ACTA ARITHMETICA
163.2 (2014)

Vandermonde nets

by

ROSWITHA HOFER (Linz) and
HARALD NIEDERREITER (Linz and Salzburg)

1. Introduction and basic definitions. In this paper, we introduce a new family of digital nets over finite fields. A *net*, or more precisely a (t, m, s)-*net*, is a finite collection of points (also called a *point set*) in the s-dimensional half-open unit cube $[0, 1)^s$ possessing equidistribution properties. A *digital net* is a net obtained by the linear algebra construction described below. Various constructions of nets are already known, and most of them are digital nets. Reviews of the theory of nets can be found in the monograph [2] and in the recent survey article [7].

Let $\mathbb{F}_q$ be the finite field of order q, where q is an arbitrary prime power, and let m and s be positive integers. In order to construct a digital (t, m, s)-net over $\mathbb{F}_q$, we choose $m \times m$ matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{F}_q$, called the *generating matrices* of the digital net. We write $\mathbb{Z}_q = \{0, 1, \ldots, q-1\} \subset \mathbb{Z}$ for the set of digits in base q. We define the map $\Psi_m : \mathbb{F}_q^m \to [0, 1)$ by

$$\Psi_m(\mathbf{h}^\top) = \sum_{j=1}^{m} \psi(h_j) q^{-j}$$

for any column vector $\mathbf{h}^\top = (h_1, \ldots, h_m)^\top \in \mathbb{F}_q^m$, where $\psi : \mathbb{F}_q \to \mathbb{Z}_q$ is a chosen bijection. With a fixed column vector $\mathbf{b}^\top \in \mathbb{F}_q^m$, we associate the point

$$(\Psi_m(C^{(1)}\mathbf{b}^\top), \ldots, \Psi_m(C^{(s)}\mathbf{b}^\top)) \in [0, 1)^s. \tag{1.1}$$

By letting $\mathbf{b}^\top$ range over all q^m column vectors in $\mathbb{F}_q^m$, we arrive at a point set consisting of q^m points in $[0, 1)^s$. This construction of digital nets can be generalized somewhat by employing further bijections between $\mathbb{F}_q$ and $\mathbb{Z}_q$ (see [6, p. 63]), but this is not needed for our purposes since our results

2010 *Mathematics Subject Classification*: Primary 11K31; Secondary 11K38.
Key words and phrases: digital net, discrepancy.

DOI: 10.4064/aa163-2-5

depend just on the generating matrices. For $i = 1, \ldots, s$ and $j = 1, \ldots, m$, let $\mathbf{c}_j^{(i)} \in \mathbb{F}_q^m$ denote the jth row vector of the matrix $C^{(i)}$.

DEFINITION 1.1. Let q be a prime power and let t, m, and s be integers with $0 \leq t \leq m$, $m \geq 1$, and $s \geq 1$. Then the point set consisting of the q^m points in (1.1) is a *digital* (t, m, s)*-net over* $\mathbb{F}_q$ if for any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = m - t$, the $m - t$ vectors $\mathbf{c}_j^{(i)} \in \mathbb{F}_q^m$ with $1 \leq j \leq d_i$ and $1 \leq i \leq s$ are linearly independent over $\mathbb{F}_q$ (the empty collection of vectors occurring in the case $t = m$ is considered linearly independent over $\mathbb{F}_q$).

It is evident that the condition in Definition 1.1 becomes the stronger the smaller the value of t. The main interest is therefore in constructing digital (t, m, s)-nets over $\mathbb{F}_q$ with a small value of t. The number t is called the *quality parameter* of a digital (t, m, s)-net over $\mathbb{F}_q$.

REMARK 1.2. The definition of a digital (t, m, s)-net over $\mathbb{F}_q$ can be translated into an explicit equidistribution property of the points of the digital net as follows. Consider any subinterval J of $[0, 1)^s$ of the form

$$J = \prod_{i=1}^{s} [a_i q^{-d_i}, (a_i + 1) q^{-d_i})$$

with $a_i, d_i \in \mathbb{Z}$, $d_i \geq 0$, $0 \leq a_i < q^{d_i}$ for $1 \leq i \leq s$, and with J having s-dimensional volume q^{t-m}. Then any such interval J contains exactly q^t points of the digital net. The proof of this fact can be found, for instance, in [2, Section 4.4.2]. From this point of view, it is again clear that we are interested in small values of t, because then the family of intervals J for which the above equidistribution property holds becomes larger.

Our starting point for the construction of new digital nets is the suggestion made in [7, Remark 6.3] to view the row vectors of the generating matrices as elements of the finite field $\mathbb{F}_{q^m}$ (which is isomorphic to $\mathbb{F}_q^m$ as an $\mathbb{F}_q$-linear space). Thus, we consider elements $\gamma_j^{(i)} \in \mathbb{F}_{q^m}$, $1 \leq i \leq s$, $1 \leq j \leq m$, and the jth row of $C^{(i)}$ is then obtained as $\mathbf{c}_j^{(i)} = \phi(\gamma_j^{(i)})$, where $\phi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ is a fixed vector space isomorphism (or, equivalently, $\mathbf{c}_j^{(i)}$ is the coordinate vector of $\gamma_j^{(i)}$ relative to a fixed ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$). Again following [7, Remark 6.3], we arrange the $\gamma_j^{(i)}$ into an $s \times m$ matrix $C = (\gamma_j^{(i)})_{1 \leq i \leq s,\, 1 \leq j \leq m}$ over $\mathbb{F}_{q^m}$, and we then have a single matrix that governs the construction of the digital net. Because of the vector space isomorphism between $\mathbb{F}_{q^m}$ and $\mathbb{F}_q^m$, the following observation is an immediate consequence of Definition 1.1.

LEMMA 1.3. *The digital net obtained from* $C = (\gamma_j^{(i)})_{1\le i\le s,\,1\le j\le m}$ *over* $\mathbb{F}_{q^m}$ *is a digital* (t,m,s)*-net over* $\mathbb{F}_q$ *if and only if, for any integers* $d_1,\dots,d_s \ge 0$ *with* $\sum_{i=1}^s d_i = m-t$, *the* $m-t$ *elements* $\gamma_j^{(i)} \in \mathbb{F}_{q^m}$ *with* $1\le j\le d_i$ *and* $1\le i\le s$ *are linearly independent over* $\mathbb{F}_q$.

