

## THE CONSTRUCTION OF EXTENSIBLE POLYNOMIAL LATTICE RULES WITH SMALL WEIGHTED STAR DISCREPANCY

JOSEF DICK

ABSTRACT. In this paper we introduce a construction algorithm for extensible polynomial lattice rules and we prove that the construction algorithm yields generating vectors of polynomials which are optimal for a range of moduli chosen in advance. The construction algorithm uses a sieve where the generating vectors are extended by one coefficient in each component at each step and where one keeps a certain number of good ones and discards the rest. We also show that the construction can be done component by component.

### 1. INTRODUCTION

We are interested in approximating a high dimensional integral  $\int_{[0,1]^s} F(\mathbf{x}) \, d\mathbf{x}$  by a quasi-Monte Carlo algorithm  $Q_{N,s}(F) = N^{-1} \sum_{n=0}^{N-1} F(\mathbf{x}_n)$ . The quadrature points  $\mathbf{x}_0, \dots, \mathbf{x}_{N-1}$  here are chosen deterministically with the aim of choosing them in a way which allows us to make use of the smoothness properties of the integrand. Indeed the Koksma-Hlawka inequality states (see [13, 18]) that

$$(1) \quad \left| \int_{[0,1]^s} F(\mathbf{x}) \, d\mathbf{x} - Q_{N,s}(F) \right| \leq V_\gamma(f) D_{N,\gamma}^*,$$

where  $V_\gamma(F)$  denotes the weighted variation of  $F$  in the sense of Hardy and Krause and where  $D_{N,\gamma}^*$  denotes the weighted star discrepancy of the points used in the quasi-Monte Carlo algorithm  $Q_{N,s}$ . Here  $\gamma = (\gamma_j)_{j \geq 1}$  is a sequence of non-negative real numbers called weights (see [18]). Let the discrepancy function  $\Delta(\alpha_1, \dots, \alpha_s)$  be given by

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

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

For  $u \subseteq \{1, \dots, s\}$  let  $\gamma_u = \prod_{j \in u} \gamma_j$ ,  $\gamma_\emptyset = 1$ ,  $|u|$  be the cardinality of  $u$ , and for a vector  $\mathbf{z} \in [0, 1]^s$  let  $\mathbf{z}_u$  denote the vector in  $[0, 1]^{|u|}$  containing only the components of  $\mathbf{z}$  whose indices are in  $u$ . Moreover we write  $(\mathbf{z}_u, \mathbf{1})$  for the vector that we obtain by replacing all the components of  $\mathbf{z}$  not in  $u$  by 1. Now for a point set  $\mathbf{x}_0, \dots, \mathbf{x}_{N-1}$  in  $[0, 1]^s$  and a sequence  $\gamma = (\gamma_j)_{j \geq 1}$  of weights the weighted star

---

Received by the editor April 19, 2006 and, in revised form, September 13, 2006.  
2000 *Mathematics Subject Classification*. Primary 11K45, 65C05, 65D30.

discrepancy  $D_{N,\gamma}^*$  is given by

$$D_{N,\gamma}^* = D_{N,\gamma}^*(\mathbf{x}_0, \dots, \mathbf{x}_{N-1}) = \sup_{\mathbf{z} \in [0,1]^s} \max_{\substack{u \subseteq \{1, \dots, s\} \\ u \neq \emptyset}} \gamma_u |\Delta(\mathbf{z}_u, \mathbf{1})|.$$

Hence by using quadrature points with small weighted star discrepancy one obtains a quadrature rule which yields a small integration error as seen by (1).

The quadrature points which we consider in this paper are polynomial lattices first introduced by Niederreiter in [12]; see also [10, 13]. Quasi-Monte Carlo rules using polynomial lattices are called polynomial lattice rules. These rules are very similar to lattice rules (see [13, 15]). A disadvantage of these types of rules used to be that the number of quadrature points had to be fixed in advance and it was not possible to extend the number of quadrature points so that the original point set could be reused. Hickernell and Hong [6] introduced a way out by a modification of lattice rules which can arbitrarily be extended in the number of quadrature points such that the original quadrature points are reused. Such lattice rules are called extensible lattice rules. The existence of such rules has been shown in [8]. Extensible polynomial lattice rules on the other hand have been introduced in [11] and the existence of good extensible polynomial lattice rules was shown in [14].

