DE GRUYTER OPEN

uniform distribution theory

DOI: 10.1515/udt-2018–0003
Unif. Distrib. Theory **13** (2018), no.1, 47–64

# ON THE DISCREPANCY OF TWO FAMILIES OF PERMUTED VAN DER CORPUT SEQUENCES

Florian Pausinger — Alev Topuzoğlu

ABSTRACT. A permuted van der Corput sequence $S_b^\sigma$ in base $b$ is a one-dimensional, infinite sequence of real numbers in the interval $[0,1)$, generation of which involves a permutation $\sigma$ of the set $\{0,1,\dots,b-1\}$. These sequences are known to have low discrepancy $D_N$, i.e. $t(S_b^\sigma) := \limsup_{N\to\infty} D_N(S_b^\sigma)/\log N$ is finite. Restricting to prime bases $p$ we present two families of generating permutations. We describe their elements as polynomials over finite fields $\mathbb{F}_p$ in an explicit way. We use this characterization to obtain bounds for $t(S_p^\sigma)$ for permutations $\sigma$ in these families. We determine the best permutations in our first family and show that all permutations of the second family improve the distribution behavior of classical van der Corput sequences in the sense that $t(S_p^\sigma) < t(S_p^{id})$.

*Communicated by Friedrich Pillichshammer*

## 1. Introduction

The irregularities of distribution of an infinite sequence $X = (x_k)_{k\geq 1} \subset [0,1)$ can be quantified by various notions of discrepancy; see [4, 5, 15]. In this paper, we study the *extreme discrepancy*, $D_N(X)$, of an infinite sequence $X$. We remark that we follow Faure and define discrepancy without the scaling factor $1/N$. A sequence $X$ is a *low discrepancy sequence* if there exists a constant $K$ independent of $N$ such that $D_N(X) \leq K \cdot \log N$ for all $N$. This terminology is motivated by a well-known result of Schmidt [22] who showed that there exists an absolute constant $\kappa$ such that for all infinite sequences $X \subset [0,1)$, we have $D_N(X) > \kappa \cdot \log N$ for infinitely many $N$. The currently best known bound $\kappa > 0.121128$ is due to Larcher [16].

2010 Mathematics Subject Classification: 11K38, 11K06, 11T06.
Keywords: van der Corput sequence; extreme discrepancy; permutation; permutation polynomial; Carlitz rank;

Let $b \geq 2$ be an integer and let $\mathfrak{S}_b$ denote the set of all permutations $\sigma$ of $\{0, 1, \ldots, b-1\}$. Classical (for $\sigma = id$) and permuted van der Corput sequences, $S_b^\sigma$, are well-known examples of low discrepancy sequences. These sequences are the basic building blocks of multi-dimensional *Halton sequences*, which play an important role in numerical integration and quasi-Monte Carlo methods; see [12] and Section 6. Faure presented explicit formulas for the discrepancy of these sequences and showed that $D_N(S_b^\sigma) \leq D_N(S_b^{id})$ for all $\sigma \in \mathfrak{S}_b$ and all $N \in \mathbb{N}$; see [6, 8]. Furthermore, Faure developed a framework to compute the asymptotic value

$$t(S_b^\sigma) := \limsup_{N \to \infty} \frac{D_N(S_b^\sigma)}{\log N},$$

which is known to be finite. This quantity can be used to compare sequences obtained by varying permutations in the sense that smaller values of $t$ indicate sequences with more regular distribution. In particular, it is known [6] that

$$t(S_b^\sigma) \leq t(S_b^{id}), \tag{1}$$

for every permutation $\sigma \in \mathfrak{S}_b$. Therefore the main question in this context is to determine permutations that improve the distribution properties of the classical van der Corput sequence. Faure calculated in [6, Théorème 6],

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

On the other hand, the smallest known asymptotic values within the family of permuted van der Corput sequences given in [6, 7] have recently been improved by Ostromoukhov [20] to $t(S_{84}^\sigma) = 0.353494\ldots$ for a particular permutation in base 84. Furthermore, Faure [7] introduced an algorithm that outputs exactly one permutation $\sigma_F \in \mathfrak{S}_b$ for every $b \geq 2$ such that $t(S_b^{\sigma_F}) < 1/\log 2$, which beautifully contrasts the result for the identity permutations.

