JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Florian PAUSINGER

Weak multipliers for generalized van der Corput sequences

Tome 24, n° 3 (2012), p. 729-749.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_3_729_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 729-749

Weak multipliers for generalized van der Corput sequences

par Florian PAUSINGER

Résumé. Les suites de Van der Corput généralisées sont des suites unidimensionnelles et infinies dans l'intervalle de l'unité. Elles sont générées par permutations des entiers de la base b et sont les éléments constitutifs des suites multi-dimensionnelles de Halton. Suites aux progrès récents d'Atanassov concernant le comportement de distribution uniforme des suites de Halton nous nous intéressons aux permutations de la formule $P(i) = ai \pmod b$ pour les entiers premiers entre eux a et b. Dans cet article nous identifions des multiplicateurs a générant des suites de Van der Corput ayant une mauvaise distribution. Nous donnons les bornes inférieures explicites pour cette distribution asymptotique associée à ces suites et relions ces dernières aux suites générées par permutation d'identité, qui sont, selon Faure, les moins bien distribuées des suites généralisées de Van der Corput dans une base donnée.

Abstract. Generalized van der Corput sequences are onedimensional, infinite sequences in the unit interval. They are generated from permutations in integer base b and are the building blocks of the multi-dimensional Halton sequences. Motivated by recent progress of Atanassov on the uniform distribution behavior of Halton sequences, we study, among others, permutations of the form $P(i) = ai \pmod b$ for coprime integers a and b. We show that multipliers a that either divide $b-1$ or $b+1$ generate van der Corput sequences with weak distribution properties. We give explicit lower bounds for the asymptotic distribution behavior of these sequences and relate them to sequences generated from the identity permutation in smaller bases, which are, due to Faure, the weakest distributed generalized van der Corput sequences.

Manuscrit reçu le 12 février 2012, révisé le 25 avril 2012.
This work is supported by the Graduate School of IST Austria (Institute of Science and Technology Austria).
Mots clefs. Uniform distribution, diaphony, generalized van der Corput sequence.
Classification math. 11K06, 11K38.

1. Introduction

The study of distribution properties of one-dimensional sequences is of great theoretical and practical importance, since it contributes to a better understanding of irregularities of distribution in multi-dimensional settings. Generalized van der Corput sequences are well known examples of low discrepancy sequences and have been extensively studied over the last 30 years. They are generated from permutations in integer base b and give rise to multi-dimensional generalized Halton sequences. Recent progress in the analysis of Halton sequences due to Atanassov [2], see also [16], and Atanassov and Durchova [3] is the reason why we are interested in linear permutations of the form $P(i) = ai \pmod b$ for coprime integers a and b.

In a recent study, Faure and Lemieux [12] suggest a construction for Halton sequences different from the one of Atanassov, which is also based on linear permutations. This construction, as they show, outperforms classical Monte Carlo integration in many practical settings. It is based on an earlier work of Faure [11], in which he gives a computational classification of multipliers a and observes that multipliers $a = 1$ or $a = b - 1$ give weak results. For an overview of related computational results of various authors we refer to the concluding section of [11].

In the present paper, we take a closer look at these observations and develop the theory of Faure [5, 7] further. Based on a new formula (Theorem 4.1) we apply known methods to determine the explicit asymptotic distribution behavior of generalized van der Corput sequences that are generated from a class of linear and linear-like (see definition in Section 2.4) permutations (Theorem 5.1). We relate our results to an earlier result of Faure, in which he shows that the original van der Corput sequences (generated from the identity permutations), are the weakest distributed sequences within the van der Corput family. His result shows that the asymptotic low-discrepancy constants of these sequences diverge with increasing base. We say a set of permutations with this behavior is not distribution preserving. Our main result implies that linear permutations in base b with a multiplier that either divides $b + 1$ or $b - 1$ behave asymptotically similar to original van der Corput sequences in smaller bases, which means that their asymptotic distribution properties get weaker as the base increases. This contrasts an earlier result of Faure [8], in which he gives an algorithm that defines permutations in every base b that behave asymptotically similar to the original van der Corput sequence in base 2.

Our results have several interesting aspects. First, we establish a new framework for the exact analysis of the asymptotic distribution behavior of generalized van der Corput sequences, which is easy to implement on the computer. Second, we apply this framework to special cases and reveal intrinsic distribution properties of certain classes of van der Corput

sequences. Indeed, our results are independent of any particular choice of an irregularity measure. Third, our computational results lead to suggestions of how to narrow the search for permutations with good distribution behavior in high bases (for b larger than 100). Fourth, our results give rise to several number theoretical questions.

Outline. In Section 2, we review the basic concepts of uniform distribution theory and define distribution preserving sets of generating permutations. In Section 3, we review the classical analysis of the diaphony of generalized van der Corput sequences due to Faure. Our results are based on a new variation of a formula for computing the diaphony (Theorem 4.1), which we derive in Section 4. In Section 5, we prove criteria for identifying multipliers that lead to sequences with weak distribution properties and give asymptotic lower bounds for their distribution behavior. In Section 6, we outline future directions and open questions. Furthermore, we provide an appendix with additional computations upon request (*florian.pausinger@ist.ac.at*).

Notation. For an arbitrary, positive integer b, we denote permutations of $\mathbb{Z}_b$ either with P or the small greek letters π and σ. The identity permutation in base b is denoted by id_b or id, and the set of all permutations of $\mathbb{Z}_b$ is denoted by $\mathfrak{S}_b$. If we write $\sigma = (0, 4, 2, 6, 1, 5, 3, 7)$, we mean that $\sigma(0) = 0, \sigma(1) = 4, \sigma(2) = 2, \ldots$. If we restrict ourselves to prime bases, we write p instead of b. We reserve the capital letter X for infinite real sequences of points in $[0, 1[$, and use letters $\mathcal{J}, \mathcal{P}$ in the calligraphic font for sets, whereas I, J denote intervals. Furthermore, log always means the natural logarithm and for $i, j \in \mathbb{Z}$, $j \oplus i := j + i \pmod b$.

2. Basic concepts

In this section, we provide the necessary background for our results. We introduce the main concepts of uniform distribution theory and define generalized van der Corput sequences as well as the class of permutations we study in the remainder of this paper.

2.1. Discrepancy theory. Let $\mathrm{I} = [0, 1[$ be the half open unit interval and let $\mathrm{J} \subset \mathrm{I}$. For an infinite sequence $X = (x_i)_{i \geq 1}$ in I and for $N \geq 1$, let $A(\mathrm{J}, N, X)$ denote the number of indices $i \leq N$ for which $x_i \in \mathrm{J}$. Let $E(\mathrm{J}, N, X) := A(\mathrm{J}, N, X) - l(\mathrm{J})N$ denote the *discrepancy function*, in which we write $l(\mathrm{J})$ for the length of the interval. Then the *star discrepancy*, $D_N^*(X)$, and the *extreme discrepancy*, $D_N(X)$, of the first N points of X are defined by

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

Moreover, we define the *diaphony* $F_N(X)$ of the first N points of X by

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

With this definition we follow [9], for the classical definition of the diaphony in terms of exponential sums see Zinterhof [17].

