ACTA ARITHMETICA
145.3 (2010)

A notion of diaphony based on p-adic arithmetic

by

PETER HELLEKALEK (Salzburg)

1. Introduction. Diaphony is a concept to measure the irregularity of the distribution of sequences on the s-dimensional torus $[0,1[^s$, similar to discrepancy. It is rooted in Fourier analysis and involves weighted Weyl sums relative to a given function system.

The now classical instance of diaphony is based on the trigonometric function system and was introduced by Zinterhof [13], see also Kuipers and Niederreiter [6, Exercise 5.27, p. 162]. The instance of dyadic diaphony, which is based on the Walsh functions in base 2, was introduced by Hellekalek and Leeb [5]. This approach has been transcribed to the case of integer bases $b \geq 2$ and also extended in a series of papers by Grozdanov et al. [2, 1].

There exists an intrinsic relation between the function system that is chosen and the type of constructions of (finite) low-discrepancy sequences that can be analyzed with the associated Weyl sums. Different types of sequences 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 type of Weyl sums with the type of sequences under study. Such suitable "matches" are, for example, the trigonometric functions and good lattice points (see Niederreiter [8, Ch. 5] and Sloan and Joe [12]), and the Walsh functions and digital nets and sequences (see Niederreiter [8, Ch. 4], Larcher [7, Sec. 2], Niederreiter and Pirsic [9], Skriganov [11], and Hellekalek [3] for details).

In this paper, we continue the study begun in Hellekalek [4] to provide the necessary tools for the construction and analysis of new types of low-discrepancy point sets and sequences based on p-adic arithmetic.

Our results are based on the introduction of a $\mathbf{p}$-adic function system $\Gamma_{\mathbf{p}}$ on the s-dimensional torus, $\mathbf{p} = (p_1, \ldots, p_s)$, that is closely related to the

2010 *Mathematics Subject Classification*: Primary 11K06; Secondary 11K38, 11K41, 11K45, 11K70, 11L03.
Key words and phrases: diaphony, Weyl's criterion, p-adic integers, Halton sequence.

DOI: 10.4064/aa145-3-5

product of the dual groups $\hat{\mathbb{Z}}_{p_i}$ of the p_i-adic integers $\mathbb{Z}_{p_i}$. Here, we allow not necessarily distinct prime bases p_i in each coordinate. We prove a version of Weyl's criterion for $\Gamma_{\mathbf{p}}$, from which the uniform distribution of the Halton sequence in base $\mathbf{p}$ follows as a simple corollary. Further, we define a new version of diaphony, the $\mathbf{p}$-*adic diaphony*, prove its essential properties, show an Erdős–Turán–Koksma-type inequality, and compute the $\mathbf{p}$-adic diaphony of regular grids.

2. The function system $\Gamma_{\mathbf{p}}$. Throughout this paper, p denotes a prime, and $\mathbf{p} = (p_1, \ldots, p_s)$ denotes a vector of s primes p_i, $1 \leq i \leq s$, not necessarily distinct. $\mathbb{N}$ stands for the positive integers, and we put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

If $\omega = (\mathbf{x}_n)_{n\geq 0}$ is a—possibly finite—sequence on the torus $[0,1[^s$ with at least N elements, and if $f : [0,1[^s \to \mathbb{C}$, we define

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

For a nonnegative integer a, let $a = \sum_{j\geq 0} a_j p^j$, $a_j \in \{0,1,\ldots,p-1\}$, 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 p-adic representation of the form $x = \sum_{j\geq 0} x_j p^{-j-1}$, $x_j \in \{0,1,\ldots,p-1\}$. If x is a p-*adic rational*, which means that $x = ap^{-g}$ with a and g integers, $0 \leq a < p^g$, $g \in \mathbb{N}$, and if $x \neq 0$, then there are two such representations.

The p-adic representation of x is uniquely determined under the condition that $x_j \neq p-1$ for infinitely many j. In the following, we will call this particular representation the *regular* (p-*adic*) *representation of* x.

Let $\mathbb{Z}_p$ denote the compact group of p-adic integers. We refer the reader to the monograph of Robert [10] for details. An element z of $\mathbb{Z}_p$ will be written as $z = \sum_{j\geq 0} z_j\, p^j$, with digits $z_j \in \{0,1,\ldots,p-1\}$.

Remark 2.1. The set of integers $\mathbb{Z}$ is embedded in $\mathbb{Z}_p$. If $z \in \mathbb{N}_0$, then at most finitely many digits z_j are different from zero. If $z \in \mathbb{Z}$, $z < 0$, then at most finitely many digits z_j are different from $p-1$. In particular, $-1 = \sum_{j\geq 0}(p-1)\, p^j$.

Definition 2.2. An element $z \in \mathbb{Z}_p$ will be called *regular* if infinitely many digits z_j are different from $p-1$. Otherwise, z is called *irregular*.

Remark 2.3. It is easy to see that the set of irregular elements of $\mathbb{Z}_p$ coincides with the set $\{-1,-2,\ldots\}$ of negative integers and that $\mathbb{N}_0$ is contained in the set of regular elements of $\mathbb{Z}_p$.

