Uniform Distribution Theory **4** (2009), no.1, 69–79

uniform distribution theory

THE QUALITY PARAMETER OF CYCLIC NETS AND HYPERPLANE NETS

Friedrich Pillichshammer — Gottlieb Pirsic

ABSTRACT. The class of so-called hyperplane nets is one of the most general sub-classes of digital (t, m, s)-nets over a finite field. In this paper a figure of merit is studied with which one can determine the net parameter t of hyperplane nets. Furthermore, existence of such digital nets of good quality is proved.

Communicated by Pierre Liardet

1. Introduction

Quasi-Monte Carlo algorithms for numerical integration approximate the integral of a function over the (often high-dimensional) unit-cube by the average of function evaluations over a well-chosen deterministic point set. Here an appropriate choice of the underlying point set becomes increasingly more important as the dimension of the problem grows. It has been shown that point sets chosen from the unit-cube having a very uniform distribution yield small integration errors, at least for functions with bounded variation in the sense of Hardy and Krause (see [7]).

Currently the best constructions of well distributed finite point sets are based on the concept of (t, m, s)-nets in base b as introduced by Niederreiter [5] (see also [7, Chapter 4] for a survey of this theory).

Definition 1 ((t, m, s)-nets)**.** Let $b \geq 2$, $s \geq 1$ and $0 \leq t \leq m$ be integers. A point set $\mathcal{P}$ consisting of b^m points in $[0, 1)^s$ forms a (t, m, s)-net in base b, if every subinterval of the form $J = \prod_{i=1}^{s} [a_i b^{-d_i}, (a_i + 1)b^{-d_i})$ of $[0, 1)^s$, with

2000 Mathematics Subject Classification: 11K31, 11K38.
Keywords: Digital nets, finite field, hyperplane nets.
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".

integers $d_i \geq 0$ and integers $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ and of volume b^{t-m}, contains exactly b^t points of $\mathcal{P}$.

Note that for any point set of b^m points there always exists a $t \in \{0, \ldots, m\}$ such that it is a (t, m, s)-net in base b, e.g., we can always choose $t = m$. Smaller values of t imply stronger equidistribution properties for nets (for example in terms of star discrepancy, see [7, Theorem 4.10]). With regard to this fact, t is often called the *quality parameter* of the net.

Concrete constructions of (t, m, s)-nets are based on the digital construction scheme which we recall in the following. To avoid too many technical notions, and since we only deal with this case, in the following we restrict ourselves to digital nets defined over the finite field $\mathbb{F}_q$ of prime-power order q. For a more general definition (over arbitrary finite, commutative rings) see for example Niederreiter [7], Larcher [2], or Larcher, Niederreiter and Schmid [4].

From now on 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

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

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 $s \geq 1$ and $m \geq 1$ 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 $1 \leq i \leq s$ and for $k \in \mathbb{Z}_{q^m}$ multiply the matrix C_i by the vector $\varphi(k)$, i.e.,

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

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 $0 \leq t \leq m$ the point set consisting of the points

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

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*.

Definition 3 (figure of merit ρ)**.** Let $C_1, \ldots, C_s$ be the generator matrices of a digital net over $\mathbb{F}_q$ and let $\mathcal{C} = \{\boldsymbol{c}_j^{(i)} \in \mathbb{F}_q^m : 1 \leq j \leq m, 1 \leq i \leq s\}$ be the system of the row vectors of these matrices ($\boldsymbol{c}_j^{(i)}$ is the j-th row vector of matrix

C_i, $1 \le j \le m$, $1 \le i \le s$). Let $\rho(\mathcal{C})$ be the largest integer d such that any system $\{\boldsymbol{c}_j^{(i)} \in \mathbb{F}_q^m \,:\, 1 \le j \le d_i,\, 1 \le i \le s\}$ with $0 \le d_i \le m$ for $1 \le i \le s$ and $\sum_{i=1}^{s} d_i = d$ is linearly independent in $\mathbb{F}_q^m$ (the empty system is viewed as linearly independent).

