Constructions of general polynomial lattice rules based on the weighted star discrepancy

Josef Dick a,1, Peter Kritzer b,2, Gunther Leobacher c, Friedrich Pillichshammer c,∗,2

a School of Mathematics, University of New South Wales, Sydney 2052, Australia
b Fachbereich Mathematik, Universität Salzburg, Hellbrunnerstraße 34, A-5020 Salzburg, Austria
c Institut für Finanzmathematik, Universität Linz, Altenbergerstraße 69, A-4040 Linz, Austria

Received 24 January 2006; revised 28 August 2006
Available online 16 October 2006
Communicated by Gary L. Mullen

Abstract

In this paper we study construction algorithms for polynomial lattice rules modulo arbitrary polynomials. Polynomial lattice rules are a special class of digital nets which yield well distributed point sets in the unit cube for numerical integration.

Niederreiter obtained an existence result for polynomial lattice rules modulo arbitrary polynomials for which the underlying point set has a small star discrepancy and recently Dick, Leobacher and Pillichshammer introduced construction algorithms for polynomial lattice rules modulo an irreducible polynomial for which the underlying point set has a small (weighted) star discrepancy.

In this work we provide construction algorithms for polynomial lattice rules modulo arbitrary polynomials, thereby generalizing the previously obtained results. More precisely we use a component-by-component algorithm and a Korobov-type algorithm. We show how the search space of the Korobov-type algorithm can be reduced without sacrificing the convergence rate, hence this algorithm is particularly fast. Our findings are based on a detailed analysis of quantities closely related to the (weighted) star discrepancy.

© 2006 Elsevier Inc. All rights reserved.

∗ Corresponding author.
E-mail addresses: josi@maths.unsw.edu.au (J. Dick), peter.kritzer@sbg.ac.at (P. Kritzer), gunther.leobacher@jku.at (G. Leobacher), friedrich.pillichshammer@jku.at (F. Pillichshammer).
1 Supported by the Australian Research Council under its Center of Excellence Program.
2 Supported by the Austrian Science Foundation (FWF) project S9609, that is part of the Austrian National Research Network “Analytic Combinatorics and Probabilistic Number Theory.”
Keywords: Weighted star discrepancy; Digital nets; Polynomial lattice rule

1. Introduction

In many applications, notably numerical integration, point sets with good distribution properties are required. To be more precise, one is frequently concerned with approximating the $s$-dimensional integral of a function $F$,

$$I_s(F) := \int_{[0,1]^s} F(x) \, dx$$

by a quasi-Monte Carlo (QMC) rule of $N$ points,

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

It is well known that point sets with good distribution properties yield a small integration error for certain classes of functions. A well-known error estimate for the integration error is given by the Koksma–Hlawka inequality (see, e.g., [7,10,18]),

$$|I_s(F) - Q_{N,s}(F)| \leq V(F) D^*_N,$$

where $V(F)$ is the variation of $F$ in the sense of Hardy and Krause and $D^*_N$ is the so-called star discrepancy of the point set used for the QMC rule. The star discrepancy of a point set consisting of $N$ points $x_0, x_1, \ldots, x_{N-1}$ in $[0,1)^s$ is defined as

$$D^*_N = D^*_N(x_0, \ldots, x_{N-1}) := \sup_{0 \leq \alpha_i \leq 1, 1 \leq i \leq s} |\Delta(\alpha_1, \ldots, \alpha_s)|.$$

Here, $\Delta(\alpha_1, \ldots, \alpha_s)$ is the discrepancy function,

$$\Delta(\alpha_1, \ldots, \alpha_s) := \frac{A_N(\prod_{i=1}^{s}[0, \alpha_i])}{N} - \alpha_1 \cdots \alpha_s,$$

where $A_N(E)$ denotes the number of indices $n$, $0 \leq n \leq N - 1$, such that $x_n \in E$.

Many constructions of point sets with particularly small star discrepancy are based on the concept of $(t,m,s)$-nets in base $b$. A detailed theory on this topic was developed in Niederreiter [16] (see also [18, Chapter 4], for a recent survey see [20]).

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

A special construction of \((t,m,s)\)-nets was proposed by Niederreiter in [17] (see also [18, 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

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

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

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

for \(0 \leq n \leq p^m - 1\). Due to the construction principle, a QMC rule using the point set \(P(g, f)\) is often called a polynomial lattice rule (modulo \(f\)). The vector \(g\) is called the generating vector of \(P(g, f)\) or the generating vector of the polynomial lattice rule, depending on the context. The polynomial \(f\) is referred to as the modulus.

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, [13,15]. We further refer the reader to several articles in which constructions of polynomial lattice rules and various aspects of their quality are studied [11–15,19].

Apart from the classical concept of the star discrepancy (which we call from now on classical star discrepancy) there is also the idea of the weighted star discrepancy introduced by Sloan and Woźniakowski in [24], who observed that different coordinates may have different influence on the quality of approximation of an integral by a QMC rule. We need some notation that will be used throughout the paper: let \(y = (\gamma_i)_{i \geq 1}\) denote a sequence of positive real numbers, the “weights,” and let \(D = \{1, 2, \ldots, s\}\) be the set of coordinate indices. For \(u \subseteq D\) let \(\gamma_u = \prod_{i \in u} \gamma_i\), \(\gamma_\emptyset = 1\), \(|u|\) be the cardinality of \(u\), and for a vector \(z \in [0, 1)^s\) let \(z_u\) denote the vector in \([0, 1)^{|u|}\) containing only the components of \(z\) whose indices are in \(u\). Moreover we write \((z_u, 1)\) for the vector that we obtain by replacing all the components of \(z\) not in \(u\) by 1. Now for a point set
\( x_0, \ldots, x_{N-1} \) in \([0, 1)^s\) and a sequence \( \gamma = (\gamma_i)_{i \geq 1} \) of weights the weighted star discrepancy \( D^*_N, \gamma \) is given by

\[
D^*_N, \gamma = D^*_N, \gamma (x_0, \ldots, x_{N-1}) := \sup_{z \in [0,1)^s} \max_{u \subseteq D, u \neq \emptyset} \gamma_u \left| \Delta(z_u, 1) \right|
\]

(Note that for the choice \( \gamma = 1 \), that is, \( \gamma_i = 1 \) for all \( i \geq 1 \), we have \( D^*_N, 1 = D^*_N \) from above, since in this case the maximum in the definition of weighted star discrepancy is always attained for \( u = D \).)

Sloan and Woźniakowski showed a weighted version of the Koksma–Hlawka inequality for all functions in the Sobolev space \( W^{(1, \ldots, 1)}_2([0,1)^s) \),

\[
\left| I_s(F) - Q_{N,s}(F) \right| \leq D^*_N, \gamma \| F \|_{s, \gamma},
\]

where the norm is defined as

\[
\| F \|_{s, \gamma} := \sum_{u \subseteq D} \gamma_u^{-1} \int_{[0,1)^{|u|}} \left| \frac{\partial |u|}{\partial x_u} F(x_u, 1) \right| dx_u.
\]

Hence, point sets with small weighted star discrepancy guarantee a small worst-case error for numerical integration in weighted spaces.

We are interested in finding point sets with small weighted star discrepancy on the one hand, and small (classical) star discrepancy on the other hand. It has been shown (see [18]) that for a given polynomial \( f \) there always exists a vector of polynomials \( g \) such that \( P(g, f) \) has small star discrepancy by averaging over all possible choices of \( g \). This result was made “more explicit” in the recent paper [5] where the authors showed that such vectors \( g \) can be found by computer search: more precisely, a component-by-component and a Korobov construction algorithm for polynomial lattice rules were introduced. Furthermore, the results for the classical star discrepancy were extended to the weighted star discrepancy. However, the results in [5] are limited to the case where \( f \) is an irreducible polynomial.

