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 für Mathematik, Universität Salzburg, Hellbrunnerstraße 34, A-5020 Salzburg, Austria*

[c] *Institut für Finanzmathematik, Universität Linz, Altenbergerstraße 69, A-4040 Linz, Austria*

Abstract

In this paper we study construction algorithms for polynomial lattice rules over 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 over 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 over 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 over 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.

Key words: weighted star discrepancy, digital nets, polynomial lattice rule

* Corresponding author

Email addresses: josi@maths.unsw.edu.au (Josef Dick), peter.kritzer@sbg.ac.at (Peter Kritzer), gunther.leobacher@jku.at (Gunther Leobacher), friedrich.pillichshammer@jku.at (Friedrich 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

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,

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

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

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

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., [6,9,12]),

$$|I_s(F) - Q_{N,s}(F)| \le V(F) D_N^*,$$

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 $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}$ in $[0,1)^s$ is defined as

$$D_N^* = D_N^*(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}) := \sup_{\substack{0\le\alpha_i\le 1\\ 1\le i\le s}} |\Delta(\alpha_1, \ldots, \alpha_s)|\,.$$

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

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

where $A_N(E)$ denotes the number of indices n, $0 \le n \le N-1$, such that $\boldsymbol{x}_n \in E$.

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 [10] (see also [12, Chapter 4], for a recent survey see [13]).

Definition 1 *Let $s \ge 1$, $b \ge 2$, and $0 \le t \le m$ be integers. A point set P consisting of b^m points in $[0,1)^s$ is called (t,m,s)-net in base b if every*

of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

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 [11] (see also [12, 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 $P(\boldsymbol{g}, f)$ 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, a QMC rule using the point set $P(\boldsymbol{g}, f)$ is often called a polynomial lattice rule. 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.

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 [17], 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 $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ 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 $\boldsymbol{z} \in [0,1)^s$ let $\boldsymbol{z}_u$ denote the vector in $[0,1)^{|u|}$ containing only the components of $\boldsymbol{z}$ whose indices are in u. Moreover we write $(\boldsymbol{z}_u, \boldsymbol{1})$ for the vector that we obtain by replacing all the components of $\boldsymbol{z}$ not in u by 1. Now for a point set $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ in $[0,1)^s$ and a sequence $\boldsymbol{\gamma} = (\gamma_i)_{i \geq 1}$ of weights the weighted star discrepancy $D^*_{N,\boldsymbol{\gamma}}$ is given by

$$D^*_{N,\boldsymbol{\gamma}} = D^*_{N,\boldsymbol{\gamma}}(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}) := \sup_{\boldsymbol{z} \in [0,1)^s} \max_{\substack{u \subseteq D \\ u \neq \emptyset}} \gamma_u \left| \Delta(\boldsymbol{z}_u, \boldsymbol{1}) \right|.$$

(Note that for the choice $\boldsymbol{\gamma} = \boldsymbol{1}$, that is, $\gamma_i = 1$ for all $i \geq 1$, we have $D^*_{N,\boldsymbol{1}} = D^*_N$ 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 $W_2^{(1,\ldots,1)}([0,1)^s)$,

$$|I_s(F) - Q_{N,s}(F)| \leq D^*_{N,\boldsymbol{\gamma}} \, \|F\|_{s,\boldsymbol{\gamma}},$$

where the norm is defined as

$$\|F\|_{s,\boldsymbol{\gamma}} := \sum_{u \subseteq D} \gamma_u^{-1} \int_{[0,1)^{|u|}} \left| \frac{\partial^{|u|}}{\partial \boldsymbol{x}_u} F(\boldsymbol{x}_u, \boldsymbol{1}) \right| \mathrm{d}\boldsymbol{x}_u.$$

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 [12]) that for a given polynomial f there always exists a vector of polynomials $\boldsymbol{g}$ such that $P(\boldsymbol{g}, f)$ has small star discrepancy by averaging over all possible choices of $\boldsymbol{g}$. This result was made "more explicit" in the recent paper [4] where the authors showed that such vectors $\boldsymbol{g}$ 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 [4] 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 [12]. We then show how the generating vector for point sets $P(\boldsymbol{g}, f)$, 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 $\mathcal{O}(p^m)$, 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 $\mathcal{O}(p^{m_1} + p^{m_2})$, where $m = m_1 + m_2$. Such types of algorithms have been proposed in [1,?], but therein the upper bounds on the worst-case error are not as good as for a full search. In our case though, the upper bound only shows an increased dependence on the dimension, which is typical for Korobov type construction algorithms, but the convergence rate is the same as for the full search of the component-by-component algorithm (this is not the case in [18] where the worst-case error in some reproducing kernel Hilbert space has been considered). 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 [14–16]).

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 $\boldsymbol{k} = (k_1, \ldots, k_r)^T, \boldsymbol{g} = (g_1, \ldots, g_r)^T \in (\mathbb{F}_p[x])^r$, we define the vector product

$$\boldsymbol{k} \cdot \boldsymbol{g} = \sum_{i=1}^{r} k_i g_i$$

and we write $g \equiv 0 (\bmod f)$ 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

$$r_p(h) := \begin{cases} 1 & \text{if } h = 0, \\ \frac{1}{p^{g+1} \sin^2(\frac{\pi}{p}\kappa_g)} & \text{if } h = \kappa_0 + \kappa_1 x + \cdots + \kappa_g x^g, \kappa_g \neq 0. \end{cases}$$

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

$$G^*_{p,m}(f) \subseteq G_{p,m}. \tag{1}$$

Let $f \in \mathbb{F}_p[x]$, $\deg(f) = m$, $\boldsymbol{g} \in \left(G^*_{p,m}(f)\right)^s$. Define

$$R(\boldsymbol{g}, f) := \sum_{\substack{\boldsymbol{h} \in G^s_{p,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 (\bmod f)}} \prod_{i=1}^{s} r_p(h_i).$$

We have

Proposition 1 *Let $f \in \mathbb{F}_p[x]$, $\deg(f) = m$, $\boldsymbol{g} \in (G^*_{p,m}(f))^s$. Then for the star discrepancy $D^*_N(\boldsymbol{g}, f)$ of $P(\boldsymbol{g}, f)$ we have*

$$D^*_N(\boldsymbol{g}, f) \leq 1 - \left(1 - \frac{1}{N}\right)^s + R(\boldsymbol{g}, f) \leq \frac{s}{N} + R(\boldsymbol{g}, f), \tag{2}$$

where $N = p^m$.

