ACTA ARITHMETICA
139.2 (2009)

A general discrepancy estimate based on p-adic arithmetics

by

Peter Hellekalek (Salzburg)

Dedicated to Harald Niederreiter on the occasion of his 65th birthday

1. Introduction. The inequality of Erdős–Turán–Koksma gives an upper bound for the discrepancy of a finite sequence ω in $[0,1[^s$ in terms of certain exponential sums; see the monographs Drmota and Tichy [1] and Kuipers and Niederreiter [7] for its general form, and Niederreiter [10] for versions adapted to certain sequences ω of rationals as they appear in applications. These inequalities are an important tool to assess the uniform distribution of low-discrepancy point sets or correlation properties of pseudo-random numbers; see the surveys of Niederreiter [11], Niederreiter and Shparlinski [13] and Hellekalek [4].

The classical inequality of Erdős–Turán–Koksma is based on the trigonometric function system. Variants have been established for Walsh and Haar function systems in an arbitrary integer base $b \geq 2$ in Hellekalek [2, 3].

What is the importance of these variants? Different types of sequences ω require different types of exponential sums to study their equidistribution properties, by means of discrepancy and other figures of merit. Hence, by varying the function system, one is able to "synchronize" the exponential sums with the type of sequence under study.

In this paper, we will introduce a function system closely related to the dual group of p-adic integers $\mathbb{Z}_p$, p a prime, and we will prove a new variant of the inequality of Erdős–Turán–Koksma. This leads to general upper bounds for discrepancy (see Theorem 3.6 and Corollary 3.7). In addition, we will prove a variant of the Weyl criterion for the p-adic function system under consideration (see Theorem 3.8). The uniform distribution of the van der Corput sequence in base p then follows as a simple consequence (see Corollary 3.9).

2000 *Mathematics Subject Classification*: 11K06, 11K38, 11K41, 11K45, 11L03.
Key words and phrases: discrepancy, inequality of Erdős–Turán–Koksma, Weyl's criterion, p-adic integers, van der Corput sequence.

DOI: 10.4064/aa139-2-3

2. Prerequisites. Throughout this paper, p denotes a prime and $\mathbb{N}$ stands for the positive integers. We put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

2.1. *The p-adic representation of real numbers.* For a nonnegative integer a, let

$$a = \sum_{j \geq 0} a_j p^j, \qquad a_j \in \{0, 1, \ldots, p-1\},$$

be the unique p-adic representation of a in base p. With the exception of at most finitely many indices j, the digits a_j are zero.

Every real number $x \in [0, 1[$ has a unique p-adic representation

$$x = \sum_{j \geq 0} x_j p^{-j-1}, \qquad x_j \in \{0, 1, \ldots, p-1\},$$

under the condition that $x_j \neq p-1$ for infinitely many j. *In the following, this uniqueness condition will be assumed without further notice.* We will also write the p-adic representation of $x \in [0, 1[$ in the form $x = 0.x_0x_1\ldots$.

For $g \in \mathbb{N}$, we denote the initial part of the p-adic representation of $x \in [0, 1[$ by $x(g) = 0.x_0x_1\ldots x_{g-1}$, and the initial part of the representation of a rational integer (or p-adic integer) a by $a(g) = \sum_{j=0}^{g-1} a_j p^j$. Then $x(g) \in \{bp^{-g} : 0 \leq b < p^g\}$ and $a(g) \in \{0, 1, \ldots, p^g - 1\}$. Further, we define $x(0) = 0$ and $k(0) = 0$.

An interval of the form $[bp^{-g}, (b+1)p^{-g}[$, $0 \leq b < p^g$, $g \geq 0$, b and g integers, is called a (*half-open*) *elementary p-adic interval of length* p^{-g}. Let $a_0, a_1, \ldots, a_{g-1}$ be arbitrary digits in $\{0, 1, \ldots, p-1\}$, $g \in \mathbb{N}$. Let $I[a_0, a_1, \ldots, a_{g-1}] = \{x = 0.x_0x_1\ldots \in [0, 1[: x_j = a_j,\ 0 \leq j \leq g-1\}$ denote the so-called *cylinder set* defined by the digits $a_0, a_1, \ldots, a_{g-1}$, where, as throughout this paper, we are assuming the uniqueness condition for the p-adic representation of x. It is easily seen that, for any elementary p-adic interval $I = [bp^{-g}, (b+1)p^{-g}[$ of length p^{-g}, $g \in \mathbb{N}$, there is a unique cylinder set $I[a_0, a_1, \ldots, a_{g-1}]$ such that $I = I[a_0, a_1, \ldots, a_{g-1}]$, and vice versa.

2.2. *The p-adic integers* $\mathbb{Z}_p$. Let $\mathbb{Z}_p$ denote the compact group of p-adic integers. We refer the reader to the monograph Robert [14] for details. An element z of $\mathbb{Z}_p$ will be written as

$$z = \sum_{j \geq 0} z_j p^j,$$

with digits $z_j \in \{0, 1, \ldots, p-1\}$.

