Finite Fields and Their Applications 17 (2011) 407–423

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Extensible hyperplane nets ☆

Gottlieb Pirsic, Friedrich Pillichshammer *

Institut für Finanzmathematik, Universität Linz, Altenbergstraße 69, A-4040 Linz, Austria

ARTICLE INFO

Article history:
Received 21 December 2010
Revised 1 February 2011
Accepted 3 February 2011
Available online 10 February 2011
Communicated by Arne Winterhof

MSC:
11K38
11K45
65C05
65D30

Keywords:
Digital nets
Hyperplane nets
Quasi-Monte Carlo
Worst-case error
Discrepancy

ABSTRACT

Extensible (polynomial) lattice point sets have the property that the number N of points in the node set of a quasi-Monte Carlo algorithm may be increased while retaining the existing points. Explicit constructions for extensible (polynomial) lattice point sets have been presented recently by Niederreiter and Pillichshammer. It is the aim of this paper to establish extensibility for a powerful generalization of polynomial lattice point sets, the so-called hyperplane nets.

1. Introduction

In the field of quasi-Monte Carlo methods, digital nets have been established as a group of point sets with particularly favorable properties such as a low-discrepancy bound of the best possible asymptotic order. Furthermore, methods of algebraic geometry proved fruitful in achieving even optimality in the constant (with respect to the asymptotic order in the dimension) amongst all currently known constructions. However, for practice it may be more favorable to look for simpler constructions which are easier to implement (efficiently) while still performing well under the discrepancy criterion

☆ The authors are supported by the Austrian Science Foundation (FWF), Project S9609, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

* Corresponding author.
E-mail addresses: gottlieb.pirsic@jku.at (G. Pirsic), friedrich.pillichshammer@jku.at (F. Pillichshammer).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.02.004

or the worst-case integration error criterion. Lattice point sets (see [14,27]) and polynomial lattice point sets (see [6,13,14]) are well-known examples of this. Although they can and have been introduced independently of net theory, they are also special cases of digital (t, m, s)-nets. A convenient feature of (polynomial) lattice point sets is their ability to extend the cardinality of a given point set in a very natural way, which is called 'extensibility' (see [3,6–10,15,20]). It is the aim of this paper to establish extensibility for a powerful generalization of polynomial lattice rules, the hyperplane nets. In doing so we will also provide a generalization of extensible polynomial lattice rules in that we allow for steps using variable and reducible polynomials instead of having only one fixed, irreducible polynomial.

The paper is organized as follows: in the next section we present the definition of hyperplane nets and we introduce the quality criterion – the worst-case integration error in a certain function space of Walsh-series – with respect to which we want to optimize the hyperplane nets. In Section 3 we state the construction algorithm for hyperplane nets and show that the constructed hyperplane nets are in fact extensible and 'good' with respect to our quality criterion. In Section 4 we state some pure existence results for extensible hyperplane nets of 'good' quality with respect to the worst-case error criterion or the (weighted) star discrepancy. In Section 5 we provide some numerical results and a discussion thereof.

2. Definitions

2.1. Hyperplane nets

Good constructions of finite point sets for quasi-Monte Carlo algorithms are based on the concept of (t, m, s)-nets in base q which were developed by Niederreiter [12] (for basic reference see also [6,14,17]).

Definition 1 *((t, m, s)-nets in base q).* Let $q \geqslant 2, m, s \geqslant 1$ be integers. A multiset of q^m points in the s-dimensional unit cube $[0, 1)^s$ is called a *(t, m, s)-net in base q* if every interval of the form

$$\prod_{i=1}^{s}\left[\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}}\right) \subseteq [0,1)^s, \quad a_i, d_i \in \mathbb{N}_0, \ \sum_{i=1}^{s} d_i = m - t,$$

contains b^t points (i.e., it contains the exact proportion of points according to its volume).

A (t, m, s)-net is well distributed if the quality parameter t is 'small'. Explicit constructions of (t, m, s)-nets are based on the *digital construction scheme* (see again [6,12,14,17]) which we recall in the following.

Throughout the paper let q be a prime-power and let $\mathbb{F}_q$ be the finite field of q elements. For a positive integer r let $\mathbb{Z}_r = \{0, \ldots, r-1\}$. Let $\varphi_1 : \mathbb{Z}_q \to \mathbb{F}_q$ be a fixed bijection with $\varphi_1(0) = 0$. The map φ_1 is extended to a map $\varphi : \mathbb{Z}_{q^m} \to \mathbb{F}_q^m$ by setting

$$\varphi(k) := \big(\varphi_1(\kappa_0), \ldots, \varphi_1(\kappa_{m-1})\big)^\top \tag{1}$$

for $k = \kappa_0 + \kappa_1 q + \cdots + \kappa_{m-1} q^{m-1}$ with $\kappa_0, \ldots, \kappa_{m-1} \in \mathbb{Z}_q$. Here $\boldsymbol{x}^\top$ means the transpose of the vector $\boldsymbol{x}$. (Later, the symbol $^\top$ is used not only for row vectors but also for any matrix. Hence in general, $A^\top$ means the transpose of a matrix A.)

Definition 2 *(Digital (t, m, s)-nets).* Let $s \geqslant 1$ and $m \geqslant 1$ be integers. Let $C_1, \ldots, C_s$ be $m \times m$ matrices over $\mathbb{F}_q$. Now we construct q^m points in $[0, 1)^s$: For $1 \leqslant i \leqslant s$ and for $k \in \mathbb{Z}_{q^m}$ multiply the matrix C_i by the vector $\varphi(k)$, i.e.,

$$C_i \varphi(k) =: \big(y_{i,1}(k), \ldots, y_{i,m}(k)\big)^\top \in \mathbb{F}_q^m,$$

and set

$$x_{k,i} := \frac{\varphi_1^{-1}(y_{i,1}(k))}{q} + \cdots + \frac{\varphi_1^{-1}(y_{i,m}(k))}{q^m}.$$

If for some integer t with $0 \leqslant t \leqslant m$ the point set consisting of the points

$$\boldsymbol{x}_k = (x_{k,1}, \ldots, x_{k,s})^\top \quad \text{for } k \in \mathbb{Z}_{q^m},$$

is a (t, m, s)-net in base q, then it is called a digital (t, m, s)-net over $\mathbb{F}_q$, or, in brief, a digital net (over $\mathbb{F}_q$). The C_i are called its *generator matrices*.

Many constructions of digital nets are inspired by a close connection between coding theory and the theory of digital nets (see, for example, Niederreiter [16,18]). Examples are the so-called $(u, u+v)$-construction (see [2,21]), the matrix-product construction (see [19]) and the Kronecker-product construction (see [2,22]). Here we deal with a construction for digital nets which is an analog to a special type of codes, namely to cyclic codes which are well known in coding theory. This construction has been introduced by Niederreiter in [16] who used the fact that cyclic codes can be defined by prescribing roots of polynomials. Later this construction has been generalized by Pirsic, Dick and Pillichshammer [26] to so-called hyperplane nets, whose definition will be given now.

Definition 3 *(Hyperplane nets).* Let integers $m \geqslant 1, s \geqslant 2$ and a prime-power q be given. Let $\mathbb{F}_{q^m}$ be a finite field with q^m elements and fix an element $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)^\top \in \mathbb{F}_{q^m}^s \setminus \{\mathbf{0}\}$. Let $\mathcal{F}$ be the space of linear forms

$$\mathcal{F} := \left\{ f(x_1, \ldots, x_s) = x_1\gamma_1 + \cdots + x_s\gamma_s \colon \gamma_1, \ldots, \gamma_s \in \mathbb{F}_{q^m} \right\} \subseteq \mathbb{F}_{q^m}[x_1, \ldots, x_s]$$

and consider the subset

$$\mathcal{F}_{\boldsymbol{\alpha}} := \left\{ f \in \mathcal{F} \colon f(\alpha_1, \ldots, \alpha_s) = 0 \right\}.$$

For each $1 \leqslant i \leqslant s$ choose an ordered basis $\mathcal{B}_i$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and define the mapping $\theta : \mathcal{F} \to \mathbb{F}_q^{ms}$ by

$$f(x) = \sum_{i=1}^{s} \gamma_i x_i \in \mathcal{F} \mapsto (\gamma_{1,1}, \ldots, \gamma_{1,m}, \ldots, \gamma_{s,1}, \ldots, \gamma_{s,m})^\top \in \mathbb{F}_q^{ms},$$

where $(\gamma_{i,1}, \ldots, \gamma_{i,m})^\top$ is the coordinate vector of γ_i with respect to the chosen basis $\mathcal{B}_i$.