DEFINITION 2.4. We define the *p-adic Monna map* φ_p by

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

REMARK 2.5. The restriction of φ_p to $\mathbb{N}_0$ is often called the *radical-inverse function.* The Monna map is surjective, but not injective. Furthermore, φ_p gives a bijection between the subset $\mathbb{N}$ of $\mathbb{Z}_p$ of positive integers and the set $\{ap^{-g} : 0 < a < p^g,\ g \in \mathbb{N},\ (a, p^g) = (a,p) = 1\}$ of all reduced p-adic fractions.

The Monna map may be inverted in the following sense.

DEFINITION 2.6. We define the *pseudoinverse* φ_p^+ of the p-adic Monna map φ_p by

$$\varphi_p^+ : [0,1[\to \mathbb{Z}_p, \qquad \varphi_p^+\Big(\sum_{j\geq 0} x_j p^{-j-1}\Big) = \sum_{j\geq 0} x_j p^j,$$

where $\sum_{j\geq 0} x_j p^{-j-1}$ stands for the regular p-adic representation of the element $x \in [0,1[$.

REMARK 2.7. The image of the torus $[0,1[$ under φ_p^+ is the set of regular elements of $\mathbb{Z}_p$. Furthermore, we have the identity $x = \varphi_p(\varphi_p^+(x))$ for all $x \in [0,1[$, but, in general, $z \neq \varphi_p^+(\varphi_p(z))$ for $z \in \mathbb{Z}_p$. For example, if $z = -1$, then $\varphi_p^+(\varphi_p(-1)) = \varphi_p^+(0) = 0 \neq -1$.

The *dual group* $\hat{\mathbb{Z}}_p$ of $\mathbb{Z}_p$ is given by $\hat{\mathbb{Z}}_p = \{\chi_k : k \in \mathbb{N}_0\}$, where

$$\chi_k : \mathbb{Z}_p \to \{c \in \mathbb{C} : |c| = 1\}, \qquad \chi_k\Big(\sum_{j\geq 0} z_j p^j\Big) = e^{2\pi i \varphi_p(k)(z_0 + z_1 p + \cdots)};$$

see Hellekalek [4]. If infinitely many digits z_i are different from zero, we will interpret the value of χ_k as an infinite product of complex numbers. All factors of this product except at most finitely many will be equal to one, and hence the value of χ_k is well-defined.

We now "lift" the characters χ_k to the torus. As in Hellekalek [4], the following function system will be the main tool in our analysis.

DEFINITION 2.8. For a nonnegative integer k, let

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

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

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

There is an obvious generalization of the preceding notions to the higher-dimensional case. In the following, let $\mathbf{p} = (p_1, \ldots, p_s)$ be a vector of s

not necessarily distinct primes p_i, let $\mathbf{x} = (x_1, \ldots, x_s) \in [0,1[^s$, and let $\mathbf{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$. We define

$$\begin{aligned} \varphi_{\mathbf{p}}(\mathbf{k}) &= (\varphi_{p_1}(k_1), \ldots, \varphi_{p_s}(k_s)), \\ \varphi_{\mathbf{p}}^+(\mathbf{x}) &= (\varphi_{p_1}^+(x_1), \ldots, \varphi_{p_s}^+(x_s)), \\ \gamma_{\mathbf{k}}(\mathbf{x}) &= \prod_{i=1}^{s} \gamma_{k_i}(x_i), \qquad \text{where } \gamma_{k_i} \in \Gamma_{p_i},\ 1 \le i \le s, \\ \Gamma_{\mathbf{p}} &= \{\gamma_{\mathbf{k}} : \mathbf{k} \in \mathbb{N}_0^s\}. \end{aligned}$$

It is elementary to show that the family of functions $\Gamma_{\mathbf{p}}$ is an orthonormal system in $L^2([0,1[^s)$. We will see below that it is even an orthonormal basis.

3. The results. For an integrable function f on $[0,1[^s$, the $\mathbf{k}$th Fourier coefficient of f with respect to the function system $\Gamma_{\mathbf{p}}$ is defined as

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

For $\mathbf{g} = (g_1, \ldots, g_s) \in \mathbb{N}_0^s$, we define the following *summation domains*:

$$\begin{aligned} \Delta_{\mathbf{p}}(\mathbf{g}) &= \{\mathbf{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s : 0 \le k_i < p_i^{g_i},\ 1 \le i \le s\}, \\ \Delta_{\mathbf{p}}^*(\mathbf{g}) &= \Delta_{\mathbf{p}}(\mathbf{g}) \setminus \{\mathbf{0}\}. \end{aligned}$$

We will use the standard convention that empty sums have the value zero.