As explicit constructions for (polynomial) lattice rules are only known in two dimensions, computer search algorithms have been employed to find good (polynomial) lattice rules; see [2, 3, 4, 16, 17] and the references therein. For extensible (polynomial) lattice rules not even search algorithms are known which are guaranteed to produce a desired extensible (polynomial) lattice rule. Although some search algorithms have been used to find extensible lattice rules [1, 7], no proof that those algorithms will work has been provided. In this paper we fill this gap for polynomial lattice rules (a similar algorithm for lattice rules is considered in [5]). Our algorithm here uses a sieve to find an extensible polynomial lattice rule which works well for a whole range of moduli; see Section 3. We also show that this construction method can be combined with a component-by-component construction method (see [16, 17]) to speed up the construction; see Section 4.

## 2. PRELIMINARIES

We give the definition of polynomial lattice rules in the following.

**2.1. Polynomial lattice rules.** Let  $p$  be a prime number, let  $\mathbb{Z}_p = \{0, \dots, p-1\}$  denote the finite field of order  $p$ ,  $\mathbb{Z}_p[x]$  the set of all polynomials over  $\mathbb{Z}_p$  and let  $\mathbb{Z}_p((x^{-1}))$  be the field of formal Laurent series over  $\mathbb{Z}_p$ , i.e. the elements of  $\mathbb{Z}_p((x^{-1}))$  are of the form

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

where  $w$  is an arbitrary integer and all  $t_l \in \mathbb{Z}_p$ . Note that  $\mathbb{Z}_p((x^{-1}))$  contains the field of rational functions over  $\mathbb{Z}_p$  as a subfield.

We now define a mapping  $\nu_p^{(m)} : \mathbb{Z}_p((x^{-1})) \rightarrow [0, 1)$  by

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

where all  $t_l \in \mathbb{Z}_p$ .

With the above notation we can now introduce polynomial lattices. For a given dimension  $s \geq 1$  choose  $f \in \mathbb{Z}_p[x]$  with  $\deg(f) = m \geq 1$  and let  $\mathbf{g} = (g_1, \dots, g_s) \in \mathbb{Z}_p^s[x]$ . Then the polynomial lattice  $P(\mathbf{g}, f)$  is given by

$$\left( \nu_p^{(m)} \left( \frac{ng_1}{f} \right), \dots, \nu_p^{(m)} \left( \frac{ng_s}{f} \right) \right) \in [0, 1)^s,$$

where  $n$  runs through all polynomials in  $\mathbb{Z}_p[x]$  with degree smaller than  $m$ . A quasi-Monte Carlo rule using the point set  $P(\mathbf{g}, f)$  as quadrature points is called a *polynomial lattice rule*.

Such rules have spurred recent interest, as they have been shown to have very similar properties to ordinary lattice rules (see [3]) and have thus been established as a true alternative to ordinary lattice rules (for a definition of ordinary lattice rules see [13, 15]).

**2.2. Extensible polynomial lattice rules.** We now follow [14] in the definition of extensible polynomial lattices. We call a sequence  $F = (f_k)_{k \geq 1}$  of polynomials from  $\mathbb{Z}_p[x]$  a divisibility chain in  $\mathbb{Z}_p[x]$  if  $f_k$  divides  $f_{k+1}$  and  $1 \leq \deg(f_k) < \deg(f_{k+1})$  for all  $k \geq 1$ .

With a given divisibility chain  $F$  we now associate the set  $Y_F$  of all  $F$ -adic polynomials. That is,  $Y_F$  is the set of all formal sums

$$A = \sum_{k=0}^{\infty} a_k f_k$$

with  $f_0 = 1$ ,  $a_k \in \mathbb{Z}_p[x]$  and  $\deg(a_k) < \deg(f_{k+1}/f_k)$  for all  $k \geq 0$ . Note that if  $a_k = 0$  for all sufficiently large  $k$ , then  $A$  is just a polynomial in  $\mathbb{Z}_p[x]$  and thus  $\mathbb{Z}_p[x] \subseteq Y_F$ . Subsequently we will call the polynomials  $a_k$  the coefficients of  $A$  or simply coefficients.