We call a sequence X *uniformly distributed* if $\frac{D_N(X)}{N} \overset{N\to\infty}{\longrightarrow} 0$ and say it is a *low discrepancy (diaphony) sequence* if there exist constants K such that for all N

$$D_N^*(X),\ D_N(X),\ F_N^2(X) < K \log N.$$

As a consequence, computing the asymptotic values

$$\begin{aligned} t^*(X) &:= \limsup_{N\to\infty}(D_N^*(X)/\log N),\\ t(X) &:= \limsup_{N\to\infty}(D_N(X)/\log N),\\ f(X) &:= \limsup_{N\to\infty}(F_N^2(X)/\log N), \end{aligned}$$

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

In [6] it is shown that the different measures of irregularity of distribution of sequences can be bounded by each other. In the one-dimensional case, we have

$$D_N^*(X) \le D_N(X) \le 2D_N^*(X), \tag{2.1}$$

$$\frac{\pi^2}{3} D_N^3(X) \le F_N^2(X) \le 11 D_N(X). \tag{2.2}$$

2.2. Generalized van der Corput sequences. In this paper, we study well known examples of one-dimensional low discrepancy sequences.

Definition. For a fixed base $b \ge 2$ and a permutation $\sigma \in \mathfrak{S}_b$, the *generalized van der Corput sequence*, S_b^σ, 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 the integer $n \ge 1$.

Remark 1. For more general definitions using sequences of permutations, we refer to [5]. Van der Corput considered the sequence that is generated from the identity permutation in base 2. However, sequences that are generated from the identity permutations in arbitrary bases are usually referred to as *original van der Corput sequences*.

Faure was able to compute the exact asymptotic discrepancy values for the original van der Corput sequences in [5, 7]:

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

$$f(S_b^{id}) = \begin{cases} \pi^2 \frac{b^4+2b^2-3}{48b^2\log b} & \text{if } b \text{ is odd,} \\ \pi^2 \frac{b^3+b^2+4}{48(b+1)\log b} & \text{if } b \text{ is even.} \end{cases}$$

In 2005, he proved that the original van der Corput sequences show the worst distribution behavior in the class of all generalized van der Corput sequences in a certain base b, [10]. It follows that the above relations give upper bounds for the discrepancy values of any sequence in base b. On the other hand, speaking of sequences with very good distribution behavior, the smallest known asymptotic values within the family of generalized van der Corput sequences given in [5, 7, 8] have recently been improved by Ostromoukhov [13] to $t^*(S_{60}^{\sigma}) = 0.222223\ldots$ and $t(S_{84}^{\sigma}) = 0.353494\ldots$ and by Schmid and the author [14] to $f(S_{57}^{\sigma}) = 1.13794\ldots$.

2.3. Distribution preserving sets of permutations. The results of the previous section show that even if every generalized van der Corput sequence is a low diaphony sequence, its diaphony constant may depend on the base b. Therefore we introduce the following optimality criterion for countable sets of permutations.

Definition. Let $\mathcal{J} \subset \mathbb{N}$ be a countable set of integers and let $\mathcal{P}$ be a countable set of permutations that contains one permutation $\sigma \in \mathfrak{S}_b$ for every $b \in \mathcal{J}$. The set $\mathcal{P}$ is *distribution preserving* if there exists a constant $K > 0$ such that $f(S_b^{\sigma}) < K$ for all $\sigma \in \mathcal{P}$.

Example. The set of identity permutations is not distribution preserving, since for every $K > 0$, we can find a b such that $f(S_b^{id}) > K$. In [8], Faure defined an algorithm and showed that for every permutation σ computed with this algorithm $t(S_b^{\sigma}) < 1/\log 2$. Note that via Inequality (2.2), we can immediately conclude that $f(S_b^{\sigma}) < 11/\log 2$. Hence, this set is an example of a distribution preserving set of permutations.

2.4. Linear-like permutations. In order to study linear permutations, which are of the form $P(i) = ai \pmod p$, it is convenient to define the wider class of *linear-like permutations*. Let p be prime, $1 \le a \le p-1$, and define the ordered tuples

$$A_s := (s + ai : 0 \le s + ai < p, i \in \mathbb{N}),$$

for $0 \le s < a$. Note that these tuples are pairwise disjoint and their union covers the entire interval of integers from 0 to $p-1$. Let $\pi \in \mathfrak{S}_a$. Writing the ordered tuples in sequence, we get a permutation in base p, namely

$$P(p, a, \pi) := (A_{\pi(0)}, \ldots, A_{\pi(a-1)}).$$

Example. Let $p = 17$, $a = 4$, then $A_0 = (0, 4, 8, 12, 16)$, $A_1 = (1, 5, 9, 13)$, $A_2 = (2, 6, 10, 14)$, $A_3 = (3, 7, 11, 15)$, and

$$\begin{aligned} P(17, 4, id_4) &= (A_0, A_1, A_2, A_3) \\ &= (0, 4, 8, 12, 16, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15). \end{aligned}$$

This class includes all linear permutations in prime base p:

Proposition 2.1. *Let $p = am + x$ be prime with $1 \leq a \leq p - 1$ and $m := \lfloor p/a \rfloor$. For a permutation $P \in \mathfrak{S}_p$ the following is equivalent: (i) P is linear, with $P(i) = ai \pmod p$, and (ii) $P = P(p, a, \pi)$ with $\pi(i) = x_a i \pmod a$ and $x_a = a - x$.*

Proof. $(i) \Rightarrow (ii)$: Let $P(i) = ai \pmod p$. Since $P(i)+a \equiv P(i+1) \pmod p$ for all i, P can be written in terms of the tuples A_s. The order π of these tuples is given by

$$\max A_{\pi(s)} + a \equiv \min A_{\pi(s+1)} \pmod p.$$

We have to show that $\pi(s) + x_a \equiv \pi(s + 1) \pmod a$. Let $\pi(s + 1) > \pi(s)$. Then $\max A_{\pi(s)} = \pi(s) + am$ and $\pi(s + 1) - \pi(s) \equiv am + a \equiv p + x_a \equiv x_a \pmod p$ and hence $\pi(s) + x_a \equiv \pi(s + 1) \pmod a$. Let $\pi(s + 1) < \pi(s)$. Then $\pi(s) > x$ and $\max A_{\pi(s)} = \pi(s) + a(m - 1)$, such that $\pi(s + 1) \equiv \pi(s) + am \equiv \pi(s) - x \pmod p$ and hence $\pi(s + 1) \equiv \pi(s) - x \equiv \pi(s) + x_a \pmod a$.

$(ii) \Rightarrow (i)$: In this case we have to show that $\max A_{\pi(s)} + a \equiv \min A_{\pi(s+1)} \pmod p$ for $\pi(s) \equiv x_a s \pmod a$. With the distinction $\pi(s) < x$ and $\pi(s) > x$ this follows analogously. □

Note that if we are interested in the one-dimensional distribution properties of permutations $P(i) = a_0 i + a_1 \pmod p$, it suffices to understand the linear permutations $P(i) = P(a, i) = ai \pmod p$. Due to [5, Théorème 4.4], we can set $a_1 = 0$ without loss of generality. Moreover, due to [15, Corollary 3], we can exploit the symmetry of these permutations to restrict this class further. Therefore, it is enough to study permutations for $1 \leq a \leq (p - 1)/2$ since for $\bar{a} := p - a$ we have that $P(a, i) = p - P(\bar{a}, i)$, which implies that the sequences generated from these permutations have the same one-dimensional distribution behavior.