Further, we define the following weight functions. For an integer vector $\mathbf{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$, let

$$\begin{aligned} \rho_{p_i}(k_i) &= \begin{cases} 1 & \text{if } k = 0, \\ p_i^{-2(t_i-1)} & \text{if } p_i^{t_i-1} \le k_i < p_i^{t_i},\ t_i \in \mathbb{N}, \end{cases} \\ \rho_{\mathbf{p}}(\mathbf{k}) &= \prod_{i=1}^{s} \rho_{p_i}(k_i). \end{aligned}$$

Lemma 3.1. *Let* $\mathbf{p}$ *and* $\mathbf{g}$ *be as above. Then:*

(i) *The sum* $\sigma_{\mathbf{p}}$ *over all weights* $\rho_{\mathbf{p}}(\mathbf{k})$ *is given by*

$$\sigma_{\mathbf{p}} = \sum_{\mathbf{k} \in \mathbb{N}_0^s} \rho_{\mathbf{p}}(\mathbf{k}) = \prod_{i=1}^{s} (p_i + 1).$$

(ii) *For the truncated sum* $\sigma_{\mathbf{p}}(\mathbf{g})$,

$$\sigma_{\mathbf{p}}(\mathbf{g}) = \sum_{\mathbf{k} \in \Delta_{\mathbf{p}}(\mathbf{g})} \rho_{\mathbf{p}}(\mathbf{k}) = \prod_{i=1}^{s} (p_i + 1 - p_i^{-g_i+1}).$$

Proof. The claim is easily established by elementary calculations. ∎

The following function will allow for a compact notation. For $k \in \mathbb{N}_0$, with p-adic representation $k = k_0 + k_1 p + \cdots$, we define

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

If $\mathbf{k} \in \mathbb{N}_0^s$, then let $v_{\mathbf{p}}(\mathbf{k}) = (v_{p_1}(k_1), \ldots, v_{p_s}(k_s))$.

Definition 3.2. A $\mathbf{p}$-adic elementary interval, or $\mathbf{p}$-*adic elint* for short, is a subinterval $I_{\mathbf{c},\mathbf{g}}$ of $[0,1[^s$ of the form

$$I_{\mathbf{c},\mathbf{g}} = \prod_{i=1}^{s} [\varphi_{p_i}(c_i), \varphi_{p_i}(c_i) + p_i^{-g_i}[,$$

where the parameters are subject to the conditions $\mathbf{g} = (g_1, \ldots, g_s) \in \mathbb{N}_0^s$, $\mathbf{c} = (c_1, \ldots, c_s) \in \mathbb{N}_0^s$, and $0 \leq c_i < p_i^{g_i}$, $1 \leq i \leq s$.

Remark 3.3. In the "classical" form, the p-adic elint $I_{\mathbf{c},\mathbf{g}}$ is written as $I_{\mathbf{c},\mathbf{g}} = \prod_{i=1}^{s} [a_i p_i^{-g_i}, (a_i + 1) p_i^{-g_i}[$, where $\varphi_{p_i}(c_i) = a_i p_i^{-g_i}$, with $a_i \in \mathbb{N}_0$, $0 \leq a_i < p_i^{g_i}$, $1 \leq i \leq s$.

Let λ denote the Lebesgue measure on $[0,1[^s$. The following lemma shows that, in the language of Fourier analysis, the characteristic function $\mathbf{1}_I$ of a $\mathbf{p}$-adic elint I is a $\Gamma_{\mathbf{p}}$-polynomial.

Lemma 3.4. *Let $I_{\mathbf{c},\mathbf{g}}$ be a p-adic elint, and let $f = \mathbf{1}_{I_{\mathbf{c},\mathbf{g}}} - \lambda(I_{\mathbf{c},\mathbf{g}})$. Then:*

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

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

(ii) *The following identity holds pointwise:*

$$f(\mathbf{x}) = \sum_{\mathbf{k} \in \Delta_{\mathbf{p}}^*(\mathbf{g})} \hat{\mathbf{1}}_{I_{\mathbf{c},\mathbf{g}}}(\mathbf{k}) \gamma_{\mathbf{k}}(\mathbf{x}), \qquad \forall \mathbf{x} \in [0,1[^s. \tag{1}$$

Proof. The proof of this lemma is completely analogous to the proof of Lemma 3.5 in Hellekalek [4], and hence will be omitted. ∎

Lemma 3.5. *For every $\mathbf{k} \neq \mathbf{0}$, $\gamma_{\mathbf{k}}$ is a step function given by*

$$\gamma_{\mathbf{k}}(\mathbf{x}) = \sum_{\mathbf{c} \in \Delta_{\mathbf{p}}(v_{\mathbf{p}}(\mathbf{k}))} e^{2\pi i \langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{c} \rangle} \mathbf{1}_{I_{\mathbf{c}, v_{\mathbf{p}}(\mathbf{k})}}(\mathbf{x}), \qquad \forall \mathbf{x} \in [0,1[^s,$$

where $\langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{c} \rangle$ denotes the inner product of the two vectors $\varphi_{\mathbf{p}}(\mathbf{k})$ and $\mathbf{c}$.

Proof. Let $\mathbf{g} = v_{\mathbf{p}}(\mathbf{k})$. The family of $\mathbf{p}$-adic elints $\{I_{\mathbf{c},\mathbf{g}} : \mathbf{c} \in \Delta_{\mathbf{p}}(\mathbf{g})\}$ is a partition of $[0,1[^s$. From the definition of the function $\gamma_{\mathbf{k}}$ it follows that $\gamma_{\mathbf{k}}$ is constant on each $I_{\mathbf{c},\mathbf{g}}$ with value $e^{2\pi i \langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{c} \rangle}$. This establishes our claim. ∎

Remark 3.6. Lemmas 3.4 and 3.5 generalize results of Hellekalek [4], where the interested reader will find further details on this topic.