Note that by taking the residue ring of all elements of  $Y_F$  taken modulo  $f_k$  for  $k \geq 1$  we obtain all polynomials in  $\mathbb{Z}_p[x]$  with degree smaller than  $\deg(f_k)$ . Throughout the paper we will use the following notation: let  $\mathbf{G} = (G_1, \dots, G_s) \in Y_F^s$ ; then by  $\mathbf{g}_k$  we denote the vector obtained by  $\mathbf{g}_k \equiv \mathbf{G} \pmod{f_k}$  for  $k \geq 1$ , i.e.,  $\mathbf{g}_k = (g_{1,k}, \dots, g_{s,k})$  with  $g_{j,k} \equiv G_j \pmod{f_k}$  and where  $\deg(g_{j,k}) < \deg(f_k)$  for all  $1 \leq j \leq s$  and all  $k \geq 1$ . An analogous notation is used for  $\mathbf{G}^*$  and  $G^*$ .

Thus for a given divisibility chain  $F$  and a generating vector  $\mathbf{G} \in Y_F^s$  we obtain for each  $k \geq 1$  a polynomial lattice  $P(\mathbf{g}_k, f_k)$  such that

$$P(\mathbf{g}_k, f_k) \subseteq P(\mathbf{g}_{k+1}, f_{k+1}) \text{ for all } k \geq 1,$$

where for each  $k \geq 1$  the set  $P(\mathbf{g}_k, f_k)$  is a polynomial lattice. Finally, the set

$$P(\mathbf{G}, F) = \bigcup_{k=1}^{\infty} P(\mathbf{g}_k, f_k)$$

is called an *extensible polynomial lattice*. A sequence of quadrature rules  $Q_{p^{\deg(f_k)}, s}$ , where  $Q_{p^{\deg(f_k)}, s}$  uses  $P(\mathbf{g}_k, f_k)$  as quadrature points, is called an *extensible polynomial lattice rule*.

In the following we will introduce, with some restrictions, a construction algorithm for extensible polynomial lattice rules. First, the range of moduli for which we want to construct an extensible polynomial lattice rule has to be chosen in advance. That is, choose  $m < n \in \mathbb{N}$ . Then for  $k = m + 1, \dots, n$  we construct polynomial lattices  $P(\mathbf{g}_k, f_k)$  such that  $P(\mathbf{g}_{m+1}, f_{m+1}) \subseteq \dots \subseteq P(\mathbf{g}_n, f_n)$ . Though

the construction algorithm below would also work in a more general setting we will in the following assume that  $f_k = f^k$ , where  $f$  is an irreducible polynomial in  $\mathbb{Z}_p[x]$  (for example  $f(x) = x$  would be a possible choice). This simplifies the notation somewhat. The number of points in  $P(\mathbf{g}_k, f^k)$  is in this case given by  $p^{k \deg(f)}$ . (Note that as we only deal with finitely extensible polynomial lattice rules it would actually be enough to replace the set  $Y_F$  with  $\mathbb{Z}_p[x]$ , as we only need to consider polynomials of finite degree.)

We now define a measure on the set of all nonzero polynomials in  $Y_F$  which are not divisible by  $f$ . Let this set be denoted by  $Y_F^*$ . Let  $V_{F,l}$  denote the subset of  $Y_F^*$  of all  $F$ -adic polynomials  $A = \sum_{k=0}^\infty a_k f^k$  for which the first  $l \geq 1$  coefficients  $a_0, \dots, a_{l-1}$  are prescribed. Then we set  $\mu_F(V_{F,l}) = (p^{\deg(f)} - 1)^{-1} p^{-(l-1)\deg(f)}$ . Now let  $\mu_F^{(s)}$  denote the product measure on  $Y_F^{*s}$  induced by  $\mu_F$ .

