ACTA ARITHMETICA
LXXX.2 (1997)

Dyadic diaphony

by

Peter Hellekalek and Hannes Leeb (Salzburg)

1. Introduction. *Diaphony* (see Zinterhof [13] and Kuipers and Niederreiter [6, Exercise 5.27, p. 162]) is a numerical quantity that measures the irregularity of the distribution of sequences in the s-dimensional unit cube $[0,1[^s$, similar to discrepancy. It has two important features. First, in any dimension, it is computable in $\mathcal{O}(sN^2)$ steps for every sequence of N points. Hence, its complexity is linear in the dimension s. Secondly, it allows theoretical analysis in terms of Weyl sums, again in similarity to discrepancy (see Hellekalek and Niederreiter [4]). For the relation to quasi-Monte Carlo quadrature formulae, see Zinterhof and Stegbuchner [14].

Throughout this paper, $\omega = (\mathbf{x}_n)_{n\geq 0}$ will denote a—possibly finite—sequence in $[0,1[^s$ with at least N elements. For integrable $f:[0,1[^s \to \mathbb{C}$, define

$$S_N(f,\omega) := \frac{1}{N}\sum_{n=0}^{N-1} f(\mathbf{x}_n) - \int\limits_{[0,1[^s} f(\mathbf{x})\,d\mathbf{x}.$$

Let $\mathcal{T}$ denote the trigonometric function system $\{e_{\mathbf{k}} : \mathbf{k}\in\mathbb{Z}^s\}$ on $[0,1[^s$,

$$e_{\mathbf{k}}(\mathbf{x}) := \prod_{i=1}^{s} e^{2\pi\sqrt{-1}k_i x_i},$$

$\mathbf{k} = (k_1,\ldots,k_s) \in \mathbb{Z}^s$, $\mathbf{x} = (x_1,\ldots,x_s) \in [0,1[^s$. $\mathcal{W}(2) = \{w_{\mathbf{k}} : \mathbf{k} = (k_1,\ldots,k_s) \in \mathbb{Z}^s, k_i \geq 0, 1 \leq i \leq s\}$ denotes the system of Walsh functions to the base 2 on $[0,1[^s$ (see Definition 2.1).

Definition 1.1. The *diaphony* $F_N(\mathcal{T},\omega)$ of the first N elements $\mathbf{x}_0,\ldots,\mathbf{x}_{N-1}$ of ω is defined as

1991 *Mathematics Subject Classification*: Primary 65C10; Secondary 11K45.

Key words and phrases: random number generators, weighted spectral test, diaphony, discrepancy, inequality of Erdős–Turán–Koksma, Weyl's Criterion.

Research supported by the Austrian Science Foundation, P11143-MAT.

$$(1) \qquad F_N(\mathcal{T},\omega) := \Big(\sum_{\mathbf{k}\neq \mathbf{0}} \frac{1}{R(\mathbf{k})^2} |S_N(e_{\mathbf{k}},\omega)|^2 \Big)^{1/2},$$

where $R(\mathbf{k}) := \prod_{i=1}^{s} \max\{1,|k_i|\}$, $\mathbf{k} = (k_1,\ldots,k_s) \in \mathbb{Z}^s$.

The spectral test of Coveyou and MacPherson [1] is one of the central theoretical concepts to test uniform pseudorandom number generators. It defines the figure of merit

$$(2) \qquad \sigma_N(\omega) := \frac{1}{\min\{\sqrt{k_1^2+\ldots+k_s^2} : \mathbf{k}\neq\mathbf{0},\ e_{\mathbf{k}}\in\mathcal{T},\ S_N(e_{\mathbf{k}},\omega)\neq 0\}}$$

relative to the trigonometric function system. If the generator produces lattice structures in $[0,1[^s$, like the well-known linear congruential generators, then the spectral test yields readily computable "figures of merit" (see Knuth [5], Ripley [8], and Tezuka [12]). For other types of generators, the situation is different. The following statement of Niederreiter [7, p. 168] applies: *"The difficulty here is to find a convincing quantitative formulation of this idea"*.