3. Classical analysis of diaphony

In this section, we recall important definitions and results of Faure. The analysis of the diaphony of S_b^σ is based on the following functions introduced and explained in [7].

Definition. For $\sigma \in \mathfrak{S}_b$, let $\mathcal{Z}_b^\sigma := (\sigma(0)/b, \sigma(1)/b, \ldots, \sigma(b - 1)/b)$. For $h \in \{0, 1, \ldots, b - 1\}$ and $x \in \left[\frac{k-1}{b}, \frac{k}{b}\right[$, where $1 \leq k \leq b$ is an integer, we

define

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

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 $h \in \{0,\dots,b-1\}$. In [5] Chaix and Faure introduced a new class of functions based on $\varphi_{b,h}^{\sigma}$:

Definition.

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

Furthermore, they showed that the diaphony of S_b^{σ} can be computed exactly using such functions and they developed a technique to obtain asymptotic values as well.

Theorem 3.1 (Théorème 4.2 in [5])**.** *For all $N \ge 1$, we have*

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

Theorem 3.2 (Théorème 4.10 in [5])**.** *Let*

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

then

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

These two theorems are the starting point of our work. The method of Faure allows an exact investigation of van der Corput sequences that are generated from arbitrary permutations. However, the separate analysis of single permutations can be tedious. Therefore, we aim to exploit the structure of whole sets of permutations to understand the distribution behavior of the corresponding sequences altogether. This requires a new representation of χ_b^{σ}-functions, which we introduce in the following section.

4. Formula in terms of difference vectors

In this section, we derive our first main result. We state a formula for the computation of χ_b^{σ} in Section 4.1 and prove it in Section 4.2. Note that, even if a big part of this paper is concerned with the study of prime bases, this formula holds for arbitrary integer bases $b \in \mathbb{N}$.

4.1. Difference vectors and statement of formula. In [5, Propriété 3.3 and Propriété 3.5], it was shown that the basic χ_b^σ-functions are continuous and piecewise quadratic on the intervals $[(k-1)/b, k/b]$, and $\chi_b^\sigma(0) = \chi_b^\sigma(1)$. Moreover,

$$\chi_b^\sigma(x) = \frac{b^2(b^2-1)}{12}x^2 + Ax + B, \tag{4.1}$$

in each interval $\left[\frac{k-1}{b}, \frac{k}{b}\right]$ $(1 \le k \le b)$, where A and B depend only on σ and k. Therefore, the set $\{\chi_b^\sigma(k/b) : 1 \le k \le b\}$ determines the function fully.

To derive a formula for $\chi_b^\sigma(k/b)$, we consider the set $\{\sigma(i) : 0 \le i \le k-1\}$ of the first k elements of the permutation σ. We order this set and denote the ordered vector by $Z_k^\sigma = (z_0, \dots, z_{k-1})$. For each Z_k^σ, we define the *k-th difference vector* $D_k^\sigma := (d_1, \dots, d_k)$ such that $d_{h+1} := z_{h+1} - z_h - 1$, for $0 \le h \le k-1$, where $z_k := b + z_0$. Note that since the elements of Z_k^σ are increasing, we always get non-negative differences. Furthermore, the indices of elements of difference vectors are always modulo k. The elements of D_k^σ represent the number of consecutive values of $\mathbb{Z}_b$ that are missing between two elements of Z_k^σ.

Example. For $\pi = P(17, 4, id)$ we have $Z_5^\pi = (0, 4, 8, 12, 16)$ and $Z_8^\pi = (0, 1, 4, 5, 8, 9, 12, 16)$, such that $D_5^\pi = (3, 3, 3, 3, 0)$ and $D_8^\pi = (0, 2, 0, 2, 0, 2, 3, 0)$.

Example. For every identity permutation and for $1 \le k \le b$, we get $D_k^{id_b} = (d_1, \dots, d_k)$ with $d_k = b - k$ and $d_h = 0$ for $h \ne k$.

Now, we are ready to state our formula for χ_b^σ in terms of difference vectors:

Theorem 4.1. *Let $b \in \mathbb{N}$. For all $\sigma \in \mathfrak{S}_b$ and all integers $1 \le k \le b$, let $D_k^\sigma = (d_1, \dots, d_k)$ be the k-th difference vector of σ. Then*

$$\chi_b^\sigma(k/b) = \frac{1}{2}\left(S_1(D_k^\sigma) + S_2(D_k^\sigma) - \frac{1}{6}(b-k)k(2bk - 2k^2 + 3k - 2)\right),$$

in which $S_1(D_1^\sigma) = 0$ and

$$S_1(D_k^\sigma) = \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 d_{h\oplus i} \quad \text{and} \quad S_2(D_k^\sigma) = \frac{k^2}{2}\sum_{h=1}^{k}(d_h+1)d_h.$$

Before we prove this formula in the following subsection, we state a corollary that was already found in [5, Propriété 3.5,(ii)].

Corollary 4.1. *For arbitrary b and σ,*

$$\chi_b^\sigma(1/b) = \chi_b^\sigma((b-1)/b) = (b^2-1)/12.$$

4.2. Derivation of formula. Throughout this section, we write $l(h,h') = d$ instead of $l([\frac{h}{b},\frac{h'}{b}[) = \frac{d}{b}$ for the length of these intervals. Moreover,

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

In [10], Faure proved that

$$\chi_b^\sigma(k/b) = \frac{1}{2}\sum_{h\neq h'}(\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2 = \frac{1}{2}\sum_{d=1}^{b-1}\left(\sum_{l(h,h')=d}(\delta_{h,h'}^\sigma)^2 - \frac{d^2k^2}{b}\right). \tag{4.2}$$

One crucial observation in the proof is that $\sum_{l(h,h')=d}\delta_{h,h'}^\sigma = kd$ for all k and all d. Formula (4.2) motivates to take a systematic look at the values $(\delta_{h,h'}^\sigma)^2$ (see also [15]). We can visualize the summands $\delta_{h,h'}^\sigma$ in a $(b-1)\times b$ matrix $M_k^\sigma = (m_{d,h})$, in which $m_{d,h} = \delta_{h,h\oplus d}^\sigma$. This means that $m_{d,h}$ represents the number of the first k elements of σ that lie in the interval $[h, h\oplus d[$, (we think of [0,1[as a torus).

$$\begin{array}{c} \\ 1 \\ . \\ . \\ d \\ . \\ . \\ b-1 \end{array}\begin{array}{c} \begin{array}{ccccccc} 0 & . & . & h & . & . & b-1 \end{array} \\ \left(\begin{array}{ccccccc} \delta_{0,1}^\sigma & . & . & . & . & . & \delta_{b-1,0}^\sigma \\ . & . & & & & . & . \\ . & & . & & . & & . \\ . & & & \delta_{h,h\oplus d}^\sigma & & & . \\ . & & . & & . & & . \\ . & . & & & & . & . \\ \delta_{0,b-1}^\sigma & . & . & . & . & . & \delta_{b-1,b-2}^\sigma \end{array}\right) \end{array}\begin{array}{l} \\ \sum_{row} = k \\ . \\ . \\ \sum_{row} = dk \\ . \\ . \\ \sum_{row} = (b-1)k \end{array}$$

Let

$$N(M_k^\sigma) := \sum_{d=1}^{b-1}\sum_{h=0}^{b-1}(m_{d,h})^2,$$

then we can rewrite Formula (4.2) as

$$\chi_b^\sigma(k/b) = \frac{1}{2}\left(N\left(M_k^\sigma\right) - \sum_{d=1}^{b-1}\frac{d^2k^2}{b}\right), \tag{4.3}$$

and we see that it suffices to study $N(M_k^\sigma)$ for $1 \le k \le b$.