We denote by $\mathcal{C}_{\boldsymbol{\alpha}}$ the orthogonal subspace in $\mathbb{F}_q^{ms}$ of the image $\mathcal{N}_{\boldsymbol{\alpha}} := \theta(\mathcal{F}_{\boldsymbol{\alpha}})$. Let

$$C_{\boldsymbol{\alpha}} = \left(C_1^\top \cdots C_s^\top\right) \in \mathbb{F}_q^{m \times sm}$$

be a matrix whose row space is $\mathcal{C}_{\boldsymbol{\alpha}}$. Then we call the digital net with the generating matrices $C_1, \ldots, C_s$ a *hyperplane net over* $\mathbb{F}_q$ *with respect to* $\mathcal{B}_1, \ldots, \mathcal{B}_s$ and $C_{\boldsymbol{\alpha}}$ is its overall generating matrix. This hyperplane net will be denoted by $\mathcal{P}_{\boldsymbol{\alpha}}$ and we say $\mathcal{P}_{\boldsymbol{\alpha}}$ is the hyperplane net associated with $\boldsymbol{\alpha}$.

Remark 1. In Definition 3 above, if $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ is of the special form $\boldsymbol{\alpha} = (1, \alpha, \alpha^2, \ldots, \alpha^{s-1})^\top$ with some $\alpha \in \mathbb{F}_{q^m}$, then we obtain a *cyclic digital net* as introduced initially by Niederreiter [16].

Remark 2. Another construction of digital nets goes by the name of *polynomial lattices* which have been introduced by Niederreiter [13] (see also [6,14]). It has been shown by Pirsic [25] that polynomial lattices appear as special cases of hyperplane nets when we choose the ordered bases $\mathcal{B}_1, \ldots, \mathcal{B}_s$ all equal to $\{1, \omega, \ldots, \omega^{m-1}\}$ if $\mathbb{F}_{q^m} = \mathbb{F}_q[\omega]$.

Further examples in [25] show that the introduction of different bases significantly enhances the range of generator matrices that are constructable by this method in comparison to polynomial lattices. Sometimes it is therefore even suggested to use primarily basis sets from certain subclasses, e.g., constant bases $\mathcal{B}_i = \mathcal{B}_1$ or bases with a triangular structure.

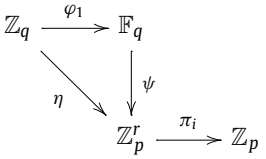
We shall from now on assume a fixed choice of bases $\mathcal{B}_1, \ldots, \mathcal{B}_s$ and will therefore not explicitly mention them anymore.

For more information on cyclic nets and hyperplane nets we refer to [6, Chapter 11].

2.2. The quality criterion

Our aim is to construct a sequence of $\boldsymbol{\alpha}_n \in \mathbb{F}_{q^{m_n}}^s$ such that $\mathcal{P}_{\boldsymbol{\alpha}_n} \subseteq \mathcal{P}_{\boldsymbol{\alpha}_{n+1}}$ and such that all $\mathcal{P}_{\boldsymbol{\alpha}_n}$ are of 'good quality'. Following [20] we use the worst-case error for quasi-Monte Carlo integration in a weighted Hilbert space of functions as quality criterion. This Hilbert space of functions is based on Walsh functions.

Definition 4 *(Walsh functions).* Let $q = p^r$, p prime, $r \in \mathbb{N}_0$ and let $\mathbb{F}_q$ and $\mathbb{Z}_q$ with ring operations modulo q and φ_1 be defined as in the first lines of Section 2.1. Moreover denote by ψ the isomorphism of additive groups $\psi : \mathbb{F}_q \to \mathbb{Z}_p^r$ and define $\eta := \psi \circ \varphi_1$. For $1 \leqslant i \leqslant r$ denote by π_i the projection $\pi_i : \mathbb{Z}_p^r \to \mathbb{Z}_p$, $\pi_i(x_1, \ldots, x_r) = x_i$.



Let now $k \in \mathbb{N}_0$ with base q representation $k = \kappa_1 + \kappa_2 q + \cdots + \kappa_m q^{m-1}$ where $\kappa_l \in \mathbb{Z}_q$ and let $x \in [0, 1)$ with base q representation $x = x_1 q^{-1} + x_2 q^{-2} + \cdots$. Then the kth Walsh function over the finite field $\mathbb{F}_q$ with respect to the bijection φ_1 is defined by

$$\mathrm{wal}_{k,\mathbb{F}_q,\varphi_1}(x) := \prod_{l=1}^{m} \prod_{i=1}^{r} \exp\left(2\pi \,\mathrm{i}\, \frac{(\pi_i \circ \eta)(\kappa_l)(\pi_i \circ \eta)(x_l)}{p}\right).$$

For convenience we will in the rest of the paper omit the subscript and simply write wal_k.

Multivariate Walsh functions are defined by multiplication of the univariate components, i.e., for $\boldsymbol{x} = (x^{(1)}, \ldots, x^{(s)}) \in [0, 1)^s$, $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$, $s > 1$, we set

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

It is well known that for any integer $s \geqslant 1$ the system $\{\mathrm{wal}_{\boldsymbol{k}} : \boldsymbol{k} \in \mathbb{N}_0^s\}$ is a complete orthonormal system in $L_2([0, 1]^s)$. For a proof and further details see [6, Appendix A].

In the following we define the weighted Hilbert function space $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$ in base q which is based on Walsh functions. For prime bases q this Hilbert function space has been introduced in [5, Section 2.2]. First we consider the one-dimensional case. The s-dimensional space will then be defined as the tensor product of those one-dimensional spaces.

For $k \in \mathbb{N}_0$ for $\gamma > 0$ and for $\beta > 1$ we define

$$r_{k,\gamma} = \begin{cases} 1 & \text{if } k = 0, \\ \gamma q^{-\beta \lfloor \log_q k \rfloor} & \text{if } k \in \mathbb{N}. \end{cases}$$

Note that $r_{k,\gamma}$ also depends on q and β. But as we consider these parameters as fixed we do not mention them explicitly.

We define the inner product of two functions F and G as

$$\langle F, G\rangle_{\mathrm{wal},\gamma} := \sum_{k=0}^{\infty} r_{k,\gamma}^{-1} \widehat{F}_{\mathrm{wal}}(k)\, \overline{\widehat{G}_{\mathrm{wal}}(k)},$$

where $\widehat{F}_{\mathrm{wal}}(k) = \int_0^1 F(x)\, \overline{\mathrm{wal}_k(x)}\, \mathrm{d}x$. The norm is given by $\|F\|_{\mathrm{wal},\gamma} := \langle F, F\rangle_{\mathrm{wal},\gamma}^{1/2}$. Then the weighted Hilbert space $\mathscr{H}_{\mathrm{wal},\beta,\gamma}$ consists of all functions with finite norm, that is,

$$\mathscr{H}_{\mathrm{wal},\beta,\gamma} := \big\{F \in L_2\big([0,1]\big) \colon \|F\|_{\mathrm{wal},\gamma} < \infty\big\}.$$

As in [5, Section 2.2] for the prime base case it can be shown that the function $K_{\mathrm{wal},\gamma}$ defined by

$$K_{\mathrm{wal},\gamma}(x, y) := \sum_{k=0}^{\infty} r_{k,\gamma}\, \mathrm{wal}_k(x)\, \overline{\mathrm{wal}_k(y)}$$

is the reproducing kernel of $\mathscr{H}_{\mathrm{wal},\beta,\gamma}$. (We refer to [1] for more information on reproducing kernel Hilbert spaces.)

We now turn to the s-dimensional case. For a sequence of non-increasing weights $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$, $\gamma_j > 0$, we define the s-dimensional weighted Hilbert space $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$ as a tensor product space, that is,

$$\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}} = \mathscr{H}_{\mathrm{wal},\beta,\gamma_1} \otimes \cdots \otimes \mathscr{H}_{\mathrm{wal},\beta,\gamma_s}.$$

Let $\boldsymbol{k} \in \mathbb{N}_0^s$, $\boldsymbol{x}, \boldsymbol{y} \in [0,1]^s$, with components denoted by k_j, x_j, y_j, respectively. The space $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$ is again a reproducing kernel Hilbert space with reproducing kernel given by

$$\begin{aligned} K_{\mathrm{wal},s,\boldsymbol{\gamma}}(\boldsymbol{x}, \boldsymbol{y}) &= \prod_{j=1}^{s} K_{\mathrm{wal},\gamma_j}(x_j, y_j) \\ &= \prod_{j=1}^{s} \sum_{k_j=0}^{\infty} r_{k_j,\gamma_j}\, \mathrm{wal}_{k_j}(x_j)\, \overline{\mathrm{wal}_{k_j}(y_j)} \\ &= \sum_{\boldsymbol{k} \in \mathbb{N}_0^s} r_{\boldsymbol{k},\boldsymbol{\gamma}}\, \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x})\, \overline{\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{y})}, \end{aligned}$$

where $r_{\boldsymbol{k},\boldsymbol{\gamma}} = \prod_{j=1}^{s} r_{k_j,\gamma_j}$ and the inner product is given by

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

and $\widehat{F}_{\mathrm{wal}}(\boldsymbol{k}) := \int_{[0,1]^s} F(\boldsymbol{x})\, \overline{\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x})}\, \mathrm{d}\boldsymbol{x}$.

