Constructions of General Polynomial Lattices for Multivariate Integration

Peter Kritzer and Friedrich Pillichshammer*

Abstract

We study a construction algorithm for certain polynomial lattice rules modulo arbitrary polynomials. The underlying polynomial lattices are special types of digital nets as introduced by Niederreiter. Dick, Kuo, Pillichshammer and Sloan recently introduced construction algorithms for polynomial lattice rules modulo irreducible polynomials which yield a small worst-case error for integration of functions in certain weighted Hilbert spaces. Here, we generalize these results to the case where the polynomial lattice rules are constructed modulo *arbitrary* polynomials.

AMS Subject Classification: 65D30, 65C05, 11K06.

1 Introduction

We study the problem of approximating the s-dimensional integral $I_s(F) := \int_{[0,1]^s} F(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}$ of a function F by a quasi-Monte Carlo (QMC) rule $Q_{N,s}(F) := \frac{1}{N}\sum_{n=0}^{N-1} F(\boldsymbol{x}_n)$ using N points $\{\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{N-1}\}$ from the unit-cube $[0,1)^s$.

In this paper, we assume that the integrand F lies in a certain weighted reproducing kernel Hilbert space. This space of functions, first introduced in [7], is based on Walsh functions which are defined as follows (for more information on Walsh functions, see, e.g., [1]).

Definition 1 *Let $p \geq 2$ be an integer. For a non-negative integer k with base p representation $k = \kappa_0 + \kappa_1 p + \cdots + \kappa_a p^a$ with $\kappa_i \in \{0,\ldots,p-1\}$, we define the Walsh function ${}_p\mathrm{wal}_k : [0,1) \to \mathbb{C}$ by*

$${}_p\mathrm{wal}_k(x) := \mathrm{e}^{2\pi \mathtt{i}(x_1\kappa_0+\cdots+x_{a+1}\kappa_a)/p},$$

for $x \in [0,1)$ with base p representation $x = \frac{x_1}{p} + \frac{x_2}{p^2} + \cdots$ (unique in the sense that infinitely many of the x_i must be different from $p-1$).

For dimension $s \geq 2$ and vectors $\boldsymbol{k} = (k_1,\ldots,k_s) \in \mathbb{N}_0^s$ and $\boldsymbol{x} = (x_1,\ldots,x_s) \in [0,1)^s$ we define ${}_p\mathrm{wal}_{\boldsymbol{k}} : [0,1)^s \to \mathbb{C}$ by

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

If the choice of p is clear from the context we simply write wal_k *or* $\mathrm{wal}_{\boldsymbol{k}}$.

*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"

Let $\alpha > 1$, $s \geq 1$, and $p \geq 2$ be fixed. We consider functions in a weighted Hilbert space $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$, where $\boldsymbol{\gamma} = (\gamma_j)_{j=1}^{\infty}$ is a sequence of real positive weights. The idea of assigning weights to the coordinates in order to model different influence on the integration error was introduced by Sloan and Woźniakowski [22]. The Hilbert space $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ is the tensor product of spaces $H_{\mathrm{wal},\gamma_1}, \ldots, H_{\mathrm{wal},\gamma_s}$ of univariate functions (see, e.g., [5, 7] for more details on the spaces $H_{\mathrm{wal},\gamma_j}$ of univariate functions). Every function F in the tensor product space $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ can be written as

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{k} \in \mathbb{N}_0^s} \widehat{F}_{\mathrm{wal}}(\boldsymbol{k}) \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}), \text{ where } \widehat{F}_{\mathrm{wal}}(\boldsymbol{k}) := \int_{[0,1]^s} F(\boldsymbol{x}) \overline{\mathrm{wal}_k(\boldsymbol{x})} \, \mathrm{d}\boldsymbol{x}.$$

For a natural number with p-adic expansion $k = \kappa_0 + \kappa_1 p + \cdots + \kappa_a p^a$, with $\kappa_a \neq 0$, let $\psi_p(k) := a$. We define

$$r(\alpha, \gamma, k) := \begin{cases} 1 & \text{if } k = 0, \\ \gamma p^{-\alpha \psi_p(k)} & \text{otherwise,} \end{cases}$$

and, for $\boldsymbol{k} = (k_1, \ldots, k_s)$, we define $r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k}) := \prod_{i=1}^{s} r(\alpha, \gamma_i, k_i)$.

Then the inner product in $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ is defined as

$$\langle F, G \rangle_{\mathrm{wal},s,\boldsymbol{\gamma}} = \sum_{\boldsymbol{k} \in \mathbb{N}_0^s} r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k})^{-1} \widehat{F}_{\mathrm{wal}}(\boldsymbol{k}) \overline{\widehat{G}_{\mathrm{wal}}(\boldsymbol{k})}$$

and the norm is given by $\|F\|_{\mathrm{wal},s,\boldsymbol{\gamma}} := \langle F, F \rangle_{\mathrm{wal},s,\boldsymbol{\gamma}}^{1/2}$.

It can easily be verified that $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ is a reproducing kernel Hilbert space (see [7]).

For approximating the integral of a function $F \in H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ by a QMC rule, it is known (see again [7]) that a suitable choice of the point set $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ used in the integration rule are so-called (t, m, s)-nets. A detailed theory on this topic was developed in [14, 16]. For a recent survey article see [18].

A special construction of (t, m, s)-nets in base p was proposed by Niederreiter in [15] (see also [16, Chapter 4.4]). Let p be a prime and let $\mathbb{F}_p$ be the finite field consisting of p elements. Further, let $\mathbb{F}_p((x^{-1}))$ be the field of formal Laurent series over $\mathbb{F}_p$ with elements of the form

$$L = \sum_{l=w}^{\infty} t_l x^{-l},$$

where w is an arbitrary integer and all $t_l \in \mathbb{F}_p$. Note that the field of rational functions is a subfield of $\mathbb{F}_p((x^{-1}))$. We further denote by $\mathbb{F}_p[x]$ the set of all polynomials over $\mathbb{F}_p$. For a given integer $m \geq 1$ and dimension $s \geq 2$, choose $f \in \mathbb{F}_p[x]$ with $\deg(f) = m$, and let $g_1, \ldots, g_s \in \mathbb{F}_p[x]$. We define the map $\phi_m : \mathbb{F}_p((x^{-1})) \to [0, 1)$ by