DEFINITION 3.7. The sum $S_N(\gamma_{\mathbf{k}},\omega)$ will be called the $\mathbf{k}$*th Weyl sum* associated with the sequence ω and the function system $\Gamma_{\mathbf{p}}$.

In the following corollary, we establish an interesting relation between the Weyl sums $S_N(\gamma_{\mathbf{k}},\omega)$ and the so-called local discrepancies $S_N(\mathbf{1}_I-\lambda(I),\omega)$, for $\mathbf{p}$-adic elints I.

COROLLARY 3.8. *Let ω be a sequence in $[0,1[^s$. Then:*

(i) *For every $\mathbf{p}$-adic elint $I_{\mathbf{c},\mathbf{g}}$,*

$$S_N(\mathbf{1}_{I_{\mathbf{c},\mathbf{g}}}-\lambda(I_{\mathbf{c},\mathbf{g}}),\omega)=\sum_{\mathbf{k}\in\Delta^*_{\mathbf{p}}(\mathbf{g})}\hat{\mathbf{1}}_{I_{\mathbf{c},\mathbf{g}}}(\mathbf{k})S_N(\gamma_{\mathbf{k}},\omega). \tag{2}$$

(ii) *For every nontrivial function $\gamma_{\mathbf{k}}$ (i.e., $\mathbf{k}\neq\mathbf{0}$),*

$$S_N(\gamma_{\mathbf{k}},\omega)=\sum_{\mathbf{c}\in\Delta_{\mathbf{p}}(\mathbf{g})}e^{2\pi i\langle\varphi_{\mathbf{p}}(\mathbf{k}),\mathbf{c}\rangle}S_N(\mathbf{1}_{I_{\mathbf{c},\mathbf{g}}}-\lambda(I_{\mathbf{c},\mathbf{g}}),\omega), \tag{3}$$

where $\mathbf{g}$ is defined as $\mathbf{g}=v_{\mathbf{p}}(\mathbf{k})$.

Proof. This is easy to see. Identity (2) follows directly from Lemma 3.4. To verify identity (3), we note that $\sum_{\mathbf{c}\in\Delta_{\mathbf{p}}(\mathbf{g})}e^{2\pi i\langle\varphi_{\mathbf{p}}(\mathbf{k}),\mathbf{c}\rangle}\lambda(I_{\mathbf{c},\mathbf{g}})=0$, which is elementary to prove. Lemma 3.5 then implies the result. ∎

LEMMA 3.9. *A sequence ω is uniformly distributed in $[0,1[^s$ if and only if*

$$\lim_{N\to\infty}S_N(\mathbf{1}_I-\lambda(I),\omega)=0$$

for all $\mathbf{p}$-adic elints I in $[0,1[^s$.

Proof. If ω is uniformly distributed then, by definition, we deduce that $\lim_{N\to\infty}S_N(\mathbf{1}_J-\lambda(J),\omega)=0$ for all subintervals J of $[0,1[^s$. In particular, this property holds for $\mathbf{p}$-adic elints.

On the other hand, let us assume $\lim_{N\to\infty}S_N(\mathbf{1}_I-\lambda(I),\omega)=0$ for all $\mathbf{p}$-adic elints I. Let J be an arbitrary interval in $[0,1[^s$. We have to show that $\lim_{N\to\infty}S_N(\mathbf{1}_J-\lambda(J),\omega)=0$.

Consider the following approximation argument, adapted from the proof of Theorem 3.6 in Hellekalek [4]. Let $\mathbf{g}=(g_1,\dots,g_s)\in\mathbb{N}^s$ be arbitrarily chosen. We consider the partition of $[0,1[^s$ given by the family of $\mathbf{p}$-adic elints $\mathcal{I}_{\mathbf{g}}=\{I_{\mathbf{c},\mathbf{g}}:\mathbf{c}\in\Delta_{\mathbf{p}}(\mathbf{g})\}$. Define $\underline{J}$ as the union of those elints $I\in\mathcal{I}_{\mathbf{g}}$ that are contained in J, $\underline{J}=\bigcup_{I\,:\,I\subseteq J}I$. Further, let $\overline{J}$ denote the union of all elints $I\in\mathcal{I}_{\mathbf{g}}$ with nonempty intersection with J, $\overline{J}=\bigcup_{I\,:\,I\cap J\neq\emptyset}I$. Then $\underline{J}\subseteq J\subseteq\overline{J}$, where $\underline{J}$ may be void. It is elementary to see that

$$\begin{aligned}|S_N(\mathbf{1}_J-\lambda_s(J),\omega)|&\le\lambda(\overline{J})-\lambda(\underline{J})\\&\quad+\max\{|S_N(\mathbf{1}_{\underline{J}}-\lambda(\underline{J}),\omega)|,|S_N(\mathbf{1}_{\overline{J}}-\lambda(\overline{J}),\omega)|\}.\end{aligned}$$

In every coordinate i, the side lengths of $\underline{J}$ and $\overline{J}$ differ at most by $2p_i^{-g_i}$. Hence, by an application of Lemma 3.9 of Niederreiter [8], we obtain the bound $\lambda(\overline{J}) - \lambda(\underline{J}) \le s\delta$, where $\delta = \max_{1\le i\le s} 2p_i^{-g_i}$.