In this paper, it is our aim to show results for the case where \( f \) is not necessarily an irreducible polynomial. We first show an average-type result which is similar to a result for the unweighted case due to Niederreiter [18]. We then show how the generating vector for point sets \( P(g, f) \), which are at least as good as average in terms of the weighted star discrepancy, can be found by computer search. We show that this can be achieved by a component-by-component construction and a Korobov-type construction. While our average-type result and our results on the component-by-component construction hold for arbitrary choices of \( f \), the results in the Korobov case are limited to the case where \( f \) is the product of different monic irreducible polynomials. The search space in this case is on the other hand much smaller. Usually, for finding \( p^m \) points one needs a search space with the number of elements of order \( O(p^m) \), but here, in case \( f \) is the product of two monic irreducible polynomials of degree \( m_1 \) and \( m_2 \), the search space has a number of elements of order \( O(p^{m_1} + p^{m_2}) \), where \( m = m_1 + m_2 \). Such types of algorithms have been proposed in [2,3], but therein the upper bounds on the worst-case error are not as good as for a full search. In our case though, the convergence rate is the same as for the full search of the component-by-component algorithm (this is not the case in [25] where the worst-case error
in some reproducing kernel Hilbert space has been considered) but with a little bit stronger dependence on the dimension, which is typical for Korobov type algorithms. The technical reason for this is that we do not rely on Jensen’s inequality for our proofs. We also show that one can use a product of more than two irreducible polynomials and thereby reduce the size of the search space even further. This yields a considerable speedup of the construction algorithm allowing us to search for polynomial lattice rules in high dimensions and a large number of points (compare also to the fast component-by-component algorithm for lattice rules in [21–23]).

Our paper is structured as follows. In the subsequent section we introduce the necessary notation and some preliminary results, whereas in Section 3 we introduce and analyze the construction algorithms. We conclude the paper with a discussion in Section 4.

2. Preliminaries

We shortly summarize some notation and results that will be needed throughout the paper. For arbitrary \( k = (k_1, \ldots, k_r)^T \), \( g = (g_1, \ldots, g_r)^T \in (\mathbb{F}_p[x])^r \), we define the vector product

\[
k \cdot g = \sum_{i=1}^{r} k_i g_i
\]

and we write \( g \equiv 0 \pmod{f} \) if \( f \) divides \( g \) in \( \mathbb{F}_p[x] \). Further, as above, we often associate a non-negative integer \( \kappa = \kappa_0 + \kappa_1 p + \cdots + \kappa_r p^r \) with the polynomial \( \kappa(x) = \kappa_0 + \kappa_1 x + \cdots + \kappa_r x^r \in \mathbb{F}_p[x] \) and vice versa.

In what follows, let \( p \) be prime, \( m \geq 1 \), and \( s \geq 2 \). Let

\[
G_{p,m} := \{ h \in \mathbb{F}_p[x]: \deg(h) < m \}.
\]

For \( h \in G_{p,m} \), let

\[
r_p(h) := \begin{cases} 
1 & \text{if } h = 0, \\
\frac{1}{p^{s+1} \sin^2 \left( \frac{\pi}{p} \kappa_s \right)} & \text{if } h = \kappa_0 + \kappa_1 x + \cdots + \kappa_s x^s, \kappa_s \neq 0.
\end{cases}
\]

Furthermore, define, for \( f \in \mathbb{F}_p[x] \), \( \deg(f) = m \),

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

It is obviously true that

\[
G_{p,m}^*(f) \subseteq G_{p,m}.
\]

Let \( f \in \mathbb{F}_p[x] \), \( \deg(f) = m \), \( g \in (G_{p,m}^*(f))^s \). Define

\[
R(g, f) := \sum_{h \in G_{p,m}^*(f) \setminus \{0\}} \prod_{i=1}^{s} r_p(h_i) \cdot \prod_{h \cdot g \equiv 0 \pmod{f}}.
\]

We have
Proposition 1. Let \( f \in \mathbb{F}_p[x] \), \( \deg(f) = m \), \( g \in (G_{p,m}^*)^s \). Then for the star discrepancy \( D_N^*(g, f) \) of \( P(g, f) \) we have

\[
D_N^*(g, f) \leq 1 - \left( 1 - \frac{1}{N} \right)^s + R(g, f) \leq \frac{s}{N} + R(g, f),
\]

(2)

where \( N = p^m \).

Proof. The assertion follows by [5, Proposition 2.1] and (1). \( \square \)

We can also define the analogue of \( R(g, f) \) for the weighted case. For \( u \subseteq D \), \( u \neq \emptyset \), define \( g_u := (g_j)_{j \in u} \) and

\[
R(g_u, f) := \sum_{h \in G_{p,m}^* \setminus \{0\} \atop h \cdot g_u \equiv 0 \pmod{f}} \prod_{i=1}^{[u]} r_p(h_i).
\]

Moreover, we put

\[
\tilde{R}(g, f) := \sum_{u \subseteq D \atop u \neq \emptyset} \gamma_u R(g_u, f).
\]

It was shown in [5] that

\[
\tilde{R}(g, f) = \sum_{h \in G_{p,m}^* \setminus \{0\} \atop h \cdot g \equiv 0 \pmod{f}} \prod_{i=1}^{s} \tilde{r}_p(h_i, \gamma_i),
\]

with

\[
\tilde{r}_p(h, \gamma) := \begin{cases} 
1 + \gamma & \text{if } h = 0, \\
\gamma r_p(h) & \text{if } h \neq 0.
\end{cases}
\]

For the weighted star discrepancy \( D_{N,\gamma}^* \) of a point set \( x_0, \ldots, x_{N-1} \) in \([0, 1]^s\) it easily follows from the definition that

\[
D_{N,\gamma}^* \leq \sum_{u \subseteq D \atop u \neq \emptyset} \gamma_u D_N^*(u),
\]

where \( D_N^*(u) \) denotes the star discrepancy of the projection of the point set \( x_0, \ldots, x_{N-1} \) to the coordinates given by \( u \). Proposition 1 yields

\[
D_N^*(u) \leq 1 - \left( 1 - \frac{1}{N} \right)^{[u]} + R(g_u, f).
\]
Consequently, we get for the weighted star discrepancy $D^*_N,\gamma$ of the point set $P(g, f)$,

$$D^*_N,\gamma(g, f) \leq \sum_{u \subseteq D \atop u \neq \emptyset} \gamma_u \left( 1 - \left(1 - \frac{1}{N}\right)^{|u|} \right) + \tilde{R}_\gamma(g, f). \quad (3)$$

Equations (2) and (3) show that the quantity $R(g, f)$ (or $\tilde{R}_\gamma(g, f)$, respectively) is intimately related to the (weighted) star discrepancy of the point set $P(g, f)$. In order to obtain upper bounds on the weighted or classical star discrepancy it suffices to obtain upper bounds on $R(g, f)$ and $\tilde{R}_\gamma(g, f)$. This is what we will be concerned with in the next section. But first we show how the quantities $R(g, f)$ and $\tilde{R}_\gamma(g, f)$ can be computed effectively. Let $x = (x_1, \ldots, x_s)$, $f \in \mathbb{F}_p[x]$ with $\deg(f) = m$, and $g \in (G^*_{p,m}(f))^s$. In [5, Section 4] it is shown that

$$R(g, f) = -1 + \frac{1}{|P(g, f)|} \sum_{x \in P(g, f)} \prod_{i=1}^{s} \phi_{p,m}(x_i)$$

and

$$\tilde{R}_\gamma(g, f) = -\prod_{i=1}^{s} (1 + \gamma_i) + \frac{1}{|P(g, f)|} \sum_{x \in P(g, f)} \prod_{i=1}^{s} (1 + \gamma_i \phi_{p,m}(x_i)), \quad (4)$$

where for $t = t_1/p + t_2/p^2 + \cdots + t_m/p^m$,

$$\phi_{p,m}(t) = \begin{cases} 
1 + i_0 \frac{p^2-1}{3p} + \frac{2}{p} t_0 (t_0 - p) & \text{if } t_1 = \cdots = t_{i_0-1} = 0 \text{ and } t_{i_0} \neq 0, \text{ with } 1 \leq i_0 \leq m, \\
1 + \frac{p^2-1}{3p} & \text{otherwise}.
\end{cases}$$

With these formulas, $R(g, f)$ as well as $\tilde{R}_\gamma(g, f)$ can be computed in $O(p^m s)$ operations.

3. Existence results and construction algorithms for polynomial lattice rules

In this section we present existence results and construction algorithms for polynomial lattice rules modulo arbitrary polynomials. The first four subsections are concerned with the weighted star discrepancy whereas the last subsection deals with the classical star discrepancy.

3.1. An average-type result

The following theorem gives, for a polynomial $f \in \mathbb{F}_p[x]$ with $\deg(f) = m$, the average of $\tilde{R}_\gamma(g, f)$ over all vectors $g \in (G^*_{p,m}(f))^s$. A proof can be obtained using a similar method as in the proof of [18, Theorem 4.43] and hence we omit the proof here. Further we remark that Theorem 1 is the weighted version of [18, Theorem 4.43]. A very similar result for irreducible polynomials $f$ is given in [5, Theorem 2.3].