The *dual group* $\hat{\mathbb{Z}}_p$ of $\mathbb{Z}_p$ is given by the functions

$$\hat{\mathbb{Z}}_p = \{\chi_0\} \cup \{z \mapsto e^{2\pi i a p^{-g}(z_0 + z_1 p + \cdots + z_{g-1}p^{g-1})} : 0 < a < p^g,\ g \in \mathbb{N}\},$$

where χ_0 denotes the trivial character $\chi_0 : z \mapsto 1$ for all $z \in \mathbb{Z}_p$. In the description of $\hat{\mathbb{Z}}_p$ above, for the fractions a/p^g, we may assume the condition $(a, p^g) = (a, p) = 1$.

DEFINITION 2.1. We define the (*p-adic*) *Monna map* φ as follows:

$$\varphi : \mathbb{Z}_p \to [0,1], \qquad \varphi\Big(\sum_{j\geq 0} z_j p^j\Big) = \sum_{j\geq 0} z_j p^{-j-1}.$$

REMARK 2.1. The Monna map φ is continuous and surjective, but *not* injective. Further, φ gives a bijection between the subset $\mathbb{N}$ of $\mathbb{Z}_p$ and the set $\{a/p^g : 0 < a < p^g,\ g \in \mathbb{N},\ (a,p^g) = (a,p) = 1\}$ of all reduced p-adic fractions.

The latter fact allows for the following notation. For a nonnegative integer k, let

$$\chi_k : \mathbb{Z}_p \to \{c \in \mathbb{C} : |c| = 1\}, \qquad \chi_k(z) = e^{2\pi i \varphi(k)(z_0 + z_1 p + \cdots)}.$$

Hence, we may write the dual group in the form $\hat{\mathbb{Z}}_p = \{\chi_k : k \in \mathbb{N}_0\}$.

We will now define a function system which will be the main tool in our discrepancy estimates. Let $x \in [0,1[$ have the p-adic representation $x = 0.x_0x_1\ldots$, where infinitely many digits x_j are different from $p-1$. By $z(x) \in \mathbb{Z}_p$ we will denote the element $z(x) = x_0 + x_1 p + \cdots$ defined by the digits of x. We have $\varphi(z(x)) = x$ for all $x \in [0,1[$.

DEFINITION 2.2. For a nonnegative integer k, let

$$\gamma_k : [0,1[\to \{c \in \mathbb{C} : |c| = 1\}, \qquad \gamma_k(x) = \chi_k(z(x)).$$

Let $\Gamma_p = \{\gamma_k : k \in \mathbb{N}_0\}$. It is easy to show that

$$\int_{[0,1[} \gamma_k(x)\,dx = 0, \qquad \forall k \in \mathbb{N}.$$

For an integrable function f on $[0,1[$, and for $k \in \mathbb{N}_0$, let $\hat{f}(k)$ denote the kth Fourier coefficient of f with respect to the function system Γ_p,

$$\hat{f}(k) = \int_{[0,1[} f(x)\overline{\gamma_k(x)}\,dx.$$

There is an obvious generalization of the preceding notions to the higher-dimensional case. In the following, let $\mathbf{x} = (x_1,\ldots,x_s) \in [0,1[^s$, let $\mathbf{k} = (k_1,\ldots,k_s) \in \mathbb{N}_0^s$, and let λ_s denote s-dimensional Lebesgue measure, where we will write λ instead of λ_1 in the case $s = 1$. We define

$$\gamma_{\mathbf{k}}(\mathbf{x}) = \prod_{i=1}^{s} \gamma_{k_i}(x_i), \qquad \Gamma_p^{(s)} = \{\gamma_{\mathbf{k}} : \mathbf{k} \in \mathbb{N}_0^s\},$$

and call $\Gamma_p^{(s)}$ the *p-adic function system on* $[0,1[^s$. We will write Γ_p instead of $\Gamma_p^{(1)}$ in the case $s = 1$.

For an integrable function f on $[0,1[^s$, the $\mathbf{k}$th Fourier coefficient of f with respect to the function system $\Gamma_p^{(s)}$ is given by

$$\hat{f}(\mathbf{k}) = \int_{[0,1[^s} f(\mathbf{x})\overline{\gamma_{\mathbf{k}}(\mathbf{x})}\,d\mathbf{x}.$$

Further, we define the weight functions

$$\rho(k) = \begin{cases} 1 & \text{if } k = 0, \\ \dfrac{2}{p^t \sin(\pi k_{t-1}/p)} & \text{if } p^{t-1} \le k < p^t,\ t \in \mathbb{N}, \end{cases}$$

$$\rho(\mathbf{k}) = \prod_{i=1}^{s} \rho(k_i), \qquad \mathbf{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s.$$

We also introduce the weights ρ^*: $\rho^*(0) = 1$, $\rho^*(k) = \rho(k)/2$ for $k \neq 0$, and, for $\mathbf{k} \in \mathbb{N}_0^s$, $\rho^*(\mathbf{k}) = \prod_{i=1}^s \rho^*(k_i)$.

