

ON THE INTRIGUING SEARCH FOR GOOD PERMUTATIONS

FLORIAN PAUSINGER

School of Mathematics & Physics, Queen's University Belfast, UNITED KINGDOM

ABSTRACT. The intriguing search for permutations that generate generalised van der Corput sequences with exceptionally small discrepancy forms an important part of the research work of Henri Faure. On the occasion of Henri's 80th birthday we aim to survey (some of) his contributions over the last four decades which considerably improved our understanding of one-dimensional van der Corput sequences and inspired a lot of related work. We recall and compare the different approaches in the search for generalised van der Corput sequences with low discrepancy, i.e., using a single generating permutation versus using a sequence of permutations. Throughout, we collect, sharpen and extend open questions which all stem from the extensive work of Henri and his coworkers and which will hopefully inspire more work in the future.

Communicated by Yann Bugeaud

Dedicated to Henri Faure on the occasion of his 80th birthday

Preface

This survey forms the basis for my presentation at MCQMC 2018 in Rennes, where I was invited to give a talk in the special session *Low discrepancy sequences and point sets* which was dedicated to Henri Faure on the occasion of his 80th birthday and organised by Friedrich Pillichshammer (JKU Linz) and Wolfgang Schmid (University of Salzburg). The main aim of this paper is to pick one particular aspect of the research of Henri Faure, i.e., the search for permutations

© 2019 BOKU-University of Natural Resources and Life Sciences and Mathematical Institute, Slovak Academy of Sciences.

2010 Mathematics Subject Classification: 11K38, 11K06, 11T06, 05A05.

Keywords: Van der Corput sequence; low discrepancy; permutation polynomial; Henri Faure.

Licensed under the Creative Commons Attribution-NC-ND 4.0 International Public License.

that generate (generalised) van der Corput sequences with exceptionally small discrepancy, which led to a series of interesting results and still leaves intriguing open questions. For a comprehensive account on the van der Corput sequence, its various generalisations and different discrepancy estimates I would like to refer to the recent survey of Faure, Kritzer, and Pillichshammer [19].

What intrigues me and motivates this article is the fact that despite the considerable amount of excellent work collected in [19] it is still not entirely clear which structure underlies those one-dimensional sequences with to-date smallest known discrepancy. The systematic search for *good* permutations which was initiated by Henri Faure gave us sequences with exceptionally small discrepancy. However, attempts to describe and reproduce the structure of such permutations have, so far, not been entirely satisfying. The search for an answer to a seemingly hopeless problem usually inspires interesting and original work. The aim of this paper is to present the history as well as the state-of-the-art in the search for one-dimensional infinite sequences with low discrepancy. Moreover, we collect new numerical results and various open problems hoping to motivate future research.

1. Extending a classical definition

1.1. A bit of context and history

The theory of uniform distribution modulo one (abbreviated as u.d. mod 1) can be traced back to the work of Tchebycheff and Kronecker in the late 19th century and of Hardy and Littlewood in the beginning of the 20th century. In a seminal paper of 1916, Weyl [59] placed the concept of u.d. mod 1 in the center of the study of Diophantine approximation in one and higher dimensions and systematised all the earlier work on the subject. We recall the basic definitions in the following and use this opportunity to introduce the notation we use throughout.

Let $X = (x_i)_{i \geq 1}$ be a sequence of real numbers. We denote the fractional part of a real number x by $\{x\}$. We put $I = [0, 1)$ and consider $[\alpha, \beta) \subseteq I$. For $N \geq 1$, let $A([\alpha, \beta), N, X)$ denote the number of indices $1 \leq i \leq N$ for which $\{x_i\} \in [\alpha, \beta)$. An infinite sequence X is *uniformly distributed modulo 1* (u.d. mod 1) if

$$\lim_{N \rightarrow \infty} \frac{A([\alpha, \beta), N, X)}{N} = \beta - \alpha, \quad (1)$$

for every subinterval $[\alpha, \beta)$ of I . The uniform distribution property (1) of an infinite sequence is usually quantified with one of several different notions of discrepancy. Following Faure, i.e., not dividing by N , we put

$$E([\alpha, \beta), N, X) = A([\alpha, \beta), N, X) - (\beta - \alpha)N,$$

and define the star discrepancy, $D_N^*(X)$, and the extreme discrepancy, $D_N(X)$, of the first N points of X as

$$D_N^*(X) = \sup_{[0, \alpha) \subseteq I} |E([0, \alpha), N, X)|, \quad \text{and} \quad D_N(X) = \sup_{[\alpha, \beta) \subseteq I} |E([\alpha, \beta), N, X)|.$$

For completeness, we also define the L^2 -discrepancy, $D_N^{(2)}(X)$, and the diaphony, $F_N(X)$, of the first N points of X as

$$D_N^{(2)}(X) := \left(\int_0^1 |E([0, \alpha), N, X)|^2 d\alpha \right)^{1/2},$$

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

This definition of diaphony is taken from [14]; for the original definition in terms of exponential sums we refer to [62].

There are two classical examples of uniformly distributed sequences. The fact that the so-called Kronecker sequence $(\{n\alpha\})_{n \geq 1}$ is u.d. mod 1 for every irrational α was established in 1909–10 independently by Bohr, Sierpinski and Weyl. Ostrowski [44] showed in 1922, that a Kronecker sequence has very small discrepancy if the irrational α has bounded partial quotients. In 1935, the van der Corput sequence, $\mathcal{S}_2$,—we recall its definition in the next section—was introduced and shown to be u.d. mod 1. In fact, it was already known to van der Corput that $D_N(\mathcal{S}_2) = O(\log N)$, see [57, 58]. Similarly, it was already known in the 1920s that the optimal order of the discrepancy of Kronecker sequences is $\log N$ as well, see [1, 44]. However, it was only shown in 1972 that this order of magnitude is best possible when Schmidt [55] improved a general lower bound result of Roth [54] for the special case of one-dimensional sequences. He proved that for any infinite sequence $X \subset I$ we have that

$$D_N(X) \geq c \cdot \log N, \tag{2}$$

for infinitely many integers N , where $c > 0$ is an absolute constant. These early results set the stage for this paper.

1.2. Chasing the constants

In 1972 the question of the optimal order of magnitude that can be achieved is finally settled and there are two different constructions available. Which one is better? And what is the largest constant c for which (2) remains true? To formalise this question we define the asymptotic constants $s(X)$ and $s^*(X)$ of an infinite sequence X as

$$s(X) = \limsup_{N \rightarrow \infty} \frac{D_N(X)}{\log N}, \quad \text{and} \quad s^*(X) = \limsup_{N \rightarrow \infty} \frac{D_N^*(X)}{\log N},$$

which are known to be finite for our particular examples above. In general, whenever $s(X)$ is finite for a sequence X , we say that this sequence has *low discrepancy*. Since we know examples of low discrepancy sequences, it makes sense to define the one-dimensional discrepancy constant $\hat{s}$ as

$$\hat{s} = \inf_X \limsup_{N \rightarrow \infty} \frac{D_N(X)}{\log N} = \inf_X s(X),$$

in which the infimum is taken over all infinite sequences X ; we define $\hat{s}^*$ in a similar fashion. In other words, $\hat{s}$ is the supremum over all c such that (2) holds for all X for infinitely many N . Larcher [37, 38] and Larcher & Puchhammer [39] recently improved earlier results of B ejian [2] and proved that

$$0.12112 < \hat{s}, \quad \text{and} \quad 0.06566 < \hat{s}^*$$

for the most recent upper bounds we refer to Table 2.

Returning to our discussion of the history, apart from a result of Haber [27] on the constant $s(\mathcal{S}_2)$ nobody had calculated such constants until then. There were only upper bounds on $s(X)$ and $s^*(X)$ for different sequences. It lasted until the late 1970s before Ramshaw [53], B ejian & Faure [3] and S os & Dupain [10] were able to give exact formulas for the asymptotic constants of various sequences; see Table 1.

TABLE 1. Sequences X with smallest known values for $s^*(X)$ and $s(X)$ before the paper of Henri Faure in 1981.

X	$s(X)$	$s^*(X)$
$\mathcal{S}_2$	$\frac{1}{3 \log 2} = 0.4808 \dots$	$\frac{1}{3 \log 2} = 0.4808 \dots$
$(\{n\alpha\})$ for $\alpha = (\sqrt{5} - 1)/2$	$\frac{1}{5 \log(1/\alpha)} = 0.4156 \dots$	$\frac{3}{20 \log(1/\alpha)} = 0.3117 \dots$
$(\{n\alpha\})$ for $\alpha = \sqrt{2} - 1$	$\frac{1}{2 \log(1/\alpha)} = 0.5672 \dots$	$\frac{1}{4 \log(1/\alpha)} = 0.2836 \dots$

At this point it seemed that the $(\{n\alpha\})$ sequence was outperforming the van der Corput sequence. The breakthrough – in case you are a fan of the van der Corput sequence – came in 1981 when Faure published his influential paper [11]. This paper contains six theorems, all of which became of great importance for the subsequent development. However, the first big contribution of this paper was the *definition* of a new family of sequences, which Faure called *generalised van der Corput sequences*.

1.3. Extending a definition

We start with the definition of the classical van der Corput sequence $\mathcal{S}_2$. Let $a_j(n)$ denote the j th coefficient in the b -adic expansion

$$n = a_0 + a_1b + a_2b^2 + \cdots = \sum_{j=1}^{\infty} a_j b^j$$

of an integer n , where $0 \leq a_j(n) \leq b-1$ and if $0 \leq n < b^k$, then $a_j(n) = 0$ for $j \geq k$. The b -adic radical inverse function is defined as $S_b : \mathbb{N}_0 \rightarrow [0, 1)$,

$$S_b(n) = \frac{a_0(n)}{b} + \frac{a_1(n)}{b^2} + \frac{a_2(n)}{b^3} + \cdots = \sum_{j=0}^{\infty} \frac{a_j(n)}{b^{j+1}} \quad \text{for } n \in \mathbb{N}_0.$$

The classical van der Corput sequence is defined as $\mathcal{S}_2 = (S_2(n))_{n \geq 0}$.

Furthermore, let $\mathfrak{S}_b$ be the set of all permutations of $\{0, 1, \dots, b-1\}$, i.e., all permutations of the first b non-negative integers, and let $\Sigma = (\sigma_j)_{j \geq 0}$ be a sequence of permutations in base b such that $\sigma_j \in \mathfrak{S}_b$ for all $j \geq 0$. Throughout this paper we sometimes write a concrete permutation σ as tuple, e.g., $\sigma = (0, 2, 4, 1, 3)$ meaning that 0 is mapped to 0, 1 is mapped to 2, 2 is mapped to 4 and so on; i.e., the number at the i th position of the tuple is the image of i under σ . Moreover, $\sigma \circ \tau$ denotes the usual composition of permutations for $\sigma, \tau \in \mathfrak{S}_b$. Following Faure [11], we define the generalised (or permuted) van der Corput sequence $\mathcal{S}_b^\Sigma = (S_b^\Sigma(n))_{n \geq 0}$ for a fixed base $b \geq 2$ and a sequence of permutations Σ by

$$S_b^\Sigma(n) = \sum_{j=0}^{\infty} \frac{\sigma_j(a_j(n))}{b^{j+1}}.$$

Every such sequence is uniformly distributed; [11, Propriété 3.1.1]. The most general definition was considered in [6] where Σ was even allowed to be a sequence of permutations in variable bases. If we consider a constant sequence of permutations, i.e., we use the same permutation σ for every j , then we write $\mathcal{S}_b^\sigma$. Hence, $\mathcal{S}_2 = \mathcal{S}_2^{id}$, where id denotes the identity permutation in $\mathfrak{S}_b$. This extension of the basic definition opens the door to a huge space of possibilities and it suggests two different approaches when trying to improve the constants in Table 1. We can either try to find a single permutation that generates a sequence with small asymptotic constant (see Section 3 and Section 4) or we can look for a sequence of permutations (see Section 5).

