Monatsh. Math. 139, 295–307 (2003)
DOI 10.1007/s00605-002-0530-z

Monatshefte für
Mathematik
Printed in Austria

The Existence of Good Extensible Polynomial Lattice Rules[1]

By

Harald Niederreiter

National University of Singapore, Republic of Singapore

Received April 30, 2002; in revised form August 21, 2002
Published online April 4, 2003

Abstract. Extensible (polynomial) lattice rules have been introduced recently and they are convenient tools for quasi-Monte Carlo integration. It is shown in this paper that for suitable infinite families of polynomial moduli there exist generating parameters for extensible rank-1 polynomial lattice rules such that for all these infinitely many moduli and all dimensions s the quantity $R^{(s)}$ and the star discrepancy are small. The case of Korobov-type polynomial lattice rules is also considered.

2000 Mathematics Subject Classification: 11K45, 65C05, 65D30
Key words: Quasi-Monte Carlo methods, digital nets, lattice rules, polynomial lattice rules

1. Introduction

A useful construction of digital nets for quasi-Monte Carlo methods is based on rational functions over finite fields. This construction was introduced by the author [12] and is also described in [13, Section 4.4]. The construction can be viewed as an analog of the construction of good lattice points (see [13, Chapter 5], [18] for the latter). Instead of an integer at least 2 which serves as the modulus for good lattice points, we choose a polynomial f over a finite field with $\deg(f) \geqslant 1$. Whereas good lattice points are determined by choosing s additional integers, where $s \geqslant 1$ is a given dimension, in the digital net construction we select s additional polynomials over the finite field. These polynomials matter only modulo f. A detailed description of the construction will be given in Section 2. This construction can now be viewed as an important special case in the theory of polynomial lattice rules which was recently developed by Lemieux and L'Ecuyer [8] (see also [7, Section 3.2.4]). In fact, the construction considered in the present paper is the rank-1 case of polynomial lattice rules, just as good lattice points are the rank-1 case of lattice rules.

Existence theorems for good lattice points form the centerpiece of the theory of rank-1 lattice rules (see [10], [13, Chapter 5], [15], [18]). Similarly, we have existence theorems for good rank-1 polynomial lattice rules (see [4], [5], [12],

[1]This research was partially supported by the grant POD0103223 with Temasek Laboratories in Singapore.

[13, Section 4.4], [17]). The proofs of these existence theorems are nonconstructive. Therefore, explicit parameters for good rank-1 polynomial lattice rules are obtained by computer search methods. The first such computer searches were carried out by Hansen, Mullen, and Niederreiter [1], and this work was continued in [5], [16], [17].

Good parameters for rank-1 lattice rules and for rank-1 polynomial lattice rules usually depend on the modulus and the dimension s. Recently, a major step was taken by Hickernell *et al.* [2] who proposed the idea of *extensible lattices*, i.e., of good parameters for rank-1 lattice rules that work simultaneously for infinitely many moduli (the moduli are, in fact, powers of a fixed integer base $b \geqslant 2$). This idea was further refined by Hickernell and Niederreiter [3] who proved an existence theorem for good parameters for rank-1 lattice rules that work not only for all moduli b^k, $k = 1, 2, \ldots$, but also for all dimensions $s \geqslant 1$ simultaneously. Of course, these parameters have to be doubly infinite in some sense (indeed, infinite tuples of b-adic integers are considered).

The main result of this paper is an analog of the existence theorem of Hickernell and Niederreiter [3] for rank-1 polynomial lattice rules (see Theorem 3 below). We arrive in this way at *extensible polynomial lattice rules* which work simultaneously for infinitely many polynomial moduli and all dimensions $s \geqslant 1$. The desirability of extensible polynomial lattice rules is briefly mentioned in L'Ecuyer and Lemieux [7, Section 3.5]. We consider not only sequences of moduli which are powers of a fixed polynomial of positive degree, but more generally divisibility chains of polynomials (see Definition 1).

In Section 2 we set up the notation, define the digital nets that form the basis of this paper, and introduce concepts that are crucial for the proof of our existence theorem. Section 3 contains the proof of this existence theorem and some consequences for the star discrepancy and the quality parameter of the digital nets. We also show how this existence theorem leads to the construction of infinite sequences with desirable properties. Section 4 establishes analogous results for a one-parameter subfamily of these digital nets, the "Korobov point sets". The method yields also a new result for Korobov lattice rules (see Remark 11).

2. Basic Definitions and Notation

Throughout this paper, p will denote a prime number and $\mathbb{F}_p$ the finite field of order p which we can identify as a set with $\{0, 1, \ldots, p-1\}$. Let $\mathbb{F}_p[x]$ be the polynomial ring over $\mathbb{F}_p$ in the variable x and $\mathbb{F}_p((x^{-1}))$ the field of formal Laurent series over $\mathbb{F}_p$ in the variable x^{-1}. Note that $\mathbb{F}_p((x^{-1}))$ contains the field $\mathbb{F}_p(x)$ of rational functions over $\mathbb{F}_p$ as a subfield. The case of a finite prime field allows us to simplify the general construction principle for digital nets by choosing all the bijections in [13, p. 63] to be identity maps.

