Journal de Théorie des Nombres
de Bordeaux **19** (2007), 501–521

Dyadic diaphony of digital sequences

par Friedrich PILLICHSHAMMER

Résumé. La diaphonie diadique est une mesure quantitative pour l'irrégularité de la distribution d'une suite dans le cube unitaire. Dans cet article nous donnons des formules pour la diaphonie diadique des $(0,s)$-suites digitales sur $\mathbb{Z}_2$, $s = 1,2$. Ces formules montrent que, pour $s \in \{1,2\}$ fixé, la diaphonie diadique a les mêmes valeurs pour chaque $(0,s)$-suite digitale. Pour $s = 1$, il résulte que la diaphonie diadique et la diaphonie des $(0,1)$-suites digitales particulières sont égales, en faisant abstraction d'une constante. On détermine l'ordre asymptotique exact de la diaphonie diadique des $(0,s)$-suites digitales et on montre que pour $s = 1$ elle satisfait un théorème de la limite centrale.

Abstract. The dyadic diaphony is a quantitative measure for the irregularity of distribution of a sequence in the unit cube. In this paper we give formulae for the dyadic diaphony of digital $(0,s)$-sequences over $\mathbb{Z}_2$, $s = 1,2$. These formulae show that for fixed $s \in \{1,2\}$, the dyadic diaphony has the same values for any digital $(0,s)$-sequence. For $s = 1$, it follows that the dyadic diaphony and the diaphony of special digital $(0,1)$-sequences are up to a constant the same. We give the exact asymptotic order of the dyadic diaphony of digital $(0,s)$-sequences and show that for $s = 1$ it satisfies a central limit theorem.

1. Introduction

The *diaphony* F_N (see [19] or [7, Definition 1.29] or [12, Exercise 5.27, p. 162]) of the first N elements of a sequence $\omega = (\boldsymbol{x}_n)_{n\ge 0}$ in $[0,1)^s$ is given by

$$F_N(\omega) = \left(\sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^s\\ \boldsymbol{k}\neq\boldsymbol{0}}} \frac{1}{\rho(\boldsymbol{k})^2} \left| \frac{1}{N} \sum_{n=0}^{N-1} \mathrm{e}^{2\pi i \langle \boldsymbol{k}, \boldsymbol{x}_n\rangle} \right|^2 \right)^{1/2},$$

where for $\boldsymbol{k} = (k_1,\ldots,k_s) \in \mathbb{Z}^s$ it is $\rho(\boldsymbol{k}) = \prod_{i=1}^s \max(1,|k_i|)$ and $\langle\cdot,\cdot\rangle$ denotes the usual inner product in $\mathbb{R}^s$. It is well known that the diaphony is a quantitative measure for the irregularity of distribution of the first N

Manuscrit reçu le 12 janvier 2006.

points of a sequence. In fact, a sequence ω is uniformly distributed modulo 1 if and only if $\lim_{N\to\infty} F_N(\omega)=0$. Throughout this paper we will call the diaphony the *classical diaphony*.

In [11] Hellekalek and Leeb introduced the notion of dyadic diaphony which is similar to the classical diaphony but with the trigonometric functions replaced by Walsh functions. Before we give the exact definition of the dyadic diaphony recall that *Walsh-functions in base* 2 can be defined as follows: for a non-negative integer k with base 2 representation $k=\kappa_m 2^m+\cdots+\kappa_1 2+\kappa_0$ and a real x with (canonical) base 2 representation $x=\frac{x_1}{2}+\frac{x_2}{2^2}+\cdots$ the k-th Walsh function in base 2 is defined as

$$\mathrm{wal}_k(x):=(-1)^{x_1\kappa_0+x_2\kappa_1+\cdots+x_{m+1}\kappa_m}.$$

For dimension $s\geq 2$, $x_1,\ldots,x_s\in[0,1)$ and $k_1,\ldots,k_s\in\mathbb{N}_0$ we define

$$\mathrm{wal}_{k_1,\ldots,k_s}(x_1,\ldots,x_s):=\prod_{j=1}^{s}\mathrm{wal}_{k_j}(x_j).$$

For vectors $\boldsymbol{k}=(k_1,\ldots,k_s)\in\mathbb{N}_0^s$ and $\boldsymbol{x}=(x_1,\ldots,x_s)\in\mathbb{R}^s$ we write

$$\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}):=\mathrm{wal}_{k_1,\ldots,k_s}(x_1,\ldots,x_s).$$

Now we can give the definition of the dyadic diaphony (see Hellekalek and Leeb [11]).

Definition. The *dyadic diaphony* $F_{2,N}$ of the first N elements of a sequence $\omega=(\boldsymbol{x}_n)_{n\geq 0}$ in $[0,1)^s$ is defined by

$$F_{2,N}(\omega)=\left(\frac{1}{3^s-1}\sum_{\substack{\boldsymbol{k}\in\mathbb{N}_0^s\\ \boldsymbol{k}\neq\boldsymbol{0}}}\frac{1}{\psi(\boldsymbol{k})^2}\left|\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\right|^2\right)^{1/2},$$

where for $\boldsymbol{k}=(k_1,\ldots,k_s)\in\mathbb{N}_0^2$ it is $\psi(\boldsymbol{k})=\prod_{i=1}^s\psi(k_i)$ and for $k\in\mathbb{N}_0$,

$$\psi(k)=\begin{cases}1 & \text{if } k=0,\\ 2^r & \text{if } 2^r\leq k<2^{r+1} \text{ with } r\in\mathbb{N}_0.\end{cases}$$

Throughout the paper we will write $r(k)=r$ if r is the unique determined integer such that $2^r\leq k<2^{r+1}$.

It is shown in [11, Theorem 3.1] that the dyadic diaphony is a quantitative measure for the irregularity of distribution of the first N points of a sequence: a sequence ω is uniformly distributed modulo 1 if and only if $\lim_{N\to\infty}F_{2,N}(\omega)=0$. Further it was shown in [5] that the dyadic diaphony is — up to a factor depending only on s — the worst-case error for quasi-Monte Carlo integration of functions from a certain Hilbert space.

We consider the dyadic diaphony of a special class of sequences in $[0,1)^s$, namely of so-called digital $(0,s)$-sequences over $\mathbb{Z}_2$ for $s=1,2$. Digital

$(0, s)$-sequences or more generally digital (t, s)-sequences were introduced by Niederreiter [15, 16] and they provide at the moment the most efficient method to generate sequences with excellent distribution properties. We remark that a digital $(0, s)$-sequence over $\mathbb{Z}_2$ only exists if $s = 1$ or $s = 2$. For higher dimensions $s \geq 3$ the concept of digital (t, s)-sequence over $\mathbb{Z}_2$ with $t > 0$ has to be stressed (see [15] or [16]).

Before we give the definition of digital $(0, s)$-sequences we introduce some notation: for a vector $\vec{c} = (\gamma_1, \gamma_2, \ldots) \in \mathbb{Z}_2^\infty$ and for $m \in \mathbb{N}$ we denote the vector in $\mathbb{Z}_2^m$ consisting of the first m components of $\vec{c}$ by $\vec{c}(m)$, i.e., $\vec{c}(m) = (\gamma_1, \ldots, \gamma_m)$. Further for an $\mathbb{N} \times \mathbb{N}$ matrix C over $\mathbb{Z}_2$ and for $m \in \mathbb{N}$ we denote by $C(m)$ the left upper $m \times m$ submatrix of C.

Definition. For $s \in \{1, 2\}$, choose s $\mathbb{N} \times \mathbb{N}$ matrices $C_1, \ldots, C_s$ over $\mathbb{Z}_2$ with the following property: for every $m \in \mathbb{N}$ and every $0 \leq n \leq m$ the vectors

$$\vec{c}_1^{(1)}(m), \ldots, \vec{c}_n^{(1)}(m), \vec{c}_1^{(s)}(m), \ldots, \vec{c}_{m-n}^{(s)}(m)$$

are linearly independent in $\mathbb{Z}_2^m$. Here $\vec{c}_i^{(j)}$ is the i-th row vector of the matrix C_j. (In particular for any $m \in \mathbb{N}$ the matrix $C_j(m)$ has full rank over $\mathbb{Z}_2$ for all $j \in \{1, \ldots, s\}$.)