Note that each of the k points contribute a triangle of 1's of the following form to the matrix:

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

This can be seen from 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. Hence, every matrix M_k^σ can be seen as a sum of k such triangles. For each $Z_k^\sigma = (z_0, \dots, z_{k-1})$ there exists such a matrix. In that way, each permutation generates a sequence $(M_k^\sigma)_{k=1}^b$ of matrices (see example below).

To derive the formula, we consider the blocks of $d_h + 1$ consecutive columns between the elements z_{h-1} and z_h of Z_k^σ separately. For $z_h \in Z_k^\sigma$ let us pick column $j = z_h$ of M_k^σ. Note that this column contains the number of points in the intervals of the form $[j/b, (j \oplus d)/b]$ with $1 \le d \le b-1$ and since $j = z_h$ all these intervals contain at least one point. The first interval with two points is at row $d = (d_{h\oplus 1} + 1) + 1$, the first interval with three points is at row $d = (d_{h\oplus 1} + 1) + (d_{h\oplus 2} + 1) + 1$ and, in the general case, the first interval with $2 \le m \le k$ points is at row $d = m + \sum_{l=1}^{m-1} d_{h\oplus l}$. We can therefore write the sum of squares of elements of any column $j = z_h$ for $k = 1$ as $\sum_{d=1}^{b-1} m_{d,j}^2 = 1^2 \cdot d_1 = b - 1$ and for $k \ge 2$ as

$$\sum_{d=1}^{b-1} m_{d,j}^2 = \sum_{i=1}^{k-1} i^2 (1 + d_{h\oplus i}) + k^2 d_h.$$

For an arbitrary column j with $z_{h-1} < j < z_h$, let $x = z_h - j$. Due to the triangle structure, we see that this column is a shifted version of column z_h. The difference is that x many 0's are inserted on top and in return x many k's are deleted on the bottom. Therefore, for $k \ge 2$, these columns contain the same number of values $1, \dots, k-1$ as column z_h, so that we can sum the squares of elements of the $z_h - z_{h-1} = d_h + 1$ many columns as follows:

$$\sum_{j=1+z_{h-1}}^{z_h} \sum_{d=1}^{b-1} m_{d,j}^2 = (d_h + 1) \sum_{i=1}^{k-1} i^2 (1 + d_{h\oplus i}) + \frac{(d_h+1) d_h}{2} k^2.$$

For $k = 1$ we get $\sum_{j=0}^{b-1} \sum_{d=1}^{b-1} m_{d,j}^2 = 1^2 \cdot (d_1 + 1) d_1 / 2$.

Example. Let $b = 7$ with $\sigma = (0, 3, 1, 6, 5, 4, 2)$. For $k = 2$, we get $Z_2^\sigma = (z_0, z_1) = (0, 3)$ and $D_2^\sigma = (d_1, d_2) = (2, 3)$, and for $k = 4$, we have $Z_4^\sigma = (z_0, z_1, z_2, z_3) = (0, 1, 3, 6)$ and $D_4^\sigma = (d_1, d_2, d_3, d_4) = (0, 1, 2, 0)$. Then

$$M_2^\sigma = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 2 & 1 & 1 & 2 \\ 2 & 1 & 2 & 2 & 1 & 2 & 2 \end{pmatrix}, \quad M_4^\sigma = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 1 & 1 & 2 & 3 \\ 3 & 2 & 1 & 2 & 2 & 3 & 3 \\ 3 & 2 & 2 & 3 & 3 & 3 & 4 \\ 3 & 3 & 3 & 4 & 3 & 4 & 4 \end{pmatrix}.$$

For $k = 2$ and M_2^σ, we get by inspection $N(M_2^\sigma) = 24 \cdot 1^2 + 9 \cdot 2^2 = 60$ and by the above formulas:

$$\sum_{j=1+z_0}^{z_1} \sum_{d=1}^{b-1} m_{d,j}^2 = (d_1+1)1^2(1+d_2) + 2^2 \frac{(d_1+1)d_1}{2} = 12 + 12 = 24,$$
$$\sum_{j=1+z_1}^{b} \sum_{d=1}^{b-1} m_{d,j}^2 = (d_2+1)1^2(1+d_1) + 2^2 \frac{(d_2+1)d_2}{2} = 12 + 24 = 36.$$

Finally, we take the sum over all $k \geq 2$ such blocks of columns to get the desired formula for $N(M_k^\sigma)$:

$$\begin{aligned} N(M_k^\sigma) &= \sum_{h=1}^{k} \left((d_h+1) \sum_{i=1}^{k-1} i^2 (1 + d_{h\oplus i}) + \frac{(d_h+1)d_h}{2} k^2 \right) \\ &= \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 (1 + d_{h\oplus i}) + \sum_{h=1}^{k} \sum_{i=1}^{k-1} i^2 (1 + d_{h\oplus i}) + \frac{k^2}{2} \sum_{h=1}^{k} (d_h+1)d_h \\ &= \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 + \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 d_{h\oplus i} + R_2(b,k) + S_2(D_k^\sigma) \\ &= R_1(b,k) + S_1(D_k^\sigma) + R_2(b,k) + S_2(D_k^\sigma), \end{aligned}$$

where $S_1(D_k^\sigma) = \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 d_{h\oplus i}$ and $S_2(D_k^\sigma) = \frac{k^2}{2} \sum_{h=1}^{k} (d_h+1)d_h$. The sums R_1 and R_2 can be computed without taking any specific structure of difference vectors into account. We only need $\sum_{h=1}^{k} d_h = b - k$:

$$\begin{aligned} R_1(b,k) &= \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 = 1/6(k-1)k(2k-1) \sum_{h=1}^{k} d_h \\ &= 1/6\,(k-1)k(2k-1)(b-k), \\ R_2(b,k) &= \sum_{h=1}^{k} \sum_{i=1}^{k-1} i^2 (1 + d_{h\oplus i}) = \sum_{h=1}^{k} \left(\sum_{i=1}^{k-1} i^2 + \sum_{i=1}^{k-1} i^2 d_{h\oplus i} \right) \\ &= \sum_{h=1}^{k} \sum_{i=1}^{k-1} i^2 + \sum_{h=1}^{k} \sum_{i=1}^{k-1} i^2 d_{h\oplus i} = k \sum_{i=1}^{k-1} i^2 + (b-k) \sum_{i=1}^{k-1} i^2 \\ &= 1/6\,b(k-1)k(2k-1). \end{aligned}$$

For the special case $k = 1$, we get $N(M_k^\sigma) = (d_1+1)d_1/2 = S_2(D_1^\sigma)$.