Proof. The assertion follows by [4, Proposition 2.1] and (1). □

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

$$R(\boldsymbol{g}_u, f) := \sum_{\substack{\boldsymbol{h} \in G^{|u|}_{p,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \cdot \boldsymbol{g}_u \equiv 0 \pmod f}} \prod_{i=1}^{|u|} r_p(h_i).$$

Moreover, we put

$$\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}, f) := \sum_{\substack{u \subseteq D \\ u \neq \emptyset}} \gamma_u R(\boldsymbol{g}_u, f).$$

It was shown in [4] that

$$\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}, f) = \sum_{\substack{\boldsymbol{h} \in G^s_{p,m} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \cdot \boldsymbol{g} \equiv 0 \pmod f}} \prod_{i=1}^{s} \widetilde{r}_p(h_i, \gamma_i),$$

with

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

For the weighted star discrepancy $D^*_{N,\boldsymbol{\gamma}}$ of a point set $\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{N-1}$ in $[0,1)^s$ it easily follows from the definition that

$$D^*_{N,\boldsymbol{\gamma}} \leq \sum_{\substack{u\subseteq D \\ u\neq\emptyset}} \gamma_u D^*_N(u),$$

where $D^*_N(u)$ denotes the star discrepancy of the projection of the point set $\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{N-1}$ to the coordinates given by u. Proposition 1 yields

$$D^*_N(u) \leq 1-\left(1-\frac{1}{N}\right)^{|u|} + R(\boldsymbol{g}_u, f).$$

Consequently, we get for the weighted star discrepancy $D^*_{N,\boldsymbol{\gamma}}$ of the point set $P(\boldsymbol{g},f)$,

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

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

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

and

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

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

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

With these formulas, $R(\boldsymbol{g}, f)$ as well as $\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}, f)$ 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 over 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 $\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}, f)$ over all vectors $\boldsymbol{g} \in (G^*_{p,m}(f))^s$. A proof can be obtained using a similar method as in the proof of [12, Theorem 4.43] and hence we omit the proof here. Further we remark that Theorem 1 is the weighted version of [12, Theorem 4.43]. A very similar result for irreducible polynomials f is given in [4, Theorem 2.3].

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

$$\begin{aligned}
&\frac{1}{\left|G^*_{p,m}(f)\right|^s} \sum_{\boldsymbol{g} \in (G^*_{p,m}(f))^s} \widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}, f) \\
&= \frac{1}{N}\left(\prod_{i=1}^{s}(1+\gamma_i(1+c_p \log N)) - \prod_{i=1}^{s}(1+\gamma_i)\right) - c_p \frac{\log N}{N} \sum_{i=1}^{s} \gamma_i \prod_{\substack{j=1 \\ j\neq i}}^{s}(1+\gamma_j) \\
&\quad + O\left(\frac{(\log\log N)^2}{N}\right) \sum_{\substack{u \subseteq D \\ |u| \geq 2}} \left(\prod_{i\in u}\left(-\gamma_i \frac{p^2-1}{3p}\right)\right)\left(\prod_{i \notin u}(1+\gamma_i)\right),
\end{aligned}$$

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.

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 $P(\boldsymbol{g}, f)$ based on the quantity $\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}, f)$.

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

(1) Set $g_1 = 1$.
(2) For $d = 2, 3, \ldots, s$ find $g_d \in G^*_{p,m}(f)$ to minimize $\widetilde{R}_{\boldsymbol{\gamma}}((g_1, \ldots, g_{d-1}, g_d), f)$.

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 $\boldsymbol{g}^* = (g_1^*, \ldots, g_s^*) \in (G^*_{p,m}(f))^s$ is constructed according to Algorithm 1. Then for all $d = 1, \ldots, s$ we have*

$$\widetilde{R}_{\boldsymbol{\gamma}}((g_1^*, \ldots, g_d^*), f) \leq \frac{1}{p^m} \prod_{i=1}^{d} \left(1 + \gamma_i \left(1 + (m + c_f)\frac{p^2 - 1}{3p}\right)\right)$$

where $c_f = \sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1}$.

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 [7, Lemma 3]. This is known as strong tractability, see [17].

Proof. W.l.o.g. we 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 $h \in G_{p,m} \setminus \{0\}$ such that $h \equiv 0(\text{mod} f)$, it follows that $\widetilde{R}_{\boldsymbol{\gamma}}((g_1^*), f) = 0$ and hence the bound holds for $d = 1$. Now we have

$$\begin{aligned}
\widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}^*), f) &= \min_{g_{d+1} \in G^*_{p,m}(f)} \widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}), f) \\
&\leq \frac{1}{\left|G^*_{p,m}(f)\right|} \sum_{g_{d+1} \in G^*_{p,m}(f)} \widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}), f).
\end{aligned}$$

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. [12, p. 77]). Thus,

$$\begin{aligned}\widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}^*), f) \leq & \frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}^*(f)} \widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}), f) \\ = & \frac{1}{\phi_p(f)} \sum_{g_{d+1} \in G_{p,m}^*(f)} \sum_{\substack{(\boldsymbol{h}, h_{d+1}) \in G_{p,m}^{d+1} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{h} \cdot \boldsymbol{g}^* + h_{d+1} g_{d+1} \equiv 0 (\bmod f)}} \prod_{i=1}^{d+1} \widetilde{r}_p(h_i, \gamma_i) \\ = & \frac{1}{\phi_p(f)} \sum_{(\boldsymbol{h}, h_{d+1}) \in G_{p,m}^{d+1} \setminus \{\boldsymbol{0}\}} \left(\prod_{i=1}^{d+1} \widetilde{r}_p(h_i, \gamma_i) \right) \sum_{\substack{g_{d+1} \in G_{p,m}^*(f) \\ \boldsymbol{h} \cdot \boldsymbol{g}^* + h_{d+1} g_{d+1} \equiv 0 (\bmod f)}} 1.\end{aligned}$$

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

$$\prod_{i=1}^{d+1} \widetilde{r}_p(h_i, \gamma_i) = \prod_{i=1}^{d+1} (1 + \gamma_i)$$

and

$$\sum_{\substack{g_{d+1} \in G_{p,m}^*(f) \\ \boldsymbol{h} \cdot \boldsymbol{g}^* + h_{d+1} g_{d+1} \equiv 0 (\bmod f)}} 1 = \left| G_{p,m}^*(f) \right| = \phi_p(f).$$

Consequently,

$$\begin{aligned}\widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}^*), f) \leq & - \prod_{i=1}^{d+1} (1 + \gamma_i) \\ & + \frac{1}{\phi_p(f)} \sum_{(\boldsymbol{h}, h_{d+1}) \in G_{p,m}^{d+1}} \left(\prod_{i=1}^{d+1} \widetilde{r}_p(h_i, \gamma_i) \right) \sum_{\substack{g_{d+1} \in G_{p,m}^*(f) \\ \boldsymbol{h} \cdot \boldsymbol{g}^* + h_{d+1} g_{d+1} \equiv 0 (\bmod f)}} 1.\end{aligned}$$