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

Let $n \in \{0, 1, \ldots, p^m - 1\}$ with p-adic expansion $n = n_0 + n_1 p + \cdots + n_{m-1} p^{m-1}$. With such an n we associate the polynomial

$$n(x) = \sum_{k=0}^{m-1} n_k x^k \in \mathbb{F}_p[x].$$

Then the point set $P(\boldsymbol{g}, f)$ is defined as the collection of the p^m points

$$\boldsymbol{x}_n = \left(\phi_m\left(\frac{n(x)g_1(x)}{f(x)}\right), \ldots, \phi_m\left(\frac{n(x)g_s(x)}{f(x)}\right)\right) \in [0,1)^s,$$

for $0 \leq n \leq p^m - 1$. Due to the construction principle, $P(\boldsymbol{g}, f)$ is often called a polynomial lattice and a QMC rule using the point set $P(\boldsymbol{g}, f)$ is often called a polynomial lattice rule (modulo f). The vector $\boldsymbol{g}$ is called the generating vector of $P(\boldsymbol{g}, f)$ or the generating vector of the polynomial lattice (rule), depending on the context. Note that the generating vectors $\boldsymbol{g}$ in the construction principle for polynomial lattice points can be restricted to the set

$$\boldsymbol{g} \in G_{p,m}^s := \{h \in \mathbb{F}_p[x] : \deg(h) < m\}^s,$$

which is what we will assume in the following.

Using a more general terminology, the construction principle for polynomial lattice rules outlined here yields polynomial lattice rules of rank 1. For the precise definition of the rank of polynomial lattice rules, see, for example, [11, 13]. We refer the interested reader to a number of further papers in which polynomial lattice rules in different settings are studied [3, 4, 9, 10, 11, 12, 13, 17, 19].

If we use a point set P with N points for QMC-integration of functions from $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$, we define the worst-case error by

$$e_{N,s}(P) := \sup_{\substack{F \in H_{\mathrm{wal},s,\boldsymbol{\gamma}} \\ \|F\|_{\mathrm{wal},s,\boldsymbol{\gamma}} \leq 1}} \left| I_s(F) - Q_{N,s}(F) \right|.$$

In this paper we study the worst-case integration error of polynomial lattice rules. In [5], Dick, Pillichshammer, Kuo and Sloan studied the construction of polynomial lattice rules for those cases where f is an irreducible polynomial over $\mathbb{F}_p$. Here, we wish to generalize their results to the case where f is not necessarily an irreducible but an arbitrary polynomial over $\mathbb{F}_p$. In particular, we are going to give an existence result for polynomial lattice rules modulo arbitrary polynomials with small worst-case integration error. Furthermore, we outline a component-by-component (CBC) construction of polynomial lattices such that their worst-case error is small. The idea of a CBC construction of point sets with low worst-case integration error is mainly due to Sloan and his collaborators, see, for example [8, 20, 21].

In [5], the authors also studied the integration of functions in certain Sobolev spaces (see [5, 7]) and gave construction algorithms for randomized polynomial lattice rules modulo irreducible polynomials with low mean square worst-case integration error with respect to these function spaces. We remark that our general results for the Hilbert space $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ can easily be transferred to the case of Sobolev spaces as well.

2 Preliminaries

We summarize some notation and results that will be needed throughout the paper. Here and in the following section we always assume p is a prime. For arbitrary $\boldsymbol{k} = (k_1, \ldots, k_s)$ and $\boldsymbol{g} = (g_1, \ldots, g_s)$ in $\mathbb{F}_p[x]^s$, we define the vector product

$$\boldsymbol{k} \cdot \boldsymbol{g} := \sum_{i=1}^{s} k_i g_i.$$

and we write $g \equiv 0 \bmod f$ if f divides g in $\mathbb{F}_p[x]$. Furthermore, we define for $f \in \mathbb{F}_p[x]$, $\deg(f) = m$,

$$G^*_{p,m}(f) := \{h \in \mathbb{F}_p[x] : \deg(h) < m, \gcd(h, f) = 1\}.$$

For $f, g \in \mathbb{F}_p[x]$ we write from now on simply (f, g) instead of $\gcd(f, g)$ for the greatest common divisor of f and g.

Further, as above, we often associate a nonnegative integer $k = \kappa_0 + \kappa_1 p + \cdots + \kappa_l p^l$ with the polynomial $k(x) = \kappa_0 + \kappa_1 x + \cdots + \kappa_l x^l \in \mathbb{F}_p[x]$ and vice versa. In this sense we have $\psi_p(k) = \deg(k)$.

The following lemma was shown in [5].

Lemma 1 *Let $f \in \mathbb{F}_p[x]$, $\deg(f) = m$, and let $\boldsymbol{g} \in G^s_{p,m}$. Then the squared worst-case error for integration in $H_{\mathrm{wal},s,\boldsymbol{\gamma}}$ using the polynomial lattice $P(\boldsymbol{g}, f)$ satisfies the equation*

$$e^2_{p^m,s}(P(\boldsymbol{g}, f)) = \sum_{\boldsymbol{k} \in \mathcal{D}} r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k}),$$

where $\mathcal{D} := \{\boldsymbol{k} \in \mathbb{F}_p[x]^s \setminus \{\boldsymbol{0}\} : \boldsymbol{k} \cdot \boldsymbol{g} \equiv 0 \bmod f\}$ is the so-called dual net (or dual polynomial lattice) of $P(\boldsymbol{g}, f)$.

The question remains how the sum over all $\boldsymbol{k} \in \mathcal{D}$ can be computed or at least bounded effectively, such that we can search for polynomial lattices with low worst-case integration error. The following lemma gives an answer to this problem, provided that the generating vector $\boldsymbol{g}$ satisfies some additional conditions.

Lemma 2 *Let $P(\boldsymbol{g}, f)$ be a polynomial lattice modulo $f \in \mathbb{F}_p[x]$, $\deg(f) = m$, with generating vector $\boldsymbol{g} \in (G^*_{p,m}(f))^s$. Then*

$$\sum_{\boldsymbol{k} \in \mathcal{D}} r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k}) \le \frac{1}{p^{\alpha m}} \prod_{i=1}^{s} (1 + 2c_{p,\alpha}\gamma_i) + \sum_{\boldsymbol{k} \in \mathcal{D}^*} r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k}),$$

where $c_{p,\alpha} := \frac{p-1}{1-p^{1-\alpha}}$ and $\mathcal{D}^* := \left\{\boldsymbol{k} \in G^s_{p,m} \setminus \{\boldsymbol{0}\} : \boldsymbol{k} \cdot \boldsymbol{g} \equiv 0 \bmod f\right\}$.

Proof. The result follows by the first part of the proof of Lemma 2 in [2], Lemma 4.40 in [16], and by noting that the generating matrices of $P(\boldsymbol{g}, f)$ are regular provided that $\boldsymbol{g} \in (G^*_{p,m}(f))^s$. □

Lemma 2 implies that if one wants to obtain upper bounds on the worst-case integration error of $P(\boldsymbol{g}, f)$ with $\deg(f) = m$ and $\boldsymbol{g} \in (G^*_{p,m}(f))^s$, it is sufficient to consider the term $\sum_{\boldsymbol{k} \in \mathcal{D}^*} r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k})$.