It was shown by Niederreiter [7, Theorem 4.28] that a digital net with generator matrices $C_1, \ldots, C_s$ is a digital (t, m, s)-net over $\mathbb{F}_q$ with

$$t = m - \rho(\mathcal{C}). \tag{2}$$

Hence the quality parameter t only depends on the generator matrices of a digital net. For an effective method to establish the quality parameter from given matrices $C_1, \ldots, C_s$ we refer to [16].

Many constructions of digital nets are inspired by a close connection between coding theory and the theory of digital nets (see, for example, Niederreiter [8] or [9]). Examples for that are the so-called $(u, u+v)$-construction (see [1, 11]), the matrix-product construction (see [10]) and the Kronecker-product construction (see [1, 12]). 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 [8] 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 [15] to so-called hyperplane nets whose definition will be given now.

Definition 4 (hyperplane nets)**.** Let integers $m \ge 1, s \ge 2$ and a prime-power q be given. Let $\mathbb{F}_{q^m}$ be a finite field with q^m elements and fix an element $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)^\top \in \mathbb{F}_{q^m}^s$, $\boldsymbol{\alpha} \ne \mathbf{0}$. Let $\mathcal{F}$ be the space of linear forms

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

and consider the subset

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

For each $1 \le i \le s$ choose an ordered basis $\mathcal{B}_i$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and define the mapping $\phi : \mathcal{F} \to \mathbb{F}_q^{ms}$ 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 $\mathcal{N}_{\boldsymbol{\alpha}} := \phi(\mathcal{F}_{\boldsymbol{\alpha}})$. Let

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

be a matrix whose row space is $\mathcal{C}_{\boldsymbol{\alpha}}$. Then $C_1, \ldots, C_s$ are the generating matrices of 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 to $\boldsymbol{\alpha}$. 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.

Remark 1. In Definition 4 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 [8]. This cyclic net will be denoted by $\mathcal{P}_\alpha$ and we say $\mathcal{P}_\alpha$ is the *cyclic net associated to* α.

Remark 2. Another construction of digital nets goes by the name of *polynomial lattices* which have been introduced by Niederreiter [6] (see also [7]). It has been shown by Pirsic [14] that polynomial lattices appear as special cases of hyperplane nets when we choose the ordered basis $\mathcal{B}_1, \ldots, \mathcal{B}_s$ all equal to $\{1, \omega, \ldots, \omega^{m-1}\}$ if $\mathbb{F}_{q^m} = \mathbb{F}_q[\omega]$.

Further examples in [14] 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 sub-classes, e.g., constant bases $\mathcal{B}_i = \mathcal{B}_1$ or with a triangular structure.

In this paper we introduce a figure of merit for hyperplane nets which allows to express the quality parameter t in terms of $\boldsymbol{\alpha}$. Based on this figure of merit we will show the existence of $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ which yields hyperplane nets and cyclic nets of good quality with respect to the quality parameter t respectively the star discrepancy. Similar results are already known for the proper sub-class of polynomial lattices (see [3, 17]). We point out that our results are valid for the much more general class of hyperplane nets.

2. Preliminary results

We use the definitions of q, $\mathbb{F}_q$, $\mathbb{Z}_r$, φ_1 and φ from Section 1.

Let $\mathbb{F}_{q^m} = \mathbb{F}_q[\omega]$ be such that $\{1, \omega, \ldots, \omega^{m-1}\}$ forms a basis of $\mathbb{F}_{q^m}$ as vector space over $\mathbb{F}_q$. Let $\omega^m = \beta_0 + \cdots + \beta_{m-1}\omega^{m-1}$ where $\beta_0, \ldots, \beta_{m-1} \in \mathbb{F}_q$ and let

P be the companion matrix of ω, i.e.,

$$P := \begin{pmatrix} 0 & 0 & 0 & \cdots & \beta_0 \\ 1 & 0 & 0 & \cdots & \beta_1 \\ 0 & 1 & 0 & \cdots & \beta_2 \\ & & \cdots\cdots\cdots\cdots & & \\ 0 & \cdots & 0 & 1 & \beta_{m-1} \end{pmatrix} \in \mathbb{F}_q^{m\times m}.$$