For a given dimension $s \geqslant 1$, let $f \in \mathbb{F}_p[x]$ with $\deg(f) = m \geqslant 1$ be a chosen polynomial modulus. Furthermore, let $\mathbf{g} = (g_1, \ldots, g_s) \in \mathbb{F}_p[x]^s$ be an s-tuple of polynomials. These are the basic parameters of the point set $P(\mathbf{g}, f)$ we are going to construct. We use the description of $P(\mathbf{g}, f)$ given in [14, Section 2.4] which, in the case we are considering (all bijections in [13, p. 63] are identity maps), is

simpler than the original definition in [12]. First, define $\tau_p^{(m)} : \mathbb{F}_p((x^{-1})) \to [0,1)$ by

$$\tau_p^{(m)}\left(\sum_{j=w}^{\infty} b_j x^{-j}\right) := \sum_{j=\max(1,w)}^{m} b_j p^{-j}, \tag{1}$$

where all $b_j \in \mathbb{F}_p = \{0,1,\ldots,p-1\}$. Then $P(\mathbf{g}, f)$ consists of the p^m points

$$\left(\tau_p^{(m)}\left(\frac{ng_1}{f}\right),\ldots,\tau_p^{(m)}\left(\frac{ng_s}{f}\right)\right) \in [0,1)^s, \tag{2}$$

where n runs through all polynomials over $\mathbb{F}_p$ with $\deg(n) < m$. It is clear that $g_1,\ldots,g_s$ are relevant only modulo f. In the case where f is irreducible over $\mathbb{F}_p$, the construction of $P(\mathbf{g}, f)$ is equivalent to a special case of an earlier construction in Niederreiter [11] (compare with [12, Remark 5] and [13, Remark 4.45]).

The point set $P(\mathbf{g}, f)$ is a digital (t, m, s)-net in base p (see [13, Theorem 4.42]) and gives rise to a rank-1 polynomial lattice rule for quasi-Monte Carlo integration. The quality of the point set $P(\mathbf{g}, f)$ can be measured in various ways, for instance, by the quality parameter t of the digital net. For our purposes, the quantity $R^{(s)}(\mathbf{g}, f)$ to be defined in (3) is the most useful one. We recall that for any s-tuple $\mathbf{h} = (h_1,\ldots,h_s) \in \mathbb{F}_p[x]^s$ with $\deg(h_i) < m = \deg(f)$ for $1 \leqslant i \leqslant s$ there is a standard way to associate a positive weight $W_p(\mathbf{h})$ (see [13, pp. 37 and 77]). For the sake of completeness we present the definition of $W_p(\mathbf{h})$. For this purpose only, we identify $\mathbb{F}_p$ as a set with $C(p) := (-p/2, p/2] \cap \mathbb{Z}$, which is a complete residue system modulo p. For a given $\mathbf{h} = (h_1,\ldots,h_s) \in \mathbb{F}_p[x]^s$ with $\deg(h_i) < m$ for $1 \leqslant i \leqslant s$, we can thus write

$$h_i(x) = \sum_{j=1}^{m} h_{ij} x^{j-1} \quad \text{for } 1 \leqslant i \leqslant s,$$

where all $h_{ij} \in C(p)$. Then we put

$$W_p(\mathbf{h}) = \prod_{i=1}^{s} Q_p(h_{i1},\ldots,h_{im}),$$

where $Q_p(r_1,\ldots,r_m)$ is defined as follows for any $(r_1,\ldots,r_m) \in C(p)^m$. First of all, we let $d(r_1,\ldots,r_m) = 0$ if $(r_1,\ldots,r_m) = \mathbf{0}$, and for $(r_1,\ldots,r_m) \neq \mathbf{0}$ we let $d(r_1,\ldots,r_m)$ be the largest index d with $r_d \neq 0$. For $p = 2$ we put

$$Q_p(r_1,\ldots,r_m) = 2^{-d(r_1,\ldots,r_m)}.$$

For $p > 2$ we put $Q_p(r_1,\ldots,r_m) = 1$ if $(r_1,\ldots,r_m) = \mathbf{0}$, and for $(r_1,\ldots,r_m) \neq \mathbf{0}$ we put

$$Q_p(r_1,\ldots,r_m) = p^{-d}\left(\csc\frac{\pi}{p}|h_d| + \sigma(d,m)\right),$$

where $d = d(r_1,\ldots,r_m)$ and where $\sigma(d,m) = 1$ for $d < m$ and $\sigma(m,m) = 0$.

With these weights $W_p(\mathbf{h})$ we then define

$$R^{(s)}(\mathbf{g}, f) := \sum_{\mathbf{h}} W_p(\mathbf{h}), \tag{3}$$

where the sum is over all nonzero s-tuples $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{F}_p[x]^s$ with $\deg(h_i) < m$ for $1 \leqslant i \leqslant s$ and

$$\sum_{i=1}^{s} h_i g_i \equiv 0 \pmod{f}.$$

Note that for $s = 1$ and $\mathbf{g} = g_1$ with $\gcd(g_1, f) = 1$, the sum in (3) is empty, and so $R^{(1)}(\mathbf{g}, f) = 0$. Like $P(\mathbf{g}, f)$, the quantity $R^{(s)}(\mathbf{g}, f)$ depends only on $\mathbf{g}$ modulo f. The aim is to make $R^{(s)}(\mathbf{g}, f)$ as small as possible for fixed s and f.

