(h_1, \ldots, h_s) \neq (0, \ldots, 0)$ and $\sum_{j=1}^s \deg(h_j) \leq \rho$ equals*

$$\Delta_b(s, \rho) := \sum_{d=0}^{s-1} \binom{s}{d} (b-1)^{s-d} \sum_{\gamma=0}^{\rho+d} \binom{s-d+\gamma-1}{\gamma} b^\gamma.$$

Proof: The result follows from [1, Lemma 10.14]. □

Theorem 12. *Let b be a prime power, let $\rho \in \mathbb{Z}$, $r, m, s \in \mathbb{N}$, $s \geq 2$, $r \leq s$ and let $f_i \in \mathbb{F}_b[x], 1 \leq i \leq r$, be irreducible and mutually relatively prime with* $\deg(f_i) = m_i$, *$m_1 + \cdots + m_r = m$.*

1. *If*

$$\sum_{\mathfrak{u} \subsetneq \{1, \ldots, r\}} \Delta_b\left(s, \rho - \sum_{i \in \mathfrak{u}} m_i\right) \prod_{i \in \mathfrak{u}} b^{m_i} < b^m,$$

then there exist $\boldsymbol{q}_i = (1, q_{i,2}, \ldots, q_{i,s}) \in G_{b,m_i}^s, 1 \leq i \leq r$, with $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r) \geq s + \rho$. Therefore the point set $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ is a digital (t, m, s)-net over $\mathbb{F}_b$ with $t \leq m - s - \rho$.

2. *If*

$$\sum_{\mathfrak{u} \subsetneq \{1, \ldots, r\}} \Delta_b\left(s, \rho - \sum_{i \in \mathfrak{u}} m_i\right) (s-1)^{r-|\mathfrak{u}|} \prod_{i \in \mathfrak{u}} b^{m_i} < b^m,$$

then there exist $q_i \in G_{b,m_i}$ such that $\boldsymbol{q}_i = (1, q_i, q_i^2, \ldots, q_i^{s-1}) \pmod{f_i}$, $1 \le i \le r$, satisfy $\rho((\boldsymbol{q}_i, f_i)_{i=1}^r) \ge s + \rho$. Therefore the point set $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ is a digital (t, m, s)-net over $\mathbb{F}_b$ with $t \le m - s - \rho$.

Proof: 1. Since $t \in \{0, \ldots, m\}$ we can assume that $-s \le \rho \le m - s$. Let

$$M(s, \rho) := \left\{ (h_1, \ldots, h_s) \in \mathbb{F}_b[x]^s : (h_1, \ldots, h_s) \ne (0, \ldots, 0), \sum_{j=1}^{s} \deg(h_j) \le \rho \right\}.$$

For given $(h_1, \ldots, h_s) \in M(s, \rho)$ we consider the number of solutions $(\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r)$, $\boldsymbol{q}_i = (1, q_{i,2}, \ldots, q_{i,s}) \in G_{b,m_i}^s$, of the congruence system

$$h_1 + h_2 q_{i,2} + \cdots + h_s q_{i,s} \equiv 0 \pmod{f_i}, \quad 1 \le i \le r.$$

Therefore we split the set $M(s, \rho)$ as follows:

$$\begin{aligned} M(s, \rho) &= \bigcup_{\mathfrak{u} \subsetneq \{1, \ldots, r\}} \{(h_1, \ldots, h_s) \in M(s, \rho) : h_1 \equiv h_2 \equiv \cdots \equiv h_s \equiv 0 \pmod{f_i} \text{ iff } i \in \mathfrak{u}\} \\ &=: \bigcup_{\mathfrak{u} \subsetneq \{1, \ldots, r\}} M(s, \rho, \mathfrak{u}). \end{aligned}$$

(If $\mathfrak{u} = \{1, \ldots, r\}$, then for each $1 \le j \le s$ we have $h_j \equiv 0 \pmod{f_1 \cdots f_r}$. Since not all h_j's are equal to zero it follows then that $\sum_{j=1}^s \deg(h_j) \ge m - s + 1$. As we assumed that $\rho \le m - s$ we find that the case $\mathfrak{u} = \{1, \ldots, r\}$ can be neglected.) Since $f_1, \ldots, f_r$ are mutually relative prime each $(h_1, \ldots, h_s) \in M(s, \rho, \mathfrak{u})$ is of the form $(a_1, \ldots, a_s) \prod_{i \in \mathfrak{u}} f_i$ and hence

$$\begin{aligned} &|M(s, \rho, \mathfrak{u})| \\ &\le \left| \left\{ (a_1, \ldots, a_s) \in \mathbb{F}_b[x]^s : (a_1, \ldots, a_s) \ne (0, \ldots, 0), \sum_{j=1}^{s} \left(\deg(a_j) + \chi_{(a_j \ne 0)} \sum_{i \in \mathfrak{u}} m_i \right) \le \rho \right\} \right| \\ &\le \left| \left\{ (a_1, \ldots, a_s) \in \mathbb{F}_b[x]^s : (a_1, \ldots, a_s) \ne (0, \ldots, 0), \sum_{j=1}^{s} \deg(a_j) \le \rho - \sum_{i \in \mathfrak{u}} m_i \right\} \right| \\ &= \Delta_b \left(s, \rho - \sum_{i \in \mathfrak{u}} m_i \right). \end{aligned}$$

For each $(h_1, \ldots, h_s) \in M(s, \rho, \mathfrak{u})$ the system

$$h_1 + h_2 q_{i,2} + \cdots + h_s q_{i,s} \equiv 0 \pmod{f_i}, \quad 1 \le i \le r,$$

has at most $\prod_{i \in \mathfrak{u}} b^{m_i(s-1)} \prod_{i \notin \mathfrak{u}} b^{m_i(s-2)} = b^{m(s-2)} \prod_{i \in \mathfrak{u}} b^{m_i}$ solutions $(\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r)$. Therefore to all nonzero $(h_1, \ldots, h_s) \in \mathbb{F}_b[x]^s$ with $\sum_{j=1}^s \deg(h_j) \le \rho$ there are assigned at most

$$b^{m(s-2)} \sum_{\mathfrak{u} \subsetneq \{1, \ldots, r\}} \Delta_b \left(s, \rho - \sum_{i \in \mathfrak{u}} m_i \right) \prod_{i \in \mathfrak{u}} b^{m_i}$$

different solutions $(\boldsymbol{q}_1,\ldots,\boldsymbol{q}_r)$, $\boldsymbol{q}_i=(1,q_{i,2},\ldots,q_{i,s})\in G_{b,m_i}^s$, satisfying the above congruence system. Now the total number of $(\boldsymbol{q}_1,\ldots,\boldsymbol{q}_r)$ under consideration equals $\prod_{i=1}^r b^{m_i(s-1)} = b^{m(s-1)}$. Thus, if