**Theorem 1.** Let $m \geq 1$, $s \geq 2$, and $f \in \mathbb{F}_p[x]$ with $\deg(f) = m$. Then
\[ \frac{1}{|G^*_p,m(f)|^s} \sum_{g \in (G^*_p,m(f))^s} \tilde{R}_\gamma(g, f) = \frac{1}{N} \left( \prod_{i=1}^{s} (1 + \gamma_i (1 + c_p \log N)) - \prod_{i=1}^{s} (1 + \gamma_i) \right) - c_p \frac{\log N}{N} \sum_{i=1}^{s} \gamma_i \prod_{j=1}^{s} (1 + \gamma_j) \]

\[ + O \left( \frac{(\log N)^2}{N} \right) \sum_{u \subseteq D, |u| \geq 2} \left( \prod_{i \in u} \left( -\gamma_i \frac{p^2 - 1}{3p} \right) \right) \left( \prod_{i \notin u} (1 + \gamma_i) \right), \]

where \( c_p = \frac{p^2 - 1}{3p \log p} \) and \( N = p^m \).

This result serves as a benchmark for our construction algorithms presented in the following subsections.

### 3.2. A component-by-component construction

Theorem 1 implies the existence of polynomials which can be used for the construction of point sets with small star discrepancy. The following algorithm provides a way to find such polynomials explicitly. We outline a component-by-component construction of \( P(g, f) \) based on the quantity \( \tilde{R}_\gamma(g, f) \).

**Algorithm 1.** Let \( p \) be prime. Given \( f \in \mathbb{F}_p[x], \deg(f) = m \geq 1, \) and a sequence of weights \( \gamma = (\gamma_i)_{i \geq 1} \):

1. Set \( g_1 = 1 \).
2. For \( d = 2, 3, \ldots, s \) and already known \( g_1, \ldots, g_{d-1} \), find \( g_d \in G^*_p,m(f) \) which minimizes \( \tilde{R}_\gamma((g_1, \ldots, g_{d-1}, g_d), f) \).

In the following theorem we show that this algorithm is guaranteed to find a good generating vector.

**Theorem 2.** Let \( p \) be prime and \( f \in \mathbb{F}_p[x] \) with \( \deg(f) = m \). Suppose \( g^* = (g^*_1, \ldots, g^*_s) \in (G^*_p,m(f))^s \) is constructed according to Algorithm 1. Then for all \( d = 1, \ldots, s \) we have

\[ \tilde{R}_\gamma((g^*_1, \ldots, g^*_d), f) \leq \frac{1}{p^m} \prod_{i=1}^{d} \left( 1 + \gamma_i \left( 1 + (m + \tilde{c}_f) \frac{p^2 - 1}{3p} \right) \right), \]

where \( \tilde{c}_f = \sum_{r|f, r \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)-1}} \).

**Remark 1.** We remark that the bound in the above theorem can be made independent of the dimension if \( \sum_{i=1}^{\infty} \gamma_i < \infty \) by using [8, Lemma 3]. This is known as strong tractability, see [24].

**Proof of Theorem 2.** Without loss of generality, we assume that the polynomial \( f \) is monic. We prove the result by induction on \( d = 1, \ldots, s \).
Since \( g_1^* \equiv 1 \) and since there is no polynomial \( h \in G_{p,m} \setminus \{0\} \) such that \( h \equiv 0 \pmod{f} \), it follows that \( \tilde{R}_\gamma((g^*_1),f) = 0 \) and hence the bound holds for \( d = 1 \). Now we have

\[
\tilde{R}_\gamma((g^*_1, g_{d+1}^*), f) = \min_{g_{d+1} \in G_{p,m}(f)} \tilde{R}_\gamma((g^*_1, g_{d+1}), f)
\]

\[
\leq \frac{1}{|G_{p,m}(f)|} \sum_{g_{d+1} \in G_{p,m}(f)} \tilde{R}_\gamma((g^*_1, g_{d+1}), f).
\]

Observe that \( |G_{p,m}(f)| = \phi_p(f) \), where \( \phi_p(f) \) is the analogue of Euler’s totient function for the field \( \mathbb{F}_p[x] \) (cf. [18, p. 77]). Thus,

\[
\tilde{R}_\gamma((g^*_1, g_{d+1}^*), f) \leq \frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}(f)} \tilde{R}_\gamma((g^*_1, g_{d+1}), f)
\]

\[
= \frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}(f)} \sum_{(h, h_{d+1}) \in G_{p,m}(f) \setminus \{0\}} \prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i)
\]

\[
= \frac{1}{\phi_p(f)} \sum_{(h, h_{d+1}) \in G_{p,m}(f) \setminus \{0\}} \left( \prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i) \right) \sum_{g_{d+1} \in G_{p,m}(f) \setminus \{0\}} 1.
\]

If \( (h, h_{d+1}) = 0 \),

\[
\prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i) = \prod_{i=1}^{d+1} (1 + \gamma_i)
\]

and

\[
\sum_{g_{d+1} \in G_{p,m}(f) \setminus \{0\}} \prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i) = \sum_{g_{d+1} \in G_{p,m}(f) \setminus \{0\}} 1 = |G_{p,m}(f)| = \phi_p(f).
\]

Consequently,

\[
\tilde{R}_\gamma((g^*_1, g_{d+1}^*), f) \leq -\prod_{i=1}^{d+1} (1 + \gamma_i)
\]

\[
+ \frac{1}{\phi_p(f)} \sum_{(h, h_{d+1}) \in G_{p,m}(f) \setminus \{0\}} \left( \prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i) \right) \sum_{g_{d+1} \in G_{p,m}(f) \setminus \{0\}} 1.
\]
For all \((h, h_{d+1}) \in G_{p,m}^{d+1}\),

\[
\sum_{g \in G_{p,m}^*(f)} \frac{1}{p^m} \sum_{v \mod f} X_p \left( \frac{v}{f} (h \cdot g^* + h_{d+1}g) \right).
\]

where \(\sum_{v \mod f}\) and \(X_p\) are defined as in [18, p. 78]. We therefore have

\[
\tilde{R}_p((g^*, g_{d+1}^*), f) \leq \prod_{i=1}^{d+1} (1 + \gamma_i)
\]

\[
+ \frac{1}{\phi_p(f)} \sum_{v \mod f} \sum_{h \in G_{p,m}^d} \left( \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) \right)
\]

\[
\times X_p \left( \frac{v}{f} h \cdot g^* \right) \sum_{h \in G_{p,m}} \sum_{g \in G_{p,m}^*(f)} \tilde{r}_p(h, \gamma_{d+1}) X_p \left( \frac{v}{f} hg \right).
\]

Define now

\[
Y_p(v, f) := \sum_{h \in G_{p,m}} \sum_{g \in G_{p,m}^*(f)} \tilde{r}_p(h, \gamma_{d+1}) X_p \left( \frac{v}{f} hg \right).
\]

Then,

\[
Y_p(0, f) = \phi_p(f) \sum_{h \mod f} \tilde{r}_p(h, \gamma_{d+1}).
\]

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

\[
Y_p(v, f) = \sum_{h \mod f} \tilde{r}_p(h, \gamma_{d+1}) \sum_{g \mod f} X_p \left( \frac{v}{f} hg \right) \sum_{l | (g, f)} \mu_p(l)
\]

\[
= \sum_{h \mod f} \tilde{r}_p(h, \gamma_{d+1}) \mu_p(l) \sum_{g \mod f} X_p \left( \frac{v}{f} hg \right)
\]

\[
= \sum_{h \mod f} \tilde{r}_p(h, \gamma_{d+1}) \mu_p(l) \sum_{a \mod f/l} X_p \left( \frac{v}{f} ha \right)
\]

Applying [18, (4.51)] to the innermost sum, we obtain
\[ Y_p(v, f) = \sum_{h \mod f} \sum_{l|f} \mu_p \left( \frac{f}{l} \right) p^{\text{deg}(l)} \tilde{r}_p(h, \gamma d + 1) \]

\[ = \sum_{l|f} \mu_p \left( \frac{f}{l} \right) p^{\text{deg}(l)} \sum_{h \mod f} \tilde{r}_p(h, \gamma d + 1). \]

Now \( l|vh \) if and only if \( l/(l, v) \) divides \( h \). Thus,

\[ Y_p(v, f) = \sum_{l|f} \mu_p \left( \frac{f}{l} \right) p^{\text{deg}(l)} E_p \left( \frac{l}{(l, v)}, f \right), \]