**2.3. A quality measure for polynomial lattice rules.** Let  $H_{p,m} = \{h \in \mathbb{Z}_p[x] : \deg(h) < m\}$  and for  $\mathbf{g} \in (\mathbb{Z}_p[x])^s$  and  $f \in \mathbb{Z}_p$  with  $\deg(f) \geq 1$  define

$$R_{p^{k \deg(f)},s,\gamma}(\mathbf{g}, f^k) = \sum_{\substack{\mathbf{h} \in H_{p,k \deg(f)}^s \setminus \{0\} \\ \mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f^k}}} \prod_{j=1}^s r_{p,\gamma_j}(h_j),$$

where  $\mathbf{h} = (h_1, \dots, h_s)$ ,  $r_{p,\gamma}(0) = 1 + \gamma$  and  $r_{p,\gamma}(h) = \gamma p^{-\kappa-1} \sin^{-2}(h^{(\kappa)}\pi/p)$  for  $h(x) = h^{(0)} + h^{(1)}x + \dots + h^{(\kappa)}x^\kappa$  with  $h^{(\kappa)} \neq 0$ . Note that  $R_{p^{k \deg(f)},s,\gamma}$  can be computed in  $\mathcal{O}(p^{k \deg(f)} s)$  operations as shown in [4] and can thus be used for computer search algorithms; see [2, 4].

From [4, Proposition 2.1] we obtain that the star discrepancy of a polynomial lattice  $P(\mathbf{g}, f^k)$  is bounded by

$$(2) \quad D_{p^{k \deg(f)},\gamma}^*(P(\mathbf{g}, f^k)) \leq \sum_{\substack{u \subseteq \{1, \dots, s\} \\ u \neq \emptyset}} \gamma_u (1 - (1 - p^{-k \deg(f)})^{|u|}) + R_{p^{k \deg(f)},s,\gamma}(\mathbf{g}, f^k).$$

Thus  $R_{p^{k \deg(f)},s,\gamma}$  can be used as a suitable quality measure for polynomial lattices. Note that the contribution of the first sum in (2) is negligible, as it converges faster than  $R_{p^{k \deg(f)},s,\gamma}$ ; see [9].

For a polynomial  $f \in \mathbb{Z}_p[x]$  with  $\deg(f) \geq 1$  now let  $H_{p,k \deg(f)}^*(f^k) = \{h \in H_{p,k \deg(f)} : \gcd(h, f) = 1\}$ . From [2, Theorem 2] (see also [13, Theorem 4.43]) we obtain that for any  $k \geq 1$  we have

$$(3) \quad \frac{1}{(p^{\deg(f)} - 1)^s p^{s(k-1)\deg(f)}} \sum_{\mathbf{g} \in (H_{p,k \deg(f)}^*(f^k))^s} R_{p^{k \deg(f)},s,\gamma}(\mathbf{g}, f^k) \leq p^{-k \deg(f)} \prod_{j=1}^s \left( 1 + \gamma_j \left( 1 + (k+1)\deg(f) \frac{p^2 - 1}{3p} \right) \right).$$

For any integer  $k \geq 1$  and real numbers  $c \geq 1$  now let

$$C_{s,p^{k \deg(f)}}(c) = \{\mathbf{G} \in Y_F^{*s} : R_{p^{k \deg(f)},s,\gamma}(\mathbf{g}_k, f^k) \leq c \Delta(R_{p^{k \deg(f)},s,\gamma})\},$$

where  $\Delta(R_{p^{k \deg(f)},s,\gamma})$  is the bound from (3) and  $\mathbf{g}_k \equiv \mathbf{G} \pmod{f^k}$ . Then, as  $R_{p^{k \deg(f)},s,\gamma}$  is non-negative, Markov's inequality implies the following result.

**Theorem 1.** *Let  $f \in \mathbb{Z}_p[x]$  be irreducible. Then for all integers  $k \geq 1$  and real numbers  $c \geq 1$  we have*

$$\mu_F^{(s)}(\mathcal{C}_{s,p^k \deg(f)}(c)) > 1 - c^{-1}.$$

3. THE SIEVE PRINCIPLE

We now want to construct polynomial lattice rules which work well for several choices of  $k$ . Let  $p^{(m+1) \deg(f)}$  be the lowest number of points and  $p^n \deg(f)$  the largest number of points in which we are interested, i.e.,  $m < n$ . Then for each  $k = m + 1, \dots, n$  we can define a set  $\mathcal{C}_{s,p^k \deg(f)}(c)$ . In order to obtain a generating vector which works well for all choices of  $k = m + 1, \dots, n$  we need to show that the intersection  $\bigcap_{k=m+1}^n \mathcal{C}_{s,p^k \deg(f)}(c)$  is not empty, or equivalently, has measure greater than 0. To this end choose  $0 < c_{m+1}, \dots, c_n < 1$ . Then we have