For all $(\boldsymbol{h}, h_{d+1}) \in G_{p,m}^{d+1}$,

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

where $\sum_{v \bmod f}$ and X_p are defined as in [12, p. 78]. We therefore have

$$\begin{aligned}\widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}^*), f) \leq & - \prod_{i=1}^{d+1} (1 + \gamma_i) + \frac{1}{\phi_p(f)} \frac{1}{p^m} \sum_{v \bmod f} \sum_{\boldsymbol{h} \in G_{p,m}^d} \left(\prod_{i=1}^{d} \widetilde{r}_p(h_i, \gamma_i) \right) \times \\ & \times X_p \left(\frac{v}{f} \boldsymbol{h} \cdot \boldsymbol{g}^* \right) \sum_{h \in G_{p,m}} \sum_{g \in G_{p,m}^*(f)} \widetilde{r}_p(h, \gamma_{d+1}) X_p \left(\frac{v}{f} h g \right).\end{aligned}$$

Define now

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

Then,

$$Y_p(0,f) = \phi_p(f) \sum_{h \bmod f} \widetilde{r}_p(h, \gamma_{d+1}).$$

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

$$\begin{aligned}
Y_p(v,f) &= \sum_{h \bmod f} \widetilde{r}_p(h, \gamma_{d+1}) \sum_{g \bmod f} X_p\left(\frac{v}{f}hg\right) \sum_{d|(g,f)} \mu_p(d) \\
&= \sum_{h \bmod f} \widetilde{r}_p(h, \gamma_{d+1}) \sum_{d|f} \mu_p(d) \sum_{\substack{g \bmod f \\ d|g}} X_p\left(\frac{v}{f}hg\right) \\
&= \sum_{h \bmod f} \widetilde{r}_p(h, \gamma_{d+1}) \sum_{d|f} \mu_p(d) \sum_{a \bmod f/d} X_p\left(\frac{v}{f}had\right) \\
&= \sum_{h \bmod f} \widetilde{r}_p(h, \gamma_{d+1}) \sum_{d|f} \mu_p\left(\frac{f}{d}\right) \sum_{a \bmod d} X_p\left(\frac{v}{d}ha\right).
\end{aligned}$$

Applying [12, (4.51)] to the innermost sum, we obtain

$$\begin{aligned}
Y_p(v,f) &= \sum_{h \bmod f} \widetilde{r}_p(h, \gamma_{d+1}) \sum_{\substack{d|f \\ d|vh}} \mu_p\left(\frac{f}{d}\right) p^{\deg(d)} \\
&= \sum_{d|f} \mu_p\left(\frac{f}{d}\right) p^{\deg(d)} \sum_{\substack{h \bmod f \\ d|vh}} \widetilde{r}_p(h, \gamma_{d+1}).
\end{aligned}$$

Now $d|vh$ if and only if $d/(d,v)$ divides h. Thus,

$$Y_p(v,f) = \sum_{d|f} \mu_p\left(\frac{f}{d}\right) p^{\deg(d)} E_p\left(\frac{d}{(d,v)}, f\right),$$

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

$$E_p(a,f) = \sum_{\substack{h \bmod f \\ a|h}} \widetilde{r}_p(h, \gamma_{d+1}).$$

If $a = f$, then

$$E_p(a,f) = \widetilde{r}_p(0, \gamma_{d+1}) = 1 + \gamma_{d+1}.$$

Now let $a \neq f$; then

$$E_p(a,f) = 1 + \gamma_{d+1} + \sum_{\substack{b \bmod f/a \\ b \neq 0}} \widetilde{r}_p(ab, \gamma_{d+1}).$$

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

$$\begin{aligned}\sum_{\substack{b \bmod f/a \\ b\neq 0}} \widetilde{r}_p(ab,\gamma_{d+1}) &= \gamma_{d+1} \sum_{\substack{b \bmod f/a \\ b\neq 0}} \frac{1}{p^{\deg(ab)+1}\sin^2(\frac{\pi}{p}\mathrm{sgn}(ab))} \\ &= \gamma_{d+1} p^{-\deg(a)-1} \sum_{\substack{b \bmod f/a \\ b\neq 0}} p^{-\deg(b)} \frac{1}{\sin^2(\frac{\pi}{p}\mathrm{sgn}(b))} \\ &= \gamma_{d+1} p^{-\deg(a)-1} \sum_{k=0}^{\deg(f/a)-1} p^{-k} p^k \sum_{z=1}^{p-1} \frac{1}{\sin^2(\frac{\pi}{p}z)} \\ &= \gamma_{d+1} \deg\left(\frac{f}{a}\right) p^{-\deg(a)-1} \sum_{z=1}^{p-1} \frac{1}{\sin^2(\frac{\pi}{p}z)} \\ &= \gamma_{d+1} T_p \deg\left(\frac{f}{a}\right) p^{-\deg(a)},\end{aligned}$$

where $T_p = \frac{p^2-1}{3p}$. Since, for $a = f$, $\deg(a/f) = 0$, we have for all $a \in S_p$ dividing f

$$\begin{aligned}E_p(a,f) &= 1 + \gamma_{d+1} + \gamma_{d+1} T_p \deg\left(\frac{f}{a}\right) p^{-\deg(a)} \\ &= 1 + \gamma_{d+1} + \gamma_{d+1} c_p \log N p^{-\deg(a)} - \gamma_i T_p \deg(a) p^{-\deg(a)},\end{aligned}$$

where c_p is defined as in Theorem 1.

Applying this formula with $a = d/(d,v)$, we obtain

$$\begin{aligned}Y_p(v,f) &= \sum_{d|f} \mu_p\left(\frac{f}{d}\right) p^{\deg(d)} \times \\ &\quad \times \left(1 + \gamma_{d+1} + \gamma_{d+1} c_p \log N p^{-\deg(d/(d,v))} - \gamma_{d+1} T_p \deg\left(\frac{d}{(d,v)}\right) p^{-\deg(d/(d,v))}\right) \\ &= \sum_{d|f} \mu_p\left(\frac{f}{d}\right) \times \\ &\quad \times \left(p^{\deg(d)}(1+\gamma_{d+1}) + \gamma_{d+1} c_p \log N p^{\deg((d,v))} - \gamma_{d+1} T_p \deg\left(\frac{d}{(d,v)}\right) p^{\deg((d,v))}\right) \\ &= \phi_p(f)(1+\gamma_{d+1}) + \gamma_{d+1} c_p \log N H_p^{(1)}(v,f) - \gamma_{d+1} T_p H_p^{(2)}(v,f),\end{aligned}$$

with

$$H_p^{(1)}(v,f) = \sum_{d|f} \mu_p\left(\frac{f}{d}\right) p^{\deg((d,v))},$$
$$H_p^{(2)}(v,f) = \sum_{d|f} \mu_p\left(\frac{f}{d}\right) \deg\left(\frac{d}{(d,v)}\right) p^{\deg((d,v))}.$$