The sets $\overline{J}$ and $\underline{J}$ are finite disjoint unions of elints $I \in \mathcal{I}_{\mathbf{g}}$. As a consequence, $S_N(\mathbf{1}_{\overline{J}} - \lambda(\overline{J}), \omega)$ is a finite sum of terms $S_N(\mathbf{1}_I - \lambda(I), \omega)$, with appropriate elints $I \in \mathcal{I}_{\mathbf{g}}$. The same is true for $S_N(\mathbf{1}_{\underline{J}} - \lambda(\underline{J}), \omega)$. From the underlying assumption it follows that

$$\limsup_{N\to\infty} |S_N(\mathbf{1}_J - \lambda(J), \omega)| \le s\delta.$$

The parameter $\mathbf{g}$ was arbitrary. Hence, δ can be made arbitrarily small. This implies that $\lim_{N\to\infty} S_N(\mathbf{1}_J - \lambda(J), \omega)$ exists and is equal to zero. ∎

Corollary 3.10. *The set of finite linear combinations of elements of $\Gamma_{\mathbf{p}}$ is dense in the set of functions $\mathbf{1}_J$, J an arbitrary subinterval of $[0,1[^s$, in the Hilbert space $L^2([0,1[^s)$.*

Proof. This follows from identity (1) and from the proof of Lemma 3.9 above. Hence, $\Gamma_{\mathbf{p}}$ is not only an ONS, but even an ONB of $L^2([0,1[^s)$. ∎

In [4, Theorem 3.8], Weyl's criterion was proved in the special case $\mathbf{p} = (p, \ldots, p)$. We generalize this result as follows and give a slightly different proof.

Theorem 3.11 (Weyl's criterion for $\Gamma_{\mathbf{p}}$). *Let ω be a sequence in $[0,1[^s$. Then ω is uniformly distributed in $[0,1[^s$ if and only if*

$$\lim_{N\to\infty} S_N(\gamma_{\mathbf{k}}, \omega) = 0, \qquad \forall \mathbf{k} \ne \mathbf{0}. \tag{4}$$

Proof. Let ω be uniformly distributed in $[0,1[^s$. Then, by Lemma 3.9, $\lim_{N\to\infty} S_N(\mathbf{1}_I - \lambda(I), \omega) = 0$ for any $\mathbf{p}$-adic elint I. In identity (3) of Corollary 3.8, the summation domain $\Delta_{\mathbf{p}}(\mathbf{g})$ is finite. Hence, the uniform distribution of ω implies relation (4).

For the inverse direction, let us assume relation (4). In identity (2) of Corollary 3.8, the summation domain $\Delta^*_{\mathbf{p}}(\mathbf{g})$ is finite. As a consequence, relation (4) implies $\lim_{N\to\infty} S_N(\mathbf{1}_I - \lambda_s(I), \omega) = 0$ for any $\mathbf{p}$-adic elint I. From Lemma 3.9, the uniform distribution of ω follows. ∎

Corollary 3.12. *Let $\omega = (\mathbf{x}_n)_{n\ge 0}$, $\mathbf{x}_n = (\varphi_{p_1}(n), \ldots, \varphi_{p_s}(n))$, be the Halton sequence in base $\mathbf{p} = (p_1, \ldots, p_s)$, with different primes p_i. Then ω is uniformly distributed in $[0,1[^s$.*

Proof. This is easily seen by Weyl's criterion for $\Gamma_{\mathbf{p}}$. We have $\gamma_{\mathbf{k}}(\mathbf{x}_n) = \prod_{j=1}^s e^{2\pi i \varphi_{p_j}(k_j) n}$. Hence, for every $\mathbf{k} \ne \mathbf{0}$,

$$|S_N(\gamma_{\mathbf{k}}, \omega)| = \frac{1}{N} \left| \frac{e^{2\pi i \langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{1}\rangle N} - 1}{e^{2\pi i \langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{1}\rangle} - 1} \right| \le \frac{1}{N} \frac{1}{|\sin \pi \langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{1}\rangle|},$$

where $\mathbf{1} = (1, \dots, 1)$, and thus, $\langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{1} \rangle = \varphi_{p_1}(k_1) + \dots + \varphi_{p_s}(k_s)$. It is easily seen that the condition $p_i \neq p_j$ for $i \neq j$ implies $\langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{1} \rangle \notin \mathbb{Z}$. Hence, $\lim_{N\to\infty} S_N(\gamma_{\mathbf{k}}, \omega) = 0$. ∎

We now introduce the **p**-adic diaphony, which is defined as the following sum of weighted Weyl sums for $\Gamma_{\mathbf{p}}$.

DEFINITION 3.13. Let $\mathbf{p} = (p_1, \dots, p_s)$, where all p_i are prime, not necessarily distinct. The **p**-*adic diaphony* $F_N(\omega)$ of the first N elements of a sequence $\omega = (\mathbf{x}_n)_{n\geq 0}$ in $[0,1[^s$ is defined by

$$F_N(\omega) = \left(\frac{1}{\sigma_{\mathbf{p}} - 1} \sum_{\mathbf{k}\neq\mathbf{0}} \rho_{\mathbf{p}}(\mathbf{k}) \, |S_N(\gamma_{\mathbf{k}}, \omega)|^2 \right)^{1/2},$$

where $\sigma_{\mathbf{p}} = \prod_{i=1}^{s} (p_i + 1)$.