The aim of our paper is to study the asymptotic constants $t(S_b^\sigma)$ for permutations $\sigma$, which belong to sets of structurally similar permutations $\mathcal{F} \subseteq \mathfrak{S}_b$ thus providing larger sets of *good* generating permutations in a given base. We focus on the case $b = p$, for a prime $p$, with the advantage 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 permutation polynomials in $\mathbb{F}_p[x]$, where, as usual, we identify $\mathbb{F}_p$ with $\{0, 1, \ldots, p-1\}$. We are mainly interested in two essentially different families of permutations; i.e., affine permutations and fractional affine permutations. For $a_0 \in \mathbb{F}_p \setminus \{0\} = \mathbb{F}_p^*$ 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 [17] and is discussed in a recent survey by Faure et al [11]. Our notation is motivated by the underlying geometric interpretation and should highlight its algebraic relation to our second family.

Our main result for affine permutations $\sigma = \sigma_{a_0,a_1}$ is an upper bound for $t(S_p^\sigma)$ in terms of the parameter $a_0$. We refer to the book of Khinchin [14] 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 1.1.** *For a prime $p$, let $a_0 \in \mathbb{F}_p^*$, $a_1 \in \mathbb{F}_p$ and $\sigma = \sigma_{a_0,a_1} \in \mathcal{F}_p^{(a)}$. Let $a_0/p = [0, \alpha_1, \alpha_2, \dots, \alpha_m]$ and set $\alpha_{\max} = \max_{1\le i\le m} \alpha_i$. Then, for all $N \in \mathbb{N}$,*

$$D_N(\mathcal{S}_p^\sigma) \le \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)} \log(N+1) \quad \textit{and} \quad t(S_p^\sigma) \le \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)}.$$

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 $p$. There is a close relation between this problem and the well-known *conjecture of Zaremba* [24]. Indeed, recent progress on this conjecture [1, 13] 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 $\alpha_{\max} \le 5$.

**Remark 1.2.** 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 1.1 is applicable at all. The bound in Theorem 1.1 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 $a_0/p$. Table 1 gives a list of such multipliers for $11 \le p \le 151$, with $\alpha_{\max}(a_0/p) \le 3$.

To present our second main result, we turn to another family of 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

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

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

TABLE 1. Good multipliers $a_0$ with $\alpha_{\max}(a_0/p) \leq 3$ for prime bases $11 \leq p \leq 151$.

| $p$ | $a_0$ | $p$ | $a_0$ |
|---|---|---|---|
| 11 | $3, 4$ | 73 | $27$ |
| 13 | $5$ | 79 | $23, 24, 29, 30$ |
| 17 | $5, 7$ | 83 | $22, 30, 34, 36$ |
| 19 | $7, 8$ | 89 | $24, 25, 26, 27, 32, 33, 34$ |
| 23 | $7, 10$ | 97 | $26, 35, 36, 41$ |
| 29 | $8, 11, 12$ | 101 | $30, 37, 39, 44$ |
| 31 | $12, 13$ | 103 | $37, 39$ |
| 37 | $10, 11$ | 107 | $41, 47$ |
| 41 | $11, 12, 15, 16, 17, 18$ | 109 | $30, 33, 40, 45, 46$ |
| 43 | $12, 18$ | 113 | $30, 49$ |
| 47 | $13, 18$ | 127 | $34, 56$ |
| 53 | $14, 19, 23$ | 131 | $36, 40, 47, 50, 55$ |
| 59 | $18, 23, 25, 26$ | 137 | $37$ |
| 61 | $17, 18, 22, 25$ | 139 | $39, 41, 57, 61$ |
| 67 | $18, 26$ | 149 | $40, 41, 44, 55, 65$ |
| 71 | $21, 26, 27, 30$ | 151 | $56, 59, 62, 64$ |

better distributed than the classical van der Corput sequence in the same base; compare (1) and (2).

**THEOREM 1.3.** *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,*

$$t(S_p^{\pi}) < t(S_p^{id}). \tag{2}$$

**Remark 1.4.** It is interesting to note that even if the set of permutations $\mathcal{F}_p^{(f)}$ is much larger than $\mathcal{F}_p^{(a)}$, the range of values for $t(S_p^{\pi})$ is smaller; see Table 2 and Section 6.3. 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.