For $n \geq 0$ let $n = n_0 + n_1 2 + n_2 2^2 + \cdots$ be the base 2 representation of n. For $j \in \{1, \ldots, s\}$ multiply the vector $\vec{n} = (n_0, n_1, \ldots)^\top$ with the matrix C_j,

$$C_j \vec{n} =: (x_n^j(1), x_n^j(2), \ldots)^\top \in \mathbb{Z}_2^\infty$$

and set

$$x_n^{(j)} := \frac{x_n^j(1)}{2} + \frac{x_n^j(2)}{2^2} + \cdots.$$

Finally set $\boldsymbol{x}_n := (x_n^{(1)}, \ldots, x_n^{(s)})$.

Every sequence $(\boldsymbol{x}_n)_{n \geq 0}$ constructed in this way is called *digital* $(0, s)$-*sequence over* $\mathbb{Z}_2$. The matrices $C_1, \ldots, C_s$ are called the *generator matrices* of the sequence.

To guarantee that the points $\boldsymbol{x}_n$ belong to $[0, 1)^s$ (and not just to $[0, 1]^s$) and also for the analysis of the sequence we need the condition that for each $n \geq 0$ and $1 \leq j \leq s$, we have $x_n^j(i) = 0$ for infinitely many i. This condition is always satisfied if we assume that for each $1 \leq j \leq s$ and $r \geq 0$ we have $c_{i,r}^j = 0$ for all sufficiently large i, where $c_{i,r}^j$ are the entries of the matrix C_j. Throughout this paper we assume that the generator matrices fulfill this condition (see [16, p.72] where this condition is called (S6)).

For example if $s = 1$ and if we choose as generator matrix the $\mathbb{N} \times \mathbb{N}$ identity matrix, then the resulting digital $(0, 1)$-sequence over $\mathbb{Z}_2$ is the well known van der Corput sequence in base 2. Hence the concept of digital $(0, 1)$-sequences over $\mathbb{Z}_2$ is a generalization of the construction principle of the van der Corput sequence.

Note that finite versions of digital sequences over $\mathbb{Z}_2$ (so-called digital nets, see [16]) have a nice group structure, namely they are isomorphic to Cartesian products of the group $\mathbb{Z}_2$. The characters of these groups however are exactly the Walsh functions as defined above. For more information we refer to [13]. This is the reason why it is more convenient to consider the dyadic diaphony of digital sequences over $\mathbb{Z}_2$ instead of the classical diaphony. Furthermore this fact was used in many papers for computing different notions of discrepancies of digital point sets (see, for example, [2, 3, 4, 5, 6, 14, 17]).

For the classical diaphony it was proved by Faure [8] that

$$(NF_N(\omega))^2 = \pi^2 \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2, \tag{1}$$

if ω is a digital $(0,1)$-sequence over $\mathbb{Z}_2$ whose generator matrix C is a non-singular upper triangular matrix. Faure (and we shall do so as well) called these sequences NUT-sequences. Here $\|\cdot\|$ denotes the distance to the nearest integer function, i.e., $\|x\| := \min(x - \lfloor x \rfloor, 1 - (x - \lfloor x \rfloor))$. See also [1, 9, 10, 18] for further results concerning the classical diaphony of special 1-dimensional sequences.

The aim of this paper is to prove a similar formula for the dyadic diaphony of digital $(0,s)$-sequences over $\mathbb{Z}_2$ for $s \in \{1,2\}$ (see Theorems 2.1 and 3.1). These formulae show that for fixed s the dyadic diaphony is invariant for digital $(0,s)$-sequences over $\mathbb{Z}_2$. Further we find that the dyadic diaphony and the classical diaphony of NUT-sequences ($s=1$) only differ by a multiplicative constant (Corollary 2.2). We obtain the exact asymptotic order of the dyadic diaphony of digital $(0,s)$-sequences over $\mathbb{Z}_2$ (Corollaries 2.3 and 3.2). Moreover it follows from our formula that the squared dyadic diaphony of digital $(0,1)$-sequences over $\mathbb{Z}_2$ satisfies a central limit theorem (Corollary 2.4). For digital $(0,2)$-sequences we will obtain a similar, but weaker result (Corollary 3.3).

2. The results for $s = 1$

First we give the formula for the dyadic diaphony of digital $(0,1)$-sequences over $\mathbb{Z}_2$. This formula shows that the dyadic diaphony is invariant for digital $(0,1)$-sequences over $\mathbb{Z}_2$.

Theorem 2.1. *Let ω be a digital $(0,1)$-sequence over $\mathbb{Z}_2$. Then for any $N \geq 1$ we have*

$$(NF_{2,N}(\omega))^2 = 3 \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 .$$

We defer the proof of this formula to Section 4.

Remark. In Theorem 2.1 we have an infinite sum for the dyadic diaphony of a digital $(0,1)$-sequence over $\mathbb{Z}_2$. This formula can easily be made computable since for $1 \le N \le 2^m$ we have $\|N/2^u\| = N/2^u$ for $u \ge m+1$. Therefore we have

$$(NF_{2,N}(\omega))^2 = 3\sum_{u=1}^{m}\left\|\frac{N}{2^u}\right\|^2 + \left(\frac{N}{2^m}\right)^2. \tag{2}$$

From Theorem 2.1 we find the surprising result that the classical diaphony and the dyadic diaphony of a NUT-sequence are essentially the same.

Corollary 2.2. *Let ω be a NUT-sequence over $\mathbb{Z}_2$. Then for any $N \ge 1$ we have*

$$F_{2,N}(\omega) = \frac{\sqrt{3}}{\pi} F_N(\omega).$$

Proof. This follows from Theorem 2.1 together with Faures formula (1). □

From (2) one can see immediately that the dyadic diaphony of a digital $(0,1)$-sequence over $\mathbb{Z}_2$ is of order $F_{2,N}(\omega) = O(\sqrt{\log N}/N)$. But we can even be much more precise. From a thorough analysis of the sum in (2) we obtain the exact dependence of the dyadic diaphony of digital $(0,1)$-sequences over $\mathbb{Z}_2$ on $\sqrt{\log N}/N$.

Corollary 2.3. *Let ω be a digital* $(0,1)$*-sequence over $\mathbb{Z}_2$. For $N \le 2^m$ we have*

$$(NF_{2,N}(\omega))^2 \le \frac{m}{3} + \frac{4}{3} - \frac{2(-1)^m}{9\cdot 2^m} - \frac{1}{9\cdot 2^{2m}}$$

and

$$\limsup_{N\to\infty} \frac{(NF_{2,N}(\omega))^2}{\log N} = \frac{1}{3\log 2}.$$

The proof of this result will be given in Section 5. We just remark that the result for the lim sup follows also from a result of Chaix and Faure [1, Théoréme 4.13] for the classical diaphony of the van der Corput sequence together with Corollary 2.2 and Theorem 2.1.

In [6] it is shown that the star discrepancy and all L_p-discrepancies of the van der Corput sequence in base 2 satisfy a central limit theorem. The same arguments as in the proof of [6, Theorem 2] can now be used to obtain the subsequent result.

Corollary 2.4. *Let ω be a digital* $(0,1)$*-sequence over $\mathbb{Z}_2$. Then for every real y we have*

$$\frac{1}{M}\#\left\{N < M : (NF_{2,N}(\omega))^2 \le \frac{1}{4}\log_2 N + y\frac{1}{4\sqrt{3}}\sqrt{\log_2 N}\right\} = \Phi(y) + o(1),$$

where

$$\Phi(y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t$$

denotes the normal distribution function and $\log_2$ *denotes the logarithm to the base 2. I.e., the squared dyadic diaphony of a digital* $(0,1)$*-sequence over* $\mathbb{Z}_2$ *satisfies a central limit theorem.*

Remark. Together with Corollary 2.2 we also obtain a central limit theorem for the square of the classical diaphony of NUT-sequences.