For $g \in \mathbb{N}$, we define the finite summation domains

$$\Delta(g) = \{\mathbf{k} = (k_1, \ldots, k_s) : 0 \le k_i < p^g,\ 1 \le i \le s\},$$
$$\Delta^*(g) = \Delta(g) \setminus \{\mathbf{0}\}.$$

The extreme discrepancy and the star discrepancy of a sequence are defined as follows (see Niederreiter [10]). Let $\mathcal{J}$ denote the class of all subintervals of $[0,1[^s$ of the form $\prod_{i=1}^s [u_i, v_i[$, $0 \le u_i < v_i \le 1$, $1 \le i \le s$, and let $\mathcal{J}^*$ denote the subclass of $\mathcal{J}$ of intervals of the type $\prod_{i=1}^s [0, v_i[$. For $J \in \mathcal{J}$, let $\mathbf{1}_J$ denote the indicator function of J, $\mathbf{1}_J(\mathbf{x}) = 1$ if $\mathbf{x} \in J$ and $\mathbf{1}_J(\mathbf{x}) = 0$ otherwise.

For a function f on $[0,1[^s$ and a sequence $\omega = (\mathbf{x}_n)_{n\ge 0}$ in $[0,1[^s$, let

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

Definition 2.3. Let $\omega = (\mathbf{x}_n)_{n\ge 0}$ be a sequence in $[0,1[^s$.

- The (*extreme*) *discrepancy* $D_N(\omega)$ of the first N elements of ω is defined as
$$D_N(\omega) = \sup_{J \in \mathcal{J}} |S_N(\mathbf{1}_J - \lambda_s(J), \omega)|.$$
- The *star discrepancy* $D_N^*(\omega)$ of the first N elements of ω is defined as
$$D_N^*(\omega) = \sup_{J \in \mathcal{J}^*} |S_N(\mathbf{1}_J - \lambda_s(J), \omega)|.$$

3. The results

Lemma 3.1. *Let $g \in \mathbb{N}$, let $a_0, \ldots, a_{g-1}$ be arbitrary digits, and let $I[a_0, \ldots, a_{g-1}]$ be the elementary p-adic interval of length $1/p^g$ defined by these digits.*

(i) *If* $p^{t-1} \le k < p^t$, $1 \le t \le g$, *then the function* γ_k *is constant on* $I[a_0, \dots, a_{g-1}]$, *with value* $\gamma_k(0.a_0 \dots a_{t-1})$, *and*

$$\hat{\mathbf{1}}_{I[a_0,\dots,a_{g-1}]}(k) = \frac{1}{p^g}\, e^{-2\pi i \varphi(k)(a_0+\dots+a_{t-1}p^{t-1})}.$$

(ii) *For all* $k \ge p^g$,

$$\hat{\mathbf{1}}_{I[a_0,\dots,a_{g-1}]}(k) = 0.$$

Proof. For any k such that $p^{t-1} \le k < p^t$, $t \in \mathbb{N}$, we have $\varphi(k) = c/p^t$, with $1 \le c < p^t$, $(c, p^t) = (c, p) = 1$.

Since $k < p^g$, the function γ_k is constant on the elementary p-adic interval $I[a_0, \dots, a_{g-1}]$, with value $\gamma_k(0.a_0 \dots a_{t-1}) = \chi_k(a_0 + \dots + a_{t-1}p^{t-1})$. Clearly,

$$\hat{\mathbf{1}}_{I[a_0,\dots,a_{g-1}]}(k) = \int\limits_{I[a_0,\dots,a_{g-1}]} \overline{\gamma_k(x)}\, dx.$$

In order to prove (ii), let $p^{t-1} \le k < p^t$, where $t \ge g+1$. Then we have the following partition into disjoint cylinder sets:

$$I[a_0, \dots, a_{g-1}] = \bigcup_{b_g=0}^{p-1} \dots \bigcup_{b_{t-1}=0}^{p-1} I[a_0, \dots, a_{g-1}, b_g, \dots, b_{t-1}].$$

This implies

$$\hat{\mathbf{1}}_{I[a_0,\dots,a_{g-1}]}(k) = \frac{1}{p^t}\, \overline{\chi_k(a_0 + \dots + a_{g-1}p^{g-1})} \cdot \sum_{b_g=0}^{p-1} (e^{-2\pi i\varphi(k)p^g})^{b_g} \cdot \dots \cdot \underbrace{\sum_{b_{t-1}=0}^{p-1} (e^{-2\pi i\varphi(k)p^{t-1}})^{b_{t-1}}}_{=0}. \ \blacksquare$$