In the following theorem, we prove that F_N is a measure of uniform distribution of sequences in $[0,1[^s$.

THEOREM 3.14. *Let ω be a sequence in $[0,1[^s$. Then, for the* **p**-*adic diaphony F_N:*

(i) *F_N is normalized:* $0 \leq F_N(\omega) \leq 1$.
(ii) *ω is uniformly distributed in $[0,1[^s$ if and only if* $\lim_{N\to\infty} F_N(\omega) = 0$.

Proof. For every $\mathbf{k}$, $|S_N(\gamma_{\mathbf{k}}, \omega)| \leq 1$. Thus, Lemma 3.1 implies (i).

In (ii), let $\lim_{N\to\infty} F_N(\omega) = 0$. As a consequence, $\lim_{N\to\infty} S_N(\gamma_{\mathbf{k}}, \omega) = 0$ for all $\mathbf{k} \neq \mathbf{0}$. Theorem 3.11, Weyl's criterion, implies the uniform distribution of ω.

On the other hand, let ω be uniformly distributed in $[0,1[^s$. Let $\mathbf{g} = (g_1, \dots, g_s) \in \mathbb{N}^s$ be arbitrary. Then we have the following upper bound:

$$F_N^2(\omega) \leq \frac{1}{\sigma_{\mathbf{p}} - 1} \sum_{\mathbf{k}\in\Delta^*_{\mathbf{p}}(\mathbf{g})} \rho_{\mathbf{p}}(\mathbf{k}) |S_N(\gamma_{\mathbf{k}}, \omega)|^2 + \frac{1}{\sigma_{\mathbf{p}} - 1} \sum_{\mathbf{k}\in\mathbb{N}_0^s \setminus \Delta_{\mathbf{p}}(\mathbf{g})} \rho_{\mathbf{p}}(\mathbf{k}).$$

This yields the inequality

$$F_N^2(\omega) \leq \frac{1}{\sigma_{\mathbf{p}} - 1} \sum_{\mathbf{k}\in\Delta^*_{\mathbf{p}}(\mathbf{g})} \rho_{\mathbf{p}}(\mathbf{k}) |S_N(\gamma_{\mathbf{k}}, \omega)|^2 + \frac{\sigma_{\mathbf{p}} - \sigma_{\mathbf{p}}(\mathbf{g})}{\sigma_{\mathbf{p}} - 1}. \tag{5}$$

From the uniform distribution of ω it follows, by an application of Weyl's criterion, that $\lim_{N\to\infty} S_N(\gamma_{\mathbf{k}}, \omega) = 0$ for all $\mathbf{k} \neq \mathbf{0}$. The summation domain $\Delta^*_{\mathbf{p}}(\mathbf{g})$ is finite, hence

$$\limsup_{N\to\infty} F_N^2(\omega) \leq \frac{\sigma_{\mathbf{p}} - \sigma_{\mathbf{p}}(\mathbf{g})}{\sigma_{\mathbf{p}} - 1}.$$

The difference $\sigma_{\mathbf{p}} - \sigma_{\mathbf{p}}(\mathbf{g})$ can be made arbitrarily small, by increasing every component g_i of the vector $\mathbf{g}$. This implies the existence of $\lim_{N\to\infty} F_N^2(\omega)$. Further, $\lim_{N\to\infty} F_N^2(\omega) = 0$, which establishes claim (ii). ∎

From inequality (5), we derive the inequality of Erdős–Turán–Koksma for the $\mathbf{p}$-adic diaphony:

Corollary 3.15.

$$F_N^2(\omega) \leq \frac{1}{\sigma_{\mathbf{p}} - 1} \sum_{\mathbf{k} \in \Delta^*_{\mathbf{p}}(\mathbf{g})} \rho_{\mathbf{p}}(\mathbf{k}) |S_N(\gamma_{\mathbf{k}}, \omega)|^2 + \frac{\sigma_{\mathbf{p}}}{\sigma_{\mathbf{p}} - 1} sw,$$

where $w = \max_i (p_i + 1)^{-1} p_i^{-g_i+1}$.

Proof. This is due to the fact that, by applying Lemma 3.9 of Niederreiter [8],

$$1 - \frac{\sigma_{\mathbf{p}}(\mathbf{g})}{\sigma_{\mathbf{p}}} = 1 - \prod_{i=1}^{s} (1 - (p_i + 1)^{-1} p_i^{-g_i+1}) \leq 1 - (1 - w)^s,$$

which is easily seen to be bounded by sw. ∎

The next result shows that the diaphony of a regular p-adic grid consisting of $N = p^{gs}$ points has an order of magnitude of $N^{-1/s}$, up to a power of $\log N$.