Proof. As already mentioned, the proof follows exactly the lines of the proof of [6, Theorem 2]. One only has to compute the expectation and the variance of the random variable

$$S_m = \sum_{w=1}^{m} \|X 2^w\|^2,$$

where X is uniformly distributed on $[0,1)$. By tedious but straightforward calculations we obtain $\mathbf{E}S_m = m/12$ and $\mathbf{Var}S_m = m/432 + 7(1 - 2^{-2m})/1620$. □

3. The results for $s = 2$

We give the formula for the dyadic diaphony of digital $(0,2)$-sequences over $\mathbb{Z}_2$ which shows that the dyadic diaphony is invariant for digital $(0,2)$-sequences as well.

Theorem 3.1. *Let* ω *be a digital* $(0,2)$*-sequence over* $\mathbb{Z}_2$*. Then for any* $N \geq 1$ *we have*

$$(NF_{2,N}(\omega))^2 = \frac{9}{4} \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 u.$$

We defer the proof of this formula to Section 4.

Remark. In Theorem 3.1 we have an infinite sum for the dyadic diaphony of a digital $(0,2)$-sequence over $\mathbb{Z}_2$. Again this formula can easily be made computable. For $1 \leq N \leq 2^m$ we have

$$(NF_{2,N}(\omega))^2 = \frac{9}{4} \sum_{u=1}^{m} \left\| \frac{N}{2^u} \right\|^2 u + \left(\frac{N}{2^m} \right)^2 \frac{4+3m}{4}. \tag{3}$$

From (3) one can see immediately that the dyadic diaphony of a digital $(0,2)$-sequence over $\mathbb{Z}_2$ is of order $F_{2,N}(\omega) = O(\log N/N)$. Also here we obtain from a thorough analysis of the sum in (3) the exact dependence of the dyadic diaphony of digital $(0,2)$-sequences over $\mathbb{Z}_2$ on $\log N/N$.

Corollary 3.2. *Let ω be a digital $(0,2)$-sequence over $\mathbb{Z}_2$. Then for any $N \le 2^m$ we have*

$$(NF_{2,N}(\omega))^2 \le \frac{m^2}{8} + \frac{7m}{8} + \frac{11}{9} + O\left(\frac{m}{2^m}\right)$$

and

$$\limsup_{N\to\infty} \frac{(NF_{2,N}(\omega))^2}{(\log N)^2} = \frac{1}{8(\log 2)^2}.$$

The proof of this result will be given in Section 5. Following this proof the $O(m/2^m)$-term in the above bound can easily be made explicit.

Unfortunately we could not show that the squared dyadic diaphony of a digital $(0,2)$-sequence over $\mathbb{Z}_2$ satisfies a central limit theorem. However, we were able to prove the following result.

Corollary 3.3. *Let ω be a digital $(0,2)$-sequence over $\mathbb{Z}_2$. Then for any $\varepsilon > 0$ we have*

$$\lim_{m\to\infty} \frac{1}{2^m} \# \left\{ N < 2^m \,:\, \frac{3}{32} - \varepsilon < \left(\frac{NF_{2,N}(\omega)}{\log_2 N}\right)^2 < \frac{3}{32} + \varepsilon \right\} = 1.$$

Proof. By tedious but straightforward calculations using Theorem 3.1 we obtain

$$\sum_{N=0}^{2^m-1} (NF_{2,N}(\omega))^2 = \frac{3}{32} m^2 2^m + O(m2^m)$$

and

$$\sum_{N=0}^{2^m-1} (NF_{2,N}(\omega))^4 = \frac{9}{1024} m^4 2^m + O(m^3 2^m).$$

From this the result immediately follows. □

4. The proofs of Theorems 2.1 and 3.1

For the proofs of Theorems 2.1 and 3.1 we need the subsequent lemma. This result was implicitly proved in [6]. For the sake of completeness we provide the short proof.

Lemma 4.1. *Let the non-negative integer U have binary expansion $U = U_0 + U_1 2 + \cdots + U_{m-1} 2^{m-1}$. For any non-negative integer $n \le U-1$ let $n = n_0 + n_1 2 + \cdots + n_{m-1} 2^{m-1}$ be the binary representation of n. For $0 \le p \le m-1$ let $U(p) := U_0 + \cdots + U_p 2^p$. Let $b_0, b_1, \ldots, b_{m-1}$ be arbitrary elements of $\mathbb{Z}_2$, not all zero. Then*

$$\sum_{n=0}^{U-1} (-1)^{b_0 n_0 + \cdots + b_{m-1} n_{m-1}} = (-1)^{b_{w+1} U_{w+1} + \cdots + b_{m-1} U_{m-1}} 2^{w+1} \left\| \frac{U}{2^{w+1}} \right\|,$$

where w is minimal such that $b_w = 1$.

Proof. From splitting up the sum we obtain

$$\begin{aligned}
&\sum_{n=0}^{U-1}(-1)^{b_0n_0+\cdots+b_{m-1}n_{m-1}}\\
&= \sum_{n=0}^{2^{w+1}(U_{w+1}+\cdots+U_{m-1}2^{m-w-2})-1}(-1)^{n_w}(-1)^{b_{w+1}n_{w+1}+\cdots+b_{m-1}n_{m-1}}\\
&+ \sum_{n=0}^{U(w)-1}(-1)^{n_w}(-1)^{b_{w+1}U_{w+1}+\cdots+b_{m-1}U_{m-1}}\\
&= 0+(-1)^{b_{w+1}U_{w+1}+\cdots+b_{m-1}U_{m-1}}\sum_{n=0}^{U(w)-1}(-1)^{n_w}\\
&= (-1)^{b_{w+1}U_{w+1}+\cdots+b_{m-1}U_{m-1}}\times\begin{cases} U(w) & \text{if } U(w)<2^w,\\ 2^{w+1}-U(w) & \text{if } U(w)\geq 2^w,\end{cases}\\
&= (-1)^{b_{w+1}U_{w+1}+\cdots+b_{m-1}U_{m-1}}2^{w+1}\times\begin{cases} \frac{U(w)}{2^{w+1}} & \text{if } \frac{U(w)}{2^{w+1}}<\frac{1}{2},\\ 1-\frac{U(w)}{2^{w+1}} & \text{if } \frac{U(w)}{2^{w+1}}\geq \frac{1}{2},\end{cases}\\
&= (-1)^{b_{w+1}U_{w+1}+\cdots+b_{m-1}U_{m-1}}2^{w+1}\left\|\frac{U(w)}{2^{w+1}}\right\|.
\end{aligned}$$

Since $\left\|\frac{U(w)}{2^{w+1}}\right\| = \left\|\frac{U}{2^{w+1}}\right\|$ the result follows. □

Now we can give the

Proof of Theorem 2.1. Let $2^r \leq k < 2^{r+1}$. Then $k = k_0 + k_1 2 + \cdots + k_r 2^r$ with $k_i \in \{0,1\}$, $0 \leq i < r$ and $k_r = 1$. Let $\langle\cdot,\cdot\rangle$ denote the usual inner product in $\mathbb{Z}_2^\infty$ and let $\vec{c}_i \in \mathbb{Z}_2^\infty$ be the i-th row vector of the generator matrix C of the digital $(0,1)$-sequence (for short we write C instead of C_1 here). Since the i-th digit $x_n(i)$ of the point x_n, $i \in \mathbb{N}$, $n \in \mathbb{N}_0$, is given by $\langle\vec{c}_i,\vec{n}\rangle$ (see Definition 1) we have

$$\begin{aligned}
\sum_{n=0}^{N-1}\mathrm{wal}_k(x_n) &= \sum_{n=0}^{N-1}(-1)^{k_0\langle\vec{c}_1,\vec{n}\rangle+\cdots+k_r\langle\vec{c}_{r+1},\vec{n}\rangle}\\
&= \sum_{n=0}^{N-1}(-1)^{\langle k_0\vec{c}_1+\cdots+k_r\vec{c}_{r+1},\vec{n}\rangle}. \qquad (4)
\end{aligned}$$