Our theorems offer two assets to the practitioner. Firstly, we provide a criterion based on continued fractions to choose a provably *good multiplier* for linear digit scrambling in prime base $p$. Secondly, we 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 as illustrated in Table 2. 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 sequences in base $p$.

We recall the necessary background on the discrepancy of permuted van der Corput sequences in Section 2 and prove Theorem 1.1 in Section 3. Theorem 1.3 is proven in Section 4, before we discuss a useful extension of $\mathcal{F}_p^{(f)}$ in Section 5. We conclude our paper with three remarks on directions for future research in Section 6.

## 2. Discrepancy of van der Corput sequences

In this section we recall the main definitions of uniform distribution theory as well as the main results of Faure concerning the exact computation of the discrepancy of permuted van der Corput sequences.

### 2.1. Discrepancy

Let $[\alpha,\beta) \subseteq [0,1)$ be a subinterval of the half open unit interval. For an infinite sequence $X=(x_k)_{k\geq 1}$ in $[0,1)$ and for $N \geq 1$, let $A([\alpha,\beta),N,X)$ denote the number of indices $k \leq N$ for which $x_k \in [\alpha,\beta)$ and let $E([\alpha,\beta),N,X) := A([\alpha,\beta),N,X)-(\beta-\alpha)N$ denote the *discrepancy function*. An infinite sequence $X$ is *uniformly distributed* if

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

for every subinterval $[\alpha,\beta)$. The *extreme discrepancy*, $D_N(X)$, of the first $N$ points of $X$ is defined as

$$D_N(X) = \sup_{[\alpha,\beta)\subseteq[0,1)} |E([\alpha,\beta),N,X)|.$$

A sequence $X$ is uniformly distributed if and only if $\lim\limits_{N\to\infty} D_N(X)/N = 0$ and it is a *low discrepancy sequence* if for all $N$, there exists a constant $K$, independent of $N$, such that $D_N(X) < K\log(N)$.

### 2.2. Permuted van der Corput sequences

The classical van der Corput sequences $V_b = \big(\mathcal{V}_b(k)\big)_{k\geq 1}$ in base $b$ are one-dimensional, infinite sequences of real numbers in the half-open unit interval $[0,1)$, which are defined by the radical inverse function. Let $\sum_{j=0}^{\infty} a_j(k)b^j$ be the $b$-adic representation of the integer $k \geq 0$, with $0 \leq k < b^n$ and $a_j(k)=0$ if $j \geq n$. Put $\mathcal{V}_b(k) = \sum_{j=0}^{\infty} \frac{a_j(k)}{b^{j+1}}$.

Let $\mathfrak{S}_b$ denote the set of all permutations of $\{0,1,\dots,b-1\}$. We follow Faure [6] and define the *permuted (generalized) van der Corput sequence*, $S_b^\sigma = \big(\mathcal{S}_b^\sigma(k)\big)_{k\geq 1}$, for a fixed base $b \geq 2$ and $\sigma \in \mathfrak{S}_b$ by

$$\mathcal{S}_b^\sigma(k) = \sum_{j=0}^{\infty} \frac{\sigma(a_j(k))}{b^{j+1}}, \ k \geq 1. \tag{3}$$

Hence $\mathcal{V}_b(k) = \mathcal{S}_b^{id}(k), k \geq 0$, where $id$ denotes the identity permutation in $\mathfrak{S}_b$.

### 2.3. Analysis of discrepancy

The analysis of the discrepancy of $S_b^\sigma$ is based on auxiliary functions that were introduced in [6]. For $\sigma \in \mathfrak{S}_b$, let $\mathcal{Z}_b^\sigma := \big(\sigma(0)/b, \sigma(1)/b, \dots, \sigma(b-1)/b\big)$. For $h \in \{0,1,\dots,b-1\}$ and $x \in \big[\frac{k-1}{b}, \frac{k}{b}\big)$, where $1 \leq k \leq b$ is an integer, we define

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

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 $h \in \{0,\dots,b-1\}$. Faure [6] introduced a further class of functions which are based on $\varphi_{b,h}^\sigma$ as

$$\psi_b^\sigma := \max_{0\leq h\leq b-1}(\varphi_{b,h}^\sigma) + \max_{0\leq h\leq b-1}(-\varphi_{b,h}^\sigma).$$