$$b^{m(s-2)} \sum_{\mathfrak{u}\subsetneq\{1,\ldots,r\}} \Delta_b\left(s,\rho-\sum_{i\in\mathfrak{u}} m_i\right)\prod_{i\in\mathfrak{u}} b^{m_i} < b^{m(s-1)},$$

that is, if

$$\sum_{\mathfrak{u}\subsetneq\{1,\ldots,r\}} \Delta_b\left(s,\rho-\sum_{i\in\mathfrak{u}} m_i\right)\prod_{i\in\mathfrak{u}} b^{m_i} < b^{m},$$

then there exists at least one $(\boldsymbol{q}_1,\ldots,\boldsymbol{q}_r)$, $\boldsymbol{q}_i=(1,q_{i,2},\ldots,q_{i,s})\in G_{b,m_i}^s$ such that for all nonzero $(h_1,\ldots,h_s)\in\mathbb{F}_b[x]^s$ with $\sum_{j=1}^s \deg(h_j)\le\rho$ we have

$$h_1+h_2q_{i,2}+\cdots+h_sq_{i,s}\not\equiv 0 \pmod{f_i}$$

for at least one $1\le i\le r$. For this $(\boldsymbol{q}_1,\ldots,\boldsymbol{q}_r)$ we have then $\rho((\boldsymbol{q}_i,f_i)_{i=1}^r)\ge s+\rho$. Hence the point set $\mathcal{P}((\boldsymbol{q}_i,f_i)_{i=1}^r)$ is a digital (t,m,s)-net over $\mathbb{F}_b$ with $t\le m-s-\rho$.

2. We proceed as above, but we note that for $(h_1,\ldots,h_s)\in M(s,\rho,\mathfrak{u})$ the system

$$h_1+h_2q_i+\cdots+h_sq_i^{s-1}\equiv 0 \pmod{f_i},\quad 1\le i\le r,$$

has at most $\prod_{i\in\mathfrak{u}} b^{m_i}\prod_{i\notin\mathfrak{u}}(s-1)=(s-1)^{r-|\mathfrak{u}|}\prod_{i\in\mathfrak{u}} b^{m_i}$ solutions. □

Lemma 13. *For a prime power b, $s\in\mathbb{N}$, $m\in\mathbb{N}_0$, $\rho\in\mathbb{Z}$ we have that*

$$\Delta_b(s,\rho-m)b^m\le\Delta_b(s,\rho).$$

Proof: The case $m=0$ is trivially fulfilled. It is enough to show that

$$\Delta_b(s,\rho-(m+1))b\le\Delta_b(s,\rho-m).$$

This however follows easily from the definition of Δ_b. □

The following corollary recovers [1, Corollary 10.15] which is obtained for the choice $r=1$.

Corollary 14. *Let b be a prime power and let $s,m,r\in\mathbb{N}$, $s\ge 2, r\le s$ and let $f_i\in\mathbb{F}_b[x], 1\le i\le r$, be irreducible and mutually relatively prime with $\deg(f_i)=m_i$, $m_1+\cdots+m_r=m$, and m sufficiently large.*

1. *There exist $\boldsymbol{q}_i=(1,q_{i,2},\ldots,q_{i,s})\in G_{b,m_i}^s, 1\le i\le r$, with*

$$\rho((\boldsymbol{q}_i,f_i)_{i=1}^r)\ge\left\lfloor m-(s-1)(\log_b m-1)+\log_b\frac{(s-1)!}{(b-1)^{s-1}(2^r-1)}\right\rfloor.$$

2. *There exist $q_i\in G_{b,m_i}$, such that $\boldsymbol{q}_i=(1,q_i,q_i^2,\ldots,q_i^{s-1}) \pmod{f_i}$, $1\le i\le r$, satisfy*

$$\rho((\boldsymbol{q}_i,f_i)_{i=1}^r)\ge\left\lfloor m-(s-1)(\log_b m-1)+\log_b\frac{(s-1)!}{(b-1)^{s-1}(s^r-1)}\right\rfloor.$$

Proof:

1. For $\rho \geq 1$ we have with Lemma 13 that

$$\begin{aligned}\sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \Delta_b\left(s, \rho - \sum_{i\in\mathfrak{u}} m_i\right)\prod_{i\in\mathfrak{u}} b^{m_i} &\leq (2^r-1)\Delta_b(s,\rho)\\ &\leq (2^r-1)\sum_{d=0}^{s-1}\binom{s}{d}(b-1)^{s-d}\binom{\rho+s-1}{s-d-1}\frac{b^{\rho+d+1}}{b-1}\\ &\leq (2^r-1)b^{\rho+1}\sum_{d=0}^{s-1}\binom{s}{d}(b-1)^{s-d-1}\frac{(\rho+s-1)^{s-d-1}}{(s-d-1)!}b^d\\ &= (2^r-1)\frac{\rho^{s-1}}{(s-1)!}b^{\rho+1}(b-1)^{s-1}\left(1+O_s\left(\frac{1}{\rho}\right)\right),\end{aligned}$$

where O_s indicates that the implied constant depends only on s. Now let

$$\rho = \left\lfloor m-(s-1)\log_b m + \log_b \frac{(s-1)!}{(b-1)^{s-1}(2^r-1)} - 1\right\rfloor,$$

which is in $\mathbb{N}$ for sufficiently large m. Then

$$\begin{aligned}&\sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \Delta_b\left(s, \rho - \sum_{i\in\mathfrak{u}} m_i\right)\prod_{i\in\mathfrak{u}} b^{m_i}\\ &\leq (2^r-1)\left(m-(s-1)\log_b m + \log_b\frac{(s-1)!}{(b-1)^{s-1}(2^r-1)}\right)^{s-1}\frac{b^m(s-1)!}{m^{s-1}(b-1)^{s-1}(2^r-1)}\\ &\times\frac{(b-1)^{s-1}}{(s-1)!}\left(1+O_s\left(\frac{1}{m}\right)\right)\\ &= b^m\left(1-(s-1)\frac{\log_b m}{m}+\frac{1}{m}\log_b\frac{(s-1)!}{(b-1)^{s-1}(2^r-1)}\right)^{s-1}\left(1+O_s\left(\frac{1}{m}\right)\right) < b^m\end{aligned}$$

for sufficiently large m and the result follows from the first part of Theorem 12.

2. From Lemma 13 we get that

$$\begin{aligned}\sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \Delta_b\left(s, \rho - \sum_{i\in\mathfrak{u}} m_i\right)(s-1)^{r-|\mathfrak{u}|}\prod_{i\in\mathfrak{u}} b^{m_i} &\leq \Delta_b(s,\rho)\sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}}(s-1)^{r-|\mathfrak{u}|}\\ &= \Delta_b(s,\rho)(s^r-1).\end{aligned}$$

The second assertion is now deduced in almost the same way from the second part of Theorem 12, one has simply to replace the term (2^r-1) by (s^r-1).