LEMMA 3.2. *Let* $g \in \mathbb{N}$, *let* $a_0, \dots, a_{g-1}$ *be arbitrary digits, and let* $I = I[a_0, \dots, a_{g-1}]$. *Then*

$$\mathbf{1}_I(x) - \lambda(I) = \sum_{1 \le k < p^g} \hat{\mathbf{1}}_I(k)\gamma_k(x), \qquad \forall x \in [0, 1[. \tag{1}$$

Proof. We note that, for $f(x) = \mathbf{1}_I(x) - \lambda(I)$, $\hat{f}(0) = 0$. Further, for all $k \ne 0$, $\hat{f}(k) = \hat{\mathbf{1}}_I(k)$. Let

$$S(x) = \sum_{1 \le k < p^g} \hat{\mathbf{1}}_I(k)\gamma_k(x), \qquad x \in [0, 1[.$$

Then

$$S(x) = \sum_{t=1}^{g} \sum_{b=1}^{p-1} \sum_{k=bp^{t-1}}^{(b+1)p^{t-1}-1} \hat{\mathbf{1}}_I(k)\gamma_k(x).$$

Lemma 3.1(i) implies that, for $p^{t-1} \le k < p^t$,

$$\hat{\mathbf{1}}_I(k)\gamma_k(x) = \frac{1}{p^g}\, e^{2\pi i\varphi(k)(x_0+\cdots+x_{t-1}p^{t-1}-(a_0+\cdots+a_{t-1}p^{t-1}))}.$$

For t with $1 \le t \le g$, let $a(t) = a_0 + \cdots + a_{t-1}p^{t-1}$. By a slight abuse of notation, we will write $x(t) = x_0+\cdots+x_{t-1}p^{t-1}$. If $bp^{t-1} \le k \le (b+1)p^{t-1} - 1$, then $\varphi(k) = (b + k_{t-2}p + \cdots + k_0p^{t-1})/p^t$. Then

$$\begin{aligned} S(x) = \frac{1}{p^g}\Big(&\sum_{b=1}^{p-1}(e^{2\pi i(x_0-a_0)/p})^b \\ &+ \sum_{t=2}^{g}\Big(\sum_{b=1}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^b \cdot \sum_{k_{t-2}=0}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^{k_{t-2}p} \\ &\cdot \ldots \cdot \sum_{k_0=0}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^{k_0p^{t-1}}\Big)\Big). \end{aligned}$$

Suppose that $x \in I = I[a_0, \ldots, a_{g-1}]$. Then $x(t) = a(t)$ for $1 \le t \le g$. As a consequence,

$$S(x) = \frac{1}{p^g}\Big(p - 1 + \sum_{t=2}^{g}(p-1)p^{t-1}\Big) = 1 - \frac{1}{p^g}.$$

Trivially, $\mathbf{1}_I(x) - \lambda(I) = 1 - 1/p^g$ in this case. Hence, if $x \in I$, identity (1) holds.

If $x \notin I = I[a_0, \ldots, a_{g-1}]$, define $t_0 = \min\{t, 1 \le t \le g : x_{t-1} \ne a_{t-1}\}$.

If $t_0 = 1$, then $x_0 - a_0 \not\equiv 0 \pmod p$. This implies

$$\sum_{b=1}^{p-1}(e^{2\pi i(x_0-a_0)/p})^b = -1,$$

and, for all other t,

$$\sum_{k_0=0}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^{k_0p^{t-1}} = 0.$$

Hence, identity (1) also holds in this case.

Now, let $2 \le t_0 \le g$. From the definition of t_0, it follows that

$$\begin{aligned} &x(t) - a(t) \\ &\quad = \begin{cases} 0, & 1 \le t < t_0, \\ (x_{t_0-1} - a_{t_0-1})p^{t_0-1} + \cdots + (x_{t-1} - a_{t-1})p^{t-1}, & t_0 \le t \le g. \end{cases} \end{aligned}$$

Hence,

$$(2)\qquad S(x)=\frac{1}{p^g}\Big(p-1+\sum_{t=2}^{t_0-1}(p-1)p^{t-1}+\sum_{t=t_0}^{g}\Big(\sum_{b=1}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^b \cdot \sum_{k_{t-2}=0}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^{k_{t-2}p}\cdot\ldots\cdot\sum_{k_0=0}^{p-1}(e^{2\pi i(x(t)-a(t))/p^t})^{k_0p^{t-1}}\Big)\Big),$$

with the convention that $\sum_{t=2}^{t_0-1}(p-1)p^{t-1}=0$ in the case $t_0=2$. The nontrivial exponents in the sums above contain a factor of the form $(x(t)-a(t))p^{-t}p^{t-1-v}$, where $0\le v\le t-2$, $2\le t_0\le t$. This factor will be an integer if and only if $0\le v\le t_0-2$. This is due to the fact that $x(t)-a(t)\in p^{t_0-1}\mathbb{Z}$ for every t such that $t_0\le t\le g$.