1.4. An influential paper

But first, let's return to our discussion of the influential paper [11]. The first three theorems of the paper establish a method to calculate the discrepancy

as well as the asymptotic constant of generalised van der Corput sequences exactly—we will come back to these results in more detail in Section 2. Using this method, Faure was able to explicitly calculate these values in three different settings, giving the final three theorems of the paper. He improved the so far best upper bounds on $\hat{s}$ and $\hat{s}^*$. In particular, he shows in [11, Théorème 4] for $b = 12$ and $\sigma = (0, 7, 3, 10, 5, 2, 9, 6, 1, 8, 4, 11)$ that

$$0.375 < s(\mathcal{S}_{12}^\sigma) < 0.38.$$

In [11, Théorème 5] another permutation in base $b = 12$ is considered. Let $\sigma = (0, 5, 9, 3, 7, 1, 10, 4, 8, 2, 6, 11)$ and define the set $A \subset \mathbb{N}$ as

$$A = \bigcup_{H=1}^{\infty} A_H, \quad \text{with} \quad A_H = \{H(H-1)+1, H(H-1)+2, \dots, H^2\}.$$

Moreover, let $\tau_b \in \mathfrak{S}_b$ with $\tau_b(k) = b - k - 1$ for $0 \leq k \leq b - 1$ and define $\Sigma_A^\sigma = (\sigma_j)_{j \geq 0}$ with $\sigma_j = \sigma$ if $j \in A$ and $\sigma_j = \tau_{12} \circ \sigma$ if $j \notin A$. Then

$$s^*(\mathcal{S}_{12}^{\Sigma_A^\sigma}) = \frac{1919}{3454 \log 12} = 0.22358 \dots$$

We will come back to this particular and important construction of a sequence of permutations out of a single permutation later in this paper. Finally, in [11, Théorème 6] the constants s and s^* for van der Corput sequences that are generated from the identity permutation in base b are calculated:

$$s(\mathcal{S}_b^{id}) = s^*(\mathcal{S}_b^{id}) = \begin{cases} \frac{b-1}{4 \log b} & \text{if } b \text{ is odd,} \\ \frac{b^2}{4(b+1) \log b} & \text{if } b \text{ is even.} \end{cases}$$

Consequently, the only sequence generated from an identity permutation that improves the result of the classical sequence in base 2 is $\mathcal{S}_3^{id}$. However,

$$s(\mathcal{S}_3^{id}) = 0.4551 \dots$$

is still larger than the value Ramshaw obtained for $(\{n\alpha\})$. We will further explore the connection between generalised van der Corput sequences and $(\{n\alpha\})$ sequences in Section 4. Importantly, it is also shown [11, Section 5.5, Corollaire 3] that the sequence generated from the identity has the largest asymptotic constant among all permuted van der Corput sequences in a fixed base b . In other words, we always have for fixed b and $\sigma \in \mathfrak{S}_b$ that

$$s(\mathcal{S}_b^\sigma) \leq s(\mathcal{S}_b^{id}). \tag{3}$$

The results and methods that Faure developed in his paper of 1981 were the starting point for the intriguing search for good permutations.

QUESTION 1. Which characteristics of a permutation or a sequence of permutations lead to a sequence with very small discrepancy? Is there a systematic way to construct/find a sequence with a very small asymptotic constant?

1.5. Asymptotic constants and diaphony

The upper bounds on the asymptotic discrepancy constants $\hat{s}$ and $\hat{s}^*$ that Faure obtained in 1981 could be improved over the years. The currently best values are collected in Table 2; see the appendix for the explicit permutations.

TABLE 2. Chronological order of improvements of upper bounds on $\hat{s}$ and $\hat{s}^*$ after 1981.

Faure	1981, [11]	$\hat{s} < 0.38$	$\hat{s}^* < 0.22358$
Faure	1992, [13]	$\hat{s} < 0.367$	
Ostromoukhov	2009, [43]	$\hat{s} < 0.354$	$\hat{s}^* < 0.222223$

Chaix & Faure extended the methods of [11] to the study of diaphony (as well as L^2 -discrepancy); see [6, Section 4.1]. It turns out that the asymptotic constant

$$f(X) = \limsup_{N \rightarrow \infty} \frac{F_N^2(X)}{\log N}$$

can be calculated with a method that is similar to the case of (star) discrepancy; see [6, Section 4.2]. In particular, this result was used to improve the until then best known bound for the diaphony of infinite one-dimensional sequences (see [6, Section 4.3]) and raised the same questions as in the case of discrepancy. Is there a permutation that can further improve the smallest known value? How can we find it? Setting

$$\hat{f} := \inf_X f(X)$$

Proinov [45] provides a first upper bound on $\hat{f}$ in 1983 using the sequence $(\{n\alpha\})$, in which α is again the conjugate golden ratio. The currently smallest known upper bound for $(\{n\alpha\})$ is due to Xiao [60] who improved the value of Proinov in 1990 to $f(\{n\alpha\}) < 7.5$. We recall the improvements of the upper bound on $\hat{f}$ in chronological order in Table 3; see the appendix for the explicit permutations. These bounds are all obtained from (generalised) van der Corput sequences. Concerning lower bounds on $\hat{f}$, Proinov [46] showed in 1986 that

$$\hat{f} > 1/4624 = 0.00021 \dots$$

TABLE 3. Improvements of the upper bound on $\hat{f}$ in chronological order.

Proinov & Grozdanov	1988,[48]	$\hat{f} < 14.238$
Proinov & Atanassov	1988,[47]	$\hat{f} < 1.583$
Chaix & Faure	1993, [6]	$\hat{f} < 1.316$
Pausinger & Schmid	2010,[50]	$\hat{f} < 1.137$

PROBLEM 1. *It is not satisfying that the upper bounds for $\hat{f}$ obtained from concrete sequences are much larger than the corresponding bounds for $\hat{s}$ while the so far best general lower bound for $\hat{f}$ is much smaller than the one for $\hat{s}$. Can the general lower bound of Proinov for $\hat{f}$ be improved?*

Outline. In Section 2 we introduce the method to calculate the discrepancy of generalised van der Corput sequences followed by Section 3 on how to find and construct good generating permutations. Section 4 introduces permutation polynomials as a way to describe the structure of generating permutations, before we turn to sequences of generating permutations in Section 5. Section 6 gives a wider context to the results of Faure and, finally, Section 7 concludes the paper.

2. Calculating the discrepancy

In the following we introduce Faure’s system of basic functions which can be used to calculate the discrepancy of generalised van der Corput sequences. Furthermore, we survey various powerful techniques for the analysis of structurally similar permutations. In the final part of this section we recall how to calculate the asymptotic discrepancy constant for a given sequence.

2.1. Basic functions and exact formulas

The exact formulas for the discrepancy (and also the diaphony) of generalised van der Corput sequences are based on a set of elementary functions which are defined for any permutation $\sigma \in \mathfrak{S}_b$. Let

$$\mathcal{X}_b^\sigma := \left(\frac{\sigma(0)}{b}, \frac{\sigma(1)}{b}, \dots, \frac{\sigma(b-1)}{b} \right).$$

ON THE INTRIGUING SEARCH FOR GOOD PERMUTATIONS

For $h \in \{0, 1, \dots, b-1\}$ and $x \in [\frac{k-1}{b}, \frac{k}{b}[$, in which $1 \leq k \leq b$ is an integer, we define

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

The functions $\varphi_{b,h}^\sigma$ are piecewise affine and are extended to the real numbers by periodicity. To simplify the formulas for (star) discrepancy it is convenient to put

$$\psi_b^{\sigma,+} = \max_{0 \leq h < b} \varphi_{b,h}^\sigma, \quad \psi_b^{\sigma,-} = \max_{0 \leq h < b} (-\varphi_{b,h}^\sigma), \quad \psi_b^\sigma = \psi_b^{\sigma,+} + \psi_b^{\sigma,-}.$$

For an infinite, one-dimensional sequence X we set

$$D_N^+ = \sup_{0 \leq \alpha \leq 1} E([0, \alpha], N, X), \quad \text{and} \quad D_N^- = \sup_{0 \leq \alpha \leq 1} (-E([0, \alpha], N, X)).$$

Then we get from [11, Théorème 1] for $N \geq 1$ that

$$\begin{aligned} D_N^+(\mathcal{S}_b^\Sigma) &= \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1},+}(N/b^j), & D_N^-(\mathcal{S}_b^\Sigma) &= \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1},-}(N/b^j), \\ D_N(\mathcal{S}_b^\Sigma) &= \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1}}(N/b^j), & D_N^*(\mathcal{S}_b^\Sigma) &= \max(D_N^+(\mathcal{S}_b^\Sigma), D_N^-(\mathcal{S}_b^\Sigma)). \end{aligned}$$

Note that the infinite series in these formulas can indeed be computed exactly; for details we refer to [11, Section 3.3.6, Corollaire 1]. Similar formulas hold for diaphony as well as L^2 -discrepancy [6].

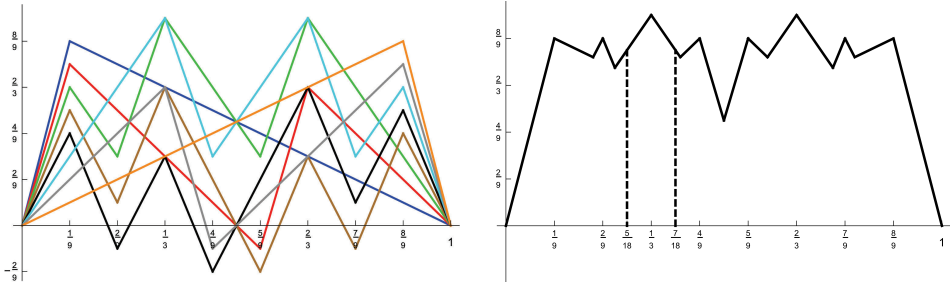


FIGURE 1. The functions $\varphi_{9,h}^\omega(x)$ (left) and $\psi_9^\omega(x)$ (right) for the permutation ω as defined in Section 3.

2.2. Symmetries, swapping and intrication of two permutations

There are several important lemmas linked to the basic functions which facilitate the analysis of structurally similar permutations as well as sequences of permutations. The subsequent Symmetry Lemma states that a shift or a reflection of a permutation does not change the discrepancy of the generated sequence which is not surprising since we interpret $[0, 1)$ as a circle.

LEMMA 1 (Symmetry Lemma). *Let $0 < a < b$ be an integer, let $\sigma \in \mathfrak{S}_b$ and let $\sigma', \sigma'' \in \mathfrak{S}_b$ be defined as*

$$\sigma'(x) = \sigma(x) + a \pmod{b}, \quad \text{and} \quad \sigma''(x) = -\sigma(x) \pmod{b} \quad \text{for } 0 \leq x \leq b-1.$$

Then it holds for all N that

$$D_N(\mathcal{S}_b^\sigma) = D_N(\mathcal{S}_b^{\sigma'}) \quad \text{and} \quad D_N(\mathcal{S}_b^\sigma) = D_N(\mathcal{S}_b^{\sigma''}).$$

The first part of the lemma was noted in [6, Théorème 4.4]; the second assertion was discussed in [51, Lemma 2.1].