It is of apparent interest to consider a matrix C that is structured. In this paper, we analyze what happens when we choose a matrix C that has a Vandermonde-type structure. Concretely, we choose an s-tuple $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_s)\in\mathbb{F}_{q^m}^s$ and then we set up the $s\times m$ matrix $C=(\gamma_j^{(i)})_{1\le i\le s,\,1\le j\le m}$ over $\mathbb{F}_{q^m}$ defined by $\gamma_j^{(1)} = \alpha_1^{j-1}$ for $1\le j\le m$ and (if $s\ge 2$) $\gamma_j^{(i)} = \alpha_i^j$ for $2\le i\le s$ and $1\le j\le m$. We use the standard convention $0^0 = 1\in\mathbb{F}_q$. For obvious reasons, we call the digital net obtained from C a *Vandermonde net over* $\mathbb{F}_q$.

REMARK 1.4. If $s\ge 2$, then for $2\le i\le s$ we do not want to put $\gamma_j^{(i)} = \alpha_i^{j-1}$ for $1\le j\le m$, since otherwise the elements $\gamma_1^{(1)} = 1\in\mathbb{F}_q$ and $\gamma_1^{(2)} = 1\in\mathbb{F}_q$ are linearly dependent over $\mathbb{F}_q$, and so the least value of t such that the resulting digital net is a digital (t,m,s)-net over $\mathbb{F}_q$ is $t=m-1$.

REMARK 1.5. A broad class of digital nets, namely that of hyperplane nets, was introduced in [9] (see also [2, Chapter 11]). Choose $\alpha_1,\dots,\alpha_s$ in $\mathbb{F}_{q^m}$ not all 0. Then for the corresponding hyperplane net relative to a fixed ordered basis $\omega_1,\dots,\omega_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the matrix $C=(\gamma_j^{(i)})_{1\le i\le s,\,1\le j\le m}$ in Lemma 1.3 is given by $\gamma_j^{(i)} = \alpha_i\omega_j$ for $1\le i\le s$ and $1\le j\le m$ (see [2, Theorem 11.5] and [7, Remark 6.4]). Thus, C is also a structured matrix, but the structure is in general not a Vandermonde structure. Consequently, Vandermonde nets are in general not hyperplane nets relative to a fixed ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

In this paper, we discuss various aspects of Vandermonde nets. Section 2 ensures the existence of Vandermonde nets having small quality parameter, and as a by-product the existence of such nets satisfying good discrepancy bounds. This by-product is improved in Section 3 by using averaging arguments. Section 4 presents an explicit construction of Vandermonde nets over $\mathbb{F}_q$ in dimensions $s\le q+1$ with best possible quality parameter. Finally, Section 5 breaks the first ground for component-by-component constructions of Vandermonde nets.

2. Existence results for a small quality parameter. For the investigation of the quality parameter of a Vandermonde net over $\mathbb{F}_q$, we make use of the following notation and conventions. We write $\mathbb{F}_q[x]$ for the ring of polynomials over $\mathbb{F}_q$ in the indeterminate x. For any integer $m \geq 1$, we put

$$H_{q,m} := \{h \in \mathbb{F}_q[x] : \deg(h) \leq m,\, h(0) = 0\},$$
$$H^*_{q,m} := \{h \in \mathbb{F}_q[x] : \deg(h) < m\},$$

where $\deg(0) := 0$. Furthermore, we define $\deg^*(h) := \deg(h)$ for $h \in \mathbb{F}_q[x]$ with $h \neq 0$ and $\deg^*(0) := -1$. We write $\boldsymbol{h} := (h_1, \ldots, h_s) \in \mathbb{F}_q[x]^s$ for a given dimension $s \geq 1$. Finally, for any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{F}^s_{q^m}$, we put

$$D_{q,m,\boldsymbol{\alpha}} := \Big\{\boldsymbol{h} \in H^*_{q,m} \times H^{s-1}_{q,m} : \sum_{i=1}^{s} h_i(\alpha_i) = 0\Big\}$$

and $D'_{q,m,\boldsymbol{\alpha}} := D_{q,m,\boldsymbol{\alpha}} \setminus \{\mathbf{0}\}$.

We define the following figure of merit. We use the standard convention that an empty sum is equal to 0.

Definition 2.1. If $D'_{q,m,\boldsymbol{\alpha}}$ is nonempty, we define the *figure of merit*

$$\varrho(\boldsymbol{\alpha}) := \min_{\boldsymbol{h} \in D'_{q,m,\boldsymbol{\alpha}}} \Big(\deg^*(h_1) + \sum_{i=2}^{s} \deg(h_i)\Big).$$

Otherwise, we define $\varrho(\boldsymbol{\alpha}) := m$.

It is trivial that we always have $\varrho(\boldsymbol{\alpha}) \geq 0$. For $s = 1$ it is clear that $\varrho(\boldsymbol{\alpha}) \leq m$. For $s \geq 2$ the $m + 1$ elements $1, \alpha_1, \ldots, \alpha_1^{m-1}, \alpha_2 \in \mathbb{F}_{q^m}$ are linearly dependent over $\mathbb{F}_q$, and so again $\varrho(\boldsymbol{\alpha}) \leq m$.

Theorem 2.2. *Let q be a prime power, $s, m \in \mathbb{N}$, and let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ be in $\mathbb{F}^s_{q^m}$. Then the Vandermonde net determined by $\boldsymbol{\alpha} \in \mathbb{F}^s_{q^m}$ is a digital (t, m, s)-net over $\mathbb{F}_q$ with $t = m - \varrho(\boldsymbol{\alpha})$.*

Proof. The case $\varrho(\boldsymbol{\alpha}) = 0$ is trivial by the parenthetical remark in Definition 1.1, and so we can assume that $\varrho(\boldsymbol{\alpha}) \geq 1$. In view of Lemma 1.3, it suffices to show that for any integers $d_1, \ldots, d_s \geq 0$ with $\sum_{i=1}^{s} d_i = \varrho(\boldsymbol{\alpha})$, the elements α_1^j for $0 \leq j \leq d_1 - 1$ and α_i^j for $1 \leq j \leq d_i$, $2 \leq i \leq s$, are linearly independent over $\mathbb{F}_q$. A purported nontrivial linear dependence relation for these elements can be written in the form

$$\sum_{i=1}^{s} h_i(\alpha_i) = 0,$$

with a nonzero s-tuple $\boldsymbol{h} = (h_1, \ldots, h_s) \in H^*_{q,m} \times H^{s-1}_{q,m}$ satisfying $\deg^*(h_1) < d_1$ and $\deg(h_i) \leq d_i$ for $2 \leq i \leq s$. It follows that

$$\deg^*(h_1) + \sum_{i=2}^{s} \deg(h_i) < \sum_{i=1}^{s} d_i = \varrho(\boldsymbol{\alpha}).$$