We are interested in approximating the integrals of functions F from $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$,

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

Multivariate integration in the space $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$ in the special case that q is a prime has been considered in many papers as, for example, [4–6,11].

Here we approximate the integral $I_s(F)$ by so-called quasi-Monte Carlo (QMC) algorithms. A QMC algorithm is an equal weight quadrature rule of the form

$$Q_{N,s}(F) = \frac{1}{N}\sum_{n=0}^{N-1} F(\boldsymbol{x}_n) \tag{2}$$

with deterministic sample points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1} \in [0,1)^s$.

We define the worst-case error for integration in the space $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$ by

$$e_{N,s} := \sup_{F\in\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}},\, \|F\|_{\mathrm{wal},s,\boldsymbol{\gamma}}\leqslant 1} \bigl|I_s(F) - Q_{N,s}(F)\bigr|.$$

If $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{q^m-1}\}$, where $\boldsymbol{x}_n = (x_{n,1}, \ldots, x_{n,s})$, is a digital net over $\mathbb{F}_q$ generated by the matrices $C_1, \ldots, C_s \in \mathbb{F}_q^{m\times m}$, then it can be shown as for the prime base case in [5, Theorem 2] that

$$e_{q^m,s}^2 = \sum_{\boldsymbol{k}\in\mathcal{D}} r_{\boldsymbol{k},\boldsymbol{\gamma}} = -1 + \frac{1}{q^m}\sum_{n=0}^{q^m-1}\prod_{i=1}^{s}\bigl(1+\gamma_i \rho_{\mathrm{wal},\beta}(x_{n,i})\bigr), \tag{3}$$

where $\mathcal{D}$ is the so-called dual net defined as

$$\mathcal{D} := \bigl\{\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s \setminus \{\boldsymbol{0}\}\colon\ C_1^\top \mathbf{k}_1 + \cdots + C_s^\top \mathbf{k}_s = \boldsymbol{0}\bigr\}.$$

Here for $k \in \mathbb{N}_0$ with q-adic expansion $k = \kappa_0 + \kappa_1 q + \cdots$ we write $\mathbf{k} := (\varphi_1(\kappa_0), \varphi_1(\kappa_1), \ldots, \varphi_1(\kappa_{m-1}))^\top$. Furthermore, $\rho_{\mathrm{wal},\beta}(0) := \mu_q(\beta)$ and for $x = \xi_{i_0} q^{-i_0} + \xi_{i_0+1} q^{-i_0-1} + \cdots$, $i_0 \in \mathbb{N}$, with $\xi_i \in \{0, \ldots, q-1\}$ for $i \geqslant i_0$ and $\xi_{i_0} \neq 0$ we have

$$\rho_{\mathrm{wal},\beta}(x) = \mu_q(\beta) - q^{(i_0-1)(1-\beta)}\bigl(\mu_q(\beta)+1\bigr),$$

where $\mu_q(\beta) := \frac{q^\beta(q-1)}{q^\beta - q}$. In particular, the worst-case error $e_{q^m,s}^2$ can be computed with a cost of $O(sq^m)$ operations. We exploit this fact for a computer search algorithm of extensible hyperplane nets (see Algorithm 1).

Let $\boldsymbol{\alpha} \in (\mathbb{F}_q[x]/(f(x)))^s$ where $\deg f = m$. Further let the matrices B_i $(i = 1, \ldots, s)$ be the transformation matrices from the bases $\mathcal{B}_i$ to the basis $\{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$, where ω is the residue class of x in $\mathbb{F}_q[x]/(f(x))$. I.e., if $\mathcal{B}_i = \{\mathfrak{b}_{i,1}, \ldots, \mathfrak{b}_{i,s}\}$ and $\mathfrak{b}_{i,j} = \sum_{k=1}^m b_{i,j,k}\omega^{k-1}$, then $B_i = (b_{i,j,k})_{j,k=1,\ldots,m}^\top$.

A combination of (3) with [24, Lemma 1] shows that the squared worst-case error of integration in $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$ using a hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$ (with bases $\mathcal{B}_i$) is given by

$$e^2_{q^m,s}(\boldsymbol{\alpha}) = \sum_{\boldsymbol{k}\in\mathcal{N}'_{\boldsymbol{\alpha}}} r_{\boldsymbol{k},\boldsymbol{\gamma}},$$

where

$$\mathcal{N}'_{\boldsymbol{\alpha}} = \left\{\boldsymbol{k}\in\mathbb{N}_0^s\setminus\{\boldsymbol{0}\}\colon \boldsymbol{\alpha}\cdot\varphi'\big(\tau(\boldsymbol{k})\big) = \sum_{i=1}^{s}\alpha^{(i)}\varphi'\big(\tau_i(k_i)\big)\equiv 0 \pmod f\right\},$$

with $\tau(\boldsymbol{k}) = (\tau_1(k_1),\ldots,\tau_s(k_s))$ and permutations $\tau_i(k) := \varphi^{-1}(B_i\varphi(k))$. The bijection φ' will in this context be considered as going from $\mathbb{N}_0$ to $\mathbb{F}_q[x]$ by mapping q-adic digits to polynomial coefficients:

$$\varphi'\left(\sum_{i=0}^{\infty}\kappa_i q^i\right) := \sum_{i=0}^{\infty}\varphi_1(\kappa_i)x^i,$$

where the bijection $\varphi_1:\mathbb{Z}_q\to\mathbb{F}_q$ is arbitrary, just $\varphi_1(0)=0$ is required. Note that in the definition of $\mathcal{N}'_{\boldsymbol{\alpha}}$ the application of mod f implicitly effects a truncation of the k_i in the argument to the $\deg f$ least significant q-adic digits.

Choosing the bases such that all their transformation matrices are upper triangular allows us to disregard the permutations τ_i: we get

$$e^2_{q^m,s}(\boldsymbol{\alpha}) = \sum_{\boldsymbol{k}\in\mathcal{N}'_{\boldsymbol{\alpha}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} = \sum_{\boldsymbol{k}\in\mathcal{N}_{\boldsymbol{\alpha}}} r_{\tau^{-1}(\boldsymbol{k}),\boldsymbol{\gamma}},$$

where

$$\mathcal{N}_{\boldsymbol{\alpha}} = \big\{\boldsymbol{k}\in\mathbb{N}_0^s\setminus\{\boldsymbol{0}\}\colon \boldsymbol{\alpha}\cdot\varphi'(\boldsymbol{k})\equiv 0 \pmod f\big\},$$

with $\varphi'(\boldsymbol{k}) = (\varphi'(k_1),\ldots,\varphi'(k_s))$. Since $\tau_i^{-1}(k_i) = \varphi^{-1}(B_i^{-1}\varphi(k_i))$, we see that the q-adic length of the k_i, which equals the maximal index j such that the jth component of $\varphi(k_i)$ is nonzero, is not changed if the B_i are upper triangular. The term $\lfloor\log_q k_i\rfloor$ in the formula for $r_{\boldsymbol{k},\boldsymbol{\gamma}}$ expresses just this length, i.e., $r_{\boldsymbol{k},\boldsymbol{\gamma}} = r_{\tau^{-1}(\boldsymbol{k}),\boldsymbol{\gamma}}$. Thus

$$e^2_{q^m,s}(\boldsymbol{\alpha}) = \sum_{\boldsymbol{k}\in\mathcal{N}_{\boldsymbol{\alpha}}} r_{\boldsymbol{k},\boldsymbol{\gamma}}.$$

This means we get exactly the same results for any choice of 'upper triangular' bases, especially for B_i equalling the identity matrices. Hyperplane nets with these parameters are just polynomial lattice point sets, except for ordering, which does not come into account here; see [6,25].

3. Construction of extensible hyperplane nets

We will now consider extensible hyperplane nets with changing extension steps, i.e., not just powers $f(x)^n$. For polynomial lattice point sets over $\mathbb{F}_p$, p a prime, changing extension steps have been considered in [15].

Before we proceed to present and assess the algorithm in Theorem 1 we investigate what further restrictions need to be imposed on the bases so that we indeed will get 'extended' nets, i.e., a sequence of subnets. We will do this in some small, easy lemmas which might be of independent interest.

