ACTA ARITHMETICA
105.2 (2002)

Digital (t, m, s)-nets and the spectral test

by

Peter Hellekalek (Salzburg)

1. Introduction. The notion of a (t, m, s)-net to a given base b is a central concept of the modern theory of uniform distribution of sequences modulo one. It has been introduced by Niederreiter [11] in a highly successful attempt to unify and extend existing construction methods for low-discrepancy point sets. Such nets are of fundamental importance in the theory and practice of quasi-Monte Carlo methods.

The optimal choice for the quality parameter t is $t = 0$. Practical construction methods for (t, m, s)-nets are based upon the concept of a *digital* (t, m, s)*-net*. We refer the reader to the surveys Niederreiter [12] and Larcher [7] for further reading.

In this paper we will study the following question. Suppose that the dimension s is given. What will be the best possible uniform distribution of a (t, m, s)-net in base b on the s-dimensional torus $[0, 1[^s$? More precisely, for an appropriately chosen measure of uniform distribution, is it possible to give exact upper and lower bounds for (digital) (t, m, s)-nets?

We will employ the concept of the generalized spectral test introduced in Hellekalek [4] to find an answer for this question. Our results include an upper bound for the general case and lower bounds for digital (t, m, s)-nets in prime base b. All bounds are best possible.

Our method is based upon the exact computation of Weyl sums with respect to an appropriate Walsh function system and the application of elementary concepts of linear algebra.

In our proofs for strict digital (t, m, s)-nets in base b we use results for associated linear codes established in Niederreiter and Pirsic [14] and Skriganov [16]. Interestingly, duality comes into play with all applications of the spectral test: see the survey Hellekalek [5].

2000 *Mathematics Subject Classification*: 11K38, 11K45, 94B05.

Research supported by Austrian Science Fund (FWF), Project no. P8303-MAT, and Austrian National Bank, Project NB7576.

2. Preliminaries. Throughout this paper, if the integer b is a prime, we will identify the ring $\mathbb{Z}_b$ of residues modulo b with the finite field $\mathbb{F}_b$. We assume that the reader is familiar with the notion of arbitrary and digital (t, m, s)-nets. The monograph [12] and the survey papers [7, 15] contain comprehensive discussions of this topic. We refer to [2, 4] for details on the b-adic representation of real numbers and integers as well as elementary properties of the Walsh functions in base b.

Representation in base b. Let $b \geq 2$ be a fixed integer. Every number $x \in [0,1[$ may be represented in the form $x = \sum_{j=0}^{\infty} x_j b^{-j-1}$, with digits $x_j \in \{0, 1, \ldots, b-1\}$. We will assume that $x_j \neq b-1$ for infinitely many j, which implies uniqueness of the representation. The "digit vector" of x will be denoted by

$$\underline{x} = (x_0, x_1, \ldots).$$

In the same fashion, with any nonnegative integer k, $k = \sum_{j=0}^{\infty} k_j b^j$, with digits $k_j \in \{0, 1, \ldots, b-1\}$, we will associate the digit vector $\underline{k} = (k_0, k_1, \ldots)$. Throughout this paper, the zero vector $(0, 0, \ldots)$ will be denoted by $\mathbf{0}$.

If $\mathbf{k} = (k^{(1)}, \ldots, k^{(s)}) \in \mathbb{Z}^s$, each $k^{(i)} \geq 0$, then the associated digit vector is defined as

$$\underline{\mathbf{k}} = (\underline{k}^{(1)}, \ldots, \underline{k}^{(s)}).$$

Analogously, we define the digit vector that is associated with an element $\mathbf{x} = (x^{(1)}, \ldots, x^{(s)}) \in [0,1[^s$ as $\underline{\mathbf{x}} = (\underline{x}^{(1)}, \ldots, \underline{x}^{(s)})$. For $x \in [0,1[$ and $k \in \mathbb{Z}$, $k \geq 0$, we define

$$\underline{k} \cdot \underline{x} = \sum_{j=0}^{\infty} k_j x_j \pmod b.$$

This quantity is well defined because only finitely many digits k_j will be different from zero. We generalize this notion to dimension s in the obvious manner:

$$\underline{\mathbf{k}} \cdot \underline{\mathbf{x}} = \sum_{i=1}^{s} \underline{k}^{(i)} \cdot \underline{x}^{(i)} \pmod b,$$

where $\mathbf{k} = (k^{(1)}, \ldots, k^{(s)}) \in \mathbb{Z}^s$ and $\mathbf{x} = (x^{(1)}, \ldots, x^{(s)}) \in [0,1[^s$.