Next is the Swapping Lemma which plays a crucial role in the asymptotic analysis of the star discrepancy of generalised van Corput sequences as well as two-dimensional Hammersley point sets (as discussed in Section 6) and first appeared as [11, Lemme 4.4.1]. Recall that we already defined $\tau_b \in \mathfrak{S}_b$ as the permutation $\tau_b(k) = b - k - 1$ for $0 \leq k \leq b-1$. The *swapping* permutation τ_b gets its name from the fact that

$$\begin{aligned} \psi_b^{\sigma \circ \tau, +} &= \psi_b^{\sigma, -}, \\ \psi_b^{\sigma \circ \tau, -} &= \psi_b^{\sigma, +}. \end{aligned}$$

This property is especially useful if $\sigma = id$ because then

$$\psi_b^{\tau, +} = \psi_b^{id, -} = 0 \quad \text{and} \quad \psi_b^{\tau, -} = \psi_b^{id, +} = \psi_b^{id}.$$

In general, we have:

LEMMA 2 (Swapping Lemma). *Let $\mathcal{N} \subset \mathbb{N}_0$ and let $\sigma \in \mathfrak{S}_b$. Further define $\Sigma_{\mathcal{N}}^\sigma = (\sigma_j)_{j \geq 0}$ as $\sigma_j = \sigma$ if $j \in \mathcal{N}$ and $\sigma_j = \tau_b \circ \sigma$ if $j \notin \mathcal{N}$. Then*

$$\begin{aligned} D_N^+(\mathcal{S}_b^{\Sigma_{\mathcal{N}}^\sigma}) &= \sum_{j \in \mathcal{N}} \psi_b^{\sigma, +}(N/b^j) + \sum_{j \notin \mathcal{N}} \psi_b^{\sigma, -}(N/b^j), \\ D_N^-(\mathcal{S}_b^{\Sigma_{\mathcal{N}}^\sigma}) &= \sum_{j \in \mathcal{N}} \psi_b^{\sigma, -}(N/b^j) + \sum_{j \notin \mathcal{N}} \psi_b^{\sigma, +}(N/b^j), \\ D_N^*(\mathcal{S}_b^{\Sigma_{\mathcal{N}}^\sigma}) &= \max\left(D_N^+(\mathcal{S}_b^{\Sigma_{\mathcal{N}}^\sigma}), D_N^-(\mathcal{S}_b^{\Sigma_{\mathcal{N}}^\sigma})\right), \\ D_N(\mathcal{S}_b^{\Sigma_{\mathcal{N}}^\sigma}) &= D_N(\mathcal{S}_b^\sigma). \end{aligned}$$

Finally, Faure defined an operation [11, Section 3.4.3] which takes two arbitrary permutations σ, τ in bases b and c and outputs a new permutation, $\sigma \cdot \tau$ in base $b \cdot c$. The motivation for this definition comes from the following property which was first noted in [11, Proposition 3.4.3].

LEMMA 3 (Intrication). *For $\sigma \in \mathfrak{S}_b$ and $\tau \in \mathfrak{S}_c$ define $\sigma \cdot \tau \in \mathfrak{S}_{bc}$ as*

$$\sigma \cdot \tau(k''b + k') = c\sigma(k') + \tau(k''), \quad \text{for } 0 \leq k' < b \quad \text{and} \quad 0 \leq k'' < c.$$

Then,

$$\psi_{bc}^{\sigma \cdot \tau}(x) = \psi_b^\sigma(cx) + \psi_c^\tau(x),$$

such that

$$\max_{x \in \mathbb{R}} \psi_{bc}^{\sigma \cdot \tau}(x) \leq \max_{x \in \mathbb{R}} \psi_b^\sigma(x) + \max_{x \in \mathbb{R}} \psi_c^\tau(x).$$

Note that if we set $\sigma = \tau$, then the intrication $\sigma \cdot \sigma$ gives a permutation in base b^2 whose ψ -function is the function F_2^σ defined in (5) below. In this special case the new permutation generates the same sequence as the original permutation.

2.3. Asymptotic analysis

The exact formulas can be used for the asymptotic analysis of the discrepancy of generalised van der Corput sequences. By [11, Théorème 2],

$$s(\mathcal{S}_b^\sigma) = \limsup_{N \rightarrow \infty} \frac{D_N(\mathcal{S}_b^\sigma)}{\log N} = \frac{\alpha_b^\sigma}{\log b}$$

with

$$\alpha_b^\sigma = \inf_{n \geq 1} \sup_{x \in \mathbb{R}} \left(\frac{1}{n} \sum_{j=1}^n \psi_b^\sigma(x/b^j) \right). \quad (4)$$

Furthermore, we introduce the function

$$F_n^\sigma(x) = \sum_{j=0}^{n-1} \psi_b^\sigma(xb^j), \quad (5)$$

and rewrite (4) as

$$\alpha_b^\sigma = \inf_{n \geq 1} \left(\max_{x \in [0,1]} F_n^\sigma(x)/n \right).$$

Note that the local maxima of ψ_b^σ have arguments of the form $x = k/b$ for $k \in \mathbb{N}$ with $0 \leq k \leq b-1$. As shown in [11, Lemme 4.2.2], the sequence $(\max_{x \in [0,1]} F_n^\sigma(x)/n)_{n \geq 1}$ is decreasing. In particular,

$$\alpha_b^\sigma \leq \dots \leq \max_{x \in [0,1]} F_2^\sigma(x)/2 \leq \max_{x \in [0,1]} F_1^\sigma(x) = \max_{x \in \mathbb{R}} \psi_b^\sigma, \quad (6)$$

with $\alpha_b^\sigma = \lim_{n \rightarrow \infty} \max_{x \in [0,1]} F_n^\sigma(x)/n$.

Finally, using the swapping permutation τ_b as well as the set $A \subset \mathbb{N}$ with

$$A = \bigcup_{H=1}^{\infty} A_H, \quad \text{with} \quad A_H = \{H(H-1)+1, H(H-1)+2, \dots, H^2\},$$

Faure proves in [11, Théorème 3]

$$s^*\left(\mathcal{S}_b^{\Sigma_A^\sigma}\right) = \limsup_{N \rightarrow \infty} \frac{D_N^*\left(\mathcal{S}_b^{\Sigma_A^\sigma}\right)}{\log N} = \frac{\alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}}{2 \log b},$$

where

$$\alpha_b^{\sigma,+} = \inf_{n \geq 1} \sup_{x \in \mathbb{R}} \left(\frac{1}{n} \sum_{j=1}^n \psi_b^{\sigma,+}(x/b^j) \right), \quad \alpha_b^{\sigma,-} = \inf_{n \geq 1} \sup_{x \in \mathbb{R}} \left(\frac{1}{n} \sum_{j=1}^n \psi_b^{\sigma,-}(x/b^j) \right).$$

3. Good permutations and how to find them

3.1. Searching for good permutations

A closer look at the permutations listed in the appendix reveals that the currently best values of Ostromoukhov are obtained for a permutation in base 84 resp. in base 60 whereas Pausinger & Schmid improved the value for the diaphony with a permutation in base 57. Given the number of permutations up to base 84, this seems much worse than looking for a needle in a haystack. So what is the secret behind the successful search for good permutations? The immediate answer appears disappointing at first. The authors of both papers used a *clever brute force* approach; i.e., testing permutations in a given base in a systematic way. However, recalling the large number of permutations, isn't it fascinating that such a strategy can work? What is hidden behind *clever*? The secret of the search algorithm(s) can be found in the definition of the basic $\varphi_{b,h}^\sigma$ functions:

OBSERVATION 1. It is enough to know the set of the first k values of σ , i.e.,

$$V_k^\sigma := \{\sigma(i) : 0 \leq i \leq k-1\},$$

to calculate $\varphi_{b,h}^\sigma(x)$ for $x \in [(k-1)/b, k/b[$ and $h \in \{0, 1, \dots, b-1\}$. Hence, the value at $\psi_b^\sigma(k/b)$ for a given set V_k^σ is the same for all permutations with this initial set of elements.

This observation suggests the following strategy. We can construct *good* permutations step by step—Ostromoukhov speaks of building a pruned tree [43, Section 5]. Knowing the first k images of a permutation, allows to calculate $\psi_b^\sigma(x)$ for $x \in [0, k/b[$. Thus, we choose a pruning threshold T and set without loss

of generality $\sigma(0) = 0$. This leaves $b - 1$ possibilities for $\sigma(1)$. We can calculate the discrepancy value for each of these possibilities. If the discrepancy is bigger than the pruning value T then the corresponding branch of the tree is pruned away. Therefore, we discard all permutations with this set of first k images. Now, we continue to $\sigma(2)$ and so on. This procedure finds all permutations σ with

$$\max_{x \in [0,1[} \psi_b^\sigma(x) < T.$$

The right choice of the pruning parameter T is the artistic part of the game. If T is too large, the final tree may contain a huge number of branches. If the value is too small, the final tree may contain no branches at all. This first list of good permutations is now the starting point for a more careful analysis. In a second step, we can sort (and shorten) our list of permutations by calculating $\max_x F_2^\sigma(x)$. This leaves us (hopefully) with a small enough set of permutations for further resp. asymptotic analysis.

3.2. Constructing good permutations

The approach chosen in the previous section led to an improvement of the upper bounds on the asymptotic constants $\hat{s}$, $\hat{s}^*$ and $\hat{f}$ which is of theoretical interest. In a more practical context one often needs a large number of good generating permutations, i.e., in simulations or in numerical integration. However, the systematic search for permutations tells us only little about the actual structure of good permutations and how to explicitly construct them. The aim of this and the next section is to review results that reveal more about the structure of good permutations.

As we have seen in Section 1.4, the asymptotic constants $s(\mathcal{S}_b^{id})$ increase with increasing base. In [13, Theorem 1.1], Faure contrasts this result by constructing a permutation $\omega = \omega_b$ in every base b with an asymptotic constant that is independent of the particular base:

THEOREM 1 (Faure [13]). *For every b there exists a permutation ω such that $s(\mathcal{S}_b^\omega) \leq 1/\log 2$.*

The proof of this result is constructive; i.e., Faure provides an algorithm to explicitly construct the permutations ω_b from permutations in smaller bases. Start with $b = 2$ and $\omega_2 = id_2 = (0, 1)$. Now suppose that all permutations ω_b have already been constructed for bases $b < b'$. If $b' = 2b$ is even, then $\omega_{b'} = id_2 \cdot \omega_b$. If $b' = 2b + 1$ is odd, then we define $\omega_{b'}$ for $0 \leq k < b$ as

$$\omega_{2b+1}(k) = \begin{cases} \omega_{2b}(k), & 0 \leq \omega_{2b}(k) < b, \\ \omega_{2b}(k) + 1, & b \leq \omega_{2b}(k) < 2b. \end{cases}$$

And for $b < k \leq 2b$,

$$\omega_{2b+1}(k) = \begin{cases} \omega_{2b}(k-1), & 0 \leq \omega_{2b}(k-1) < b, \\ \omega_{2b}(k-1) + 1, & b \leq \omega_{2b}(k-1) < 2b. \end{cases}$$

Finally, set $\omega_{2b+1}(b) = b$.

As an illustration let $b_n = 2^n - 1$, such that $b_2 = 3$, $b_3 = 7$, $b_4 = 15$ and $b_5 = 31$. Then

$$\begin{aligned} \sigma_3 &= (0, 1, 2), & \sigma_7 &= (0, 4, 1, 3, 5, 2, 6), \\ \sigma_{15} &= (0, 8, 4, 12, 1, 9, 3, 7, 11, 5, 13, 2, 10, 6, 14), \\ \sigma_{31} &= (0, 16, 8, 24, 4, 20, 12, 28, 1, 17, 9, 25, 3, 19, 7, \\ &\quad 15, 23, 11, 27, 5, 21, 13, 29, 2, 18, 10, 26, 6, 22, 14, 30). \end{aligned}$$

Moreover, note that for bases of the form $b = 2^n$, the algorithm returns permutations that correspond to the first 2^n points of the classical van der Corput sequence $\mathcal{S}_2$.