Next, we introduce some concepts pertaining to polynomials over finite fields. Let Φ_p denote the analog of Euler's totient function for the polynomial ring $\mathbb{F}_p[x]$ (see [9, Section 3.4]). For nonzero $f \in \mathbb{F}_p[x]$, $\Phi_p(f)$ is the number of $g \in \mathbb{F}_p[x]$ with $\gcd(g, f) = 1$ and $\deg(g) < \deg(f)$. For $\deg(f) \geqslant 1$ we have the formula

$$\Phi_p(f) = p^{\deg(f)} \prod_{q|f} (1 - p^{-\deg(q)}), \tag{4}$$

where q runs through all monic irreducible factors of f in $\mathbb{F}_p[x]$.

Definition 1. A sequence $F = (f_k)_{k=1}^{\infty}$ of polynomials from $\mathbb{F}_p[x]$ is called a *divisibility chain* in $\mathbb{F}_p[x]$ if f_k divides f_{k+1} and $1 \leqslant \deg(f_k) < \deg(f_{k+1})$ for all $k \geqslant 1$.

For any given divisibility chain $F = (f_k)_{k=1}^{\infty}$ in $\mathbb{F}_p[x]$, it is clear from (4) that the sequence of positive numbers

$$\frac{\Phi_p(f_k)}{p^{\deg(f_k)}}, \quad k = 1, 2, \ldots,$$

is nonincreasing. Therefore it is meaningful to put

$$\alpha_F := \lim_{k \to \infty} \frac{\Phi_p(f_k)}{p^{\deg(f_k)}}. \tag{5}$$

With F we associate the set Y_F of *F-adic polynomials*. That is, Y_F is the set of all formal sums

$$A = \sum_{j=0}^{\infty} a_j f_j \tag{6}$$

with $f_0 = 1$, $a_j \in \mathbb{F}_p[x]$, and $\deg(a_j) < \deg(f_{j+1}) - \deg(f_j)$ for all $j \geqslant 0$. If $a_j = 0$ for all sufficiently large j, then A can be identified in a canonical way with a polynomial over $\mathbb{F}_p$. Thus, we have $\mathbb{F}_p[x] \subset Y_F$.

For $A \in Y_F$ as in (6) and $k = 1, 2, \ldots$, we put

$$A \pmod{f_k} := \sum_{j=0}^{k-1} a_j f_j \in \mathbb{F}_p[x].$$

Note that the degree of this polynomial is smaller than $\deg(f_k)$. For $\mathbf{B} = (B_1, \ldots, B_s) \in Y_F^s$, $s \geqslant 1$, and $k = 1, 2, \ldots$, we define $\mathbf{B}(\mathrm{mod} f_k)$ by carrying out the reduction modulo f_k componentwise, i.e.,

$$\mathbf{B}(\mathrm{mod} f_k) := (B_1(\mathrm{mod}\, f_k), \ldots, B_s(\mathrm{mod}\, f_k)) \in \mathbb{F}_p[x]^s.$$

We extend the definition in (3) by setting

$$R^{(s)}(\mathbf{B}, f_k) := R^{(s)}(\mathbf{B}(\mathrm{mod}\, f_k), f_k). \tag{7}$$

For $\mathbf{A} = (A_1, A_2, \ldots) \in Y_F^\infty$ and $s = 1, 2, \ldots$ we define the projection

$$\mathbf{A}^{(s)} := (A_1, \ldots, A_s) \in Y_F^s.$$

The quantity we will be interested in is $R^{(s)}(\mathbf{A}^{(s)}, f_k)$. This quantity is thus obtained by considering the first s components of $\mathbf{A} \in Y_F^\infty$, reducing each of these components modulo f_k, and then applying (3).

We conclude this preparatory section by introducing suitable probability measures. Let Y_F be the set of F-adic polynomials as above. It is clear that Y_F has a probability measure λ_F such that the set of $A \in Y_F$ with specified first k coefficients $a_0, a_1, \ldots, a_{k-1}$ in (6), or equivalently with $A(\mathrm{mod} f_k)$ specified, has measure $p^{-\deg(f_k)}$. Now let

$$U_F := \{A \in Y_F : \gcd(A(\mathrm{mod}\, f_k), f_k) = 1 \quad \text{for all } k \geqslant 1\} \tag{8}$$

and

$$U_F^{(k)} := \{A \in Y_F : \gcd(A(\mathrm{mod}\, f_k), f_k) = 1\} \quad \text{for } k = 1, 2, \ldots.$$

Since F is a divisibility chain, we have $U_F^{(1)} \supseteq U_F^{(2)} \supseteq \ldots$. Therefore

$$U_F = \bigcap_{k=1}^{\infty} U_F^{(k)}$$

satisfies

$$\lambda_F(U_F) = \lim_{k \to \infty} \lambda_F(U_F^{(k)}) = \alpha_F,$$

where α_F is defined in (5). Now we assume that $\alpha_F > 0$. Then we restrict λ_F to U_F and renormalize to get a probability measure μ_F on U_F. In other words,

$$\mu_F = \frac{1}{\alpha_F} \lambda_F^*, \tag{9}$$

where λ_F^* denotes the restriction of λ_F to U_F. Let μ_F^∞ be the complete product measure on U_F^∞ induced by μ_F.