Now, if we have the representation of α in $\mathbb{F}_{q^m}$ as $\alpha = \sum_{l=0}^{m-1} a_l\omega^l$, where $a_0,\ldots,a_{m-1} \in \mathbb{F}_q$, then we define

$$\psi(\alpha) := (a_0,\ldots,a_{m-1})^\top \in \mathbb{F}_q^m \quad \text{and} \quad \Psi(\alpha) := \sum_{l=0}^{m-1} a_l P^l \in \mathbb{F}_q^{m\times m}.$$

With these definitions for any $\alpha,\beta \in \mathbb{F}_{q^m}$ we have

$$\psi(\alpha\beta) = \Psi(\alpha)\psi(\beta).$$

This follows by first showing the identity for α and β equal to powers of ω and then using linearity.

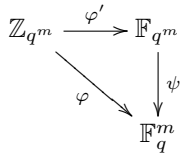
Note that for any $\alpha,\beta \in \mathbb{F}_{q^m}^* := \mathbb{F}_{q^m} \setminus \{0\}$ we have $\Psi(\alpha)\psi(\beta) = \psi(\alpha\beta) \neq \mathbf{0} \in \mathbb{F}_q^m$ as $\alpha\beta \neq 0 \in \mathbb{F}_{q^m}$. Hence it follows that for any $\alpha \in \mathbb{F}_{q^m}^*$ the matrix $\Psi(\alpha)$ is regular.

Furthermore, for $k = \sum_{l=0}^{m-1} \kappa_l q^l \in \mathbb{Z}_{q^m}$ and a bijection $\varphi_1 : \mathbb{Z}_q \to \mathbb{F}_q$ let

$$\varphi'(k) := \sum_{l=0}^{m-1} \varphi_1(\kappa_l)\omega^l.$$

Observe that $\varphi(k) = \psi(\varphi'(k))$ if φ is defined as in (1).

The above definition can be summarized in the following commutative diagram:



Remark 3. Let $m, s, \mathbb{F}_q$ and $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}$, $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_s)^\top$, be given as above and define s matrices $B_i = (\psi(b_{i,1}),\ldots,\psi(b_{i,m}))$, where the $b_{i,1},\ldots,b_{i,s}$ constitute the chosen basis $\mathcal{B}_i$ for $1 \le i \le s$. Then (see [15]) the matrices $C_i = (\Psi(\alpha_i)B_i)^\top$ for $1 \le i \le s$ can be chosen for generator matrices of the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$. Furthermore it follows that C_i is regular whenever $\alpha_i \neq 0$.

For hyperplane nets we can express the associated dual space in terms of $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$. The following lemma has been given implicitly already in [15, Lemma 2.5]. In view of Remark 2 this lemma corresponds to [7, Lemma 4.40].

Lemma 1. *Let the $m \times m$ matrices $C_1, \ldots, C_s$ be the generator matrices of a hyperplane net over $\mathbb{F}_q$ as given in Remark 3. Then for any integers $k_1, \ldots, k_s \in \mathbb{Z}_{q^m}$ we have*

$$C_1^\top \varphi(k_1) + \cdots + C_s^\top \varphi(k_s) = \mathbf{0} \in \mathbb{F}_q^m \tag{3}$$

if and only if

$$\alpha_1 \varphi'(\tau_1(k_1)) + \cdots + \alpha_s \varphi'(\tau_s(k_s)) = 0 \in \mathbb{F}_{q^m} \tag{4}$$

with permutations $\tau_i(k) = \varphi^{-1}(B_i \varphi(k))$, and B_i as in Remark 3 for all $1 \le i \le s$.