Let $\zeta_t=e^{2\pi i(x(t)-a(t))/p^t}$, and put

$$S_{t,v}=\sum_{k_v=0}^{p-1}\zeta_t^{k_vp^{t-1-v}},\qquad 0\le v\le t-2.$$

If $t\ge t_0+1$, then the product $\prod_{v=0}^{t-2}S_{t,v}$ will contain the factor S_{t,t_0-1}. It is easily seen that $S_{t,t_0-1}=0$. As a consequence, the above product will be zero. Hence, in (2), the sum $\sum_{t=t_0}^{g}$ has only one nonzero term, namely for $t=t_0$. This term has the value $-p^{t_0-1}$. As a consequence, $S(x)=p^{-g}(-1+p^{t_0-1}-p^{t_0-1})=-1/p^g$. This proves identity (1) in the case $2\le t_0\le g$ and completes the proof of this lemma. ∎

Lemma 3.3. *Let $0<\beta<1$ and let $I=[0,\beta[$. Suppose that $p^{t-1}\le k<p^t$, $t\in\mathbb{N}$. Then*:

(i) *The Fourier coefficient $\hat{\mathbf{1}}_I(k)$ has the following value*:

$$\hat{\mathbf{1}}_I(k)=\frac{1}{p^t}\,\overline{\chi_k(\beta_0+\cdots+\beta_{t-2}p^{t-2})}\cdot\left(\frac{e^{-2\pi ik_{t-1}\beta_{t-1}/p}-1}{e^{-2\pi ik_{t-1}/p}-1}+e^{-2\pi ik_{t-1}\beta_{t-1}/p}p^t(\beta-\beta(t))\right).$$

(ii) *The following estimate holds*:

$$|\hat{\mathbf{1}}_I(k)|\le\frac{1}{p^t\sin(\pi k_{t-1}/p)}.$$

Proof. To show (i), we note that, because of $k\ge p^{t-1}$, it follows from Lemma 3.1(ii) that

$$\int_0^{\beta(t-1)}\overline{\gamma_k(x)}\,dx=0.$$

Hence

$$\begin{aligned}\hat{\mathbf{1}}_I(k) &= \int_{\beta(t-1)}^{\beta} \overline{\gamma_k(x)}\,dx = \int_{I[\beta_0,\ldots,\beta_{t-2}]} \mathbf{1}_{[\beta(t-1),\beta[}(x)\,\overline{\gamma_k(x)}\,dx \\ &= \overline{\gamma_k(\beta(t-1))} \int_{\beta(t-1)}^{\beta} e^{-2\pi i\varphi(k)x_{t-1}p^{t-1}}\,dx \\ &= \overline{\gamma_k(\beta(t-1))} \int_{\beta(t-1)}^{\beta} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx.\end{aligned}$$

The digit x_{t-1} may take different values on the interval $[\beta(t-1),\beta[$. Hence, in the case where $\beta_{t-1}\neq 0$, we have

$$\begin{aligned}\int_{\beta(t-1)}^{\beta} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx &= \int_{\beta(t-1)}^{\beta(t)} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx + \int_{\beta(t)}^{\beta} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx \\ &= \sum_{b=0}^{\beta_{t-1}-1} \int_{I[\beta_0,\ldots,\beta_{t-2},b]} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx \\ &\quad + \int_{I[\beta_0,\ldots,\beta_{t-2},\beta_{t-1}]} \mathbf{1}_{[\beta(t),\beta[}(x)e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx \\ &= \frac{1}{p^t}\,\frac{e^{-2\pi i k_{t-1}\beta_{t-1}/p}-1}{e^{-2\pi i k_{t-1}/p}-1} \\ &\quad + e^{-2\pi i k_{t-1}\beta_{t-1}/p}(\beta-\beta(t)).\end{aligned}$$

If $\beta_{t-1}=0$, then $\beta(t-1)=\beta(t)$ and, as a consequence,

$$\int_{\beta(t-1)}^{\beta(t)} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx = 0,$$

which implies

$$\begin{aligned}\int_{\beta(t-1)}^{\beta} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx &= \int_{\beta(t)}^{\beta} e^{-2\pi i k_{t-1}x_{t-1}/p}\,dx = e^{-2\pi i k_{t-1}\beta_{t-1}/p}(\beta-\beta(t)) \\ &= \beta-\beta(t).\end{aligned}$$

This ends the proof of (i).

In order to prove (ii), we put $c=e^{-2\pi i k_{t-1}/p}$ and $d=p^t(\beta-\beta(t))$. Due to the condition $p^{t-1}\leq k<p^t$, the digit k_{t-1} is different from zero and

$k_{t-1}/p \notin \mathbb{Z}$, which implies $c \neq 1$. From (i), we deduce the identity

$$|\hat{\mathbf{1}}_I(k)| = \frac{1}{p^t}\left|\frac{c^{\beta_{t-1}}-1}{c-1} + c^{\beta_{t-1}}d\right|.$$

It is $0 \leq d < 1$. Hence

$$|\hat{\mathbf{1}}(k)| \leq \frac{1}{p^t}\left(\left|\frac{1}{c-1}+d\right| + \frac{1}{|c-1|}\right).$$