Analyzing $H_p^{(1)}(v,f)$ as in [12], 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

$$\begin{aligned}
\widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}^*), f) \le & -\prod_{i=1}^{d+1}(1+\gamma_i) + \frac{1}{\phi_p(f)}\frac{1}{p^m}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) Y_p(0,f) \\
& + \frac{1}{\phi_p(f)}\frac{1}{p^m}\sum_{\substack{v \bmod f \\ v\neq 0}}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) Y_p(v,f) \\
= & -\prod_{i=1}^{d+1}(1+\gamma_i) + \frac{1}{p^m}\sum_{\boldsymbol{h}\in G_{p,m}^{d+1}}\prod_{i=1}^{d+1}\widetilde{r}_p(h_i,\gamma_i) \\
& + \frac{1+\gamma_{d+1}}{p^m}\sum_{\substack{v \bmod f \\ v\neq 0}}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) \\
& - \frac{1}{\phi_p(f)}\frac{\gamma_{d+1}}{p^m}\sum_{\substack{v \bmod f \\ v\neq 0}}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) T_p H_p^{(2)}(v,f) \\
= & \frac{1}{p^m}\sum_{\boldsymbol{h}\in G_{p,m}^{d+1}}\prod_{i=1}^{d+1}\widetilde{r}_p(h_i,\gamma_i) + (1+\gamma_{d+1})\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}^*, f) - \frac{1+\gamma_{d+1}}{p^m}\sum_{\boldsymbol{h}\in G_{p,m}^d}\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i) \\
& - \frac{1}{\phi_p(f)}\frac{\gamma_{d+1}}{p^m}\sum_{\substack{v \bmod f \\ v\neq 0}}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) T_p H_p^{(2)}(v,f).
\end{aligned}$$

The last equality follows from the formula

$$(1+\gamma_{d+1})\widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}^*, f) = -\prod_{i=1}^{d+1}(1+\gamma_i) + \frac{1+\gamma_{d+1}}{p^m}\sum_{v \bmod f}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right).$$

Now we consider the term

$$K_p^d(f) := -\frac{1}{\phi_p(f)}\frac{1}{p^m}\sum_{\substack{v \bmod f \\ v\neq 0}}\sum_{\boldsymbol{h}\in G_{p,m}^d}\left(\prod_{i=1}^{d}\widetilde{r}_p(h_i,\gamma_i)\right) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) T_p H_p^{(2)}(v,f).$$

To this end let

$$T(f) := \sum_{\substack{v \bmod f \\ v \neq 0}} J_p(v,f) X_p\left(\frac{v}{f}\boldsymbol{h}\cdot\boldsymbol{g}^*\right),$$

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 [12, pp. 82ff.], where it is shown that

$$J_p(v,f) = \frac{\deg(r)}{\phi_p\big(r^{e_r(f)-e_r(v)}\big)},$$

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 $0 \leq \deg(v) \leq \deg(f_1 f_2)$ 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 [12, p. 84]). We get

$$\begin{aligned}
T(f_1 f_2) &= \sum_{\substack{v \bmod f_1 f_2 \\ v \neq 0}} J_p(v, f_1 f_2) X_p\left(\frac{v}{f_1 f_2}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) \\
&= \sum_{\substack{v \bmod f_1 f_2 \\ v \neq 0 \\ \exists ! r : e_r(v) < e_r(f_1 f_2) \\ r | f_1}} J_p(v, f_1 f_2) X_p\left(\frac{v}{f_1 f_2}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) \\
&\quad + \sum_{\substack{v \bmod f_1 f_2 \\ v \neq 0 \\ \exists ! r : e_r(v) < e_r(f_1 f_2) \\ r | f_2}} J_p(v, f_1 f_2) X_p\left(\frac{v}{f_1 f_2}\boldsymbol{h}\cdot\boldsymbol{g}^*\right).
\end{aligned}$$

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

$$\begin{aligned}
&T(f_1 f_2) = \\
&= \sum_{\substack{v_1 f_2 \bmod f_1 f_2 \\ v_1 f_2 \neq 0 \\ \exists ! r : e_r(v_1 f_2) < e_r(f_1 f_2) \\ r | f_1}} J_p(v_1 f_2, f_1 f_2) X_p\left(\frac{v_1 f_2}{f_1 f_2}\boldsymbol{h}\cdot\boldsymbol{g}^*\right) + \sum_{\substack{v_2 f_1 \bmod f_1 f_2 \\ v_2 f_1 \neq 0 \\ \exists ! r : e_r(v_2 f_1) < e_r(f_1 f_2) \\ r | f_2}} J_p(v_2 f_1, f_1 f_2) X_p\left(\frac{v_2 f_1}{f_1 f_2}\boldsymbol{h}\cdot\boldsymbol{g}^*\right).
\end{aligned}$$

However, the latter expression equals

$$\sum_{\substack{v_1 \bmod f_1\\ v_1\neq 0\\ \exists! r: e_r(v_1)<e_r(f_1)}} J_p(v_1,f_1)X_p\left(\frac{v_1}{f_1}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)+\sum_{\substack{v_2 \bmod f_2\\ v_2\neq 0\\ \exists! r: e_r(v_2)<e_r(f_2)}} J_p(v_2,f_2)X_p\left(\frac{v_2}{f_2}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)=$$
$$=T(f_1)+T(f_2).$$

Hence T is additive. Let r be a monic and irreducible polynomial and $e\geq 1$, then

$$\begin{aligned}
T(r^e) &= \sum_{k=0}^{e-1}\sum_{\substack{v \bmod r^e\\ e_r(v)=k}} J_p(v,r^e)X_p\left(\frac{v}{r^e}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\\
&= \sum_{k=0}^{e-1}\sum_{\substack{v \bmod r^e\\ e_r(v)=k}} \frac{\deg(r)}{\phi_p(r^{e-k})}X_p\left(\frac{v}{r^e}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\\
&= \deg(r)\sum_{k=0}^{e-1}\frac{1}{\phi_p(r^{e-k})}\sum_{\substack{v \bmod r^e\\ e_r(v)=k}} X_p\left(\frac{v}{r^e}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\\
&= \deg(r)\sum_{k=0}^{e-1}\frac{1}{\phi_p(r^{e-k})}\times\\
&\quad\times\left[\sum_{r^k q \bmod r^e} X_p\left(\frac{r^k q}{r^e}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)-\sum_{r^{k+1} q \bmod r^e} X_p\left(\frac{r^{k+1} q}{r^e}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\right]\\
&= \deg(r)\sum_{k=0}^{e-1}\frac{1}{\phi_p(r^{e-k})}\sum_{q \bmod r^{e-k}} X_p\left(\frac{q}{r^{e-k}}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\\
&\quad-\deg(r)\sum_{k=1}^{e}\frac{1}{\phi_p(r^{e-k+1})}\sum_{q \bmod r^{e-k}} X_p\left(\frac{q}{r^{e-k}}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\\
&= \deg(r)\sum_{k=1}^{e-1}\left[\frac{1}{\phi_p(r^{e-k})}-\frac{1}{\phi_p(r^{e-k+1})}\right]\sum_{q \bmod r^{e-k}} X_p\left(\frac{q}{r^{e-k}}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)\\
&\quad+\deg(r)\frac{1}{\phi_p(r^e)}\sum_{q \bmod r^e} X_p\left(\frac{q}{r^e}\boldsymbol{h}\cdot\boldsymbol{g}^*\right)-\deg(r)\frac{1}{\phi_p(r)}\\
&\geq -\deg(r)\frac{1}{\phi_p(r)} = -\frac{\deg(r)}{p^{\deg(r)}-1}.
\end{aligned}$$

