Uniform Distribution Theory **6** (2011), no.2, 31–46

uniform distribution theory

# A LOWER BOUND FOR THE DIAPHONY OF GENERALISED VAN DER CORPUT SEQUENCES IN ARBITRARY BASE $b$

Florian Pausinger – Wolfgang Ch. Schmid

ABSTRACT. The diaphony is a common measure for uniformity of a given infinite sequence. We discuss a method of Faure which he used to obtain an upper bound for the diaphony of generalised van der Corput sequences in arbitrary base $b$. We extend this method to derive a lower bound as well as a criterion to decide whether two sequences have the same distribution behaviour.

*Communicated by Vassil Grozdanov*

## 1. Introduction

Faure ([1] together with Chaix, [2]) developed the basic tools for the investigation of the distribution behaviour of generalised van der Corput sequences, which can be generated by permutations. In the last years these tools turned out to be useful in many other and more general situations (see [7], [8], [9], [10]). In 1992 Faure (see [4]) was able to improve his first results by giving new permutations, that generate sequences with very good distribution behaviour. Recently, due to improved computer systems, it was possible to further improve these results (see [11] and [12]). However, this computer-based search does not tell much about the structure of good permutations. In this paper we will analyse the main tool for computing the diaphony of generalised van der Corput sequences and we will derive a lower bound for it (see Theorem 5) as well as a criterion for deciding if two permutations have the same value for the diaphony. We will reveal the structure of optimal subsolutions for the challenging problem

2010 Mathematics Subject Classification: 11K06, 11K38.
Keywords: Diaphony, generalised van der Corput sequence.
This work 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".

of constructing optimal permutations. Since the basic tools we use can be applied to more general problems in higher dimensions, our results are not only interesting for the one dimensional generalised van der Corput sequences.

## 2. Definitions and Notations

Let $X = (x_i)_{i\geq 1}$ be an infinite sequence in the half open unit interval $[0,1[$. For $N \geq 1$ and for reals $0 \leq \alpha < \beta \leq 1$ let $A([\alpha,\beta[,N,X)$ denote the number of indices $i \leq N$ for which $x_i \in [\alpha,\beta[$. The discrepancy function of $X$ is defined as $E([\alpha,\beta[,N,X) := A([\alpha,\beta[,N,X) - (\beta-\alpha)N$.

Throughout the paper let $b \geq 2$ and $n \geq 1$ be integers. Let $\mathfrak{S}_b$ be the set of all permutations of $\{0,1,\ldots,b-1\}$. The identity in $\mathfrak{S}_b$ is always denoted by $id$. In all examples and concrete results we will write down the permutations in the following way: For $\sigma = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,4\,2\,6\,1\,5\,3\,7 \end{pmatrix}$ we will write $\sigma = (0,4,2,6,1,5,3,7)$.

**Definition 1** (Zinterhof, [13])**.** *For any one dimensional, infinite sequence $X$ the diaphony $F$ of the first $N$ points of $X$ is defined by*

$$F(N,X) := \left(2 \cdot \sum_{m=1}^{\infty} \frac{1}{m^2} \left| \sum_{n=1}^{N} \exp^{2\pi i m x_n} \right|^2 \right)^{1/2}.$$

**Remark 1.** *Note that there is an equivalent definition for the diaphony (details in* [5]*): For any one dimensional, infinite sequence $X$ the diaphony $F$ of the first $N$ points of $X$ is defined by*

$$F(N,X) := \left(2\pi^2 \int_0^1 \int_0^1 |E([\alpha,\beta[,N,X)|^2 d\alpha d\beta\right)^{1/2}.$$

We call a one dimensional sequence $X$ a *low discrepancy sequence* if there exists a constant $c$ such that for all $N$

$$F^2(N,X) \leq c \cdot \log N.$$

As a consequence computing

$$f(X) := \limsup_{N\to\infty} (F^2(N,X)/\log N)$$

enables us to look for sequences with "best distribution" behaviour.

**Definition 2.** *For a fixed base $b \geq 2$ and a permutation $\sigma \in \mathfrak{S}_b$ the generalised van der Corput sequence $S_b^\sigma$ is defined by*

$$S_b^\sigma(n) = \sum_{j=0}^{\infty} \sigma(a_j(n)) b^{-j-1},$$

*where $\sum_{j=0}^{\infty} a_j(n) b^j$ is the $b$-adic representation of an integer $n \geq 1$.*

The analysis of the diaphony of $S_b^\sigma$ is based on special functions which have been first introduced by Faure in [2] and which are defined as follows:

**Definition 3.** *For $\sigma \in \mathfrak{S}_b$ let $Z_b^\sigma := (\sigma(0)/b, \sigma(1)/b, \ldots, \sigma(b-1)/b)$. For $h \in \{0, 1, \ldots, b-1\}$ and $x \in \left[\frac{k-1}{b}, \frac{k}{b}\right[$, where $k \in \{1, \ldots, b\}$ we define*

$$\varphi_{b,h}^\sigma(x) := \begin{cases} A([0, h/b[; k; Z_b^\sigma) - hx, & \text{if } 0 \leq h \leq \sigma(k-1), \\ (b-h)x - A([h/b, 1[; k; Z_b^\sigma), & \text{if } \sigma(k-1) < h < b. \end{cases}$$

*The function $\varphi_{b,h}^\sigma$ is extended to the reals by periodicity.*

Note that $\varphi_{b,h}^\sigma(0) = 0$ for any $\sigma \in \mathfrak{S}_b$ and any $h \in \{0, \ldots, b-1\}$.