Now, for every real number δ with $0 \leq \delta \leq 1$, we have the inequality

$$\left|\frac{1}{c-1}+\delta\right| \leq \frac{1}{|c-1|}.$$

The result follows. ∎

COROLLARY 3.4. *Let* $f(x) = \mathbf{1}_I(x) - \lambda(I)$, *where* $I = [ap^{-g}, bp^{-g}[$, $0 \leq a < b \leq p^g$, *with* a, b, *and* g *integers*, $g \geq 1$. *Then* $\hat{f}(0) = 0$, $\hat{f}(k) = \hat{\mathbf{1}}_I(k)$ *for all* $k \geq 1$, *and*:

(i) *If* $k \geq p^g$, *then* $\hat{f}(k) = 0$.
(ii) *If* $p^{t-1} \leq k < p^t$, $1 \leq t \leq g$, *then*

$$|\hat{f}(k)| \leq \frac{2}{p^t \sin(\pi k_{t-1}/p)} \quad (= \rho(k)).$$

Proof. The first statement follows from Lemma 3.1(ii). The second statement is a consequence of the identity $\hat{f}(k) = \hat{\mathbf{1}}_{[0,bp^{-g}[}(k) - \hat{\mathbf{1}}_{[0,ap^{-g}[}(k)$. Lemma 3.3(ii) gives the result. ∎

LEMMA 3.5. *Let* $f(\mathbf{x}) = \mathbf{1}_I(\mathbf{x}) - \lambda_s(I)$, *where* $I = \prod_{i=1}^s [a_i p^{-g}, b_i p^{-g}[$, $0 \leq a_i < b_i \leq p^g$, $g \geq 1$. *Then*:

(i) *For all* $\mathbf{k} \in \mathbb{N}_0^s \setminus \Delta^*(g)$,

$$\hat{f}(\mathbf{k}) = 0.$$

(ii) *For all* $\mathbf{k} \in \Delta^*(g)$,

$$|\hat{f}(\mathbf{k})| \leq \rho(\mathbf{k}).$$

(iii) *The following identity holds*:

$$f(\mathbf{x}) = \sum_{\mathbf{k}\in\Delta^*(g)} \hat{\mathbf{1}}_I(\mathbf{k})\gamma_{\mathbf{k}}(\mathbf{x}), \qquad \forall \mathbf{x} \in [0,1[^s. \tag{3}$$

Proof. Clearly, $\hat{f}(\mathbf{0}) = 0$. For all $\mathbf{k} \neq \mathbf{0}$ we have the identity $\hat{f}(\mathbf{k}) = \hat{\mathbf{1}}_I(\mathbf{k})$. Further, $\hat{\mathbf{1}}_I(\mathbf{k}) = \prod_{i=1}^s \hat{\mathbf{1}}_{I_i}(k_i)$, where $I_i = [a_i p^{-g}, b_i p^{-g}[$, and $\mathbf{k} = (k_1, \ldots, k_s)$.

If $\mathbf{k} \in \mathbb{N}_0^s \setminus \Delta^*(g)$, then either $\mathbf{k} = \mathbf{0}$, hence $\hat{f}(\mathbf{k}) = \hat{f}(\mathbf{0}) = 0$, or $\mathbf{k} \neq \mathbf{0}$ and there exists an i such that $k_i \geq p^g$. Corollary 3.4(i) implies $\hat{\mathbf{1}}_{I_i}(k_i) = 0$. As a consequence, $\hat{f}(\mathbf{k}) = \hat{\mathbf{1}}_I(\mathbf{k}) = 0$. This proves (i).

(ii) is a direct consequence of the second part of Corollary 3.4 and the definition of the function ρ.

(iii) follows from $\mathbf{1}_I(\mathbf{x}) = \prod_{i=1}^s \mathbf{1}_{I_i}(x_i)$ for $\mathbf{x} \in [0,1[^s$, and Lemma 3.2. ∎

THEOREM 3.6. *Let p be a prime number, let ω be an arbitrary sequence in $[0,1[^s$, and let g be a positive integer. Then*

$$D_N(\omega) \le 1 - (1-2/p^g)^s + \sum_{\mathbf{k}\in\Delta^*(g)} \rho(\mathbf{k})|S_N(\gamma_{\mathbf{k}},\omega)|, \tag{4}$$

$$D_N^*(\omega) \le 1 - (1-1/p^g)^s + \sum_{\mathbf{k}\in\Delta^*(g)} \rho^*(\mathbf{k})|S_N(\gamma_{\mathbf{k}},\omega)|. \tag{5}$$

Proof. For a given positive integer g, consider the tiling of $[0,1[^s$ by elementary p-adic cubes $C = \prod_{i=1}^s [a_i p^{-g}, (a_i+1)p^{-g}[$, $0 \le a_i < p^g$, $1 \le i \le s$, of side length $1/p^g$.