For short, we denote the sum $\sum_{\boldsymbol{k} \in \mathcal{D}^*} r(\alpha, \boldsymbol{\gamma}, \boldsymbol{k})$ by $S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f)$ in the following. Using the same arguments as in [6, Section 4] one can show that

$$S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f) = -1 + \frac{1}{|P(\boldsymbol{g}, f)|} \sum_{\boldsymbol{x} \in P(\boldsymbol{g}, f)} \prod_{i=1}^{s} \chi_{p,m,\gamma_i}(x_i)$$

where $\boldsymbol{x} = (x_1, \ldots, x_s)$ and for any $x = \xi_1/p + \xi_2/p^2 + \cdots$ and $\gamma > 0$ we have

$$\chi_{p,m,\gamma}(x) = \begin{cases} 1 + \frac{\gamma}{p^{(\alpha-1)(i_0-1)}} \left(c_{p,\alpha}(p^{(i_0-1)(\alpha-1)} - 1) - 1\right) & \text{if } \xi_1 = \cdots = \xi_{i_0-1} = 0 \text{ and} \\ & \xi_{i_0} \neq 0 \text{ with } 1 \le i_0 \le m, \\ 1 + \frac{\gamma}{p^{(\alpha-1)m}} c_{p,\alpha}(p^{m(\alpha-1)} - 1) & \text{otherwise,} \end{cases}$$

where $c_{p,\alpha}$ is as in Lemma 2. Hence $S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f)$ can be computed in $O(sp^m)$ operations.

3 Existence Results and Construction Algorithms for Polynomial Lattices Modulo Arbitrary Polynomials

The following lemma gives, for a polynomial $f \in \mathbb{F}_p[x]$ with $\deg(f) = m$, a bound on the average of $S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f)$ over all vectors $\boldsymbol{g} \in (G^*_{p,m}(f))^s$. From this result we are going to deduce that polynomial lattice rules with "low" worst-case error must exist.

Lemma 3 *Let $m \geq 1$, $s \geq 2$, and $f \in \mathbb{F}_p[x]$ with* $\deg(f) = m$*. Then*

$$\frac{1}{\left|G^*_{p,m}(f)\right|^s} \sum_{\boldsymbol{g} \in (G^*_{p,m}(f))^s} S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f) \leq \frac{2}{p^m} \left(\prod_{i=1}^{s} (1 + \gamma_i c_{p,\alpha}) - 1 \right),$$

where $c_{p,\alpha}$ is defined as in Lemma 2.

Proof. The proof is based on ideas from [16, Proof of Theorem 4.43]. Without loss of generality, we may assume that f is monic. First observe that $\left|G^*_{p,m}(f)\right| = \phi_p(f)$, where $\phi_p(f)$ is the analogue of Euler's totient function for the field $\mathbb{F}_p[x]$ (cf. [16, p. 77]). We have

$$\begin{aligned} M_s(f) &:= \frac{1}{\left|G^*_{p,m}(f)\right|^s} \sum_{\boldsymbol{g} \in (G^*_{p,m}(f))^s} S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f) \\ &= \frac{1}{(\phi_p(f))^s} \sum_{\boldsymbol{g} \in (G^*_{p,m}(f))^s} \sum_{\substack{\boldsymbol{h} \in G^s_{p,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{g} \cdot \boldsymbol{h} \equiv 0 \bmod f}} \prod_{i=1}^{s} r(\alpha, \gamma_i, h_i) \\ &= \frac{1}{(\phi_p(f))^s} \sum_{\boldsymbol{h} \in G^s_{p,m} \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{s} r(\alpha, \gamma_i, h_i) \sum_{\substack{\boldsymbol{g} \in (G^*_{p,m}(f))^s \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 \bmod f}} 1. \end{aligned}$$

If $\boldsymbol{h} = \boldsymbol{0}$, then $\prod_{i=1}^{s} r(\alpha, \gamma_i, h_i) = 1$ and

$$\sum_{\substack{\boldsymbol{g} \in (G^*_{p,m}(f))^s \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 \bmod f}} 1 = \left|G^*_{p,m}\right|^s = (\phi_p(f))^s.$$

Therefore,

$$M_s(f) = \left(\frac{1}{(\phi_p(f))^s} \sum_{\boldsymbol{h} \in G^s_{p,m}} \prod_{i=1}^{s} r(\alpha, \gamma_i, h_i) \sum_{\substack{\boldsymbol{g} \in (G^*_{p,m}(f))^s \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 \bmod f}} 1 \right) - 1.$$

For all $\boldsymbol{h} \in G^s_{p,m}$,

$$\sum_{\substack{\boldsymbol{g} \in (G^*_{p,m}(f))^s \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 \bmod f}} 1 = \sum_{\boldsymbol{g} \in (G^*_{p,m}(f))^s} p^{-m} \sum_{v \in G_{p,m}} X_p \left(\frac{v}{f} \boldsymbol{h} \boldsymbol{g} \right),$$

where X_p is defined as in [16, p. 78]. We obtain

$$\begin{aligned}
&\sum_{\boldsymbol{h}\in G_{p,m}^s} \prod_{i=1}^{s} r(\alpha,\gamma_i,h_i) \sum_{\substack{\boldsymbol{g}\in (G_{p,m}^*(f))^s \\ \boldsymbol{h}\cdot\boldsymbol{g}\equiv 0 \bmod f}} 1 \\
&= \sum_{\boldsymbol{h}\in G_{p,m}^s} \prod_{i=1}^{s} r(\alpha,\gamma_i,h_i) \frac{1}{p^m} \sum_{\boldsymbol{g}\in (G_{p,m}^*(f))^s} \sum_{v\in G_{p,m}} X_p\left(\frac{v}{f}\boldsymbol{hg}\right) \\
&= \frac{1}{p^m} \sum_{v\in G_{p,m}} \sum_{\boldsymbol{h}\in G_{p,m}^s} \sum_{\boldsymbol{g}\in (G_{p,m}^*(f))^s} X_p\left(\frac{v}{f}\boldsymbol{hg}\right) \prod_{i=1}^{s} r(\alpha,\gamma_i,h_i) \\
&= \frac{1}{p^m} \sum_{v\in G_{p,m}} \prod_{i=1}^{s} Y^{(i)}(v,f),
\end{aligned}$$

with

$$Y^{(i)}(v,f) = \sum_{h\in G_{p,m}} \sum_{g\in G_{p,m}^*(f)} X_p\left(\frac{v}{f}hg\right) r(\alpha,\gamma_i,h).$$