3.3. A conjecture

Faure conjectures that Theorem 1 holds with the stronger bound $1/(2 \log 2)$ and that this bound is sharp. He partitions the set of integers into intervals $B_n = [2^{n-1}, 2^n - 1]$, sets $d_b^\omega = \max_{x \in \mathbb{R}} \psi_b^\omega(x)$ and conjectures that

$$\max_{b \in B_n} \frac{d_b^\omega}{\log b} = \frac{d_{b_n}^\omega}{\log b_n} \quad \text{for } b_n = 2^n - 1.$$

In particular he conjectures, based on calculations for $2 \leq b \leq 255$, that

$$d_{b_n}^\omega = \begin{cases} \frac{n}{2} - \frac{1}{3} & \text{if } n \text{ is even,} \\ \frac{n}{2} - \frac{1}{3} - \frac{1}{6b_n} & \text{if } n \text{ is odd.} \end{cases}$$

Hence,

$$\frac{d_{b_n}^\omega}{\log b_n} \leq \frac{1}{2 \log 2} \quad \text{with} \quad \lim_{n \rightarrow \infty} \frac{d_{b_n}^\omega}{\log b_n} = \frac{1}{2 \log 2}.$$

We have carefully investigated this conjecture and slightly sharpen it in the following. Moreover, we will outline in Section 7 why we believe that this conjecture is important and difficult and why it deserves further attention in the future. We have extended the computations of Faure and verified his conjecture up to base 1023; see Figure 2. These computations suggest the following sharper version:

CONJECTURE 1. *Let $\omega = \omega_b$ be the permutation obtained from the algorithm of Faure and let B_n and b_n be as above. Then we conjecture for all $n \geq 4$,*

$$\min_{b \in B_n} \frac{d_b^\omega}{\log b} = \frac{d_{b_{\min}}^\omega}{\log(b_{\min})} \leq \frac{d_b^\omega}{\log b} \leq \frac{d_{b_n}^\omega}{\log b_n} = \max_{b \in B_n} \frac{d_b^\omega}{\log b},$$

in which $b \in B_n$ and $b_{\min} = 2^{n-1} + 2^{n-4} = 9 \cdot 2^{n-4}$.

ON THE INTRIGUING SEARCH FOR GOOD PERMUTATIONS

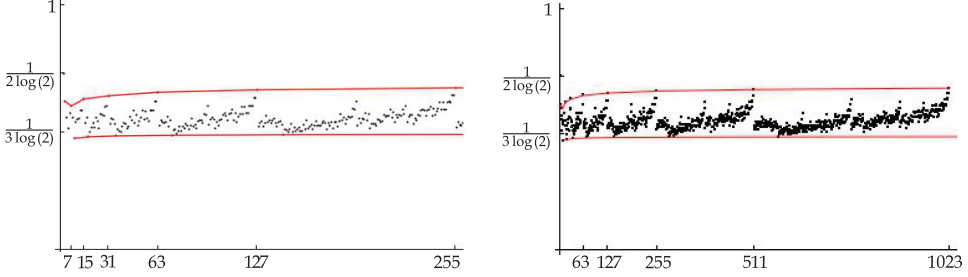


FIGURE 2. Plot of $(b, d_b^\omega / \log b)$ for $2 \leq b \leq 2^{10} - 1$ and ω as defined by Faure. The two red lines connect all minimal resp. maximal values of the intervals B_n .

Interestingly, the minimum is not obtained in bases of the form 2^n corresponding to the original van der Corput sequence. We obtain the following result for $\sigma = \omega_{b_{min}}$:

THEOREM 2. *For every $b_m = 9 \cdot 2^m$, $m \geq 0$, there exists a permutation σ such that $s(\mathcal{S}_{b_m}^\sigma) < 1/(3 \log 2) = s(\mathcal{S}_2^{id})$.*

Proof. Set $I_k := [k/(2b), (k+1)/(2b)]$, with $k \in \{0, \dots, 2b-1\}$. Following [6, 11], we call the interval I_k *dominated*, if there exists a set $\mathcal{N}$ of integers with $k \notin \mathcal{N}$ such that $\psi_b^\sigma(x) \leq \max_{j \in \mathcal{N}} \psi_b^\sigma((x + (j-k))/(2b))$, for all $x \in I_k$. Otherwise, the interval is called *dominant*.

We prove the theorem in two steps. First, we investigate ψ_9^ω and determine its dominant intervals. Second, we study ψ_{18}^ω and deduce a general formula for the dominant intervals of $\psi_{b_m}^\omega$, for $b_m = 9 \cdot 2^m$.

In Table 4 we tabulated the piecewise linear functions $\varphi_{9,h}^\omega$ for $0 \leq h \leq 8$. From Figure 1 it is easy to see that $[5/18, 7/18]$ is dominant for ψ_9^ω . Furthermore, note that $\psi_2^{id}(x) = x$, for $x \in [0, 1/2]$ and $\psi_2^{id}(x) = -x + 1$, for $x \in [1/2, 1]$.

For $x \in [5/18, 6/18]$ we have $\psi_9^\omega(x) = 3x$, whereas for $x \in [6/18, 7/18]$ we obtain $\psi_9^\omega(x) = -3x + 2$. Recall that $\omega_{18} = id_2 \cdot \omega_9$ and hence by Lemma 3

$$\psi_{18}^\omega(x) = \psi_{2 \cdot 9}^{id_2 \cdot \sigma_9}(x) = \psi_2^{id_2}(9x) + \psi_9^{\omega_9}(x).$$

Intuitively, we shift and squeeze $\psi_2^{id}(x)$ appropriately and add it to $\psi_9^\omega(x)$ in every interval of the form $[k/9, (k+1)/9]$. Therefore, we obtain two identical dominant intervals for ψ_{18}^ω , namely $[5/18, 6/18]$ and $[6/18, 7/18]$ and we see that ψ_{18}^ω obtains its maxima at $5/18$ and $7/18$.

FLORIAN PAUSINGER

TABLE 4. The piecewise linear functions $\varphi_{9,h}^\omega$ on $[0, 1/2]$.

$\varphi_{9,h}(x)$	$x \in [0, 1/9]$	$[1/9, 2/9]$	$[2/9, 3/9]$	$[3/9, 4/9]$	$[4/9, 1/2]$
$h=0$	0	0	0	0	0
1	$8x$	$-x + 1$	$-x + 1$	$-x + 1$	$-x + 1$
2	$7x$	$-2x + 1$	$-2x + 1$	$-2x + 1$	$-2x + 1$
3	$6x$	$-3x + 1$	$6x - 1$	$-3x + 2$	$-3x + 2$
4	$5x$	$-4x + 1$	$5x - 1$	$-4x + 2$	$-3x + 2$
5	$4x$	$-5x + 1$	$4x - 1$	$-5x + 2$	$4x - 2$
6	$3x$	$3x$	$3x$	$-6x + 3$	$3x - 1$
7	$2x$	$2x$	$2x$	$-7x + 3$	$2x - 1$
8	x	x	x	x	x

TABLE 5. The function ψ_9^ω on $[0, 1/2]$ together with the indices h of the corresponding functions $\varphi_{9,h}^\omega$.

	$[0, 1/9]$	$[1/9, 1/5]$	$[1/5, 2/9]$	$[2/9, 1/4]$
$\psi_9^\omega(x)$	$8x$	$-x + 1$	$4x$	$-5x + 2$
(max, min)	(1,0)	(1,0)	(1,5)	(1,5)
	$[1/4, 3/9]$	$[3/9, 2/5]$	$[2/5, 4/9]$	$[4/9, 1/2]$
$\psi_9^\omega(x)$	$3x$	$-3x + 2$	$2x$	$-7x + 4$
(max, min)	(6,0)	(3,0)	(3,5)	(3,5)

In general, we get for $m \geq 1$,

$$\psi_{b_m}^\omega(x) = \psi_9^\omega(x) + \sum_{i=0}^{m-1} \psi_2^{id}(9 \cdot 2^i x),$$

which obtains its maximum at

$$x_m = \frac{3}{9} + \sum_{i=1}^m \frac{(-1)^i}{9 \cdot 2^i}, \quad \text{for } m > 0.$$

If m is even, the dominant interval is $J_m = [x_m - 1/b_m, x_m]$ and if m is odd, we get $J_m = [x_m, x_m + 1/b_m]$, and

$$\begin{aligned} \psi_{b_m}^\omega(x) &= 3x + \sum_{i=1}^m (-1)^i (b_{i-1}x - b_{i-1}x_{i-1}) \\ &= \frac{1}{9} (8 + 3m + (-2)^m (-8 + 27x)), \quad \text{for } m > 0 \quad \text{and} \quad x \in J_m. \end{aligned}$$

Finally, $\psi_{b_m}^\omega(x_m) = \frac{m+3}{3}$, and hence by (6),

$$s(\mathcal{S}_{b_m}^{\omega_m}) \leq \frac{m+3}{3 \log b_m} = \frac{m+3}{3 \log(9 \cdot 2^m)} < \frac{1}{3 \log 2},$$

as it is claimed. $\square$

REMARK 1. We also have a proof confirming the predicted values of $d_{b_n}^\omega$. However, this proof is long and technical so we omit it here. The main challenge is anyway to show that these two permutations give indeed the minimum and maximum in each interval B_n .

To conclude this section, we believe that the algorithm of Faure can be interpreted in a vague sense as transferring the structure of the original van der Corput sequence in base 2 to arbitrary integer bases. The numerical results show that the discrepancy of sequences generated by a permutation ω is always close to the discrepancy of $\mathcal{S}_2^{id}$.

4. Two families of permutations

The algorithm of Faure is the main motivation for the results of Pausinger & Topuzoğlu [51] presented (among other things) in this section. One disadvantage of Faure's algorithm is that we only get one permutation in a given base, and constructing this permutation requires the construction of permutations in smaller bases. In [51] the authors aim to give discrepancy bounds for sequences generated from structurally similar permutations in a given (prime) base p . The advantage of restricting to prime bases p is that finite fields $\mathbb{F}_p$ of p elements are polynomially complete. This means that any self map, and in particular any permutation of $\mathbb{F}_p$, can be expressed as a polynomial over $\mathbb{F}_p$. Therefore, we consider in the following permutation polynomials in $\mathbb{F}_p[x]$, where we identify $\mathbb{F}_p$ with $\{0, 1, \dots, p-1\}$. In this section we are mainly interested in two essentially different families of permutations; i.e., affine permutations and fractional affine permutations. The main idea is to describe structurally similar permutations with very few parameters. Ideally these parameters connect the construction of the permutation with a discrepancy estimate of the resulting sequence and, therefore, provide some insight into the structure of good and weak permutations.

4.1. Affine permutations

For fixed but arbitrary $a_0 \in \mathbb{F}_p \setminus \{0\} = \mathbb{F}_p^*$ and $a_1 \in \mathbb{F}_p$ we call the permutation $\sigma = \sigma_{a_0, a_1}$ *affine* if

$$\sigma_{a_0, a_1}(x) = a_0 x + a_1,$$

and we denote the family of affine permutations in base p with $\mathcal{F}_p^{(a)}$. Note that affine permutations are also known as *linear digit scramblings*. This name goes back to a paper of Matoušek [41] and is also discussed in [19]. Our notation is motivated by the underlying geometric interpretation and should highlight its algebraic relation to the second family.

Interestingly, we can find an upper bound for $s(\mathcal{S}_p^\sigma)$ for affine permutations $\sigma = \sigma_{a_0, a_1}$ in terms of the parameter a_0 . We refer to the book of Khinchin [32] for an introduction to continued fractions. Using the standard notation we denote the finite continued fraction expansion of the rational number $\alpha \in [0, 1)$ by

$$\alpha = [0, \alpha_1, \alpha_2, \dots, \alpha_m].$$

THEOREM 3 (Pausinger & Topuzoğlu [51]). *For a prime p , let*

$$a_0 \in \mathbb{F}_p^*, a_1 \in \mathbb{F}_p \quad \text{and} \quad \sigma = \sigma_{a_0, a_1} \in \mathcal{F}_p^{(a)}.$$

Let

$$a_0/p = [0, \alpha_1, \alpha_2, \dots, \alpha_m] \quad \text{and set} \quad \alpha_{\max} = \max_{1 \leq i \leq m} \alpha_i.$$

Then, for all $N \in \mathbb{N}$,

$$D_N(\mathcal{S}_p^\sigma) \leq \frac{\alpha_{\max} + 1}{\log(\alpha_{\max} + 1)} \log(N + 1) \quad \text{and} \quad s(\mathcal{S}_p^\sigma) \leq \frac{\alpha_{\max} + 1}{\log(\alpha_{\max} + 1)}.$$

The main idea of the proof is to combine a result of Niederreiter with the asymptotic method of Faure. Niederreiter proved an upper bound for the discrepancy of the first N points of any $(\{n\alpha\})$ sequence in terms of $\alpha_{\max}$ provided α has bounded partial quotients; [36, Chapter 2, Theorem 3.4]. It is observed that the first $N = p$ points of a van der Corput sequence generated from an affine permutation are similarly distributed as the first $N = p$ points of an $(n\alpha)$ -sequence if the continued fraction of a_0/p coincides with the initial segment of the expansion of α . The bound of Niederreiter for $1 \leq N \leq p$ is used to get upper bounds for the values of Faure's ψ_b^σ -functions. These upper bounds then suffice to get the stated bounds on the discrepancy constants.