Let J be an arbitrary subinterval of $[0,1[^s$ and define $\underline{J}$ as the union of those cubes C that are contained in J, that is, $\underline{J} = \bigcup_{C\subseteq J} C$. Further, let $\bar{J} = \bigcup_{C\cap J\neq\emptyset} C$. Then $\underline{J} \subseteq J \subseteq \bar{J}$, where $\underline{J}$ may be void. It is elementary to see that

$$|S_N(\mathbf{1}_J - \lambda_s(J),\omega)| \le \lambda_s(\bar{J}) - \lambda_s(\underline{J}) + \max\{|S_N(\mathbf{1}_{\underline{J}} - \lambda_s(\underline{J}),\omega)|, |S_N(\mathbf{1}_{\bar{J}} - \lambda_s(\bar{J}),\omega)|\}.$$

In every coordinate i, the side lengths of $\underline{J}$ and $\bar{J}$ differ at most by $2/p^g$. Hence, by an application of Niederreiter [10, Lemma 3.9],

$$\lambda_s(\bar{J}) - \lambda_s(\underline{J}) \le 1 - (1-2/p^g)^s.$$

This implies

$$D_N(\omega) \le 1 - (1-2/p^g)^s + \max_I\{|S_N(\mathbf{1}_I - \lambda_s(I),\omega)|\},$$

with the maximum taken over all intervals $I = \prod_{i=1}^s [a_i p^{-g}, b_i p^{-g}[$, $0 \le a_i < b_i \le p^g$, $1 \le i \le s$, $g \ge 1$. We then apply Lemma 3.5, which gives

$$D_N(\omega) \le 1 - (1-2/p^g)^s + \sum_{\mathbf{k}\in\Delta^*(g)} \rho(\mathbf{k})|S_N(\gamma_{\mathbf{k}},\omega)|. \tag{6}$$

In the case of the star discrepancy, because of the special form of the intervals, the side lengths differ at most by $1/p^g$. Therefore, the bound for the approximation error $\lambda_s(\bar{J}) - \lambda_s(\underline{J})$ reduces to $1-(1-1/p^g)^s$. Further, Lemma 3.3(ii) and its application to the s-dimensional case yield the following estimate for the Fourier coefficients of the function $f(\mathbf{x}) = \mathbf{1}_I(\mathbf{x}) - \lambda_s(I)$, where $I = \prod_{i=1}^s [0, b_i p^{-g}[$, $0 < b_i \le p^g$, $1 \le i \le s$, $g \ge 1$:

$$|\hat{f}(\mathbf{k})| \le \rho^*(\mathbf{k}), \quad \forall \mathbf{k} \in \Delta^*(g).$$

The estimate of the star discrepancy follows. ∎

COROLLARY 3.7. *Let ω and g be as in Theorem 3.6. Suppose that B is a global bound for the exponential sums $S_N(\gamma_{\mathbf{k}}, \omega)$ for all $\mathbf{k}$ in the finite domain $\Delta^*(g)$,*

$$|S_N(\gamma_{\mathbf{k}}, \omega)| \le B, \qquad \forall \mathbf{k} \in \Delta^*(g).$$

Then

$$D_N(\omega) \le 1 - (1 - 2/p^g)^s + B(2.43g \ln p + 1)^s,$$
$$D_N^*(\omega) \le 1 - (1 - 1/p^g)^s + B(1.22g \ln p + 1)^s.$$

Proof. This is easily seen. We first discuss the estimate for the extreme discrepancy $D_N(\omega)$. The discrepancy bound (6) implies that we only have to estimate

$$\sum_{\mathbf{k} \in \Delta^*(g)} \rho(\mathbf{k}) = \sum_{\mathbf{k} \in \Delta(g)} \rho(\mathbf{k}) - 1.$$

Because of the identities

$$\sum_{\mathbf{k} \in \Delta(g)} \rho(\mathbf{k}) = \Big(\sum_{k=0}^{p^g - 1} \rho(k) \Big)^s$$

and

$$\sum_{k=0}^{p^g-1} \rho(k) = 1 + \sum_{t=1}^{g} \sum_{b=1}^{p-1} \sum_{k=bp^{t-1}}^{(b+1)p^{t-1}-1} \rho(k),$$

we obtain

$$\sum_{\mathbf{k} \in \Delta(g)} \rho(\mathbf{k}) = (1 + 2gC(p))^s,$$

where $C(p) = (1/p) \sum_{b=1}^{p-1} 1/\sin(\pi b/p)$. From Niederreiter [9, p. 574, inequality (5)] it follows that $C(p) < (2/\pi) \ln p + 2/5$. An elementary calculation gives the result.