Now

$$Y^{(i)}(0,f) = \phi_p(f) \sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h);$$

thus

$$\begin{aligned}
&\sum_{\boldsymbol{h}\in G_{p,m}^s} \prod_{i=1}^{s} r(\alpha,\gamma_i,h_i) \sum_{\substack{\boldsymbol{g}\in (G_{p,m}^*(f))^s \\ \boldsymbol{h}\cdot\boldsymbol{g}\equiv 0 \bmod f}} 1 \\
&= \frac{1}{p^m}(\phi_p(f))^s \prod_{i=1}^{s} \left(\sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h) \right) + \frac{1}{p^m} \sum_{\substack{v\in G_{p,m} \\ v\neq 0}} \prod_{i=1}^{s} Y^{(i)}(v,f).
\end{aligned}$$

Let μ_p be the Möbius function on the multiplicative semigroup S_p of monic polynomials over $\mathbb{F}_p$. Note that μ_p is multiplicative. For fixed $v \in \mathbb{F}_p[x]$ with $0 \leq \deg(v) < m$ we obtain

$$\begin{aligned}
Y^{(i)}(v,f) &= \sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h) \sum_{g\in G_{p,m}} X_p\left(\frac{v}{f}hg\right) \sum_{l|(g,f)} \mu_p(l) \\
&= \sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h) \sum_{l|f} \mu_p(l) \sum_{\substack{g\in G_{p,m} \\ l|g}} X_p\left(\frac{v}{f}hg\right) \\
&= \sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h) \sum_{l|f} \mu_p(l) \sum_{a\in G_{p,\deg(f/l)}} X_p\left(\frac{v}{f}hal\right) \\
&= \sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h) \sum_{l|f} \mu_p\left(\frac{f}{l}\right) \sum_{a\in G_{p,\deg(l)}} X_p\left(\frac{v}{f}ha\right),
\end{aligned}$$

where, in the last step, we changed l into f/l. Applying [16, (4.51)] to the innermost sum, we obtain

$$\begin{aligned} Y^{(i)}(v,f) &= \sum_{h \in G_{p,m}} r(\alpha, \gamma_i, h) \sum_{\substack{l|f \\ l|vh}} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \\ &= \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \sum_{\substack{h \in G_{p,m} \\ l|vh}} r(\alpha, \gamma_i, h). \end{aligned}$$

Now l divides vh if and only if $l/(l,v)$ divides h; thus

$$Y^{(i)}(v,f) = \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} E^{(i)}\left(\frac{l}{(l,v)}, f\right),$$

where, for an $a \in S_p$ dividing f, we put

$$E^{(i)}(a,f) = \sum_{\substack{h \in G_{p,m} \\ a|h}} r(\alpha, \gamma_i, h).$$

If $a = f$, then $E^{(i)}(a,f) = r(\alpha, \gamma_i, 0) = 1$. Now let $a \neq f$; then

$$E^{(i)}(a,f) = 1 + \sum_{\substack{b \in G_{p,\deg(f/a)} \\ b \neq 0}} r(\alpha, \gamma_i, ab).$$

We have

$$\begin{aligned} \sum_{\substack{b \in G_{p,\deg(f/a)} \\ b \neq 0}} r(\alpha, \gamma_i, ab) &= \gamma_i \sum_{\substack{b \in G_{p,\deg(f/a)} \\ b \neq 0}} p^{-\alpha \deg(ab)} \\ &= \gamma_i p^{-\alpha \deg(a)} \sum_{\substack{b \in G_{p,\deg(f/a)} \\ b \neq 0}} p^{-\alpha \deg(b)} \\ &= \gamma_i p^{-\alpha \deg(a)} (p-1) \sum_{k=0}^{\deg(f/a)-1} \left(p^{(1-\alpha)}\right)^k \\ &= \gamma_i p^{-\alpha \deg(a)} (p-1) \frac{p^{(1-\alpha)\deg(f/a)} - 1}{p^{1-\alpha} - 1}. \end{aligned}$$

Note that, if $a = f$, then $\deg(f/a) = \deg(1) = 0$, so in this case

$$\frac{p^{(1-\alpha)\deg(f/a)} - 1}{p^{1-\alpha} - 1} = 0.$$

Thus, for all $a \in S_p$ dividing f, we have

$$E^{(i)}(a,f) = 1 + \gamma_i p^{-\alpha \deg(a)} (p-1) \frac{p^{(1-\alpha)\deg(f/a)} - 1}{p^{1-\alpha} - 1}.$$

Applying this formula with $a = \frac{l}{(l,v)}$, we obtain

$$\begin{aligned}
Y^{(i)}(v,f) &= \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \left(1 + \gamma_i p^{-\alpha\deg(l/(l,v))}(p-1)\frac{p^{(1-\alpha)(m-\deg(l/(l,v)))}-1}{p^{1-\alpha}-1}\right) \\
&= \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \left(1 + \gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{-\alpha\deg(l/(l,v))} p^{(1-\alpha)(m-\deg(l/(l,v)))}\right. \\
&\quad \left. -\gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{-\alpha\deg(l/(l,v))}\right) \\
&= \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \left(1 + \gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{(1-\alpha)m-\deg(l/(l,v))}\right. \\
&\quad \left. -\gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{-\alpha\deg(l/(l,v))}\right) \\
&= \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} + \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{(1-\alpha)m} p^{-\deg(l/(l,v))} \\
&\quad - \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg(l)} \gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{-\alpha\deg(l/(l,v))} \\
&= \phi_p(f) + \gamma_i \frac{p-1}{p^{1-\alpha}-1} p^{(1-\alpha)m} \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg((l,v))} \\
&\quad -\gamma_i \frac{p-1}{p^{1-\alpha}-1} \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{(1-\alpha)\deg(l)} p^{\alpha\deg((l,v))}.
\end{aligned}$$

For short we write

$$H(v,f) := \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{(1-\alpha)\deg(l)} p^{\alpha\deg((l,v))}$$

and

$$H^{(1)}(v,f) := \sum_{l|f} \mu_p\left(\frac{f}{l}\right) p^{\deg((l,v))}.$$

From these we can write

$$Y^{(i)}(v,f) = \phi_p(f) - \gamma_i p^{(1-\alpha)m} c_{p,\alpha} H^{(1)}(v,f) + \gamma_i c_{p,\alpha} H(v,f),$$

where $c_{p,\alpha} := \frac{p-1}{1-p^{1-\alpha}}$.