But since $\boldsymbol{h} \in D'_{q,m,\boldsymbol{\alpha}}$, this contradicts the definition of $\varrho(\boldsymbol{\alpha})$. ∎

Remark 2.3. It is of interest to compare Vandermonde nets with the polynomial lattice point sets introduced in [5] (see also [2, Chapter 10], [6, Section 4.4], and the recent survey article [8] for the theory of polynomial lattice point sets). We consider polynomial lattice point sets with a modulus $f \in \mathbb{F}_q[x]$ which is irreducible over $\mathbb{F}_q$ of degree m. An s-dimensional polynomial lattice point set depends also on the choice of polynomials $g_1, \ldots, g_s \in H^*_{q,m}$. One arrives at a digital (t, m, s)-net over $\mathbb{F}_q$ with a quality parameter t depending on a figure of merit analogous to $\varrho(\boldsymbol{\alpha})$ in Definition 2.1. The crucial condition $\sum_{i=1}^{s} h_i(\alpha_i) = 0$ in the definition of $D_{q,m,\boldsymbol{\alpha}}$ above is now replaced by

$$\sum_{i=1}^{s} h_i g_i \equiv 0 \pmod{f}. \tag{2.1}$$

Let $\theta \in \mathbb{F}_{q^m}$ be a root of f. Then each $\alpha_i \in \mathbb{F}_{q^m}$ in the definition of a Vandermonde (t, m, s)-net over $\mathbb{F}_q$ can be written as $\alpha_i = f_i(\theta)$ with a unique $f_i \in H^*_{q,m}$. Thus, we arrive at the condition $0 = \sum_{i=1}^{s} h_i(\alpha_i) = \sum_{i=1}^{s} h_i(f_i(\theta))$ in the definition of $D_{q,m,\boldsymbol{\alpha}}$, which is equivalent to

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

This is similar to (2.1), but with the products $h_i g_i$ replaced by the compositions $h_i \circ f_i$. We note that polynomial lattice point sets belong to the family of hyperplane nets (see [2, Theorem 11.7]), and so Vandermonde nets are in general not polynomial lattice point sets (see Remark 1.5).

Remark 2.4. Since polynomial lattice point sets are available also for a reducible modulus $f \in \mathbb{F}_q[x]$ (see [2, Definition 10.1]), we may extend the definition of Vandermonde nets in an analogous way. For an arbitrary (and thus not necessarily irreducible) $f \in \mathbb{F}_q[x]$ with $\deg(f) = m \geq 1$, we consider the residue class ring $\mathbb{F}_q[x]/(f)$. Given a dimension $s \geq 1$, we choose $g_1, \ldots, g_s \in H^*_{q,m}$. Note that $\mathbb{F}_q[x]/(f)$ is a vector space over $\mathbb{F}_q$, with the canonical ordered basis B given by the residue classes of the monomials $1, x, \ldots, x^{m-1}$ modulo f. Now we construct a digital net over $\mathbb{F}_q$ with generating matrices $C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{m \times m}$ as follows. For $1 \leq j \leq m$, the jth row vector of $C^{(1)}$ is given by the coordinate vector of the residue class of g_1^{j-1} modulo f relative to the ordered basis B. If $s \geq 2$, then for $2 \leq i \leq s$ and $1 \leq j \leq m$, the jth row vector of $C^{(i)}$ is given by the coordinate vector of the residue class of g_i^j modulo f relative to the ordered basis B. We leave the theory of these more general Vandermonde nets for future work. As for polynomial lattice point sets, the theory of general Vandermonde nets will be significantly more complicated for reducible moduli f.

Now we establish existence results for Vandermonde (t, m, s)-nets over $\mathbb{F}_q$ with a small quality parameter t. We use an elimination method which is inspired by a similar method for polynomial lattice point sets (see [4, Section 3] and [2, Section 10.1]). We first show a simple enumeration result.

Lemma 2.5. *For a prime power q, for $l \in \mathbb{N}$ and $n \in \mathbb{Z}$, the number $A_q(l, n)$ of $(h_1, \dots, h_l) \in \mathbb{F}_q[x]^l$ with $h_i \neq 0$ and $h_i(0) = 0$ for $1 \leq i \leq l$ and $\sum_{i=1}^{l} \deg(h_i) = n$ is given by*

$$A_q(l, n) = \binom{n-1}{n-l}(q-1)^l q^{n-l},$$

where we use the convention for binomial coefficients that $\binom{m}{k} = 0$ whenever $k > m$ or $k < 0$.

Proof. Note that $h_i \neq 0$ and $h_i(0) = 0$ imply $\deg(h_i) \geq 1$, and so trivially $A_q(l, n) = 0$ for $n < l$. For $n \geq l$, we count the number of l-tuples $(d_1, \dots, d_l) \in \mathbb{N}^l$ such that $\sum_{i=1}^{l} d_i = n$, or equivalently the number of l-tuples $(d_1 - 1, \dots, d_l - 1) \in \mathbb{N}_0^l$ such that $\sum_{i=1}^{l}(d_i - 1) = n - l$. The latter number of l-tuples is given by $\binom{n-1}{n-l}$. For each $(d_1, \dots, d_l) \in \mathbb{N}^l$ with $\sum_{i=1}^{l} d_i = n$, there are $(q-1)^l q^{d_1 - 1} \cdots q^{d_l - 1} = (q-1)^l q^{n-l}$ different $(h_1, \dots, h_l) \in \mathbb{F}_q[x]^l$ satisfying $h_i(0) = 0$ and $\deg(h_i) = d_i$ for $1 \leq i \leq l$, and the result follows. ∎

Next we estimate the number $M_q(m, s, \sigma)$ of $(\alpha_1, \dots, \alpha_s) \in \mathbb{F}_{q^m}^s$ such that $\sum_{i=1}^{s} h_i(\alpha_i) = 0$ for at least one nonzero s-tuple $(h_1, \dots, h_s) \in H_{q,m}^* \times H_{q,m}^{s-1}$ satisfying

$$\deg^*(h_1) + \sum_{i=2}^{s} \deg(h_i) \leq \sigma. \tag{2.2}$$

We assume that $\sigma \in \mathbb{Z}$ and $0 \leq \sigma \leq m - 1$. We have

$$M_q(m, s, \sigma) \leq M_q^{(1)}(m, s, \sigma) + M_q^{(2)}(m, s, \sigma), \tag{2.3}$$

where $M_q^{(1)}(m, s, \sigma)$, respectively $M_q^{(2)}(m, s, \sigma)$, is the number of $(\alpha_1, \dots, \alpha_s) \in \mathbb{F}_{q^m}^s$ such that $\sum_{i=1}^{s} h_i(\alpha_i) = 0$ for at least one nonzero s-tuple $(h_1, \dots, h_s) \in H_{q,m}^* \times H_{q,m}^{s-1}$ with $h_1 = 0$, respectively $h_1 \neq 0$, satisfying (2.2).