Let us denote by $\mathcal{P}(C)$ the digital $(t,m,1)$-net associated to a generator matrix $C\in\mathbb{F}_q^{m\times m}$. (The restriction to $s=1$ is actually without limitation of generality and only for convenience's sake.)

Lemma 1. *Let $m_1 < m_2$, $C_1 \in \mathbb{F}_q^{m_1 \times m_1}$, $C_2 \in \mathbb{F}_q^{m_2 \times m_2}$, where C_1 is regular. An inclusion $\mathcal{P}(C_1) \subseteq \mathcal{P}(C_2)$ holds iff there exists a regular matrix T such that C_1 is the upper left submatrix of C_2T, i.e., more exactly,*

$$C_2T = \begin{pmatrix} C_1 & U \\ 0 & D \end{pmatrix} \quad \text{for some matrices } U, D.$$

Proof. The 'if' part is obvious. (Consider the first q^{m_1} points of $\mathcal{P}(C_2T)$ and note that $\mathcal{P}(C_2T)$ is just a reordering of $\mathcal{P}(C_2)$.)

For the 'only if' part, let $\mathbf{c}_1, \ldots, \mathbf{c}_{m_1}$ be the column vectors of C_1. The inclusion $\mathcal{P}(C_1) \subseteq \mathcal{P}(C_2)$ implies there are vectors $\mathbf{t}_1, \ldots, \mathbf{t}_{m_1}$ such that $C_2\mathbf{t}_i = \iota(\mathbf{c}_i)$, $i = 1, \ldots, m_1$ (here $\iota : \mathbb{F}_q^{m_1} \to \mathbb{F}_q^{m_2}$ is the natural injection mapping into the first m_1 coordinates). Since C_1 is regular, the matrix $(\mathbf{t}_1 \cdots \mathbf{t}_{m_1}) \in \mathbb{F}_q^{m_2 \times m_1}$ is of full rank m_1 and can be completed to a square regular matrix $T \in \mathbb{F}_q^{m_2 \times m_2}$ which then fulfils the requirements. □

Remark 3. If the inclusion is only required to be *up to truncation*, i.e., if there is a subset of $\mathcal{P}(C_2)$ that equals $\mathcal{P}(C_1)$ after truncating to m_1 fractional q-adic digits, the lower left submatrix of C_2T does not need to be the zero matrix but can be arbitrary.

Lemma 2. *Let $m_1 < m_2$, $C_1 \in \mathbb{F}_q^{m_1 \times m_1}$, $C_2 \in \mathbb{F}_q^{m_2 \times m_2}$ and let $B_1 \in \mathbb{F}_q^{m_1 \times m_1}$, $B_2 \in \mathbb{F}_q^{m_2 \times m_2}$ be regular matrices where B_2 is of the form*

$$B_2 = \begin{pmatrix} B_1 & U \\ L & D \end{pmatrix}.$$

Then, if $L = 0$,

$$\mathcal{P}(C_1) \subseteq \mathcal{P}(C_2) \quad \text{iff} \quad \mathcal{P}(B_1C_1) \subseteq \mathcal{P}(B_2C_2).$$

If $L \neq 0$ but $U = 0$, then the inclusions hold only up to truncation.

Proof. If $\mathcal{P}(C_1) \subseteq \mathcal{P}(C_2)$, by Lemma 1 there exists a regular matrix T such that C_1 is the upper left submatrix of C_2T.

First consider $L = 0$. Then, by the following calculation, the same matrix transforms the two pairs of nets:

$$B_2(C_2T) = \begin{pmatrix} B_1 & U \\ 0 & D \end{pmatrix} \begin{pmatrix} C_1 & U_2 \\ 0 & D_2 \end{pmatrix} = \begin{pmatrix} B_1C_1 & U_3 \\ 0 & D_3 \end{pmatrix},$$

for some matrices U_i, D_i. Similarly for $U = 0$,

$$B_2(C_2T) = \begin{pmatrix} B_1 & 0 \\ L & D \end{pmatrix} \begin{pmatrix} C_1 & U_2 \\ L_2 & D_2 \end{pmatrix} = \begin{pmatrix} B_1C_1 & U_3 \\ L_3 & D_3 \end{pmatrix},$$

for some matrices U_i, L_i, D_i. □

Remark 4. In the higher-dimensional case we can take different $B_{1,i}$, $B_{2,i}$ for each $i = 1, \ldots, s$, i.e., there is no restriction to just one transformation matrix for all coordinates.

Corollary 1. *Let $f, g \in \mathbb{F}_q[x]$ and let $\mathbb{K}_1 := \mathbb{F}_q[x]/(f)$ and $\mathbb{K}_2 := \mathbb{F}_q[x]/(fg)$. Consider*

$$\alpha_1 \in \mathbb{K}_1, \qquad \alpha_2 \in \mathbb{K}_2, \quad \text{such that} \quad \alpha_2 \equiv \alpha_1 \pmod f.$$

Further choose bases $\mathcal{B}_1 \subseteq \mathbb{K}_1$, $\mathcal{B}_2 \subseteq \mathbb{K}_2$ such that for their transformation matrices B_1, B_2 we have

$$B_2 = \begin{pmatrix} B_1 & L \\ U & D \end{pmatrix},$$

with some matrices L, U, D, where at least one of L and U is a null matrix. Then the hyperplane net $\mathcal{P}_{\alpha_1}$ with basis $\mathcal{B}_1$ is a subset of the hyperplane net $\mathcal{P}_{\alpha_2}$ with basis $\mathcal{B}_2$. The inclusion is in the strict sense if $L = 0$ and only up to truncation if $L \neq 0$, $U = 0$.

Proof. First supposing that the B_j are identity matrices we have by [25] that the corresponding hyperplane nets are (reordered) polynomial lattice rule point sets for which we know that the inclusion relation holds. Also from [25] we know that in this case the generator matrices are of the form $\Psi_1(\alpha_1)^\top, \Psi_2(\alpha_2)^\top$ with appropriate maps $\Psi_1 : \mathbb{K}_1 \to \mathbb{F}_q^{m_1 \times m_1}$, $\Psi_2 : \mathbb{K}_2 \to \mathbb{F}_q^{m_2 \times m_2}$, whereas if we include the bases in the construction, the matrices are $(\Psi_1(\alpha_1)B_1)^\top, (\Psi_2(\alpha_2)B_2)^\top$. Application of the previous lemma leads to the result. □

From here on we are considering a special subclass of hyperplane nets, namely polynomial lattice rules with the added generality of basis transformation matrices that are block diagonal with specific upper triangular blocks. By the previous corollary we know that a stepwise extension of the generating and transformation matrices leads to an inclusion chain of nets. (Furthermore, for slightly more general transformation matrices we still have a weaker inclusion chain, that holds up to truncation.)

As quality criterion we use the worst-case error of quasi-Monte Carlo integration in $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$. In the notation we henceforth omit the sub-indices q^m and s, i.e., we write simply $e^2(\boldsymbol{\alpha})$. Algorithm 1 is inspired by an idea of Korobov [10] for lattice point sets.

Algorithm 1 Construction of extensible hyperplane nets.

Require: Let $f_k \in \mathbb{F}_q[x]$, $k \geqslant 1$, be a sequence of polynomials and set $F_n := \prod_{k=1}^{n} f_k$ and $m_n := \deg F_n$ for $n \geqslant 1$. For each $i \in \{1, \ldots, s\}$ and all $n \geqslant 1$ choose a basis $\mathcal{B}_{n,i} = \{\mathfrak{b}_{n,i,1}, \ldots, \mathfrak{b}_{n,1,m_n}\}$ of the polynomial residue class ring $R_n := \mathbb{F}_q[x]/(F_n)$ over $\mathbb{F}_q$ such that the transformation matrices between any $\mathcal{B}_{n,i}$, $\mathcal{B}_{n,i'}$ are upper triangular.