□

If we combine Corollary 14 with Theorem 12 and with Niederreiter's discrepancy bound for (t,m,s)-nets stated in (1) we obtain the existence of PLPSs $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ whose star-discrepancy is of order

$$D^*_{b^m}(\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)) = O_{s,b}(m^{2s-2}b^{-m}).$$

This result can be improved with a more direct analysis of the star-discrepancy of PLPSs which is the topic of the following section.

4 The star-discrepancy of PLPSs

In this section we deal with the classical star-discrepancy as well as the weighted star-discrepancy of PLPSs $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$. Before we state any results we recall the definition of the weighted star-discrepancy.

The weighted star-discrepancy was introduced by Sloan and Woźniakowski [18] with the aim to provide a "weighted" version of the Koksma-Hlawka inequality which takes imbalances in the importance of the projections of integrands into account. For more information we refer to [1, 13, 18]. We consider weights of product form which are independent of the dimension s. Let $\boldsymbol{\gamma} = (\gamma_i)_{i\geq 1}$ be a sequence of nonnegative real numbers and let $[s] := \{1, \ldots, s\}$. Then for $\emptyset \neq \mathfrak{u} \subseteq [s]$ the weight $\gamma_{\mathfrak{u}}$ is given by $\gamma_{\mathfrak{u}} = \prod_{i\in\mathfrak{u}} \gamma_i$.

For $\emptyset \neq \mathfrak{u} \subseteq [s]$, let $|\mathfrak{u}|$ denote the cardinality of $\mathfrak{u}$, and for a vector $\boldsymbol{z} \in [0,1]^s$ or a subset $J \subseteq [0,1]^s$ let $\boldsymbol{z}(\mathfrak{u})$ or $J(\mathfrak{u})$ denote the projection onto $[0,1]^{|\mathfrak{u}|}$ consisting of the components whose indices are contained in $\mathfrak{u}$. Hence $\boldsymbol{z}(\mathfrak{u}) \in [0,1]^{|\mathfrak{u}|}$ and $J(\mathfrak{u}) \subseteq [0,1]^{|\mathfrak{u}|}$.

Definition 15. For a point set $\mathcal{P}$ of N points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ in $[0,1)^s$ and given weights $\boldsymbol{\gamma} = (\gamma_i)_{i\geq 1}$, the weighted star-discrepancy is defined by

$$D^*_{N,\boldsymbol{\gamma}}(\mathcal{P}) = \sup_J \max_{\emptyset\neq\mathfrak{u}\subseteq[s]} \gamma_{\mathfrak{u}} \left| \frac{1}{N} \sum_{k=0}^{N-1} \chi_{J(\mathfrak{u})}(\boldsymbol{x}_k(\mathfrak{u})) - \lambda_{|\mathfrak{u}|}(J(\mathfrak{u})) \right|,$$

where the supremum is extended over all subintervals J of $[0,1)^s$ of the form $\prod_{i=1}^s [0, \alpha_i)$.

We will give now an upper bound on the (weighted) star-discrepancy of a PLPS $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$. The quantities R_b and $\widetilde{R}_{b,\boldsymbol{\gamma}}$ defined in the following are useful to obtain such a bound as they capture the essential part of the (weighted) star-discrepancy.

For $f_i \in \mathbb{F}_b[x]$, $\deg(f_i) = m_i, m_1 + \cdots + m_r = m$, and $\boldsymbol{q}_i \in \mathbb{F}_b[x]^s$, $1 \leq i \leq r$, define

$$R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) := \sum_{\boldsymbol{h}\in\mathcal{D}((\boldsymbol{q}_i,f_i)_{i=1}^r)'} r_b(\boldsymbol{h}),$$

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

$$r_b(h) := \begin{cases} 1 & \text{if } h = 0, \\ \frac{C}{b^{a+1}} & \text{if } h = \kappa_0 + \kappa_1 x + \cdots + \kappa_a x^a,\ \kappa_a \neq 0, \end{cases}$$

with $C := 1 + \max\limits_{1\leq x<b} \max\limits_{1\leq y<b} \left|\sum_{a=0}^{y-1} \prod_{i=1}^{\ell} \exp\left(2\pi \mathtt{i} \frac{(\pi_i\circ\psi\circ\varphi)(x)(\pi_i\circ\psi\circ\varphi)(a)}{p}\right)\right|$, where $\varphi : \mathbb{Z}_b \to \mathbb{F}_b$ is a fixed bijection, ψ is the isomorphism of additive groups $\psi : \mathbb{F}_b \to \mathbb{Z}_p^\ell$ if $b = p^\ell$, and define $\eta := \psi \circ \varphi$. For $1 \leq i \leq \ell$ we denote by π_i the projection $\pi_i : \mathbb{Z}_p^\ell \to \mathbb{Z}_p$, $\pi_i(x_1, \ldots, x_\ell) = x_i$. (Note that $C = C(b) \leq b$.)

$$\begin{tikzcd}
\mathbb{Z}_b \arrow[r, "\varphi"] \arrow[dr, "\eta"'] & \mathbb{F}_b \arrow[d, "\psi"] & \\
& \mathbb{Z}_p^\ell \arrow[r, "\pi_i"] & \mathbb{Z}_p
\end{tikzcd}$$

Furthermore we define

$$\widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r) := \sum_{\boldsymbol{h}\in\mathcal{D}((\boldsymbol{q}_i,f_i)_{i=1}^r)'} r_b(\boldsymbol{h}, \boldsymbol{\gamma}),$$

where for $h = (h_1, \ldots, h_s)$ we write $r_b(\boldsymbol{h}, \boldsymbol{\gamma}) := r_b(h_1, \gamma_1) \cdots r_b(h_s, \gamma_s)$ and for $h \in G_{b,m}$ and $\gamma \geq 0$,

$$r_b(h, \gamma) := \begin{cases} 1 + \gamma & \text{if } h = 0, \\ \gamma r_b(h) & \text{if } h \neq 0, \end{cases}$$

where $r_b(h)$ as above.

In Appendix A (see Proposition 28) it is shown that $R_b((\boldsymbol{q}_i, f_i)_{i=1}^r)$ and $\widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ can be computed in $O(b^m s)$ operations.

Now we are ready to give an upper bound on the (weighted) star-discrepancy in terms of R_b and $\widetilde{R}_{b,\boldsymbol{\gamma}}$, respectively.

Proposition 16. *Let b be a prime power and let $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ a sequence of weights. For the (weighted) star-discrepancy of the PLPS $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ we have*

1. $$D_{b^m}^*(\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)) \leq 1 - \left(1 - \frac{1}{b^m}\right)^s + 2R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) \leq \frac{s}{b^m} + 2R_b((\boldsymbol{q}_i, f_i)_{i=1}^r),$$
2. $$D_{b^m,\boldsymbol{\gamma}}^*(\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)) \leq \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} \left(1 - \left(1 - \frac{1}{b^m}\right)^{|\mathfrak{u}|}\right) + 2\widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r).$$

Proof:

1. This estimate follows from [3, Theorem 1] in combination with [16, Lemma 2.5] and Lemma 6.

2. This estimate follows from

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

where $\mathcal{P}(\mathfrak{u})$ in $[0,1)^{|\mathfrak{u}|}$ consists of the points $\boldsymbol{x}_n(\mathfrak{u})$ whenever $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ consists of $\boldsymbol{x}_n$ for $0 \leq n < b^m$ and the fact that

$$\widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r) = \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} R_b((\boldsymbol{q}_i(\mathfrak{u}), f_i)_{i=1}^r). \tag{4}$$

The proof of (4) follows exactly along the lines of the proof of [1, Lemma 5.42].