In Hellekalek [3] the first author has presented a solution to this problem. He has interpreted the diaphony $F_N(\mathcal{T},\omega)$ as a *weighted* spectral test. The weights are given by the coefficients $1/R(\mathbf{k})^2$.

Tezuka [11] considered a discrete version of (2) for the Walsh system $\mathcal{W}(2)$, namely the behaviour of the Weyl sums

$$(3) \qquad \{S_N(w_{\mathbf{k}},\omega) : \mathbf{k} = (k_1,\ldots,k_s)\neq\mathbf{0},\ 0\leq k_i < 2^g,\ 1\leq i\leq s\},$$

g a fixed positive integer, for finite sequences ω produced by generalized feedback shift register pseudorandom number generators. Neither a quantitative formulation of this *discrete* Walsh spectral test nor something like Tezuka's Walsh spectral test for other types of uniform pseudorandom number generators is known.

Hence, it is an interesting question of metric and computational number theory to investigate if a *dyadic* version of diaphony exists and if it has similar properties and an analogous interpretation as the classical version. In this paper, we shall answer this question.

Definition 1.2. The *dyadic diaphony* $F_N(\mathcal{W}(2),\omega)$ of the first N elements of the sequence ω in $[0,1[^s$ is defined by

$$(4) \qquad F_N(\mathcal{W}(2),\omega) := \Big(\frac{1}{3^s-1} \sum_{\mathbf{k}\neq\mathbf{0}} \varrho(\mathbf{k})\, |S_N(w_{\mathbf{k}},\omega)|^2 \Big)^{1/2},$$

where, for an integer vector $\mathbf{k} = (k_1,\ldots,k_s)$ with nonnegative coordinates k_i,

$$\varrho(\mathbf{k}) := \prod_{i=1}^{s} \varrho(k_i),$$

$$\varrho(k) := \begin{cases} 2^{-2g} & \text{if } 2^g \le k < 2^{g+1} \text{ with } g \ge 0,\ g \in \mathbb{Z}, \\ 1 & \text{if } k = 0. \end{cases} \tag{5}$$

We shall establish that $F_N(\mathcal{W}(2), \omega)$ is a measure of uniform distribution (see Theorem 3.1). As corollaries, we shall obtain Weyl's Criterion relative to the Walsh function system and the inequality of Erdős–Turán–Koksma for $F_N(\mathcal{W}(2), \omega)$. In Proposition 3.4 we shall compute the value of the dyadic diaphony for regular dyadic grids. Then we shall show that the weights $\varrho(\mathbf{k})$ are the Walsh coefficients of a certain function ϕ defined on $[0,1[^s$ (see Corollary 4.4). This property of the dyadic diaphony is essential to allow its computation in $\mathcal{O}(sN^2)$ steps (see Theorem 3.5).

In what follows, we shall denote the dyadic diaphony $F_N(\mathcal{W}(2), \omega)$ of the first N elements of ω by $F_N(\omega)$.

2. Prerequisites. The comprehensive monograph of Schipp, Wade and Simon [9] serves as a reference for all the results we shall need from dyadic Harmonic Analysis.

For a nonnegative integer k, let

$$k = \sum_{j=0}^{\infty} k_j 2^j, \qquad k_j \in \{0,1\},$$

be the unique dyadic expansion of k. Every number $x \in [0,1[$ has a unique dyadic expansion

$$x = \sum_{j=0}^{\infty} x_j \, 2^{-j-1}, \qquad x_j \in \{0,1\},$$

under the condition that $x_j \neq 1$ for infinitely many j. In the following, this uniqueness condition will be assumed without further notice.

Notation. (i) Let $x \in [0,1[$, with dyadic expansion $x = 0.x_0x_1\ldots$, and let k be a nonnegative integer, $k = \sum_{j=0}^{\infty} k_j\, 2^j$. For $g \in \mathbb{N}$, we define

$$x(g) := 0.x_0x_1\ldots x_{g-1}, \qquad k(g) := \sum_{j=0}^{g-1} k_j\, 2^j.$$

Then $x(g) \in \{a \cdot 2^{-g} : a = 0,1,\ldots,2^g - 1\}$ and $k(g) \in \{0,1,\ldots,2^g-1\}$. Further, put $x(0) := 0$, $k(0) := 0$.