1: Find $\boldsymbol{\alpha}_1$ by minimizing $e^2(\boldsymbol{\alpha}_1)$ over all $\boldsymbol{\alpha}_1 \in R_1^s$.
2: **for** $n > 1$ **do**
3: find $\boldsymbol{\alpha}_n := \boldsymbol{\alpha}_{n-1} + \boldsymbol{z}F_{n-1}$ by minimizing $e^2(\boldsymbol{\alpha}_{n-1} + \boldsymbol{z}F_{n-1})$ over all $\boldsymbol{z} \in \mathbb{F}_q[x]^s$ with $\deg z_i < \deg f_n$ for all $i \in \{1, \ldots, s\}$.
4: **return** α_n
5: **end for**

Now we state and prove the main result of this paper:

Theorem 1. *Let $f_k \in \mathbb{F}_q[x]$, $k \geqslant 1$, be a sequence of polynomials and set $F_n := \prod_{k=1}^{n} f_k$ and $m_n := \deg F_n$ for $n \geqslant 1$. For each $i \in \{1, \ldots, s\}$ and all $n \geqslant 1$ choose a basis $\mathcal{B}_{n,i} = \{\mathfrak{b}_{n,i,1}, \ldots, \mathfrak{b}_{n,i,m_n}\}$ of the polynomial residue class ring $R_n := \mathbb{F}_q[x]/(F_n)$ over $\mathbb{F}_q$ such that $\mathfrak{b}_{n,i,j} = \mathfrak{b}_{n+1,i,j}$ and the transformation matrices between any $\mathcal{B}_{n,i}$, $\mathcal{B}_{n,i'}$ are upper triangular and block diagonal, with the blocks consisting of transformation matrices between $\mathcal{B}_{n+1,i} \setminus \mathcal{B}_{n,i}$, $\mathcal{B}_{n+1,i'} \setminus \mathcal{B}_{n,i'}$ (i.e., the matrices have the appropriate form to apply Corollary 1).*

Assume that $\boldsymbol{\alpha}_n$ is constructed according to Algorithm 1. Define $\mu_q(\beta) := \frac{q^\beta(q-1)}{q^\beta - q}$. Then we have

$$e^2(\boldsymbol{\alpha}_1) \leqslant \left(\prod_{i=1}^{s} \big(1 + \gamma_i \mu_q(\beta)\big) - 1 \right) \frac{2}{q^{\deg f_1}},$$

$$e^2(\boldsymbol{\alpha}_n) \leqslant e^2(\boldsymbol{\alpha}_1) \left(\sum_{d \mid (F_n/f_1)} q^{-(\beta-1)\deg d} \right) \frac{q^{\deg f_1}}{q^{\deg F_n}}$$

$$\leqslant \left(\prod_{i=1}^{s} \big(1 + \gamma_i \mu_q(\beta)\big) - 1 \right) \left(\sum_{d \mid (F_n/f_1)} q^{-(\beta-1)\deg d} \right) \frac{2}{q^{m_n}}.$$

In the case of irreducible $f_i = f$ for all i, we can replace the second factor in the previous two lines (i.e., the sum over all divisors of F_n/f_1) by

$$\min\bigl\{n, 1 + \bigl(q^{(\beta-1)\deg f} - 1\bigr)^{-1}\bigr\},$$

which is less than n for $\beta \geqslant 1 + \log_q(2)/\deg f$.

If $\boldsymbol{\alpha}_1$ is chosen arbitrarily, the first inequality for $e^2(\boldsymbol{\alpha}_n)$ still holds. For $f_i = f$, Remarks 10 and 11 in [20] apply analogously, i.e., the bounds hold with minor adaption if the algorithm is started with an arbitrary vector and/or at a later iteration level n.

Proof. The theorem will be proven using an inequality recursion of $e^2(\boldsymbol{\alpha}_n)$ in n. We start by deriving an inhomogeneous recursion and will then step by step resolve it.

Let $n \geqslant 2$. We set $Z_n = \{f \in \mathbb{F}_q[x]\colon \deg f < \deg f_n\}^s$ and $\widetilde{\mathbb{N}}^s = \mathbb{N}_0^s \setminus \{\mathbf{0}\}$. Define

$$\begin{aligned} A_{\boldsymbol{k}} &:= \{\boldsymbol{z} \in Z_n\colon \boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}+F_{n-1}\boldsymbol{z}}\} \\ &= \bigl\{\boldsymbol{z} \in Z_n\colon F_{n-1}\varphi'(\boldsymbol{k}) \cdot \boldsymbol{z} \equiv -\varphi'(\boldsymbol{k}) \cdot \boldsymbol{\alpha}_{n-1} \pmod{F_n}\bigr\}. \end{aligned}$$

Then we have

$$\begin{aligned} e^2(\boldsymbol{\alpha}_n) &\leqslant \frac{1}{\#Z_n} \sum_{\boldsymbol{z} \in Z_n} e^2(\boldsymbol{\alpha}_{n-1} + F_{n-1}\boldsymbol{z}) \\ &= \frac{1}{\#Z_n} \sum_{\boldsymbol{z} \in Z_n} \sum_{\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}+F_{n-1}\boldsymbol{z}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \\ &\leqslant \frac{1}{\#Z_n} \sum_{\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \#A_{\boldsymbol{k}}, \end{aligned}$$

since $\mathcal{N}_{\boldsymbol{\alpha}_{n-1}} \supseteq \bigcup_{\boldsymbol{z} \in Z_n} \mathcal{N}_{\boldsymbol{\alpha}_{n-1}+F_{n-1}\boldsymbol{z}}$ (note that in $\mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$ the modulus is F_{n-1} while in $\mathcal{N}_{\boldsymbol{\alpha}_{n-1}+F_{n-1}\boldsymbol{z}}$ it is F_n). For any $\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$, i.e., $\varphi'(\boldsymbol{k}) \cdot \boldsymbol{\alpha}_{n-1} \equiv 0 \pmod{F_{n-1}}$, we can cancel F_{n-1} and get

$$A_{\boldsymbol{k}} = \bigl\{\boldsymbol{z} \in Z_n\colon \varphi'(\boldsymbol{k}) \cdot \boldsymbol{z} \equiv -\varphi'(\boldsymbol{k}) \cdot \boldsymbol{\alpha}_{n-1}/F_{n-1} \pmod{f_n}\bigr\}.$$

The sets $A_{\boldsymbol{k}}$ are solution spaces of linear equation systems over Z_n. Their size depends on $\boldsymbol{k}$ in the following way: if the GCD of f_n and the coefficients $\varphi'(\boldsymbol{k})$ on the left-hand side, call it $d = \gcd(\varphi'(\boldsymbol{k}), f_n)$, does not divide the right-hand side, or put differently, if $\varphi'(\boldsymbol{k}) \cdot \boldsymbol{\alpha}_{n-1} \not\equiv 0 \pmod{dF_{n-1}}$ the system has no solution and $A_{\boldsymbol{k}}$ is empty. Else, after cancelling the common factor d from the equation we get a solution space of dimension $s-1$ over the polynomial residue class ring $\mathbb{F}_q[x]/(f_n/d)$, i.e., $q^{(s-1)\deg(f_n/d)}$ solutions which lift to $\#A_{\boldsymbol{k}} = q^{(s-1)\deg(f_n/d)} q^{s\deg d} = (q^{\deg d}/q^{\deg f_n})\#Z_n$ solutions $\boldsymbol{z}$ in Z_n.

We partition those $\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$ with nonempty solution spaces into distinct sets $\mathcal{M}_{n-1,d}$ associated to the divisors of f_n:

$$\mathcal{N}_{\boldsymbol{\alpha}_{n-1}} \supset \bigcup_{d \mid f_n} \mathcal{M}_{n-1,d},$$

where

$$\mathcal{M}_{n-1,d} := \bigl\{\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}\colon \gcd\bigl(\varphi'(\boldsymbol{k}), f_n\bigr) = d,\ \varphi'(\boldsymbol{k}) \cdot \boldsymbol{\alpha}_{n-1} \equiv 0 \pmod{dF_{n-1}}\bigr\}.$$

Another partition, but of the complete set $\mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$, associated to the divisors of f_n is

$$\mathcal{N}_{\boldsymbol{\alpha}_{n-1}} = \bigcup_{d|f_n} \mathcal{M}^+_{n-1,d},$$

where

$$\mathcal{M}^+_{n-1,d} := \{\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}} \colon \gcd(\varphi'(\boldsymbol{k}), f_n) = d\}.$$

Clearly $\mathcal{M}_{n-1,1} = \mathcal{M}^+_{n-1,1}$ and $\mathcal{M}_{n-1,d} \subseteq \mathcal{M}^+_{n-1,d} \subseteq d\mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$. (Here in the term $d\mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$ and in the following the action of $d \in Z_n$ on $\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}$ is understood to be $(\varphi')^{-1}(d\varphi'(\boldsymbol{k}))$.)

Then

$$\begin{aligned} e^2(\boldsymbol{\alpha}_n) &\leqslant \frac{1}{q^{\deg f_n}} \sum_{d|f_n} q^{\deg d} \sum_{\boldsymbol{k} \in \mathcal{M}_{n-1,d}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \\ &= \frac{1}{q^{\deg f_n}} \left(e^2(\boldsymbol{\alpha}_{n-1}) + \sum_{d|f_n,\, d\neq 1} \left(q^{\deg d} \sum_{\boldsymbol{k} \in \mathcal{M}_{n-1,d}} r_{\boldsymbol{k},\boldsymbol{\gamma}} - \sum_{\boldsymbol{k} \in \mathcal{M}^+_{n-1,d}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \right) \right) \\ &\leqslant \frac{1}{q^{\deg f_n}} \left(e^2(\boldsymbol{\alpha}_{n-1}) + \sum_{d|f_n,\, d\neq 1} q^{\deg d} \sum_{\boldsymbol{k} \in \mathcal{M}_{n-1,d}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \right) \end{aligned} \tag{4}$$

and this holds for all $n \geqslant 2$.