□

Remark 17. Note that $\sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} \left(1 - \left(1 - \frac{1}{b^m}\right)^{|\mathfrak{u}|}\right) = O_{\boldsymbol{\gamma},s}(b^{-m})$. If $\sum_{j \geq 1} \gamma_j < \infty$, then $\sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} \left(1 - \left(1 - \frac{1}{b^m}\right)^{|\mathfrak{u}|}\right) \leq \max(1, \Gamma) b^{-m} \exp(\sum_{j \geq 1} \gamma_j)$, where $\Gamma := \sum_{j \geq 1} \gamma_j / (1 + \gamma_j)$. See [1, Lemma 5.41].

The following lemma will be useful for our subsequent investigations. The proof of this result is straight forward (cf. [1, Lemma 10.22]).

Lemma 18. *For any prime power b and $\boldsymbol{\gamma} = (\gamma_i)_{i \geq i}$ a sequence of weights, we have*

$$\sum_{\boldsymbol{h} \in G_{b,m}^s} r_b(\boldsymbol{h}) = \left(1 + \frac{mC(b-1)}{b}\right)^s$$

and

$$\sum_{\boldsymbol{h} \in G_{b,m}^s} r_b(\boldsymbol{h}, \boldsymbol{\gamma}) = \prod_{i=1}^{s} \left(1 + \gamma_i \left(1 + \frac{mC(b-1)}{b}\right)\right).$$

Existence results. We show that for given $f_1, \ldots, f_r$, there always exists at least one vector $(\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r)$ such that $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ has appropriate (weighted) star-discrepancy. The bound on the average in the subsequent theorem serves as a benchmark for constructions of PLPSs with low (weighted) star-discrepancy.

Theorem 19. *Let b be a prime power, $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ a sequence of weights, $s, m, r \in \mathbb{N}$, $r \leq s$, and let $f_i \in \mathbb{F}_b[x]$, $1 \leq i \leq r$, be irreducible and mutually relatively prime with* $\deg(f_i) = m_i$, $m_1 + \cdots + m_r = m$. *Then we have*

$$\frac{1}{\prod_{i=1}^r |G_{b,m_i}^*|^s} \sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ 1 \leq i \leq r}} R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) \leq \frac{2^r - 1}{\prod_{i=1}^r (b^{m_i} - 1)} \left(\left(1 + \frac{mC(b-1)}{b}\right)^s - 1\right)$$

and

$$\begin{aligned} &\frac{1}{\prod_{i=1}^r |G_{b,m_i}^*|^s} \sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ 1 \leq i \leq r}} \widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r) \\ &\leq \frac{2^r - 1}{\prod_{i=1}^r (b^{m_i} - 1)} \left[\prod_{j=1}^{s} \left(1 + \gamma_j \left(1 + \frac{mC(b-1)}{b}\right)\right) - \prod_{j=1}^{s} (1 + \gamma_j)\right]. \end{aligned}$$

Proof: First observe that $|G_{b,m_i}^*| = b^{m_i} - 1$. We have

$$\begin{aligned} &\frac{1}{\prod_{i=1}^r |G_{b,m_i}^*|^s} \sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ 1 \leq i \leq r}} R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) \\ &= \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)^s} \sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ 1 \leq i \leq r}} \sum_{\boldsymbol{h} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)'} r_b(\boldsymbol{h}) \\ &= \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)^s} \sum_{\boldsymbol{h} \in G_{b,m}^s \setminus \{\boldsymbol{0}\}} r_b(\boldsymbol{h}) \sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ \boldsymbol{h} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)}} 1, \end{aligned}$$

where we used the definition of $R_b((\boldsymbol{q}_i, f_i)_{i=1}^r)$ and changed the order of summation. The last summation is extended over all $\boldsymbol{q}_i \in (G_{b,m_i}^*)^s$ for $1 \leq i \leq r$, for which $\boldsymbol{h} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)'$. Hence for a fixed $\boldsymbol{h} \in G_{b,m}^s \setminus \{\boldsymbol{0}\}$ we have

$$\sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ \boldsymbol{h} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)}} 1 = |\{(\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r) : \boldsymbol{q}_i \in (G_{b,m_i}^*)^s, \boldsymbol{h} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i}\}|$$

$$= \prod_{i=1}^{r} |\left\{ \boldsymbol{q} \in (G^*_{b,m_i})^s : \boldsymbol{h} \cdot \boldsymbol{q} \equiv 0 \pmod{f_i} \right\}|.$$

Now for a given $\boldsymbol{h} = (h_1, \ldots, h_s) \in G^s_{b,m} \setminus \{\boldsymbol{0}\}$ the number of solutions $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,s}) \in (G^*_{b,m_i})^s$ of

$$h_1 q_{i,1} + h_2 q_{i,2} + \cdots + h_s q_{i,s} \equiv 0 \pmod{f_i}$$

equals (note that f_j is assumed to be irreducible)

$$\begin{cases} 0 & \text{if } h_j \not\equiv 0 \pmod{f_i} \text{ for exactly one } j \text{ and } h_k \equiv 0 \pmod{f_i}\, \forall k \neq j, \\ (b^{m_i} - 1)^s & \text{if } h_1 \equiv h_2 \equiv \cdots \equiv h_s \equiv 0 \pmod{f_i}, \\ \leq (b^{m_i} - 1)^{s-1} & \text{else.} \end{cases}$$

Now we have

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^r |G^*_{b,m_i}|^s} \sum_{\substack{\boldsymbol{q}_i \in (G^*_{b,m_i})^s \\ 1 \leq i \leq r}} R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) \\
&= \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)^s} \sum_{\boldsymbol{h} \in G^s_{b,m} \setminus \{\boldsymbol{0}\}} r_b(\boldsymbol{h}) \prod_{i=1}^{r} |\left\{ \boldsymbol{q} \in (G^*_{b,m_i})^s : \boldsymbol{h} \cdot \boldsymbol{q} \equiv 0 \pmod{f_i} \right\}| \\
&\leq \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)^s} \sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \sum_{\substack{\boldsymbol{h} \in G^s_{b,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \equiv \boldsymbol{0} \pmod{f_i} \forall i \in \mathfrak{u} \\ \boldsymbol{h} \not\equiv \boldsymbol{0} \pmod{f_i} \forall i \notin \mathfrak{u}}} r_b(\boldsymbol{h}) \prod_{i \in \mathfrak{u}} (b^{m_i} - 1)^s \prod_{i \notin \mathfrak{u}} (b^{m_i} - 1)^{s-1} \\
&= \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)} \sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \sum_{\substack{\boldsymbol{h} \in G^s_{b,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \equiv \boldsymbol{0} \pmod{f_i} \forall i \in \mathfrak{u} \\ \boldsymbol{h} \not\equiv \boldsymbol{0} \pmod{f_i} \forall i \notin \mathfrak{u}}} r_b(\boldsymbol{h}) \prod_{i \in \mathfrak{u}} (b^{m_i} - 1) \\
&\leq \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)} \sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \prod_{i \in \mathfrak{u}} (b^{m_i} - 1) \sum_{\substack{\boldsymbol{h} \in G^s_{b,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \equiv \boldsymbol{0} \pmod{f_i} \forall i \in \mathfrak{u}}} r_b(\boldsymbol{h}),
\end{aligned}$$