Let $C = (c_{i,j})_{i,j\geq 1}$. For $k \in \mathbb{N}$, $k = k_0 + k_1 2 + \cdots + k_r 2^r$, $k_i \in \{0,1\}$, $0 \leq i < r$ and $k_r = 1$ define $u(k) := \min\{l \geq 1 : k_0 c_{1,l} + \cdots + k_r c_{r+1,l} = 1\}$. Note that since C generates a digital $(0,1)$-sequence over $\mathbb{Z}_2$ we obviously have $u(k) \leq r+1$. For fixed k, $2^r \leq k < 2^{r+1}$ let $\vec{b} = (b_0, b_1, \ldots)^\top :=$

$k_0\vec{c}_1 + \cdots + k_r\vec{c}_{r+1}$. Let $N = N_0 + N_1 2 + \cdots + N_{m-1}2^{m-1}$. If $u(k) \le m$ we obtain from (4) together with Lemma 4.1,

$$\begin{aligned}\sum_{n=0}^{N-1} \mathrm{wal}_k(x_n) &= \sum_{n=0}^{N-1} (-1)^{\langle \vec{b}, \vec{n}\rangle} = \sum_{n=0}^{N-1} (-1)^{n_0 b_0 + \cdots + n_{m-1} b_{m-1}} \\ &= \sum_{n=0}^{N-1} (-1)^{n_{u(k)-1} + \cdots} = (-1)^{N_{u(k)} b_{u(k)} + \cdots} 2^{u(k)} \left\| \frac{N}{2^{u(k)}} \right\|.\end{aligned}$$

But if $u(k) > m$ the above equality is trivially true. Therefore we have

$$\begin{aligned}2(NF_{2,N}(\omega))^2 &= \sum_{k=1}^{\infty} \frac{1}{2^{2r(k)}} \left(2^{u(k)} \left\| \frac{N}{2^{u(k)}} \right\| \right)^2 \\ &= \sum_{r=0}^{\infty} \frac{1}{2^{2r}} \sum_{k=2^r}^{2^{r+1}-1} 2^{2u(k)} \left\| \frac{N}{2^{u(k)}} \right\|^2 \\ &= \sum_{r=0}^{\infty} \frac{1}{2^{2r}} \sum_{u=1}^{r+1} 2^{2u} \left\| \frac{N}{2^u} \right\|^2 \sum_{\substack{k=2^r \\ u(k)=u}}^{2^{r+1}-1} 1 \\ &= \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 2^{2u} \sum_{r=u-1}^{\infty} \frac{1}{2^{2r}} \sum_{\substack{k=2^r \\ u(k)=u}}^{2^{r+1}-1} 1.\end{aligned}$$

Now we have to evaluate the sum $\sum_{\substack{k=2^r \\ u(k)=u}}^{2^{r+1}-1} 1$ for $r \ge u-1$ and $u \ge 1$. This is the number of vectors $(k_0, \ldots, k_{r-1})^\top \in \mathbb{Z}_2^r$ such that

$$C(r+1)^\top \begin{pmatrix} k_0 \\ \vdots \\ k_{r-1} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ x_{u+1} \\ \vdots \\ x_{r+1} \end{pmatrix} \in \mathbb{Z}_2^{r+1} \tag{5}$$

for arbitrary $x_{u+1}, \ldots, x_{r+1} \in \mathbb{Z}_2$. (Recall that for an integer $m \ge 1$ we denote by $C(m)$ the left upper $m \times m$ submatrix of the matrix C, see Section 1.)

We consider two cases:

(i) Assume that $r = u - 1$. Then system (5) becomes

$$C(r+1)^\top \begin{pmatrix} k_0 \\ \vdots \\ k_{r-1} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Since the $(r+1)\times(r+1)$ matrix $C(r+1)^\top$ is regular over $\mathbb{Z}_2$ it is clear that there exists a vector $\vec{k} = (k_0, \ldots, k_r) \in \mathbb{Z}_2^{r+1}$ such that $C(r+1)^\top \vec{k} = (0, \ldots, 0, 1)^\top$. Assume that $k_r = 0$, then we have $C(r)^\top (k_0, \ldots, k_{r-1})^\top = (0, \ldots, 0)^\top$. Again we know that $C(r)^\top$ is regular over $\mathbb{Z}_2$ and therefore we obtain $k_0 = \cdots = k_{r-1} = 0$. Hence $\vec{k} = \vec{0}$, the zero vector in $\mathbb{Z}_2^{r+1}$. This is now a contradiction since $\vec{k}$ is a solution of the system $C(r+1)^\top \vec{k} = (0, \ldots, 0, 1)^\top$. Therefore we have

$$\sum_{\substack{k=2^{u-1} \\ u(k)=u}}^{2^u-1} 1 = 1.$$

(ii) Assume that $r \geq u$. Since $C(r)$ is regular over $\mathbb{Z}_2$ it is clear that $D(r) := (C(r)^\top)^{-1}$ is regular over $\mathbb{Z}_2$. Hence for any vector $\vec{k} \in \mathbb{Z}_2^r$ there is a vector $\vec{l} \in \mathbb{Z}_2^r$ such that $\vec{k} = D(r)\vec{l}$. Therefore system (5) can be rewritten as

$$C(r+1)^\top \begin{pmatrix} D(r)\vec{l} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ x_{u+1} \\ \vdots \\ x_{r+1} \end{pmatrix}$$

with $\vec{l} \in \mathbb{Z}_2^r$. Now we use the definition of the matrix $D(r)$ and find that the above system is equivalent to the system

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \\ d_1 & d_2 & \ldots & d_{r-1} & d_r \end{pmatrix} \begin{pmatrix} l_0 \\ \vdots \\ l_{r-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ x_{u+1} \\ \vdots \\ x_{r+1} \end{pmatrix} + \vec{c}_{r+1}(r+1)^\top,$$

where $(d_1, \dots, d_r) := (c_{1,r+1}, \dots, c_{r,r+1})D(r)$. Now one can easily see that for arbitrary $x_{u+1}, \dots, x_r$ there exists exactly one solution $\vec{l} = (l_0, \dots, l_{r-1})^\top \in \mathbb{Z}_2^r$ such that the first r lines of the above system are fulfilled. Further there is exactly one possible choice of $x_{r+1} \in \mathbb{Z}_2$ such that this vector $\vec{l}$ is a solution of the above system. Therefore we obtain

$$\sum_{\substack{k=2^r\\u(k)=u}}^{2^{r+1}-1} 1 = 2^{r-u}.$$

Now we have

$$2(NF_{2,N}(\omega))^2 = \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 2^{2u} \left(\frac{1}{2^{2(u-1)}} + \sum_{r=u}^{\infty} \frac{1}{2^{2r}} 2^{r-u} \right) = 6 \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2.$$

The result follows. $\square$

Proof of Theorem 3.1. Let $\omega = (\boldsymbol{x}_n)_{n\geq 0}$ be a digital $(0,2)$-sequence over $\mathbb{Z}_2$. Let $\boldsymbol{x}_n = (x_n, y_n)$ for $n \geq 0$. Clearly the sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ are digital $(0,1)$-sequences over $\mathbb{Z}_2$. We have

$$\begin{aligned}
(NF_{2,N}(\omega))^2 &= \frac{1}{8} \sum_{\substack{\boldsymbol{k}\in\mathbb{N}_0^2\\ \boldsymbol{k}\neq\boldsymbol{0}}} \frac{1}{\psi(\boldsymbol{k})} \left| \sum_{n=0}^{N-1} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) \right|^2 \\
&= \frac{1}{8} \sum_{k=1}^{\infty} \frac{1}{2^{2r(k)}} \left| \sum_{n=0}^{N-1} \mathrm{wal}_k(x_n) \right|^2 + \frac{1}{8} \sum_{l=1}^{\infty} \frac{1}{2^{2r(l)}} \left| \sum_{n=0}^{N-1} \mathrm{wal}_l(y_n) \right|^2 \\
&\quad + \frac{1}{8} \sum_{k,l=1}^{\infty} \frac{1}{2^{2r(k)+2r(l)}} \left| \sum_{n=0}^{N-1} \mathrm{wal}_k(x_n)\mathrm{wal}_l(y_n) \right|^2 \\
&= \frac{3}{2} \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 + \frac{1}{8} \sum_{k,l=1}^{\infty} \frac{1}{2^{2r(k)+2r(l)}} \left| \sum_{n=0}^{N-1} \mathrm{wal}_k(x_n)\mathrm{wal}_l(y_n) \right|^2, \qquad (6)
\end{aligned}$$

where for the last equality we used Theorem 2.1. We have to consider

$$\Sigma := \sum_{k,l=1}^{\infty} \frac{1}{2^{2r(k)+2r(l)}} \left| \sum_{n=0}^{N-1} \mathrm{wal}_k(x_n)\mathrm{wal}_l(y_n) \right|^2.$$