We first consider $M_q^{(1)}(m, s, \sigma)$. Initially, we fix the number d of zero entries in a nonzero s-tuple $(0, h_2, \dots, h_s) \in H_{q,m}^* \times H_{q,m}^{s-1}$. Note that $1 \leq d \leq s - 1$ and that (2.2) yields

$$s - d \leq \sum_{i=2}^{s} \deg(h_i) =: n \leq \sigma + 1.$$

There exists an index $j \in \{2, \dots, s\}$ such that $1 \leq \deg(h_j) \leq \lfloor n/(s-d) \rfloor$. Then for each of the $q^{m(s-1)}$ choices of $(\alpha_1, \dots, \alpha_{j-1}, \alpha_{j+1}, \dots, \alpha_s) \in \mathbb{F}_{q^m}^{s-1}$, there are at most $\lfloor n/(s-d) \rfloor$ choices of $\alpha_j \in \mathbb{F}_{q^m}$ such that

$$h_j(\alpha_j) = -\sum_{\substack{i=1\\ i\neq j}}^{s} h_i(\alpha_i). \tag{2.4}$$

There are $\binom{s-1}{d-1}$ choices for the positions of the zero entries in $(0, h_2, \ldots, h_s)$, and for each such choice there are $A_q(s-d, n)$ choices for the $s-d$ nonzero entries. Using Lemma 2.5, we arrive at the bound

$$\begin{aligned} &M_q^{(1)}(m,s,\sigma) \\ &\quad \le \sum_{d=1}^{s-1} \binom{s-1}{d-1} \sum_{n=s-d}^{\sigma+1} \binom{n-1}{n-s+d} (q-1)^{s-d} q^{n-s+d} q^{m(s-1)} \left\lfloor \frac{n}{s-d} \right\rfloor. \end{aligned}$$

The estimation of $M_q^{(2)}(m,s,\sigma)$ proceeds in a similar way. Let d be the number of zero entries in an s-tuple $(h_1, \ldots, h_s) \in H_{q,m}^* \times H_{q,m}^{s-1}$ with $h_1 \neq 0$. Then $0 \le d \le s-1$ and

$$s - d - 1 \le \sum_{i=1}^{s} \deg(h_i) =: n \le \sigma.$$

There exists an index $j \in \{1, \ldots, s\}$ with $h_j \neq 0$ and $\deg(h_j) \le \lfloor n/(s-d) \rfloor$. As above, each choice of $(\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_s) \in \mathbb{F}_{q^m}^{s-1}$ leaves at most $\lfloor n/(s-d) \rfloor$ choices of $\alpha_j \in \mathbb{F}_{q^m}$ satisfying (2.4). Since $h_1 \neq 0$, there are $\binom{s-1}{d}$ choices for the positions of the zero entries in $(h_1, \ldots, h_s)$, and for each such choice there are $A_q(s-d, n+1)$ choices for the $s-d$ nonzero entries (replace $h_1(x)$ by $xh_1(x)$ in order to arrive at the counting problem in Lemma 2.5). Using Lemma 2.5, we obtain

$$\begin{aligned} &M_q^{(2)}(m,s,\sigma) \\ &\le \sum_{d=0}^{s-1} \binom{s-1}{d} \sum_{n=s-d-1}^{\sigma} \binom{n}{n+1-s+d} (q-1)^{s-d} q^{n+1-s+d} q^{m(s-1)} \left\lfloor \frac{n}{s-d} \right\rfloor \\ &\le \sum_{d=0}^{s-1} \binom{s-1}{d} \sum_{n=s-d}^{\sigma+1} \binom{n-1}{n-s+d} (q-1)^{s-d} q^{n-s+d} q^{m(s-1)} \left\lfloor \frac{n}{s-d} \right\rfloor. \end{aligned}$$

Now we use (2.3) and $\binom{s-1}{d-1} + \binom{s-1}{d} = \binom{s}{d}$ for $0 \le d \le s-1$, and this yields

$$\begin{aligned} M_q(m,s,\sigma) &\le \sum_{d=0}^{s-1} \binom{s}{d} \sum_{n=s-d}^{\sigma+1} \binom{n-1}{n-s+d} (q-1)^{s-d} q^{n-s+d} q^{m(s-1)} \left\lfloor \frac{n}{s-d} \right\rfloor \\ &= q^{m(s-1)} \sum_{d=0}^{s-1} \binom{s}{d} (q-1)^{s-d} \sum_{n=0}^{\sigma-s+d+1} \binom{n+s-d-1}{n} \left\lfloor \frac{n+s-d}{s-d} \right\rfloor q^n. \end{aligned}$$

We define

$$\Delta_q(s,\sigma) := \sum_{d=0}^{s-1} \binom{s}{d} (q-1)^{s-d} \sum_{n=0}^{\sigma-s+d} \binom{n+s-d-1}{n} \left\lfloor \frac{n+s-d}{s-d} \right\rfloor q^n.$$

Now we come to the crucial step: if $\Delta_q(s,\sigma+1) < q^m$ and therefore $M_q(m,s,\sigma) < q^{ms}$, then it follows that there exists at least one $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_s) \in \mathbb{F}_{q^m}^s$ such that $\sum_{i=1}^s h_i(\alpha_i) \neq 0$ for every nonzero s-tuple $(h_1,\dots,h_s) \in H_{q,m}^* \times H_{q,m}^{s-1}$ satisfying (2.2). Hence, for such $\boldsymbol{\alpha}$, the figure of merit $\varrho(\boldsymbol{\alpha})$ satisfies $\varrho(\boldsymbol{\alpha}) \geq \sigma+1$. From Theorem 2.2 we deduce that the corresponding Vandermonde net satisfies $t \leq m-\sigma-1$. We have thus shown the following theorem.

THEOREM 2.6. *Let q be a prime power and let $s,m \in \mathbb{N}$. If $\Delta_q(s,\sigma) < q^m$ for some $\sigma \in \mathbb{N}$ with $\sigma \leq m$, then there exists an $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ with $\varrho(\boldsymbol{\alpha}) \geq \sigma$. This $\boldsymbol{\alpha}$ generates a Vandermonde (t,m,s)-net over $\mathbb{F}_q$ with $t \leq m-\sigma$.*

COROLLARY 2.7. *Let q be a prime power and let $s,m \in \mathbb{N}$. Then there exists an $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ with*

$$\varrho(\boldsymbol{\alpha}) \geq \lfloor m - s\log_q m - 3 \rfloor,$$

where $\log_q$ denotes the logarithm to the base q.