(note that $\mathfrak{u} \neq \{1, \ldots, r\}$ since $\boldsymbol{h} \neq \boldsymbol{0}$). Now we compute

$$\begin{aligned}
\sum_{\substack{\boldsymbol{h} \in G^s_{b,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \equiv \boldsymbol{0} \pmod{f_i} \forall i \in \mathfrak{u}}} r_b(\boldsymbol{h}) &= \sum_{\mathfrak{v} \subsetneq [s]} \prod_{j \in \mathfrak{v}} r_b(0) \prod_{j \notin \mathfrak{v}} \sum_{\substack{h_j \in G_{b,m} \setminus \{0\} \\ h_j \equiv 0 \pmod{f_i} \forall i \in \mathfrak{u}}} r_b(h_j) \\
&\leq \sum_{\mathfrak{v} \subsetneq [s]} \prod_{j \notin \mathfrak{v}} \sum_{g \in G_{b,m} \setminus \{0\}} r_b\left(g \prod_{i \in \mathfrak{u}} f_i \right) \\
&= \sum_{\mathfrak{v} \subsetneq [s]} \prod_{j \notin \mathfrak{v}} \frac{1}{\prod_{i \in \mathfrak{u}} b^{m_i}} \frac{mC(b-1)}{b} \\
&\leq \frac{1}{\prod_{i \in \mathfrak{u}} b^{m_i}} \sum_{\mathfrak{v} \subsetneq [s]} \prod_{j \notin \mathfrak{v}} \frac{mC(b-1)}{b} \\
&= \frac{1}{\prod_{i \in \mathfrak{u}} b^{m_i}} \left(\left(1 + \frac{mC(b-1)}{b} \right)^s - 1 \right),
\end{aligned}$$

where we have used Lemma 18.

Altogether we have now

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^r |G_{b,m_i}^*|^s} \sum_{\substack{\boldsymbol{q}_i \in (G_{b,m_i}^*)^s \\ 1 \le i \le r}} R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) \\
&\le \frac{1}{\prod_{i=1}^r (b^{m_i}-1)} \sum_{\mathfrak{u} \subsetneq \{1,\ldots,r\}} \left(\left(1+\frac{mC(b-1)}{b}\right)^s - 1\right) \prod_{i \in \mathfrak{u}} \frac{b^{m_i}-1}{b^{m_i}} \\
&\le \frac{2^r-1}{\prod_{i=1}^r (b^{m_i}-1)} \left(\left(1+\frac{mC(b-1)}{b}\right)^s - 1\right).
\end{aligned}$$

This proves the unweighted result. The average of $\widetilde{R}_{b,\gamma}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ can be estimated in a similar way. □

Remark 20. In the case where $r = 1$ the obtained result is comparable with [1, Theorem 10.21] and [1, Theorem 10.24] for prime bases b.

As a consequence of Theorem 19, we obtain the following existence results.

Corollary 21. *Let b be a prime power, $\boldsymbol{\gamma} = (\gamma_i)_{i \ge 1}$ a sequence of weights, let $s, m, r \in \mathbb{N}$, $r \le s$, and let $f_i \in \mathbb{F}_b[x]$, $1 \le i \le r$, be irreducible and mutually relatively prime with* $\deg(f_i) = m_i$, $m_1 + \cdots + m_r = m$. *Then for $0 \le \alpha < 1$ there are more than $\alpha \prod_{i=1}^r |G_{b,m_i}^*|^s$ vectors of polynomials $(\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r) \in \prod_{i=1}^r (G_{b,m_i}^*)^s$ such that*

$$D_{b^m}^*(\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)) \le \frac{s}{b^m} + \frac{1}{1-\alpha} \frac{2 \cdot (2^r-1)}{\prod_{i=1}^r (b^{m_i}-1)} \left(1 + \frac{mC(b-1)}{b}\right)^s$$

and

$$\begin{aligned}
D_{b^m}^*(\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)) \;\le\; & \sum_{\emptyset \ne \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} \left(1 - \left(1 - \frac{1}{b^m}\right)^{|\mathfrak{u}|}\right) \\
& + \frac{1}{1-\alpha} \frac{2 \cdot (2^r-1)}{\prod_{i=1}^r (b^{m_i}-1)} \prod_{j=1}^s \left(1 + \gamma_j \left(1 + \frac{mC(b-1)}{b}\right)\right).
\end{aligned}$$

Proof: The result follows from Proposition 16 and Theorem 19 by using standard arguments (as used, for example, in [1, Proof of Corollary 10.23]). □

A Higher rank - Component by component construction. Now that we know that for given irreducible and mutually relatively prime polynomials $f_i \in \mathbb{F}_b[x]$, $1 \le i \le r$, there exists a sufficiently large number of good vectors $(\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r)$ which yield PLPSs with reasonable low (weighted) star-discrepancy, we want to find such vectors by computer search. Unfortunately, a full search is not possible (except maybe for small values of m, s), since we have to check b^{ms} vectors of polynomials. We will use a component-by-component construction, an idea that was introduced by Korobov [4] for ordinary latice rules and that was later re-invented by Sloan and Reztsov [17]. The same idea applies to higher rank PLPSs (see [1, Algorithm 10.26] for the case $r = 1$).

Algorithm 22. Given a prime power b, $s, m, r \in \mathbb{N}$, $r \leq s$, and polynomials $f_i \in \mathbb{F}_b[x]$, $1 \leq i \leq r$, with $\deg(f_i) = m_i$, $m_1 + \cdots + m_r = m$ (and a sequence $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ of weights).

1. Choose $q_{i,1} = 1$ for all $1 \leq i \leq r$.
2. For $d > 1$, assume we have already constructed $q_{i,1}, \ldots, q_{i,d-1} \in G^*_{b,m_i}$ for all $i \in \{1, \ldots, r\}$. Then find $q_{i,d} \in G^*_{b,m_i}$ for $1 \leq i \leq r$, which minimizes the quantity $R_b(((q_{i,1}, \ldots, q_{i,d-1}, q_{i,d}), f_i)_{i=1}^r)$ (or $\widetilde{R}_{b,\boldsymbol{\gamma}}(((q_{i,1}, \ldots, q_{i,d-1}, q_{i,d}), f_i)_{i=1}^r)$ in the weighted case) as a function of $(q_{1,d}, \ldots, q_{r,d})$.