Assume that $2^r \leq k < 2^{r+1}$ and $2^t \leq l < 2^{t+1}$. Then $k = k_0 + k_1 2 + \dots + k_r 2^r$ with $k_i \in \{0,1\}$, $0 \leq i < r$ and $k_r = 1$ and $l = l_0 + l_1 2 + \dots + l_t 2^t$ with $l_j \in \{0,1\}$, $0 \leq j < t$ and $l_t = 1$. Let $\vec{c}_i \in \mathbb{Z}_2^\infty$ be the i-th row vector of the generator matrix C_1 and let $\vec{d}_i \in \mathbb{Z}_2^\infty$ be the i-th row vector of the generator matrix C_2, $i \in \mathbb{N}$. Since the i-th digit $x_n(i)$ of x_n is given by $\langle \vec{c}_i, \vec{n} \rangle$ and the

i-th digit $y_n(i)$ of y_n is given by $\langle \vec{d}_i, \vec{n}\rangle$ (see Definition 1) we have

$$\begin{aligned}\sum_{n=0}^{N-1} \mathrm{wal}_k(x_n)\mathrm{wal}_l(y_n) &= \sum_{n=0}^{N-1} (-1)^{k_0\langle \vec{c}_1,\vec{n}\rangle+\cdots+k_r\langle \vec{c}_{r+1},\vec{n}\rangle+l_0\langle \vec{d}_1,\vec{n}\rangle+\cdots+l_t\langle \vec{d}_{t+1},\vec{n}\rangle}\\ &= \sum_{n=0}^{N-1} (-1)^{\langle k_0\vec{c}_1+\cdots+k_r\vec{c}_{r+1}+l_0\vec{d}_1+\cdots+l_t\vec{d}_{t+1},\vec{n}\rangle}.\end{aligned}$$

Let $C_1 = (c_{i,j})_{i,j\geq 1}$ and $C_2 = (d_{i,j})_{i,j\geq 1}$. Define

$$u(k,l) := \min\{j \geq 1 \,:\, k_0c_{1,j} + \cdots + k_rc_{r+1,j} + l_0d_{1,j} + \cdots + l_td_{t+1,j} = 1\}.$$

Since C_1, C_2 generate a digital $(0,2)$-sequence over $\mathbb{Z}_2$ we obviously have $u(k,l) \leq r+t+2$. As in the proof of Theorem 2.1 we now apply Lemma 4.1 and obtain

$$\left|\sum_{n=0}^{N-1} \mathrm{wal}_k(x_n)\mathrm{wal}_l(y_n)\right| = 2^{u(k,l)} \left\| \frac{N}{2^{u(k,l)}}\right\|.$$

Therefore we have

$$\begin{aligned}\Sigma &= \sum_{k,l=1}^{\infty} \frac{1}{2^{2r(k)+2r(l)}} 2^{2u(k,l)} \left\|\frac{N}{2^{u(k,l)}}\right\|^2\\ &= \sum_{r,t=0}^{\infty} \frac{1}{2^{2r+2t}} \sum_{k=2^r}^{2^{r+1}-1} \sum_{l=2^t}^{2^{t+1}-1} 2^{2u(k,l)} \left\|\frac{N}{2^{u(k,l)}}\right\|^2\\ &= \sum_{r,t=0}^{\infty} \frac{1}{2^{2r+2t}} \sum_{u=1}^{r+t+2} 2^{2u} \left\|\frac{N}{2^u}\right\|^2 \underbrace{\sum_{k=2^r}^{2^{r+1}-1} \sum_{l=2^t}^{2^{t+1}-1}}_{u(k,l)=u} 1.\end{aligned}$$

We have to evaluate the double-sum $\underbrace{\sum_{k=2^r}^{2^{r+1}-1} \sum_{l=2^t}^{2^{t+1}-1}}_{u(k,l)=u} 1$ for $1 \leq u \leq r+t+2$.

To this end we define the $(r+t+2)\times(r+t+2)$ matrix

$$\mathcal{C}(r,t) := \begin{pmatrix} c_{1,1} & \ldots & c_{r+1,1} & d_{1,1} & \ldots & d_{t+1,1}\\ c_{1,2} & \ldots & c_{r+1,2} & d_{1,2} & \ldots & d_{t+1,2}\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ c_{1,r+t+2} & \ldots & c_{r+1,r+t+2} & d_{1,r+t+2} & \ldots & d_{t+1,r+t+2}\end{pmatrix}.$$

Note that since C_1, C_2 generate a digital $(0,2)$-sequence over $\mathbb{Z}_2$, it follows that $\mathcal{C}(r,t)$ is regular.

Now the value of the above double-sum is exactly the number of digits $k_0, \dots, k_{r-1}, l_0, \dots, l_{t-1} \in \mathbb{Z}_2$ such that

$$\mathcal{C}(r,t)\begin{pmatrix} k_0 \\ \vdots \\ k_{r-1} \\ 1 \\ l_0 \\ \vdots \\ l_{t-1} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ x_{u+1} \\ \vdots \\ x_{r+t+2} \end{pmatrix} \tag{7}$$

for arbitrary $x_{u+1}, \dots, x_{r+t+2} \in \mathbb{Z}_2$. We consider three cases:

(i) Assume that $u = r+t+2$. Then system (7) becomes

$$\mathcal{C}(r,t)\vec{h} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{8}$$

Since $\mathcal{C}(r,t)$ is regular there exists a vector $\vec{h} = (k_0, \dots, k_r, l_0, \dots, l_t)^\top \in \mathbb{Z}_2^{r+t+2}$, $\vec{h} \neq \vec{0}$, such that $\mathcal{C}(r,t)\vec{h} = (0, \dots, 0, 1)^\top$. Assume that $l_t = 0$. Then

$$\begin{pmatrix} c_{1,1} & \dots & c_{r+1,1} & d_{1,1} & \dots & d_{t,1} \\ c_{1,2} & \dots & c_{r+1,2} & d_{1,2} & \dots & d_{t,2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c_{1,r+t+2} & \dots & c_{r+1,r+t+2} & d_{1,r+t+2} & \dots & d_{t,r+t+2} \end{pmatrix} \begin{pmatrix} k_0 \\ \vdots \\ k_r \\ l_0 \\ \vdots \\ l_{t-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

But then

$$\begin{pmatrix} c_{1,1} & \dots & c_{r+1,1} & d_{1,1} & \dots & d_{t,1} \\ c_{1,2} & \dots & c_{r+1,2} & d_{1,2} & \dots & d_{t,2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c_{1,r+t+1} & \dots & c_{r+1,r+t+1} & d_{1,r+t+1} & \dots & d_{t,r+t+1} \end{pmatrix} \begin{pmatrix} k_0 \\ \vdots \\ k_r \\ l_0 \\ \vdots \\ l_{t-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the above matrix is again regular we obtain that the vector $(k_0, \dots, k_r, l_0, \dots, l_{t-1}) = (0, \dots, 0)$ and therefore $\vec{h} = \vec{0}$, a contradiction. Hence $l_t = 1$ and in the same way one can show that $k_r = 1$. We have shown that system (8) has exactly one solution and therefore we have

$$\underbrace{\sum_{k=2^r}^{2^{r+1}-1}\sum_{l=2^t}^{2^{t+1}-1}}_{u(k,l)=u} 1 = 1.$$