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

\[ E_p(a, f) = \sum_{h \mod f} \tilde{r}_p(h, \gamma d + 1). \]

If \( a = f \), then

\[ E_p(a, f) = \tilde{r}_p(0, \gamma d + 1) = 1 + \gamma d + 1. \]

Now let \( a \neq f \); then

\[ E_p(a, f) = 1 + \gamma d + 1 + \sum_{b \mod f/a \atop b \neq 0} \tilde{r}_p(ab, \gamma d + 1). \]

We have, by denoting by \( \text{sgn}(b) \) the leading coefficient of a polynomial \( b \), and by noting that \( a \) is monic,

\[ \sum_{b \mod f/a \atop b \neq 0} \tilde{r}_p(ab, \gamma d + 1) = \gamma d + 1 \sum_{b \mod f/a \atop b \neq 0} 1 \frac{1}{p^{\text{deg}(ab) + 1} \sin^2 \left( \frac{\pi}{p} \text{sgn}(ab) \right)} \]

\[ = \gamma d + 1 p^{-\text{deg}(a) - 1} \sum_{b \mod f/a \atop b \neq 0} p^{-\text{deg}(b)} \frac{1}{\sin^2 \left( \frac{\pi}{p} \text{sgn}(b) \right)} \]

\[ = \gamma d + 1 p^{-\text{deg}(a) - 1} \sum_{k=0}^{\text{deg}(f/a) - 1} p^{-k} \sum_{z=1}^{p-1} \frac{1}{\sin^2 \left( \frac{\pi}{p} z \right)} \]

\[ = \gamma d + 1 \deg \left( \frac{f}{a} \right) p^{-\text{deg}(a) - 1} \sum_{z=1}^{p-1} \frac{1}{\sin^2 \left( \frac{\pi}{p} z \right)} \]

\[ = \gamma d + 1 T_p \deg \left( \frac{f}{a} \right) p^{-\text{deg}(a)}. \]
where \( T_p = \frac{p^2 - 1}{3p} \). Since, for \( a = f \), \( \deg(f/a) = 0 \), we have for all \( a \in S_p \) dividing \( f \)

\[
E_p(a, f) = 1 + \gamma_{d+1} + \gamma_{d+1} T_p \deg\left(\frac{f}{a}\right) p^{-\deg(a)}
\]

\[
= 1 + \gamma_{d+1} + \gamma_{d+1} c_p (\log N) p^{-\deg(a)} - \gamma_{d+1} T_p \deg(a) p^{-\deg(a)},
\]

where \( c_p \) is defined as in Theorem 1.

Applying this formula with \( a = l/(l, v) \), we obtain

\[
Y_p(v, f) = \sum_{l|f} \mu_p \left( \frac{f}{l} \right) p^{\deg(l)} \left( 1 + \gamma_{d+1} + \gamma_{d+1} c_p (\log N) p^{-\deg(l/(l, v))} \right)
\]

\[
- \gamma_{d+1} T_p \deg\left(\frac{l}{(l, v)}\right) p^{-\deg((l, v))}
\]

\[
= \sum_{l|f} \mu_p \left( \frac{f}{l} \right) \left( p^{\deg(l)} (1 + \gamma_{d+1}) + \gamma_{d+1} c_p (\log N) p^{\deg((l, v))} \right)
\]

\[
- \gamma_{d+1} T_p \deg\left(\frac{l}{(l, v)}\right) p^{\deg((l, v))}
\]

\[
= \phi_p(f) (1 + \gamma_{d+1}) + \gamma_{d+1} c_p (\log N) H_p^{(1)}(v, f) - \gamma_{d+1} T_p H_p^{(2)}(v, f),
\]

with

\[
H_p^{(1)}(v, f) = \sum_{l|f} \mu_p \left( \frac{f}{l} \right) \deg\left(\frac{l}{(l, v)}\right) p^{\deg((l, v))},
\]

\[
H_p^{(2)}(v, f) = \sum_{l|f} \mu_p \left( \frac{f}{l} \right) \deg\left(\frac{l}{(l, v)}\right) p^{\deg((l, v))}.
\]

Analyzing \( H_p^{(1)}(v, f) \) as in [18, p. 82f], we find that

\[
Y_p(v, f) = \phi_p(f) (1 + \gamma_{d+1}) - \gamma_{d+1} T_p H_p^{(2)}(v, f).
\]

Therefore we have

\[
\tilde{K}_Y ((g^*, g_{d+1}^*), f) \leq - \prod_{i=1}^{d+1} (1 + \gamma_i) + \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{h \in G_{p, m}^d} \left( \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) \right) Y_p(0, f)
\]

\[
+ \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{v \mod f} \sum_{h \in G_{p, m}^d} \left( \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) \right) X_p \left( \frac{v}{f} \cdot h \cdot g^* \right) Y_p(v, f)
\]
\[
= - \prod_{i=1}^{d+1} \frac{1}{1 + \gamma_i} + \frac{1}{p^m} \sum_{h \in G_{p,m}^{d+1}} \prod_{i=1}^{d+1} \tilde{t}_p(h_i, \gamma_i)
\]
\[
+ \frac{1}{p^m} \sum_{v \mod f} \sum_{h \in G_{p,m}^d} \left( \prod_{i=1}^{d} \tilde{t}_p(h_i, \gamma_i) \right) X_p \left( \frac{v}{f} h \cdot g^* \right)
\]
\[
- \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{v \mod f} \sum_{h \in G_{p,m}^{d}} \left( \prod_{i=1}^{d} \tilde{t}_p(h_i, \gamma_i) \right) X_p \left( \frac{v}{f} h \cdot g^* \right) T_p H_p^{(2)}(v, f)
\]
\[
= \frac{1}{p^m} \sum_{h \in G_{p,m}^{d+1}} \prod_{i=1}^{d+1} \tilde{t}_p(h_i, \gamma_i) + (1 + \gamma_{d+1}) \tilde{R}_p(g^*, f) - \frac{1 + \gamma_{d+1}}{p^m} \sum_{h \in G_{p,m}^{d}} \prod_{i=1}^{d} \tilde{t}_p(h_i, \gamma_i)
\]
\[
- \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{v \mod f} \sum_{h \in G_{p,m}^{d}} \left( \prod_{i=1}^{d} \tilde{t}_p(h_i, \gamma_i) \right) X_p \left( \frac{v}{f} h \cdot g^* \right) T_p H_p^{(2)}(v, f).
\]

The last equality follows from the formula
\[
(1 + \gamma_{d+1}) \tilde{R}_p(g^*, f)
\]
\[
= - \prod_{i=1}^{d+1} \frac{1}{1 + \gamma_i} + \frac{1 + \gamma_{d+1}}{p^m} \sum_{v \mod f} \sum_{h \in G_{p,m}^{d}} \left( \prod_{i=1}^{d} \tilde{t}_p(h_i, \gamma_i) \right) X_p \left( \frac{v}{f} h \cdot g^* \right).
\]

Now we consider the term
\[
K_p^d(f) := - \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{v \mod f} \sum_{h \in G_{p,m}^{d}} \left( \prod_{i=1}^{d} \tilde{t}_p(h_i, \gamma_i) \right) X_p \left( \frac{v}{f} h \cdot g^* \right) T_p H_p^{(2)}(v, f).
\]

To this end let
\[
T(f) := \sum_{v \mod f} J_p(v, f) X_p \left( \frac{v}{f} h \cdot g^* \right),
\]

where \( J_p(v, f) = H_p^{(2)}(v, f)/\phi_p(f) \).