Walsh functions in base b. For $\mathbf{x} \in [0,1[^s$ and $\mathbf{k} \in \mathbb{Z}^s$ with all $k^{(i)} \geq 0$, we define the $\mathbf{k}$*th Walsh function* $w_{\mathbf{k}}$ in base b on the s-dimensional torus $[0,1[^s$ as follows. Let $e(z) = e^{2\pi i z/b}$ for $z \in \mathbb{Z}$. Then

$$w_{\mathbf{k}}(\mathbf{x}) = e(\underline{\mathbf{k}} \cdot \underline{\mathbf{x}}).$$

The reader will note that we have slightly abused the notion of an inner product of digit vectors. If $\underline{k}^{(i)}$ and $\underline{x}^{(i)}$ are not of the same length, then the missing digits in the b-adic representation are assumed to be filled up with zeros.

Weight functions. For a digit vector $\underline{k} = (k_0, k_1, \ldots)$ in base b with only finitely many digits k_j different from zero, let $v(\underline{k})$ denote the following *weight function*:

$$v(\underline{k}) = \begin{cases} 1 + \max\{j : k_j \neq 0\} & \text{if } \underline{k} \neq (0, 0, \ldots), \\ 0 & \text{otherwise.} \end{cases}$$

This type of weight function has been introduced in [14] and [16] (see also [10, pp. 158, 163] for a first, implicit version of this concept). We observe that the condition $b^g \leq k < b^{g+1}$, $g \geq 0$, for the integer k is equivalent to the condition $v(\underline{k}) = g + 1$ for the weight of its digit vector $\underline{k}$. The *weight* $V(\underline{\mathbf{k}})$ of a vector $\underline{\mathbf{k}} = (\underline{k}^{(1)}, \ldots, \underline{k}^{(s)})$ of digit vectors $\underline{k}^{(i)}$ is defined as

$$V(\underline{\mathbf{k}}) = \sum_{i=1}^{s} v(\underline{k}^{(i)}).$$

Weyl sums. For a sequence $\omega = (\mathbf{x}_n)_{n \geq 0}$ on the torus $[0, 1[^s$, and a Riemann-integrable function $f : [0, 1[^s \to \mathbb{C}$, let

$$S_N(f, \omega) = \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n) \tag{1}$$

denote the mean value of the function f with respect to the first N elements of ω. If $f = w_{\mathbf{k}}$ for some $\mathbf{k}$, then we speak of a *Weyl sum*.

Weyl's criterion. Weyl's criterion for the Walsh system (see [3, 4]) tells us that the uniform distribution modulo one of a sequence ω is equivalent to the condition

$$\lim_{N \to \infty} S_N(w_{\mathbf{k}}, \omega) = 0 \quad \forall \mathbf{k} \neq \mathbf{0}.$$

Spectral test. The *Walsh spectral test* defined below molds Weyl's criterion into a quantitative form, into a measure of the uniform distribution of sequences modulo one.

Definition 1. For an integer vector $\mathbf{k} = (k^{(1)}, \ldots, k^{(s)})$ with each $k^{(i)} \geq 0$, let $r(\mathbf{k}) = b^{V(\underline{\mathbf{k}})}$. For an arbitrary sequence $\omega = (\mathbf{x}_n)_{n \geq 0}$ in $[0, 1[^s$, the *Walsh spectral test* $\sigma_N(\omega)$ of the first N elements of ω is defined as the quantity

$$\sigma_N(\omega) = \sup_{\mathbf{k} \neq \mathbf{0}} \frac{|S_N(w_{\mathbf{k}}, \omega)|}{r(\mathbf{k})}. \tag{2}$$

Uniform distribution of the sequence ω is equivalent to the relation

$$\lim_{N \to \infty} \sigma_N(\omega) = 0$$

(see [4]).

Digital nets and codes. Let $\omega = (\mathbf{x}_n)_{n=0}^{b^m - 1}$ be a digital (t, m, s)-net in base b and let b be a prime number. Choosing fixed bijections from the set

of digits $\{0, 1, \ldots, b-1\}$ to the finite field $\mathbb{F}_b$, we may write $\underline{\mathbf{x}_n}$ in the form

$$\underline{\mathbf{x}_n} = (\underline{n}C_1, \underline{n}C_2, \ldots, \underline{n}C_s), \quad 0 \le n < b^m,$$

with some $m \times m$ matrices C_i over $\mathbb{F}_b$, $1 \le i \le s$. Hence, we may view the set $\underline{\omega} = \{\underline{\mathbf{x}_n}, 0 \le n < b^m\}$ as a linear subspace of the vector space $\mathbb{F}_b^{sm}$, in other words, as a linear code over $\mathbb{F}_b$. Let $\underline{\omega}^\perp$ denote its dual code. The definition of the weight functions v and V extends to $\mathbb{F}_b^m$ and $\mathbb{F}_b^{sm}$ in an obvious manner. We refer the reader to [14, 16] for details.