For the last sum in (4) we get

$$\sum_{\boldsymbol{k} \in \mathcal{M}_{n-1,d}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \leqslant \sum_{\boldsymbol{k} \in d\mathcal{N}_{\boldsymbol{\alpha}_{n-1}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} = \sum_{\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}} r_{d\boldsymbol{k},\boldsymbol{\gamma}} \leqslant \frac{1}{q^{\beta \deg d}} \sum_{\boldsymbol{k} \in \mathcal{N}_{\boldsymbol{\alpha}_{n-1}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} = \frac{e^2(\boldsymbol{\alpha}_{n-1})}{q^{\beta \deg d}}. \tag{5}$$

So from (4) and (5) we get the inequality

$$\begin{aligned} e^2(\boldsymbol{\alpha}_n) &\leqslant e^2(\boldsymbol{\alpha}_{n-1}) \frac{1}{q^{\deg f_n}} \left(1 + \sum_{d|f_n,\, d\neq 1} \frac{1}{q^{(\beta-1)\deg d}} \right) \\ &\leqslant e^2(\boldsymbol{\alpha}_1) \prod_{k=2}^{n} \frac{1}{q^{\deg f_k}} \sum_{d|f_k} q^{-(\beta-1)\deg d} \\ &= e^2(\boldsymbol{\alpha}_1) \frac{q^{\deg f_1}}{q^{\deg F_n}} \sum_{d|(F_n/f_1)} q^{-(\beta-1)\deg d}. \end{aligned} \tag{6}$$

For the recursion start $n = 1$, we get the same estimate of the 'initial error' as in [20, Theorem 3]. We rewrite the derivation of the bound in our notation

$$\begin{aligned} e^2(\boldsymbol{\alpha}_1) &\leqslant \frac{1}{q^{s \deg f_1}} \sum_{\boldsymbol{z} \in Z_1} e^2(\boldsymbol{z}) \\ &= \frac{1}{q^{s \deg f_1}} \sum_{\boldsymbol{k} \in \widetilde{\mathbb{N}}^s} r_{\boldsymbol{k},\boldsymbol{\gamma}} \#\{\boldsymbol{z} \in Z_1 \colon \varphi'(\boldsymbol{k}) \cdot \boldsymbol{z} \equiv \boldsymbol{0} \pmod{f_1}\} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{\boldsymbol{k}\in\widetilde{\mathbb{N}}^s \\ \varphi'(\boldsymbol{k})\equiv\boldsymbol{0} \pmod{f_1}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} + \frac{1}{q^{\deg f_1}} \sum_{\substack{\boldsymbol{k}\in\widetilde{\mathbb{N}}^s \\ \varphi'(\boldsymbol{k})\not\equiv\boldsymbol{0} \pmod{f_1}}} r_{\boldsymbol{k},\boldsymbol{\gamma}} \\
&= \left(1 - \frac{1}{q^{\deg f_1}}\right) \sum_{\boldsymbol{k}\in\widetilde{\mathbb{N}}^s} r_{f_1\boldsymbol{k},\boldsymbol{\gamma}} + \frac{1}{q^{\deg f_1}} \sum_{\boldsymbol{k}\in\widetilde{\mathbb{N}}^s} r_{\boldsymbol{k},\boldsymbol{\gamma}} \\
&\leqslant \frac{2}{q^{\deg f_1}} \sum_{\boldsymbol{k}\in\widetilde{\mathbb{N}}^s} r_{\boldsymbol{k},\boldsymbol{\gamma}} \\
&= \frac{2}{q^{\deg f_1}} \left(\prod_{i=1}^{s} \bigl(1 + \gamma_i \mu_q(\beta)\bigr) - 1 \right), \qquad (7)
\end{aligned}
$$

where $\mu_q(\beta) = \frac{q^\beta(q-1)}{q^\beta - q}$. This proves the theorem for f_i nonconstant in i. For irreducible $f_i = f$, $i > 0$, proceeding analogously as in the proof of [20, Theorem 3], we can improve (6) to

$$e^2(\boldsymbol{\alpha}_n) \leqslant q^{-(n-1)\deg f} e^2(\boldsymbol{\alpha}_1) + q^{-\beta\deg f} e^2(\boldsymbol{\alpha}_{n-1})$$

which, by the same calculations as there, leads to the stated result. □

Remark 5. Observe that in the case of f_k nonconstant in k, we get the same bound for any refinement or coarsening of the steps, i.e., regardless whether we take irreducible f_k or some consecutive products of the same sequence. Since the search space for composite f_k is larger, an improvement might have been expected, but unfortunately this does not show up with the methods used here.

Also, perhaps for a related reason, it does not seem possible to deduce an improvement for the case of $f_k = f_1$ for all k, with composite f_1.

4. Existence results

We can also give pure existence results similar to the one in [15] for polynomial lattices. Using definitions and notation from [15], see also [6, Ch. 10.4], let the divisibility chain F be given by $(F_n)_{n\geqslant 1}$, i.e., the cumulative products of the f_k as we consider them in this paper. Furthermore let a sequence of bases be given, such that the initial s terms of the sequence form an s-dimensional basis of the same kind as for Theorem 1.

The existence results state that out of a parameter space that is infinite in m and s (this space is in fact $\mathbb{F}_q[\![x]\!]^\infty$, the space of sequences of formal power series over $\mathbb{F}_q$) we can pick a nonempty but arbitrarily small subspace (the size being expressed by a measure $\mu_F^{(\infty)}$) such that for the hyperplane nets constructed with $\boldsymbol{\alpha}$ taken from outside of this exceptional subspace certain bounds hold.

Let λ_F be the measure induced by the map from $\mathbb{F}_q[\![x]\!]$ to $[0,1)$ defined by φ_1^{-1} and the map $x \mapsto q^{-1}$, and let U_F denote the subset of power series whose reductions modulo any F_n are invertible modulo F_n, i.e., $U_F = \{f \in \mathbb{F}_q[\![x]\!],\ \forall n \geqslant 1\colon \gcd(f \bmod F_n, F_n) = 1\}$. Then, assuming $\lambda_F(U_F) > 0$, we define the measure μ_F on U_F by restricting and normalizing: $\mu_F = (\lambda_F|_{U_F})/\lambda_F(U_F)$. Finally, $\mu_F^{(\infty)}$ is the complete product measure on U_F^∞ induced by μ_F.

Corollary 2. *Let F be a divisibility chain such that $\lambda_F(U_F) > 0$. Then for every $\varepsilon > 0$, there exists a $\mu_F^{(\infty)}$-measurable set $E \subseteq U_F^\infty \subseteq \mathbb{F}_q[\![x]\!]^\infty$ such that for all $\boldsymbol{\alpha} \in U_F^\infty \setminus E$ we have*

$$e^2\bigl(\boldsymbol{\alpha}^{(s)}\bigr) \leqslant \frac{(2c_\varepsilon s(\log(s+1))^{1+\varepsilon} k(\log(k+1))^{1+\varepsilon})^{1/\lambda}}{q^{\deg(F_k)/\lambda}} \left(\prod_{i=1}^{s} \bigl(1 + \gamma_i^\lambda \mu_q(\lambda\beta)\bigr) - 1 \right)^{1/\lambda},$$

for all $1/\beta < \lambda \leqslant 1$, all $k \in \mathbb{N}$ and $s \in \mathbb{N}$, where $\boldsymbol{\alpha}^{(s)}$ is the projection to the first s coordinates and the constant $c_\varepsilon > 0$ depends only on ε and a bound on the size of the exceptional set E (i.e., $\mu_F^{(\infty)}(E)$ can be made arbitrarily small at the cost of larger c_ε).

Proof. Using Jensen's inequality (i.e. $(\sum a_k)^\lambda \leqslant \sum a_k^\lambda$ for any $0 < \lambda \leqslant 1$) we obtain

$$e^{2\lambda}_{\boldsymbol{\gamma},\beta}(\boldsymbol{\alpha}) \leqslant e^2_{\boldsymbol{\gamma}^\lambda,\lambda\beta}(\boldsymbol{\alpha}),$$

where $\boldsymbol{\gamma}^\lambda$ denotes the sequence $\gamma_1^\lambda, \gamma_2^\lambda, \ldots$.