In [1] Chaix and Faure introduced a new class of functions based on $\varphi_{b,h}^\sigma$:

**Definition 4.**

$$\chi_b^\sigma := \sum_{0 \leq h < h' < b} (\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2.$$

**Proposition 1** (Propriété 3.3 and Propriété 3.5 in [1])**.** *The following holds:*

- *The functions $\chi_b^\sigma$ are continuous, piecewise quadratic on the intervals $[k/b, (k+1)/b]$, and $\chi_b^\sigma(0) = \chi_b^\sigma(1)$.*
- *For each interval $[k/b, (k+1)/b]$ the parabolic arcs of $\chi_b^\sigma$ are translated versions of the parabola $y = b^2(b^2-1)x^2/12$.*

The starting point for our work are two theorems that show that the diaphony of $S_b^\sigma$ can be computed exactly. The first theorem states how to compute the diaphony of the first $N$ points of $S_b^\sigma$, whereas the second theorem lets us investigate the asymptotic behaviour.

**Theorem 1** (Théorème 4.2 in [1])**.** *For all $N \geq 1$, we have*

$$F^2(N, S_b^\sigma) = 4\pi^2 \sum_{j=1}^{\infty} \chi_b^\sigma(Nb^{-j})/b^2.$$

**Theorem 2** (Théorème 4.10 in [1]). *Let*

$$\gamma_b^\sigma := \inf_{n\geq 1} \sup_{x\in[0,1]} \left( \sum_{j=1}^{n} \chi_b^\sigma(xb^{-j})/n \right),$$

*then*

$$f(S_b^\sigma) = \limsup_{N\to\infty} (F^2(N, S_b^\sigma)/\log N) = 4\pi^2\gamma_b^\sigma/(b^2\log b).$$

## 3. Crucial Lemma of Faure

In [6] Faure proved the following lemma:

**Lemma 1.** *For any permutation $\sigma \in \mathfrak{S}_b$, we have $\chi_b^\sigma \leq \chi_b^{id}$.*

We would like to recall parts of the proof in order to introduce the techniques leading to our lower bounds in the next two sections.

First note that

$$\chi_b^\sigma = \sum_{0\leq h<h'<b} (\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2 = \frac{1}{2} \sum_{h\neq h'} (\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2$$

and that on each interval $\left[\frac{k-1}{b}, \frac{k}{b}\right]$ $(1 \leq k \leq b)$, $\chi_b^\sigma$ has the form

$$\chi_b^\sigma(x) = \frac{b^2(b^2-1)}{12} x^2 + Ax + B,$$

with A and B depending on $\sigma$ and $k$; thus $\chi_b^{id} - \chi_b^\sigma$ is an affine function, such that $\chi_b^{id} - \chi_b^\sigma \geq 0$ if and only if $\chi_b^{id}(\frac{k}{b}) \geq \chi_b^\sigma(\frac{k}{b})$ for all $1 \leq k \leq b$. On the other hand, for arbitrary $h \neq h'$, $\varphi_{b,h'}^\sigma(\frac{k}{b}) - \varphi_{b,h}^\sigma(\frac{k}{b}) = E\left(\left[\frac{h}{b}, \frac{h'}{b}\right[, k, Z_b^\sigma\right)$ since $\varphi_{b,h}^\sigma = E\left(\left[0, \frac{h}{b}\right[, k, Z_b^\sigma\right)$. Therefore proving the lemma amounts to proving that for fixed $k$ $(1 \leq k \leq b)$

$$\sum_{h\neq h'} \left( E\left(\left[\frac{h}{b}, \frac{h'}{b}\right[, k, Z_b^\sigma\right)\right)^2 \leq \sum_{h\neq h'} \left( E\left(\left[\frac{h}{b}, \frac{h'}{b}\right[, k, Z_b^{id}\right)\right)^2. \qquad (1)$$

To obtain this result we split up the sum into sets of couples $(h, h')$ satisfying $l([\frac{h}{b}, \frac{h'}{b}[) = \frac{d}{b}$ (where $l$ denotes the length of the interval), with $1 \leq d \leq b-1$, so that we get $(b-1)$ sets, each one containing $b$ terms and we proceed to compare the two sums set by set with fixed $d$. In other words we take (as Faure called it) a window $(\frac{d}{b})$-wide and we move the window along the torus $[0, 1[$ with the step

$\frac{1}{b}$ (from $[0, \frac{d}{b}[$ to $[\frac{1}{b}, \frac{d+1}{b}[$, and so on until $[1-\frac{1}{b}, \frac{d-1}{b}[$), calculating at each step the discrepancy function

$$E\left(\left[\frac{h}{b}, \frac{h'}{b}\right[, k, Z_b^\sigma\right) = \delta_{h,h'}^\sigma - \frac{dk}{b}, \quad with \;\; \delta_{h,h'}^\sigma := A\left(\left[\frac{h}{b}, \frac{h'}{b}\right[, k, Z_b^\sigma\right)$$

and summing the squares.
For simplicity we write $l(h,h') = d$ instead of $l([\frac{h}{b}, \frac{h'}{b}[) = \frac{d}{b}$. In that way we get,

$$\sum_{l(h,h')=d} \left(\delta_{h,h'}^\sigma - \frac{dk}{b}\right)^2 = \sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2 - \frac{2dk}{b} \sum_{l(h,h')=d} \delta_{h,h'}^\sigma + \frac{d^2k^2}{b^2} \sum_{l(h,h')=d} 1.$$

Now we claim that $\sum_{l(h,h')=d} \delta_{h,h'}^\sigma = dk$, (and therefore independent of $\sigma$): Indeed we have $k$ points of $Z_b^\sigma$ and each one occurs $d$ times in $A([\frac{h}{b}, \frac{h'}{b}[, k, Z_b^\sigma)$ when the window moves from $[0, \frac{d}{b}[$ to $[1-\frac{1}{b}, \frac{d-1}{b}[$. Thus we obtain

$$\sum_{l(h,h')=d} \left(\delta_{h,h'}^\sigma - \frac{dk}{b}\right)^2 = \sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2 - \frac{d^2k^2}{b} \tag{2}$$

for any $\sigma$, so that we only need to compare

$$\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2 \;\; \text{to} \sum_{l(h,h')=d} (\delta_{h,h'}^{id})^2 \tag{3}$$

with the condition

$$\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma) = \sum_{l(h,h')=d} (\delta_{h,h'}^{id}) = kd. \tag{4}$$

Since we are here only interested in the techniques of the first part of the proof we omit the rest, where the two sums are compared and where it is shown that the identical permutation maximizes the sum for each $k$. □

In the following we are interested in extending the technique used in this lemma. Our goal is to minimize these sums for each $k$.