3. Results. In this section, we will show a general upper bound for the spectral test for arbitrary (t, m, s)-nets in base $b \ge 2$, b some fixed integer (see Theorem 4). Further, we will prove lower bounds for *digital* (t, m, s)-nets in prime base b in Theorem 6. Finally, we will determine the exact value of the spectral test for *strict* digital (t, m, s)-nets for a prime base b (see Corollary 8). It follows that the bounds given in Theorems 4 and 6 are best possible.

The first lemma is a basic tool in the study of (t, m, s)-nets by Walsh functions. It was first proved in [8, Lemma 2a]. Our proof uses elementary "geometrical" arguments.

LEMMA 1. *Let $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ be a (t, m, s)-net in base b, $b \ge 2$ an arbitrary integer. Then*

$$S_{b^m}(w_{\mathbf{k}}, \omega) = 0 \quad \forall \mathbf{k} : 0 < V(\underline{\mathbf{k}}) \le m - t. \tag{3}$$

Proof. Suppose that $\mathbf{k} = (k^{(1)}, \ldots, k^{(s)})$ is such that $0 < V(\underline{\mathbf{k}}) \le m - t$. This implies that not all $k^{(i)}$ are equal to zero and that $v(\underline{k}^{(i)}) = g_i$ with some integer $g_i \ge 0$, $1 \le i \le s$, where $\sum_{i=1}^s g_i \le m - t$. In other words, $k^{(i)} < b^{g_i}$, $1 \le i \le s$. It is elementary to see from its definition that the Walsh function $w_{\mathbf{k}}$ is constant on every elementary b-adic interval $J_{\mathbf{a}}$, $\mathbf{a} = (a^{(1)}, \ldots, a^{(s)})$, of the form $J_{\mathbf{a}} = \prod_{i=1}^s [a^{(i)} b^{-g_i}, (a^{(i)} + 1) b^{-g_i}[$, where $0 \le a^{(i)} < b^{g_i}$, $1 \le i \le s$. Let $c_{\mathbf{a}}$ denote the value of $w_{\mathbf{k}}$ on $J_{\mathbf{a}}$. Then $w_{\mathbf{k}}$ can be written as the step function $w_{\mathbf{k}} = \sum_{\mathbf{a}} c_{\mathbf{a}} 1_{J_{\mathbf{a}}}$, where summation is over all possible vectors $\mathbf{a}$ and $1_{J_{\mathbf{a}}}$ denotes the characteristic function of the interval $J_{\mathbf{a}}$, $1_{J_{\mathbf{a}}}(\mathbf{x}) = 1$ if $\mathbf{x} \in J_{\mathbf{a}}$, and $1_{J_{\mathbf{a}}}(\mathbf{x}) = 0$ otherwise. Hence, $S_{b^m}(w_{\mathbf{k}}, \omega) = \sum_{\mathbf{a}} c_{\mathbf{a}} S_{b^m}(1_{J_{\mathbf{a}}}, \omega)$.

Let λ_s stand for the Lebesgue measure on $[0, 1[^s$. The volume $\lambda_s(J_{\mathbf{a}})$ of $J_{\mathbf{a}}$ is independent of $\mathbf{a}$, $\lambda_s(J_{\mathbf{a}}) = b^{-\sum_{i=1}^s g_i}$. It is a basic fact about Walsh functions that the integral of $w_{\mathbf{k}}$ over the whole unit cube $[0, 1[^s$ is zero. This implies $\sum_{\mathbf{a}} c_{\mathbf{a}} = 0$, which gives the identity

$$S_{b^m}(w_{\mathbf{k}}, \omega) = \sum_{\mathbf{a}} c_{\mathbf{a}} S_{b^m}(1_{J_{\mathbf{a}}} - \lambda_s(J_{\mathbf{a}}), \omega).$$