By additivity we obtain

$$T(f)\geq -\sum_{\substack{r\mid f\\ r\text{ irreducible}}}\frac{\deg(r)}{p^{\deg(r)}-1}$$

and therefore

$$K_p^d(f) \le \frac{T_p}{p^m} \left(\sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} \right) \sum_{\boldsymbol{h} \in G_{p,m}^d} \prod_{i=1}^{d} \widetilde{r}_p(h_i,\gamma_i).$$

We obtain

$$\widetilde{R}_{\boldsymbol{\gamma}}((\boldsymbol{g}^*, g_{d+1}^*), f) \le \frac{1}{p^m} \sum_{\boldsymbol{h} \in G_{p,m}^{d+1}} \prod_{i=1}^{d+1} \widetilde{r}_p(h_i,\gamma_i) + (1+\gamma_{d+1}) \widetilde{R}_{\boldsymbol{\gamma}}(\boldsymbol{g}^*, f)$$
$$- \frac{1+\gamma_{d+1}}{p^m} \sum_{\boldsymbol{h} \in G_{p,m}^d} \prod_{i=1}^{d} \widetilde{r}_p(h_i,\gamma_i) + \frac{T_p \gamma_{d+1}}{p^m} \left(\sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} \right) \sum_{\boldsymbol{h} \in G_{p,m}^d} \prod_{i=1}^{d} \widetilde{r}_p(h_i,\gamma_i). \tag{5}$$

Now we have

$$\sum_{\boldsymbol{h} \in G_{p,m}^d} \prod_{i=1}^{d} \widetilde{r}_p(h_i,\gamma_i) = \prod_{i=1}^{d} \left(1 + \gamma_i \left(1 + m\frac{p^2-1}{3p}\right)\right)$$

and thus it follows that

$$\frac{1}{p^m} \sum_{\boldsymbol{h} \in G_{p,m}^{d+1}} \prod_{i=1}^{d+1} \widetilde{r}_p(h_i,\gamma_i) - \frac{1+\gamma_{d+1}}{p^m} \sum_{\boldsymbol{h} \in G_{p,m}^d} \prod_{i=1}^{d} \widetilde{r}_p(h_i,\gamma_i)$$
$$+ \frac{T_p \gamma_{d+1}}{p^m} \left(\sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} \right) \sum_{\boldsymbol{h} \in G_{p,m}^d} \prod_{i=1}^{d} \widetilde{r}_p(h_i,\gamma_i)$$
$$= \frac{1}{p^m} \prod_{i=1}^{d} \left(1 + \gamma_i \left(1 + m\frac{p^2-1}{3p}\right)\right)$$
$$\left(1 + \gamma_{d+1}\left(1 + m\frac{p^2-1}{3p}\right) - 1 - \gamma_{d+1} + \gamma_{d+1}\frac{p^2-1}{3p} \left(\sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} \right)\right)$$
$$= \frac{\gamma_{d+1}}{p^m} \prod_{i=1}^{d} \left(1 + \gamma_i \left(1 + m\frac{p^2-1}{3p}\right)\right) \frac{p^2-1}{3p} \left(m + \sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} \right).$$

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

Remark 2 (1) Using ideas from [12, p. 84f.] it can be shown that

$$c_f = \sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} = O(\log m).$$

(2) If $f(x) = x^m$ we obtain

$$c_f = \sum_{\substack{r|f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)} - 1} = \frac{1}{p-1}.$$

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 [8], which is the reason why such lattice points are frequently called Korobov lattice points. A construction for polynomial Korobov lattice rules was proposed in [4] 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 [18].

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 [4, Algorithm 3.9] with f replaced by f_1.*

(2) Let the vector

$$w_s(b) := f_1(1, b, \ldots, b^{s-1}) + f_2(1, g_*, \ldots, g_*^{s-1}) \pmod{f}$$

and find $b_* \in G_{p,m_2} \setminus \{0\}$ such that $\widetilde{R}_{\boldsymbol{\gamma}}(w_s(b), f)$ is minimized with respect to b.

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 $b_* \in G_{p,m_2} \setminus \{0\}$ is chosen according to Algorithm 2, then we have*

$$\begin{aligned}
&\widetilde{R}_{\boldsymbol{\gamma}}(w_s(b_*), f) \\
&\leq \left(\frac{1}{p^{m_2}} + \frac{s-1}{p^{m_2}-1}\right) \frac{s-1}{p^{m_1}-1} \left(-\prod_{i=1}^{s}(1+\gamma_i) + \prod_{i=1}^{s}\left(1+\gamma_i\left(1+m_1\frac{p^2-1}{3p}\right)\right)\right) \\
&\quad + \frac{s-1}{p^{m_2}-1}\frac{s-1}{p^{m_1}-1}\left(-\prod_{i=1}^{s}(1+\sqrt{\gamma_i}) + \prod_{i=1}^{s}\left(1+\sqrt{\gamma_i}\left(1+m_2\frac{p^2-1}{3p}\right)\right)\right) \times \\
&\quad \times \left(-\prod_{i=1}^{s}(1+\sqrt{\gamma_i}) + \prod_{i=1}^{s}\left(1+\sqrt{\gamma_i}\left(1+m_1\frac{p^2-1}{3p}\right)\right)\right) \\
&\quad + \frac{s-1}{p^{m_2}-1}\frac{1}{p^{m_1}}\left(-\prod_{i=1}^{s}(1+\gamma_i) + \prod_{i=1}^{s}\left(1+\gamma_i\left(1+m_2\frac{p^2-1}{3p}\right)\right)\right).
\end{aligned}$$

Remark 3 If the weights satisfy $\sum_{i=1}^{\infty} \sqrt{\gamma_i} < \infty$ then using [7, 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 [17].