## 4. A First Lower Bound

According to the idea of the previous section, if we fix $k$, $(1 \le k \le b)$, we are only interested in the $(b-1)$ sums of the form $\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2$, for which we know that $\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma) = kd$ for any permutation $\sigma$. However the summands $\delta_{h,h'}^\sigma$ of these second sums might differ depending on the permutation and therefore the according sum of squares might be different for different permutations.

We can visualize the summands $\delta^{\sigma}_{h,h'}$ in a $(b-1)\times b$ matrix $\mathcal{M}^{\sigma}_{k}=(m_{i,j})$, where $m_{i,j}=\delta^{\sigma}_{j,j\oplus i}$ with $j\oplus i:=j+i \pmod b$. This means that $m_{i,j}$ represents the number of points lying in the interval $[j,j+i[$.

$$\begin{array}{r} \\ d=1 \\ \vdots \\ \vdots \\ d=i \\ \vdots \\ \vdots \\ d=b-1 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} 0 & . & . & j & . & . & b-1 \end{array} \\
\left(\begin{array}{ccccccc}
\delta^{\sigma}_{0,1} & . & . & . & . & . & \delta^{\sigma}_{b-1,0} \\
. & . & & & & . & . \\
. & & . & & . & & . \\
. & & & \delta^{\sigma}_{j,j\oplus i} & & & . \\
. & & . & & . & & . \\
. & . & & & & . & . \\
\delta^{\sigma}_{0,b-1} & . & . & . & . & . & \delta^{\sigma}_{b-1,b-2}
\end{array}\right)
\end{array}
\begin{array}{l} \\ \sum_{row}=k \\ \vdots \\ \vdots \\ \sum_{row}=ik \\ \vdots \\ \vdots \\ \sum_{row}=(b-1)k \end{array}$$

If we turn now from $k$ to $k+1$ points, or, in other words, if we compare $\mathcal{M}^{\sigma}_{k}$ and $\mathcal{M}^{\sigma}_{k+1}$, we see that the two matrices differ in the following triangle of 1's, in which the first 1 is added at position $m_{1,j}$ if the point is added at position $j$:

$$\left(\begin{array}{ccccccccc}
 & & & 1 & & & & & \\
 & & . & . & & & & & \\
 & . & & . & & & & & \\
1 & . & . & 1 & & & & & \\
. & & & . & & & & & 1 \\
. & & & . & & & & . & . \\
. & & & . & & & . & & . \\
1 & . & . & 1 & 0 & 1 & . & . & 1
\end{array}\right)$$

This triangle appears due to the fact that there is exactly one interval of length 1, namely $[j,j+1[$, with an additional point, if a point is added at position $j$. Moreover there are exactly two intervals of length 2, namely $[j-1,j+1[$ and $[j,j+2[$, containing an additional point, if a point is added at position $j$ and so on. Before we summarize various properties of the matrices in a lemma, it is convenient to define a counting function:

**Definition 5.** *The function $\#_{\mathcal{M}^{\sigma}_{k}}(u)$ counts how often the value $u$, for $0\le u\le k$, appears in $\mathcal{M}^{\sigma}_{k}$ and $\#_{l,\mathcal{M}^{\sigma}_{k}}(u)$ counts how often $u$ appears in the $l$-th row of $\mathcal{M}^{\sigma}_{k}$. For convenience we will write $\#(u)$ resp. $\#_l(u)$ instead of $\#_{\mathcal{M}^{\sigma}_{k}}(u)$ resp. $\#_{l,\mathcal{M}^{\sigma}_{k}}(u)$, if it is clear which matrix is meant.*

Note that for any matrix $\#(u)=\sum_{l=1}^{b-1}\#_l(u)$.

**Lemma 2.** *For fixed base $b$ and $\sigma \in \mathfrak{S}_b$ and for $1 \le k \le b$ the corresponding matrix $\mathcal{M}_k^\sigma = (m_{i,j})$ has the following properties:*

(i) *For each row $i$ of $\mathcal{M}_k^\sigma$ we have $\sum_{j=0}^{b-1} m_{i,j} = ik$.*

(ii) *For each row $i$ of $\mathcal{M}_k^\sigma$ it holds that $|m_{i,j} - m_{i,j\oplus 1}| \in \{0,1\}$.*

(iii) *For each column $j$ of $\mathcal{M}_k^\sigma$ we have $m_{i,j} \le m_{i+1,j}$.*

(iv) *For each $m_{i,j}$ we have $m_{i,j} \le \min\{i,k\}$.*

(v) *$\sum_{u=0}^{b} \#(u) = b(b-1)$ and $\sum_{u=0}^{b} \#(u)u = k\frac{(b-1)b}{2}$.*

Proof. **(i)** This is obvious. **(ii)** Since it is not allowed to put points at the same position, it is not possible that two triangles lie on each other and so it is not possible that two consecutive values in row $i$ of $\mathcal{M}_k^\sigma$ differ by more than 1. **(iii)** The matrix $\mathcal{M}_k^\sigma$ is created by $k$ triangles. For each triangle we have that if 1 is added at $m_{i,j}$, then also at all positions $m_{i',j}$ with $i < i' \le (b-1)$. **(iv)** This holds since $i$ denotes the length of the interval and $k$ the number of already distributed points. **(v)** The matrix $\mathcal{M}_k^\sigma$ is a $(b-1) \times b$ matrix; so there are exactly $(b-1)b$ many entries with a certain value $u$. Moreover one triangle consists of $\frac{b(b-1)}{2}$ 1's. Therefore the sum of $k$ triangles is $k\frac{(b-1)b}{2}$. □

Note that these matrices have another crucial property, namely

$$\#(u) = \#(k-u),$$

for all $0 \le u \le k$. This will be proved in Corollary 4.