If we plug the above into Equation (4.3) we obtain Theorem 4.1. This formula reveals the crucial dependence of the matrices on the structure of the difference vectors.

5. Linear-like permutations that are not distribution preserving

In this section we present our second main result. We show for different sets of linear-like permutations that they are not distribution preserving. We use these results in two different ways:

- First, we can explicitly determine the asymptotic diaphony constants for every linear permutation with multiplier a that either divides $(p+1)$ or $(p-1)$.
- Second, we get an estimate how likely we pick a weak multiplier, if we randomly pick a multiplier in a given (high) base.

In the following we consider permutations of the form

$$P(am+x, a, id_a) \text{ and } P(am+x, a, revid_a)$$

for prime bases $p = am + x$, with $m := \lfloor p/a \rfloor$ and

$$revid_a := (0, a-1, a-2, \ldots, 1).$$

Recall from Proposition 2.1 that for $p = am + 1$ we get $x_a = a - 1$ thus

$$P(am+1, a, revid_a)$$

is linear. Moreover, for $p = am + a - 1$, we get $x_a = 1$ and hence

$$P(am+a-1, a, id_a)$$

is also linear (see Figure 5.1).

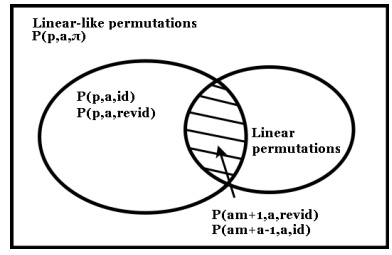

FIGURE 5.1. Relations between the different classes of permutations.

First we study the difference vectors of these permutations in Section 5.1 and 5.2. Then, in Section 5.3, we prove lower bounds for their asymptotic diaphony values, before we conclude our considerations with two examples in Section 5.4.

5.1. General structure of difference vectors. Before we apply Theorem 4.1 to permutations of the form

$$\sigma_1 = P(am+x, a, id_a) \text{ and } \sigma_2 = P(am+x, a, revid_a),$$

we distinguish three different cases of difference vectors.

• First, we consider the a special difference vectors generated by the ordered sets $\mathcal{Z}_l := \left\{ z : z \in \bigcup_{s=0}^{l-1} A_{\pi(s)} \right\}$, and we denote their cardinality, which is also the length of the corresponding difference vector, by k_l. Note that for $i > j$, A_i can be obtained from A_j by adding $i - j$ to each element and deleting the last element if it is greater than p. Therefore, we can state a general formula for $D_{k_l}^{\sigma_1} = (d_1, \ldots, d_{k_l})$ and $1 \le h \le k_l$

$$d_h = \begin{cases} \max\{0, x - l\}, & \text{if } h = k_l, \\ a - l, & \text{if } h \equiv 0 \pmod{l} \text{ and } h \neq k_l, \\ 0, & \text{if } h \not\equiv 0 \pmod{l} \text{ and } h \neq k_l. \end{cases}$$

This shows that the difference vectors contain m elements $(a - l)$ and possibly an additional nonzero element $(x - l)$.

We get similar difference vectors $D_{k_l}^{\sigma_2} = (d_1, \ldots, d_{k_l})$

$$d_h = \begin{cases} \min\{x - 1, a - l\}, & \text{if } h = k_l, \\ a - l, & \text{if } h \equiv 1 \pmod{l} \text{ and } h \neq k_l, \\ 0, & \text{if } h \not\equiv 1 \pmod{l} \text{ and } h \neq k_l. \end{cases}$$

Here we have m elements $(a-l)$ and possibly an additional nonzero element $\min\{x - 1, a - l\}$ in the difference vectors.

• Second, we consider difference vectors for arbitrary k, with $k_l < k < k_{l+1}$ and $1 \le l \le a - 1$. Note that if we add elements of $A_{\pi(l)}$ to $\mathcal{Z}_l$ these elements are increasing and therefore change the differences in $D_{k_l}^{\sigma_1}$ one after the other. For each element we insert, we add a 0 to the new difference vector and decrease an existing nonzero element by 1. Let $\Delta = k - k_l$, then for $D_k^{\sigma_1} = (d_1, \ldots, d_k)$ we get

$$d_h = \begin{cases} D_{k_l}^{\sigma_1}(h + \Delta), & \text{if } h > \Delta \cdot (l + 1), \\ a - l - 1, & \text{if } h \equiv 0 \pmod{l + 1}, h \le \Delta \cdot (l + 1), \\ 0, & \text{if } h \not\equiv 0 \pmod{l + 1}, h \le \Delta \cdot (l + 1), \end{cases}$$

where $D_{k_l}^{\sigma_1}(h + \Delta)$ denotes the $(h + \Delta)$-th element of $D_{k_l}^{\sigma_1}$. We obtain $D_k^{\sigma_2}$ in a similar fashion.

• Finally, what remains is the case $1 \le k < k_1$. In this case we always have k nonzero elements in $D_k^{\sigma_1}$. Namely

$$d_h = \begin{cases} a - 1, & \text{if } h < k, \\ p - k - (k - 1)(a - 1), & \text{if } h = k. \end{cases}$$

These vectors are the same for σ_2.

Remark 2. With these general difference vectors it is possible to explicitly compute $N(M_k^\sigma)$ for any k and any permutation σ_1 or σ_2. We omit the general computation and restrict ourselves to the special cases when σ_i is linear, (see shaded area in Figure 5.1). The results carry over to the general

case without problem, however, the length of the computations increase significantly without any additional insights.

5.2. Special cases. In this section we consider the two special cases when σ_1 or σ_2 are linear.

5.2.1. ***The case*** $\boldsymbol{\sigma = P(am+a-1, a, id_a)}$**.** We distinguish three cases of difference vectors according to the previous section.

• First Case: For $p = am+a-1$, we have $x = a-1$, $\max\{0, x-l\} = a-1-l$ and $k_l = ml + l$ with $1 \le l < a$.