Since $id \in \mathcal{F}_p^{(a)}$ (for $a_0 = 1, a_1 = 0$) it is clear that the number $\alpha_{\max}$ may depend on p ; i.e., the continued fraction expansion of $1/p$ contains p . One interesting problem is therefore to determine, in case there are any, which values

of a_0 and p guarantee an absolute bound for $\alpha_{\max}$, i.e., a bound, which is independent of p similar to Faure's Theorem 1. There is a close relation between this problem and the well-known *conjecture of Zaremba* [61]. Indeed, recent progress on this conjecture [4, 31] shows the existence of an infinite set $\mathcal{N}$ of primes such that for each $p \in \mathcal{N}$, there exists an a_0 with $\alpha_{\max} \leq 5$.

REMARK 2. Since the current results on the conjecture of Zaremba are only for an infinite subset of primes and are non-constructive, one may wonder if Theorem 3 is applicable at all. The bound in Theorem 3 is favorable only when a_0 and p are chosen such that $\alpha_{\max}$ is small. We call such a parameter a_0 a good multiplier in base p . In fact, for practical purposes one can easily obtain good multipliers by looking at the continued fraction expansions of a_0/p . We refer to [51, Table 1] for a list of multipliers for $11 \leq p \leq 151$, with $\alpha_{\max}(a_0/p) \leq 3$.

REMARK 3. A generalized Halton sequence is a multi-dimensional sequence, whose i th coordinate is a permuted van der Corput sequence; see also Section 6. Faure [16] and Faure & Lemieux [20] derived in numerical experiments various selection criteria for good (and weak) multipliers a_0 (or f in the notation of these papers) for the generation of Halton sequences with small discrepancy. Theorem 3 (and related results from [49]) explain some of the observations and suggestions made in [16, 20].

Let $\mathfrak{F}_n$ denote the n th Fibonacci number. It is well known that

$$\lim_{n \rightarrow \infty} \mathfrak{F}_{n-1}/\mathfrak{F}_n = (\sqrt{5} - 1)/2$$

and the continued fraction expansion of $\mathfrak{F}_{n-1}/\mathfrak{F}_n$ contains only 1s (apart from a leading 0). The bound in Theorem 3 as well as the main idea of its proof indicate that affine permutations in base $\mathfrak{F}_n$ with multiplier $\mathfrak{F}_{n-1}$ may generate sequences with smallest asymptotic constants within the family of affine permutations. This is also in accordance with the widely held belief that $\alpha = (\sqrt{5} - 1)/2$ generates the $(\{n\alpha\})$ sequence with the smallest asymptotic constant. We investigated these special permutations numerically and summarise our results in the following conjecture.

CONJECTURE 2. Let $p_n = \mathfrak{F}_n$ and $\mu_n = \sigma_{p_{n-1}, 0}$. Moreover, define the sequence $(z(n))_{n \geq 1}$ as $z(n) := z(n-1) + z(n-3) + z(n-4)$, with $z(1) = 1, z(2) = 1, z(3) = 1, z(4) = 2$. We conjecture that

$$\max_{x \in [0, 1]} \psi_{p_n}^{\mu_n}(x) = \psi_{p_n}^{\mu_n} \left(\frac{z(n-2)}{p_n} \right) = \psi_{p_n}^{\mu_n} \left(\frac{z(n-1)}{p_n} \right).$$

Furthermore, the dominant interval is $\left[\frac{z(n-2)}{p_n}, \frac{z(n-2)+1}{p_n} \right]$ and

$$\alpha_{p_n}^{\mu_n} = \lim_{m \rightarrow \infty} \alpha_{p_n, m}^{\mu_n} \quad \text{with} \quad \alpha_{p_n, m}^{\mu_n} = \frac{1}{m} \sum_{j=0}^{m-1} \psi_{p_n}^{\mu_n}(\hat{x}_{n, m} p_n^j)$$

in which $\hat{x}_{n, m} = \sum_{i=1}^m \frac{z(n-2)}{p_n^i}$.

Based on this conjecture we calculated bounds for $s(\mathcal{S}_{p_n}^{\mu_n})$ which we collect in Table 6 and Table 7. These results confirm the intuition that affine permutations generate van der Corput sequences whose distribution behavior is similar to what can be achieved with $(\{n\alpha\})$ sequences. Theorem 3 links $(\{n\alpha\})$ sequences to generalised van der Corput sequences. Comparing the best known asymptotic constants due to Faure and Ostromoukhov with the lower bounds in Table 6 and Table 7 raises once again the question: *What is the hidden structure that can not be captured by affine permutations resp. $(\{n\alpha\})$ sequences?*

TABLE 6. Bounds on asymptotic constants of $\mathcal{S}_{p_n}^{\mu_n}$ generated from Fibonacci-linear permutations with $p_n = \mathfrak{F}_n$ being the n th Fibonacci number and μ_n being the affine permutation with multiplier p_{n-1} . The lower bounds are calculated via Conjecture 2, the upper bounds are calculated from the maximum of the corresponding ψ -functions.

n	$\mathfrak{F}_n$	
8	21	$0.4269 \leq s(\mathcal{S}_{21}^{\mu}) < 0.4693$
9	34	$0.4382 \leq s(\mathcal{S}_{34}^{\mu}) < 0.4588$
10	55	$0.4159 \leq s(\mathcal{S}_{55}^{\mu}) < 0.4538$
11	89	$0.4050 \leq s(\mathcal{S}_{89}^{\mu}) < 0.4506$
12	144	$0.4221 \leq s(\mathcal{S}_{144}^{\mu}) < 0.4472$
13	233	$0.4301 \leq s(\mathcal{S}_{233}^{\mu}) < 0.4441$
14	377	$0.4160 \leq s(\mathcal{S}_{377}^{\mu}) < 0.4418$
15	610	$0.4086 \leq s(\mathcal{S}_{610}^{\mu}) < 0.4399$
16	987	$0.4202 \leq s(\mathcal{S}_{987}^{\mu}) < 0.4383$

4.2. Fractional affine permutations

For $a_0 \in \mathbb{F}_p^*$ and $a_1, a_2 \in \mathbb{F}_p$ we call the permutation $\pi = \pi_{a_0, a_1, a_2}$ *fractional affine* if

$$\pi_{a_0, a_1, a_2}(x) = (a_0 x + a_1)^{p-2} + a_2,$$

ON THE INTRIGUING SEARCH FOR GOOD PERMUTATIONS

TABLE 7. Bounds on asymptotic constants for Fibonacci-linear, $\mathcal{S}_{p_n}^{\mu_n}$, with $p_n = \mathfrak{F}_n$ being the n th Fibonacci number and μ_n being the affine permutation with multiplier p_{n-1} . The lower bounds are calculated via Conjecture 2.

n	$\mathfrak{F}_n$	
17	1597	$0.4263 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
18	2584	$0.4159 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
19	4181	$0.4102 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
20	6765	$0.4192 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
21	10946	$0.4241 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
22	17711	$0.4159 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
23	28657	$0.4112 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
24	46368	$0.4185 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
25	75025	$0.4226 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
26	121393	$0.4158 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
27	196418	$0.4119 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
28	317811	$0.4181 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
29	514229	$0.4216 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$
30	832040	$0.4158 \leq s(\mathcal{S}_{\mathfrak{F}_n}^{\mu})$

and we denote the family of fractional affine permutations with $\mathcal{F}_p^{(f)}$. This family does not contain the identity; in fact $\mathcal{F}_p^{(a)}$ and $\mathcal{F}_p^{(f)}$ are always disjoint. Interestingly, it turns out that permutations in $\mathcal{F}_p^{(f)}$ define sequences all of which are better distributed than the classical van der Corput sequence in the same base; compare (3) and (7).

THEOREM 4 (Pausinger & Topuzoglu [51]). *Let $a_0 \in \mathbb{F}_p^*$ and $a_1, a_2 \in \mathbb{F}_p$ and let $\pi = \pi_{a_0, a_1, a_2} \in \mathcal{F}_p^{(f)}$. Then,*

$$s(\mathcal{S}_p^{\pi}) < s(\mathcal{S}_p^{id}). \quad (7)$$

REMARK 4. Even if the set of permutations $\mathcal{F}_p^{(f)}$ is much larger than $\mathcal{F}_p^{(a)}$, the range of values for $s(\mathcal{S}_p^{\pi})$ is smaller. While $\mathcal{F}_p^{(a)}$ contains permutations generating sequences with very small as well as largest possible discrepancy (in the context of permuted van der Corput sequences), the permutations in $\mathcal{F}_p^{(f)}$ avoid this extremal behavior; see [51, Table 2] for numerical results.

To get an idea of the proof of this result let $\sigma \in \mathfrak{S}_b$. Faure showed [11, Corollaire 3] that

$$\psi_b^\sigma\left(\frac{k}{b}\right) \leq k\left(1 - \frac{k}{b}\right), \quad (8)$$

for $0 \leq k \leq b-1$.

Since $D_k(S_b^\sigma) = \psi_b^\sigma(k/b)$ for $1 \leq k \leq b-1$, we obtain equality in (8) if and only if all k points lie in an interval of length k/b , since $k - \frac{k^2}{b} = k\left(1 - \frac{k}{b}\right)$. The identity permutation satisfies this for every k from which Faure obtains

$$\max_{1 \leq k \leq b} \psi_b^{id}(k/b) = \psi_b^{id}\left(\frac{\lfloor b/2 \rfloor}{b}\right) \quad \text{and} \quad \psi_b^\sigma(x) \leq \psi_b^{id}(x),$$

for all $x \in [0, 1]$ and all $\sigma \in \mathfrak{S}_b$. In addition,

$$\psi_b^{id}(k/b) = \psi_b^\sigma(k/b)$$

whenever $V_k^\sigma = \{1, \dots, k\} \oplus a$, where $a \in \mathbb{N}$ is constant and $\oplus$ denotes addition modulo b . Moreover, Faure finds for odd b [11, Théorème 6] that

$$\alpha_b^{id} = \lim_{n \rightarrow \infty} \alpha_{b,n}^{id} \quad \text{with} \quad \alpha_{b,n}^{id} = \frac{1}{n} \sum_{j=1}^n \psi_b^{id}\left(\frac{\tilde{x}_n}{b^j}\right),$$

in which

$$\tilde{x}_n = \sum_{j=1}^n \frac{b-1}{2} b^{j-1}.$$

It turns out [51, Lemma 4.1] that fractional affine permutations never map the set $\{0, 1, \dots, (p-1)/2\}$ to a set of the form $V_{(p-1)/2}^{id} \oplus a$, for an $a \in \mathbb{F}_p$. Consequently,

$$\max_{1 \leq k \leq p} \psi_b^\pi(k/p) < \max_{1 \leq k \leq p} \psi_p^{id}(k/p),$$

for all $\pi = \pi_{a_0, a_1, a_2} \in \mathcal{F}_p^{(f)}$ from which the result follows.

The observations and calculations mentioned in Remark 4 suggest the following conjecture.