3. A General Existence Theorem

For $s \geqslant 1$ and a polynomial $f \in \mathbb{F}_p[x]$ with $\deg(f) \geqslant 1$, let $G_s(f)$ be the set of all s-tuples $\mathbf{g} = (g_1, \ldots, g_s) \in \mathbb{F}_p[x]^s$ with $\gcd(g_i, f) = 1$ and $\deg(g_i) < \deg(f)$ for $1 \leqslant i \leqslant s$. Note that $\mathrm{card}(G_s(f)) = \Phi_p(f)^s$. The following result is implied by [13, Theorem 4.43].

Lemma 2. *For any dimension $s \geq 1$ and any $f \in \mathbb{F}_p[x]$ with $\deg(f) \geq 1$ we have*

$$\frac{1}{\Phi_p(f)^s} \sum_{\mathbf{g} \in G_s(f)} R^{(s)}(\mathbf{g}, f) \leq \frac{(c_p \deg(f))^s}{p^{\deg(f)}}$$

with a constant $c_p > 0$ depending only on p.

Based on this bound on the average value of $R^{(s)}(\mathbf{g}, f)$ over $G_s(f)$, we can now establish our main result for divisibility chains F with $\alpha_F > 0$ (see (5) for the definition of α_F).

Theorem 3. *Let $F = (f_k)_{k=1}^{\infty}$ be a divisibility chain in $\mathbb{F}_p[x]$ with $\alpha_F > 0$. Suppose that $\varepsilon > 0$ is given. Then there exists a μ_F^{∞}-measurable set $E \subset U_F^{\infty}$ such that for all $\mathbf{A} \in U_F^{\infty} \backslash E$ we have*

$$R^{(s)}(\mathbf{A}^{(s)}, f_k) \leq C(\alpha_F, p, s, \varepsilon) \frac{(\deg(f_k))^s k(\log(k+1))^{1+\varepsilon}}{p^{\deg(f_k)}}$$

for all $k \geq 1$ and $s \geq 1$, where the constant $C(\alpha_F, p, s, \varepsilon)$ depends only on $\alpha_F, p, s,$ and ε. Furthermore, we can make $\mu_F^{\infty}(E)$ arbitrarily close to zero by choosing $C(\alpha_F, p, s, \varepsilon)$ large enough.

Proof. First we fix $k \geq 1$ and $s \geq 1$. Note that $R^{(s)}(\mathbf{A}^{(s)}, f_k)$ depends only on the first s components of $\mathbf{A} \in U_F^{\infty}$ and on their residues modulo f_k. Therefore $R^{(s)}(\mathbf{A}^{(s)}, f_k)$ is μ_F^{∞}-integrable as a function of $\mathbf{A} \in U_F^{\infty}$, and we have

$$e_{k,s} := \int_{U_F^{\infty}} R^{(s)}(\mathbf{A}^{(s)}, f_k) d\mu_F^{\infty}(\mathbf{A}) = \int_{U_F^s} R^{(s)}(\mathbf{B}, f_k) d\mu_F^s(\mathbf{B}),$$

where μ_F^s is the product measure on U_F^s induced by μ_F. In view of (9) and with the obvious meaning of λ_F^s, we get

$$\begin{aligned} e_{k,s} &= \frac{1}{\alpha_F^s} \int_{U_F^s} R^{(s)}(\mathbf{B}, f_k)\ d\lambda_F^s(\mathbf{B}) \\ &\leq \frac{1}{\alpha_F^s} \sum_{\mathbf{g} \in G_s(f_k)} R^{(s)}(\mathbf{g}, f_k) p^{-s \deg(f_k)} \\ &\leq \frac{(c_p \deg(f_k))^s}{\alpha_F^s p^{\deg(f_k)}}, \end{aligned}$$

where we used Lemma 2 in the last step. For given $\varepsilon > 0$ we put

$$\beta_k := c(\varepsilon) k(\log(k+1))^{1+\varepsilon} \quad \text{for } k = 1, 2, \ldots,$$

where $c(\varepsilon)$ is chosen such that

$$c(\varepsilon) > \sum_{k=1}^{\infty} \frac{1}{k(\log(k+1))^{1+\varepsilon}}.$$

For any $k \geq 1$ and $s \geq 1$ we define

$$E_{k,s} := \left\{ \mathbf{A} \in U_F^{\infty} : R^{(s)}(\mathbf{A}^{(s)}, f_k) > \frac{\beta_k \beta_s (c_p \deg(f_k))^s}{\alpha_F^s p^{\deg(f_k)}} \right\}.$$