For a monic irreducible polynomial \( r \) over \( \mathbb{F}_p \) and \( v \in \mathbb{F}_p[x] \) let \( e_r(v) \) be defined as in [18, p. 82ff], where it is shown that
\[
J_p(v, f) = \frac{\deg(r)}{\phi_p(r^e_r(f) - e_r(v))},
\]

if there is exactly one \( r \) satisfying \( e_r(v) < e_r(f) \), and \( J_p(v, f) = 0 \) otherwise.
Let now \( f_1, f_2 \) be two polynomials over \( \mathbb{F}_p \) with \( (f_1, f_2) = 1 \). Let \( v \in \mathbb{F}_p[x] \) with \( 0 \leq \deg(v) < \deg(f_1 f_2) \) such that there is exactly one \( r \) satisfying \( e_r(v) < e_r(f_1 f_2) \). It then follows that \( r \) divides exactly one of \( f_1 \) and \( f_2 \) (see [18, p. 84]). We get

\[
T(f_1 f_2) = \sum_{\substack{v \mod f_1 f_2 \\ v \neq 0}} J_p(v, f_1 f_2) X_p \left( \frac{v}{f_1 f_2} h \cdot g^* \right)
\]

\[
= \sum_{\substack{v \mod f_1 f_2 \\ v \neq 0}} J_p(v, f_1 f_2) X_p \left( \frac{v}{f_1 f_2} h \cdot g^* \right)
\]

\[
\exists r: e_r(v) < e_r(f_1 f_2) \quad \text{and} \quad r | f_1
\]

\[
+ \sum_{\substack{v \mod f_1 f_2 \\ v \neq 0}} J_p(v, f_1 f_2) X_p \left( \frac{v}{f_1 f_2} h \cdot g^* \right).
\]

If \( r | f_1, v = v_1 f_2 \) with \( v_1 \in \mathbb{F}_p[x], 0 \leq \deg(v) < \deg(f_1) \), and

\[
J_p(v, f_1 f_2) = J_p(v_1 f_2, f_1 f_2) = J_p(v_1, f_1),
\]

and analogously if \( r | f_2 \), which yields

\[
T(f_1 f_2) = \sum_{\substack{v_1 f_2 \mod f_1 f_2 \\ v_1 f_2 \neq 0}} J_p(v_1 f_2, f_1 f_2) X_p \left( \frac{v_1 f_2}{f_1 f_2} h \cdot g^* \right)
\]

\[
\exists r: e_r(v_1 f_2) < e_r(f_1 f_2) \quad \text{and} \quad r | f_1
\]

\[
+ \sum_{\substack{v_2 f_1 \mod f_1 f_2 \\ v_2 f_1 \neq 0}} J_p(v_2 f_1, f_1 f_2) X_p \left( \frac{v_2 f_1}{f_1 f_2} h \cdot g^* \right).
\]

However, the latter expression equals

\[
\sum_{\substack{v_1 \mod f_1 \\ v_1 \neq 0}} J_p(v_1, f_1) X_p \left( \frac{v_1}{f_1} h \cdot g^* \right) + \sum_{\substack{v_2 \mod f_2 \\ v_2 \neq 0}} J_p(v_2, f_2) X_p \left( \frac{v_2}{f_2} h \cdot g^* \right)
\]

\[
= T(f_1) + T(f_2).
\]

Hence \( T \) is additive. Let \( r \) be a monic and irreducible polynomial and \( e \geq 1 \), then
\[
T(r^e) = \sum_{k=0}^{e-1} \sum_{v \mod r^e \atop e_r(v) = k} J_p(v, r^e) X_p\left(\frac{v}{r^e} h \cdot g^*\right)
\]

\[
= \sum_{k=0}^{e-1} \sum_{v \mod r^e \atop e_r(v) = k} \frac{\deg(r)}{\phi_p(r^{e-k})} X_p\left(\frac{v}{r^e} h \cdot g^*\right)
\]

\[
= \deg(r) \sum_{k=0}^{e-1} \frac{1}{\phi_p(r^{e-k})} \sum_{v \mod r^e \atop e_r(v) = k} X_p\left(\frac{v}{r^e} h \cdot g^*\right)
\]

\[
= \deg(r) \sum_{k=0}^{e-1} \frac{1}{\phi_p(r^{e-k})}
\]

\[
\times \left[ \sum_{r^kq \mod r^e} X_p\left(\frac{r^kq}{r^e} h \cdot g^*\right) - \sum_{r^{k+1}q \mod r^e} X_p\left(\frac{r^{k+1}q}{r^e} h \cdot g^*\right) \right]
\]

\[
= \deg(r) \sum_{k=0}^{e-1} \frac{1}{\phi_p(r^{e-k})} \sum_{q \mod r^{e-k}} X_p\left(\frac{q}{r^e} h \cdot g^*\right)
\]

\[
- \deg(r) \sum_{k=1}^{e} \frac{1}{\phi_p(r^{e-k+1})} \sum_{q \mod r^{e-k}} X_p\left(\frac{q}{r^e} h \cdot g^*\right)
\]

\[
= \deg(r) \sum_{k=1}^{e-1} \left[ \frac{1}{\phi_p(r^{e-k})} - \frac{1}{\phi_p(r^{e-k+1})} \right] \sum_{q \mod r^{e-k}} X_p\left(\frac{q}{r^e} h \cdot g^*\right)
\]

\[
+ \deg(r) \frac{1}{\phi_p(r^e)} \sum_{q \mod r^e} X_p\left(\frac{q}{r^e} h \cdot g^*\right) - \deg(r) \frac{1}{\phi_p(r)}
\]

\[
\geq -\deg(r) \frac{1}{\phi_p(r)} = -\frac{\deg(r)}{p^{\deg(r)} - 1}.
\]

By additivity we obtain

\[
T(f) \geq -\sum_{r \mid f \atop r \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1}
\]

and therefore

\[
K^d_{p}(f) \leq \frac{T_p}{p^{dm}} \left( \sum_{r \mid f \atop r \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} \right) \sum_{h \in G_{p,m}} \prod_{i=1}^{d} \tilde{T}_p(h_i, \gamma_i).
\]

We obtain
\[ \tilde{R}_\gamma((g^*, g_{d+1}^*), f) \leq \frac{1}{p^m} \sum_{h \in G_{d+1}^d} \prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i) + (1 + \gamma_{d+1}) \tilde{R}_\gamma(g^*, f) \]

\[ - \frac{1}{p^m} \sum_{h \in G_d^{d+1}} \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) \]

\[ + \frac{T_p \gamma_{d+1}}{p^m} \left( \sum_{r \mid f \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} \right) \sum_{h \in G_{d+1}^{d+1}} \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i). \] (5)

Now we have (see [6, Appendix C])

\[ \sum_{h \in G_d^{d+1}} \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) = \prod_{i=1}^{d} \left( 1 + \gamma_i (1 + m \frac{p^2 - 1}{3p}) \right) \]

and thus it follows that

\[ \frac{1}{p^m} \sum_{h \in G_{d+1}^d} \prod_{i=1}^{d+1} \tilde{r}_p(h_i, \gamma_i) - \frac{1 + \gamma_{d+1}}{p^m} \sum_{h \in G_d^{d+1}} \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) \]

\[ + \frac{T_p \gamma_{d+1}}{p^m} \left( \sum_{r \mid f \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} \right) \sum_{h \in G_{d+1}^{d+1}} \prod_{i=1}^{d} \tilde{r}_p(h_i, \gamma_i) \]

\[ = \frac{1}{p^m} \prod_{i=1}^{d} \left( 1 + \gamma_i \left( 1 + m \frac{p^2 - 1}{3p} \right) \right) \]

\[ \times \left( 1 + \gamma_{d+1} \left( 1 + m \frac{p^2 - 1}{3p} \right) - 1 - \gamma_{d+1} + \gamma_{d+1} \frac{p^2 - 1}{3p} \left( \sum_{r \mid f \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} \right) \right) \]

\[ = \frac{\gamma_{d+1}}{p^m} \prod_{i=1}^{d} \left( 1 + \gamma_i \left( 1 + m \frac{p^2 - 1}{3p} \right) \right) \frac{p^2 - 1}{3p} \left( m + \sum_{r \mid f \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} \right). \]

From (5) and the last equality the result follows now by induction. \qed

**Remark 2.** (1) Using ideas from [18, p. 84f] it can be shown that

\[ \tilde{c}_f = \sum_{r \mid f \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} = O(\log m). \]
(2) If \( f(x) = x^m \) we obtain

\[
\tilde{c}_f = \sum_{r|f \text{ irreducible}} \frac{\deg(r)}{p^{\deg(r)} - 1} = \frac{1}{p - 1}.
\]

3.3. A Korobov-type construction if \( f \) is the product of two monic irreducible polynomials

In the theory of good lattice points, lattice points whose coordinates are successive powers of a single integer are of great interest. Such a choice was first proposed by Korobov [9], which is the reason why such lattice points are frequently called Korobov lattice points. Polynomial Korobov lattice rules were already studied in [12] and a construction algorithm for polynomial Korobov lattice rules with low weighted star discrepancy was proposed in [5] for the case where \( f \) is irreducible. Here, we present a Korobov-type construction for the case where \( f \) is the product of two monic irreducible polynomials. Our method is motivated by ideas in [25].