For $v \in \mathbb{F}_p[x]$ with $0 \leq \deg(v) < m$, we have $H^{(1)}(v,f) = 0$ as in [16, pp. 82f.], and so we obtain

$$Y^{(i)}(v,f) = \phi_p(f) + \gamma_i c_{p,\alpha} H(v,f).$$

Thus,

$$\begin{aligned} M_s(f) &= \frac{1}{(\phi_p(f))^s}\left(\frac{1}{p^m}(\phi_p(f))^s\prod_{i=1}^{s}\left(\sum_{h\in G_{p,m}} r(\alpha,\gamma_i,h)\right)\right) \\ &\quad +\frac{1}{p^m}\sum_{\substack{v\in G_{p,m}\\ v\neq 0}}\prod_{i=1}^{s}(\phi_p(f)+\gamma_i c_{p,\alpha}H(v,f))-1 \\ &= \frac{1}{p^m}\prod_{i=1}^{s}E^{(i)}(1,f)+\frac{1}{N}\sum_{\substack{v\in G_{p,m}\\ v\neq 0}}\prod_{i=1}^{s}(1+\gamma_i c_{p,\alpha}J_p(v,f))-\left(1-\frac{1}{p^m}\right)-\frac{1}{p^m}, \end{aligned}$$

where $J_p(v,f) := H(v,f)/\phi_p(f)$. Let us now analyze $H(v,f)$. First note that $H(v,f)$ is multiplicative in f.

In the following, let b be a monic, irreducible polynomial over $\mathbb{F}_p$. We define $e_b(v)$ as the largest integer z such that b^z divides v. From the definition of the Möbius function, it follows that

$$H\left(v,b^k\right) = p^{(1-\alpha)\deg\left(b^k\right)}p^{\alpha\deg\left(\left(b^k,v\right)\right)} - p^{(1-\alpha)\deg\left(b^{k-1}\right)}p^{\alpha\deg\left(\left(b^{k-1},v\right)\right)}.$$

Hence, if $e_b(v)\geq k$, it follows that $H\left(v,b^k\right)=0$. Otherwise, we have

$$H\left(v,b^k\right) = p^{\alpha e_b(v)\deg(b)}p^{(1-\alpha)\deg\left(b^k\right)}\left(1-p^{(\alpha-1)\deg(b)}\right).$$

In the following, we assume $f=b_1^{k_1}\cdots b_t^{k_t}$, where the polynomials b_j are monic, irreducible and pairwise distinct. From our observations, we obtain

$$H(v,f) = \begin{cases} \prod_{j=1}^{t} H\left(v,b_j^{e_{b_j}(f)}\right) & \text{if } e_{b_j}(v) < e_{b_j}(f)\ \forall j=1,\ldots,t, \\ 0 & \text{otherwise.} \end{cases}$$

We now define

$$\begin{aligned} H_i(f) &:= \phi_p(f)^{-i}\sum_{\substack{v\in G_{p,m}\\ v\neq 0}} H(v,f)^i \\ &= \phi_p(f)^{-i}\sum_{\substack{v\in G_{p,m}\\ v\neq 0,\, e_{b_j}(v)<k_j\forall j}}\prod_{j=1}^{t}p^{i\alpha e_{b_j}(v)\deg(b_j)}p^{i(1-\alpha)\deg\left(b_j^{k_j}\right)}\left(1-p^{(\alpha-1)\deg(b_j)}\right)^i \\ &= \phi_p(f)^{-i}\prod_{j=1}^{t}p^{i(1-\alpha)\deg\left(b_j^{k_j}\right)}\left(1-p^{(\alpha-1)\deg(b_j)}\right)^i\sum_{\substack{v\in G_{p,m}\\ v\neq 0,\, e_{b_j}(v)<k_j\forall j}}\prod_{j=1}^{t}p^{i\alpha e_{b_j}(v)\deg(b_j)} \\ &=: \phi_p(f)^{-i}\prod_{j=1}^{t}p^{i(1-\alpha)\deg\left(b_j^{k_j}\right)}\left(1-p^{(\alpha-1)\deg(b_j)}\right)^i\Sigma_*(f). \end{aligned}$$

Now,

$$\begin{aligned}
\Sigma_*(f) &= \sum_{l_1=0}^{k_1-1}\cdots\sum_{l_t=1}^{k_t-1} \sum_{\substack{a\\(a,f)=1\\ \deg(a)<m-\sum_{j=1}^t \deg(b_j^{l_j})}} \prod_{j=1}^t p^{i\alpha\deg\left(b_j^{l_j}\right)}\\
&= \sum_{l_1=0}^{k_1-1}\cdots\sum_{l_t=1}^{k_t-1}\prod_{j=1}^t p^{i\alpha\deg\left(b_j^{l_j}\right)} \sum_{\substack{a\\(a,f)=1\\ \deg(a)<m-\sum_{j=1}^t \deg\left(b_j^{l_j}\right)}} 1.
\end{aligned}$$

We have

$$\sum_{\substack{a\\(a,f)=1\\ \deg(a)<m-\sum_{j=1}^t \deg\left(b_j^{l_j}\right)}} 1 = \phi_p\left(\frac{f}{b_1^{l_1}\cdots b_t^{l_t}}\right) = \prod_{j=1}^t \phi_p\left(b_j^{k_j-l_j}\right).$$

Hence

$$\begin{aligned}
\Sigma_*(f) &= \sum_{l_1=0}^{k_1-1}\cdots\sum_{l_t=1}^{k_t-1}\prod_{j=1}^t p^{i\alpha\deg\left(b_j^{l_j}\right)}\phi_p\left(b_j^{k_j-l_j}\right)\\
&= \sum_{l_1=0}^{k_1-1}\cdots\sum_{l_t=1}^{k_t-1}\prod_{j=1}^t p^{i\alpha\deg\left(b_j^{l_j}\right)} p^{\deg\left(b_j^{k_j-l_j}\right)}\left(1-\frac{1}{p^{\deg(b_j)}}\right)\\
&= \phi_p(f)\sum_{l_1=0}^{k_1-1}\cdots\sum_{l_t=1}^{k_t-1}\prod_{j=1}^t p^{(i\alpha-1)\deg\left(b_j^{l_j}\right)}\\
&= \phi_p(f)\prod_{j=1}^t \frac{p^{(i\alpha-1)\deg\left(b_j^{k_j}\right)}-1}{p^{(i\alpha-1)\deg(b_j)}-1}.
\end{aligned}$$