Let $1/\beta < \lambda \leqslant 1$ (for this choice $\mu_b(\lambda\beta)$ is well defined). Averaging over all $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ where $\deg(\alpha_i) < \deg(F_k)$ for $1 \leqslant i \leqslant s$ and using the same arguments as in (7) we obtain

$$\begin{aligned}\frac{1}{q^{s\deg F_k}} \sum_{\boldsymbol{\alpha}} e^{2\lambda}_{\boldsymbol{\gamma},\beta}(\boldsymbol{\alpha}) &\leqslant \frac{1}{q^{s\deg F_k}} \sum_{\boldsymbol{\alpha}} e^2_{\boldsymbol{\gamma}^\lambda,\lambda\beta}(\boldsymbol{\alpha}) \\ &\leqslant \frac{2}{q^{\deg F_k}} \left(\prod_{i=1}^{s} \bigl(1 + \gamma_i^\lambda \mu_q(\lambda\beta)\bigr) - 1 \right). \end{aligned} \tag{8}$$

For $k, s \in \mathbb{N}$ and $c \in (0, 1]$ define the set

$$\mathcal{Q}^{(\infty)}_{s,k}(c) := \left\{ \boldsymbol{\alpha} \in U_F^\infty \colon e^2_{\boldsymbol{\gamma},\beta}\bigl(\boldsymbol{\alpha}^{(s)}\bigr) \leqslant \frac{(2c)^{1/\lambda}}{q^{(\deg F_k)/\lambda}} \left(\prod_{i=1}^{s} \bigl(1 + \gamma_i^\lambda \mu_b(\lambda\beta)\bigr) - 1 \right)^{1/\lambda} \right\}.$$

From (8) and an application of Markov's inequality, we obtain

$$\mu_F^{(\infty)}\bigl(\mathcal{Q}^{(\infty)}_{s,k}(c)\bigr) > 1 - \frac{1}{c},$$

and this holds for any $1/\beta < \lambda \leqslant 1$.

In order to obtain an $\boldsymbol{\alpha} \in U_F^\infty$ which works well for all choices of $k, s \in \mathbb{N}$, we need to show that the intersection $\bigcap_{s,k\in\mathbb{N}} \mathcal{Q}^{(\infty)}_{s,k}(c)$ has measure greater than zero. This however follows with the same arguments as used in [6, Proof of Theorem 10.41]. □

Remark 6. Similar as in [6, Remark 10.43] we observe that the cost for the existence of a parameter that holds for all $k, s \in \mathbb{N}$ compared to fixed k and s (i.e., the bound in (8)) is a factor $(s(\log(s+1))^{1+\varepsilon} k(\log(k+1))^{1+\varepsilon})^{1/\lambda}$.

In Theorem 1 we cannot immediately get a similar result with the same method using Jensen's inequality, since the minimization step may lead to different $\boldsymbol{\alpha}$ for different choices of λ.

The quantities $R_q(\boldsymbol{\alpha})$ and $\widetilde{R}_{q,\boldsymbol{\gamma}}(\boldsymbol{\alpha})$ defined in [23] are of a very similar nature to the worst-case error $e^2(\boldsymbol{\alpha})$. They are related to the star discrepancy and weighted star discrepancy, i.e., we have for the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$, with $\boldsymbol{\alpha} \in (\mathbb{F}_{q^m}^*)^s$,

$$D^*_{q^m}(\mathcal{P}_{\boldsymbol{\alpha}}) \leqslant \frac{s}{q^m} + 2R_q(\boldsymbol{\alpha})$$

and similarly for the weighted case. For more information we refer to [23] or to [6, Section 11.3].

Corollary 3. *Let F be a divisibility chain such that $\lambda_F(U_F) > 0$. Then for every $\varepsilon > 0$, there exists a $\mu_F^{(\infty)}$-measurable set $E \subseteq U_F^\infty \subseteq \mathbb{F}_q[[x]]^\infty$ such that for all $\boldsymbol{\alpha} \in U_F^\infty \setminus E$ we have*

$$R_q\big(\boldsymbol{\alpha}^{(s)}\big) \leqslant \frac{c_\varepsilon s(\log(s+1))^{1+\varepsilon} k(\log(k+1))^{1+\varepsilon}}{q^{\deg(F_k)} - 1} \big(1 + \deg(F_k) q\big)^s$$

and

$$\widetilde{R}_{q,\boldsymbol{\gamma}}\big(\boldsymbol{\alpha}^{(s)}\big) \leqslant \frac{c_\varepsilon s(\log(s+1))^{1+\varepsilon} k(\log(k+1))^{1+\varepsilon}}{q^{\deg(F_k)} - 1} \prod_{i=1}^{s} \big(1 + \gamma_i \big(1 + \deg(F_k) q\big)\big)$$

for all $k \in \mathbb{N}$ and $s \in \mathbb{N}$. Again, $\boldsymbol{\alpha}^{(s)}$ is the projection to the first s coordinates and the constant $c_\varepsilon > 0$ depends only on ε and a bound on the size of the exceptional set E (i.e., $\mu_F^{(\infty)}(E)$ can be made arbitrarily small at the cost of larger c_ε).

Again, the assertions of this corollary follow by an easy adaption of the proof technique of [6, Theorem 10.41], using the bound [23, Theorem 1] in place of [6, Lemma 10.42].

5. Numerical investigation

Using an implementation of the algorithms in the computer algebra system MATHEMATICA [28], we tried to analyze the behavior with respect to different types of parameters. Specifically, we compared sequences with constant vs. varying, irreducible vs. compound polynomials up to degree 3, in base 2, for point sizes up to 2^{12}. As bases the following were used, described by their transformations matrices B_i: the identity matrix, upper triangular block diagonal matrices with all nonzero entries equal to 1 (we henceforth call this the 'constant-1' matrix), with Pascal matrices (i.e., the binomial coefficients modulo p) in the blocks and also with random entries.

Our investigations focused on $e^2_{\boldsymbol{\gamma}}(\boldsymbol{\alpha})$, the squared worst-case error of integration in $\mathscr{H}_{\mathrm{wal},s,\beta,\boldsymbol{\gamma}}$. Plots of the dyadic logarithm of the error (against the dyadic logarithm of the point size) exhibited a very close approximation of all cases to an asymptotic of roughly $\log_2(N^{-1.3})$, this to such an extent that all plots blended into a single line. To improve the visibility of the differences a 'normalized' logarithmic error, i.e., $\log_2(N^{1.3} e^2_{\boldsymbol{\gamma}}(\boldsymbol{\alpha}))$, is shown. Also, in the presentation of the results the 'constant-1' matrix was chosen exemplarily, other bases showed similar behavior.

The parameters in detail:

- Basic parameters: $s = 5$, $q = 2$, $\beta = 2$, $\gamma_i = i^{-2}$.
- $f_i = (x+1)^i$, $i = 1, 2, 3$; $f_4 = x^2 + x + 1$.
- Transformation matrices: identity; constant 1 in upper triangular blocks (also tested, not presented here: Pascal and random matrices in upper triangular blocks).
- Test lines (the labels refer to the legends in the figures):
  - **1**: constant deg 1 steps: $\{f_1, f_1, f_1, f_1, f_1, f_1, f_1, f_1, f_1, f_1, f_1, f_1\}$,
  - **2**: constant deg 2 steps: $\{f_2, f_2, f_2, f_2, f_2, f_2\}$,
  - **2′**: constant irr. deg 2 steps: $\{f_4, f_4, f_4, f_4, f_4, f_4\}$,
  - **3**: constant deg 3 steps: $\{f_3, f_3, f_3, f_3\}$,
  - **123**: mixed steps A: $\{f_1, f_2, f_3, f_1, f_2, f_3\}$,
  - **321**: mixed steps B: $\{f_3, f_2, f_1, f_3, f_2, f_1\}$.

Our results were not fully conclusive, perhaps owing to the still comparatively small number of steps we could carry out in the tests. We observed the following:

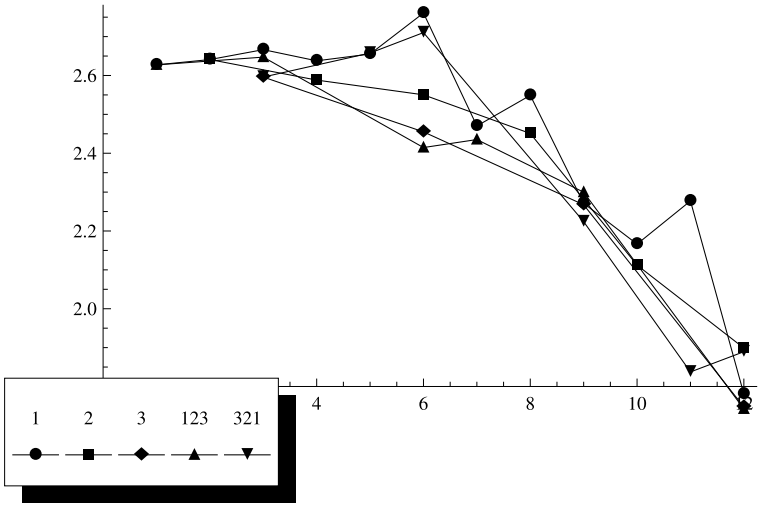


Fig. 1. Different step sizes.