P r o o f. By Remark 3 we have

$$\begin{aligned} \mathbf{0} &= \sum_{i=1}^s C_i^\top \varphi(k_i) = \sum_{i=1}^s \Psi(\alpha_i) B_i \varphi(k_i) \\ &= \sum_{i=1}^s \Psi(\alpha_i) \varphi(\tau_i(k_i)) = \sum_{i=1}^s \psi(\alpha_i \varphi'(\tau_i(k_i))) = \psi\Big(\sum_{i=1}^s \alpha_i \varphi'(\tau_i(k_i)) \Big), \end{aligned}$$

and this holds if and only if $\sum_{i=1}^s \alpha_i \varphi'(\tau_i(k_i)) = 0$. □

3. The quality parameter of hyperplane nets

For polynomial lattices there exists a so-called figure of merit [7, Definition 4.39] which is based on the associated dual space and with which one can express the quality parameter t of a polynomial lattice considered as digital net, see [7, Theorem 4.42]. These ideas can be transferred to the more general concept of hyperplane nets.

Definition 5. For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)^\top \in \mathbb{F}_{q^m}^s$ the figure of merit $\rho(\boldsymbol{\alpha})$ is defined as

$$\rho(\boldsymbol{\alpha}) = s - 1 + \min \sum_{i=1}^s \lfloor \log_q(k_i) \rfloor,$$

where the minimum is extended over all $k_1, \ldots, k_s \in \mathbb{Z}_{q^m}$, not all zero, such that $\alpha_1 \varphi'(\tau_1(k_1)) + \cdots + \alpha_s \varphi'(\tau_s(k_s)) = 0 \in \mathbb{F}_{q^m}$. Here $\log_q$ denotes the logarithm to base q and we use the convention $\lfloor \log_q(0) \rfloor := -1$.

With this figure of merit at hand we may now give a formula for the quality parameter t of a hyperplane net.

Theorem 1. *The hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$ associated to $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ is a digital (t, m, s)-net over $\mathbb{F}_q$ with $t = m - \rho(\boldsymbol{\alpha})$.*

Proof. Let $\boldsymbol{c}_j^{(i)}$ be the j-th row vector of the i-th generator matrix C_i of the hyperplane net. Then by (2), $t = m - \rho(\mathcal{C}) =: m - \rho_1$, where $\rho_1 + 1$ is the smallest integer such that there exist $d_1, \ldots, d_s \in \mathbb{N}_0$ with $\sum_{i=1}^s d_i = \rho_1 + 1$ and $\lambda_{i,j} \in \mathbb{F}_q$, $1 \le i \le s$, $1 \le j \le m$ such that

$$\sum_{i=1}^{s} \sum_{j=1}^{d_i} \lambda_{i,j} \boldsymbol{c}_j^{(i)} = 0. \tag{5}$$

Equivalently, by the isomorphism φ, the integer $\rho_1 + 1$ is minimal such that there exist $k_i \in \mathbb{Z}_{q^m}$, $i = 1, \ldots, s$ such that (3) holds, where $k_i = \sum_{j=1}^m \nu_{i,j} q^{j-1}$, with

$$\rho_1 + 1 = \sum_{i=1}^{s} d_i := \sum_{i=1}^{s} \max\{j : \nu_{i,j} \neq 0\} = \sum_{i=1}^{s} \lfloor \log_q(k_i) + 1 \rfloor$$

(choose $k_i = \varphi^{-1}((\lambda_{i,1}, \ldots, \lambda_{i,m})^\top)$ with the $\lambda_{i,j}$ from above).

Finally, by Lemma 1

$$\begin{aligned} &\min \left\{ \sum_{i=1}^{s} \lfloor \log_q(k_i) + 1 \rfloor : \ (3) \text{ holds} \right\} \\ &= \quad \min \left\{ \sum_{i=1}^{s} \lfloor \log_q(k_i) + 1 \rfloor : \ (4) \text{ holds} \right\} = \rho(\boldsymbol{\alpha}) + 1, \end{aligned}$$

so that putting everything together

$$t = m - \rho(\mathcal{C}) = m - \left(\min \left\{ \sum_{i=1}^{s} d_i : \ (5) \text{ holds} \right\} - 1 \right) = m - \rho(\boldsymbol{\alpha})$$

as required. □

From the definition of the figure of merit $\rho(\boldsymbol{\alpha})$ and from Theorem 1 we see that it is sufficient to consider vectors $\boldsymbol{\alpha}$ of the form $\boldsymbol{\alpha} = (1, \alpha_2, \ldots, \alpha_s)^\top$ only, where 1 denotes the neutral element with respect to multiplication in $\mathbb{F}_q$. The following result is the analogon of [3, Theorem 1] and [17, Theorem 6] for the much more general class of hyperplane nets.