Let \( f \in \mathbb{F}_p[x] \) be the product of two different monic irreducible polynomials \( f_1, f_2 \in \mathbb{F}_p[x] \) with \( \deg(f_i) = m_i \) and \( m_1 + m_2 = m = \deg(f) \).

Algorithm 2.

(1) Find optimal \( g \in G_{p,m_1} \setminus \{0\} \) using [5, Algorithm 3.9] with \( f \) replaced by \( f_1 \).
(2) For the \( g \) already found in the first step and for \( b \in G_{p,m_2} \setminus \{0\} \), let the vector

\[
w_s(b) := (f_1, f_1b, \ldots, f_1b^{s-1}) + (f_2, f_2g, \ldots, f_2g^{s-1}) \quad (\text{mod } f).
\]

Then, find \( b \in G_{p,m_2} \setminus \{0\} \) which minimizes \( \tilde{R}_y(w_s(b), f) \).

Theorem 3. Let \( f \in \mathbb{F}_p[x] \) be the product of two different monic irreducible polynomials \( f_1, f_2 \in \mathbb{F}_p[x] \) with \( \deg(f_i) = m_i \) and \( m_1 + m_2 = m \). Assume \( b_s \in G_{p,m_2} \setminus \{0\} \) is chosen according to Algorithm 2, then we have

\[
\tilde{R}_y(w_s(b_s), f) \leq \left( \frac{1}{p^{m_2}} + \frac{s-1}{p^{m_2} - 1} \right) \frac{s-1}{p^{m_1} - 1} \left( -\prod_{i=1}^{s} (1 + \sqrt[3]{\gamma_i}) + \prod_{i=1}^{s} \left( 1 + \sqrt[3]{\gamma_i} \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \right)
\]

\[
+ \frac{s-1}{p^{m_2} - 1} \frac{s-1}{p^{m_1} - 1} \left( -\prod_{i=1}^{s} (1 + \sqrt[3]{\gamma_i}) + \prod_{i=1}^{s} \left( 1 + \sqrt[3]{\gamma_i} \left( 1 + m_2 \frac{p^2 - 1}{3p} \right) \right) \right)
\]

\[
\times \left( -\prod_{i=1}^{s} (1 + \sqrt[3]{\gamma_i}) + \prod_{i=1}^{s} \left( 1 + \sqrt[3]{\gamma_i} \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \right)
\]

\[
+ \frac{s-1}{p^{m_2} - 1} \frac{1}{p^{m_1}} \left( -\prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_2 \frac{p^2 - 1}{3p} \right) \right) \right)
\].
Remark 3. If the weights satisfy $\sum_{i=1}^{\infty} \sqrt{\gamma_i} < \infty$ then using [8, Lemma 3] one can show that the bound in the above theorem depends only polynomially on the dimension $s$. This is known as tractability, see [24].

Proof. Define

$$
\tilde{M}_s^K(f) := \frac{1}{p^{m_2} - 1} \sum_{b \in G_{p,m_2}^s \setminus \{0\}} \tilde{R}_f(w_s(b), f).
$$

It follows from Algorithm 2 that $\tilde{R}_f(w_s(b), f) \leq \tilde{M}_s^K(f)$ and therefore it suffices to show that $\tilde{M}_s^K(f)$ satisfies the bound given in Theorem 3. We have

$$
\tilde{M}_s^K(f) = \frac{1}{p^{m_2} - 1} \sum_{h \in G_{p,m}^s \setminus \{0\}} \prod_{i=1}^{s} \tilde{r}_p(h_i, \gamma_i) \sum_{b \in G_{p,m_2}^s \setminus \{0\}} \delta_f(w_s(b) \cdot h),
$$

where for polynomials $f$ and $a \in \mathbb{F}_p[x]$ we define

$$
\delta_f(a) := \begin{cases} 1 & \text{if } a \equiv 0 \pmod{f}, \\ 0 & \text{if } a \not\equiv 0 \pmod{f}. \end{cases}
$$

Since $\gcd(f_1, f_2) = 1$, for polynomials $a_1, a_2 \in \mathbb{F}_p[x]$ it is easy to prove that

$$
f_1 a_1 + f_2 a_2 \equiv 0 \pmod{f}
$$

if and only if

$$
a_1 \equiv 0 \pmod{f_2} \quad \text{and} \quad a_2 \equiv 0 \pmod{f_1}.
$$

Therefore we obtain

$$
\delta_f(w_s(b) \cdot h) = \delta_{f_1}(h \cdot (1, g_s, \ldots, g_{s-1})) \delta_{f_2}(h \cdot (1, b, \ldots, b_{s-1}))
$$

and hence

$$
\tilde{M}_s^K(f) = \frac{1}{p^{m_2} - 1} \sum_{h \in G_{p,m}^s \setminus \{0\}} \left( \prod_{i=1}^{s} \tilde{r}_p(h_i, \gamma_i) \right) \delta_{f_1}(h \cdot (1, g_s, \ldots, g_{s-1})) \times \sum_{b \in G_{p,m_2}^s \setminus \{0\}} \delta_{f_2}(h \cdot (1, b, \ldots, b_{s-1})).
$$
\[
= \frac{1}{p^{m_2} - 1} \sum_{h \in G_{p,m} \setminus \{0\}, \ h_i \equiv 0 \pmod{f_2}, 1 \leq i \leq s} \left( \prod_{i=1}^{s} \tilde{\tau}_p(h_i, \gamma_i) \right) \delta_{f_1}(h \cdot (1, g_*, \ldots, g_*^{s-1}))
\]
\[
\times \sum_{b \in G_{p,m_2} \setminus \{0\}} \delta_{f_2}(h \cdot (1, b, \ldots, b^{s-1}))
\]
\[
+ \frac{1}{p^{m_2} - 1} \sum_{h \in G_{p,m} \setminus \{0\}, \ \exists i: h_i \not\equiv 0 \pmod{f_2}} \left( \prod_{i=1}^{s} \tilde{\tau}_p(h_i, \gamma_i) \right) \delta_{f_1}(h \cdot (1, g_*, \ldots, g_*^{s-1}))
\]
\[
\times \sum_{b \in G_{p,m_2} \setminus \{0\}} \delta_{f_2}(h \cdot (1, b, \ldots, b^{s-1}))
\]
\[=: \Sigma_1 + \Sigma_2.
\]

If there is an index \(i\) such that \(h_i \not\equiv 0 \pmod{f_2}\) then
\[
\sum_{b \in G_{p,m_2} \setminus \{0\}} \delta_{f_2}(h \cdot (1, b, \ldots, b^{s-1})) \leq s - 1,
\]
since \(f_2\) is irreducible. Otherwise
\[
\sum_{b \in G_{p,m_2} \setminus \{0\}} \delta_{f_2}(h \cdot (1, b, \ldots, b^{s-1})) = p^{m_2} - 1.
\]

Now
\[
\Sigma_1 = \sum_{\tilde{h} \in G_{p,m_1} \setminus \{0\}} \prod_{i=1}^{s} \tilde{\tau}_p(\tilde{h}_i, f_2, \gamma_i) \delta_{f_1}(\tilde{h} \cdot (1, g_*, \ldots, g_*^{s-1})),
\]
since \(\gcd(f_1, f_2) = 1\). If \(\tilde{h}_i = 0\), then \(\tilde{\tau}_p(\tilde{h}_i, f_2, \gamma_i) = \tilde{\tau}_p(\tilde{h}_i, \gamma_i)\) and otherwise (since \(f_2\) is monic)
\[
\tilde{\tau}_p(\tilde{h}_i, f_2, \gamma_i) = \frac{1}{p^{m_2} \tilde{\tau}_p(\tilde{h}_i, \gamma_i)}.
\]
Therefore
\[
\Sigma_1 \leq \frac{1}{p^{m_2}} \sum_{\tilde{h} \in G_{p,m_1} \setminus \{0\}} \prod_{i=1}^{s} \tilde{\tau}_p(\tilde{h}_i, \gamma_i) =: \frac{1}{p^{m_2}} \tilde{R}_f(v_s(g_*), f_1).
\]

We consider \(\Sigma_2\):
\[
\Sigma_2 \leq \frac{s - 1}{p^{m_2} - 1} \sum_{h \in G_{p,m} \setminus \{0\}} \left( \prod_{i=1}^{s} \tilde{\tau}_p(h_i, \gamma_i) \right) \delta_{f_1}(h \cdot (1, g_*, \ldots, g_*^{s-1}))
\]
\[
= \frac{s - 1}{p^{m_2} - 1} \sum_{h \in G_{p,m_1} \setminus \{0\}} \left( \prod_{i=1}^{s} \tilde{\tau}_p(h_i, \gamma_i) \right) \delta_{f_1}(h \cdot (1, g_*, \ldots, g_*^{s-1}))
\]
\[\sum_2 \leq \frac{s - 1}{p^{m_2} - 1} \tilde{R}_Y(v_s(g_*), f_1) + \frac{s - 1}{p^{m_2} - 1} \tilde{R}_Y(v_s(g_*), f_1) \sum_{q \in G_{p,m}^s \setminus \{0\}} \prod_{i=1}^{s} \tilde{r}_p(q_i, \sqrt{\gamma_i}) + \frac{s - 1}{p^{m_2} - 1} \tilde{R}_Y(v_s(g_*), f_1) \sum_{q \in G_{p,m}^s \setminus \{0\}} \prod_{i=1}^{s} \tilde{r}_p(q_i, \sqrt{\gamma_i}) \]

where \(\sqrt{\gamma} = (\sqrt{\gamma_1}, \sqrt{\gamma_2}, \ldots)\).