Generally, if we have a vector $m_d = (m_{d,0}, \dots, m_{d,b-1})$ and know for some fixed $k$ that $\sum_{j=0}^{b-1} m_{d,j} = kd$, then

$$\min_{m_d} \sum_{j=0}^{b-1} (m_{d,j})^2 = (b-\gamma)\left(\left\lfloor \frac{kd}{b} \right\rfloor\right)^2 + \gamma\left(\left\lfloor \frac{kd}{b} + 1 \right\rfloor\right)^2 =: L_b^{k,d} \tag{5}$$

for $kd \equiv \gamma \pmod b$, with $\gamma \in \{0, \dots, b-1\}$. This follows immediately from the fact that for $a$, $b \in \mathbb{N}$ with $b \ge a$

$$a^2 + b^2 < (a-1)^2 + (b+1)^2.$$

Consequently Lemma 2(i) enables us to find a minimal possible value for the sums in Equation (2) for each $k$ and each $d$.

**Theorem 3.** *For arbitrary base $b$ and arbitrary $\sigma \in \mathfrak{S}_b$ and for each $k$, $1 \le k \le b$,*

$$\chi_b^\sigma\left(\frac{k}{b}\right) \ge L_b^k$$

*holds, where* $L_b^k := \frac{1}{2}\sum_{d=1}^{b-1}\left(L_b^{k,d} - \frac{d^2k^2}{b}\right)$ *and* $L_b^{k,d} := (b-\gamma)(\lfloor\frac{kd}{b}\rfloor)^2 + \gamma(\lfloor\frac{kd}{b}+1\rfloor)^2$*, for* $kd \equiv \gamma \pmod b$*, with* $\gamma \in \{0,\dots,b-1\}$*.*

P r o o f. For arbitrary $\sigma$ we have $\chi_b^\sigma = \frac{1}{2}\sum_{h\neq h'}(\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2$ and we know for fixed $k$, $\varphi_{b,h'}^\sigma\left(\frac{k}{b}\right) - \varphi_{b,h}^\sigma\left(\frac{k}{b}\right) = E\left(\left[\frac{h}{b},\frac{h'}{b}\right[, k, Z_b^\sigma\right)$. Moreover we already know for fixed $d = h'-h$

$$E\left(\left[\frac{h}{b},\frac{h'}{b}\right[, k, Z_b^\sigma\right) = \delta_{h,h'}^\sigma - \frac{dk}{b} \quad \textit{with} \quad \delta_{h,h'}^\sigma := A\left(\left[\frac{h}{b},\frac{h'}{b}\right[, k, Z_b^\sigma\right).$$

Due to the observations in (2) and (5) it follows that

$$\begin{aligned}\sum_{l(h,h')=d}\left(E\left(\left[\frac{h}{b},\frac{h'}{b}\right[, k, Z_b^\sigma\right)\right)^2 &= \sum_{l(h,h')=d}\left(\delta_{h,h'}^\sigma - \frac{dk}{b}\right)^2\\ &= \sum_{l(h,h')=d}(\delta_{h,h'}^\sigma)^2 - \frac{d^2k^2}{b} \geq L_b^{k,d} - \frac{d^2k^2}{b}.\end{aligned}$$

We can now take the sum over all $d$ and derive the following lower bound for arbitrary fixed $k$:

$$2\chi_b^\sigma\left(\frac{k}{b}\right) = \sum_{h\neq h'}\left(E\left(\left[\frac{h}{b},\frac{h'}{b}\right[, k, Z_b^\sigma\right)\right)^2 \geq \sum_{d=1}^{b-1}\left(L_b^{k,d} - \frac{d^2k^2}{b}\right) = 2L_b^k.$$

□

**Remark 2.** *Due to the fact that on each interval* $\left[\frac{k-1}{b},\frac{k}{b}\right]$ $(1\leq k\leq b)$*, every* $\chi_b^\sigma$*-function is of the form* $\chi_b^\sigma(x) = \frac{b^2(b^2-1)}{12}x^2 + Ax + B$*, with* $A$ *and* $B$ *only depending on* $\sigma$ *and* $k$*, it suffices to determine the values* $L_b^k$ *for each* $k$ *in order to get a lower-bound function for all* $x\in[0,1]$*. With this lower-bound function the usual observations concerning asymptotics can be performed; especially determining dominating intervals (see* [4] *and* [12]*) and therefore getting lower bounds for one-dimensional diaphony.*

**Remark 3.** *Note that this lower bound does not take the structure of the triangles of 1's into account. In general it is not possible to obtain matrices* $\mathcal{M}_k^\sigma$ *such that* $\chi_b^\sigma(\frac{k}{b}) = L_b^k$*.*

## 5. Main Results

In this section we continue our study of the matrices $\mathcal{M}_k^\sigma$. We give a criterion when two matrices have the same sum of squares of all entries (see Theorem

4). This result is useful if one wants to show that certain permutations generate sequences with the same distribtuion behaviour (see Corollary 1, 2, 3). Moreover, we improve the lower bound of Theorem 3 (see Theorem 5). It is convenient to introduce some further notation before we state our results.