$$\begin{aligned} \mu_F^{(s)}\left(\bigcap_{k=m+1}^n \mathcal{C}_{s,p^k \deg(f)}(c_k)\right) &\geq 1 - \mu_F^{(s)}\left(\bigcup_{k=m+1}^n \mathcal{C}'_{s,p^k \deg(f)}(c_k)\right) \\ &\geq 1 - \sum_{k=m+1}^n \mu_F^{(s)}(\mathcal{C}'_{s,p^k \deg(f)}(c_k)) \\ &> 1 - \sum_{k=m+1}^n c_k^{-1}, \end{aligned}$$

where  $\mathcal{C}'_{s,p^k \deg(f)}(c)$  stands for the complement of  $\mathcal{C}_{s,p^k \deg(f)}(c)$ , i.e.,  $\mathcal{C}'_{s,p^k \deg(f)}(c) = Y_F^{*s} \setminus \mathcal{C}_{s,p^k \deg(f)}(c)$ . Thus by choosing  $c_{m+1}, \dots, c_n$  such that

$$\sum_{k=m+1}^n c_k^{-1} \leq 1$$

it follows that the measure of  $\bigcap_{k=m+1}^n \mathcal{C}_{s,p^k \deg(f)}(c_k)$  is greater than 0 and hence this set is not empty, which implies that there is a generating vector which works well for all  $m < k \leq n$ . For example choosing all  $c_k = n - m$  would be a possible choice.

A straightforward algorithm would now find sets  $\mathcal{C}_{s,p^k \deg(f)}(c_k)$  for all  $k = m + 1, \dots, n$  and then search for a vector which lies in all of those sets. Note that for a vector  $\mathbf{G}$  in a set  $\mathcal{C}_{s,p^k \deg(f)}(c)$  only the first  $k$  coefficients in each coordinate matter, i.e., for any other vector  $\mathbf{L} \in Y_F^{*s}$  with  $\mathbf{L} \equiv \mathbf{G} \pmod{f^k}$  we have  $R_{p^k \deg(f),s}(\mathbf{L}) = R_{p^k \deg(f),s}(\mathbf{G})$ , hence there is only a finite set of relevant coefficients for each vector in  $\mathcal{C}_{s,p^k \deg(f)}(c)$  and the remaining coefficients can be chosen arbitrarily. On the other hand the number of vectors in  $\mathcal{C}_{s,p^k \deg(f)}(c)$  is of course infinite.

**3.1. The Sieve Algorithm.** Let us now start with  $k = m + 1$ . Then we use computer search to find  $(1 - c_{m+1}^{-1})p^{s(m+1) \deg(f)}$  vectors which satisfy the desired bound. Next we want to find vectors which are in the intersection  $\mathcal{C}_{s,p^{(m+1) \deg(f)}}(c_{m+1}) \cap \mathcal{C}_{s,p^{(m+2) \deg(f)}}(c_{m+2})$ . As the vectors now also need to lie in  $\mathcal{C}_{s,p^{(m+1) \deg(f)}}(c_{m+1})$  we only need to extend the vectors from the previous search by one new coefficient in each coordinate. Out of those newly obtained vectors we keep at least  $\lfloor (1 - c_{m+1}^{-1} - c_{m+2}^{-1})p^{s(m+1) \deg(f)} + 1 \rfloor$  new vectors which satisfy the desired bound and discard the rest of them. The existence of a sufficient number of good generating vectors is secured by the above arguments.

We continue this way, always adding coefficients to the remaining set of vectors which are left over from the previous step until we finally obtain a vector which lies in the set  $\bigcap_{k=m+1}^n \mathcal{C}_{s,p^k \deg(f)}(c_k)$ .

**3.2. An upper bound on  $R_{p^k \deg(f),s,\gamma}$  for vectors found by the Sieve Algorithm.** The following theorem is now implied by the observations above.