CONJECTURE 3. *There exists an increasing function $\kappa : \mathbb{N} \rightarrow \mathbb{R}$ with $\kappa(p) < s(\mathcal{S}_p^\pi)$ for all $\pi \in \mathcal{F}_p^{(f)}$ and $\lim_{n \rightarrow \infty} \kappa(n) = \infty$. In other words, there is no infinite subset of fractional affine permutations such that the corresponding asymptotic constants can be bounded by an absolute constant – in contrast to the infinite sets of permutations in Theorem 1 and Theorem 3.*

We can even go one step further and extend the family of affine permutations. First, we consider fractional linear transformations

$$R_1(x) = \frac{\alpha_2 x + \beta_2}{\alpha_1 x + \beta_1}, \quad \alpha_2 \beta_1 - \beta_2 \alpha_1 \neq 0,$$

ON THE INTRIGUING SEARCH FOR GOOD PERMUTATIONS

and the permutations of $\mathbb{F}_p$, defined as $\bar{\pi}(x) = R_1(x)$ for $x \in \mathbb{F}_p \setminus \{-\beta_1/\alpha_1\}$, and $\bar{\pi}(-\beta_1/\alpha_1) = -\alpha_2/\alpha_1$. Clearly, $\bar{\pi}(x)$ can be expressed as

$$\bar{\pi}(x) = \pi_{a_0, a_1, a_2}(x) = (a_0x + a_1)^{p-2} + a_2,$$

where

$$a_0 \neq 0, \quad \alpha_1 = a_0, \quad \beta_1 = a_1, \quad \alpha_2 = a_0a_2, \quad \beta_2 = a_1a_2 + 1.$$

Similarly, we consider permutations

$$\tau(x) = \tau_{A_0, A_1, A_2, A_3}(x) = ((A_0x + A_1)^{p-2} + A_2)^{p-2} + A_3$$

for

$$A_0, A_2 \in \mathbb{F}_p^* \quad \text{and} \quad A_1, A_3 \in \mathbb{F}_p,$$

and the fractional transformations

$$R_2(x) = \frac{\alpha_3x + \beta_3}{\alpha_2x + \beta_2},$$

where α_2, β_2 are as above, and $\alpha_3 = A_0(A_2A_3 + 1)$, $\beta_3 = A_1(A_2A_3 + 1) + a_3$. We note that $\tau(x) = R_2(x)$ for $x \in \mathbb{F}_p \setminus \{X_1, X_2\}$, with

$$X_1 = -A_1/A_0, \quad \text{and} \quad X_2 = -(A_1A_2 + 1)/(A_0A_2),$$

and set $\tau(X_1) = \alpha_3/\alpha_2$, $\tau(X_2) = R_2(X_1)$.

Interestingly, it was observed in [51] that for every permutation π there exists a permutation τ such that $\pi(x) = \tau(x)$ for all $x \in \mathbb{F}_p \setminus \{X_1, X_2\}$; i.e., we can attach $p - 1$ permutations τ to each permutation π .

THEOREM 5 (Pausinger & Topuzoglu [51]). *Fix $a_0, a_1, a_2 \in \mathbb{F}_p$, with $a_0, a_2 \neq 0$ and set (in $\mathbb{F}_p$)*

$$A_0 = -a_0a_2^2, \quad A_1 = -a_1a_2^2 - a_2, \quad A_2 = 1/a_2.$$

Consider $\pi = \pi_{a_0, a_1, a_2} \in \mathcal{F}_p^{(f)}$ and $\tau = \tau_{A_0, A_1, A_2, 0}$. Then $\pi(x) = \tau(x)$ for all $x \in \mathbb{F}_p$, except for

$$X_1 = -(a_1a_2 + 1)/a_0a_2, \quad X_2 = -a_1/a_0,$$

for which $\pi(X_1) = \tau(X_2)$ and $\pi(X_2) = \tau(X_1)$.

It turns out that all permutations in a fixed base p of the form $\tau_{A_0, A_1, A_2, A_3}$ generate sequences whose discrepancy is very similar to the corresponding permutation π_{a_0, a_1, a_2} . In particular, extremal discrepancy behaviour is again omitted (see Remark 4).

CONJECTURE 4. *We believe Theorem 4 and Conjecture 3 also hold for the larger but structurally similar set of permutations of the form $\tau_{A_0, A_1, A_2, A_3}$.*

4.3. Directions for future work

Theorem 3 and 4 offer two assets to the practitioner. Firstly, they provide a criterion based on continued fractions to choose a provably *good multiplier* for linear digit scrambling in prime base p . Secondly, they show that picking any permutation from $\mathcal{F}_p^{(a)}$ ensures to avoid extremal discrepancy behavior of the resulting sequence - independent of the particular choice of parameters. That is, any choice of parameters a_0, a_1, a_2 gives a sequence that is better than the worst and worse than the best generalised van der Corput sequences in base p .

Every permutation of $\mathbb{F}_p$ can be represented by a polynomial

$$P_n(x) = \left(\cdots ((a_0x + a_1)^{p-2} + a_2)^{p-2} \cdots + a_n \right)^{p-2} + a_{n+1}, \quad n \geq 0$$

for $a_0a_2 \cdots a_n \neq 0$, with an associated fractional transformation

$$R_n(x) = \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_nx + \beta_n},$$

where α_i, β_i , $i \geq 2$ can be described recursively. This is due to a well-known result of Carlitz [5], and leads to the concept of the *Carlitz rank* of permutations. For details we refer to [56] and the references therein. The Carlitz rank is a particular measure of the complexity of a permutation. The results of this section can be seen as a study of permutations of small Carlitz rank, i.e., Carlitz rank 0, 1, 2. Thus, this is a first step towards a systematic study of the distribution properties of permutations of fixed Carlitz rank n . Numerical investigations of permutations of Carlitz rank 3 show that certain subsets improve the smallest values obtained for affine permutations.

PROBLEM 2. *Study permutations of larger Carlitz rank and characterise the structure of those permutations that improve the best results for affine permutations. Prove results similar to Theorem 3 and 4.*

PROBLEM 3. *Study the permutation of Ostromoukhov in base 84. Is there a compact way to describe Ostromoukhov's permutation as a polynomial resp. with few parameters?*

5. Sequences of permutations

A second approach to improving the asymptotic constants of classical van der Corput sequences is to study particular sequences of permutations. In this context the Swapping Lemma plays a crucial role. The result of Faure [11, Théorème 3] for the star discrepancy presented in Section 2.3 is a first success in this direction. Since

$$\psi_b^{id,-} = 0,$$

it is possible to calculate the asymptotic constants for sequences $\mathcal{S}_b^{\Sigma^{id}}$. In fact,

$$s^*(\mathcal{S}_b^{\Sigma^{id}}) = \frac{\alpha_b^{id,+}}{2 \log b} = \begin{cases} \frac{b-1}{8 \log b} & \text{if } b \text{ is odd,} \\ \frac{b^2}{8(b+1) \log b} & \text{if } b \text{ is even.} \end{cases}$$

Thus, this construction improves the constants $s^*(\mathcal{S}_b^{id})$ obtained for the classical van der Corput sequences by a factor of 2 – which is known to be the best possible reduction; see [19, Section 2.3]. The smallest value is obtained for $b = 3$ with $s^*(\mathcal{S}_3^{\Sigma^{id}}) = 0.2275\dots$ being quite close to the currently smallest known value.

In this context there is another interesting structural result obtained for $b = 2$ by Kritzer, Larcher & Pillichshammer in [35]. They consider general sequences Σ of the two permutations $id_2 = (0, 1)$ and $\tau_2 = (1, 0)$ in base 2 and define for $m \in \mathbb{N}$

$$S_m(\Sigma) := \max(\#\{0 \leq j \leq m-1 : \sigma_j = \tau_2\}, \#\{0 \leq j \leq m-1 : \sigma_j = id_2\})$$

and

$$T_m(\Sigma) := \#\{1 \leq j \leq m-1 : \sigma_{j-1} = \tau_2 \text{ and } \sigma_j = id_2\}.$$

It turns out that these two quantities can be used to give precise discrepancy estimates for generalised van der Corput sequences.

THEOREM 6 (Kritzer, Larcher & Pillichshammer [35]). *If $\Sigma = (\sigma_j)_{j \geq 0}$ is a sequence of the two permutations id_2 and τ_2 , then*

$$\frac{S_m(\Sigma)}{3} + \frac{T_m(\Sigma)}{48} - 4 \leq \max_{1 \leq N \leq 2^m} D_N^*(S_b^\Sigma) \leq \frac{S_m(\Sigma)}{3} + \frac{2T_m(\Sigma)}{9} + \frac{56}{9}.$$

This theorem shows that essentially two properties of Σ influence the star discrepancy of generalised van der Corput sequences. These are the number of identity permutations compared to the number of transpositions as well as their distribution. In particular, it shows that it is favourable to have, for each m , about the same number of identity permutations and transpositions with as few changes as possible. This result hints that the original choice of Faure from [11, Théorème 3] is best possible.

It would be very interesting to extend Theorem 6 beyond base 2. Sequences Σ_A^σ having the desirable structure have been studied in the context of Hammersley point sets as discussed in the next section. However, it seems all these approaches rely on the Swapping Lemma in a crucial way—what happens in the case of more involved sequences of permutations?

PROBLEM 4. *Study more general sequences of permutations and extend Theorem 6 beyond base 2. What happens, e.g., in base 3 or 5? Is $s^*(\mathcal{S}_3^{\Sigma^{id}})$ already best possible among all sequences of permutations in base 3? What happens if we use sequences of affine and swapped affine permutations in larger bases?*

6. Faure's method in a wider context

The aim of this section is to give an idea how Faure's methods have been used in a wider context over the years. We highlight a number of theorems that would be immediately affected by any improvement of the result of Ostromoukhov.

6.1. Generalised Hammersley point sets

The definition of star and extreme discrepancy for multi-dimensional point sets and sequences is a straightforward generalisation of the one dimensional notion in which the supremum is taken over all axis-aligned sub-rectangles of $[0, 1]^d$ instead of all subintervals of $[0, 1]$; see [8, 9, 36]. The radical inverse function $S_b(n)$ can be used to construct multidimensional point sets and sequences with low discrepancy. Kuipers & Niederreiter write in the Notes to Section 3 in [36, Chapter 2] that such constructions go back to the seminal paper of Roth [54] from 1954 in which he used the radical inverse function $S_2(n)$ to construct a point set in two dimensions. Later Halton [28] showed that the infinite sequence $\mathcal{H}_{\mathbf{b}} = (H_{\mathbf{b}}(n))_{n \geq 1}$, in which $\mathbf{b} = (b_1, \dots, b_d)$ is a d -tuple of pairwise coprime integers and

$$H_{\mathbf{b}}(n) = (S_{b_1}(n), \dots, S_{b_d}(n))$$

is uniformly distributed [28]. Sequences of the form $\mathcal{H}_{\mathbf{b}}$ are nowadays referred to as *Halton sequences*. In the context of numerical integration there is the related concept of a *Hammersley point set* [30]. The main difference is that the number of points, N , is fixed in the case of Hammersley point sets and the last coordinate of the n th point is equal to n/N for $1 \leq n \leq N$. It is widely believed that both constructions yield examples of point sets and sequences with the optimal order of star discrepancy. However, this question is only settled for one dimensional sequences and two dimensional point sets (see [55]) and is still open in larger dimensions.