(ii) An interval of the form

$$J(g,a) := [a \cdot 2^{-g}, (a+1)\cdot 2^{-g}[, \qquad 0 \le a < 2^g,\ g \ge 0,$$

a and g integers, is called an *elementary dyadic interval* of length 2^{-g}.

(iii) Let $b_0, b_1, \ldots, b_{g-1}$ be arbitrary digits in $\{0,1\}$. Let

$$I(b_0, b_1, \ldots, b_{g-1}) := \{x \in [0,1[\, : x_j = b_j, \ 0 \le j \le g-1\}$$

denote the *cylinder set of order g defined by* $b_0, b_1, \ldots, b_{g-1}$. Then, for any elementary dyadic interval $J(g,a)$ of length 2^{-g}, $g \in \mathbb{N}$, there is a unique cylinder set $I(b_0, b_1, \ldots, b_{g-1})$ such that $J(g,a) = I(b_0, b_1, \ldots, b_{g-1})$. We only have to observe that $a \cdot 2^{-g} = 0.b_0 b_1 \ldots b_{g-1}$ with suitable digits b_j.

(iv) Let λ denote the Lebesgue measure on $[0,1[$.

(v) By a *dyadic rational c*, we understand an element $c = 0.c_0 c_1 \ldots \in [0,1[$ such that only finitely many digits c_j are different from zero.

(vi) The dyadic logarithm of $x \in [0,1[$ will be denoted by $\log_2 x$. If $x = 2^{-g} + x_g 2^{-g-1} + \ldots$, then the integer part of $\log_2 x$ is given by $\lfloor \log_2 x \rfloor = -g$.

Definition 2.1. The kth *Walsh function* w_k, $k \ge 0$, to the base 2 is defined as

$$w_k(x) := \prod_{j=0}^{\infty} (-1)^{x_j k_j}, \tag{6}$$

where $x = 0.x_0 x_1 \ldots$ is the unique dyadic expansion of $x \in [0,1[$ and $k = \sum_{j=0}^{\infty} k_j \, 2^j$ is the unique dyadic expansion of the nonnegative integer k. If $\mathbf{k} = (k_1, \ldots, k_s)$ is an integer vector with nonnegative coordinates, then the $\mathbf{k}$th *Walsh function* $w_{\mathbf{k}}$ on $[0,1[^s$ is defined as

$$w_{\mathbf{k}}(\mathbf{x}) := \prod_{i=1}^{s} w_{k_i}(x_i), \qquad \mathbf{x} = (x_1, \ldots, x_s) \in [0,1[^s. \tag{7}$$

If ϕ is an integrable function on $[0,1[^s$ and if $\mathbf{k} = (k_1, \ldots, k_s)$ is an integer vector with nonnegative coordinates, then let $\widehat{\phi}(\mathbf{k})$ denote the $\mathbf{k}$th Walsh coefficient of ϕ,

$$\widehat{\phi}(\mathbf{k}) := \int\limits_{[0,1[^s} \phi(\mathbf{x}) w_{\mathbf{k}}(\mathbf{x}) \, d\mathbf{x},$$

with respect to the Walsh function $w_{\mathbf{k}}$.

Definition 2.2. For two digits d and d' in $\{0,1\}$, let

$$d \oplus d' := d + d' \pmod 2.$$

For two numbers $x, y \in [0,1[$ with dyadic expansions $x = \sum_{j=0}^{\infty} x_j \, 2^{-j-1}$ and $y = \sum_{j=0}^{\infty} y_j \, 2^{-j-1}$, let $x \dot{+} y$ denote the *dyadic sum* of x and y,

$$x \dot{+} y := \sum_{j=0}^{\infty} (x_j \oplus y_j) \, 2^{-j-1} \pmod 1.$$

If $\mathbf{x}, \mathbf{y} \in [0,1[^s$, $\mathbf{x} = (x_1, \ldots, x_s)$, $\mathbf{y} = (y_1, \ldots, y_s)$, then

$$\mathbf{x} \dot{+} \mathbf{y} := (x_1 \dot{+} y_1, \ldots, x_s \dot{+} y_s).$$

Remark 2.1. (1) The digits $(x \dot{+} y)_j$ of the dyadic expansion of the number $x \dot{+} y \in [0,1[$ need not coincide with $x_j \oplus y_j$. Each of the following conditions:

(C1) $x \dot{+} y$ *not* a dyadic rational,

(C2) x or y dyadic rationals,

implies the equality

$$(x \dot{+} y)_j = x_j \oplus y_j, \qquad \forall j \geq 0. \tag{8}$$

(2) If the above identity (8) holds for $x, y \in [0,1[$, then

$$w_k(x \dot{+} y) = w_k(x)\, w_k(y). \tag{9}$$

For functions $\varphi, \psi \in L^1([0,1[)$ and $x \in [0,1[$, we define the *convolution* $\varphi * \psi$ of φ and ψ as

$$\varphi * \psi(x) := \int\limits_{[0,1[} \varphi(t)\, \psi(t \dot{+} x)\, dt. \tag{10}$$

As in the case of the trigonometric function system,

$$\widehat{\varphi * \psi}(k) = \widehat{\varphi}(k)\widehat{\psi}(k) \qquad \forall k \geq 0.$$

3. The results. In this section we present the main results of this paper. For the definition of the Walsh functions and the dyadic sum, we refer to Section 2.

Theorem 3.1. *Let* $\omega = (\mathbf{x}_n)_{n \geq 0}$ *be a sequence in* $[0,1[^s$. *Then*, *for the dyadic diaphony* $F_N(\omega)$,

(a) $$0 \leq F_N(\omega) \leq 1,$$

(b) $$\omega \textit{ is uniformly distributed} \bmod 1 \Leftrightarrow \lim_{N\to\infty} F_N(\omega) = 0.$$

Proof. Property (a) is trivial. In (b), let $\lim_{N\to\infty} F_N(\omega) = 0$. Then $\lim_{N\to\infty} S_N(w_{\mathbf{k}}, \omega) = 0$ for every $\mathbf{k} \neq \mathbf{0}$. From Lemma 2 in Hellekalek [2] it follows that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n) = 0 \tag{11}$$

for all functions $f(\mathbf{x}) = \mathbf{1}_I(\mathbf{x}) - \lambda(I)$, where I is a dyadic subinterval of $[0,1[^s$ and $\lambda(I)$ is its Lebesgue measure. This implies the uniform distribution modulo one of ω.

On the other hand, let ω be uniformly distributed in $[0,1[^s$. For $g \in \mathbb{N}$, define

$$C_s(2^g) := \{\mathbf{k} = (k_1, \ldots, k_s) : 0 \leq k_i < 2^g,\ 1 \leq i \leq s\},$$

and

$$C_s^*(2^g) := C_s(2^g) \setminus \{\mathbf{0}\}.$$

Then

$$\sum_{\mathbf{k}\neq\mathbf{0}} \varrho(\mathbf{k}) = 3^s - 1, \qquad \sum_{\mathbf{k}\in C_s^*(2^g)} \varrho(\mathbf{k}) = (3-2^{-(g-1)})^s - 1,$$

and hence

$$\sum_{\mathbf{k}\notin C_s(2^g)} \varrho(\mathbf{k}) \le 3^{s-1}\cdot\frac{s}{2^{g-1}}.$$

This yields the estimate

$$F_N^2(\omega) \le \frac{1}{3^s-1}\sum_{\mathbf{k}\in C_s^*(2^g)} \varrho(\mathbf{k})|S_N(w_{\mathbf{k}},\omega)|^2 + \frac{3^{s-1}}{3^s-1}\cdot\frac{s}{2^{g-1}}. \tag{12}$$

Now, every Walsh function $w_{\mathbf{k}}$ is a step function on $[0,1[^s$. Hence, the uniform distribution of ω implies $\lim_{N\to\infty} S_N(w_{\mathbf{k}},\omega)=0$. The result follows. ∎

From Theorem 3.1 and its proof we get

Corollary 3.2 (Weyl's Criterion relative to $\mathcal{W}(2)$).

$$\omega \textit{ is uniformly distributed } \bmod 1 \Leftrightarrow \lim_{N\to\infty} S_N(w_{\mathbf{k}},\omega)=0\ \forall\mathbf{k}\neq\mathbf{0}.$$

The one-dimensional version of this result has been presented without proof in Sloss and Blyth [10, Theorem 1].