Moreover, in [6, Théorème 1 and Théorème 2] a technique is developed to compute the discrepancy of $S_b^\sigma$ exactly. Firstly, it is shown that for all $N \geq 1$

$$D_N(S_b^\sigma) = \sum_{j=1}^{\infty} \psi_b^\sigma\left(\frac{N}{b^j}\right). \tag{4}$$

Secondly, for

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

Faure obtains

$$t(S_b^\sigma) = \limsup_{N\to\infty} \frac{D_N(S_b^\sigma)}{\log N} = \frac{\alpha_b^\sigma}{\log b}. \tag{5}$$

Note that the extremal values of $\psi_b^\sigma(y)$, $y \in [0,1)$ are attained when $y = k/b$, where $1 \leq k \leq b-1$. Considering $\psi_b^\sigma(0) = \psi_b^\sigma(1) = 0$ and putting $\max \psi_b^\sigma := \alpha_0$, one has $1/n \sum_{j=1}^{n} \psi_b^\sigma(xb^{-j}) < \alpha_0$ and hence an upper bound for the asymptotic constant can be obtained as

$$t(S_b^\sigma) \leq \frac{\alpha_0}{\log b}, \qquad \text{see [10, Lemma 1].}$$

We conclude this section with a useful lemma:

**Lemma 2.1.** *Let* $0 < a < b$ *be an integer, let* $\sigma \in \mathfrak{S}_b$ *and let* $\sigma', \sigma'' \in \mathfrak{S}_b$ *be defined as*

$$\sigma'(x) = \sigma(x) + a \pmod{b}, \qquad \text{and} \qquad \sigma''(x) = -\sigma(x) \pmod{b}$$

*for* $0 \le x \le b-1$, *then for all* $N$,

$$D_N(S_b^\sigma) = D_N\big(S_b^{\sigma'}\big) \qquad \text{and} \qquad D_N(S_b^\sigma) = D_N\big(S_b^{\sigma''}\big).$$

Proof. In the following we think of $[0, b)$ as a torus; i.e., addition and substraction is performed modulo $b$ and for $\alpha, \beta \in [0, b)$ with $\alpha > \beta$ we define $[\alpha, \beta) := [0, \beta) \cup [\alpha, b)$. Note that the first part of the lemma was already observed by Chaix and Faure [3, Théorème 4.4]. Their proof relies on the observation that if $\sigma(x) \in [\alpha, \beta) \subset [0, b)$, then $\sigma'(x) \in [\alpha + a, \beta + a) \subset [0, b)$. The second assertion can be shown along the same lines, observing that if $\sigma(x) \in [\alpha, \beta) \subset [0, b)$ then $\sigma''(x) \in (-\beta, -\alpha]$ and therefore $\sigma''(x) \in [-\beta + 1, -\alpha + 1) \subset [0, b)$. $\square$

## 3. Affine permutations

We obtain Theorem 1.1 by combining two earlier results. For the first part we observe that a bound for $\psi_p^\sigma$, $\sigma \in \mathcal{F}_p^{(a)}$, can be given using an idea that Niederreiter used to bound the discrepancy of Kronecker sequences. The second part follows by applying a method of Faure.

**Lemma 3.1.** *For a prime* $p$, *let* $\sigma = \sigma_{a_0,a_1} \in \mathcal{F}_p^{(a)}$ *and* $a_0/p = [0, \alpha_1, \alpha_2, \ldots, \alpha_m]$ *be the finite continued fraction expansion of* $a_0/p$. *Then for* $1 \le N < p$,

$$D_N(S_p^\sigma) = \psi_p^\sigma(N/p) \le K_{\alpha_{\max}} \log N,$$

*where* $\alpha_{\max} := \max_{1 \le i \le m} \alpha_i$ *and* $K_{\alpha_{\max}}$ *is a constant that depends on* $\alpha_{\max}$ *only.*

Proof. First we note by Lemma 2.1 that the parameter $a_1$ has no influence on the discrepancy of $S_p^{\sigma_{a_0,a_1}}$. Therefore, in what follows we set $a_1 = 0$. We prove this lemma by a finite version of the argument of Niederreiter for infinite Kronecker sequences; see [15, Chapter 2, Theorem 3.4]. To see the connection to Kronecker sequences, we observe that the first $p$ points of $S_p^{\sigma_{a_0,a_1}}$ are of the form $\{k \cdot a_0/p\}$ for $k = 0, 1, \ldots, p-1$, where $\{\beta\}$ denotes the fractional part of $\beta$.