Then

$$\frac{(c_p \deg(f_k))^s}{\alpha_F^s p^{\deg(f_k)}} \geqslant e_{k,s} \geqslant \int_{E_{k,s}} R^{(s)}(\mathbf{A}^{(s)}, f_k)\, d\mu_F^\infty(\mathbf{A}) \geqslant \frac{\beta_k \beta_s (c_p \deg(f_k))^s}{\alpha_F^s p^{\deg(f_k)}} \mu_F^\infty(E_{k,s}),$$

and so

$$\mu_F^\infty(E_{k,s}) \leqslant \frac{1}{\beta_k \beta_s}.$$

With

$$E := \bigcup_{k=1}^\infty \bigcup_{s=1}^\infty E_{k,s}$$

we have

$$\mu_F^\infty(E) \leqslant \sum_{k=1}^\infty \sum_{s=1}^\infty \frac{1}{\beta_k \beta_s} = \left(\sum_{k=1}^\infty \frac{1}{\beta_k} \right)^2 < 1$$

by the choice of the β_k. Note that we can make $\mu_F^\infty(E)$ arbitrarily close to zero by choosing $c(\varepsilon)$ large enough. For any $\mathbf{A} \in U_F^\infty \backslash E$ we have

$$R^{(s)}(\mathbf{A}^{(s)}, f_k) \leqslant \frac{\beta_k \beta_s (c_p \deg(f_k))^s}{\alpha_F^s p^{\deg(f_k)}} = C(\alpha_F, p, s, \varepsilon) \frac{(\deg(f_k))^s k (\log(k+1))^{1+\varepsilon}}{p^{\deg(f_k)}}$$

for all $k \geqslant 1$ and $s \geqslant 1$, which is the desired bound. □

Remark 4. Consider the divisibility chain $F = (f^k)_{k=1}^\infty$ in $\mathbb{F}_p[x]$ consisting of the powers of a polynomial $f \in \mathbb{F}_p[x]$ with $\deg(f) \geqslant 1$. Then it is clear that $\alpha_F > 0$. In fact, from (4) and (5) we get

$$\alpha_F = \frac{\Phi_p(f)}{p^{\deg(f)}}.$$

Thus, Theorem 3 applies in this special case, as do the following results in this section.

With $\mathbf{A}^{(s)}$ and f_k there is associated the point set $P(\mathbf{g}_k^{(s)}, f_k)$, where $\mathbf{g}_k^{(s)} := \mathbf{A}^{(s)} (\mathrm{mod} f_k)$. This point set has $N_k := p^{\deg(f_k)}$ points. If we use $k \leqslant \deg(f_k)$ for all $k \geqslant 1$, then in terms of N_k the bound in Theorem 3 yields

$$R^{(s)}(\mathbf{A}^{(s)}, f_k) = O(N_k^{-1} (\log N_k)^{s+1} (\log\log(N_k+1))^{1+\varepsilon}) \tag{10}$$

for all $\mathbf{A} \in U_F^\infty \backslash E$ and all $k \geqslant 1$ and $s \geqslant 1$, where the implied constant depends only on α_F, p, s, and ε. If k and s are fixed, then the best known existence theorem

is the one implied by Lemma 2, namely that for some $\mathbf{g} \in G_s(f_k)$, with $\mathbf{g}$ depending on k and s, we have

$$R^{(s)}(\mathbf{g}, f_k) = O(N_k^{-1}(\log N_k)^s)$$

with an implied constant depending only on p and s. Thus, the price of having an $\mathbf{A} \in U_F^\infty \backslash E$ which works for all k and s simultaneously is an extra factor of the order of magnitude $(\log N_k)(\log\log(N_k+1))^{1+\varepsilon}$.

Corollary 5. *For $\mathbf{A} \in U_F^\infty \backslash E$ let $\mathbf{g}_k^{(s)} = \mathbf{A}^{(s)} (\mathrm{mod}\, f_k)$ as above. Then the star discrepancy $D_{N_k}^*$ of the point set $P(\mathbf{g}_k^{(s)}, f_k)$ satisfies*

$$D_{N_k}^* = O(N_k^{-1}(\log N_k)^{s+1}(\log\,\log\,(N_k+1))^{1+\varepsilon})$$

for all $k \geqslant 1$ and $s \geqslant 1$, where the implied constant depends only on $\alpha_F, p, s,$ and ε.

Proof. Since in our construction of the digital nets $P(\mathbf{g}, f)$ all bijections in [13, p. 63] are identity maps (compare with Section 2), we can apply the discrepancy bound in [12, Theorem 5] (see also [13, eq. (4.49)]). This yields

$$D_{N_k}^* \leqslant \frac{s}{N_k} + R^{(s)}(\mathbf{A}^{(s)}, f_k) \tag{11}$$

for the star discrepancy $D_{N_k}^*$ of $P(\mathbf{g}_k^{(s)}, f_k)$. The rest follows from (10). □

We noted in Section 2 that $P(\mathbf{g}, f)$ is a digital (t, m, s)-net in base p. For $P(\mathbf{g}_k^{(s)}, f_k)$ the following bound on the quality parameter t can be derived.

Corollary 6. *For $\mathbf{A} \in U_F^\infty \backslash E$ let $\mathbf{g}_k^{(s)} = \mathbf{A}^{(s)} (\mathrm{mod}\, f_k)$ as above. Then for all $k \geqslant 1$ and $s \geqslant 1$, the point set $P(\mathbf{g}_k^{(s)}, f_k)$ is a digital $(t_k^{(s)}, \deg(f_k), s)$-net in base p with*

$$t_k^{(s)} \leqslant s \log_p \deg(f_k) + \log_p[k(\log(k+1))^{1+\varepsilon}] + C'(\alpha_F, p, s, \varepsilon),$$

where $\log_p$ denotes the logarithm to the base p and $C'(\alpha_F, p, s, \varepsilon)$ depends only on $\alpha_F, p, s,$ and ε.