From inequality (12) we obtain an upper bound for $F_N(\omega)$ in terms of the Weyl sums $S_N(w_{\mathbf{k}},\omega)$ over finite domains $C_s^*(2^g)$, the so-called *inequality of Erdős–Turán–Koksma*:

Corollary 3.3.

$$F_N^2(\omega) \le \frac{s}{2^g}\cdot\frac{2}{3}\cdot\frac{1}{1-3^{-s}} + \frac{1}{3^s-1}\sum_{\mathbf{k}\in C_s^*(2^g)} \varrho(\mathbf{k})|S_N(w_{\mathbf{k}},\omega)|^2. \tag{13}$$

The next result shows that the dyadic diaphony of a regular dyadic grid consisting of $N=2^{gs}$ points has an order of magnitude of $N^{-1/s}$.

Proposition 3.4. *Let ω be the regular dyadic grid*

$$\{(a_1/2^g,\ldots,a_s/2^g) : 0\le a_i < 2^g,\ a_i\in\mathbb{Z},\ 1\le i\le s\}. \tag{14}$$

Then

$$F_{2^{gs}}^2(\omega) = \frac{1}{3^s-1}((1+2^{-2g+1})^s - 1). \tag{15}$$

Proof. It is elementary to show that

$$S_{2^g}\big(w_k,(a\cdot 2^{-g})_{a=0}^{2^g-1}\big) = \begin{cases} 1 & \text{if } 2^g \mid k,\\ 0 & \text{otherwise.}\end{cases}$$

From this identity, the final result follows easily. ∎

THEOREM 3.5. *Let*

$$\varphi(x) := \begin{cases} 3 - 3 \cdot 2^{1+\lfloor \log_2 x \rfloor} & \text{if } x \in \,]0,1[, \\ 3 & \text{if } x = 0, \end{cases} \tag{16}$$

and $\phi : [0,1[^s \to \mathbb{R}$,

$$\phi(\mathbf{x}) := -1 + \prod_{i=1}^{s} \varphi(x_i), \quad \mathbf{x} = (x_1, \ldots, x_s)$$

(*see Corollary* 4.4 *for the background*). *Then*, *for every sequence* $\omega = (\mathbf{x}_n)_{n\geq 0}$ *in* $[0,1[^s$ *such that the coordinates of all points* $\mathbf{x}_n$ *fulfill Condition* (C1) *or* (C2) *in Remark* 2.1, *in particular*, *if the coordinates of all points* $\mathbf{x}_n$ *are dyadic rationals*, *we have the identity*

$$F_N^2(\omega) = \frac{1}{3^s - 1} \cdot \frac{1}{N^2} \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} \phi(\mathbf{x}_n \dot{+} \mathbf{x}_m). \tag{17}$$

Remark 3.6. In any practical computation, we are restricted to a given finite number of binary digits, hence to finite sequences ω of dyadic rational points. As a consequence, the condition on the points of ω in Theorem 3.5 above is satisfied automatically. As identity (17) shows, it takes $\mathcal{O}(sN^2)$ steps to compute $F_N(\omega)$ for every sequence ω that has been generated by a digital machine. Examples are the finite sequences that arise in quasi-Monte Carlo integration or from pseudorandom number generators. For details on such point sets, the reader is referred to the monograph of Niederreiter [7].

4. The proof of Theorem 3.5

LEMMA 4.1. *Let* $c \neq 0$ *be a dyadic rational*, *let* $T_c : [0,1[\,\to [0,1[$, $T_c(x) := x \dot{+} c$, *denote the translation by* c, *and define* $g := -\lfloor \log_2 c \rfloor$. *Then*, *for all integers* a *with* $0 \leq a \leq 2^{g-1} - 1$,

$$\begin{aligned} T_c(J(g,2a)) &= J(g,2a+1), \\ T_c(J(g,2a+1)) &= J(g,2a). \end{aligned} \tag{18}$$