(ii) Assume that $u = r+t+1$. Let $x \in \mathbb{Z}_2$. Since $\mathcal{C}(r,t)$ is regular there exists exactly one vector $\vec{h} \in \mathbb{Z}_2^{r+t+2}$ such that

$$\mathcal{C}(r,t)\vec{h} = (0,\ldots,0,1,x)^\top.$$

Assume that $\vec{h}$ is of the form $\vec{h} = (k_0,\ldots,k_{r-1},1,l_0,\ldots,l_{t-1},1)^\top \in \mathbb{Z}_2^{r+t+2}$. In particular we have

$$\begin{pmatrix} c_{1,1} & \ldots & c_{r+1,1} & d_{1,1} & \ldots & d_{t+1,1} \\ c_{1,2} & \ldots & c_{r+1,2} & d_{1,2} & \ldots & d_{t+1,2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{1,r+t} & \ldots & c_{r+1,r+t} & d_{1,r+t} & \ldots & d_{t+1,r+t} \end{pmatrix} \vec{h} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{9}$$

Since

$$\begin{pmatrix} c_{1,1} & \ldots & c_{r,1} & d_{1,1} & \ldots & d_{t,1} \\ c_{1,2} & \ldots & c_{r,2} & d_{1,2} & \ldots & d_{t,2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{1,r+t} & \ldots & c_{r,r+t} & d_{1,r+t} & \ldots & d_{t,r+t} \end{pmatrix}$$

is regular we find that $\vec{h}$ is the unique solution of (9). Hence $\vec{h}$ is exactly the same vector as in the first case where $u = r+t+2$. But then $\vec{h}$ cannot be a solution of $\mathcal{C}(r,t)\vec{h} = (0,\ldots,0,1,x)^\top$. Therefore we obtain

$$\underbrace{\sum_{k=2^r}^{2^{r+1}-1}\sum_{l=2^t}^{2^{t+1}-1}}_{u(k,l)=u} 1 = 0.$$

(iii) Assume that $1 \le u \le r+t$. We rewrite system (7) in the form

$$\begin{pmatrix} c_{1,1} & \ldots & c_{r,1} & d_{1,1} & \ldots & d_{t,1} \\ c_{1,2} & \ldots & c_{r,2} & d_{1,2} & \ldots & d_{t,2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{1,r+t} & \ldots & c_{r,r+t} & d_{1,r+t} & \ldots & d_{t,r+t} \\ c_{1,r+t+1} & \ldots & c_{r,r+t+1} & d_{1,r+t+1} & \ldots & d_{t,r+t+1} \\ c_{1,r+t+2} & \ldots & c_{r,r+t+2} & d_{1,r+t+2} & \ldots & d_{t,r+t+2} \end{pmatrix} \begin{pmatrix} k_0 \\ \vdots \\ k_{r-1} \\ l_0 \\ \vdots \\ l_{t-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ x_{u+1} \\ \vdots \\ x_{r+t} \\ x_{r+t+1} \\ x_{r+t+2} \end{pmatrix} + \vec{y}_{r,t}$$

where $\vec{y}_{r,t} = (c_{r+1,1} + d_{t+1,1}, \ldots, c_{r+1,r+t+2} + d_{t+1,r+t+2})^\top \in \mathbb{Z}_2^{r+t+2}$. Since the upper $(r+t) \times (r+t)$ sub-matrix of the above matrix is regular we find for arbitrary $x_{u+1}, \ldots, x_{r+t}$ exactly one solution of the first $r+t$ rows of the above system. This solution can be made a solution of the whole system by an adequate choice of x_{r+t+1} and x_{r+t+2}. Therefore we have

$$\underbrace{\sum_{k=2^r}^{2^{r+1}-1} \sum_{l=2^t}^{2^{t+1}-1}}_{u(k,l)=u} 1 = 2^{r+t-u}.$$

Now we have

$$\begin{aligned}
\Sigma &= \sum_{r,t=0}^{\infty} \frac{1}{2^{2r+2t}} \left(\sum_{u=1}^{r+t} 2^{2u} \left\| \frac{N}{2^u} \right\|^2 2^{r+t-u} + 2^{2(r+t+2)} \left\| \frac{N}{2^{r+t+2}} \right\|^2 \right) \\
&= \sum_{r,t=0}^{\infty} \frac{1}{2^{r+t}} \sum_{u=1}^{r+t} 2^u \left\| \frac{N}{2^u} \right\|^2 + 16 \sum_{r,t=0}^{\infty} \left\| \frac{N}{2^{r+t+2}} \right\|^2 \\
&= \sum_{u=1}^{\infty} 2^u \left\| \frac{N}{2^u} \right\|^2 \sum_{\substack{r,t=0 \\ r+t \geq u}}^{\infty} \frac{1}{2^{r+t}} + 16 \sum_{u=2}^{\infty} \left\| \frac{N}{2^u} \right\|^2 \sum_{\substack{r,t=0 \\ r+t=u-2}}^{\infty} 1 \\
&= \sum_{u=1}^{\infty} 2^u \left\| \frac{N}{2^u} \right\|^2 \sum_{w=u}^{\infty} \frac{w+1}{2^w} + 16 \sum_{u=2}^{\infty} \left\| \frac{N}{2^u} \right\|^2 (u-1) \\
&= \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 (2u+4) + 16 \sum_{u=2}^{\infty} \left\| \frac{N}{2^u} \right\|^2 (u-1) \\
&= \sum_{u=1}^{\infty} \left\| \frac{N}{2^u} \right\|^2 (18u-12).
\end{aligned}$$

The result follows by inserting this expression into (6). $\square$

5. The proofs of Corollaries 2.3 and 3.2

We will say that a real β in $[0,1)$ is m-bit if $\beta = \frac{b_1}{2} + \cdots + \frac{b_m}{2^m}$ with $b_i \in \{0,1\}$. I.e., an m-bit number is of the form $k/2^m$ with $k \in \{0,1,\ldots,2^m-1\}$.

The essential technical tool for the proof of Corollary 2.3 is provided by

Lemma 5.1. *Assume that $\beta = 0, b_1 b_2 \ldots$ (this here and in the following always means base 2 representation) has two equal consecutive digits $b_i b_{i+1}$*

with $i \le m-1$ and let i be minimal with this property, i.e.,

$$\begin{aligned}
\beta &= 0,01\dots0100b_{i+2}\dots \quad \textit{or}\\
\beta &= 0,10\dots0100b_{i+2}\dots \quad \textit{or}\\
\beta &= 0,01\dots1011b_{i+2}\dots \quad \textit{or}\\
\beta &= 0,10\dots1011b_{i+2}\dots \quad .
\end{aligned}$$

Replace β by

$$\begin{aligned}
\gamma &= 0,10\dots1010b_{i+2}\dots \quad \textit{resp.}\\
\gamma &= 0,01\dots1010b_{i+2}\dots \quad \textit{resp.}\\
\gamma &= 0,10\dots0101b_{i+2}\dots \quad \textit{resp.}\\
\gamma &= 0,01\dots0101b_{i+2}\dots \quad .
\end{aligned}$$

Then

$$\sum_{u=0}^{m-1}\|2^u\gamma\|^2 = \sum_{u=0}^{m-1}\|2^u\beta\|^2 + \begin{cases} \frac{1}{9}\left(1-\frac{(-1)^i}{2^i}\right)^2(1-\tau) & \textit{in the first two cases,}\\ \frac{1}{9}\left(1-\frac{(-1)^i}{2^i}\right)^2\tau & \textit{in the last two cases,}\end{cases}$$

where $\tau := 0,b_{i+2}b_{i+3}\dots$.

Remark. In any case we have $\sum_{u=0}^{m-1}\|2^u\gamma\|^2 \ge \sum_{u=0}^{m-1}\|2^u\beta\|^2$ with equality iff $\tau = 1$ in the first two cases and iff $\tau = 0$ in the last two cases.