Proof. Let $D_{N_k}^*$ be as in Corollary 5. Then by [13, eq. (4.47) and Theorem 4.42] we obtain

$$D_{N_k}^* \geqslant \frac{p-1}{2p} p^{-\rho(\mathbf{g}_k^{(s)}, f_k)} = \frac{p-1}{2p} p^{t_k^{(s)}} N_k^{-1} \geqslant \frac{1}{4} p^{t_k^{(s)}} N_k^{-1}$$

for all $k \geqslant 1$ and $s \geqslant 1$. On the other hand, Theorem 3 and (11) yield

$$D_{N_k}^* \leqslant s N_k^{-1} + C(\alpha_F, p, s, \varepsilon)(\deg(f_k))^s k(\log(k+1))^{1+\varepsilon} N_k^{-1}$$

for all $k \geqslant 1$ and $s \geqslant 1$. We get the desired result by combining these inequalities. □

Remark 7. It may be an interesting research problem to find out whether there are always $\mathbf{A} \in U_F^\infty$ for which an improved bound on $t_k^{(s)}$ can be obtained. In the special case where $f_k(x) = x^k$ for all $k \geqslant 1$, a slight improvement on Corollary 6 follows from the existence theorem of Larcher [4]. In the general case, one will

probably need to argue directly, i.e., not via the star discrepancy. The methods developed by Larcher and Niederreiter [6] may be helpful here.

Hickernell *et al.* [2] showed that s-dimensional lattice rules that are extensible in the moduli yield infinite sequences in $[0,1]^s$ with desirable properties. In this way, the restriction that lattice rules work only with finite point sets can be overcome. The results of Hickernell and Niederreiter [3] demonstrate that, with a suitable choice of parameters, these infinite sequences have small star discrepancy and that the construction can also be extended in the dimensions s.

We now describe an analogous construction based on extensible polynomial lattice rules. Let $F = (f_k)_{k=1}^{\infty}$ be an arbitrary divisibility chain in $\mathbb{F}_p[x]$. Then any polynomial $n \in \mathbb{F}_p[x]$ can be written in the form

$$n = \sum_{j=0}^{k-1} n_j f_j \tag{12}$$

with $f_0 = 1$, $n_j \in \mathbb{F}_p[x]$, and $\deg(n_j) < \deg(f_{j+1}) - \deg(f_j)$ for $0 \leqslant j \leqslant k-1$. This representation is unique except for the addition of terms with zero coefficients. Thus, the following "radical-inverse function"

$$\phi_F(n) := \sum_{j=0}^{k-1} \frac{n_j}{f_{j+1}} \in \mathbb{F}_p(x) \tag{13}$$

is well defined. This generalizes a definition given by Tezuka [19]. Next, we introduce an "infinite" analog of (1) by defining $\tau_p : \mathbb{F}_p((x^{-1})) \to [0,1]$ via

$$\tau_p\left(\sum_{j=w}^{\infty} b_j x^{-j}\right) := \sum_{j=\max(1,w)}^{\infty} b_j p^{-j}, \tag{14}$$

where all $b_j \in \mathbb{F}_p = \{0,1,\ldots,p-1\}$. Finally, given $\mathbf{B} = (B_1,\ldots,B_s) \in Y_F^s$, $s \geqslant 1$, we get the infinite sequence $\sigma(\mathbf{B},F)$ consisting of the points

$$(\tau_p(\phi_F(n)B_1),\ldots,\tau_p(\phi_F(n)B_s)) \in [0,1]^s, \tag{15}$$

where n runs through all polynomials over $\mathbb{F}_p$ arranged according to nondecreasing degrees. Here, if n is as in (12) with the least $k \geqslant 1$, then $\phi_F(n)B_i$ with $1 \leqslant i \leqslant s$ is interpreted to be the rational function $\phi_F(n) \cdot (B_i(\mathrm{mod} f_k))$ over $\mathbb{F}_p$.

For a given $k \geqslant 1$ we now consider the first $N_k = p^{\deg(f_k)}$ terms of the sequence $\sigma(\mathbf{B},F)$. Then n in (15) runs through all polynomials over $\mathbb{F}_p$ of degree smaller than $\deg(f_k)$. Thus, n is of the form (12) with the n_j running through all polynomials over $\mathbb{F}_p$ with $\deg(n_j) < \deg(f_{j+1}) - \deg(f_j)$ for $0 \leqslant j \leqslant k-1$. It follows then from (13) that $\phi_F(n)$ runs through all rational functions of the form a/f_k with $a \in \mathbb{F}_p[x]$ and $\deg(a) < \deg(f_k)$. A comparison with (2) now shows that by considering the first N_k terms of the sequence $\sigma(\mathbf{B},F)$ and truncating these points in $[0,1]^s$ to the precision $p^{-\deg(f_k)}$, we get the point set $P(\mathbf{g}_k, f_k)$ with $\mathbf{g}_k = \mathbf{B}(\mathrm{mod}\, f_k)$. The truncation is required because of the difference in the definitions of the maps $\tau_p^{(m)}$ and τ_p in (1) and (14), respectively.