**Theorem 2.** *Let  $m < n \in \mathbb{N}$ . Let  $\mathbf{g}^* \in Y_F^{*s}$  be constructed by the Sieve Algorithm. Then for all  $k = m + 1, \dots, n$  we have*

$$R_{p^k \deg(f),s,\gamma}(\mathbf{g}^*) \leq c_k \Delta(R_{p^k \deg(f),s,\gamma}).$$

Using the Sieve Algorithm based on  $R_{p^m,s,\gamma}$  we can now obtain polynomial lattices with small star discrepancy as implied by (2) and Theorem 2. Note that strong tractability results, i.e., an upper bound on the worst-case error which is independent of the dimension, can be obtained if  $\sum_{j=1}^\infty \gamma_j < \infty$ ; see [2, 4].

4. A COMPONENT-BY-COMPONENT SIEVE ALGORITHM

In this section we show that polynomial lattice rules can also be constructed component-by-component, a method first introduced in [17] and further considered in [16]. The main advantage is that this algorithm is much faster, as the size of the search space is drastically reduced.

Before we can introduce this algorithm we need some further details. First note that for given  $d \geq 1$  and  $G_1, \dots, G_d \in Y_F^*$  we can write

$$\begin{aligned} R_{p^k \deg(f),d,\gamma}(\mathbf{g}_k, f^k) &= (1 + \gamma_d) R_{p^k \deg(f),d-1,\gamma}((g_{1,k}, \dots, g_{d-1,k}), f^k) \\ &+ S_{p^k \deg(f),d,\gamma}((g_{1,k}, \dots, g_{d-1,k}, g_{d,k}), f^k), \end{aligned} \tag{4}$$

where

$$\begin{aligned} &S_{p^k \deg(f),d,\gamma}((g_{1,k}, \dots, g_{d-1,k}, g_{d,k}), f^k) \\ &= \sum_{h_d \in H_{p,k \deg(f)} \setminus \{0\}} \sum_{\substack{h \in H_{p,k \deg(f)}^{d-1} \\ (h, h_d) \cdot \mathbf{g}_k \equiv 0 \pmod{f^k}}} \prod_{j=1}^d r_{p,\gamma_j}(h_j). \end{aligned}$$

From the proof of [2, Theorem 2] we obtain that for any  $k \geq 1, d \geq 2$  and fixed  $G_1^*, \dots, G_{d-1}^* \in Y_F^*$  we have

$$\begin{aligned} &\frac{1}{(p^{\deg(f)} - 1)p^{(k-1)\deg(f)}} \sum_{g \in H_{p,k \deg(f)}^*(f^k)} S_{p^k \deg(f),d,\gamma}((g_1^*, \dots, g_{d-1,k}^*, g), f^k) \\ (5) \quad &\leq p^{-k \deg(f)} \gamma_d \deg(f) (k + 1) \frac{p^2 - 1}{3p} \prod_{j=1}^{d-1} \left( 1 + \gamma_j \left( 1 + k \deg(f) \frac{p^2 - 1}{3p} \right) \right). \end{aligned}$$

For  $d \geq 2$  and given  $G_1, \dots, G_{d-1} \in Y_F^*$  now let

$$\begin{aligned} &\mathcal{D}_{d,p^k \deg(f)}((G_1, \dots, G_{d-1}), c) \\ &= \{G_d \in Y_F^* : S_{p^k \deg(f),d,\gamma}((g_{1,k}, \dots, g_{d-1,k}, g_{d,k}), f^k) \leq c \Delta(S_{p^k \deg(f),d,\gamma})\}, \end{aligned}$$

where  $\Delta(S_{p^k \deg(f),d,\gamma})$  denotes the bound in (5).