Proof of Lemma 5.1. This is simple calculation. We just handle the first case here.

$$\begin{aligned}
&\sum_{u=0}^{m-1}(\|2^u\gamma\|^2 - \|2^u\beta\|^2) \qquad (10)\\
&= \|\gamma\|^2 - \|2^i\beta\|^2 + \sum_{u=0}^{i-1}(\|2^u(2\gamma)\|^2 - \|2^u\beta\|^2).
\end{aligned}$$

Here $\|\gamma\| = \frac{1}{3}\left(1+\frac{1}{2^i}\right) - \frac{\tau}{2^{i+1}}$ and $\|2^i\beta\| = \frac{\tau}{2}$. Further, for even u we have

$$\|2^u(2\gamma)\| = \frac{1}{3}\left(1-\frac{2^{u+1}}{2^i}\right) + \frac{\tau}{2^{i-u}} \quad \text{and} \quad \|2^u\beta\| = \frac{1}{3}\left(1-\frac{2^{u+1}}{2^i}\right) + \frac{\tau}{2^{i+1-u}},$$

and for odd u we have

$$\|2^u(2\gamma)\| = \frac{1}{3}\left(1+\frac{2^{u+1}}{2^i}\right) - \frac{\tau}{2^{i-u}} \quad \text{and} \quad \|2^u\beta\| = \frac{1}{3}\left(1+\frac{2^{u+1}}{2^i}\right) - \frac{\tau}{2^{i+1-u}}.$$

Inserting this into (10) we obtain

$$\sum_{u=0}^{m-1}(\|2^u\gamma\|^2 - \|2^u\beta\|^2) = \frac{1}{9}\left(1+\frac{1}{2^i}\right)^2(1-\tau).$$

The other cases are calculated in the same way. $\square$

From Lemma 5.1 we obtain the subsequent result concerning the maximum of $\sum_{u=0}^{m-1} \|2^u\beta\|^2$ over all β. We remark that in [14] the authors considered the same problem without the square at the $\|\cdot\|$-function.

Lemma 5.2. *Consider $\beta \in \mathbb{R}$ with the canonical base 2 representation (i.e., with infinitely many digits equal to zero). Then there exists*

$$\max_{\beta} \sum_{u=0}^{m-1} \|2^u\beta\|^2 = \frac{m}{9} + \frac{1}{9} - (-1)^m \frac{2}{27\cdot 2^m} - \frac{1}{27\cdot 2^{2m}}$$

and it is attained if and only if β is of the form β_0 with

$$\beta_0 = \frac{2}{3}\left(1 - \left(-\frac{1}{2}\right)^{m+1}\right) \text{ or } \beta_0 = \frac{1}{3}\left(1 - \left(-\frac{1}{2}\right)^{m}\right).$$

Remark. Note that

$$\frac{2}{3}\left(1 - \left(-\frac{1}{2}\right)^{m+1}\right) = \begin{cases} 0,1010\ldots101 & \text{if } m \text{ is odd,} \\ 0,1010\ldots011 & \text{if } m \text{ is even,} \end{cases}$$

and

$$\frac{1}{3}\left(1 - \left(-\frac{1}{2}\right)^{m}\right) = \begin{cases} 0,0101\ldots011 & \text{if } m \text{ is odd,} \\ 0,0101\ldots101 & \text{if } m \text{ is even.} \end{cases}$$

Proof of Lemma 5.2. For any $\gamma = 0, c_1c_2\ldots c_m c_{m+1}\ldots$ with fixed $c_1,\ldots,c_m$ the sum $\sum_{u=0}^{m-1} \|2^u\gamma\|^2$ obviously becomes maximal if $c_m = 0$ and $c_{m+1} = c_{m+2} = \cdots = 1$, or if $c_m = 1$ and $c_{m+1} = c_{m+2} = \cdots = 0$. Hence by Lemma 5.1 the

$$\sup_{\beta} \sum_{u=0}^{m-1} \|2^u\beta\|^2$$

only can be attained, respectively approached by

$$\begin{aligned} &\beta_1 = 0,1010\ldots10\,111\ldots \text{ or} \\ &\quad (b_m \text{ is the last zero}) \\ &\beta_2 = 0,0101\ldots01 \text{ or} \\ &\beta_3 = 0,1010\ldots11 \\ &\quad (b_m \text{ is the last one}) \end{aligned}$$

if m is even, and by

$$\begin{aligned} &\beta_4 = 0,0101\ldots10\,111\ldots \text{ or} \\ &\quad (b_m \text{ is the last zero}) \\ &\beta_5 = 0,1010\ldots01 \text{ or} \\ &\beta_6 = 0,0101\ldots11 \\ &\quad (b_m \text{ is the last one}) \end{aligned}$$

if m is odd.

Now we check easily that

$$\sum_{u=0}^{m-1} \|2^u\beta_k\|^2 = \frac{m}{9} + \frac{1}{9} - (-1)^m \frac{2}{27\cdot 2^m} - \frac{1}{27\cdot 2^{2m}}$$

for $k = 1, \dots, 6$ and the result follows. $\square$

We give the *Proof of Corollary 2.3.* We have

$$\max_{N\le 2^m} \sum_{u=1}^{m} \left\| \frac{N}{2^u} \right\|^2 = \max_{\beta\ m-\mathrm{bit}} \sum_{u=0}^{m-1} \|2^u\beta\|^2 = \frac{m}{9} + \frac{1}{9} - (-1)^m \frac{2}{27\cdot 2^m} - \frac{1}{27\cdot 2^{2m}}$$

by Lemma 5.2. The result follows now together with (2). $\square$

For the proof of Corollary 3.2 we can in principle proceed as for the proof of Corollary 2.3. However, in this case the detailed computations are by far more involved than above. First we have

Lemma 5.3. *Assume that $\beta = 0, b_1b_2\dots$ has two equal consecutive digits b_ib_{i+1} with $i \le m-1$ and let i be minimal with this property, i.e.,*

$$\begin{aligned} \beta &= 0,01\dots 0100 b_{i+2}\dots \quad \textit{or}\\ \beta &= 0,10\dots 0100 b_{i+2}\dots \quad \textit{or}\\ \beta &= 0,01\dots 1011 b_{i+2}\dots \quad \textit{or}\\ \beta &= 0,10\dots 1011 b_{i+2}\dots\ . \end{aligned}$$

Replace β by

$$\begin{aligned} \gamma &= 0,10\dots 1010 b_{i+2}\dots \quad \textit{resp.}\\ \gamma &= 0,01\dots 1010 b_{i+2}\dots \quad \textit{resp.}\\ \gamma &= 0,10\dots 0101 b_{i+2}\dots \quad \textit{resp.}\\ \gamma &= 0,01\dots 0101 b_{i+2}\dots\ . \end{aligned}$$

Then

$$\sum_{u=0}^{m-1} \|2^u\gamma\|^2(m-u) = \sum_{u=0}^{m-1} \|2^u\beta\|^2(m-u) +$$
$$\begin{cases} \left(\frac{m}{9}\left(1-\frac{(-1)^i}{2^i}\right)^2 - \frac{i}{9} + \frac{4}{27\cdot 2^i}\left(\frac{1}{2^i} - (-1)^i\right)\right)(1-\tau) & \textit{in the first two cases,}\\ \left(\frac{m}{9}\left(1-\frac{(-1)^i}{2^i}\right)^2 - \frac{i}{9} + \frac{4}{27\cdot 2^i}\left(\frac{1}{2^i} - (-1)^i\right)\right)\tau & \textit{in the last two cases,} \end{cases}$$

where $\tau := 0, b_{i+2}b_{i+3}\dots$.

Remark. In any case, for $m > 3$, we have $\sum_{u=0}^{m-1} \|2^u\gamma\|^2(m-u) \ge \sum_{u=0}^{m-1} \|2^u\beta\|^2(m-u)$.