If $\alpha_F > 0$ and $\mathbf{A} \in U_F^{\infty} \backslash E$, then we can give the following discrepancy bound for the first N_k terms of the sequence $\sigma(\mathbf{A}^{(s)},F)$. This bound follows from

Corollary 5 and the fact noted above that the first N_k terms of $\sigma(\mathbf{A}^{(s)}, F)$ are at a distance $O(N_k^{-1})$ from the corresponding points of $P(\mathbf{g}_k^{(s)}, f_k)$. Therefore, the star discrepancies of $P(\mathbf{g}_k^{(s)}, f_k)$ and of the first N_k terms of $\sigma(\mathbf{A}^{(s)}, F)$ differ by $O(N_k^{-1})$.

Corollary 8. *Let $F = (f_k)_{k=1}^{\infty}$ be a divisibility chain in $\mathbb{F}_p[x]$ with $\alpha_F > 0$ and let $\varepsilon > 0$. Then for $\mathbf{A} \in U_F^{\infty} \backslash E$ the star discrepancy $D_{N_k}^*$ of the first $N_k = p^{\deg(f_k)}$ terms of the sequence $\sigma(\mathbf{A}^{(s)}, F)$ satisfies*

$$D_{N_k}^* = O(N_k^{-1}(\log N_k)^{s+1}(\log\log(N_k+1))^{1+\varepsilon})$$

for all $k \geqslant 1$ and $s \geqslant 1$, where the implied constant depends only on α_F, p, s, and ε.

We emphasize that the sequence $\sigma(\mathbf{A}^{(s)}, F)$ in Corollary 8 can be extended in all dimensions $s \geqslant 1$, in the sense that $\mathbf{A}^{(s)} \in U_F^s$ is obtained from a fixed suitable $\mathbf{A}$ in the infinite product U_F^{∞} by projecting to the first s components.

4. A One-Parameter Family of Polynomial Lattice Rules

We consider a one-parameter family of polynomial lattice rules which was introduced in [12, Remark 4]. Let f be an irreducible polynomial over $\mathbb{F}_p$. Then the digital nets $P(\mathbf{g}, f)$ considered here have $\mathbf{g}$ of the special form

$$\mathbf{g} = (1, g, g^2, \ldots, g^{s-1}) \in \mathbb{F}_p[x]^s$$

for some $g \in \mathbb{F}_p[x]$. We get in this way polynomial analogs of Korobov lattice rules (compare with [7, Section 3]).

We show an analog of Theorem 3 for this family, but here we can extend only in the dimensions $s \geqslant 1$. Put

$$T(f) := \{g \in \mathbb{F}_p[x] : \deg(g) < \deg(f)\},$$

and for $h \in T(f)$ set

$$\mathbf{h}^{(s)} := (1, h, h^2, \ldots, h^{s-1}) \in \mathbb{F}_p[x]^s.$$

Theorem 9. *Let f be an irreducible polynomial over $\mathbb{F}_p$. Then there exists a polynomial $h \in T(f)$ such that*

$$R^{(s)}(\mathbf{h}^{(s)}, f) \leqslant C_p(s)\frac{(\deg(f))^s}{p^{\deg(f)}} \quad \text{for all } s \geqslant 1$$

with a constant $C_p(s)$ depending only on p and s. In fact, for arbitrarily small $\varepsilon > 0$ we can get at least $(1-\varepsilon)p^{\deg(f)}$ such polynomials h by choosing $C_p(s)$ large enough.

Proof. Put

$$K_s(f) := \{\mathbf{g} = (1, g, g^2, \ldots, g^{s-1}) \in \mathbb{F}_p[x]^s : g \in T(f)\}.$$

Then it was shown in [12, Remark 4] that for all $s \geqslant 1$ we have

$$L_s(f) := \frac{1}{p^{\deg(f)}} \sum_{\mathbf{g} \in K_s(f)} R^{(s)}(\mathbf{g}, f) \leqslant \frac{s-1}{p^{\deg(f)}}(C_p \deg(f)\log p)^s$$

with a constant $C_p > 0$. Let

$$\beta_s := cs(\log(s+1))^2 \quad \text{for } s = 1, 2, \ldots,$$

where the constant c is chosen such that

$$c > \sum_{s=1}^{\infty} \frac{1}{s(\log(s+1))^2}.$$

For any $s \geqslant 1$ we define

$$E_s := \left\{ h \in T(f) : R^{(s)}(\mathbf{h}^{(s)}, f) > \frac{\beta_s(s-1)}{p^{\deg(f)}} (C_p \deg(f) \log p)^s \right\}.$$

Then

$$\begin{aligned}(s-1)(C_p \deg(f)\log p)^s &\geqslant p^{\deg(f)} L_s(f) \geqslant \sum_{h \in E_s} R^{(s)}(\mathbf{h}^{(s)}, f) \\ &\geqslant \operatorname{card}(E_s) \frac{\beta_s(s-1)}{p^{\deg(f)}} (C_p \deg(f)\log p)^s,\end{aligned}$$

and so

$$\operatorname{card}(E_s) \leqslant \frac{p^{\deg(f)}}{\beta_s}.$$

With

$$E := \bigcup_{s=1}^{\infty} E_s$$

we have

$$\operatorname{card}(E) \leqslant p^{\deg(f)} \sum_{s=1}^{\infty} \frac{1}{\beta_s} < p^{\deg(f)} = \operatorname{card}(T(f))$$

by the choice of the β_s. Thus, there exists an $h \in T(f) \backslash E$, and for this h we have

$$R^{(s)}(\mathbf{h}^{(s)}, f) \leqslant \frac{cs(s-1)(\log(s+1))^2}{p^{\deg(f)}} (C_p \deg(f) \log p)^s$$

for all $s \geqslant 1$. By choosing c sufficiently large, we can satisfy the second part of the theorem. □