**4.1. The Component-by-Component Sieve Algorithm.** The Component-by-Component Sieve Algorithm now works the following way. Again choose  $m$  and  $n$  as for the Sieve Algorithm. We start with dimension  $s = 1$ . As we assumed that  $f$  is irreducible we may without loss of generality choose  $G_1^* = 1$ . This is because in dimension  $s = 1$  any polynomial  $G_1$  which is not divisible by  $f$  yields the same polynomial lattice. Note that in this case it follows that  $R_{p^{k \deg(f)}, 1, \gamma}((g_{1,k}^*), f^k) = 0$ . Now with  $G_1^* = 1$  fixed we seek the next coordinate  $G_2$ , but here we can just employ the Sieve Algorithm of the previous section where  $G_1^*$  is fixed and the sets  $\mathcal{C}_{2, p^{k \deg(f)}}(c_k)$  are replaced by  $\mathcal{D}_{2, p^{k \deg(f)}}((G_1^*), c)$ , and the quality measure  $R_{p^{k \deg(f)}, 2, \gamma}(\mathbf{g}_k, f^k)$  replaced by  $S_{p^{k \deg(f)}, 2, \gamma}((g_{1,k}^*), f^k)$ . Note that the latter can be computed using the identity (4). This way we obtain a vector  $G_2^*$  which lies in the set  $\bigcap_{k=m+1}^n \mathcal{D}_{2, p^{k \deg(f)}}((G_1^*), c_k)$ . Now with  $G_1^*, G_2^*$  fixed, using the Sieve Algorithm again, we can now obtain a vector  $G_3^*$  which lies in the set  $\bigcap_{k=m+1}^n \mathcal{D}_{3, p^{k \deg(f)}}((G_1^*, G_2^*), c_k)$ . In general, for  $d = 2, \dots, s$  we can use the Sieve Algorithm to obtain numbers  $G_d^*$  which lie in the intersection of the sets  $\mathcal{D}_{d-1, p^{k \deg(f)}}((G_1^*, \dots, G_{d-1}^*), c_k)$ . The construction cost is now much reduced because the size of the set  $\mathcal{D}_{d-1, p^{k \deg(f)}}((G_1^*, \dots, G_{d-1}^*), c_k)$  is much smaller compared to the size of  $\mathcal{C}_{s, p^{k \deg(f)}}(c_k)$ .

**4.2. An upper bound on  $R_{p^{k \deg(f)}, s, \gamma}$  for vectors found by the Component-by-Component Sieve Algorithm.** The following theorem is now implied by the construction of the vector  $\mathbf{G}^* = (G_1^*, \dots, G_s^*)$ .

**Theorem 3.** *Let  $m < n \in \mathbb{N}$ . Let  $\mathbf{G}^* \in Y_F^{*s}$  be constructed by the Component-by-Component Sieve Algorithm. Then for all  $k = m + 1, \dots, n$  we have*

$$R_{p^{k \deg(f)}, s, \gamma}(\mathbf{G}^*, f^k) \leq c_k \Delta(R_{p^{k \deg(f)}, s, \gamma}).$$

Using the Component-by-Component Sieve Algorithm based on  $R_{p^m, s, \gamma}$  we can now obtain polynomial lattices with small star discrepancy as implied by (2) and Theorem 3. Note that strong tractability results, i.e., an upper bound on the worst-case error which is independent of the dimension, can be obtained if  $\sum_{j=1}^\infty \gamma_j < \infty$ ; see [2, 4].

5. SOME GENERALIZATIONS AND OBSERVATIONS

Note that if we choose the  $c_k$ 's such that  $\sum_{k=m+1}^n c_k^{-1} < 1$  one can continue the (Component-by-Component) Sieve Algorithm at a later stage if necessary. Further it is clear from the (Component-by-Component) Sieve Algorithm that one does not necessarily have to increase the number of points by a factor of  $p^{\deg(f)}$  in each step. Because of the probabilistic arguments involved one can actually choose arbitrary powers of  $p^{\deg(f)}$ . (Note that the smallest possible value of  $p^{\deg(f)}$  is 2, which is for example obtained by choosing  $p = 2$  and  $f(x) = x$ .) Hence we do not need to let  $k$  run from  $m + 1$  to  $n$ , but we could choose a finite subset  $K \subset \mathbb{N}$  and construct a generating vector which works well for all choices  $k$  in  $K$ .

A simple way of choosing the values of  $c_k$  would be  $c_k = n - m$  for all  $k = m + 1, \dots, n$ . On the other hand this might give a suboptimal bound for small  $k$ . Hence one strategy of choosing  $c_k$  would be to obtain a balance of the bound in Theorem 2 across all choices of  $k$ . Further note that the (Component-by-Component) Sieve Algorithm does not necessarily have to start with the smallest value of  $k$ , but can start at any value  $k \in K$ . In order to speed up the algorithm it would of course

be advantageous to order the values of  $k \in K$  such that the number of vectors which one needs to consider in the (Component-by-Component) Sieve Algorithm is minimized.

Using the fact that there are different generating vectors which yield the same polynomial lattice rule, the number of generating vectors in the (Component-by-Component) Sieve Algorithm can be reduced even further which will make the construction faster.