Proof. For $s=1$ we can achieve $\varrho(\boldsymbol{\alpha}) = \varrho((\alpha_1)) = m$ by choosing $\alpha_1 \in \mathbb{F}_{q^m}$ as a root of an irreducible polynomial over $\mathbb{F}_q$ of degree m. If $s \geq 2$, it suffices to prove by Theorem 2.6 that for

$$\sigma_1 := \lfloor m - s\log_q m - 3 \rfloor$$

we have $\Delta_q(s,\sigma_1) < q^m$. We can assume that $\sigma_1 \geq 1$, for otherwise the result is trivial. In the following, we derive a general upper bound on $\Delta_q(s,\sigma)$ for $\sigma \geq 1$ and then in a second step we use the specific form of σ_1. First of all, we have

$$\begin{aligned}
\Delta_q(s,\sigma) &\leq \sum_{d=0}^{s-1} \binom{s}{d} \left\lfloor \frac{\sigma}{s-d} \right\rfloor (q-1)^{s-d} \sum_{n=0}^{\sigma-s+d} \binom{n+s-d-1}{s-d-1} q^n \\
&\leq \sum_{d=0}^{s-1} \binom{s}{d} \frac{\sigma}{s-d} (q-1)^{s-d-1} \binom{\sigma-1}{s-d-1} q^{\sigma-s+d+1} \\
&\leq q^{\sigma-s+1} \sum_{d=0}^{s-1} \binom{s}{d} \frac{\sigma}{s-d} (q-1)^{s-d-1} \frac{(\sigma-1)^{s-d-1}}{(s-d-1)!} q^d \\
&= s\sigma q^{\sigma-s+1} \sum_{d=0}^{s-1} \binom{s-1}{d} \frac{1}{(s-d)\cdot(s-d)!} [(q-1)(\sigma-1)]^{s-d-1} q^d.
\end{aligned}$$

Now $(k+1)\cdot(k+1)! \ge 4^k$ for $k \ge 0$, and so $(s-d)\cdot(s-d)! \ge 4^{s-d-1}$ for $d = 0,1,\dots,s-1$. It follows that

$$\begin{aligned}\Delta_q(s,\sigma) &\le s\sigma q^{\sigma-s+1}\sum_{d=0}^{s-1}\binom{s-1}{d}\left[\frac{q-1}{4}(\sigma-1)\right]^{s-d-1} q^d\\ &= s\sigma q^{\sigma-s+1}\left(\frac{q-1}{4}(\sigma-1)+q\right)^{s-1} = s\sigma q^{\sigma}\left(\frac{q-1}{4q}(\sigma-1)+1\right)^{s-1},\end{aligned}$$

and so

$$\Delta_q(s,\sigma) \le s\sigma q^{\sigma}\left(\frac{\sigma+3}{4}\right)^{s-1} \quad \text{for } \sigma \ge 1.$$

Now we use $s \ge 2$ and the special form of σ_1 to obtain

$$\Delta_q(s,\sigma_1) < \sigma_1 q^{\sigma_1}(\sigma_1+3)^{s-1} < mq^m m^{-s} m^{s-1} = q^m,$$

and this yields the desired result. ∎

We recall the definition of the *star discrepancy* D_N^* of any N points $\mathbf{y}_1,\dots,\mathbf{y}_N \in [0,1)^s$, namely

$$D_N^* = \sup_J \left|\frac{Z(J)}{N} - \lambda_s(J)\right|,$$

where the supremum is extended over all subintervals J of $[0,1)^s$ with one vertex at the origin, where $Z(J)$ is the number of integers n with $1 \le n \le N$ and $\mathbf{y}_n \in J$, and where λ_s denotes the s-dimensional Lebesgue measure. Point sets with small star discrepancy are crucial ingredients of quasi-Monte Carlo methods for numerical integration (see [2, Chapter 2]).

Using the well-known star discrepancy bound for (t,m,s)-nets in base q (see [6, Theorem 4.10]) together with Theorem 2.2 and Corollary 2.7, we arrive at the following result.

Corollary 2.8. *Let q be a prime power and let $s,m \in \mathbb{N}$. Then there exists an $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ such that the star discrepancy of the corresponding Vandermonde net satisfies*

$$D_N^* = O_{q,s}(N^{-1}(\log N)^{2s-1}),$$

where $N = q^m$.

3. Further existence results for small discrepancy. Throughout this section, we assume that q is a prime, that $\mathbb{F}_q$ is identified with $\mathbb{Z}_q$, and that $\psi : \mathbb{F}_q \to \mathbb{Z}_q$ is the identity map. Then we know from [2, Theorem 5.34] that the star discrepancy of a digital net generated by $C^{(1)},\dots,C^{(s)} \in \mathbb{F}_q^{m\times m}$ satisfies

$$D_{q^m}^* \le 1 - \left(1 - \frac{1}{q^m}\right)^s + R_q(C^{(1)},\dots,C^{(s)}), \tag{3.1}$$

where

$$R_q(C^{(1)},\dots,C^{(s)}) := \sum_{(\mathbf{k}_1,\dots,\mathbf{k}_s)\in F'} \rho_q^{(s)}(\mathbf{k}_1,\dots,\mathbf{k}_s)$$

with

$$F' = \{(\mathbf{k}_1,\dots,\mathbf{k}_s) : \mathbf{k}_1 C^{(1)} + \cdots + \mathbf{k}_s C^{(s)} = \mathbf{0}\} \setminus \{\mathbf{0}\}.$$

Here $\mathbf{k}_i \in \mathbb{F}_q^m$ for $1 \le i \le s$. Furthermore $\rho_q^{(s)}(\mathbf{k}_1,\dots,\mathbf{k}_s) := \prod_{i=1}^s \rho_q(\mathbf{k}_i)$, where for $\mathbf{k} = (k_1,\dots,k_m) \in \mathbb{F}_q^m$ we put

$$\rho_q(\mathbf{k}) := \begin{cases} 1 & \text{if } \mathbf{k} = \mathbf{0}, \\ \dfrac{1}{q^r \sin(\pi k_r/q)} & \text{if } \mathbf{k} = (k_1,\dots,k_r,0,\dots,0),\ k_r \ne 0. \end{cases}$$