Proof. We have $2a \cdot 2^{-g} = 0.a_{g-2} \ldots a_0 0$. Hence

$$J(g,2a) = I(a_{g-2}, \ldots, a_0, 0), \qquad J(g,2a+1) = I(a_{g-2}, \ldots, a_0, 1).$$

Every $x \in J(g,2a)$ has the form

$$x = 0.a_{g-2} \ldots a_0 0 x_g x_{g+1} \ldots$$

Because $g = -\lfloor \log_2 c \rfloor$,

$$c = 0.0 \ldots 01 c_g c_{g+1} \ldots$$

with a block of $g-1$ leading zeros. Thus

$$x \dot{+} c = 0.a_{g-2} \ldots a_0 1 \ldots \in J(g, 2a+1).$$

It is clear from the analysis of the dyadic expansions above that the map $T_c : J(g, 2a) \to J(g, 2a+1)$ is a bijection. Further, $(T_c)^{-1} = T_c$. ■

Lemma 4.2. *Let* $f(x) := \mathbf{1}_{[0,1/3[}(x)$. *Then* $\widehat{f}(0) = 1/3$, *and*, *for all* k, $2^g \le k < 2^{g+1}$, $g \ge 0$,

$$|\widehat{f}(k)| = \tfrac{1}{3} \cdot 2^{-g}.$$

Proof. We use Lemma 1 in Hellekalek [2] to derive the result. ■

Lemma 4.3. *Let* f *be as in Lemma* 4.2. *Then*

$$f * f(x) = \begin{cases} \frac{1}{3} - \frac{2}{3} \cdot 2^{\lfloor \log_2 x \rfloor} & \textit{if } x \in \,]0,1[, \\ \frac{1}{3} & \textit{if } x = 0. \end{cases} \tag{19}$$

Proof. We have

$$f * f(x) = \int\limits_{[0,1/3[} \mathbf{1}_{[0,1/3[}(t \dot{+} x)\, dt = \lambda([0,1/3[\cap ([0,1/3[\dot{+} x)). \tag{20}$$

Now, let $x = c$ be a dyadic rational, $c \ne 0$, define $g := -\lfloor \log_2 c \rfloor$, and let $\beta := 1/3$. If a is defined by $\beta(g) = a \cdot 2^{-g}$, then

$$[0, \beta[\,= [\beta(g), \beta[\cup \bigcup_{b=0}^{a-1} J(g, b) \quad \text{(disjoint)}. \tag{21}$$

If g is even and, hence, a is odd, then Lemma 4.1 implies that

$$[0, \beta(g)[\dot{+} c = [0, \beta(g) - 2^{-g}[\cup [\beta(g), \beta(g) + 2^{-g}[, \tag{22}$$

and

$$[\beta(g), \beta[\dot{+} c \subseteq [\beta(g) - 2^{-g}, \beta(g)[.$$

This implies that

$$\lambda([0, \beta[\cap ([0, \beta[\dot{+} c)) = (\beta(g) - 2^{-g}) + \lambda([\beta(g), \beta[) + \lambda(T_c[\beta(g), \beta[).$$

The transformation T_c preserves the measure λ, hence

$$\lambda([0, \beta[\cap ([0, \beta[\dot{+} c)) = \tfrac{1}{3} - \tfrac{2}{3} \cdot 2^{-g}. \tag{23}$$

The case g odd (and hence a even) is treated in the same way. We use Lebesgue's theorem of dominated convergence to extend the identity (23) from dyadic rationals c to the case of arbitrary elements x in $[0,1[$. ■

Corollary 4.4. (i) *Let* $\varphi : [0,1[\,\to \mathbb{R}$, $\varphi(x) := 3f * 3f$, f *as in Lemma* 4.2, *and let* $\phi : [0,1[^s \to \mathbb{R}$,

$$\phi(\mathbf{x}) := -1 + \prod_{i=1}^{s} \varphi(x_i), \qquad \mathbf{x} = (x_1, \ldots, x_s).$$

Then Lemmas 4.2 *and* 4.3 *imply*

$$\widehat{\varphi}(k) = \varrho(k) = \begin{cases} 2^{-2g} & \textit{if } 2^g \le k < 2^{g+1}, \ \textit{with } g \ge 0, \\ 1 & \textit{if } k = 0, \end{cases} \tag{24}$$

and

$$\widehat{\phi}(\mathbf{k}) = \begin{cases} \varrho(\mathbf{k}) & \textit{if } \mathbf{k} \neq \mathbf{0}, \\ 0 & \textit{if } \mathbf{k} = \mathbf{0}. \end{cases} \tag{25}$$

(ii) *The function* φ *and*, *hence*, ϕ *is represented pointwise by its Walsh series. We even have uniform convergence of the Walsh series. This fact is important in the proof of Theorem* 3.5.