Theorem 2. *Let $s \geq 2$, $m \geq 1$ and let q be a prime-power. Choose ordered bases $\mathcal{B}_1, \ldots, \mathcal{B}_s$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For $\rho \in \mathbb{Z}$ define*

$$\Delta_q(s,\rho) = \sum_{d=0}^{s-1} \binom{s}{d} (q-1)^{s-d} \sum_{\gamma=0}^{\rho+d} \binom{s-d+\gamma-1}{\gamma} q^{\gamma} + 1 - q^{\rho+s}.$$

1. *If $\Delta_q(s,\rho) < q^m$, then there exists an $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ of the form $\boldsymbol{\alpha} = (1, \alpha_2, \ldots, \alpha_s)^\top$ with $\rho(\boldsymbol{\alpha}) \geq s + \rho$. Therefore the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$ is a digital (t,m,s)-net over $\mathbb{F}_q$ with $t \leq m - s - \rho$.*
2. *If $\Delta_q(s,\rho) < \frac{q^m}{s-1}$, then there exists an element $\alpha \in \mathbb{F}_{q^m}$ such that $\boldsymbol{\alpha} = (1, \alpha, \ldots, \alpha^{s-1})^\top$ satisfies $\rho(\boldsymbol{\alpha}) \geq s + \rho$. Therefore the cyclic net $\mathcal{P}_\alpha$ is a digital (t,m,s)-net over $\mathbb{F}_q$ with $t \leq m - s - \rho$.*

The proof of Theorem 2 is nearly the same as that of [3, Theorem 1]. However, to see the differences we present the proof of the first part of Theorem 2. First of all we need the following result.

Lemma 2. *Let q be a prime-power and let l, k be integers with $l \geq 1$. Then the number $A_q(l,k)$ of $(h_1, \ldots, h_l)^\top \in (\mathbb{Z}_{q^m}^*)^l$ such that $\sum_{i=1}^{l} \lfloor \log_q(h_i) \rfloor \leq k$ is given by*

$$A_q(l,k) = (q-1)^l \sum_{\gamma=0}^{k} \binom{l+\gamma-1}{\gamma} q^{\gamma}.$$

Proof. We have $A_q(l,k) = \sum_{\gamma=0}^{k} D_q(l,\gamma)$ where $D_q(l,\gamma)$ denotes the number of $(h_1, \ldots, h_l)^\top \in (\mathbb{Z}_{q^m}^*)^l$ such that $\sum_{i=1}^{l} \lfloor \log_q(h_i) \rfloor = \gamma$. Now for $\gamma \geq 0$ there are $\binom{l+\gamma-1}{\gamma}$ l-tuples $(d_1, \ldots, d_l)$ with integers $d_i \geq 0$ for $1 \leq i \leq l$ and $\sum_{i=1}^{l} d_i = \gamma$. For each such l-tuple $(d_1, \ldots, d_l)$ there are $(q-1)^l q^{d_1 + \cdots + d_l} = (q-1)^l q^{\gamma}$ elements $(h_1, \ldots, h_l)^\top \in (\mathbb{Z}_{q^m}^*)^l$ such that $\lfloor \log_q(h_i) \rfloor = d_i$ for $1 \leq i \leq l$. The result follows. □

We give the proof of Theorem 2.

Proof. Let $M_q(s,\rho)$ be the number of $(k_1, \ldots, k_s)^\top \in \mathbb{Z}_{q^m}^s$ with $(k_2, \ldots, k_s) \neq (0, \ldots, 0)$ and $\sum_{i=1}^{s} \lfloor \log_q(k_i) \rfloor \leq \rho$. Using the notation and the result of Lemma 2, we get

$$M_q(s,\rho) = \sum_{d=0}^{s-1} \binom{s}{d} A_q(s-d, \rho+d) + 1 - q^{\rho+s} = \Delta_q(s,\rho).$$

(Recall the convention that $\lfloor \log_q(0) \rfloor = -1$.)