Proof. Define

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

It follows from Algorithm 2 that $\widetilde{R}_{\boldsymbol{\gamma}}(w_s(b_*), f) \le \widetilde{M}_s^{(K)}(f)$ and therefore it suffices to show that $\widetilde{M}_s^{(K)}(f)$ satisfies the bound from Theorem 3. We have

$$\begin{aligned}\widetilde{M}_s^{(K)}(f) &= \frac{1}{p^{m_2}-1} \sum_{b \in G_{p,m_2} \setminus \{0\}} \sum_{\substack{\boldsymbol{h} \in G_{p,m}^s \setminus \{\boldsymbol{0}\} \\ w_s(b)\cdot \boldsymbol{h} \equiv 0 \pmod{f}}} \prod_{i=1}^{s} \widetilde{r}_p(h_i, \gamma_i) \\ &= \frac{1}{p^{m_2}-1} \sum_{\boldsymbol{h} \in G_{p,m}^s \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{s} \widetilde{r}_p(h_i, \gamma_i) \sum_{b \in G_{p,m_2} \setminus \{0\}} \delta_f(w_s(b) \cdot \boldsymbol{h}),\end{aligned}$$

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

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

and hence

$$\begin{aligned}
\widetilde{M}_s^{(K)}(f) &= \frac{1}{p^{m_2}-1}\sum_{\boldsymbol{h}\in G_{p,m}^s\setminus\{\boldsymbol{0}\}}\left(\prod_{i=1}^s \widetilde{r}_p(h_i,\gamma_i)\right)\delta_{f_1}(\boldsymbol{h}\cdot(1,g_*,\ldots,g_*^{s-1}))\times\\
&\quad\times\sum_{b\in G_{p,m_2}\setminus\{0\}}\delta_{f_2}(\boldsymbol{h}\cdot(1,b,\ldots,b^{s-1}))\\
&= \frac{1}{p^{m_2}-1}\sum_{\substack{\boldsymbol{h}\in G_{p,m}^s\setminus\{\boldsymbol{0}\}\\ h_i\equiv 0 \pmod{f_2}, 1\le i\le s}}\left(\prod_{i=1}^s \widetilde{r}_p(h_i,\gamma_i)\right)\delta_{f_1}(\boldsymbol{h}\cdot(1,g_*,\ldots,g_*^{s-1}))\times\\
&\quad\times\sum_{b\in G_{p,m_2}\setminus\{0\}}\delta_{f_2}(\boldsymbol{h}\cdot(1,b,\ldots,b^{s-1}))\\
&\quad+\frac{1}{p^{m_2}-1}\sum_{\substack{\boldsymbol{h}\in G_{p,m}^s\setminus\{\boldsymbol{0}\}\\ \exists i: h_i\not\equiv 0 \pmod{f_2}}}\left(\prod_{i=1}^s \widetilde{r}_p(h_i,\gamma_i)\right)\delta_{f_1}(\boldsymbol{h}\cdot(1,g_*,\ldots,g_*^{s-1}))\times\\
&\quad\times\sum_{b\in G_{p,m_2}\setminus\{0\}}\delta_{f_2}(\boldsymbol{h}\cdot(1,b,\ldots,b^{s-1}))\\
&=: \Sigma_1+\Sigma_2.
\end{aligned}$$

If there is an index i such that $h_i \not\equiv 0 \pmod{f_2}$ then

$$\sum_{b\in G_{p,m_2}\setminus\{0\}}\delta_{f_2}(\boldsymbol{h}\cdot(1,b,\ldots,b^{s-1}))\le s-1,$$

since f_2 is irreducible. Otherwise

$$\sum_{b\in G_{p,m_2}\setminus\{0\}}\delta_{f_2}(\boldsymbol{h}\cdot(1,b,\ldots,b^{s-1}))=p^{m_2}-1.$$

Now

$$\Sigma_1=\sum_{\widetilde{\boldsymbol{h}}\in G_{p,m_1}^s\setminus\{\boldsymbol{0}\}}\prod_{i=1}^s \widetilde{r}_p(\widetilde{h}_i f_2,\gamma_i)\delta_{f_1}(\widetilde{\boldsymbol{h}}\cdot(1,g_*,\ldots,g_*^{s-1})),$$

since $\gcd(f_1,f_2)=1$. If $\widetilde{h}_i=0$, then $\widetilde{r}_p(\widetilde{h}_i f_2,\gamma_i)=\widetilde{r}_p(\widetilde{h}_i,\gamma_i)$ and otherwise (since f_2 is monic) $\widetilde{r}_p(\widetilde{h}_i f_2,\gamma_i)=\frac{1}{p^{m_2}}\widetilde{r}_p(\widetilde{h}_i,\gamma_i)$. Therefore

$$\Sigma_1\le\frac{1}{p^{m_2}}\sum_{\substack{\widetilde{\boldsymbol{h}}\in G_{p,m_1}^s\setminus\{\boldsymbol{0}\}\\ \widetilde{\boldsymbol{h}}\cdot(1,g_*,\ldots,g_*^{s-1})\equiv 0 \pmod{f_1}}}\prod_{i=1}^s \widetilde{r}_p(\widetilde{h}_i,\gamma_i)=:\frac{1}{p^{m_2}}\widetilde{R}_{\boldsymbol{\gamma}}(v_s(g_*),f_1).$$

We consider Σ_2:

$$\begin{aligned}
\Sigma_2 \leq & \frac{s-1}{p^{m_2}-1} \sum_{\boldsymbol{h} \in G^s_{p,m} \setminus \{\boldsymbol{0}\}} \left(\prod_{i=1}^{s} \widetilde{r}_p(h_i, \gamma_i) \right) \delta_{f_1}(\boldsymbol{h} \cdot (1, g_*, \ldots, g_*^{s-1})) \\
= & \frac{s-1}{p^{m_2}-1} \sum_{\boldsymbol{h} \in G^s_{p,m_1} \setminus \{\boldsymbol{0}\}} \left(\prod_{i=1}^{s} \widetilde{r}_p(h_i, \gamma_i) \right) \delta_{f_1}(\boldsymbol{h} \cdot (1, g_*, \ldots, g_*^{s-1})) \\
& + \frac{s-1}{p^{m_2}-1} \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \sum_{\widetilde{\boldsymbol{h}} \in G^s_{p,m_1}} \left(\prod_{i=1}^{s} \widetilde{r}_p(q_i f_1 + \widetilde{h}_i, \gamma_i) \right) \delta_{f_1}((\boldsymbol{q} f_1 + \widetilde{\boldsymbol{h}}) \cdot (1, g_*, \ldots, g_*^{s-1})) \\
= & \frac{s-1}{p^{m_2}-1} \widetilde{R}_{\boldsymbol{\gamma}}(v_s(g_*), f_1) \\
& + \frac{s-1}{p^{m_2}-1} \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \sum_{\boldsymbol{h} \in G^s_{p,m_1} \setminus \{\boldsymbol{0}\}} \left(\prod_{i=1}^{s} \widetilde{r}_p(q_i f_1 + h_i, \gamma_i) \right) \delta_{f_1}(\boldsymbol{h} \cdot (1, g_*, \ldots, g_*^{s-1})) \\
& + \frac{s-1}{p^{m_2}-1} \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{s} \widetilde{r}_p(q_i f_1, \gamma_i).
\end{aligned}$$