Lemma 3.1. *Let $C^{(1)},\dots,C^{(s)} \in \mathbb{F}_q^{m\times m}$ be the generating matrices of the Vandermonde net corresponding to $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_s) \in \mathbb{F}_{q^m}^s$. Then*

$$R_q(\boldsymbol{\alpha}) := R_q(C^{(1)},\dots,C^{(s)}) = \sum_{\boldsymbol{h}\in D'_{q,m,\boldsymbol{\alpha}}} \rho_q^{(s)}(\boldsymbol{h}),$$

where for $\boldsymbol{h} \in H_{q,m}^* \times H_{q,m}^{s-1}$ we put $\rho_q^{(s)}(\boldsymbol{h}) = \rho_q(xh_1(x))\rho_q(h_2)\cdots\rho_q(h_s)$. Here for $h \in H_{q,m}$ we define

$$\rho_q(h) = \begin{cases} 1 & \text{if } h = 0, \\ \dfrac{1}{q^r \sin(\pi k_r/q)} & \text{if } h = k_1 x + \cdots + k_r x^r,\ k_r \ne 0. \end{cases}$$

Proof. This follows immediately from the form of the generating matrices $C^{(1)},\dots,C^{(s)}$ of a Vandermonde net and from the definition of $D'_{q,m,\boldsymbol{\alpha}}$. ∎

Lemma 3.2. *For every prime q and every $v, m \in \mathbb{N}$, we have*

$$\sum_{h\in H_{q,m}} \rho_q(h) \le \begin{cases} m/2 + 1 & \text{if } q = 2, \\ ((2/\pi)\log q + 2/5)m + 1 & \text{if } q > 2, \end{cases}$$

and

$$\sum_{\boldsymbol{h}\in H_{q,m}^*\times H_{q,m}^{v-1}} \rho_q^{(v)}(\boldsymbol{h}) \le \begin{cases} (m/2+1)^v & \text{if } q = 2, \\ (((2/\pi)\log q + 2/5)m + 1)^v & \text{if } q > 2. \end{cases}$$

Proof. This follows from the proof of [6, Lemma 3.13]. ∎

Theorem 3.3. *Let q be a prime and let $s, m \in \mathbb{N}$. Then there exists an $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ such that the star discrepancy of the corresponding Vandermonde net satisfies*

$$D_{q^m}^* < 1 - \left(1 - \frac{1}{q^m}\right)^s + \frac{m}{q^m} \begin{cases} (m/2+1)^s & \text{if } q = 2, \\ (((2/\pi)\log q + 2/5)m + 1)^s & \text{if } q > 2. \end{cases}$$

Proof. We consider the average $M_{s,q,m}$ of $R_q(\boldsymbol{\alpha})$ over all $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$, that is,

$$\begin{aligned} M_{s,q,m} &= \frac{1}{q^{ms}} \sum_{\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s} R_q(\boldsymbol{\alpha}) \\ &= \frac{1}{q^{ms}} \sum_{\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s} \sum_{\boldsymbol{h} \in D'_{q,m,\boldsymbol{\alpha}}} \rho_q^{(s)}(\boldsymbol{h}) \\ &= \frac{1}{q^{ms}} \sum_{\boldsymbol{h} \in (H_{q,m}^* \times H_{q,m}^{s-1}) \setminus \{\boldsymbol{0}\}} A(\boldsymbol{h}) \rho_q^{(s)}(\boldsymbol{h}), \end{aligned}$$

where $A(\boldsymbol{h})$ is the number of $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{F}_{q^m}^s$ such that $\sum_{i=1}^s h_i(\alpha_i) = 0$. Now for every $\boldsymbol{h} \in (H_{q,m}^* \times H_{q,m}^{s-1}) \setminus \{\boldsymbol{0}\}$, $A(\boldsymbol{h})$ is at most $mq^{m(s-1)}$. Hence

$$M_{s,q,m} \le \frac{m}{q^m} \sum_{\boldsymbol{h} \in (H_{q,m}^* \times H_{q,m}^{s-1}) \setminus \{\boldsymbol{0}\}} \rho_q^{(s)}(\boldsymbol{h}) < \frac{m}{q^m} \sum_{\boldsymbol{h} \in H_{q,m}^* \times H_{q,m}^{s-1}} \rho_q^{(s)}(\boldsymbol{h}).$$

The last sum can be bounded using Lemma 3.2. The result of the theorem follows now from (3.1). ∎

In terms of the number $N = q^m$ of points, the bound on the star discrepancy D_N^* in Theorem 3.3 is of the form $D_N^* = O_s(N^{-1}(\log N)^{s+1})$.

4. An explicit construction. In this section, q is again an arbitrary prime power. For any dimension s with $1 \le s \le q+1$ and any integer $m \ge 2$, we construct a Vandermonde (t, m, s)-net over $\mathbb{F}_q$ with the least possible quality parameter $t = 0$. It is well known (see [6, Corollary 4.21]) that for $m \ge 2$, a $(0, m, s)$-net in base q cannot exist for $s \ge q+2$, and so our construction is best possible in terms of the dimension s.

Let $\theta \in \mathbb{F}_{q^m}$ be a root of an irreducible polynomial over $\mathbb{F}_q$ of degree $m \ge 2$. In the construction of Vandermonde nets in Section 1, we put $\alpha_1 = \theta$ and (if $s \ge 2$) $\alpha_i = (\theta + c_i)^{-1}$ for $i = 2, \ldots, s$, where $c_2, \ldots, c_s$ are distinct elements of $\mathbb{F}_q$. Note that $\theta + c_i \ne 0$ for $2 \le i \le s$ since $\theta \notin \mathbb{F}_q$. Furthermore, the condition $s \le q+1$ guarantees that we can find $s-1$ distinct elements $c_2, \ldots, c_s \in \mathbb{F}_q$.