### 5.1. Further Notation

Let $\sigma \in \mathfrak{S}_b$ and let $\mathcal{Z}_{b,k}^{\sigma}$, or short $\mathcal{Z}_{b,k}$, be the set of the first $k$ values of the permutation $\sigma$. For each set $\mathcal{Z}_{b,k}^{\sigma}$ there exists a $(b-1) \times b$ matrix $\mathcal{M}_k^{\sigma}$ of the above form. Hence each permutation generates a sequence $(\mathcal{M}_k^{\sigma})_{k=1}^{b}$ of matrices. Let

$$\mathcal{N}(\mathcal{M}_k^{\sigma}) := \sum_{i=1}^{b-1} \sum_{j=0}^{b-1} (m_{i,j})^2.$$

If a set $\mathcal{Z}_{b,k}^{\sigma}$ contains $j$ consecutive numbers we call this a $j$-block or block of length $j$; if $j'$ consecutive numbers are missing we call this a gap of length $j'$. Moreover if we consider two integers $u, v \in \mathcal{Z}_{b,k}^{\sigma}$ and their corresponding triangles of 1's, then these triangles intersect at certain positions $m_{i,j}$ of the matrix. We denote the number of matrix positions, where these triangles intersect, with $\mathcal{F}(u, v)$. Note that we only consider pairwise intersections of triangles and that we write $\mathcal{F}(u, v)$ instead of $\mathcal{F}((u, v))$.

**Example.** Let $\mathcal{Z}_{15,5} = \{0, 1, 2, 8, 9\}$. Then we have a block of length 3, a block of length 2 and two gaps of length 5.

**Example.** Let $b = 6$, $u = 2$, $v = 4$, then we have $\mathcal{F}(2, 4) = 7$:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 1 & 0 \\ 1 & 2 & 2 & 1 & 1 & 1 \\ 2 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}$$

In general we can compute this area of intersection of two triangles in the following way:

**Lemma 3.** *Let $b$ be a given base, $0 \leq u \leq b-1$ and $0 \leq i < \frac{b}{2}$. Then*

$$\mathcal{F}(u, u \oplus i) = \frac{(b-i-1)(b-i)}{2} + \frac{(i-1)i}{2}. \tag{6}$$

Proof. Note that we are on a discrete torus of length $b$. The triangles of 1's we place there have length $(b-1)$ and therefore occupy exactly $\frac{(b-1)b}{2}$ positions. If we place one triangle at position $u$, then the formula says that for $i = 0$,

$\mathcal{F}(u,u) = \frac{(b-1)b}{2}$, which is correct since the two triangles are lying on each other. If we shift the second triangle one position to the right, the length of the triangle of intersection decreases by 1 and therefore the two triangles have $\frac{(b-2)(b-1)}{2}$ many positions of intersection. Since we are on a torus of length $b$, we get for $i \geq 2$ two triangles of intersection. For each position we shift, we decrease the length of one triangle by one, whereas the length of the second triangle is increased by one thus giving the formula. □

Note that the number of 0's in a matrix $\mathcal{M}_k^\sigma$ already determines the number and the length of the gaps in the corresponding set $\mathcal{Z}_{b,k}^\sigma$. This is due to the fact that if there is a gap of length $j$ between two consecutive blocks, this corresponds to a triangle of $\frac{j(j+1)}{2}$ many 0's in the matrix. The sum of the lengths of all gaps always equals $(b-k)$. Note that in row 2 we then always have exactly $((b-k)-N)$ 0's, where $N$ denotes the number of gaps. If we apply this idea repeatedly the statement follows.

### 5.2. On Sets of Numbers with the Same Value for $\mathcal{N}(\mathcal{M}_k^\sigma)$

In this subsection we are interested in the structure of sets $\mathcal{Z}_{b,k}^\sigma$ that have the same value for $\mathcal{N}(\mathcal{M}_k^\sigma)$ for fixed $k$, but different $\sigma$.

Let $\mathcal{Z}_{b,k}^{\sigma_1} \neq \mathcal{Z}_{b,k}^{\sigma_2}$. Then we define new sets

$$A_1 := \{(u,v) : u,v \in \mathcal{Z}_{b,k}^{\sigma_1}\},$$
$$A_2 := \{(u,v) : u,v \in \mathcal{Z}_{b,k}^{\sigma_2}\}$$

containing all pairs of elements of $\mathcal{Z}_{b,k}^{\sigma_1}$ resp. $\mathcal{Z}_{b,k}^{\sigma_2}$; hence $|A_1| = |A_2| = \binom{k}{2}$.

**Theorem 4.** *Let* $\mathcal{Z}_{b,k}^{\sigma_1} \neq \mathcal{Z}_{b,k}^{\sigma_2}$.

$$\mathcal{N}(\mathcal{M}_k^{\sigma_1}) = \mathcal{N}(\mathcal{M}_k^{\sigma_2})$$

*if and only if there exists a bijective map* $f : A_1 \to A_2$ *such that* $\mathcal{F}(u,v) = \mathcal{F}(f(u,v))$.

Proof. "⇐": We have to show that for any bijective function $f$, that maps pairs of points into pairs of points such that their area of intersection remains the same, there exists a bijection $h$ between the corresponding matrices such that

$$m_{i,j}^{\sigma_1} = m_{h(i,j)}^{\sigma_2}.$$

We will show that having the same pairwise intersections imply having the same values in each row of the matrix (only the order might be different which does not change the sum of the squares). We will prove this by contradiction. Suppose there is one row $i$ such that the two matrices $\mathcal{M}_k^{\sigma_1}$ and $\mathcal{M}_k^{\sigma_2}$ do not contain the

same values in this row. Recall that the sum of all values in a row is always the same in both matrices (see Lemma 2(i)). W.l.o.g. let the first matrix contain a greater value in row $i$, which also means more smaller values appear than in the second matrix. However this means that there exist triangles in the first matrix that have a greater area of intersection than in the second matrix. But this is a contradiction to our assumption.