For a given nonzero element $(k_1,\dots,k_s)^\top \in \mathbb{Z}_{q^m}^s$ the equation $\varphi'(\tau_1(k_1)) + \alpha_2\varphi'(\tau_2(k_2)) + \cdots + \alpha_s\varphi'(\tau_s(k_s)) = 0$ has no solution if $k_2 = \cdots = k_s = 0$ (note that $\varphi(\tau_i(0)) = 0$ for all $1 \le i \le s$), and it has exactly $q^{m(s-2)}$ solutions $\boldsymbol{\alpha} = (1,\alpha_2,\dots,\alpha_s)^\top \in \mathbb{F}_{q^m}^s$ otherwise (note that $\varphi' \circ \tau_i$ are bijections for all $1 \le i \le s$). Therefore, to all nonzero $(k_1,\dots,k_s)^\top$ with $\sum_{i=1}^s \lfloor \log_q(k_i) \rfloor \le \rho$ there are assigned altogether at most $M_q(s,\rho)q^{m(s-2)}$ different solutions $\boldsymbol{\alpha} = (1,\alpha_2,\dots,\alpha_s)^\top \in \mathbb{F}_{q^m}^s$ of the above equation. Now the total number of $\boldsymbol{\alpha} = (1,\alpha_2,\dots,\alpha_s)^\top \in \mathbb{F}_{q^m}^s$ is $q^{m(s-1)}$. Thus, if $M_q(s,\rho)q^{m(s-2)} < q^{m(s-1)}$, that is, if $\Delta_q(s,\rho) < q^m$, then there exists at least one $\boldsymbol{\alpha} = (1,\alpha_2,\dots,\alpha_s)^\top \in \mathbb{F}_{q^m}^s$ such that $\varphi'(\tau_1(k_1)) + \alpha_2\varphi'(\tau_2(k_2)) + \cdots + \alpha_s\varphi'(\tau_s(k_s)) \ne 0$ for all nonzero $(k_1,\dots,k_s)^\top \in \mathbb{Z}_{q^m}^s$ with $\sum_{i=1}^s \lfloor \log_q(k_i) \rfloor \le \rho$. For this $\boldsymbol{\alpha}$ we have then $\rho(\boldsymbol{\alpha}) \ge s + \rho$. By Theorem 1 the point set $\mathcal{P}_{\boldsymbol{\alpha}}$ is a digital (t,m,s)-net over $\mathbb{F}_q$ with $t \le m - s - \rho$. □

The proof of the following corollary is identical to the one of [3, Corollary 1].

Corollary 1. *Let $s \ge 2$ be an integer, let q be a prime-power and let m be a sufficiently large integer.*

1. *There exists a vector $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ with*
$$\rho(\boldsymbol{\alpha}) \ge \lfloor m - (s-1)(\log_q m - 1) + \log_q(s-1)! \rfloor.$$
2. *There exists an element $\alpha \in \mathbb{F}_{q^m}$ such that $\boldsymbol{\alpha} = (1,\alpha,\dots,\alpha^{s-1})^\top$ satisfies*
$$\rho(\boldsymbol{\alpha}) \ge \lfloor m - (s-1)(\log_q m - 1) + \log_q(s-2)! \rfloor.$$

The following result on the star discrepancy of hyperplane nets and cyclic nets can be obtained from Corollary 1 in combination with [7, Theorem 4.10].