Now, let $1 = q_0 < q_1 < \cdots < q_r < \cdots < p$ be the denominators of the *convergents* (see [14] for a definition) to $a_0/p$. For a given $1 \le N \le p$, there exists $r \ge 0$ such that $q_r \le N < q_{r+1}$ and we have $N = b_r q_r + N_{r-1}$ with $0 \le N_{r-1} < q_r$.

We note that $(\alpha_{r+1}+1)q_r \geq q_{r+1} > N$, and so, $b_r \leq \alpha_{r+1}$. If $r > 0$, we may write $N_{r-1} = b_{r-1}q_{r-1} + N_{r-2}$ with $0 \leq N_{r-2} < q_{r-1}$. Again we find $b_{r-1} \leq \alpha_r$. Continuing in this manner, we arrive at a representation for $N$ of the form $N = \sum_{i=0}^{r} b_i q_i$ with $0 \leq b_i \leq \alpha_{i+1}$ for $0 \leq i \leq r$, and $b_r \geq 1$.

We decompose the interval $[1, N]$ into $b_r + b_{r-1} + \cdots + b_0$ subintervals, such that the first $b_r$ intervals are of length $q_r$, the next $b_{r-1}$ intervals are of length $q_{r-1}$ and so on. Using this decomposition, we also decompose the given sequence $\{a_0/p\}, \{2a_0/p\}, \ldots, \{Na_0/p\}$ into $b_r + b_{r-1} + \cdots + b_0$ sequences $\{na_0/p\}$ in which $n$ runs through the corresponding subintervals of $[1, N]$ We estimate the discrepancy of such a finite sequence $\{na_0/p\}$, in which $n$ runs through $q_i$ consecutive integers, say $n = n_0 + j$ with $1 \leq j \leq q_i$. We have

$$\frac{a_0}{p} = \frac{p_i}{q_i} + \frac{x}{q_i q_{i+1}}, \quad \text{with} \quad |x| \leq 1.$$

Therefore,

$$\left\{ n\frac{a_0}{p} \right\} = \left\{ n_0\frac{a_0}{p} + \frac{jp_i}{q_i} + \frac{jx}{q_i q_{i+1}} \right\}.$$

Referring to the proof of Niederreiter we can conclude that the discrepancy $D_{q_i}$ of the finite sequence $\{na_0/p\}$, $n_0 + 1 \leq n \leq n_0 + q_i$, satisfies

$$\frac{1}{N} D_{q_i} \leq \frac{1}{q_i} + \frac{1}{q_{i+1}}.$$

Consequently, by [15, Chapter 2, Theorem 2.6] we can estimate the discrepancy of the original sequence based on the decomposition we chose, and get

$$D_N(S_p^\sigma) \leq \sum_{i=0}^{r} b_i \left( \frac{q_i}{q_{i+1}} + 1 \right) \leq r + 1 + \sum_{i=0}^{r} b_i,$$

which is shown to simplify to

$$D_N(S_p^\sigma) \leq 3 + \left( \frac{1}{\log \xi} + \frac{\alpha_{\max}}{\log(\alpha_{\max}+1)} \right) \log N,$$

for $\xi = (1+\sqrt{5})/2$. In [18], see also [19, Corollary 3.5], Niederreiter improved this result to

$$D_N(S_p^\sigma) \leq \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)} \log(N+1).$$

□

**Lemma 3.2.** *For a prime $p$, let $\sigma = \sigma_{a_0,a_1} \in \mathcal{F}_p^{(a)}$ and let $\alpha_{\max}$ be defined as above. Then we have that*

$$t(S_p^\sigma) \le \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)}. \tag{6}$$

P r o o f. Starting from the bound on the maximum of $\psi_p^\sigma(N/p)$, we apply the asymptotic method of F a u r e [6, Théorème 2]. Recall that

$$t(S_p^\sigma) = \lim_{N\to\infty} \frac{D_N(S_p^\sigma)}{\log N} = \frac{\alpha_p^\sigma}{\log p}, \quad \text{with} \quad \alpha_p^\sigma = \inf_{n\ge 1} \sup_{x\in\mathbb{R}} \left( 1/n \sum_{j=1}^{n} \psi_p^\sigma(x/p^j) \right).$$