Proof of Lemma 5.3. We have

$$\sum_{u=0}^{m-1}(\|2^u\gamma\|^2 - \|2^u\beta\|^2)(m-u)$$
$$= m\|\gamma\|^2-(m-i)\|2^i\beta\|^2+\sum_{u=0}^{i-1}\left(\|2^u(2\gamma)\|^2(m-u-1) - \|2^u\beta\|^2(m-u)\right).$$

The result now follows as in the proof of Lemma 5.1 by some tedious but straightforward algebra. □

With Lemma 5.3 we obtain

Lemma 5.4. *We have*

$$\max_{\beta\ m-bit}\sum_{u=0}^{m-1}\|2^u\beta\|^2(m-u)$$
$$=\begin{cases} \frac{m^2}{18}+\frac{m}{18}+\frac{8}{81}+\frac{1}{2^m}\left(\frac{4}{27}\left(1-\frac{1}{2^m}\right)\left(m+\frac{2}{3}\right)-\frac{8}{81\cdot 2^m}\right) & \text{if } m \text{ is even,}\\ \frac{m^2}{18}+\frac{m}{18}+\frac{8}{81}+\frac{1}{2^m}\left(\frac{m}{27}+\frac{1}{27}\left(1-\frac{1}{2^m}\right)\left(m+\frac{4}{3}\right)\right) & \text{if } m \text{ is odd.}\end{cases}$$

For even m the maximum is attained if and only if

$$\beta=\begin{cases} 0,0101\ldots0110=\frac{1}{3}\left(1+\frac{1}{2^{m-1}}\right) & \text{and}\\ 0,1010\ldots1010=\frac{2}{3}\left(1-\frac{1}{2^m}\right).\end{cases}$$

For odd m the maximum is attained if and only if

$$\beta=\begin{cases} 0,0101\ldots011=\frac{1}{3}\left(1+\frac{1}{2^m}\right) & \text{and}\\ 0,1010\ldots101=\frac{2}{3}\left(1-\frac{1}{2^{m+1}}\right).\end{cases}$$

Proof. For short we write $f_m(\beta):=\sum_{u=0}^{m-1}\|2^u\beta\|^2(m-u)$. Let $m\geq 2$ be even. It follows from Lemma 5.3 that the m-bit number β which maximizes our sum has to be of the form

$$\beta_1=0,0101\ldots01b_{m-1}b_m \quad\text{or}\quad \beta_2=0,1010\ldots10b_{m-1}b_m.$$

First we deal with $\beta_1=0,0101\ldots01b_{m-1}b_m$. Now we consider four cases corresponding to the possible choices for b_{m-1} and b_m.

- If $(b_{m-1},b_m)=(0,0)$, then
$$f_m(\beta_1)=\frac{m^2}{18}+\frac{m}{18}-\frac{1}{81}-\frac{8}{27}\frac{m}{2^m}-\frac{16}{27}\frac{m}{2^{2m}}-\frac{16}{81}\frac{1}{2^m}-\frac{64}{81}\frac{1}{2^{2m}}.$$
- If $(b_{m-1},b_m)=(1,1)$, then
$$f_m(\beta_1)=\frac{m^2}{18}+\frac{m}{18}-\frac{1}{81}+\frac{10}{27}\frac{m}{2^m}-\frac{25}{27}\frac{m}{2^{2m}}+\frac{20}{81}\frac{1}{2^m}-\frac{100}{81}\frac{1}{2^{2m}}.$$
- If $(b_{m-1},b_m)=(1,0)$, then
$$f_m(\beta_1)=\frac{m^2}{18}+\frac{m}{18}+\frac{8}{81}+\frac{4}{27}\frac{m}{2^m}-\frac{4}{27}\frac{m}{2^{2m}}+\frac{8}{81}\frac{1}{2^m}-\frac{16}{81}\frac{1}{2^{2m}}.$$

- If $(b_{m-1}, b_m) = (0,1)$, then

$$f_m(\beta_1) = \frac{m^2}{18} + \frac{m}{18} + \frac{8}{81} - \frac{2}{27}\frac{m}{2^m} - \frac{1}{27}\frac{m}{2^{2m}} - \frac{4}{81}\frac{1}{2^m} - \frac{4}{81}\frac{1}{2^{2m}}.$$

Therefore we find that the choice $(b_{m-1}b_m) = (1,0)$ gives the maximal value, i.e., $\beta_1 = 0,0101\dots0110$. For $\beta_2 = 0,1010\dots10b_{m-1}b_m$ we find in the same way that $(b_{m-1}, b_m) = (1,0)$ gives the maximal value, i.e., $\beta_2 = 0,1010\dots1010$. Since

$$f_m(\beta_1) = f_m(\beta_2) = \frac{m^2}{18}+\frac{m}{18}+\frac{8}{81}+\frac{1}{2^m}\left(\frac{4}{27}\left(1-\frac{1}{2^m}\right)\left(m+\frac{2}{3}\right) - \frac{8}{81\cdot 2^m}\right)$$

the result follows for even $m \geq 2$.

For odd $m \geq 3$ the result can be proved analogously. □

We give the *Proof of Corollary 3.2.* We have

$$\max_{N\leq 2^m}\sum_{u=1}^{m}\left\|\frac{N}{2^u}\right\|^2 u = \max_{\beta\ m-\mathrm{bit}}\sum_{u=0}^{m-1}\|2^u\beta\|^2(m-u) = \frac{m^2}{18}+\frac{m}{18}+\frac{8}{81}+O\left(\frac{m}{2^m}\right)$$

by Lemma 5.4. The result follows now together with (3). □

Acknowledgement

The author is supported by the Austrian Science Foundation (FWF), Project S9609, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory". Furthermore, the author wishes to thank Peter Kritzer for his comments for improving the style of the paper and Ligia Loretta Cristea for the translation of the abstract.

References

[1] H. Chaix and H. Faure, *Discrépance et diaphonie en dimension un.* Acta Arith. **63** (1993), 103–141.

[2] J. Dick and F. Pillichshammer, *Multivariate integration in weighted Hilbert spaces based on Walsh functions and weighted Sobolev spaces.* J. Complexity **21** (2005), 149–195.

[3] J. Dick and F. Pillichshammer, *Dyadic diaphony of digital nets over* $\mathbb{Z}_2$. Monatsh. Math. **145** (2005), 285–299.

[4] J. Dick and F. Pillichshammer, *On the mean square weighted* $\mathcal{L}_2$*-discrepancy of randomized digital* (t,m,s)*-nets over* $\mathbb{Z}_2$. Acta Arith. **117** (2005), 371–403.

[5] J. Dick and F. Pillichshammer, *Diaphony, discrepancy, spectral test and worst-case error.* Math. Comput. Simulation **70** (2005), 159–171.

[6] M. Drmota, G. Larcher and F. Pillichshammer, *Precise distribution properties of the van der Corput sequence and related sequences.* Manuscripta Math. **118** (2005), 11–41.

[7] M. Drmota and R.F. Tichy, *Sequences, Discrepancies and Applications.* Lecture Notes in Mathematics **1651**, Springer-Verlag, Berlin, 1997.

[8] H. Faure, *Discrepancy and diaphony of digital* $(0,1)$*-sequences in prime base.* Acta Arith. **117** (2004), 125–148.

[9] H. Faure, *Irregularites of distribution of digital* $(0,1)$*-sequences in prime base.* Integers **5** (2005), A7, 12 pages.

[10] V.S. Grozdanov, *On the diaphony of one class of one-dimensional sequences*. Internat. J. Math. Math. Sci. **19** (1996), 115–124.

[11] P. Hellekalek and H. Leeb, *Dyadic diaphony*. Acta Arith. **80** (1997), 187–196.

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

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

[14] G. Larcher and F. Pillichshammer, *Sums of distances to the nearest integer and the discrepancy of digital nets*. Acta Arith. **106** (2003), 379–408.

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

[16] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*. No. **63** in CBMS-NSF Series in Applied Mathematics. SIAM, Philadelphia, 1992.

[17] F. Pillichshammer, *Digital sequences with best possible order of L_2–discrepancy*. Mathematika **53** (2006), 149–160.

[18] P.D. Proinov and V.S. Grozdanov, *On the diaphony of the van der Corput-Halton sequence*. J. Number Theory **30** (1988), 94–104.

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

Friedrich Pillichshammer
Universtät Linz
Institut für Finanzmathematik
Altenbergerstrasse 69
A-4040 Linz, Austria
E-mail : friedrich.pillichshammer@jku.at