Remark 10. Some of the consequences of Theorem 3 can also be drawn here. For instance, if $h \in T(f)$ is as in Theorem 9, then with $N = p^{\deg(f)}$ the star discrepancy D_N^* of the point set $P(\mathbf{h}^{(s)}, f)$ satisfies

$$D_N^* = O(N^{-1}(\log N)^s) \quad \text{for all } s \geqslant 1,$$

with an implied constant depending only on p and s. Note that for sufficiently large p the constant C_p in the proof of Theorem 9 satisfies $C_p < 1$, and so for such p the

coefficient of the main term $N^{-1}(\log N)^s$ in the above bound for D_N^* can be made absolute. In fact, we have

$$D_N^* \leqslant \frac{d_s(\log N)^s}{N} + \frac{s}{N} \quad \text{for all } s \geqslant 1,$$

provided that p is so large that $C_p < 1$. The coefficient d_s satisfies $d_s \to 0$ as $s \to \infty$. But obviously this bound is nontrivial only if $s < N$.

Remark 11. A similar result holds for Korobov lattice rules with a prime modulus p. Instead of the averaging result in [12, Remark 4] which was used in the proof of Theorem 9, we now employ [13, Theorem 5.18] which says that for all $s \geqslant 1$ we have

$$\frac{1}{p}\sum_{g=0}^{p-1} R^{(s)}((1, g, g^2, \ldots, g^{s-1}), p) \leqslant \frac{s-1}{p}(2\log p + 1)^s,$$

where $R^{(s)}(\ldots)$ is defined by [13, Definition 5.4] for $s \geqslant 2$ and $R^{(1)}(\ldots) = 0$. Thus, the same method as in the proof of Theorem 9 yields the existence of a $g \in \{0, 1, \ldots, p-1\}$ such that

$$R^{(s)}((1, g, g^2, \ldots, g^{s-1}), p) \leqslant B(s)p^{-1}(\log p)^s \quad \text{for all } s \geqslant 1,$$

with a constant $B(s)$ depending only on s. We cannot consider higher powers of p since in this case the required averaging results are not available for arbitrary s.

References

[1] Hansen T, Mullen GL, Niederreiter H (1993) Good parameters for a class of node sets in quasi-Monte Carlo integration. Math Comp **61**: 225–234

[2] Hickernell FJ, Hong HS, L'Ecuyer P, Lemieux C (2000) Extensible lattice sequences for quasi-Monte Carlo quadrature. SIAM J Sci Comput **22**: 1117–1138

[3] Hickernell FJ, Niederreiter H (2002) The existence of good extensible rank-1 lattices. J Complexity (to appear)

[4] Larcher G (1993) Nets obtained from rational functions over finite fields. Acta Arith **63**: 1–13

[5] Larcher G, Lauß A, Niederreiter H, Schmid WCh (1996) Optimal polynomials for (t, m, s)-nets and numerical integration of multivariate Walsh series. SIAM J Numer Analysis **33**: 2239–2253

[6] Larcher G, Niederreiter H (1995) Generalized (t, s)-sequences, Kronecker-type sequences, and diophantine approximations of formal Laurent series. Trans Amer Math Soc **347**: 2051–2073

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

[8] Lemieux C, L'Ecuyer P (2001) Randomized polynomial lattice rules for multivariate integration and simulation. SIAM J Sci Comput (to appear)

[9] Lidl R, Niederreiter H (1994) Introduction to Finite Fields and Their Applications, rev edn. Cambridge: Univ Press

[10] Niederreiter H (1978) Existence of good lattice points in the sense of Hlawka. Monatsh Math **86**: 203–219

[11] Niederreiter H (1986) Low-discrepancy point sets. Monatsh Math **102**: 155–167

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

[13] Niederreiter H (1992) Random Number Generation and Quasi-Monte Carlo Methods. Philadelphia: SIAM

[14] Niederreiter H (1993) Finite fields, pseudorandom numbers, and quasirandom points. In: Mullen GL, Shiue PJ-S (eds) Finite Fields, Coding Theory, and Advances in Communications and Computing, pp 375–394. New York: Dekker

[15] Niederreiter H (1993) Improved error bounds for lattice rules. J Complexity **9**: 60–75
[16] Pirsic G, Schmid WCh (2001) Calculation of the quality parameter of digital nets and application to their construction. J Complexity **17**: 827–839
[17] Schmid WC (2000) Improvements and extensions of the ''Salzburg tables'' by using irreducible polynomials. In: Niederreiter H, Spanier J (eds) Monte Carlo and Quasi-Monte Carlo Methods 1998, pp 436–447. Berlin: Springer
[18] Sloan IH, Joe S (1994) Lattice Methods for Multiple Integration. Oxford: Oxford University Press
[19] Tezuka S (1993) Polynomial arithmetic analogue of Halton sequences. ACM Trans Modeling and Computer Simulation **3**: 99–107

Author's address: Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore, e-mail: nied@math.nus.edu.sg