In [18] Faure considered generalised two-dimensional Hammersley point sets, $\mathcal{H}_{b,m}^{\Sigma}$, which are deduced from generalised van der Corput sequences and defined as

$$\mathcal{H}_{b,m}^{\Sigma} := \left\{ \left(S_b^{\Sigma}(n), \frac{n-1}{b^m} \right) : 1 \leq n \leq b^m \right\}.$$

Faure remarks that in order to match the traditional definitions of arbitrary Hammersley point sets which are m -bits, i.e., whose b -adic expansions do not exceed m bits, he restricts to infinite sequences of permutations Σ such that $\sigma_r(0) = 0$ for all $r \geq m$, such that the distribution behaviour of $\mathcal{H}_{b,m}^{\Sigma}$ only depends on the first m permutations

$$\sigma = (\sigma_0, \dots, \sigma_{m-1}).$$

This restriction is indicated by writing $\mathcal{H}_{b,m}^\sigma$. The classical Hammersley point set in base b can be obtained if we set $\sigma_r = id$ for all permutations. Faure discusses in the introduction of [18] important contributions of Halton & Zaremba [29], De Clerck [7] and Larcher & Pillichshammer [40] to the exact calculation of the (star) discrepancy of particular two-dimensional Hammersley point sets as well as approximative formulas for the leading terms within a small error (usually lower than a small additive constant that does not play a role in the asymptotic analysis of the discrepancy) by himself [12], Kritzer [34] and Kritzer, Larcher & Pillichshammer [35].

The main contribution of Faure's paper is the following formula [18, Theorem 1] for the star discrepancy of generalised Hammersley point sets.

THEOREM 7 (Faure [18]). *For any $m \in \mathbb{N}$ and any $\sigma = (\sigma_0, \dots, \sigma_{m-1}) \in \mathfrak{S}_b^m$ we have with some $c_m \in [0, 2]$,*

$$D_{b^m}^*(\mathcal{H}_{b,m}^\sigma) = \max \left(\max_{1 \leq n \leq b^m} \sum_{j=1}^m \psi_b^{\sigma_{j-1},+} \left(\frac{n}{b^j} \right), \max_{1 \leq n \leq b^m} \sum_{j=1}^m \psi_b^{\sigma_{j-1},-} \left(\frac{n}{b^j} \right) \right) + c_m.$$

He continues his investigations with a detailed study of particular sequences of permutations σ . In particular, he studies tuples of permutations consisting of id and τ_b . Following Kritzer who studied such arrangements in base 2 [34], he defines

$$i\tau = (id, \dots, id, \tau, \dots, \tau),$$

in which, for even m , $m/2$ copies of id are followed by $m/2$ copies of τ or, in the case of odd m , $(m-1)/2$ copies of id are followed by $(m+1)/2$ copies of τ . Using Theorem 7 Faure is able to derive a formula for $\mathcal{H}_{b,m}^{i\tau}$ in [18, Theorem 2] and, in particular, derives the following asymptotic results in [18, Corollary 2]:

$$\lim_{m \rightarrow \infty} \frac{D_{b^m}^*(\mathcal{H}_{b,m}^{i\tau})}{\log b^m} = \frac{b-1}{8 \log b}, \quad \text{if } b \text{ is odd and}$$

$$\lim_{m \rightarrow \infty} \frac{D_{b^m}^*(\mathcal{H}_{b,m}^{i\tau})}{\log b^m} = \frac{b^2}{8(b+1) \log b}, \quad \text{if } b \text{ is even.}$$

This recovers the earlier results of [34, 35] for $b = 2$ and shows that the best constant is obtained for $b = 3$ with $1/(4 \log 3) = 0.227 \dots$. Interestingly, it is shown [18, Theorem 3] that these asymptotic values can not be improved by any other σ in which each component σ_j , $1 \leq j \leq m$ is either id or τ . However, [18, Theorem 4] shows that the asymptotic values actually *depend* on the distribution of id and τ in σ .

Furthermore, Faure considers swapping with an arbitrary permutation and studies sequences σ that are generated from permutations σ and $\bar{\sigma} := \tau \circ \sigma$.

Defining $\sigma\bar{\sigma}$ analogously to $i\tau$, he obtains a formula for $D_{b^m}^*(\mathcal{H}_{b,m}^{\sigma\bar{\sigma}})$ in [18, Theorem 5] and gets the asymptotic formula

$$\lim_{m \rightarrow \infty} \frac{D_{b^m}^*(\mathcal{H}_{b,m}^{\sigma\bar{\sigma}})}{\log b^m} = \frac{\alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}}{2 \log b}. \quad (9)$$

From this he is able to slightly improve the best asymptotic results for $\sigma = i\tau$ by using those permutations that also give the best possible asymptotic star discrepancy constant for generalised van der Corput sequences. Ostromoukhov shows in [43, Theorem 5] that for his record permutation, $\sigma_{60} = \sigma$, in base 60 $\psi_{60}^{\sigma,-} = 0$ and hence $\psi_{60}^{\sigma} = \psi_{60}^{\sigma,+}$. Consequently, $\alpha_{60}^{\sigma,-} = 0$ and we get from (9)

$$\lim_{m \rightarrow \infty} \frac{D_{60^m}^*(\mathcal{H}_{60,m}^{\sigma\bar{\sigma}})}{\log 60^m} = \frac{\alpha_b^{\sigma,+}}{2 \log 60} = \frac{32209}{17700} \frac{1}{2 \log 60} = 0.222223.$$

Finally, Faure and Pillichshammer also thoroughly studied the L_p -discrepancy of generalised Hammersley point sets and derived various interesting results. In particular, they showed in [21] that the L_p -discrepancy, for finite p , of classical Hammersley point sets is not of optimal order according to the known lower bounds for arbitrary N -element point sets. Interestingly, this can be overcome when using certain generalised Hammersley point sets. In particular, there are various papers that provide constructions of such point sets with optimal order of L_2 -discrepancy; see [21, 22, 25], [23] with Schmid and Piršic and [24] with Piršic as well as [19, Section 4.1] for a more information.

6.2. Digital $(0, 1)$ -sequences in prime base

It can be easily shown that for every

$$m \in \mathbb{N} \quad \text{and} \quad k \in \{0, 1, \dots, b^m - 1\}$$

exactly one of b^m consecutive elements of the van der Corput sequence in base b belongs to a b -adic elementary interval of the form

$$[k/b^m, (k+1)/b^m).$$

This important property forms the basis for the definition of the much larger set of $(0, 1)$ -sequences whose definition goes back to Niederreiter [42]. The methods of Faure can be extended to this larger set of sequences. In the following we briefly review some of the results in this direction without going into details; we refer to [19, Section 3.2] for a more thorough introduction of the related concepts.

Interestingly, it is known that among *all* $(0, 1)$ -sequences in base b the classical van der Corput sequence in base b has the worst star discrepancy [17, 33, 52]. In [14] Faure considers a particular subset of digital $(0, 1)$ -sequences, so called

NUT digital $(0, 1)$ -sequences over $\mathbb{F}_p$, with p prime, for which he obtains formulas for the discrepancy in the spirit of the results of Section 2.1. These results were later extended to arbitrary integer bases resp. to the even larger class of NUT $(0, 1)$ -sequences over $\mathbb{Z}_b$ [26].

Finally, and this is the main reason why we gave this brief outlook, it turns out that the asymptotic constants α_b^σ can be used to formulate best possible lower bounds for the star discrepancy of NUT $(0, 1)$ -sequences over $\mathbb{Z}_b$, which form so far the most general family of van der Corput type sequences for which such a result exists; see [19, Theorem 36 and its corollaries]. In this context, the permutation of Ostromoukhov can again be used to generate a sequence with to date smallest known asymptotic constant.

7. Why things remain intriguing

We have given a broad overview of the use of permutations in uniform distribution theory. Henri Faure provided the necessary tools to calculate and compare sequences generated from different permutations. Even the most modern and general constructions of low discrepancy sequences can benefit from good *seeds*, i.e., good generating permutations. Despite all the efforts and the various great structural results, our main question remains open. *What is the hidden structure behind the best permutations?* We have seen that this structure is not linear-like since $(\{n\alpha\})$ sequences as well as van der Corput sequences generated from affine permutations can be improved using the permutations of Ostromoukhov. So the structure imposed by affine permutations seems to be too rigid. We have also seen that a clever alternation of $(0, 1)$ and $(1, 0)$ gives sequences of permutations whose corresponding van der Corput sequence has almost smallest known star discrepancy. However, the results of Faure for Hammersley point sets hint that using Ostromoukhov's permutations in a similar fashion yields once again slightly better results.

Thus the problem remains intriguing! Is there such thing as a best permutation? And if yes, how could we know that we have found it? We believe that the infimum in the definition of $\hat{s}$ and $\hat{s}^*$ is indeed an infimum (and not a minimum) and that we can always find a permutation in a larger base that slightly improves the so far smallest value. For this reason we find Conjecture 1 very interesting. Because the main difficulty in this conjecture is the fact that we study infinitely many sequences whose asymptotic constants seem to converge to a particular value. We believe that the solution of this conjecture may require an idea that could also be useful in the search for optimal permutations resp. for improving the results of Ostromoukhov.

Appendix A. List of good permutations

In this appendix we list the permutations that generate generalised van der Corput sequences with to-date smallest known asymptotic extreme discrepancy, star discrepancy and diaphony constants. We reformulate the corresponding results in our notation.

A.1. Extreme discrepancy

Let

$$\sigma_{36} = (0, 25, 17, 7, 31, 11, 20, 3, 27, 13, 34, 22, 5, 15, 29, 9, 23, 1, \\ 18, 32, 8, 28, 14, 4, 21, 33, 12, 26, 2, 19, 10, 30, 6, 16, 24, 35),$$

and let

$$\sigma_{84} = (0, 22, 64, 32, 50, 76, 10, 38, 56, 18, 72, 45, 6, 28, 59, 79, 41, 13, 67, 25, 54, \\ 2, 36, 70, 16, 48, 81, 30, 61, 8, 43, 74, 20, 52, 4, 34, 66, 15, 46, 77, 26, 11, \\ 62, 39, 82, 57, 23, 69, 33, 3, 51, 19, 73, 42, 7, 60, 29, 80, 47, 14, 65, 35, 1, \\ 53, 24, 68, 12, 40, 78, 58, 27, 5, 44, 71, 17, 55, 37, 83, 21, 49, 75, 9, 31, 63).$$

THEOREM 8 (Faure [13], Ostromoukhov [43]). *For $b = 36$ and σ_{36} we have*

$$s(\mathcal{S}_{36}^{\sigma_{36}}) = \frac{46}{35 \log 36} = 0.3667 \dots;$$

for $b = 84$ and σ_{84} we have

$$s(\mathcal{S}_{84}^{\sigma_{84}}) = \frac{130}{83 \log 84} = 0.3534 \dots$$

A.2. Star discrepancy

Let

$$\sigma_{60} = (0, 15, 30, 40, 2, 48, 20, 35, 8, 52, 23, 43, 12, 26, 55, 4, 32, 45, 17, 37, \\ 6, 50, 28, 10, 57, 21, 41, 13, 33, 54, 1, 25, 46, 18, 38, 5, 49, 29, 9, 58, \\ 22, 42, 14, 34, 53, 3, 27, 47, 16, 36, 7, 51, 19, 44, 31, 11, 56, 24, 39, 59).$$

THEOREM 9 (Ostromoukhov [43]). *For $b = 60$ and σ_{60} we have*

$$s^*(\mathcal{S}_{60}^{\Sigma_A^{\sigma_{60}}}) = \frac{32209}{35400 \log 60} = 0.222223 \dots$$

A.3. Diaphony

Let

$$\sigma_{19} = (0, 11, 5, 15, 9, 3, 17, 7, 13, 1, 12, 6, 16, 2, 8, 14, 4, 10, 18),$$

and let

$$\begin{aligned} \sigma_{57} = (0, 24, 37, 8, 43, 18, 52, 29, 11, 48, 33, 4, 21, 40, 14, 54, 26, 45, 6, \\ 35, 16, 50, 31, 2, 20, 39, 10, 47, 27, 55, 13, 42, 23, 3, 32, 51, 17, 36, \\ 7, 46, 28, 56, 15, 41, 22, 5, 34, 49, 9, 25, 53, 38, 12, 30, 1, 19, 44). \end{aligned}$$