THEOREM 4.1. *Let q be a prime power and let $s, m \in \mathbb{N}$ with $s \le q+1$ and $m \ge 2$. Then the construction above yields a Vandermonde (t, m, s)-net over $\mathbb{F}_q$ with $t = 0$.*

Proof. We proceed by Lemma 1.3. The case $s = 1$ is trivial by the definition of θ, and so we can assume that $s \ge 2$. For any integers $d_1, \ldots, d_s \ge 0$

with $\sum_{i=1}^{s} d_i = m$, we show that the m elements θ^j, $0 \le j \le d_1 - 1$, and $(\theta + c_i)^{-j}$ for $1 \le j \le d_i$ and $2 \le i \le s$ are linearly independent over $\mathbb{F}_q$. Consider a linear dependence relation

$$\sum_{j=0}^{d_1-1} e_{1j}\theta^j + \sum_{i=2}^{s}\sum_{j=1}^{d_i} e_{ij}(\theta + c_i)^{-j} = 0$$

with all $e_{1j}, e_{ij} \in \mathbb{F}_q$. Multiply by $\prod_{k=2}^{s}(\theta + c_k)^{d_k}$ and put

$$p_1(x) = \sum_{j=0}^{d_1-1} e_{1j}x^j \in \mathbb{F}_q[x] \quad \text{and} \quad p_i(x) = \sum_{j=1}^{d_i} e_{ij}(x + c_i)^{d_i - j} \in \mathbb{F}_q[x]$$

for $2 \le i \le s$. Then

$$p_1(\theta)\prod_{k=2}^{s}(\theta + c_k)^{d_k} + \sum_{i=2}^{s} p_i(\theta)\prod_{\substack{k=2\\k\ne i}}^{s}(\theta + c_k)^{d_k} = 0. \tag{4.1}$$

Assume that for some integer r with $2 \le r \le s$ we have $p_r(x) \ne 0$. Then $d_r \ge 1$ and $\deg(p_r(x)) < d_r$. On the left-hand side of (4.1) we have a polynomial in θ of degree $< \sum_{i=1}^{s} d_i = m$, and so this polynomial is the zero polynomial. Thus, we get the polynomial identity

$$p_1(x)\prod_{k=2}^{s}(x + c_k)^{d_k} + \sum_{i=2}^{s} p_i(x)\prod_{\substack{k=2\\k\ne i}}^{s}(x + c_k)^{d_k} = 0 \tag{4.2}$$

in $\mathbb{F}_q[x]$. By considering this identity modulo $(x + c_r)^{d_r}$, we obtain

$$p_r(x)\prod_{\substack{k=2\\k\ne r}}^{s}(x + c_k)^{d_k} \equiv 0 \pmod{(x + c_r)^{d_r}}.$$

The product over k on the left-hand side is coprime to the modulus, and so it follows that $(x + c_r)^{d_r}$ divides $p_r(x)$. But $\deg(p_r(x)) < d_r$, thus we arrive at a contradiction. Therefore $p_i(x) = 0$ for $2 \le i \le s$, and so (4.2) shows that $p_1(x) = 0$. Hence all coefficients $e_{1j}, e_{ij} \in \mathbb{F}_q$ in the original linear dependence relation are equal to 0. ∎

The fact that we can explicitly construct optimal Vandermonde (t, m, s)-nets over $\mathbb{F}_q$ for all dimensions $s \le q + 1$ represents an advantage over polynomial lattice point sets (see Remark 2.3 for the latter point sets). Explicit constructions of good polynomial lattice point sets are known only for $s = 1$ and $s = 2$ (see [2, p. 305]), whereas for $s \ge 3$ one has to resort to search algorithms in order to obtain good s-dimensional polynomial lattice point sets.

5. Component-by-component constructions. As in Section 3 we assume that q is a prime, that $\mathbb{F}_q$ is identified with $\mathbb{Z}_q$, and that $\psi : \mathbb{F}_q \to \mathbb{Z}_q$ is the identity map. Therefore the discrepancy bound in (3.1) as well as Lemmas 3.1 and 3.2 are valid. In the following, we introduce two component-by-component search algorithms for good Vandermonde nets in arbitrarily high dimensions, in the spirit of the search algorithms introduced in [3] and [10] for good lattice point sets and in [1] for good polynomial lattice point sets.

ALGORITHM 5.1. Given a prime q and $s, m \in \mathbb{N}$.

1. Choose $\alpha_1 \in \mathbb{F}_{q^m}$ as a root of an irreducible polynomial over $\mathbb{F}_q$ of degree m.
2. For $d \in \mathbb{N}$ with $2 \le d \le s$, assume that we have already constructed $\alpha_1, \ldots, \alpha_{d-1} \in \mathbb{F}_{q^m}$. We find $\alpha_d \in \mathbb{F}_{q^m}$ that minimizes the quantity

$$R_q((\alpha_1, \ldots, \alpha_{d-1}, \alpha_d))$$

as a function of α_d.

THEOREM 5.2. *Let q be a prime and let $s, m \in \mathbb{N}$. Suppose that $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ is constructed according to Algorithm* 5.1. *Then for all $d \in \mathbb{N}$ with $1 \le d \le s$ we have*

$$R_q((\alpha_1, \ldots, \alpha_d)) \le \frac{m}{q^m} \begin{cases} (m/2 + 1)^d & \text{if } q = 2, \\ (((2/\pi)\log q + 2/5)m + 1)^d & \text{if } q > 2. \end{cases}$$

Proof. The proof is carried out by induction on d. For $d = 1$ we have

$$R_q((\alpha_1)) = \sum_{h \in D'_{q,m,(\alpha_1)}} \rho_q(h) = 0,$$

since $D'_{q,m,(\alpha_1)}$ is an empty set (note that $\alpha_1 \in \mathbb{F}_{q^m}$ is a root of an irreducible polynomial over $\mathbb{F}_q$ of degree m and therefore not a root of a nonzero polynomial $h \in H^*_{q,m}$).

Suppose now that for some $1 \le d < s$, we have already constructed $(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}^d_{q^m}$ and the bounds in the theorem hold. Then consider $(\alpha_1, \ldots, \alpha_d, \alpha_{d+1})$. We have

$$\begin{aligned} R_q((\alpha_1, \ldots, \alpha_d, \alpha_{d+1})) &= \sum_{(\boldsymbol{h}, h_{d+1}) \in D'_{q,m,(\alpha_1,\ldots,\alpha_d,\alpha_{d+1})}} \rho_q^{(d)}(\boldsymbol{h}) \rho_q(h_{d+1}) \\ &= \sum_{\boldsymbol{h} \in D'_{q,m,(\alpha_1,\ldots,\alpha_d)}} \rho_q^{(d)}(\boldsymbol{h}) + \theta(\alpha_{d+1}) \\ &= R_q((\alpha_1, \ldots, \alpha_d)) + \theta(\alpha_{d+1}), \end{aligned}$$

where we split off the terms with $h_{d+1} = 0$ and where

$$\theta(\alpha_{d+1}) = \sum_{h_{d+1} \in H_{q,m} \setminus \{0\}} \rho_q(h_{d+1}) \sum_{\substack{\boldsymbol{h} \in H^*_{q,m} \times H^{d-1}_{q,m} \\ (\boldsymbol{h}, h_{d+1}) \in D'_{q,m,(\alpha_1,\ldots,\alpha_d,\alpha_{d+1})}}} \rho_q^{(d)}(\boldsymbol{h}).$$