If $q_i = 0$ we have $\widetilde{r}_p(q_i f_1 + h_i, \gamma_i) = \widetilde{r}_p(h_i, \gamma_i) \leq \widetilde{r}_p(q_i, \sqrt{\gamma_i}) \widetilde{r}_p(h_i, \sqrt{\gamma_i})$. Otherwise we have

$$\widetilde{r}_p(q_i f_1 + h_i, \gamma_i) = \frac{\gamma_i}{p^{m_1}} r_p(q_i) \leq \widetilde{r}_p(h_i, \sqrt{\gamma_i}) \widetilde{r}_p(q_i, \sqrt{\gamma_i}).$$

Therefore we obtain

$$\begin{aligned}
\Sigma_2 \leq & \frac{s-1}{p^{m_2}-1} \widetilde{R}_{\boldsymbol{\gamma}}(v_s(g_*), f_1) \\
& + \frac{s-1}{p^{m_2}-1} \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \sum_{\boldsymbol{h} \in G^s_{p,m_1} \setminus \{\boldsymbol{0}\}} \left(\prod_{i=1}^{s} \widetilde{r}_p(q_i, \sqrt{\gamma_i}) \widetilde{r}_p(h_i, \sqrt{\gamma_i}) \right) \times \\
& \times \delta_{f_1}(\boldsymbol{h} \cdot (1, g_*, \ldots, g_*^{s-1})) \\
& + \frac{s-1}{p^{m_2}-1} \frac{1}{p^{m_1}} \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{s} \widetilde{r}_p(q_i, \gamma_i) \\
= & \frac{s-1}{p^{m_2}-1} \widetilde{R}_{\boldsymbol{\gamma}}(v_s(g_*), f_1) + \frac{s-1}{p^{m_2}-1} \widetilde{R}_{\sqrt{\boldsymbol{\gamma}}}(v_s(g_*), f_1) \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{s} \widetilde{r}_p(q_i, \sqrt{\gamma_i}) \\
& + \frac{s-1}{p^{m_2}-1} \frac{1}{p^{m_1}} \sum_{\boldsymbol{q} \in G^s_{p,m_2} \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{s} \widetilde{r}_p(q_i, \gamma_i),
\end{aligned}$$

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

By a slightly more careful derivation of [4, Theorem 3.10] we obtain

$$\widetilde{R}_{\boldsymbol{\gamma}}(v_s(g_*), f_1) \leq \frac{s-1}{p^{m_1}-1} \left(- \prod_{i=1}^{s} (1 + \gamma_i) + \prod_{i=1}^{s} \left(1 + \gamma_i \left(1 + m_1 \frac{p^2-1}{3p} \right) \right) \right) \tag{6}$$

and from [4, Lemma 3.3] we know that

$$\sum_{\boldsymbol{q}\in G^s_{p,m_2}\setminus\{\boldsymbol{0}\}} \prod_{i=1}^s \widetilde{r}_p(q_i,\gamma_i) = -\prod_{i=1}^s(1+\gamma_i) + \prod_{i=1}^s\left(1+\gamma_i\left(1+m_2\frac{p^2-1}{3p}\right)\right).$$

Therefore we obtain

$$\begin{aligned}\widetilde{M}_s^{(K)}(f) \leq & \frac{1}{p^{m_2}}\frac{s-1}{p^{m_1}-1}\left(-\prod_{i=1}^s(1+\gamma_i)+\prod_{i=1}^s\left(1+\gamma_i\left(1+m_1\frac{p^2-1}{3p}\right)\right)\right)\\ & +\frac{s-1}{p^{m_2}-1}\frac{s-1}{p^{m_1}-1}\left(-\prod_{i=1}^s(1+\gamma_i)+\prod_{i=1}^s\left(1+\gamma_i\left(1+m_1\frac{p^2-1}{3p}\right)\right)\right)\\ & +\frac{s-1}{p^{m_2}-1}\frac{s-1}{p^{m_1}-1}\left(-\prod_{i=1}^s(1+\sqrt{\gamma_i})+\prod_{i=1}^s\left(1+\sqrt{\gamma_i}m_2\frac{p^2-1}{3p}\right)\right)\times\\ & \times\left(-\prod_{i=1}^s(1+\sqrt{\gamma_i})+\prod_{i=1}^s\left(1+\sqrt{\gamma_i}\left(1+m_1\frac{p^2-1}{3p}\right)\right)\right)\\ & +\frac{s-1}{p^{m_2}-1}\frac{1}{p^{m_1}}\left(-\prod_{i=1}^s(1+\gamma_i)+\prod_{i=1}^s\left(1+\gamma_i\left(1+m_2\frac{p^2-1}{3p}\right)\right)\right).\end{aligned}$$

The result follows. □

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 degree $m_1,m_2,\ldots$ $\ldots,m_t$ 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 [4, Algorithm 3.9] with f replaced by f_1.*

(2) For fixed $l=2,\ldots,t$ let $c_{l-1}:=\prod_{j=1}^{l-1}f_j$. Let the vector

$$w_{s,l}(b):=c_{l-1}(1,b,\ldots,b^{s-1})+f_l w_{s,l-1}(a_{l-1})(\mathrm{mod}\, c_{l-1}f_l),$$

where $w_{s,l-1}(a_{l-1})$ is the vector found in the previous step, and find $b\in G_{p,m_l}\setminus\{0\}$ such that $\widetilde{R}_{\boldsymbol{\gamma}}(w_{s,l}(b),f)$ is minimized with respect to b.

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 $w_{s,t}(a_t)$ is constructed according to Algorithm 3, then we have*

$$\widetilde{R}_{\boldsymbol{\gamma}}(w_{s,t}(a_t), f) \leq \prod_{j=1}^{t} \left[\left(\frac{1}{p^{m_j}} + 2\frac{s-1}{p^{m_j}-1} \right) \prod_{i=1}^{s} \left(1 + \gamma_i' m_j \frac{p^2-1}{3p} \right) \right],$$

where $\gamma_i' = \max\{\gamma_i, \gamma_i^{1-1/t}, \gamma_i^{1-2/t}, \ldots, \gamma_i^{1/t}\}$.

Remark 4 If the weights satisfy $\sum_{i=1}^{\infty} \gamma_i^{1/t} < \infty$ then using [7, 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 [17].

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

$$\begin{aligned}\widetilde{R}_{\boldsymbol{\gamma}}(w_{s,t}(a_t), f) \leq & \left(\frac{1}{p^{m_t}} + 2\frac{s-1}{p^{m_t}-1} \right) \prod_{i=1}^{s} \left(1 + \gamma_i' m_t \frac{p^2-1}{3p} \right) \times \\ & \times \max(\widetilde{R}_{\boldsymbol{\gamma}}(w_{s,t-1}(a_{t-1}), f), \widetilde{R}_{\boldsymbol{\gamma}^{1-1/t}}(w_{s,t-1}(a_{t-1}), f)),\end{aligned}$$

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

3.5 Results for the unweighted star discrepancy

In this section we present results for the classical star discrepancy. 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 $R(\boldsymbol{g}, f)$ over all vectors $\boldsymbol{g} \in (G_{p,m}^*(f))^s$.