Remark 23. The quantities $R_b((\boldsymbol{q}_i, f_i)_{i=1}^r)$ and $\widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ can be computed in $O(b^m s)$ operations (see Proposition 28). Hence the cost of Algorithm 22 is of $O(b^{2m} s^2)$ operations.

In the following theorem, we show that Algorithm 22 is guaranteed to find good vectors $\boldsymbol{q}_i, 1 \leq i \leq r$, where the polynomials $f_i, 1 \leq i \leq r$ are irreducible and mutually relatively prime.

Theorem 24. *Let b be a prime power, $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ a sequence of weights, let $s, m, r \in \mathbb{N}$, $r \leq s$, let $f_i \in \mathbb{F}_b[x]$, $1 \leq i \leq r$, be irreducible and mutually relatively prime with* $\deg(f_i) = m_i$, $m_1 + \cdots + m_r = m$. *Suppose $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,s}) \in (G^*_{b,m_i})^s$ for $1 \leq i \leq r$ is constructed according to Algorithm 22. Then for all $1 \leq d \leq s$ we have*

$$R_b(((q_{i,1}, \ldots, q_{i,d}), f_i)_{i=1}^r) \leq \frac{2^r - 1}{\prod_{i=1}^r (b^{m_i} - 1)} \left(1 + \frac{mC(b-1)}{b}\right)^d$$

and

$$\widetilde{R}_{b,\boldsymbol{\gamma}}(((q_{i,1}, \ldots, q_{i,d}), f_i)_{i=1}^r) \leq \frac{2^r - 1}{\prod_{i=1}^r (b^{m_i} - 1)} \prod_{j=1}^d \left(1 + \gamma_j \left(1 + \frac{mC(b-1)}{b}\right)\right).$$

Corresponding bounds on the (weighted) star discrepancy can be obtained from Proposition 16.

Proof: We only prove the first part. To prove the second part, simply replace $r_b(\boldsymbol{h})$ and R_b by $r_b(\boldsymbol{h}, \boldsymbol{\gamma})$ and $\widetilde{R}_{b,\boldsymbol{\gamma}}$ respectively.

Since the f_i, $1 \leq i \leq r$, are irreducible and mutually relatively prime it follows that $R_b((1, f_i)_{i=1}^r) = 0$ and the result follows for $d = 1$.

Suppose now that for some $1 \leq d < s$ we have already constructed $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,d}) \in (G^*_{b,m_i})^d$ for $1 \leq i \leq r$ and

$$R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) \leq \frac{2^r - 1}{\prod_{i=1}^r (b^{m_i} - 1)} \left(1 + \frac{mC(b-1)}{b}\right)^d.$$

Now we consider $(\boldsymbol{q}_i, q_{i,d+1}) := (q_{i,1}, \ldots, q_{i,d}, q_{i,d+1})$. We have

$$R_b(((\boldsymbol{q}_i, q_{i,d+1}), f_i)_{i=1}^r) = \sum_{(\boldsymbol{h}, h_{d+1}) \in \mathcal{D}(((\boldsymbol{q}_i, q_{i,d+1}), f_i)_{i=1}^r)'} r_b(\boldsymbol{h}) r_b(h_{d+1})$$

$$
\begin{aligned}
&= \sum_{\boldsymbol{h} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)'} r_b(\boldsymbol{h}) + \theta(q_{1,d+1}, \dots, q_{r,d+1}) \\
&= R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) + \theta(q_{1,d+1}, \dots, q_{r,d+1}),
\end{aligned}
$$

where we have separated out the $h_{d+1} = 0$ terms, and

$$
\theta(q_{1,d+1}, \dots, q_{r,d+1}) := \sum_{h_{d+1} \in G_{b,m}^*} r_b(h_{d+1}) \sum_{\substack{\boldsymbol{h} \in G_{b,m}^d \\ (\boldsymbol{h}, h_{d+1}) \in \mathcal{D}(((\boldsymbol{q}_i, q_{i,d+1}), f_i)_{i=1}^r)'}} r_b(\boldsymbol{h}).
$$

Here the last summation is over all $\boldsymbol{h} \in G_{b,m}^d$ for which $(\boldsymbol{h}, h_{d+1}) \in \mathcal{D}(((\boldsymbol{q}_i, q_{i,d+1}), f_i)_{i=1}^r)'$. Since $(q_{1,d+1}, \dots, q_{r,d+1})$ is a minimizer of $R_b(((\boldsymbol{q}_i, q_{i,d+1}), f_i)_{i=1}^r)$ and since the only dependence on $q_{i,d+1}$ for $1 \le i \le r$ is in θ it follows that $(q_{1,d+1}, \dots, q_{r,d+1})$ is also a minimizer of θ and hence we obtain

$$
\begin{aligned}
&\theta(q_{1,d+1}, \dots, q_{r,d+1}) \\
&\le \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)} \sum_{\substack{z_i \in G_{b,m_i}^* \\ 1 \le i \le r}} \theta(z_1, \dots, z_r) \\
&= \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)} \sum_{\substack{z_i \in G_{b,m_i}^* \\ 1 \le i \le r}} \sum_{h_{d+1} \in G_{b,m}^*} r_b(h_{d+1}) \sum_{\substack{\boldsymbol{h} \in G_{b,m}^d \\ (\boldsymbol{h}, h_{d+1}) \in \mathcal{D}(((\boldsymbol{q}_i, z_i), f_i)_{i=1}^r)'}} r_b(\boldsymbol{h}) \\
&= \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)} \sum_{h_{d+1} \in G_{b,m}^*} r_b(h_{d+1}) \sum_{\boldsymbol{h} \in G_{b,m}^d} r_b(\boldsymbol{h}) \sum_{\substack{z_i \in G_{b,m_i}^* \\ (\boldsymbol{h}, h_{d+1}) \in \mathcal{D}(((\boldsymbol{q}_i, z_i), f_i)_{i=1}^r)'}} 1.
\end{aligned}
$$

The condition $(\boldsymbol{h}, h_{d+1}) \in \mathcal{D}(((\boldsymbol{q}_i, z_i), f_i)_{i=1}^r)'$ is equivalent to the equation system

$$
z_i h_{d+1} \equiv -\boldsymbol{h} \cdot \boldsymbol{q}_i \pmod{f_i} \quad \text{for all } 1 \le i \le r.
$$

For fixed i, we consider now several cases to determine the number of solutions z_i of $z_i h_{d+1} \equiv -\boldsymbol{h} \cdot \boldsymbol{q}_i \pmod{f_i}$:

1. If $h_{d+1} \equiv 0 \pmod{f_i}$ and $-\boldsymbol{h} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i}$, then there are $b^{m_i} - 1$ solutions.