By a slightly more careful derivation of [5, Theorem 3.10] we obtain

\[\tilde{R}_Y(v_s(g_*), f_1) \leq \frac{s - 1}{p^{m_1} - 1} \left( -\prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \right) \] (6)
and from [5, Lemma 3.3] we know that
\[ \sum_{q \in G_{p,m_2} \setminus \{0\}} \prod_{i=1}^{s} \tilde{r}_p(q_i, \gamma_i) = - \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_2 \frac{p^2 - 1}{3p} \right) \right). \]

Therefore we obtain
\[ \tilde{M}_s^K(f) \leq \frac{1}{p^{m_2}} \frac{s - 1}{p^{m_1} - 1} \left( - \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \]
\[ + \frac{s - 1}{p^{m_2} - 1} \frac{s - 1}{p^{m_1} - 1} \left( - \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \right) \]
\[ + \frac{s - 1}{p^{m_2} - 1} \frac{s - 1}{p^{m_1} - 1} \left( - \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \right) \]
\[ \times \left( - \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_1 \frac{p^2 - 1}{3p} \right) \right) \right) \]
\[ + \frac{s - 1}{p^{m_2} - 1} \frac{1}{p^{m_1}} \left( - \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_2 \frac{p^2 - 1}{3p} \right) \right) \right). \]

The result follows. \( \Box \)

3.4. A Korobov-type construction if \( f \) is the product of \( t \) irreducible polynomials

The results in Section 3.3 can be generalized to the case where \( f = \prod_{j=1}^{t} f_j \), with \( f_1, f_2, \ldots, f_t \) being distinct monic irreducible polynomials (\( t \geq 2 \)) with degrees \( m_1, m_2, \ldots, m_t \) and \( m_1 + \cdots + m_t = m \), where \( m \) is the degree of \( f \). Algorithm 2 can be generalized to

**Algorithm 3.**

1. Find optimal \( a_1 \in G_{p,m_1} \setminus \{0\} \) using [5, Algorithm 3.9] with \( f \) replaced by \( f_1 \).
2. For fixed \( l = 2, \ldots, t \) let \( \zeta_{l-1} := \prod_{j=1}^{l-1} f_j \). Recursively define the vector
   \[ w_{s,l-1}(a_l) := \left( \zeta_{l-1}, \zeta_{l-1} a_l, \ldots, \zeta_{l-1} a_l^{s-1} \right) + f_l w_{s,l-1}(a_{l-1}) \quad \left( \text{mod } \zeta_{l-1} f_l \right), \]
where \( w_{s,l-1}(a_{l-1}) \) (with \( w_{s,1}(a_1) := a_1 \)) is the vector found in the previous step, i.e., \( a_{l-1} \in G_{p,m_{l-1}} \setminus \{0\} \) is such that \( \tilde{R}_p(w_{s,l-1}(a_{l-1}), f) \) is minimized. Find \( a_l \in G_{p,m_l} \setminus \{0\} \) which minimizes \( \tilde{R}_p(w_{s,l}(a_l), f) \).

We now have

**Theorem 4.** Let \( f \in \mathbb{F}_p[x] \) be the product of \( t \geq 2 \) different monic irreducible polynomials \( f_1, \ldots, f_t \in \mathbb{F}_p[x] \) with \( \deg(f_i) = m_i \) and \( m_1 + \cdots + m_t = m \). Assume \( a_t^* \) is constructed according to Algorithm 3, then we have
\[
\tilde{R}_\gamma(w_{s,i}(a_i^*), f) \leq \prod_{j=1}^{t} \left[ \left( \frac{1}{p^{m_j}} + 2 \frac{s - 1}{p^{m_j} - 1} \right) \prod_{i=1}^{s} \left( 1 + \gamma'_i m_j \frac{p^2 - 1}{3p} \right) \right],
\]

where

\[
\gamma'_i = \max \{ \gamma_i, \gamma_1^{1-1/t}, \gamma_1^{1-2/t}, \ldots, \gamma_1^{1/t} \} = \begin{cases} 
\gamma_1^{1/t} & \text{if } \gamma_i \leq 1, \\
\gamma_i & \text{if } \gamma_i \geq 1.
\end{cases}
\]

**Remark 4.** If the weights satisfy \( \sum_{i=1}^{\infty} \gamma_i^{1/t} < \infty \) then using [8, Lemma 3] one can show that the bound in the above theorem depends only polynomially on the dimension \( s \). This is known as tractability, see [24].

**Proof of Theorem 4.** Using the proof technique from Theorem 3 one can show that

\[
\tilde{R}_\gamma(w_{s,i-1}(a_i^*), f) \leq \left( \frac{1}{p^{m_i}} + 2 \frac{s - 1}{p^{m_i} - 1} \right) \prod_{i=1}^{s} \left( 1 + \gamma'_i m_i \frac{p^2 - 1}{3p} \right) \times \max(\tilde{R}_\gamma(w_{s,i-1}(a_i^*), f), \tilde{R}_{\gamma^{1-1/t}}(w_{s,i-1}(a_i^*), f)),
\]

where \( \gamma^{1-1/t} = (\gamma_1^{1-1/t}, \gamma_2^{1-1/t}, \ldots) \). Hence by repeated use of the above inequality and (6) we obtain the result. \( \square \)

### 3.5. Results for the unweighted star discrepancy

In this section we present results for the classical star discrepancy. The algorithms presented in this subsection are the same as the corresponding algorithms already presented for the weighted case but with the difference that they are based on the quantity \( R(g, f) \) instead of \( \tilde{R}_\gamma(g, f) \). This modification of the algorithms provides better bounds for the unweighted star discrepancy than for the algorithms which use \( \tilde{R}_\gamma(g, f) \) with the special choice of weights \( \gamma_i = 1 \) for all \( i \geq 1 \). Since the proofs of the theorems in this section are similar to those of the corresponding theorems in Section 3, these are omitted here.

Similar to the weighted case we have the following theorem which gives the average of \( R(g, f) \) over all vectors \( g \in (G_{p,m}(f))^s \).

**Theorem 5.** Let \( f \in \mathbb{F}_p[x] \), \( \deg(f) = m \). We have

\[
M_s(f) := \frac{1}{|G_{p,m}(f)|^s} \sum_{g \in (G_{p,m}(f))^s} R(g, f)
= \frac{1}{N} \left( c_p \log N + 1 \right)^s - sc_p \frac{\log N}{N} + O\left( \frac{(\log \log N)^2}{N} \right),
\]

where \( N = p^m \), and \( c_p \) is defined as in Theorem 1.

**Proof.** The proof is again similar to that of [18, Theorem 4.43]. \( \square \)

We also have a component-by-component construction for the unweighted case.
Algorithm 4. Let $p$ be prime. Given $f \in \mathbb{F}_p[x]$, $\deg(f) = m \geq 1$:

1. Set $g_1 = 1$.
2. For $d = 2, 3, \ldots, s$ and already known $g_1, \ldots, g_{d-1}$, find $g_d \in G_{p, m}(f)$ which minimizes $R((g_1, \ldots, g_{d-1}, g_d), f)$.

Theorem 6. Let $p$ be a prime and let $f \in \mathbb{F}_p[x]$ with $\deg(f) = m \geq 1$. Suppose $g^* = (g_1^*, \ldots, g_s^*)$ is constructed according to Algorithm 4. Then for all $d = 2, \ldots, s$ we have

$$R((g_1^*, \ldots, g_d^*), f) \leq \frac{1}{p^m} \left(1 + \left(m + \tilde{c}_f \frac{p^2 - 1}{3p}\right)^d\right),$$

where $\tilde{c}_f$ is defined as in Theorem 2.