Thus, we always have $m+1$ nonzero elements in the difference vectors $D^\sigma_{k_l}$ and

$$\begin{aligned} S_2(D^\sigma_{k_l}) &= \frac{k_l^2}{2}\left(\sum_{h=1}^{k_l} d_h^2 + \sum_{h=1}^{k_l} d_h\right) \\ &= 1/2\ l^2(m+1)^2(a-l)(a(m+1) - l(m+1) + m - 1). \end{aligned}$$

Furthermore, for $y = 1, \dots, m$, with $d_{y\cdot l} = (a-l)$, we can write

$$\begin{aligned} d_{y\cdot l}\sum_{i=1}^{k_l-1} i^2 d_{yl\oplus i} = (a-l)\Bigg((a-l)\sum_{j=1}^{m-y}(jl)^2 + (a-l-1)((m-y+1)l)^2 \\ +(a-l)\sum_{j=1}^{y-1}((m-y+1)l + jl)^2\Bigg). \end{aligned}$$

For $d_{k_l} = (a-l-1)$ we get

$$d_{k_l}\sum_{i=1}^{k_l-1} i^2 d_{k_l\oplus i} = (a-l-1)(a-l)\sum_{j=1}^{m}(jl)^2.$$

Hence, if we combine the above formulas, we get

$$\begin{aligned} S_1(D^\sigma_{k_l}) &= \sum_{h=1}^{k_l} d_h \sum_{i=1}^{k_l-1} i^2 d_{h\oplus i} \\ &= 1/6\ l^2 m(m+1)(2m+1)(a-l)(a(m+1) - l(m+1) - 2). \end{aligned}$$

• Second Case: Now we compute the sums S_1 and S_2 for arbitrary difference vectors with $k_l < k < k_{l+1}$ and $1 \le l \le a-1$. Let $\Delta = k - k_l$. According to the general formula we have $(\Delta+1)$ nonzero differences with value $(a-l-1)$ and $(m-\Delta)$ differences with value $(a-l)$.

Therefore we get

$$\begin{aligned} S_2(D_k^\sigma) &= \frac{k^2}{2}\left(\sum_{h=1}^{k} d_h^2 + \sum_{h=1}^{k} d_h\right) \\ &= 1/2\ k^2(a-l)(m(a+l+1)+a-2k+l-1). \end{aligned}$$

In order to compute S_1 we have to distinguish the two different values of positive d_h more carefully. First, for $y = 1, \ldots, \Delta$, we have $d_{y\cdot(l+1)} = a-l-1$, such that

$$\begin{aligned} &d_{y\cdot(l+1)} \cdot \sum_{i=1}^{k-1} i^2 d_{y\cdot(l+1)\oplus i} = \\ &d_{y\cdot(l+1)}\left((a-l-1)\sum_{j=1}^{\Delta-y}(j(l+1))^2 + (a-l)\sum_{j=1}^{m-\Delta}((\Delta-y)(l+1)+jl)^2\right. \\ &\quad + (a-l-1)((\Delta-y)(l+1)+(m-\Delta+1)l)^2 \\ &\quad \left. + (a-l-1)\sum_{j=1}^{y-1}((\Delta-y)(l+1)+(m-\Delta+1)l+j(l+1))^2\right). \end{aligned}$$

Second, for $y = 1, \ldots, m-\Delta$, we have $d_{\Delta\cdot(l+1)+y\cdot l} = a-l$ such that:

$$\begin{aligned} &d_{\Delta\cdot(l+1)+y\cdot l}\sum_{i=1}^{k-1} i^2 d_{\Delta\cdot(l+1)+y\cdot l+i} = \\ &\quad (a-l)\left((a-l)\sum_{j=1}^{m-\Delta-y}(jl)^2 + (a-l-1)((m-\Delta-y+1)l)^2\right. \\ &\qquad + (a-l-1)\sum_{j=1}^{\Delta}((m-\Delta-y+1)l+j(l+1))^2 \\ &\qquad \left. + (a-l)\sum_{j=1}^{y-1}((m-\Delta-y+1)l+\Delta(l+1)+jl)^2\right). \end{aligned}$$

What remains is the difference $d_k = a-l-1$, for which we get

$$(a-l-1)\left((a-l-1)\sum_{j=1}^{\Delta}(j(l+1))^2 + (a-l)\sum_{j=1}^{m-\Delta}(\Delta(l+1)+jl)^2\right).$$

Thus, we considered all $(m+1)$ positive elements of the difference vectors and therefore all nonzero summands of $S_1(D_k^\sigma)$. The final expression we obtain for $S_1(D_k^\sigma)$ can be found in the appendix.

• Third case: For $2 \le k < k_1$, we compute the sums S_1 and S_2 in an analogous fashion:

$$S_2(D_k^\sigma) = \frac{k^2}{2}((k-1)(a-1)^2 + (a(2-k+m)-2)^2 + am + a - 1 - k)$$

Moreover,

$$\sum_{h=1}^{k} d_h d_{h\oplus i} = (k-2)(a-1)^2 + 2(a-1)(a(2-k+m)-2),$$

hence

$$\begin{aligned} S_1(D_k^\sigma) &= \sum_{i=1}^{k-1} i^2 \sum_{h=1}^{k} d_h d_{h\oplus i} \\ &= -\frac{1}{6}(a-1)(k-1)k(2k-1)(a(k-2(m+1))+k+2). \end{aligned}$$

• Summary: For given p and σ as well as any $1 \le k \le p$, we obtain a value for $\chi_p^\sigma(k/p)$ if we plug the according values for S_1 and S_2, which we have computed in this section, into the general formula of Theorem 4.1.

5.2.2. ***The case $\sigma = P(am+1, a, revid_a)$.*** For $p = am + 1$, we have $x = 1$, $\min\{x - 1, a - l\} = 0$ and $k_l = ml + 1$ for $1 \le l < a$. Note that the difference vectors are very similar to those of the last section. The only difference is that the nonzero elements are now followed by zeros, whereas before zeros were followed by nonzero elements. Again we distinguish three cases. If we follow the ideas of the previous section we can derive similar formulas for the sums S_1 and S_2 (see appendix) and thus, via Theorem 4.1, also for $\chi_p^\sigma(k/p)$.

5.3. Asymptotics of special cases. In this subsection we consider the asymptotic distribution behavior of the two special classes of linear-like permutations we have studied so far and bound their asymptotic diaphony values γ_p^σ (see Theorem 3.2) from below. For simplicity, we will not precisely prove for which k the according χ_p^σ-functions attain their maximum. We only guess the dominant intervals (see definition below) and compute lower bounds for the asymptotic diaphony values based on these guesses. However, note that our guesses are motivated by exhaustive computations and can therefore, without proof, be assumed to give the (almost) exact asymptotic diaphony values.

Definitions. In order to compute γ_p^σ we introduce supporting functions $g_{p,n}^\sigma : [0,1] \to \mathbb{R}$:

$$g_{p,n}^\sigma(x) = \frac{1}{n}\sum_{j=1}^{n} \chi_p^\sigma(xp^j).$$

$P(p,a,\pi)$				
p	a	m	π	Interval
$am+a-1$	even	even	id_a	$[k^*, k^*+1]$
	even	odd	id_a	$[k^*-1, k^*]$
	odd	odd	id_a	$[k^*-1, k^*]$
$am+1$	even	even	$revid_a$	$[k^*, k^*+1]$
	even	odd	$revid_a$	$[k^*, k^*+1]$
	odd	even	$revid_a$	$[k^*, k^*+1]$

TABLE 5.1. Dominant intervals for the different cases.