2. If $h_{d+1} \equiv 0 \pmod{f_i}$ and $-\boldsymbol{h} \cdot \boldsymbol{q}_i \not\equiv 0 \pmod{f_i}$, then we have no solution.

3. $h_{d+1} \not\equiv 0 \pmod{f_i}$ and $-\boldsymbol{h} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i}$, then there is no solution $z_i \in G_{b,m_i}^*$, since f_i is irreducible.

4. If $h_{d+1} \not\equiv 0 \pmod{f_i}$ and $-\boldsymbol{h} \cdot \boldsymbol{q}_i \not\equiv 0 \pmod{f_i}$, then we have exactly one solution.

Altogether we obtain

$$
\begin{aligned}
&\theta(q_{1,d+1}, \dots, q_{r,d+1}) \\
&\le \frac{1}{\prod_{i=1}^r (b^{m_i} - 1)} \sum_{\mathfrak{u} \subsetneq \{1,\dots,r\}} \sum_{\substack{h_{d+1} \in G_{b,m}^* \\ h_{d+1} \equiv 0 \pmod{f_i}\, \forall i \in \mathfrak{u} \\ h_{d+1} \not\equiv 0 \pmod{f_i}\, \forall i \notin \mathfrak{u}}} r_b(h_{d+1}) \sum_{\substack{\boldsymbol{h} \in G_{b,m}^d \\ \boldsymbol{h} \cdot \boldsymbol{q}_i \equiv 0 \pmod{f_i}\, \forall i \in \mathfrak{u} \\ \boldsymbol{h} \cdot \boldsymbol{q}_i \not\equiv 0 \pmod{f_i}\, \forall i \notin \mathfrak{u}}} r_b(\boldsymbol{h}) \prod_{i \in \mathfrak{u}} (b^{m_i} - 1)
\end{aligned}
$$

$$\begin{aligned}
&\le \frac{1}{\prod_{i=1}^r (b^{m_i}-1)} \sum_{\mathfrak{u}\subsetneq\{1,\ldots,r\}} \prod_{i\in\mathfrak{u}} (b^{m_i}-1) \sum_{\substack{h_{d+1}\in G^*_{b,m}\\ h_{d+1}\equiv 0 \pmod{f_i}\,\forall i\in\mathfrak{u}}} r_b(h_{d+1}) \sum_{\boldsymbol{h}\in G^d_{b,m}} r_b(\boldsymbol{h})\\
&= \frac{1}{\prod_{i=1}^r (b^{m_i}-1)} \left(1+\frac{mC(b-1)}{b}\right)^d \sum_{\mathfrak{u}\subsetneq\{1,\ldots,r\}} \prod_{i\in\mathfrak{u}} (b^{m_i}-1) \sum_{\substack{h_{d+1}\in G^*_{b,m}\\ h_{d+1}=g\prod_{i\in\mathfrak{u}} f_i}} r_b(h_{d+1})\\
&\le \frac{1}{\prod_{i=1}^r (b^{m_i}-1)} \left(1+\frac{mC(b-1)}{b}\right)^d \sum_{\mathfrak{u}\subsetneq\{1,\ldots,r\}} \prod_{i\in\mathfrak{u}} \frac{b^{m_i}-1}{b^{m_i}} \sum_{g\in G^*_{b,m}} r_b(g)\\
&\le \frac{2^r-1}{\prod_{i=1}^r (b^{m_i}-1)} \left(1+\frac{mC(b-1)}{b}\right)^d \sum_{g\in G^*_{b,m}} r_b(g),
\end{aligned}$$

where we have used Lemma 18. Now we obtain

$$\begin{aligned}
&R_b(((\boldsymbol{q}_i, q_{i,d+1}), f_i)_{i=1}^r)\\
&\le R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) + \frac{2^r-1}{\prod_{i=1}^r (b^{m_i}-1)} \left(1+\frac{mC(b-1)}{b}\right)^d \sum_{g\in G^*_{b,m}} r_b(g)\\
&\le \frac{2^r-1}{\prod_{i=1}^r (b^{m_i}-1)} \left(1+\frac{mC(b-1)}{b}\right)^d \sum_{g\in G_{b,m}} r_b(g)\\
&= \frac{2^r-1}{\prod_{i=1}^r (b^{m_i}-1)} \left(1+\frac{mC(b-1)}{b}\right)^{d+1},
\end{aligned}$$

where we have used Lemma 18 again. The result follows by induction. □

The following result can be proven in the same way as [1, Corollary 5.45]. It shows that the bound on the weighted star discrepancy can be made independent of the dimension s under certain assumptions on the weights $\boldsymbol{\gamma}$.

Corollary 25. *Let b be a prime power, $\boldsymbol{\gamma} = (\gamma_i)_{i\ge 1}$ a sequence of weights, let $s, m, r \in \mathbb{N}$, $r \le s$, let $f_i \in \mathbb{F}_b[x]$, $1 \le i \le r$, be irreducible and mutually relatively prime with* $\deg(f_i) = m_i$, $m_1 + \cdots + m_r = m$. *Suppose $\boldsymbol{q}_i = (q_{i,1}, \ldots, q_{i,s}) \in (G^*_{b,m_i})^s$ for $1 \le i \le r$ is constructed according to Algorithm 22 using $\widetilde{R}_{b,\boldsymbol{\gamma}}$.*

If $\sum_{i=1}^\infty \gamma_i < \infty$, then for any $\delta > 0$ there exists a constant $c_{\boldsymbol{\gamma},\delta} > 0$, independent of s and m, such that the weighted star discrepancy of $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ satisfies

$$D^*_{b^m,\boldsymbol{\gamma}}(\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r) \le \frac{c_{\boldsymbol{\gamma},\delta}}{b^{m(1-\delta)}}. \qquad (5)$$

In particular, the bound on the weighted star discrepancy is independent of the dimension s.

Appendix A: Calculation of R_b and $\widetilde{R}_{b,\boldsymbol{\gamma}}$

In this section we show that the quantities R_b and $\widetilde{R}_{b,\boldsymbol{\gamma}}$ can be computed efficiently. We will need the definition of Walsh functions over the finite field $\mathbb{F}_b$.

Definition 26 (Walsh functions)**.** Let $b = p^\ell$ with a prime p and a positive integer ℓ, let $k \in \mathbb{N}_0$ with base b representation $k = \kappa_0 + \kappa_1 b + \cdots + \kappa_{m-1} b^{m-1}$, where $\kappa_l \in \mathbb{Z}_b$ and let $x \in [0,1)$ with base b representation $x = \frac{x_1}{b} + \frac{x_2}{b^2} + \cdots$. Then the k-th Walsh function over the finite field $\mathbb{F}_b$ with respect to the bijection φ is defined by

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

where π_i and η are as before (page 12). For convenience we will in the following 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

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

If we consider Walsh functions $_{\mathbb{F}_{b,\varphi}}\mathrm{wal}_k$ in conjunction with digital nets over $\mathbb{F}_b$ and implied bijection φ (cf. Definition 2), then b and φ, respectively, are always considered to be the same.