The case of $D_N^*(\omega)$ is completely analogous, one only has to replace the weight function ρ by ρ^*. ∎

THEOREM 3.8 (Weyl Criterion for $\Gamma_p^{(s)}$). *Let ω be a sequence in $[0,1[^s$. Then ω is uniformly distributed modulo one if and only if*

$$\lim_{N \to \infty} S_N(\gamma_{\mathbf{k}}, \omega) = 0, \qquad \forall \mathbf{k} \ne \mathbf{0}. \tag{7}$$

Proof. Let ω be uniformly distributed modulo one. Then

$$\lim_{N \to \infty} S_N(\mathbf{1}_J - \lambda_s(J), \omega) = 0$$

for any subinterval J of $[0,1[^s$. The function $\gamma_{\mathbf{k}}$ is constant on appropriately chosen elementary p-adic intervals I (see Lemma 3.1). Hence, $\gamma_{\mathbf{k}}$ is a finite linear combination of the indicator functions $\mathbf{1}_I$ of such intervals I. This

implies that $S_N(\gamma_{\mathbf{k}}, \omega)$ is a finite linear combination of terms of the form $S_N(\mathbf{1}_I - \lambda_s(I), \omega)$ and, hence, converges to zero if N goes to infinity.

If we assume relation (7), then inequality (6) implies $\lim_{N\to\infty} D_N(\omega) = 0$, from which the uniform distribution of ω follows. ∎

REMARK 3.1. The weight function ρ of the present paper is equal to the weight function ρ_{Walsh} of Hellekalek [2], although the p-adic functions $\gamma_{\mathbf{k}}$ are different from the Walsh functions in base p. When we compare the system $\Gamma_p^{(s)}$ to the Walsh system in base p, there is one important arithmetic aspect to note. The Walsh functions are the appropriate tool for the analysis of those digital sequences and nets where the construction rule involves inner products of digit vectors, and hence is related to the theory of linear codes; see Niederreiter [10, Sec. 4.3], Larcher [8, Sec. 2], Niederreiter and Pirsic [12], Skriganov [15], and Hellekalek [5] for details. In marked contrast to the Walsh system, the system $\Gamma_p^{(s)}$ will be well-suited to study the uniform distribution of sequences ω that stem from elementary arithmetic operations with integers, hence, elements of $\mathbb{Z}_p$, like the van der Corput sequence in base p. The following corollary will illustrate this point of view.

COROLLARY 3.9. *Let $\omega = (x_n)_{n\geq 0}$, $x_n = \varphi(n)$, be the van der Corput sequence in prime base p. Then ω is uniformly distributed modulo one.*

Proof. This is easily seen by the Weyl Criterion for Γ_p: We have $\gamma_k(x_n) = e^{2\pi i \varphi(k) n}$. Hence, for every $k \neq 0$,

$$|S_N(\gamma_k, \omega)| = \frac{1}{N}\left|\frac{e^{2\pi i\varphi(k)N} - 1}{e^{2\pi i\varphi(k)} - 1}\right| \leq \frac{1}{N}\,\frac{1}{|\sin \pi\varphi(k)|}.$$

This implies $\lim_{N\to\infty} S_N(\gamma_k, \omega) = 0$. ∎

Acknowledgements. The author would like to thank Pierre Liardet, CMI, Université de Provence, Marseille, and Hans-Georg Feichtinger, leader of the Numerical Harmonic Analysis Group (NuHAG), University of Vienna, for their hospitality during the research visits where this paper was written.

References

[1] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, Lecture Notes in Math. 1651, Springer, Berlin, 1997.

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

[3] —, *General discrepancy estimates III: the Erdős–Turán–Koksma inequality for the Haar function system*, Monatsh. Math. 120 (1995), 25–45.

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

[5] —, *Digital (t, m, s)-nets and the spectral test*, Acta Arith. 105 (2002), 197–204.

[6] P. Hellekalek and G. Larcher (eds.), *Random and Quasi-Random Point Sets*, Lecture Notes in Statist. 138, Springer, New York, 1998.
[7] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.
[8] G. Larcher, *Digital point sets*, in: Hellekalek and Larcher [6], 167–222.
[9] H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method. III*, Math. Comp. 30 (1976), 571–597.
[10] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.
[11] —, *Nets*, (t, s)*-sequences*, *and codes*, in: Monte Carlo and Quasi-Monte Carlo Methods 2006, A. Keller, S. Heinrich, and H. Niederreiter (eds.), Springer, New York, 2008, 83–100.
[12] H. Niederreiter and G. Pirsic, *Duality for digital nets and its applications*, Acta Arith. 97 (2001), 173–182.
[13] H. Niederreiter and I. E. Shparlinski, *Recent advances in the theory of nonlinear pseudorandom number generators*, in: Monte Carlo and Quasi-Monte Carlo Methods 2000, K.-T. Fang, F. J. Hickernell, and H. Niederreiter (eds.), Springer, New York, 2002, 86–102.
[14] A. M. Robert, *A Course in p-Adic Analysis*, Springer, Berlin, 2000.
[15] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz 13 (2001), no. 2, 191–239 (in Russian); English transl.: St. Petersburg Math. J. 13 (2002), 301–337.

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

Received on 3.11.2008
and in revised form on 21.1.2009 (5845)