"$\Rightarrow$": Let $\mathcal{M}_k^{\sigma_1} = (m_{i,j}^{\sigma_1})$ and $\mathcal{M}_k^{\sigma_2} = (m_{i,j}^{\sigma_2})$. Then

$$\mathcal{N}(\mathcal{M}_k^{\sigma_1}) = \sum_{i=1}^{b-1}\sum_{j=0}^{b-1}(m_{i,j}^{\sigma_1})^2 = \sum_{i=1}^{b-1}\sum_{j=0}^{b-1}(m_{i,j}^{\sigma_2})^2 = \mathcal{N}(\mathcal{M}_k^{\sigma_2}) \tag{7}$$

means that there exists a bijective map $h$ with $m_{i,j}^{\sigma_1} = m_{h(i,j)}^{\sigma_2}$ for all $1 \le i \le b-1$ and $0 \le j \le b-1$, since we are summing squares. However this $h$ is not uniquely determined. We will show that there is a map $h$ that preserves the rowindex $i$ such that $m_{i,j}^{\sigma_1} = m_{h(i,j)}^{\sigma_2} = m_{i,j'}^{\sigma_2}$.

Suppose there is no such $h$ that preserves rowindices. This means that there is a row $i$ and a value $l$ such that $\#_{i,\mathcal{M}_k^{\sigma_1}}(l) > \#_{i,\mathcal{M}_k^{\sigma_2}}(l)$. Since the sums of the two rows are the same, we will also get $\#_{i,\mathcal{M}_k^{\sigma_1}}(l+1) \neq \#_{i,\mathcal{M}_k^{\sigma_2}}(l+1)$ and $\#_{i,\mathcal{M}_k^{\sigma_1}}(l-1) \neq \#_{i,\mathcal{M}_k^{\sigma_2}}(l-1)$. Even if the sum of the two rows might be the same when changing the number of certain values, the squares of the summands are different. Moreover there is no possibility due to the monotonicity of the columns (see Lemma 2(iii) ) to equal the number of summands in the two matrices with values $l-1$, $l$ and $l+1$ again. (Note that the sums of the rows before and after should also not change.) But this is a contradiction to our assumption. Consequently there must be a map $h$ that preserves rowindices.

Now take such an $h$ and suppose there is no $f$ of the above form. This means that for all possible $f$ there exists at least one pair $(u,v)$ such that $\mathcal{F}(u,v) \neq \mathcal{F}(f(u,v))$. This means that it is not possible to find a map $f$ such that the corresponding matrices have the same number of entries with a certain value $l$ in each row. But this is a contradiction since we know that $h$ maps all rows into rows with the same values. Hence there exists such an $f$. □

**Corollary 1.** *Let $\sigma_1, \sigma_2 \in \mathfrak{S}_b$ with $\mathcal{Z}_{b,k}^{\sigma_1} \neq \mathcal{Z}_{b,k}^{\sigma_2}$. If there exists an integer $m$ such that $\mathcal{Z}_{b,k}^{\sigma_2} = m \oplus \mathcal{Z}_{b,k}^{\sigma_1} := \{m \oplus i : i \in \mathcal{Z}_{b,k}^{\sigma_1}\}$, then $\mathcal{N}(\mathcal{M}_k^{\sigma_1}) = \mathcal{N}(\mathcal{M}_k^{\sigma_2})$.*

Proof. For arbitrary $u, v \in \mathcal{Z}_{b,k}^{\sigma_1}$ define

$$f(u,v) = (u \oplus m, v \oplus m).$$

Then $f(u,v)$ is a uniquely determined element of $A_2$ with $\mathcal{F}(u,v) = \mathcal{F}(f(u,v))$. □

The next corollary is a theorem of Chaix and Faure, which we reformulate in our notation.

**Corollary 2** (Théorème 4.4 in [1]). *Let $m$ be an integer with $0 < m < b$ and $\sigma, \tau \in \mathfrak{S}_b$ with*

$$\tau(l) = \sigma(l) \oplus m,$$

*with $0 \leq l \leq b-1$. Then*

$$F(N, S_b^\sigma) = F(N, S_b^\tau).$$

Proof. Note that we can apply Corollary 1 for each pair of sets $\left(\mathcal{Z}_{b,l}^\sigma, \mathcal{Z}_{b,l}^\tau\right)$ with $0 \leq l \leq b-1$. This means that the corresponding functions $\chi_b^\sigma$ and $\chi_b^\tau$ have the same value for each $x = \frac{l}{b}$ and are therefore identical (see Remark 2). □

**Remark 4.** *This justifies why we only consider permutations $\sigma$ with $\sigma(0) = 0$.*

**Corollary 3.** *Let $\sigma, \tau \in \mathfrak{S}_b$ with $\sigma(0) = \tau(0) = 0$ and*

$$\tau(l) = b - \sigma(l),$$

*for $1 \leq l \leq b-1$. Then*

$$F(N, S_b^\sigma) = F(N, S_b^\tau).$$

Proof. Note that we can choose the map $f(u, v) = (b-u, b-v)$, where we set $b - 0 = 0$, in each step $l$. Hence $\mathcal{N}(\mathcal{M}_l^\sigma) = \mathcal{N}(\mathcal{M}_l^\tau)$ for all $1 \leq l \leq b-1$. □

Now we can prove another property of the matrices $\mathcal{M}_k^\sigma$ which we already mentioned in Section 4.