Following [5, 7] we examine intervals $\mathrm{I}_h^n := [h/p^n, (h+1)/p^n]$, with $h \in 0, \dots, p^n - 1$, for given $g_{p,n}^\sigma$. We call the interval I_h^n *dominated*, if there exists a set $\mathcal{J}$ of integers with $h \notin \mathcal{J}$ such that

$$g_{p,n}^\sigma(x) \le \max_{j \in \mathcal{J}} g_{p,n}^\sigma((x + (j-h))/b^n),$$

for all $x \in \mathrm{I}_h^n$. Otherwise the interval is called *dominant*. It is enough to consider dominant intervals of the functions $g_{p,n}^\sigma$ to determine the supremum of $g_{p,n+1}^\sigma$.

Results. Our computations indicate that the maximum of χ_p^σ for $\sigma_1 = P(am+a-1, a, id_a)$ is at

$$k^* = (\lceil a/2 \rceil - 1)\,(m+1) + \lfloor (m+1)/2 \rfloor,$$

and for $\sigma_2 = P(am+1, a, revid_a)$ it is at

$$k^* = (\lceil a/2 \rceil - 1)m + \lceil m/2 \rceil.$$

We guess the dominant intervals of $g_{p,n}^\sigma$ accordingly and collect our guesses, depending on the parity of a and m, in Table 5.1.

Theorem 5.1. *Let $\mathcal{J}$ be the set of prime numbers.*

- *For every $p \in \mathcal{J}$, take a multiplier $2 \le a \le p-2$ that divides $p+1$. Then the set of linear permutations*

$$\mathcal{P} = \{P(p, a, id_a) : p \in \mathcal{J}, a | (p+1)\}$$

  is not distribution preserving.
- *For every $p \in \mathcal{J}$, take a multiplier $2 \le a \le p-2$ that divides $p-1$. Then the set of linear permutations*

$$\mathcal{P} = \{P(p, a, revid_a) : p \in \mathcal{J}, a | (p-1)\}$$

  is not distribution preserving.

Proof. We split the proof into two parts. First, we show the general idea to derive a lower bound for the asymptotic constant of a given permutation in base p. Then we apply this method to derive our explicit bounds.

For k^*, we consider the interval $\mathrm{J} = [k^*/p, (k^*+1)/p]$ (or a translation of it; see Table 5.1) and use Theorem 4.1 to compute the values $\chi_p^\sigma(k^*/p)$ and $\chi_p^\sigma((k^*+1)/p)$. Therefore we can compute the coefficients of χ_p^σ in the interval J by applying Equation (4.1) and solving the linear system

$$\chi_p^\sigma(k^*/p) = \frac{p^2(p^2-1)}{12}\left(\frac{k^*}{p}\right)^2 + A\frac{k^*}{p} + B,$$
$$\chi_p^\sigma((k^*+1)/p) = \frac{p^2(p^2-1)}{12}\left(\frac{k^*+1}{p}\right)^2 + A\frac{k^*+1}{p} + B,$$

for A and B. Consequently, due to Theorem 3.2,

$$\begin{aligned}\gamma_p^\sigma &= \inf_{n\geq 1}\sup_{x\in[0,1]}\left(\sum_{j=1}^{n}\chi_p^\sigma(xp^j)/n\right)\\ &\geq \inf_{n\geq 1}\frac{1}{n}\left(\frac{p^2(p^2-1)}{12}\left(\bar{x}_0^2+\sum_{i=1}^{n-1}p^i\bar{x}_i^2\right)+A\sum_{i=1}^{n-1}p^i\bar{x}_i+nB\right) =: g_p^\sigma,\end{aligned}$$

where $\bar{x}_i := (k^*+1)/p^n + \sum_{j=i+1}^{n-1}(k^*/p^j)$. Finally

$$f(S_p^\sigma) = \frac{4\pi^2\gamma_p^\sigma}{p^2\log p} \geq \frac{4\pi^2 g_p^\sigma}{p^2\log p}.$$

Now we apply this method. Let $p = am+a-1$ and set $k^* = (\lceil a/2\rceil - 1)\times(m+1) + \lfloor (m+1)/2\rfloor$. For even $a = 2s$ and $m = 2t$, $p = 4st + 2s - 1$ and $k^* = (s-1)(2t+1)+t$.

The above calculations give for $n\to\infty$

$$\begin{aligned}\gamma_p^\sigma \geq{}& \frac{s^5 - 3s^4 + 8s^3t^5 + 4s^3 - 3s^2 + \left(20s^3 - 12s^2\right)t^4}{12(2st+s-1)}\\ &+ \frac{\left(8s^5 + 20s^3 - 16s^2 + 4s\right)t^3 + \left(12s^5 - 12s^4 + 14s^3 - 8s^2 + s\right)t^2}{12(2st+s-1)}\\ &+ \frac{\left(6s^5 - 12s^4 + 12s^3 - 6s^2\right)t + s}{12(2st+s-1)} =: g_p^\sigma.\end{aligned}$$

We see that the leading terms of g_p^σ are of the form $c_1\cdot s^2t^4$ and $c_2\cdot s^4t^2$ for some constants c_1 and c_2. Hence, for

$$f(S_p^\sigma) \geq \frac{4\pi^2 g_p^\sigma}{p^2\log p} = \frac{4\pi^2 g_p^\sigma}{(4st+2s-1)^2\log(4st+2s-1)},$$

we obtain leading terms of the form $s^2/\log(4st+2s-1)$ and $t^2/\log(4st+2s-1)$ again multiplied by certain constants. Thus, depending on whether $s\geq t$ or $t > s$, we always get at least one term that grows beyond any bound if we increase the base, since $\lim_{n\to\infty}\frac{n^2}{\log n^2} = \infty$.

Exactly the same analysis can be done for the cases when a is even and m is odd as well as when a is odd and m is odd. Moreover, we can also analyze permutations $P(am+1, a, revid_a)$ following the same line of arguments (see appendix). □

Remark 3. These results also hold for the similar sets of linear-like permutations $\mathcal{P} = \{P(p, a, id_a) : p \in \mathcal{J}, a|(p-1)\}$ and $\mathcal{P} = \{P(p, a, revid_a) : p \in \mathcal{J}, a|(p+1)\}$ (see Remark 2).

Remark 4. The above proof confirms our computational results for these special cases: For fixed p, if a and m are equal or nearly equal, the corresponding sequences show a better distribution behavior than if one of the parameters is much larger than the other. If we develop this idea further and assume for simplicity that $a = m = 2s$, such that $p = 4s^2 + x$, we see that the above asymptotic constants are close to $\pi^2 s^2/(12 \log 2s) \approx f(S_{2s}^{id})$. Hence, $f(S_{\bar{p}}^{id})$, with $\bar{p} = \sqrt{p - x}$ is a (heuristic) lower bound for the best permutations of the two classes we have studied in this section.

5.4. Examples. According to the introduction of this section, we can think of two different ways how to apply Theorem 5.1. We can explicitly compute asymptotic diaphony constants, which is especially interesting for sequences in small bases. In high bases, the fact that our sets are not distribution preserving tells us that the corresponding sequences are weakly distributed and therefore not interesting for specific applications.