From [16, Lemma 2.5] and Lemma 6 we immediately derive the following lemma that gives an important indicator function.

Lemma 27. *Let b be a prime power and let $C_1, \ldots, C_s$ be the generating matrices of a PLPS $\mathcal{P}((\boldsymbol{q}_i, f_i)_{i=1}^r) = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{b^m-1}\}$. Then for any vector $\boldsymbol{k} \in \{0, \ldots, b^m - 1\}^s$ we have*

$$\frac{1}{b^m} \sum_{h=0}^{b^m-1} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_h) = \begin{cases} 1 & \textit{if } \boldsymbol{k} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r), \\ 0 & \textit{else.} \end{cases}$$

Now we have

$$\begin{aligned} R_b((\boldsymbol{q}_i, f_i)_{i=1}^r) &= \sum_{\boldsymbol{h} \in \mathcal{D}((\boldsymbol{q}_i, f_i)_{i=1}^r)'} r_b(\boldsymbol{h}) \\ &= -1 + \sum_{\boldsymbol{k} \in \{0, \ldots, b^m-1\}^s} r_b(\boldsymbol{k}) \frac{1}{b^m} \sum_{n=0}^{b^m-1} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) \\ &= -1 + \frac{1}{b^m} \sum_{n=0}^{b^m-1} \prod_{j=1}^{s} \left(\sum_{k=0}^{b^m-1} r_b(k)\, \mathrm{wal}_k(x_{n,j}) \right) \\ &= -1 + \frac{1}{b^m} \sum_{n=0}^{b^m-1} \prod_{j=1}^{s} \phi_{b,m}(x_{n,j}), \qquad (6) \end{aligned}$$

where we identify a polynomial $k(x) = \kappa_0 + \kappa_1 x + \cdots + \kappa_{m-1} x^{m-1} \in G_{b,m}$ with the integer $k = \varphi^{-1}(\kappa_0) + \varphi^{-1}(\kappa_1) b + \cdots + \varphi^{-1}(\kappa_{m-1}) b^{m-1}$ and where we used the definition

$$\phi_{b,m}(x) := \sum_{h=0}^{b^m-1} r_b(h)\, \mathrm{wal}_h(x).$$

Now from the proof of [15, Proposition 3] we get

$$\phi_{b,m}(x) = 1 + \sum_{h=1}^{b^m-1} r_b(h)\,\mathrm{wal}_h(x) = 1 + \frac{C}{b}((b-1)(m_0(x)-1)-1), \tag{7}$$

with C as in the definition of r_b and for $x \in b^{-m}\mathbb{Z}_{b^m} \setminus \{0\}$, $m_0(x) := \max\{l \leq m : x < b^{-(l-1)}\} = \lceil -\log_b x \rceil$ and $m_0(0) := m + \frac{b}{b-1}$. Note that it is enough to consider $x \in b^{-m}\mathbb{Z}_{b^m}$ only.

Using (4) we have

$$\begin{aligned} \widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r) &= \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} R_b((\boldsymbol{q}_i(\mathfrak{u}), f_i)_{i=1}^r) \\ &= -\sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} + \frac{1}{b^m} \sum_{n=0}^{b^m-1} \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \gamma_{\mathfrak{u}} \prod_{j \in \mathfrak{u}} \phi_{b,m}(x_{n,j}) \\ &= -\prod_{j=1}^{s}(1+\gamma_j) + \frac{1}{b^m} \sum_{n=0}^{b^m-1} \prod_{j=1}^{s}(1+\gamma_j \phi_{b,m}(x_{n,j})). \end{aligned} \tag{8}$$

We summarize:

Proposition 28. *Let b be a prime power, $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ a sequence of weights and let $s, m, r \in \mathbb{N}$, $r \leq s$, and let $f_i \in \mathbb{F}_b[x]$, $1 \leq i \leq r$, $\deg(f_i) = m_i$, $m_1 + \cdots + m_r = m$, and $\boldsymbol{q}_i \in G_{b,m}^s$, $1 \leq i \leq r$. Using* (6), (7) *and* (8) *one can compute $R_b((\boldsymbol{q}_i, f_i)_{i=1}^r)$ and $\widetilde{R}_{b,\boldsymbol{\gamma}}((\boldsymbol{q}_i, f_i)_{i=1}^r)$ in $O(b^m s)$ operations.*

References

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

[2] Drmota, M. and Tichy, R. F.: *Sequences, Discrepancies and Applications.* Lecture Notes in Mathematics 1651, Springer, Berlin, 1997.

[3] 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.

[4] Korobov, N. M.: *Number-theoretic methods in approximate analysis* Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1963. (Russian)

[5] Kuipers, L. and Niederreiter, H.: *Uniform Distribution of Sequences.* John Wiley, New York, 1974; reprint, Dover Publications, Mineola, NY, 2006.

[6] Larcher, G.: Digital point sets: analysis and application. In: *Random and Quasi-Random Point Sets*, pages 167–222. Springer Lecture Notes in Statistics 138, New York, 1998.

[7] Larcher, G., Niederreiter, H., and Schmid, W.Ch.: Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration. Monatsh. Math., **121**: 231–253, 1996.

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

[9] L'Ecuyer, P.: Polynomial integration lattices. In: *Monte Carlo and quasi-Monte Carlo methods 2002*, pages 73–98, Springer, Berlin, 2004,

[10] Niederreiter, H.: Point sets and sequences with small discrepancy. Monatsh. Math., **104**: 273–337, 1987.

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

[12] Niederreiter, H.: *Random Number Generation and Quasi-Monte Carlo Methods.* No. 63 in CBMS-NSF Series in Applied Mathematics. SIAM, Philadelphia, 1992.

[13] Novak, E. and Woźniakowski, H.: *Tractability of Multivariate Problems. Volume II: Standard Information for Functionals*, EMS Tracts in Mathematics, 12. European Mathematical Society (EMS), Zürich, 2010.

[14] Pillichshammer, F.: Polynomial lattice point sets. Submitted, 2011.

[15] Pillichshammer, F. and Pirsic, G.: Discrepancy of hyperplane nets and cyclic nets. In: *Monte Carlo and quasi-Monte Carlo methods 2008*, pages 573–587, Springer, Berlin, 2009.

[16] 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.

[17] Sloan, I. H. and Reztsov, A. V.: Component-by component construction of good lattice rules. Math. Comp. 71: 263–273, 2002.

[18] Sloan, I. H. and Woźniakowski, H.: When are quasi-Monte Carlo algorithms efficient for high dimensional integrals?, J. Complexity, **14**: 1–33, 1998.

Authors' address:
Institut für Finanzmathematik, Universität Linz, Altenbergerstr. 69, 4040 Linz, Austria
E-mail: `julia.greslehner@gmx.at` and `friedrich.pillichshammer@jku.at`