We arrive at

$$\begin{aligned}
H_i(f) &= \phi_p(f)^{1-i}\prod_{j=1}^t p^{i(1-\alpha)\deg\left(b_j^{k_j}\right)}\left(1-p^{(\alpha-1)\deg(b_j)}\right)^i \frac{p^{(i\alpha-1)\deg\left(b_j^{k_j}\right)}-1}{p^{(i\alpha-1)\deg(b_j)}-1}\\
&= \prod_{j=1}^t p^{\deg\left(b_j^{k_j}\right)(1-i)}\left(1-\frac{1}{p^{\deg(b_j)}}\right)^{1-i} p^{i(1-\alpha)\deg\left(b_j^{k_j}\right)}\\
&\quad\times\left(1-p^{(\alpha-1)\deg(b_j)}\right)^i \frac{p^{(i\alpha-1)\deg\left(b_j^{k_j}\right)}-1}{p^{(i\alpha-1)\deg(b_j)}-1}\\
&= \prod_{j=1}^t \left(1-\frac{1}{p^{\deg(b_j)}}\right)^{1-i}\left(1-p^{(\alpha-1)\deg(b_j)}\right)^i\frac{1}{p^{(i\alpha-1)\deg(b_j)}-1}\\
&\quad\times\prod_{j=1}^t p^{\deg\left(b_j^{k_j}\right)(1-i)} p^{i(1-\alpha)\deg\left(b_j^{k_j}\right)}\left(p^{(i\alpha-1)\deg\left(b_j^{k_j}\right)}-1\right).
\end{aligned}$$

Therefore,

$$|H_i(f)| \leq \prod_{j=1}^{t} \left(1 - \frac{1}{p^{\deg(b_j)}}\right)^{1-i} \left(p^{(\alpha-1)\deg(b_j)} - 1\right)^i \frac{1}{p^{(i\alpha-1)\deg(b_j)} - 1} \leq 1.$$

This means

$$\begin{aligned} \frac{1}{p^m} \sum_{\substack{v \in G_{p,m} \\ v \neq 0}} \prod_{i=1}^{s} (1 + \gamma_i c_{p,\alpha} J_p(v,f)) - (1 - 1/p^m) &= \frac{1}{p^m} \sum_{u \subseteq \{1,\ldots,s\}, u \neq \emptyset} \gamma_u c_{p,\alpha}^{|u|} H_{|u|}(f) \\ &\leq \frac{1}{p^m} \sum_{u \subseteq \{1,\ldots,s\}, u \neq \emptyset} \gamma_u c_{p,\alpha}^{|u|} \\ &= \frac{1}{p^m} \left(\prod_{i=1}^{s} (1 + \gamma_i c_{p,\alpha}) - 1 \right). \end{aligned}$$

On the other hand,

$$\frac{1}{p^m} \prod_{i=1}^{s} E^{(i)}(1,f) - \frac{1}{p^m} \leq \frac{1}{p^m} \left(\prod_{i=1}^{s} (1 + \gamma_i c_{p,\alpha}) - 1 \right).$$

This yields the result. □

Theorem 1 *Let p be prime and $f \in \mathbb{F}_p[x]$ with $\deg(f) = m \geq 1$ and $\alpha > 1$. Then there exists a vector $\boldsymbol{g} \in (G^*_{p,m}(f))^s$ such that*

$$S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f) \leq \frac{2^{1/\lambda}}{p^{m/\lambda}} \left(\prod_{i=1}^{s} (1 + \gamma_i^{\lambda} c_{p,\alpha\lambda}) - 1 \right)^{1/\lambda}$$

for any $1/\alpha < \lambda \leq 1$.

Proof. This result follows from Lemma 3 together with the fact that for all $\lambda \in (1/\alpha, 1]$ we have

$$S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}, f) \leq (S_{\alpha\lambda,\boldsymbol{\gamma}^{\lambda}}(\boldsymbol{g}, f))^{1/\lambda},$$

where $\boldsymbol{\gamma}^{\lambda} = (\gamma_j^{\lambda})_{j \geq 1}$, which in turn follows from Jensen's inequality which states that for a sequence (a_k) of non-negative real numbers we have $(\sum a_k)^{\lambda} \leq \sum a_k^{\lambda}$, for any $0 < \lambda \leq 1$. □

Theorem 1, together with Lemma 1 and Lemma 2, implies the existence of generating vectors $\boldsymbol{g}$ yielding polynomial lattices with squared worst-case integration error of order $p^{-\alpha m + \varepsilon}$ for any $\varepsilon > 0$. Furthermore we remark that the bound on the worst-case error can be made independent of the dimension if $\sum_{i \geq 1} \gamma_i^{\lambda} < \infty$. This is known as strong tractability, see [22]. For a more detailed (strong) tractability discussion of this problem just follow the proof of [5, Corollary 4.5]. Now we introduce an algorithm that provides a way of finding such vectors explicitly. The algorithm is based on a component-by-component construction.

Algorithm 1 *Given a prime number p, a dimension s, an integer $m \geq 1$ and weights $\boldsymbol{\gamma} = (\gamma_j)_{j \geq 1}$.*

1. *Choose a polynomial $f \in \mathbb{F}_p[x]$ with $\deg(p) = m$.*
2. *Set $g_1^* = 1$.*
3. *For $d = 2, 3, \ldots, s$, and $g_1^*, \ldots, g_{d-1}^*$ found in the previous steps, find $g_d^* \in G_{p,m}^*(f)$ by minimizing the quantity $S_{\alpha,\boldsymbol{\gamma}}((g_1^*, \ldots, g_{d-1}^*, g_d), f)$ as a function of g_d.*

Theorem 2 *Let p be prime and $f \in \mathbb{F}_p[x]$ with $\deg(f) = m \geq 1$. Suppose $(g_1^*, \ldots, g_s^*) \in (G_{p,m}^*(f))^s$ is constructed by Algorithm 1. Then for all $d = 1, 2, \ldots, s$ we have*

$$S_{\alpha,\boldsymbol{\gamma}}((g_1^*, \ldots, g_d^*), f) \leq \frac{1}{p^{m/\lambda}} \prod_{i=1}^{d} \left(1 + \gamma_i^\lambda 2 c_{p,\alpha\lambda}\right)^{1/\lambda}$$

for all $\lambda \in (1/\alpha, 1]$.

Proof. Without loss of generality, we may assume that the polynomial f is monic. We prove the result by induction on $d = 1, \ldots, s$.

Since $g_1^* = 1$ and since there is no polynomial $k \in G_{p,m} \setminus \{0\}$ such that $k \equiv 0 \pmod{f}$, it follows that $S_{\alpha,\boldsymbol{\gamma}}(g_1^*, f) = 0$. Hence the bound holds trivially for $d = 1$.

Assume we have already shown that

$$S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}^*, f) \leq \frac{1}{p^{m/\lambda}} \prod_{i=1}^{d} \left(1 + \gamma_i^\lambda 2 c_{p,\alpha\lambda}\right)^{1/\lambda}$$

for $d \geq 1$ and any $1/\alpha < \lambda \leq 1$.