Proof. Part (i) is trivial. Part (ii) follows from direct comparison of the values of $\varphi(x)$ and of its Walsh series expansion $\sum_k \widehat{\varphi}(k)\, w_k(x)$ for $x \in [2^{-g}, 2^{-g+1}[$, $g \geq 1$. It is elementary to show that even *uniform* convergence of the Walsh series holds. ■

Proof of Theorem 3.5. From Corollary 4.4(i) it follows that the Walsh series of ϕ has the form

$$\phi = \sum_{\mathbf{k}\neq\mathbf{0}} \varrho(\mathbf{k}) w_{\mathbf{k}}.$$

Part (ii) of the same corollary tells us that ϕ is equal to its Walsh series at every point of $[0,1[^s$. Further, for arbitrary $\mathbf{x}$ and $\mathbf{y}$ in $[0,1[^s$ such that the coordinates of $\mathbf{x}$ and $\mathbf{y}$ fulfill either condition (C1) or (C2) of Remark 2.1,

$$w_{\mathbf{k}}(\mathbf{x} \dot{+} \mathbf{y}) = w_{\mathbf{k}}(\mathbf{x})\, w_{\mathbf{k}}(\mathbf{y}),$$

for all Walsh functions $w_{\mathbf{k}}$. The result follows by a simple calculation. ■

References

[1] R. R. Coveyou and R. D. MacPherson, *Fourier analysis of uniform random number generators*, J. Assoc. Comput. Mach. 14 (1967), 100–119.

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

[3] —, *Correlations between pseudorandom numbers*: *theory and numerical practice*, in: P. Hellekalek, G. Larcher, and P. Zinterhof (eds.), Proc. 1st Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, 1994, volume ACPC/TR 95-4 of Technical Report Series, Austrian Center for Parallel Computation, University of Vienna, 1995, 43–73.

[4] P. Hellekalek and H. Niederreiter, *The weighted spectral test*: *diaphony*, in preparation, 1996.

[5] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Reading, Mass., 1981.

[6] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.

[7] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[8] B. D. Ripley, *Stochastic Simulation*, Wiley, New York, 1987.

[9] F. Schipp, W. R. Wade, and P. Simon (with the collaboration of J. Pál), *Walsh Series. An Introduction to Dyadic Harmonic Analysis*, Adam Hilger, Bristol, 1990.

[10] B. G. Sloss and W. F. Blyth, *Walsh functions and uniform distribution* mod 1, Tôhoku Math. J. 45 (1993), 555–563.

[11] S. Tezuka, *Walsh-spectral test for GFSR pseudorandom numbers*, J. Assoc. Comput. Mach. 30 (1987), 731–735.

[12] —, *Uniform Random Numbers: Theory and Practice*, Kluwer, Boston, 1995.

[13] P. Zinterhof, *Über einige Abschätzungen bei der Approximation von Funktionen mit Gleichverteilungsmethoden*, Sitzungsber. Österr. Akad. Wiss. Math.-Natur. Kl. II 185 (1976), 121–132.

[14] P. Zinterhof und H. Stegbuchner, *Trigonometrische Approximation mit Gleichverteilungsmethoden*, Studia Sci. Math. Hungar. 13 (1978), 273–289.

Institut für Mathematik
Universität Salzburg
Hellbrunner Straße 34
A-5020 Salzburg, Austria
E-mail: peter.hellekalek@sbg.ac.at
leeb@random.mat.sbg.ac.at
Web: http://random.mat.sbg.ac.at/team/

Received on 11.4.1996
and in revised form on 1.10.1996 (2967)