Corollary 2. *Let $s \ge 2$ be an integer, let q be a prime-power and let m be a sufficiently large integer.*

1. *There exists a vector $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^s$ such that the star discrepancy of the hyperplane net $\mathcal{P}_{\boldsymbol{\alpha}}$ satisfies*
$$D_{q^m}^*(\mathcal{P}_{\boldsymbol{\alpha}}) = O(m^{2s-2}q^{-m})$$
with an implied constant only depending on q and s.
2. *There exists an element $\alpha \in \mathbb{F}_{q^m}$ such that the star discrepancy of the cyclic net $\mathcal{P}_\alpha$ satisfies*
$$D_{q^m}^*(\mathcal{P}_\alpha) = O(m^{2s-2}q^{-m})$$
with an implied constant only depending on q and s.

More detailed results on the discrepancy of hyperplane nets can be found in the paper [13].

Acknowledgement. The authors are grateful to the anonymous referee for urging us to more clarity in the presentation and pointing out a flaw in our original definition.

REFERENCES

[1] BIERBRAUER, J. – EDEL, Y. – SCHMID, W. CH.: *Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays*, J. Combin. Des. **10** (2002), 403–418,

[2] LARCHER, G.: *Digital point sets: analysis and application*, in: *Random and Quasi-Random Point Sets*, Lecture Notes in Statistic **138**, Springer, New York, 1998, pp. 167–222.

[3] LARCHER, G. – LAUSS, A. – NIEDERREITER, H. – SCHMID, W. CH.: *Optimal polynomials for (t, m, s)-nets and numerical integration of multivariate Walsh series*, SIAM J. Numer. Anal. **33** (1996), 2239–2253.

[4] LARCHER, G. – NIEDERREITER, H. – SCHMID, W.CH.: *Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration*, Monatsh. Math. **121** (1996), 231–253.

[5] NIEDERREITER, H.: *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273–337.

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

[7] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*, *CBMS-NSF Series in Applied Mathematics* **63** SIAM, Philadelphia, 1992.

[8] NIEDERREITER, H.: *Digital nets and coding theory*, in: *Coding, Cryptography and Combinatorics*, Birkhäuser, Basel, 2004, pp. 247–257.

[9] NIEDERREITER, H.: *Nets, (t, s)-sequences and codes*, in: *Monte Carlo and Quasi-Monte Carlo Methods 2006*, Springer, Berlin, 2008, pp. 83–100.

[10] NIEDERREITER, H. – ÖZBUDAK, F.: *Matrix-product constructions of digital nets*, Finite Fields Appl. **10** (2004), 464–479.

[11] NIEDERREITER, H. – PIRSIC, G.: *Duality for digital nets and its applications*, Acta Arith., **97** (2002), 173–182.

[12] NIEDERREITER, H. – PIRSIC, G.: *A Kronecker product construction for digital nets*, in: *Monte Carlo and Quasi-Monte Carlo Methods 2000*, Springer, Berlin, 2002, pp. 396–405.

[13] PILLICHSHAMMER, F. – PIRSIC, G.: *Discrepancy of hyperplane nets and cyclic nets*, in: *Monte Carlo and Quasi-Monte Carlo Methods 2008*, Springer, Berlin (to appear).

[14] PIRSIC, G.: *A small taxonomy of integration node sets*, Österreich. Akad. Wiss. Math.-Natur. Kl., Sitzungsber. Abt. II, **214** (2005) 133–140.
[15] PIRSIC, G. – DICK, J. – PILLICHSHAMMER, F.: *Cyclic digital nets, hyperplane nets, and multivariate integration in Sobolev spaces*, SIAM J. Numer. Anal. **44** (2006), 385–411.
[16] PIRSIC, G. – SCHMID, W. CH.: *Calculation of the quality parameter of digital nets and application to their construction*, J. Complexity **17** (2001), 827–839.
[17] SCHMID, W. CH.: *Improvements and extensions of the "Salzburg tables" by using irreducible polynomials*, in: *Monte Carlo and quasi-Monte Carlo methods 1998*, Springer, Berlin, 2000, pp. 436–447.

Received July 2, 2008
Accepted May 23, 2009

Friedrich Pillichshammer
Gottlieb Pirsic
Institut für Finanzmathematik
Universität Linz
Altenbergstraße 69
A-4040 Linz
AUSTRIA
E-mail: friedrich.pillichshammer@jku.at
gpirsic@gmail.com