THEOREM 10 (Chaix & Faure [6], Pausinger & Schmid [50]). *For $b=19$ and σ_{19} we have*

$$f(\mathcal{S}_{19}^{\sigma_{19}}) = \frac{3826\pi^2}{27 \cdot 19^2 \log 19} = 1.31574 \dots;$$

and for $b = 57$ and σ_{57} we have

$$f(\mathcal{S}_{57}^{\sigma_{57}}) = \frac{42407\pi^2}{28 \cdot 57^2 \log 57} = 1.13794 \dots$$

REFERENCES

- [1] BEHNKE, H.: *Zur Theorie der diophantischen Approximationen*, Abh. Math. Sem. Hamburg **3** (1924), 261–318; **4** (1926), 33–46.
- [2] BÉJIAN, R.: *Minoration de la discr pance d’une suite quelconque sur T* , Acta Arith. **41** (1982), 185–202.
- [3] B JIAN, R.—FAURE, H.: *Discr pance de la suite de van der Corput*, C.R. Acad. Sci. Paris Ser. A **285** (1977), 313–316.
- [4] BOURGAIN, J.—KONTOROVICH, A.: *On Zaremba’s conjecture*, Ann. of Math. (2) **180** (2014), 1–60.
- [5] CARLITZ, L.: *Permutations in a finite field*. Proc. Amer. Math. Soc. **4** (1953), 538.
- [6] CHAIX, H.—FAURE, H.: *Discr pance et diaphonie en dimension un*, Acta Arith. **63** (1993), 103–141.
- [7] DE CLERCK, L.: *A method for exact calculation of the star discrepancy of plane sets applied to sequences of Hammersley*, Monatsh. Math. **101** (1986), 261–278.
- [8] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.
- [9] DRMOTA, M.—TICHY, R.F.: *Sequences, Discrepancies and Applications. Lecture Notes in Mathematics Vol. 1651*. Springer Verlag, Berlin, 1997.
- [10] DUPAIN, Y.—S S, V.: *On the discrepancy of $(n\alpha)$ sequences. Topics in classical number theory*, Vol. I, II (Budapest, 1981), Colloq. Math. Soc. Janos Bolyai **34** (1984), 355–387.
- [11] FAURE, H.: *Discr pance de suites associ es   un syst me de num ration (en dimension un)*, Bull. Soc. Math. France **109** (1981), 143–182.
- [12] ———: *On the star-discrepancy of generalized Hammersley sequences in two dimensions*, Monatsh. Math. **101** (1986), 291–300.

- [13] FAURE, H.: *Good permutations for extreme discrepancy*, J. Number Theory **42** (1992), 47–56.
- [14] ——— *Discrepancy and diaphony of digital $(0, 1)$ -sequences in prime base*, Acta Arith. **117** (2005), 125–148.
- [15] ——— *Irregularities of distribution of digital $(0, 1)$ -sequences in prime base*, Integers **5** (2005), no. 3, #A07.
- [16] ——— *Selection criteria for (random) generation of digital $(0, s)$ -sequences*. In: Proceedings of the 6th international conference Monte Carlo and quasi-Monte Carlo methods in scientific computing Juan-les-Pins, France, July 7–10, 2004, *Monte Carlo and Quasi-Monte Carlo Methods 2004* (H. Niederreiter and D. Talay, eds.). Springer Berlin (2006), pp. 113–126.
- [17] ——— *Van der Corput sequences towards $(0, 1)$ -sequences in base b* , J. Théor. Nombres Bordeaux **19** (2007), 125–140.
- [18] ——— *Star extreme discrepancy of generalized two-dimensional Hammersley point sets*, Unif. Distrib. Theory **3** (2008), 45–65.
- [19] FAURE, H.—KRITZER, P.—PILLICHSHAMMER, F.: *From van der Corput to modern constructions of sequences for quasi-Monte Carlo rules*, Indag. Math., New Ser. **26** (2015), 760–822.
- [20] FAURE, H.—LEMIEUX, C.: *Generalized Halton sequences in 2008: A comparative study*, ACM Trans. Model. Comp. Sim. **19** (2009), 15:1–31.
- [21] FAURE, H.—PILLICHSHAMMER, F.: *L_p discrepancy of generalized two-dimensional Hammersley point sets*, Monatsh. Math. **158** (2009), 31–61.
- [22] FAURE, H.—PILLICHSHAMMER, F.: *L_2 discrepancy of two dimensional digitally shifted Hammersley point sets in base b* . In: Proceedings of the 8th international conference Monte Carlo and quasi-Monte Carlo methods in scientific computing, Montréal, Canada, July 6–11, 2008, *Monte Carlo and quasi-Monte Carlo methods 2008* (P. L’Ecuyer and A. B. Owen, eds.) Springer Berlin (2009), pp. 355–368.
- [23] FAURE, H.—PILLICHSHAMMER, F.—PIRSIC, G.—SCHMID, W. CH.: *L_2 discrepancy of generalized two dimensional Hammersley point sets scrambled with arbitrary permutations*, Acta Arith. **141** (2010), 395–418.
- [24] FAURE, H.—PILLICHSHAMMER, F.—PIRSIC, G.: *L_2 discrepancy of linearly digit scrambled Zaremba point sets*, Unif. Distrib. Theory **6** (2011), 59–81.
- [25] FAURE, H.—PILLICHSHAMMER, F.: *L_2 discrepancy of generalized Zaremba point sets*, J. Théor. Nombres Bordeaux **23** (2011), 121–136.
- [26] ——— *A generalization of NUT digital $(0, 1)$ -sequences and best possible lower bounds for star discrepancy*, Acta Arith. **158** (2013), 321–340.
- [27] HABER, S.: *On a sequence of points of interest for numerical quadrature*, J. Res. Nat. Bur. Stand. Sect. B **70B** (1966), no. 2. 127–136.
- [28] HALTON, J. H.: *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*. Numer. Math. **2** (1960), 84–90.
- [29] HALTON, J. H.—ZAREMBA, S. K.: *The extreme and the L^2 discrepancies of some plane sets*, Monatsh. Math. **73** (1969), 316–328.
- [30] HAMMERSLEY, J. M.: *Monte Carlo methods for solving multivariable problems*, Ann. New York Acad. Sci. **86** (1960), 844–874.
- [31] HUANG, S.: *An improvement to Zaremba’s conjecture*, Geom. Funct. Anal. **25** (2015), no. 3, 860–914.
- [32] KHINCHIN, A. YA. : *Continued Fractions*. the University of Chicago Press, Chicago, Ill.-London 1964.

ON THE INTRIGUING SEARCH FOR GOOD PERMUTATIONS

- [33] KRITZER. P.: *A new upper bound on the star discrepancy of $(0, 1)$ -sequences*, *Integers* **5(3)** (2005), A11.
- [34] ——— *On some remarkable properties of the two-dimensional Hammersley point set in base 2*, *J. Théor. Nombres Bordeaux* **18** (2006), 203–221.
- [35] KRITZER. P.—LARCHER, G.—PILLICHSHAMMER, F.: *A thorough analysis of the discrepancy of shifted Hammersley and van der Corput point sets*, *Ann. Mat. Pura Appl.* **186** (2007), 229–250.
- [36] KUIPERS, L.—NIEDERREITER, H.: *Uniform Distribution of Sequences*. Wiley, New York, 1974.
- [37] LARCHER, G.: *On the star-discrepancy of sequences in the unit-interval*, *J. Complexity* **31** (2015), 474–485.
- [38] ——— *On the discrepancy of sequences in the unit-interval*, *Indag. Math. (N.S.)* **27** (2016), 546–558.
- [39] LARCHER, G.—PUCHHAMMER, F.: *An improved bound for the star discrepancy of sequences in the unit interval*, *Unif. Distrib. Theory* **11** (2016), 1–14.
- [40] ——— *Sums of distances to the nearest integer and the discrepancy of digital nets*, *Acta Arith.* **106.4** (2003), 379–408.
- [41] MATOUŠEK, J.: *On the L_2 -discrepancy for anchored boxes*, *J. Complexity* **14** (1998), 527–556.
- [42] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, 1992.
- [43] OSTROMOUKHOV, V.: *Recent progress in improvement of extreme discrepancy and star discrepancy of one-dimensional sequences*. In: *Monte Carlo and Quasi-Monte Carlo Methods 2008* (L’Ecuyer, P. and A. B. Owen, eds.), Springer-Verlag, Berlin, 2009, 561–572.
- [44] OSTROWSKI, A.: *Bemerkungen zur Theorie der Diophantischen Approximationen I, II, III*, *Abh. Math. Sem. Hamburg* **1** (1922), no. 1, 77–98, 249–250; **4** (1925), no. 1, 224.
- [45] PROINOV, P. D.: *Estimation of L^2 -discrepancy of a class of infinite sequences*, *C.R. Acad. Bulgare Sci.* **36** (1983), 37–40.
- [46] ——— *On irregularities of distribution*. *C.R. Acad Bulgare Sci.* **39** (1986), 31–34.
- [47] PROINOV, P. D.—ATANASSOV, E.Ÿ.: *On the distribution of the van der Corput generalized sequence*, *C.R. Acad. Sci. Paris Sér. I Math.* **307** (1988), 895–900.
- [48] PROINOV, P. D.—GROZDANOV, V. S.: *On the diaphony of the van der Corput-Halton sequence*, *J. Number Theory* **30** (1988), 94–104.
- [49] PAUSINGER, F.: *Weak multipliers for generalized van der Corput sequences*, *J. Théor. Nombres Bordeaux* **24** (2012), no. 3, 729–749.
- [50] PAUSINGER, F.—SCHMID, W. CH. : *A good permutation for one-dimensional diaphony*, *Monte Carlo Methods Appl.* **16** (2010), 307–322.
- [51] F. PAUSINGER — A. TOPUZOĞLU: *On the discrepancy of two families of permuted van der Corput sequences*, *Unif. Distrib. Theory* **13** (2018), 47–64.
- [52] PILLICHSHAMMER, F.: *On the discrepancy of $(0, 1)$ -sequences*, *J. Number Theory* **104** (2004), 301–314.
- [53] RAMSHAW, L.: *On the discrepancy of the sequence formed by the multiples of an irrational number*, *J. Number Theory* **30** (1981), 138–175.
- [54] ROTH, K. F.: *On irregularities of distribution*, *Mathematika* **1** (1954), 73–79.
- [55] SCHMIDT, W. M.: *Irregularities of distribution VII*, *Acta Arith.* **21** (1972), 45–50.
- [56] TOPUZOĞLU, A.: *The Carlitz rank of permutations of finite fields: a survey*, *J. Symb. Comput.* **64** (2014), 53–66.

- [57] VAN DER CORPUT, J. G.: *Verteilungsfunktionen. I*, Proc. Kon. Ned. Akad. v. Wetensch. **38** (1935), 813–821.
- [58] ——— *Verteilungsfunktionen. II*, Proc. Kon. Ned. Akad. v. Wetensch. **38** (1935), 1058–1066.
- [59] WEYL, H.: *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. **77** (1916), 313–352.
- [60] XIAO, Y. J.: *Suites équiréparties associées aux automorphismes du tore*. C.R. Acad. Sci. Paris Sér. I Math. **311** (1990), 579–582.
- [61] ZAREMBA, S. K.: *La méthode des bons treillis pour le calcul des intégrals multiples*. In: Proc. Sympos. Univ. Montréal, September 9–14, 1971, *Applications of Number Theory to Numerical Analysis* (S.K. Zaremba, ed.), Academic Press, New York (1972), pp. 39–119.
- [62] ZINTERHOF, P.: *Über einige Abschätzungen bei der Approximation von Funktionen mit Gleichverteilungsmethoden*, Österr. Akad. Wiss. SB II **185** (1976), 121–132.

Received June 20, 2018

Accepted July 27, 2018

Florian Pausinger

School of Mathematics & Physics

Queen's University Belfast

BT7 1NN, Belfast

UNITED KINGDOM

E-mail: f.pausinger@qub.ac.uk