**Corollary 4.** *If $\#(u)$ denotes how often the value $u$ appears in $\mathcal{M}_k^\sigma$, then $\#(u) = \#(k-u)$, especially $\#(0) = \#(k)$.*

Proof. Consider an arbitrary set $\mathcal{Z}_{b,k}^\sigma$. Due to Corollary 3 we already know that for the set $\mathcal{Z}_{b,k}^\tau$, with $\tau(l) = b - \sigma(l)$ $(1 \leq l \leq k)$, we get $\mathcal{N}(\mathcal{M}_k^\sigma) = \mathcal{N}(\mathcal{M}_k^\tau)$. This implies $\#_{\mathcal{M}_k^\sigma}(u) = \#_{\mathcal{M}_k^\tau}(u)$, for all $0 \leq u \leq k$. Observe that any column vector $j$ of the matrices encode the positions of the points in the following way: If value $j$ is in $\mathcal{Z}_{b,k}^\sigma$, then there is a 1 in the first row of the column $j$ and if the first point to the right is at position $j+h$ then the first 2 in column $j$ appears in row $h+1$ and so on. For any column $j$, we call a column $j'$ the inverted column of $j$ if for all entries of the two columns $m_{i,j} + m_{i,j'} = k$ holds.

Observe now that column $b-j+1$ of $\mathcal{M}_k^\tau$ is the inverted column of column $j$ of $\mathcal{M}_k^\sigma$. This is true, because whenever we add a triangle of 1's to the first matrix, we add at the same time a triangle of 0's. So if we consider row $b-1$ of this matrix, then there have to be exactly $k$ positions with a value of $k-1$ (after adding $k$ triangles to this matrix), since in each step there is always one

position where 0 is added. Moreover if we consider the column vectors from bottom to top, they encode the positions of these places with value $k-1$: If the next position with value $k-1$ is $h$ positions to the left, the first value $k-2$ of this column is at row $b-1-h$ and so on. However considering the positions of the values $k-1$ in row $b-1$ of $\mathcal{M}_k^\sigma$, that is considering the positions where a triangle of 0's is added in each step, is the same as considering $\mathcal{Z}_{b,k}^\tau$. The only difference is that in $\mathcal{Z}_{b,k}^\tau$ we add triangles of 1's at these positions and therefore get inverted columns.

The corollary follows since for every value $u$ in $\mathcal{M}_k^\sigma$ there is exactly one value $k-u$ in $\mathcal{M}_k^\tau$ and since we know that $\#_{\mathcal{M}_k^\sigma}(u) = \#_{\mathcal{M}_k^\tau}(u)$, for all $0 \le u \le k$. □

### 5.3. An Improved Lower Bound

In this subsection we improve Theorem 3. We know from Lemma 2(v), that, since any matrix $\mathcal{M}_k^\sigma$ is created by the intersection of $k$ many triangles, $\sum_{u=0}^{b} \#(u)u = k\frac{(b-1)b}{2}$ does not depend on $\sigma$. However its value $\mathcal{N}(\mathcal{M}_k^\sigma)$ varies depending on the values $\#(u)$. If we want to minimize $\mathcal{N}(\mathcal{M}_k^\sigma)$, then we have to look for an intersection of these $k$ many triangles such that their area of intersection is minimal. Hence we are interested in the set with minimal pairwise intersections $\mathcal{Z}_{b,k}^*$ which we define via the property

$$\sum_{(u,v)\in(\mathcal{Z}_{b,k}^*)^2} \mathcal{F}(u,v) \le \sum_{(u,v)\in(\mathcal{Z}_{b,k}^\sigma)^2} \mathcal{F}(u,v).$$

**Lemma 4.** *For $\mathcal{Z}_{b,k}^*$ it holds that*

$$\mathcal{N}(\mathcal{M}_k^{\mathcal{Z}_{b,k}^*}) = \min_{\mathcal{Z}_{b,k}^\sigma} \mathcal{N}(\mathcal{M}_k^{\mathcal{Z}_{b,k}^\sigma}).$$

Proof. Look at any column vector of $\mathcal{M}_k^\sigma$ whose first element is 1. Then the first 2 of this vector is at row $i$ if its first point to the right is $i-1$ positions to the right. The first 3 in this vector is at row $i'$ if the second point to the right is $i'-1$ positions to the right and so on. In this way the column vectors encode the positions of the $k$ many points. From this point of view having a minimal area of intersection means that these changes of values in the column vectors take place as late as possible (for $u > 0$). So this minimal set $\mathcal{Z}_{b,k}^*$ indeed gives the smallest possible value $\mathcal{N}(\mathcal{M}_k^{\mathcal{Z}_{b,k}^*})$. □

As a consequence of this lemma we can state the following improvement of Theorem 3:

**Theorem 5.** *For arbitrary base $b$ and arbitrary $\sigma \in \mathfrak{S}_b$ and for each $k$, $1 \leq k \leq b$, we have that*

$$\chi_b^\sigma\left(\frac{k}{b}\right) \geq \frac{1}{2}\left(\mathcal{N}\left(\mathcal{M}_k^{\mathcal{Z}_{b,k}^*}\right) - \sum_{d=1}^{b-1} \frac{d^2k^2}{b}\right) \geq L_b^k.$$

Proof. Due to Lemma 4 $\mathcal{N}(\mathcal{M}_k^{\mathcal{Z}_{b,k}^*})$ is the smallest value any matrix $\mathcal{M}_k^{\mathcal{Z}_{b,k}^\sigma}$ can obtain for arbitrary $\sigma$, whereas we have seen in Theorem 3 that $L_b^k$ is the smallest value that is in general possible for any matrix with the condition that the sum of each row $i$ is $ik$. □

**Remark 5.** *Note that this construction really improves Theorem 3 since there are always permutations that obtain the values we compute for step $k$, namely those permutations, whose first $k$ values are the values of $\mathcal{Z}_{b,k}^*$. However from this point of view it is also obvious that there is no general permutation that is optimal in each step, since the minimal set for a certain $k$ is usually not contained in the minimal set of $k' > k$.*

### 5.4. Construction of Minimal Sets

With Theorem 5 in mind let us briefly outline a possible way of computing the set $\mathcal{Z}_{b,k}^*$ for arbitrary $b$ and $k$. We suggest (without proof) a recursive approach for given $b$ and $k$. Note that in contrast to the bounds in Theorem 3, computing and analysing the set $\mathcal{Z}_{b,k}^*$ is much trickier and we did not succeed in finding a nice closed form expression for it.