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

$$\begin{aligned}M_s(f) := & \frac{1}{\left|G_{p,m}^*(f)\right|^s} \sum_{\boldsymbol{g} \in (G_{p,m}^*(f))^s} R(\boldsymbol{g}, f) \\ = & \frac{1}{N}(c_p \log N + 1)^s - s c_p \frac{\log N}{N} + O\left(\frac{(\log\log N)^2}{N} \right),\end{aligned}$$

where $N = p^m$, and c_p is defined as above.

Proof. The proof is again similar to that of Theorem 4.43 in [12]. □

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 $d = 2, 3, \ldots, s$ find $g_d \in G^*_{p,m}(f)$ to minimize $R((g_1, \ldots, g_{d-1}, g_d), f)$.

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

$$\begin{aligned} R((g_1^*, \ldots, g_d^*), f) \leq & \frac{1}{p^m}\left(1 + m\frac{p^2-1}{3p}\right)^d \\ & + \frac{1}{p^m}\left(1 + m\frac{p^2-1}{3p}\right)^{d-1} \frac{2(p^2-1)}{3p} \left(\sum_{\substack{r \mid f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} \right). \end{aligned}$$

Proof. The proof is similar to that of Theorem 2. □

Remark 5 If $f(x) = x^m$ we have

$$\sum_{\substack{r \mid f \\ r \text{ irreducible}}} \frac{\deg(r)}{p^{\deg(r)}-1} = \frac{1}{p-1}$$

and therefore

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

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 [4, Algorithm 2.9] with f replaced by f_1.*
(2) Let the vector

$$w_s(b) := f_1(1, b, \ldots, b^{s-1}) + f_2(1, g_*, \ldots, g_*^{s-1}) \pmod{f}$$

and find $b_* \in G_{p,m_2} \setminus \{0\}$ such that $R(w_s(b), f)$ is minimized with respect to b.

Theorem 7 *Let $f \in \mathbb{F}_p[x]$ be the product of two different 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*

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

Proof. The proof is similar to that of Theorem 3. □

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

Algorithm 6 *(1) Find optimal $a_1 \in G_{p,m_1} \setminus \{0\}$ using [4, Algorithm 3.9] with f replaced by f_1.*

(2) For fixed $l = 2, \ldots, t$ let $c_{l-1} := \prod_{j=1}^{l-1} f_j$. Let the vector

$$w_{s,l}(b) := c_{l-1}(1, b, \ldots, b^{s-1}) + f_l w_{s,l-1}(a_{l-1})(\mathrm{mod} c_{l-1}f_l),$$

where $w_{s,l-1}(a_{l-1})$ is the vector found in the previous step, and find $b \in G_{p,m_l} \setminus \{0\}$ such that $R(w_{s,l}(b), f)$ is minimized with respect to b.

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 $w_{s,t}(a_t)$ is constructed according to Algorithm 6, then we have*

$$\begin{aligned}
R(w_{s,t}(a_t),f) \leq{}& \frac{s-1}{p^{m_1}-1}\left(1+m_1\frac{p^2-1}{3p}\right)^s \times \\
&\times \prod_{j=2}^{t}\left(\frac{1}{p^{m_j}}+\frac{s-1}{p^{m_j}-1}\left(1+m_j\frac{p^2-1}{3p}\right)^s\right) \\
&+\sum_{j=2}^{t}\frac{s-1}{p^{m_j}-1}\frac{1}{p^{\widetilde{m}_{j-1}}}\left(-1+\left(1+m_j\frac{p^2-1}{3p}\right)^s\right) \times \\
&\times \prod_{k=j+1}^{t}\left(\frac{1}{p^{m_k}}+\frac{s-1}{p^{m_k}-1}\left(1+m_k\frac{p^2-1}{3p}\right)^s\right),
\end{aligned}$$

where $\widetilde{m}_j = m_1 + \cdots + m_j$.

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 $\widetilde{R}_\gamma$ 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 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 [1] were 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 [3]; compare for example Table 1 with [4, Table 5.2]).

Fast component-by-component constructions of lattice rules have been introduced in [14–16]. It should also be possible to apply those ideas to the construction of polynomial lattice rules over reducible polynomials.

References

[1] J. Dick and F.Y. Kuo, Reducing the construction cost of the component-by-component construction of good lattice rules, Math. Comp. 73 (2004) 1967-1988.

[2] J. Dick and F.Y. Kuo, Constructing good lattice rules with millions of points, in: H. Niederreiter (Ed.), Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer, Berlin, 2004, pp. 181–197.

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

m	irreducible f	reducible f
2	0.5503950	0.6112040
3	0.5910270	0.6325640
4	0.5487220	0.5623250
5	0.4532520	0.4591280
6	0.3588920	0.3543220
7	0.2648100	0.2684380
8	0.1907370	0.1927350
9	0.1351930	0.1345680
10	0.0923820	0.0945389
11	0.0627568	0.0633650
12	0.0416007	0.0423129

Table 1
Comparison between irreducible and reducible f of the $\widetilde{R}_{\boldsymbol{\gamma}}$-values for the Korobov rule with parameters $s = 50$, $\gamma_j = \frac{1}{j^2}$.

[4] J. Dick, G. Leobacher and F. Pillichshammer, Construction algorithms for digital nets with small weighted star discrepancy, SIAM J. Num. Anal. 43 (2005) 76–95.

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

[6] M. Drmota and R. F. Tichy, Sequences, Discrepancies and Applications, Springer, Berlin, 1997.

[7] F. Hickernell and H. Niederreiter, The existence of good extensible rank-1 lattices, J. Complexity 19 (2003) 286-300.

[8] N.M. Korobov, Properties and calculation of optimal coefficients, Dokl. Akad. Nauk SSSR 132 (1960) 1009–1012. In Russian.

[9] L. Kuipers and H. Niederreiter, Uniform Distribution of Sequences, John Wiley, New York, 1974.

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

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

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

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

[14] D. Nuyens and R. Cools, Fast component-by-component constructions, a reprise for different kernels, in: H. Niederreiter and D. Talay (Eds.), Monte Carlo and Quasi-Monte Carlo Methods 2004, Springer, to appear.

[15] D. Nuyens and R. Cools, Fast algorithms for component-by-component construction of rank-1 lattice rules in shift-invariant reproducing kernel Hilbert spaces, Math. Comp., to appear.

[16] D. Nuyens and R. Cools, Fast component-by-component construction of rank-1 lattice rules with a non-prime number of points, J. Complexity 22 (2006) 4–28.

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

[18] X. Wang, I.H. Sloan and J. Dick, On Korobov lattice rules in weighted Korobov spaces, SIAM J. Num. Anal. 42 (2004) 1760–1779.