Note that α_{d+1} is a minimizer of $R_q((\alpha_1,\ldots,\alpha_d,\cdot))$ and the only dependence on α_{d+1} is in θ. Therefore α_{d+1} is a minimizer of θ. We obtain

$$\begin{aligned}
\theta(\alpha_{d+1}) &\le \frac{1}{q^m} \sum_{\beta \in \mathbb{F}_{q^m}} \theta(\beta) \\
&= \frac{1}{q^m} \sum_{\beta \in \mathbb{F}_{q^m}} \sum_{h_{d+1} \in H_{q,m} \setminus \{0\}} \rho_q(h_{d+1}) \sum_{\substack{\boldsymbol{h} \in H^*_{q,m} \times H^{d-1}_{q,m} \\ (\boldsymbol{h}, h_{d+1}) \in D'_{q,m,(\alpha_1,\ldots,\alpha_d,\beta)}}} \rho_q^{(d)}(\boldsymbol{h}) \\
&= \frac{1}{q^m} \sum_{h_{d+1} \in H_{q,m} \setminus \{0\}} \rho_q(h_{d+1}) \sum_{\boldsymbol{h} \in H^*_{q,m} \times H^{d-1}_{q,m}} \rho_q^{(d)}(\boldsymbol{h}) \sum_{\substack{\beta \in \mathbb{F}_{q^m} \\ (\boldsymbol{h}, h_{d+1}) \in D'_{q,m,(\alpha_1,\ldots,\alpha_d,\beta)}}} 1.
\end{aligned}$$

The condition $(\boldsymbol{h}, h_{d+1}) \in D'_{q,m,(\alpha_1,\ldots,\alpha_d,\beta)}$ is equivalent to the equation

$$h_{d+1}(\beta) = -\sum_{i=1}^{d} h_i(\alpha_i).$$

Since $h_{d+1} \in H_{q,m} \setminus \{0\}$, this equation has at most m different solutions $\beta \in \mathbb{F}_{q^m}$. Altogether we arrive at the bound

$$\begin{aligned}
R_q((\alpha_1,\ldots,\alpha_d,\alpha_{d+1})) &\le R_q((\alpha_1,\ldots,\alpha_d)) \\
&\quad + \frac{m}{q^m} \sum_{h_{d+1} \in H_{q,m} \setminus \{0\}} \rho_q(h_{d+1}) \sum_{\boldsymbol{h} \in H^*_{q,m} \times H^{d-1}_{q,m}} \rho_q^{(d)}(\boldsymbol{h}).
\end{aligned}$$

The proof is completed by using the induction hypothesis and Lemma 3.2. ∎

Theorem 5.2 ensures that Algorithm 5.1 produces vectors $\boldsymbol{\alpha} \in \mathbb{F}^s_{q^m}$ whose existence was guaranteed by Theorem 3.3 in Section 3. But Algorithm 5.1 does not make use of the explicit construction in Section 4 for low dimensions. The following algorithm suggests as initial values the explicitly constructed $\alpha_1,\ldots,\alpha_{q+1}$ of Section 4 for a component-by-component procedure.

Algorithm 5.3. Given are a prime q and $s, m \in \mathbb{N}$ with $s > q+1$ and $m \ge 2$.

1. Choose $\alpha_1,\ldots,\alpha_{q+1} \in \mathbb{F}_{q^m}$ as in the explicit construction of Section 4.

2. For $d \in \mathbb{N}$ with $q+2 \leq d \leq s$, assume that we have already constructed $\alpha_1, \ldots, \alpha_{d-1} \in \mathbb{F}_{q^m}$. We find $\alpha_d \in \mathbb{F}_{q^m}$ that minimizes the quantity $R_q((\alpha_1, \ldots, \alpha_{d-1}, \alpha_d))$ as a function of α_d.

Although Algorithm 5.3 starts from an (in the quality parameter point of view) optimal vector in $\mathbb{F}_{q^m}^{q+1}$, one cannot be certain that the algorithm is competitive with Algorithm 5.1. A straightforward generalization of the proof of Theorem 5.2 would involve an upper bound for $R_q(C^{(1)}, \ldots, C^{(q+1)})$, where $C^{(1)}, \ldots, C^{(q+1)}$ are the generating matrices of a $(0, m, q+1)$-net over $\mathbb{F}_q$. However, the known bound for $R_q(C^{(1)}, \ldots, C^{(q+1)})$ in [6, Theorem 4.34] is not strong enough for all settings. Unfortunately, particularly for large values of q, one will obtain a weaker bound than in Theorem 5.2. It will be an interesting project for the future to implement Algorithms 5.1 and 5.3 and compare their performance.

Acknowledgments. R. Hofer was partially supported by the Austrian Science Foundation (FWF), Projects P21943 and P24302. Furthermore, she would like to thank Peter Hellekalek and the University of Salzburg, where part of this paper was written, for their great hospitality during the research visit.

References

[1] 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.

[2] J. Dick and F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge Univ. Press, Cambridge, 2010.

[3] N. M. Korobov, *Number-Theoretic Methods in Approximate Analysis*, Fizmatgiz, Moscow, 1963 (in Russian).

[4] G. Larcher, A. Lauss, H. Niederreiter, and W. Ch. Schmid, *Optimal polynomials for (t, m, s)-nets and numerical integration of multivariate Walsh series*, SIAM J. Numer. Anal. 33 (1996), 2239–2253.

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

[6] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Reg. Conf. Ser. Appl. Math. 63, SIAM, Philadelphia, PA, 1992.

[7] H. Niederreiter, *Finite fields and quasirandom points*, in: Finite Fields and Their Applications: Character Sums and Polynomials, P. Charpin et al. (eds.), de Gruyter, Berlin, 2013, 169–196.

[8] F. Pillichshammer, *Polynomial lattice point sets*, in: Monte Carlo and Quasi-Monte Carlo Methods 2010, L. Plaskota and H. Woźniakowski (eds.), Springer, Berlin, 2012, 189–210.

[9] G. Pirsic, J. Dick, and F. Pillichshammer, *Cyclic digital nets, hyperplane nets, and multivariate integration in Sobolev spaces*, SIAM J. Numer. Anal. 44 (2006), 385–411.

[10] I. H. Sloan and A. V. Reztsov, *Component-by-component construction of good lattice rules*, Math. Comp. 71 (2002), 263–273.

Roswitha Hofer
Institute of Financial Mathematics
Johannes Kepler University Linz
Altenbergerstr. 69
A-4040 Linz, Austria
E-mail: roswitha.hofer@jku.at

Harald Niederreiter
Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz, Austria
and
Department of Mathematics
University of Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg, Austria
E-mail: ghnied@gmail.com

Received on 6.8.2013 (7546)