The (t, m, s)-net property of ω implies that every interval $J_{\mathbf{a}}$ contains the

same number of points of ω. This number is equal to $b^{m-\sum_{i=1}^{s} g_i}$. Hence,

$$S_{b^m}(1_{J_{\mathbf{a}}} - \lambda_s(J_{\mathbf{a}}), \omega) = \frac{1}{b^m}\left(b^{m-\sum_{i=1}^{s} g_i} - b^m \lambda_s(J_{\mathbf{a}})\right) = 0,$$

for all choices of $\mathbf{a}$. The result follows. ∎

LEMMA 2. *Let $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ be a finite sequence of b^m points in the s-dimensional unit cube $[0,1[^s$ and suppose that*

$$S_{b^m}(w_{\mathbf{k}}, \omega) = 0 \quad \forall \mathbf{k} : 0 < V(\underline{\mathbf{k}}) \le m - t. \tag{4}$$

Then ω is a (t,m,s)-net.

Proof. Suppose that J is an arbitrary elementary b-adic interval of the form

$$J = \prod_{i=1}^{s} [a^{(i)} b^{-g_i}, (a^{(i)}+1) b^{-g_i}[,$$

with $0 \le a^{(i)} < b^{g_i}$, $g_i \ge 0$, and $\sum_{i=1}^{s} g_i = m - t$. We put

$$f(\mathbf{x}) = 1_J(\mathbf{x}) - \lambda_s(J), \quad \mathbf{x} \in [0,1[^s.$$

In order to show that ω is a (t,m,s)-net in base b, it suffices to prove that $S_{b^m}(f,\omega) = 0$.

If $\widehat{1}_J(\mathbf{k})$ denotes the $\mathbf{k}$th Walsh coefficient of the function 1_J, then, due to [2, Lemmas 2 and 3], the following identity holds:

$$f(\mathbf{x}) = \sum_{\mathbf{k} \in \Delta^*} \widehat{1}_J(\mathbf{k}) w_{\mathbf{k}}(\mathbf{x}) \quad \forall \mathbf{x} \in [0,1[^s,$$

where $\Delta^* = \{\mathbf{k} \ne \mathbf{0} : 0 \le k^{(i)} < b^{g_i},\ 1 \le i \le s\}$. From this relation, we deduce that $S_{b^m}(f,\omega) = \sum_{\mathbf{k} \in \Delta^*} \widehat{1}_J(\mathbf{k}) S_{b^m}(w_{\mathbf{k}}, \omega)$. Further, the condition $\mathbf{k} \in \Delta^*$ implies $V(\underline{\mathbf{k}}) \le \sum_{i=1}^{s} g_i = m - t$. Hence, all Weyl sums $S_{b^m}(w_{\mathbf{k}}, \omega)$ will be equal to zero. This implies $S_{b^m}(f,\omega) = 0$. ∎

COROLLARY 3. *Let $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ be a finite sequence of b^m points in the s-dimensional unit cube $[0,1[^s$. Then ω is a (t,m,s)-net if and only if*

$$S_{b^m}(w_{\mathbf{k}}, \omega) = 0 \quad \forall \mathbf{k} : 0 < V(\underline{\mathbf{k}}) \le m - t.$$

THEOREM 4. *Let $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ be a (t,m,s)-net in base b, $b \ge 2$ an arbitrary integer. Then*

$$\sigma_{b^m}(\omega) \le 1/b^{m-t+1}. \tag{5}$$

Proof. Corollary 3 implies that we only have to consider those $\mathbf{k}$ which satisfy $V(\underline{\mathbf{k}}) > m - t$. It is elementary to see that

$$\sigma_{b^m}(\omega) = \max\left\{ \max_{\mathbf{k}:\, m-t < V(\underline{\mathbf{k}}) \le m} \frac{|S_N(w_{\mathbf{k}}, \omega)|}{r(\mathbf{k})}, \sup_{\mathbf{k}:\, V(\underline{\mathbf{k}}) > m} \frac{|S_N(w_{\mathbf{k}}, \omega)|}{r(\mathbf{k})} \right\}.$$

Now,

$$\sup_{\mathbf{k}:\, V(\underline{\mathbf{k}})>m} \frac{|S_N(w_{\mathbf{k}},\omega)|}{r(\mathbf{k})} \le \frac{1}{b^{m+1}}.$$

It is obvious that

$$\max_{\mathbf{k}:\, m-t<V(\underline{\mathbf{k}})\le m} \frac{|S_N(w_{\mathbf{k}},\omega)|}{r(\mathbf{k})} \le \frac{1}{b^{m-t+1}}.$$

The result follows. ∎

The next lemma is a special case of a known result on character sums over abelian groups (see [9], and also [1, Lemma 4A] for a restatement in terms of Walsh functions, without proof). Our proof is elementary and self-contained.