We have

$$\begin{aligned} S_{\alpha,\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}), f) &= \sum_{\substack{(\boldsymbol{k}, k_{d+1}) \in G_{p,m}^{d+1} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g_{d+1} \equiv 0 \pmod{f}}} r(\alpha, \boldsymbol{\gamma}, (\boldsymbol{k}, k_{d+1})) \\ &= S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}^*, f) + \theta(g_{d+1}), \end{aligned}$$

where

$$\theta(g_{d+1}) = \sum_{\substack{(\boldsymbol{k}, k_{d+1}) \in G_{p,m}^{d+1} \\ k_{d+1} \neq 0 \\ \boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g_{d+1} \equiv 0 \pmod{f}}} r(\alpha, \boldsymbol{\gamma}, (\boldsymbol{k}, k_{d+1})).$$

As g_{d+1}^* is chosen such that $S_{\alpha,\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}), f)$ is minimized and since $S_{\alpha,\boldsymbol{\gamma}}(\boldsymbol{g}^*, f)$ is independent of g_{d+1} it follows that for all $g_{d+1} \in G_{p,m}^*(f)$ and all $\lambda > 0$ we have

$$\theta(g_{d+1}^*)^\lambda \leq \theta(g_{d+1})^\lambda$$

and therefore together with Jensen's inequality we obtain for all $1/\alpha < \lambda \le 1$,

$$\begin{aligned}
\theta(g_{d+1}^*) &\le \left(\frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}^*(f)} \theta(g_{d+1})^\lambda\right)^{1/\lambda} \\
&\le \left(\frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}^*(f)} \sum_{\substack{(\boldsymbol{k},k_{d+1}) \in G_{p,m}^{d+1} \\ k_{d+1} \ne 0 \\ \boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g_{d+1} \equiv 0 \pmod f}} r(\alpha\lambda, \boldsymbol{\gamma}^\lambda, (\boldsymbol{k}, k_{d+1}))\right)^{1/\lambda}.
\end{aligned}$$

We now consider

$$\begin{aligned}
M &:= \frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}^*(f)} \sum_{\substack{(\boldsymbol{k},k_{d+1}) \in G_{p,m}^{d+1} \\ k_{d+1} \ne 0 \\ \boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g_{d+1} \equiv 0 \pmod f}} r(\alpha\lambda, \boldsymbol{\gamma}^\lambda, (\boldsymbol{k}, k_{d+1})) \\
&= \frac{1}{\phi_p(f)} \sum_{\substack{(\boldsymbol{k},k_{d+1}) \in G_{p,m}^{d+1} \\ k_{d+1} \ne 0}} \prod_{i=1}^{d+1} r(\alpha\lambda, \gamma_i^\lambda, k_i) \sum_{\substack{g_{d+1} \in G_{p,m}^*(f) \\ \boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g_{d+1} \equiv 0 \pmod f}} 1.
\end{aligned}$$

Since

$$\sum_{\substack{g_{d+1} \in G_{p,m}^*(f) \\ \boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g_{d+1} \equiv 0 \pmod f}} 1 = \sum_{g \in G_{p,m}^*(f)} \frac{1}{p^m} \sum_{v \in G_{p,m}} X_p\left(\frac{v}{f}(\boldsymbol{k}\boldsymbol{g}^* + k_{d+1} g)\right)$$

we have

$$\begin{aligned}
M &= \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{v \in G_{p,m}} \sum_{\boldsymbol{k} \in G_{p,m}^d} r(\alpha\lambda, \boldsymbol{\gamma}^\lambda, \boldsymbol{k}) X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right) \\
&\times \left(\sum_{k \in G_{p,m}} \sum_{g \in G_{p,m}^*(f)} r(\alpha\lambda, \gamma_{d+1}^\lambda, k) X_p\left(\frac{v}{f} kg\right) - \phi_p(f)\right).
\end{aligned}$$

Let

$$Y(v,f) = \sum_{k \in G_{p,m}} \sum_{g \in G_{p,m}^*(f)} r(\alpha\lambda, \gamma_{d+1}^\lambda, k) X_p\left(\frac{v}{f} kg\right).$$

Then we have

$$Y(0,f) = \phi_p(f) \sum_{k \in G_{p,m}} r(\alpha\lambda, \gamma_{d+1}^\lambda, k)$$

and from the proof of Lemma 3 we know that

$$Y(v,f) = \phi_p(f) + \gamma_{d+1}^\lambda c_{p,\alpha\lambda} H(v,f),$$

where

$$H(v,f) = \sum_{l \mid f} \mu_p\left(\frac{f}{l}\right) p^{(1-\alpha\lambda)\deg(l)} p^{\alpha\lambda \deg((l,v))}.$$

Thus

$$\begin{aligned}
M &= -\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})\frac{1}{p^m}\sum_{v\in G_{p,m}} X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)\\
&\quad +\frac{1}{\phi_p(f)}\frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})Y(0,f)\\
&\quad +\frac{1}{\phi_p(f)}\frac{1}{p^m}\sum_{v\in G_{p,m}\setminus\{0\}}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)Y(v,f)\\
&= -\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})\frac{1}{p^m}\sum_{v\in G_{p,m}} X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)+\frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^{d+1}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})\\
&\quad +\frac{1}{p^m}\sum_{v\in G_{p,m}\setminus\{0\}}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)\\
&\quad +\frac{1}{\phi_p(f)}\frac{1}{p^m}\gamma_{d+1}^\lambda c_{p,\alpha\lambda}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})\sum_{v\in G_{p,m}\setminus\{0\}} H(v,f)X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)
\end{aligned}$$

Since

$$\begin{aligned}
&\frac{1}{p^m}\sum_{v\in G_{p,m}\setminus\{0\}}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)\\
&\quad = \sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})\frac{1}{p^m}\sum_{v\in G_{p,m}} X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)-\frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})
\end{aligned}$$

we have

$$M=\frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^{d+1}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})-\frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})+K_p^d(f)$$

where

$$K_p^d(f):=\frac{1}{\phi_p(f)}\frac{1}{p^m}\gamma_{d+1}^\lambda c_{p,\alpha\lambda}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})\sum_{v\in G_{p,m}\setminus\{0\}} H(v,f)X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right).$$

Now we consider

$$T(f):=\frac{1}{\phi_p(f)}\sum_{v\in G_{p,m}\setminus\{0\}} H(v,f)X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right).$$