#### ACKNOWLEDGMENTS

Valuable comments from F. Pillichshammer, B. Waterhouse and the referee are gratefully acknowledged. The support of the ARC under its Center of Excellence program is also gratefully acknowledged.

#### REFERENCES

- [1] R. Cools, F.Y. Kuo and D. Nuyens, Constructing embedded lattice rules for multivariate integration. *SIAM J. Sci. Comp.*, 28 (2006), 2162–2188. MR2272256
- [2] J. Dick, P. Kritzer, G. Leobacher and F. Pillichshammer, Constructions of general polynomial lattice rules based on the weighted star discrepancy. To appear in *Finite Fields and their Appl.*, 2007.
- [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. MR2164102 (2006e:65049)
- [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. MR2177135 (2006h:11090)
- [5] J. Dick, F. Pillichshammer and B.J. Waterhouse, A Sieve Algorithm for the construction of extensible lattice rules. To appear in *Math. Comp.* (2007).
- [6] F.J. Hickernell and H.S. Hong, Computing multivariate normal probabilities using rank-1 lattice sequences. In: *Proceedings of the Workshop on Scientific Computing*, Hong Kong, G. H. Golub, S. H. Lui, F. T. Luk, and R. J. Plemmons (Eds.), Springer, Singapore, 1997, 209–215. MR1729661
- [7] F.J. Hickernell, H.S. Hong, P. L'Écuyer and C. Lemieux, Extensible lattice sequences for quasi-Monte Carlo quadrature. *SIAM J. Sci. Comput.*, 22 (2000), 1117–1138. MR1785348 (2001h:65032)
- [8] F.J. Hickernell and H. Niederreiter, The existence of good extensible rank-1 lattices. *J. Complexity*, 19 (2003), 286–300. MR1984115 (2004c:65015)
- [9] S. Joe, Component by component construction of rank-1 lattice rules having  $O(n^{-1}(\ln(n))^d)$  star discrepancy. In: *Monte Carlo and quasi-Monte Carlo methods 2002*, H. Niederreiter (Ed.), Springer, Berlin, 2004, 293–298. MR2076940
- [10] P. L'Écuyer, Polynomial integration lattices. In: *Monte Carlo and Quasi-Monte Carlo Methods 2002*, H. Niederreiter (Ed.), Springer, Berlin, 2004, 73–98. MR2076607
- [11] P. L'Écuyer and C. Lemieux, Recent advances in randomized quasi-Monte Carlo methods. In: *Modeling Uncertainty: An Examination of Stochastic Theory, Methods and Applications*, M. Dror, P. L'Écuyer and F. Szidarovszky (Eds.), Kluwer, Boston, 2002, 419–474. MR1893290
- [12] H. Niederreiter, Low-discrepancy point sets obtained by digital constructions over finite fields. *Czechoslovak Math. J.*, 42 (1992), 143–166. MR1152177 (93c:11055)
- [13] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*. CBMS–NSF Series in Applied Mathematics 63, SIAM, Philadelphia, 1992. MR1172997 (93h:65008)
- [14] H. Niederreiter, The existence of good extensible polynomial lattice rules. *Monatsh. Math.*, 139 (2003), 295–307. MR2001711 (2004j:11087)
- [15] I.H. Sloan and S. Joe, *Lattice Methods for Multiple Integration*. Clarendon Press, Oxford, 1994. MR1442955 (98a:65026)
- [16] I.H. Sloan, F.Y. Kuo and S. Joe, Constructing randomly shifted lattice rules in weighted Sobolev spaces. *SIAM J. Numer. Anal.*, 40 (2002), 1650–1665. MR1950616 (2003m:65031)

- [17] I.H. Sloan and A.V. Reztsov, Component-by-component construction of good lattice rules. *Math. Comp.*, 71 (2002), 263–273. MR1862999 (2002h:65028)
- [18] I.H. Sloan and H. Woźniakowski, When are quasi-Monte Carlo algorithms efficient for high dimensional integrals? *J. Complexity*, 14 (1998), 1–33. MR1617765 (99d:65384)

SCHOOL OF MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY 2052, AUSTRALIA  
*Current address:* UNSW Asia, 1 Kay Siang Road, Singapore 248922  
*E-mail address:* `j.dick@unswasia.edu.sg`