Theorem 3.16. *Let* $\mathbf{p} = (p, \ldots, p)$, *where* p *is a prime, let* $g \in \mathbb{N}$, *and let* ω *denote the regular* p*-adic grid with mesh width* p^{-g} *in every coordinate,*

$$\omega = ((a_1 p^{-g}, \ldots, a_s p^{-g}))_{a_1=0,\ldots,a_s=0}^{p^g-1,\ldots,p^g-1}.$$

Then, with $N = p^{gs}$ *denoting the number of elements of* ω*:*

(i) *The* $\mathbf{p}$*-adic diaphony* $F_N(\omega)$ *is given by the identity*

$$((p + 1)^s - 1) F_N^2(\omega) = (1 + \Sigma)^s - 1,$$

where $\Sigma = \sum_{k \geq p^g} \rho_p(k) |S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})|^2$.

(ii) *There exist positive constants* C_1 *and* C_2, *explicitly computable and depending only on the dimension* s *and on the base* p, *such that*

$$C_1 \frac{1}{N^{1/s}} \leq F_N(\omega) \leq C_2 \frac{\sqrt{\log_p N}}{N^{1/s}},$$

where $\log_p N$ *denotes the logarithm of* N *to the base* p.

Remark 3.17. The number $p^{-1/2} \Sigma^{1/2}$ is the p-adic diaphony of the one-dimensional sequence $(ap^{-g})_{a=0}^{p^g-1}$. This follows from identity (6) below.

Proof of Theorem 3.16. It is easy to see that

$$S_N(\gamma_{\mathbf{k}}, \omega) = \frac{1}{N} \sum_{\mathbf{a} \in \Delta_{\mathbf{p}}(\mathbf{g})} e^{2\pi i \langle \varphi_{\mathbf{p}}(\mathbf{k}), \mathbf{a} \rangle}$$

with $\mathbf{g} = (g, \dots, g)$. Because of the independence of the coordinates, we may write

$$S_N(\gamma_{\mathbf{k}}, \omega) = \prod_{j=1}^{s} \frac{1}{p^g} \sum_{a_j=0}^{p^g-1} e^{2\pi i \varphi_p(k_j) a_j}.$$

For the one-dimensional sum $p^{-g} \sum_{a=0}^{p^g-1} e^{2\pi i \varphi_p(k) a} = S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})$, we get

$$\text{(6)} \qquad \frac{1}{p^g} \sum_{a=0}^{p^g-1} e^{2\pi i \varphi_p(k) a} = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{if } 1 \le k < p^g, \\ \dfrac{1}{p^g} \dfrac{\sin(\pi \varphi_p(k) p^g)}{\sin(\pi \varphi_p(k))} \dfrac{e^{\pi i \varphi_p(k) p^g}}{e^{\pi i \varphi_p(k)}} & \text{if } k \ge p^g. \end{cases}$$

The domain $\mathbb{N}_0^s \setminus \{\mathbf{0}\}$ can be split into disjoint subsets A and $V(t)$, $0 \le t \le s-1$, where $A = \{\mathbf{k} \in \mathbb{N}_0^s : \exists i, 1 \le i \le s, \text{ such that } 1 \le k_i < p^g\}$, and $V(t)$ is defined as the set of all $\mathbf{k} \in \mathbb{N}_0^s$ such that exactly t coordinates of the vector $\mathbf{k}$ are zero and the remaining $s-t$ coordinates are larger or equal to p^g,

$$\mathbb{N}_0^s \setminus \{\mathbf{0}\} = A \cup \bigcup_{t=0}^{s-1} V(t).$$

We note that $\sigma_{\mathbf{p}} = (p+1)^s$. Hence, we obtain the following formula for the $\mathbf{p}$-adic diaphony:

$$\begin{aligned} ((p+1)^s - 1) F_N^2(\omega) &= \sum_{t=0}^{s-1} \sum_{\mathbf{k} \in V(t)} \rho_{\mathbf{p}}(\mathbf{k}) |S_N(\gamma_{\mathbf{k}}, \omega)|^2 \\ &= \sum_{t=0}^{s-1} \binom{s}{t} \Sigma^{s-t} = (1+\Sigma)^s - 1, \end{aligned}$$

where

$$\Sigma = \sum_{k \ge p^g} \rho_p(k) |S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})|^2.$$

This proves part (i) of the theorem.

For the lower bound for $F_N(\omega)$, we note that $((p+1)^s - 1) F_N^2(\omega) \ge s\Sigma$. We will show that $\Sigma \ge 4\pi^{-2} p^{-2g} = 4\pi^{-2} N^{-2/s}$.

If we consider only the first term in Σ, for $k = p^g$, then we obtain the bound

$$\Sigma \ge \rho_p(p^g) |S_{p^g}(\gamma_{p^g}, (ap^{-g})_{a=0}^{p^g-1})|^2.$$

We have $\rho_p(p^g) = 1/p^{2g}$ and $\varphi_p(p^g) = 1/p^{g+1}$. Further, for any x, $0 \le x \le 1$, we have $2\langle\!\langle x \rangle\!\rangle \le \sin \pi x \le \pi \langle\!\langle x \rangle\!\rangle$, where $\langle\!\langle x \rangle\!\rangle$ denotes the distance of x to the nearest integer. As a consequence of identity (6), we obtain

$$|S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})| = \frac{1}{p^g} \frac{\sin(\pi/p)}{\sin(\pi/p^{g+1})} \geq \frac{2}{\pi}.$$

Hence, $\Sigma \geq 4\pi^{-2}p^{-2g}$, and we may take $C_1 = 2\pi^{-1}\sqrt{s/((p+1)^s-1)}$.