LEMMA 5. *Let* $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ *be a digital* (t,m,s)*-net in base* b*,* b *a prime. Then*

(i) *For all* $\mathbf{k}$*, the Weyl sums* $S_{b^m}(w_{\mathbf{k}},\omega)$ *take only two values*:

$$S_{b^m}(w_{\mathbf{k}},\omega) \in \{0,1\} \quad \forall \mathbf{k}. \tag{6}$$

(ii) *Nonzero Weyl sums may be characterized as follows*:

$$S_{b^m}(w_{\mathbf{k}},\omega) = 1 \Leftrightarrow \underline{\mathbf{k}} \in \underline{\omega}^{\perp}. \tag{7}$$

Proof. The points of ω have a b-adic representation of length m in every coordinate. For this reason, we may restrict our attention to those indices $\mathbf{k} = (k^{(1)},\dots,k^{(s)}) \in \mathbb{Z}^s$ where each $k^{(i)}$ has the property $0 \le k^{(i)} < b^m$. Let n satisfy $0 \le n < b^m$. The map

$$\underline{n} \mapsto \underline{k}^{(i)} \cdot \underline{n}C_i$$

is a linear functional on the vector space $\mathbb{F}_b^m$, hence there exists a uniquely determined element $\underline{a}^{(i)} \in \mathbb{F}_b^m$ such that

$$\underline{k}^{(i)} \cdot \underline{n}C_i = \underline{a}^{(i)} \cdot \underline{n} \quad \forall \underline{n} \in \mathbf{F}_b^m,$$

for $1 \le i \le s$. It follows that

$$\begin{aligned} \underline{\mathbf{k}} \cdot (\underline{n}C_1, \underline{n}C_2, \dots, \underline{n}C_s) &= (\underline{a}^{(1)} + \underline{a}^{(2)} + \ldots + \underline{a}^{(s)}) \cdot \underline{n} \\ &= \underline{a} \cdot \underline{n} \quad \forall \underline{n} \in \mathbb{F}_b^m, \end{aligned} \tag{8}$$

with $\underline{a} = \underline{a}^{(1)} + \underline{a}^{(2)} + \ldots + \underline{a}^{(s)}$. As a consequence,

$$S_{b^m}(w_{\mathbf{k}},\omega) = \begin{cases} 1 & \text{if } \underline{a} = \underline{0}, \\ 0 & \text{otherwise.} \end{cases}$$

This proves (i).

For (ii), let $\underline{\mathbf{k}} \in \underline{\omega}^{\perp}$. This is to say,

$$\underline{\mathbf{k}} \cdot (\underline{n}C_1, \underline{n}C_2, \dots, \underline{n}C_s) = 0 \quad \forall \underline{n} \in \mathbb{F}_b^m.$$

This implies that $w_{\mathbf{k}}(x_n) = 1$ for all $\underline{n} \in \mathbb{F}_b^m$, and, hence, $S_{b^m}(w_{\mathbf{k}}, \omega) = 1$. If we assume that $S_{b^m}(w_{\mathbf{k}}, \omega) = 1$, then necessarily $\underline{a} = \underline{0}$, which implies $\underline{\mathbf{k}} \in \underline{\omega}^{\perp}$. ∎

THEOREM 6. *Let* $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ *be a digital* (t, m, s)*-net in base* b*,* b *a prime. Then*

$$\sigma_{b^m}(\omega) \geq 1/b^{m+1}. \tag{9}$$

Proof. Let $\underline{\omega}$ denote the linear code in $\mathbb{F}_b^{sm}$ associated with ω. The elements of $\underline{\omega}$ have the form

$$(\underline{n}C_1, \underline{n}C_2, \ldots, \underline{n}C_s), \quad 0 \leq n < b^m.$$

The dimension of $\underline{\omega}$ is less than or equal to m. Let $\delta(\underline{\omega}^{\perp})$ denote the minimum distance of the dual code $\underline{\omega}^{\perp}$,

$$\delta(\underline{\omega}^{\perp}) = \min\{V(\underline{\mathbf{k}}) : \underline{\mathbf{k}} \in \underline{\omega}^{\perp} \setminus \{\mathbf{0}\}\}.$$