Proof. The proof is similar to that of Theorem 2. \qed

Remark 5. If $f(x) = x^m$ we obtain, by Remark 2(2),

$$R((1, g_2^*, \ldots, g_d^*), f) \leq \frac{1}{p^m} \left(1 + \frac{p + 1}{3p} + m \frac{p^2 - 1}{3p}\right)^d$$

for all $d = 2, \ldots, s$.

We also have a Korobov-type construction as in the weighted case if $f$ is the product of two irreducible monic polynomials.

Algorithm 5.

1. Find optimal $g \in G_{p, m_1} \setminus \{0\}$ using [5, Algorithm 2.9] with $f$ replaced by $f_1$.
2. For the $g$ already found in the first step and for $b \in G_{p, m_2} \setminus \{0\}$, let the vector

$$\bar{w}_s(b) := (f_1, f_1 b, \ldots, f_1 b^{s-1}) + (f_2, f_2 g, \ldots, f_2 g^{s-1}) \pmod{f}.$$  

Then, find $b \in G_{p, m_2} \setminus \{0\}$ which minimizes $R(\bar{w}_s(b), f)$.

Theorem 7. Let $f \in \mathbb{F}_p[x]$ be the product of two different monic irreducible polynomials $f_1, f_2 \in \mathbb{F}_p[x]$ with $\deg(f_i) = m_i$ and $m_1 + m_2 = m$. Assume $b^* \in G_{p, m_2} \setminus \{0\}$ is chosen according to Algorithm 5, then we have

$$R(\bar{w}_s(b^*), f) \leq \frac{s}{p^{m_1} - 1} \frac{s}{p^{m_2} - 1} \left(1 + m_1 \frac{p^2 - 1}{3p}\right)^s \left(1 + m_2 \frac{p^2 - 1}{3p}\right)^s.$$

Proof. The proof is similar to that of Theorem 3. \qed

Finally, there is an algorithm for the case where $f$ is the product of $t$ monic irreducible polynomials.
Algorithm 6.

1. Find optimal \( a_1 \in \mathbb{G}_{p,m} \setminus \{0\} \) using \([5, \text{Algorithm 2.9}]\) with \( f \) replaced by \( f_1 \).
2. For fixed \( l = 2, \ldots, t \) let \( \zeta_{l-1} := \prod_{j=1}^{l-1} f_j \). Recursively define the vector
   \[
   w_{s,l}(a_l) := (\zeta_{l-1}, \zeta_{l-1}a_l, \ldots, \zeta_{l-1}a_l^{s-1}) \pmod{\zeta_{l-1}f_1},
   \]
   where \( w_{s,l-1}(a_{l-1}) \) (with \( w_{s,1}(a_1) := a_1 \)) is the vector found in the previous step, i.e., \( a_{l-1} \in \mathbb{G}_{p,m_{l-1}} \setminus \{0\} \) is such that \( R(w_{s,l-1}(a_{l-1}), f) \) is minimized. Find \( a_l \in \mathbb{G}_{p,m_l} \setminus \{0\} \) which minimizes \( R(w_{s,l}(a_l), f) \).

We now have

**Theorem 8.** Let \( f \in \mathbb{F}_p[x] \) be the product of \( t \) different monic irreducible polynomials \( f_1, \ldots, f_t \in \mathbb{F}_p[x] \) with \( \deg(f_i) = m_i \) and \( m_1 + \cdots + m_t = m \). Assume \( a_t^* \) is constructed according to Algorithm 6, then we have

\[
R(w_{s,t}(a_t^*), f) \leq \frac{s-1}{p^{m_1} - 1} \left( 1 + m_1 \frac{p^2 - 1}{3p} \right)^s \times \prod_{j=2}^{t} \left( \frac{1}{p^{m_j}} + \frac{s-1}{p^{m_j} - 1} \left( 1 + m_j \frac{p^2 - 1}{3p} \right)^s \right)
+ \sum_{j=2}^{t} \frac{s-1}{p^{m_j} - 1} \left( -1 + \left( 1 + m_j \frac{p^2 - 1}{3p} \right)^s \right) \times \prod_{k=j+1}^{t} \left( \frac{1}{p^{m_k}} + \frac{s-1}{p^{m_k} - 1} \left( 1 + m_k \frac{p^2 - 1}{3p} \right)^s \right),
\]

where \( \tilde{m}_j = m_1 + \cdots + m_j \).

**Proof.** The proof is similar to that of Theorem 4.

4. Discussion

In this paper we were able to provide error estimates for component-by-component/Korobov constructions of polynomial lattice rules based on reducible polynomials. Though dropping the assumption of irreducibility weakens the estimates, the actual error seems to be quite unaffected by this. Indeed, as one can see by example of Table 1, the values for \( \tilde{R}_f \) are comparable for irreducible and reducible \( f \).

For the Korobov construction the question arises how to choose \( m_1 \) and \( m_2 \) for a given value of \( m \). In terms of the construction cost the minimal value is obtained for \( m_1 = m_2 \) (if \( m \) is even). On the other hand, the choice of \( m_1 \) and \( m_2 \) for given \( m \) might also influence the quality of the
Table 1
Comparison between irreducible and reducible $f$ of the $\tilde{R}_f$-values
for the Korobov rule with parameters $s = 50, \gamma_j = \frac{1}{j^2}$

<table>
<thead>
<tr>
<th>$m$</th>
<th>Irreducible $f$</th>
<th>Reducible $f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.5503950</td>
<td>0.6112040</td>
</tr>
<tr>
<td>3</td>
<td>0.5910270</td>
<td>0.6325640</td>
</tr>
<tr>
<td>4</td>
<td>0.5487220</td>
<td>0.5623250</td>
</tr>
<tr>
<td>5</td>
<td>0.4532520</td>
<td>0.4591280</td>
</tr>
<tr>
<td>6</td>
<td>0.3588920</td>
<td>0.3543220</td>
</tr>
<tr>
<td>7</td>
<td>0.2648100</td>
<td>0.2684380</td>
</tr>
<tr>
<td>8</td>
<td>0.1907370</td>
<td>0.1927350</td>
</tr>
<tr>
<td>9</td>
<td>0.1351930</td>
<td>0.1345680</td>
</tr>
<tr>
<td>10</td>
<td>0.0923820</td>
<td>0.0945389</td>
</tr>
<tr>
<td>11</td>
<td>0.0627568</td>
<td>0.0633650</td>
</tr>
<tr>
<td>12</td>
<td>0.0416007</td>
<td>0.0423129</td>
</tr>
</tbody>
</table>

Korobov polynomial lattice rule. Note that the bound in Theorem 3 is symmetrical in $m_1$ and $m_2$ apart from the term

$$\frac{s-1}{p^{m_1}-1} \frac{s-1}{p^{m_2}-1} \left( -\prod_{i=1}^{s}(1+\gamma_i) + \prod_{i=1}^{s} \left( 1 + \gamma_i \left( 1 + m_1 \frac{p^2-1}{3p} \right) \right) \right).$$

This would suggest that choosing $m_1$ slightly smaller than $m_2$ could yield a better result, as in this case the upper bound becomes smaller. On the other hand, Table 1 already suggested that there is no noticeable difference between irreducible and reducible polynomials, hence it seems reasonable to assume that all partitions of $m$ into $m_1, m_2 \geq 1$ would yield similar results. Indeed, further numerical investigations show that there is no noticeable difference between different choices for $m_1$ and $m_2$. Hence the best choice of $m_1$ and $m_2$ is $m_1 = m_2$ (or $m_1 \approx m_2$ if $m$ is not even) as in this case the construction cost is minimized (see also [2] where there is a comprehensive numerical investigation of these questions for lattice rules; results for polynomial lattice rules are expected to be similar to those for lattice rules, see the numerical results in [4]; compare for example Table 1 with [5, Table 5.2]).

We point out that the component-by-component constructions outlined here yield polynomial lattice rules that are extensible in the dimension. On the other hand, Niederreiter [19] proved the existence of good polynomial lattice rules which are extensible in the dimension and in the modulus. See also [1].

Fast component-by-component constructions of lattice rules have been introduced in [21–23]. It should also be possible to apply those ideas to the construction of polynomial lattice rules modulo reducible polynomials.

References


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