For the upper bound for $F_N(\omega)$, we note that $((p+1)^s-1)F_N^2(\omega) \leq s2^{s-1}\Sigma$. In Σ, we partition the summation domain $\{k \geq p^g\}$ into the two disjoint subsets $D = \{p^g \leq k < p^{2g+1}\}$ and $E = \{k \geq p^{2g+1}\}$.

From Lemma 3.1, it follows that

$$\sum_{k\in E} \rho_p(k)|S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})|^2 \leq \sum_{k\geq p^{2g+1}} \rho_p(k) = \frac{1}{p^{2g}}.$$

In order to compute $\rho_p(k)$ and $\varphi_p(k)$, we split the summation over D as follows:

$$\begin{aligned}\sum_{k\in D} &\rho_p(k)|S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})|^2 \\ &= \sum_{t=g+1}^{2g+1}\sum_{b=1}^{p-1}\sum_{k=bp^{t-1}}^{(b+1)p^{t-1}-1} \frac{1}{p^{2t-2}}\left(\frac{1}{p^g}\frac{\sin(\pi\varphi_p(k)p^g)}{\sin(\pi\varphi_p(k))}\right)^2 \\ &\leq \frac{1}{p^{2g}}\sum_{t=g+1}^{2g+1}\frac{1}{p^{2t-2}}\sum_{b=1}^{p-1}\sum_{k=bp^{t-1}}^{(b+1)p^{t-1}-1}\frac{1}{4\langle\!\langle\varphi_p(k)\rangle\!\rangle^2}.\end{aligned}$$

If k runs from bp^{t-1} up to $(b+1)p^{t-1}-1$, then $\varphi_p(k)$ runs through all the numbers $a/p^{t-1}+b/p^t$, $0 \leq a \leq p^{t-1}-1$, in some order. For this reason,

$$\sum_{k=bp^{t-1}}^{(b+1)p^{t-1}-1} \frac{1}{\langle\!\langle\varphi_p(k)\rangle\!\rangle^2} = \sum_{a=0}^{p^{t-1}-1}\frac{1}{\langle\!\langle a/p^{t-1}+b/p^t\rangle\!\rangle^2}.$$

It is an elementary, but somewhat tedious task to estimate the last sum by $3p^{2t}(1/b^2+1/(p-b)^2)$. This yields the estimate

$$\sum_{k\in D} \rho_p(k)|S_{p^g}(\gamma_k, (ap^{-g})_{a=0}^{p^g-1})|^2 \leq 6p^2\frac{g}{p^{2g}}.$$

Altogether, we obtain the bound

$$F_N^2(\omega) \leq \frac{2^{s-1}(6p^2+1)}{(p+1)^s-1}\frac{sg}{p^{2g}}.$$

This finishes the proof. ■

Acknowledgements. The author would like to thank Makoto Matsumoto, Hiroshima University, and Hans-Georg Feichtinger, leader of the Numerical Harmonic Analysis Group (NuHAG), University of Vienna, for their hospitality during the research visits where parts of this paper were written, and Harald Niederreiter, University of Salzburg, and RICAM, Austrian Academy of Sciences, Linz, for several helpful comments.

References

[1] V. Grozdanov, *The weighted b-adic diaphony*, J. Complexity 22 (2006), 490–513.
[2] V. Grozdanov and S. Stoilova, *The general diaphony*, C. R. Acad. Bulgare Sci. 57 (2004), 13–18.
[3] P. Hellekalek, *Digital (t, m, s)-nets and the spectral test*, Acta Arith. 105 (2002), 197–204.
[4] —, *A general discrepancy estimate based on p-adic arithmetics*, ibid. 139 (2009), 117–129.
[5] P. Hellekalek and H. Leeb, *Dyadic diaphony*, ibid. 80 (1997), 187–196.
[6] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.
[7] G. Larcher, *Digital point sets: analysis and application*, in: Random and Quasi-Random Point Sets, P. Hellekalek and G. Larcher (eds.), Lecture Notes in Statist. 138, Springer, New York, 1998, 167–222.
[8] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.
[9] H. Niederreiter and G. Pirsic, *Duality for digital nets and its applications*, Acta Arith. 97 (2001), 173–182.
[10] A. M. Robert, *A Course in p-Adic Analysis*, Springer, Berlin, 2000.
[11] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz 13 (2001), 191–239 (in Russian).
[12] I. H. Sloan and S. Joe, *Lattice Methods for Multiple Integration*, Clarendon Press, Oxford, 1994.
[13] P. Zinterhof, *Über einige Abschätzungen bei der Approximation von Funktionen mit Gleichverteilungsmethoden*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 185 (1976), 121–132.

Peter Hellekalek
Department of Mathematics
University of Salzburg
Hellbrunnerstrasse 34
5020 Salzburg, Austria
E-mail: peter.hellekalek@sbg.ac.at

Received on 5.11.2009
and in revised form on 21.4.2010 (6202)