Example. Let $p = 19$. Then $a = 1, 2, 3, 6, 9$ are divisors of $p - 1 = 18$ and $a = 1, 2, 4, 5, 10$ are divisors of $p + 1 = 20$. Therefore, due to symmetry, we can explicitly determine the distribution behavior of linear permutations with multipliers $a = 1, 2, 3, 4, 5, 6, 9, 10, 13, 14, 15, 16, 17, 18$. Furthermore, let $19 = 4 \cdot 4 + 3$, such that $a = m = 4 = 2s$. With $\sigma = P(19, 4, id_4)$, we can follow the idea of Remark 4 and get

$$f(S_{19}^{id}) = 25.3485\ldots \geq f(S_{19}^{\sigma}) \geq 2.7394\ldots \geq f(S_4^{id}) = 2.6417\ldots,$$

in which we used the results for the original van der Corput sequences of Faure as well as the bound we computed in Theorem 5.1. To illustrate Remark 4 further, consider $p = 109 = 10 \cdot 10 + 9 = 5 \cdot 21 + 4$ with $\sigma_1 = P(109, 10, id_{10})$ and $\sigma_2 = P(109, 5, id_5)$, then

$$f(S_{109}^{\sigma_2}) \geq 22.0762\ldots \geq f(S_{109}^{\sigma_1}) \geq 9.5570\ldots \geq f(S_{10}^{id}) = 8.9622\ldots$$

Example. Let $p = 173$. The divisors of 172 and 174 let us identify 18 weak multipliers. The probability of picking a weak multiplier at random is therefore approximately 0.1. However, for $p = 109$ we find 30 weak multipliers with this method, which yields a probability of $30/109 \geq 0.25$.

6. Permutation polynomials and future directions

Our main result, Theorem 5.1, is a negative assertion. We show that for any integer base b, a wide class of permutations, including certain linear permutations, generate sequences that behave asymptotically similar to sequences generated from identity permutations in smaller bases. Hence, these permutations are not suitable for scrambling of Halton sequences in quasi-Monte Carlo methods.

Future work should concentrate on finding rules for the generation of distribution preserving sets of permutations, which are amenable for theoretical investigations of multi-dimensional Halton sequences. Due to promising numerical results, we wish to introduce and motivate the study of permutation polynomials.

A *permutation polynomial* (for a given ring or field) is a polynomial that acts as a permutation P of the elements of the ring. A well known result of Carlitz [4] about permutation polynomials of a finite field implies that every permutation P in base p can be represented by a polynomial

$$P_n(x) = (\dots((a_0x + a_1)^{p-2} + a_2)^{p-2} \dots + a_n)^{p-2} + a_{n+1}, \tag{6.1}$$

for some $n \geq 0$. Defining $P_0(x) := a_0x + a_1$, we can also express (6.1) as $P_n(x) = (P_{n-1}(x))^{p-2} + a_{n+1}$, for $n \geq 1$. The smallest integer n such that P_n defines P is called the *Carlitz rank* of P. This notion is introduced and studied in [1], where also a formula for the number of permutations with fixed Carlitz rank $n < (p-1)/2$ can be found.

In the present paper we study distribution properties of permutations $P = P_0(x)$, where we set without loss of generality $a_1 = 0$. We observed that the behavior of these permutations heavily depends on the parameter a_0. In [14], we computationally determined the smallest possible asymptotic constants for sequences in small bases (≤ 50). Even if the best linear permutations generate sequences with a very good uniform distribution behavior, they do not reach these smallest possible values. Therefore we ask:

- Is it possible to describe sets of permutations with good distribution behavior in a systematic way with permutation polynomials?
- Are there distribution preserving sets of permutations with fixed Carlitz rank n?

Remark 5. Computational results indicate a positive answer to the second question for $n = 0$ and $n = 3$ and a negative answer for $n = 1$ and $n = 2$.

Acknowledgements

I had the first ideas for the present paper during a short stay at Sabancı University in Istanbul. I would like to thank Alev Topuzoglu for her kind hospitality and her valuable comments on a draft version of this paper. In addition, I am thankful to Herbert Edelsbrunner and the anonymous

referee for many suggestions that helped to improve the readability and presentation of my manuscript.

References

[1] E. Aksoy, A. Cesmelioglu, W. Meidl, A. Topuzoglu, *On the Carlitz rank of permutation polynomials*. Finite Fields Appl. **15** (2009), 428–440.
[2] E. Atanassov, *On the discrepancy of Halton sequences*. Math. Balkanica **18** (2004), 15–32.
[3] E. Atanassov and M. Durchova, *Generating and testing the modified Halton sequences*. In: Fifth International Conference on Numerical Methods and Applications, Borovets 2002, Springer-Verlag, Ed. Lecture Notes in Computer Science, vol. 2542 (2003), Berlin, 91–98.
[4] L. Carlitz, *Permutations in a finite field*. Proc. Amer. Math. Soc. **4** (1953), 538.
[5] H. Chaix and H. Faure, *Discrépance et diaphonie en dimension un*. Acta Arith. **63** (1993), 103–141.
[6] M. Drmota and R.F Tichy, *Sequences, Discrepancies and Applications*. Lecture Notes in Math. 1651. Springer-Verlag, Berlin, 1997.
[7] H. Faure, *Discrépance de suites associées à un système de numération (en dimension un)*. Bull. Soc. Math. France **109** (1981), 143–182.
[8] H. Faure, *Good permutations for extreme discrepancy*. J. Number Theory **42** (1992), 47–56.
[9] H. Faure, *Discrepancy and diaphony of digital* $(0,1)$*-sequences in prime base*. Acta Arith. **117** (2005), 125–148.
[10] H. Faure, *Irregularities of distribution of digital* $(0,1)$*-sequences in prime base*. Electron. J. Combinatorial Number Theory **5** (2005), no. 3.
[11] H. Faure, *Selection criteria for (random) generation of digital* $(0,s)$*-sequences*. In: Monte Carlo and Quasi-Monte Carlo Methods 2004, H. Niederreiter and D. Talay, Ed. Springer (2006), 113–126.
[12] H. Faure and C. Lemieux, *Generalized Halton sequences in 2008: A comparative study*. ACM Trans. Model. Comp. Sim. **19** (2009), Article 15:1–31.
[13] 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.
[14] F. Pausinger and W. Ch. Schmid, *A good permutation for one-dimensional diaphony*. Monte Carlo Methods Appl. **16** (2010), 307–322.
[15] F. Pausinger and W. Ch. Schmid, *A lower bound for the diaphony of generalised van der Corput sequences in arbitrary base b*. Unif. Distrib. Theory **6** (2011), no. 2, 31–46.
[16] X. Wang, C. Lemieux and H. Faure, *A note on Atanassov's discrepancy bound for the Halton sequence*. Technical report, Department of Statistics and Actuarial Science, University of Waterloo, (2008).
[17] P. Zinterhof, *Über einige Abschätzungen bei der Approximation von Funktionen mit Gleichverteilungsmethoden*. Österr. Akad. Wiss. SB II **185** (1976) 121–132.

Florian Pausinger
IST Austria (Institute of Science and Technology Austria),
Am Campus 1,
3400-Klosterneuburg, Austria
E-mail: florian.pausinger@ist.ac.at