As $\left|X_p\left(\frac{v}{f}\boldsymbol{k}\boldsymbol{g}^*\right)\right|=1$ for all $v\in G_{p,m}$ we have $|T(f)|\le|H_1(f)|\le 1$ (see the proof of Lemma 3) and therefore we have

$$K_p^d(f)\le\frac{\gamma_{d+1}^\lambda c_{p,\alpha\lambda}}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^d} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k})$$

and

$$\begin{aligned} M &\leq \frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^{d+1}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k}) - \frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^{d}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k}) \\ &\quad + \frac{\gamma_{d+1}^\lambda c_{p,\alpha\lambda}}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^{d}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k}) \\ &= \frac{1}{p^m}\sum_{\boldsymbol{k}\in G_{p,m}^{d}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k}) \left(\sum_{k\in G_{p,m}} r(\alpha\lambda,\gamma_{d+1}^\lambda,k) - 1 + \gamma_{d+1}^\lambda c_{p,\alpha\lambda}\right) \end{aligned}$$

We have

$$\sum_{k\in G_{p,m}} r(\alpha\lambda,\gamma_{d+1}^\lambda,k) \leq 1 + \gamma_{d+1}^\lambda c_{p,\alpha\lambda}$$

and

$$\sum_{\boldsymbol{k}\in G_{p,m}^{d}} r(\alpha\lambda,\boldsymbol{\gamma}^\lambda,\boldsymbol{k}) \leq \prod_{i=1}^d \left(1+\gamma_i^\lambda c_{p,\alpha\lambda}\right)$$

where $c_{p,\alpha\lambda} = \frac{p-1}{1-p^{1-\alpha\lambda}}$. Hence

$$M \leq \frac{1}{p^m}\prod_{i=1}^d \left(1+\gamma_i^\lambda c_{p,\alpha\lambda}\right)\gamma_{d+1}^\lambda 2c_{p,\alpha\lambda}.$$

From the induction hypothesis together with another application of Jensen's inequality we obtain

$$\begin{aligned} S_{\alpha,\boldsymbol{\gamma}}((\boldsymbol{g}^*,g_{d+1}^*),f) &\leq \left(\frac{1}{p^m}\prod_{i=1}^d \left(1+\gamma_i^\lambda 2c_{p,\alpha\lambda}\right)\right)^{1/\lambda} + M^{1/\lambda} \\ &\leq \left(\frac{1}{p^m}\prod_{i=1}^d \left(1+\gamma_i^\lambda 2c_{p,\alpha\lambda}\right) + \frac{1}{p^m}\prod_{i=1}^d \left(1+\gamma_i^\lambda c_{p,\alpha\lambda}\right)\gamma_{d+1}^\lambda 2c_{p,\alpha\lambda}\right)^{1/\lambda} \\ &\leq \frac{1}{p^{m/\lambda}}\prod_{i=1}^{d+1}\left(1+\gamma_i^\lambda 2c_{p,\alpha\lambda}\right)^{1/\lambda}. \end{aligned}$$

□

References

[1] Chrestenson, H.E.: A class of generalized Walsh functions. Pacific J. Math. **5**, 17–31, 1955.

[2] Dick, J., Kritzer, P., and Kuo, F.Y.: Approximation of Functions Using Digital Nets. Preprint, 2006.

[3] Dick, J., Kritzer, P., Leobacher, G. and Pillichshammer, F.: Constructions of general polynomial lattice rules based on the weighted star discrepancy. Finite Fields Appl., to appear, 2007.

[4] Dick, J., Kritzer, P., Pillichshammer, F. and Schmid, W. Ch.: On the existence of higher order polynomial lattices with large figure of merit. Submitted, 2006.

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

[6] Dick, J., Leobacher, G., and Pillichshammer, F.: Construction algorithms for digital nets with small weighted star discrepancy. SIAM J. Numer. Anal. **43**, 149–195.

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

[8] Kuo, F.Y.: Component-by-component constructions achieve the optimal rate of convergence for multivariate integration in weighted Korobov and Sobolev spaces. J. Complexity **19**, 301–320, 2003.

[9] Larcher, G.: Digital point sets: Analysis and applications, in: P. Hellekalek and G. Larcher (Eds.), Random and Quasi-Random Point Sets, Lecture Notes in Statistics vol. 138, Springer, New York, 1998, pp. 167–222.

[10] Larcher, G., Lauss, A., Niederreiter, H. and Schmid, W. Ch.: Optimal polynomials for (t, m, s)-nets and numerical integration of multivariate Walsh series, SIAM Journal on Numerical Analysis **33**, 2239–2253, 1996.

[11] L'Ecuyer, P.: Polynomial integration lattices, in: H. Niederreiter (Ed.), Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer, Berlin, 2004, pp. 73–98.

[12] L'Ecuyer, P. and Lemieux, C.: Recent advances in randomized quasi-Monte Carlo methods, in: M. Dror, P. L'Ecuyer and F. Szidarovszky (Eds.), Modeling Uncertainty: An Examination of Stochastic Theory, Methods, and Applications, Kluwer Academic Publishers, Boston, 2002, pp. 419–474.

[13] Lemieux, C. and L'Ecuyer, P.: Randomized polynomial lattice rules for multivariate integration and simulation, SIAM Journal on Scientific Computing **24**, 1768–1789, 2003.

[14] Niederreiter, H.: Point Sets and Sequences with Small Discrepancy. Monatsh. Math. **104**, 273–337, 1987.

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

[16] Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods, CBMS-NSF Series in Applied Mathematics, **63**, SIAM, Philadelphia, 1992.

[17] Niederreiter, H.: The existence of good extensible polynomial lattice rules, Monatsh. Math. **139**, 295–307, 2003.

[18] Niederreiter, H.: Constructions of (t, m, s)-nets and (t, s)-sequences, Finite Fields Appl. **11**, 578–600, 2005.

[19] Nuyens, D. and Cools, R.: Fast component-by-component constructions, a reprise for different kernels, in: H. Niederreiter, D. Talay (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2004, Springer, Berlin, 2004, pp. 373–378.

[20] Sloan, I.H., Kuo, F.Y., and Joe, S.: Constructing randomly shifted lattice rules in weighted Sobolev spaces. SIAM J. Numer. Anal. **40**, 1650–1655, 2002.

[21] Sloan, I.H., Kuo, F.Y., and Joe, S.: On the step-by-step construction of quasi-Monte Carlo integration rules that achieve strong tractability error bounds in weighted Sobolev spaces. Math. Comp. **71**, 1609–1640, 2002.

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

Authors' Addresses:

Peter Kritzer, Fachbereich Mathematik, Universität Salzburg, Hellbrunnerstr. 34, A-5020 Salzburg, Austria. Email: peter.kritzer@sbg.ac.at

Friedrich Pillichshammer, Institut für Finanzmathematik, Universität Linz, Altenbergerstr. 69, A-4040 Linz, Austria. Email: friedrich.pillichshammer@jku.at