Because the dimension $\dim(\underline{\omega}^{\perp})$ of $\underline{\omega}^{\perp}$ is greater than or equal to $(s-1)m$, the generalized Singleton bound proved in [14, Prop. 1, p. 175] implies

$$\delta(\underline{\omega}^{\perp}) \leq sm - \dim(\underline{\omega}^{\perp}) + 1 \leq m + 1.$$

This estimate, together with Lemma 5, yields

$$\begin{aligned} \sigma_{b^m}(\omega) &= \sup_{\underline{\mathbf{k}} \in \underline{\omega}^{\perp} \setminus \{\mathbf{0}\}} \frac{1}{r(\underline{\mathbf{k}})} = \sup_{\underline{\mathbf{k}} \in \underline{\omega}^{\perp} \setminus \{\mathbf{0}\}} \frac{1}{b^{V(\underline{\mathbf{k}})}} \\ &= \frac{1}{b^{\min V(\underline{\mathbf{k}})}} = \frac{1}{b^{\delta(\underline{\omega}^{\perp})}} \geq \frac{1}{b^{m+1}}. \ \blacksquare \end{aligned} \tag{10}$$

THEOREM 7. *Let* $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ *be a strict digital* (t, m, s)*-net in base* b*,* b *a prime. Then*

$$\sigma_{b^m}(\omega) \geq 1/b^{m-t+1}. \tag{11}$$

Proof. The fact that ω is a *strict* (t, m, s)-net in base b implies the existence of an index $\mathbf{k}^*$ with the properties

$$V(\underline{\mathbf{k}}^*) = m - t + 1 \quad \text{and} \quad S_{b^m}(w_{\mathbf{k}^*}, \omega) \neq 0.$$

For, otherwise, by Lemma 2, the net ω would be a $(t-1, m, s)$-net. This would contradict the strictness of ω.

Now, ω is also a *digital* (t, m, s)-net. The definition of the spectral test and an application of Lemma 5 imply that

$$\sigma_{b^m}(\omega) \geq |S_{b^m}(w_{\mathbf{k}^*}, \omega)| / r(\mathbf{k}^*) = 1/b^{m-t+1}. \ \blacksquare$$

COROLLARY 8. *Let* $\omega = (\mathbf{x}_n)_{n=0}^{b^m-1}$ *be a strict digital* (t, m, s)*-net in base* b*,* b *a prime. Then*

$$\sigma_{b^m}(\omega) = 1/b^{m-t+1}. \tag{12}$$

Proof. This result follows from Theorems 4 and 7. ∎

References

[1] W. W. L. Chen and M. M. Skriganov, *Explicit constructions in the classical mean squares problem in irregularities of point distribution*, J. Reine Angew. Math. 545 (2002), 67–95.

[2] P. Hellekalek, *General discrepancy estimates*: *the Walsh function system*, Acta Arith. 67 (1994), 209–218.

[3] —, *On correlation analysis of pseudorandom numbers*, in: [13], 251–265.

[4] —, *On the assessment of random and quasi-random point sets*, in: [6], 49–108.

[5] —, *On the spectral test*, preprint, University of Salzburg, 2001.

[6] P. Hellekalek and G. Larcher (eds.), *Random and Quasi-Random Point Sets*, Lecture Notes in Statist. 138, Springer, New York, 1998.

[7] G. Larcher, *Digital point sets*: *analysis and application*, in: [6], 167–222.

[8] G. Larcher, H. Niederreiter and W. C. Schmid, *Digital nets and sequences constructed over finite rings and their applications to quasi-Monte Carlo integration*, Monatsh. Math. 121 (1996), 231–253.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

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

[11] —, *Point sets and sequences with small discrepancy*, ibid. 104 (1987), 273–337.

[12] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[13] H. Niederreiter, P. Hellekalek, G. Larcher and P. Zinterhof (eds.), *Monte Carlo and Quasi-Monte Carlo Methods 1996*, Lecture Notes in Statist. 127, Springer, New York, 1997.

[14] H. Niederreiter and G. Pirsic, *Duality for digital nets and its applications*, Acta Arith. 97 (2001), 173–182.

[15] H. Niederreiter and C. P. Xing, *The algebraic-geometry approach to low-discrepancy sequences*, in: [13], 139–160.

[16] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz 13 (2001), 191–239 (in Russian).

Institut für Mathematik
Universität Salzburg
Hellbrunner Straße 34
A-5020 Salzburg, Austria
E-mail: peter.hellekalek@sbg.ac.at

Received on 15.6.2001
and in revised form on 18.1.2002 (4055)