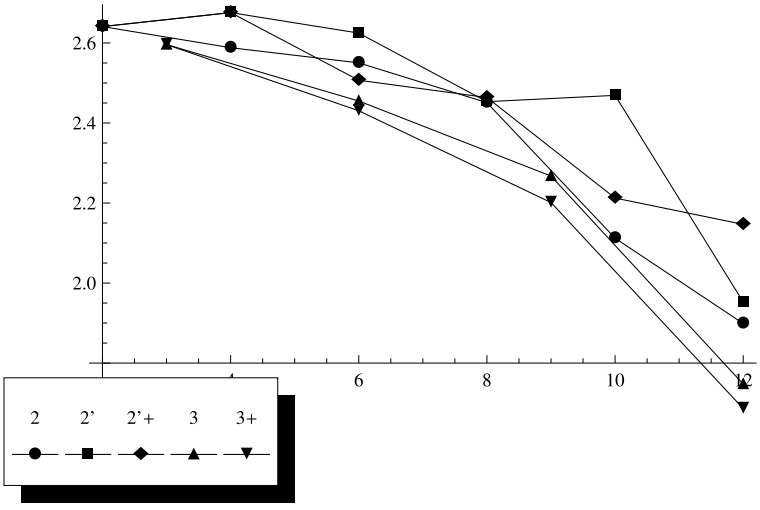


Fig. 2. Different bases.

- Iteration steps where we extend by a polynomial that is a product perform better than several single steps associated to its factors (see Fig. 1) – heuristically, this would be expected, since the search space is larger for the compound polynomial.
- Iteration steps with compound polynomials performed better than those with irreducible polynomials of the same degree (see Fig. 2), which seems to contradict the theoretical bounds, although it must be said that the difference is very small.
- Different transformation matrices actually only effect small differences (see Figs. 2, 3, a + indicates use of the 'constant-1' matrix). Sometimes there are gains, but in this test series no pronounced overall improvement could be seen.
- There seems to be still some room for improvement from the upper bounds, possibly even in asymptotics. E.g., for the cases **1** and **2** the order of the theoretical bounds are $N^{-0.4}$ and $N^{-0.85}$ respectively, compared to the observed order of $N^{-1.3}$ in both cases.

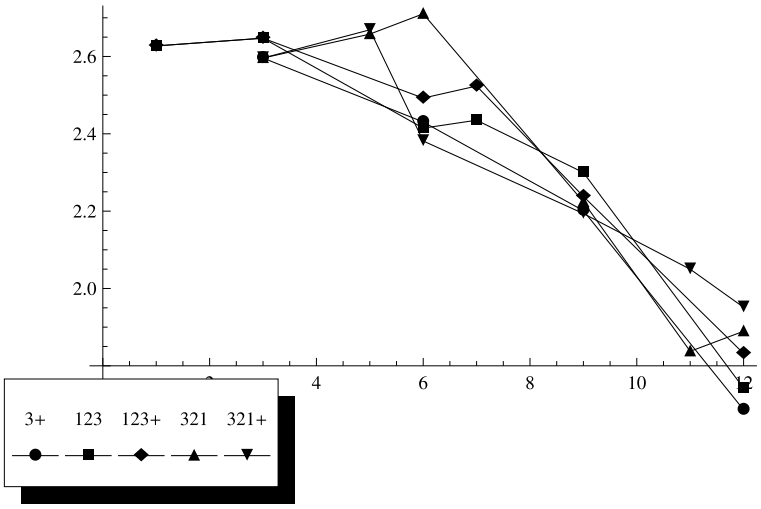


Fig. 3. Mixed steps and different bases.

Acknowledgments

The authors thank the anonymous referees for helpful comments and suggestions which helped to improve the presentation of this paper.

References

[1] N. Aronszajn, Theory of reproducing kernels, Trans. Amer. Math. Soc. 68 (1950) 337–404.
[2] J. Bierbrauer, Y. Edel, W.Ch. Schmid, Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays, J. Combin. Des. 10 (2002) 403–418.
[3] J. Dick, The construction of extensible polynomial lattice rules with small weighted star discrepancy, Math. Comp. 76 (2007) 2077–2085.
[4] J. Dick, F.Y. Kuo, F. Pillichshammer, I.H. Sloan, Construction algorithms for polynomial lattice rules for multivariate integration, Math. Comp. 74 (2005) 1895–1921.
[5] J. Dick, F. Pillichshammer, Multivariate integration in weighted Hilbert spaces based on Walsh functions and weighted Sobolev spaces, J. Complexity 21 (2005) 149–195.
[6] J. Dick, F. Pillichshammer, Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration, Cambridge University Press, Cambridge, 2010.
[7] J. Dick, F. Pillichshammer, B.J. Waterhouse, The construction of good extensible rank-1 lattices, Math. Comp. 77 (2008) 1345–1373.
[8] F.J. Hickernell, H.S. Hong, P. L'Ecuyer, C. Lemieux, Extensible lattice sequences for quasi-Monte Carlo quadrature, SIAM J. Sci. Comput. 22 (2000) 1117–1138.
[9] F.J. Hickernell, H. Niederreiter, The existence of good extensible rank-1 lattices, J. Complexity 19 (2003) 286–300.
[10] N.M. Korobov, On the calculation of optimal coefficients, Soviet Math. Dokl. 26 (1982) 590–593.
[11] P. Kritzer, F. Pillichshammer, Constructions of general polynomial lattices for multivariate integration, Bull. Aust. Math. Soc. 76 (2007) 93–110.
[12] H. Niederreiter, Point sets and sequences with small discrepancy, Monatsh. Math. 104 (1987) 273–337.
[13] H. Niederreiter, Low-discrepancy point sets obtained by digital constructions over finite fields, Czechoslovak Math. J. 42 (1992) 143–166.
[14] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, CBMS-NSF Ser. in Appl. Math., vol. 63, SIAM, Philadelphia, 1992.
[15] H. Niederreiter, The existence of good extensible polynomial lattice rules, Monatsh. Math. 139 (2003) 295–307.
[16] H. Niederreiter, Digital nets and coding theory, in: Coding, Cryptography and Combinatorics, Birkhäuser, Basel, 2004, pp. 247–257.
[17] H. Niederreiter, Constructions of (t, m, s)-nets and (t, s)-sequences, Finite Fields Appl. 11 (2005) 578–600.
[18] H. Niederreiter, Nets, (t, s)-sequences and codes, in: Monte Carlo and Quasi-Monte Carlo Methods 2006, Springer, Berlin, 2008, pp. 83–100.
[19] H. Niederreiter, F. Özbudak, Matrix-product constructions of digital nets, Finite Fields Appl. 10 (2004) 464–479.

[20] H. Niederreiter, F. Pillichshammer, Construction algorithms for good extensible lattice rules, Constr. Approx. 30 (2009) 361–393.
[21] H. Niederreiter, G. Pirsic, Duality for digital nets and its applications, Acta Arith. 97 (2002) 173–182.
[22] H. Niederreiter, G. Pirsic, A Kronecker product construction for digital nets, in: Monte Carlo and Quasi-Monte Carlo Methods 2000, Springer, Berlin, 2002, pp. 396–405.
[23] F. Pillichshammer, G. Pirsic, Discrepancy of hyperplane nets and cyclic nets, in: Monte Carlo and Quasi-Monte Carlo Methods 2008, Springer, Berlin, 2009, pp. 573–587.
[24] F. Pillichshammer, G. Pirsic, The quality parameter of cyclic nets and hyperplane nets, Unif. Distrib. Theory 4 (2009) 69–79.
[25] G. Pirsic, A small taxonomy of integration node sets, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 214 (2005) (2006) 133–140.
[26] G. Pirsic, J. Dick, F. Pillichshammer, Cyclic digital nets, hyperplane nets, and multivariate integration in Sobolev spaces, SIAM J. Numer. Anal. 44 (2006) 385–411.
[27] I.H. Sloan, S. Joe, Lattice Methods for Multiple Integration, Clarendon Press, Oxford, 1994.
[28] Wolfram Research, Inc., Mathematica, Version 7.0, Wolfram Research, Inc., Champaign, IL, 2008.