The following strategy can be used to computationally determine lower bound sets. Start with one single block of length $k$ (respectively the corresponding matrix). In a first step reduce the number of zeros in the matrix, then reduce the length of the blocks. This can be done by reducing the length of the initial block by one and putting this point at position $b-2$. Then reduce the length of the initial block again and put this point at position $b-4$. Repeat this until there are $(b-k)$ gaps. Now there is one long block and several blocks of length 1 in the set. If $k \geq b/2$ always take one element of the long block and use it to extend the shortest block by 1. Continue like that until this process would yield a new longest block. If $k < b/2$ do the same, but with the gaps between two blocks.

After these two steps we obtain a set with a certain amount of blocks (or gaps) of at most two different lengths $J_1$ and $J_2$. Next we want to order these different blocks in an optimal way. The crucial observation is that we can reformulate this problem in terms of the initial problem and hence we can solve the problem recursively. We are interested in ordering $m = \#(J_1) + \#(J_2)$ blocks of length

$J_1$ resp. $J_2$ (w.l.o.g $\#(J_1) \geq \#(J_2)$) such that their pairwise area of intersection is minimal. This is the same as asking how to arrange $\#(J_1)$ points on a circle with $m$ positions. Since $m < b$ we have reduced our problem. Once we obtain a solution for the reduced problem we can construct a solution to the initial problem by recalling that each point in the solution of the reduced problem stands for a block of length $J_1$ and each gap denotes a block of length $J_2$. All we need to do is to identify each point or gap of the subsolution with a block of a certain length and to add gaps of length 1 in between.

## 6. Conclusion

In this paper we extended a method of Faure from [6] in order to derive a lower bound for the diaphony of generalised van der Corput sequences in arbitrary base $b$. We saw that it is in general not possible to find a permutation whose diaphony takes our lower bound values in each step $k$. In order to determine the class of optimal permutations, future work should focus on constructing permutations that are in a certain sense good in each step $k$. We have to find permutations that deviate in each step only a little from the optimal sets $\mathcal{Z}^*_{b,k}$.

Moreover, we proved a criterion to decide whether two sequences have the same distribution behaviour with respect to the diaphony. This criterion can be useful in future work if one is interested in a classification of permutations concerning their distribution behaviour.

REFERENCES

[1] H. Chaix and H. Faure: *Discrépance et diaphonie en dimension un*, Acta Arith. **63** (1993), 103–141.
[2] H. Faure: *Discrépance de suites associées à un système de numération (en dimension un)*, Bull. Soc. Math. France **109** (1981), 143–182.
[3] H. Faure: *Discrépance quadratique de la suite de van der Corput et de sa symètrique*, Acta Arith. **55** (1990), 333–350.
[4] H. Faure: *Good Permutations for Extreme Discrepancy*, Journal of Number Theory **42** (1992), 47-56.
[5] H. Faure: *Discrepancy and diaphony of digital* $(0,1)$*-sequences in prime base*, Acta Arith. **117** (2005), 125–148.
[6] H. Faure: *Irregularities of Distribution of Digital* $(0,1)$*-Sequences in Prime Base*, Electronic Journal of Combinatorial Number Theory **5** (2005), no. 3.
[7] H. Faure and F. Pillichshammer: *$L_p$ discrepancy of generalized two-dimensional Hammersley point sets*, Monatsh. Math. **158** (2009) 31–61.

[8] H. Faure and F. Pillichshammer: *$L_2$ discrepancy of two-dimensional digitally shifted Hammersley point sets in base b*, Monte Carlo and Quasi-Monte Carlo Methods 2008 (2009), Springer, 355–368.

[9] H. Faure, F. Pillichshammer, G. Pirsic and W. Ch. Schmid: *$L_2$ discrepancy of generalized two-dimensional Hammersley point sets scrambled with arbitrary permutations*, Acta Arith. **141** (2010): 395–418.

[10] H. Faure and F. Pillichshammer: *$L_2$ discrepancy of generalized Zaremba point sets*, to appear in J. Th. Nombres de Bordeaux, 2011.

[11] V. Ostromoukhov: *Recent Progress in Improvement of Extreme Discrepancy and Star Discrepancy of One-Dimensional Sequences*, In: Monte Carlo and Quasi-Monte Carlo Methods 2008 (2009), Springer, 561-572.

[12] F. Pausinger and W. Ch. Schmid: *A good permutation for one-dimensional diaphony*, Monte Carlo Methods and Appl. **16** (2010), 307–322.

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

Received January 31, 2011
Accepted June 6, 2011

**Florian Pausinger**
*I.S.T Austria*
*Am Campus 1*
*A-3400 Klosterneuburg*
*AUSTRIA*
*E-mail*: florian.pausinger@ist.ac.at

**Wolfgang Ch. Schmid**
*Fachbereich Mathematik*
*Universität Salzburg*
*Hellbrunnerstraße 34*
*A-5020 Salzburg*
*AUSTRIA*
*E-mail*: wolfgang.schmid@sbg.ac.at