Since,

$$\alpha_p^\sigma \le \max_{x\in[0,1]} \psi_p^\sigma(x) \le \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)} \cdot \log p,$$

we get

$$t(S_p^\sigma) = \frac{\alpha_p^\sigma}{\log p} \le \frac{1}{\log p} \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)} \cdot \log p = \frac{\alpha_{\max}+1}{\log(\alpha_{\max}+1)}. \qquad \square$$

## 4. Fractional affine permutations

The aim of this section is to prove Theorem 1.3. We first recall how Faure calculated $t(S_b^{id})$ before we show that $t(S_b^\pi) < t(S_b^{id})$ for every $\pi = \pi_{a_0,a_1,a_2} \in \mathcal{F}_p^{(f)}$.

Let $\sigma \in \mathfrak{S}_b$. Faure showed [6, Corollaire 3] that

$$\psi_b^\sigma\left(\frac{k}{b}\right) \le k\left(1 - \frac{k}{b}\right), \tag{7}$$

for $0 \le k \le b-1$. Since $D_k(S_b^\sigma) = \psi_b^\sigma(k/b)$ for $1 \le k \le b-1$, we obtain equality in (7) 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

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

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

Moreover, Faure finds for odd $b$ [6, Théorème 6] that

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

in which

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

In the following $\oplus$ denotes addition modulo $b$ and we put for any $\sigma \in \mathfrak{S}_b$ and $k \le b$,

$$J_k^{\sigma} = \{\sigma(x) : 1 \le x \le k\}.$$

Hence, $J_k^{id} = \{1, \dots, k\}$ for any $b \ge 2, \sigma = id, k \le b$. It turns out that fractional affine permutations never map the set $\{0, 1, \dots, (p-1)/2\}$ to a set of the form $J_{(p-1)/2}^{id} \oplus a$, for an $a \in \mathbb{F}_p$.

**Lemma 4.1.** *Let $\pi = \pi_{a_0,a_1,a_2} \in \mathcal{F}_p^{(f)}$ and $q = (p-1)/2$. Then $J_q^{\pi_{a_0}} \neq J_q^{id} \oplus a$ for all $a \in \mathbb{F}_p$.*

Proof. We apply again Lemma 2.1 and set $a_2 = 0$ in the following. First, we consider the case $a_1 = 0$ and write $\pi_{a_0} = \pi_{a_0,0,0}$. It suffices to show that for every $a_0 \in \mathbb{F}_p^*$ there exist $x, x' \in \{1, \dots, q\}$ such that

$$\pi_{a_0}(x') = \pi_{a_0}(x) + q, \tag{8}$$

since this implies that no permutation $\pi_{a_0}$ maps the set $\{1, \dots, q\}$ into an interval of the form $J_q^{id} \oplus a$. We can solve (8) for $x'$ and get

$$x(1 + a_0 q x)^{p-2} = x'. \tag{9}$$

If we fix $x$ in (9) and let $a_0$ run through $\mathbb{F}_p$, we obtain a permutation of $\mathbb{F}_p$ that gives for every $a_0$ and fixed $x$, the unique $x'$ such that (8) is satisfied. In particular, note that $x = x'$ if and only if $a_0 = 0$.

Next we write all $q$ permutations of the form (9) into a matrix such that row $i$ contains the permutation for $x = i$ and column $j$ contains all solutions $x'$ of (8) for fixed $a_0$ and $x \in \{1, \dots, q\}$. We observe that all $q$ rows in this matrix are shifted versions of each other; i.e., all $q$ permutations are shifted versions of $(1 + a_0 q)^{p-2}$ obtained for $x = 1$. In particular, there is a $k$ such that

$$x\bigl(1 + (a_0 + k)xq\bigr)^{p-2} = (x+m)\bigl(1 + a_0(x+m)q\bigr)^{p-2}, \tag{10}$$

for all $x$, $m$ and $a_0$. This means that the entry for $x'$ in row x and column $a_0 + k$ is the same as the entry in row $x + m$ and column $a_0$. Solving (10) for $k$ leads to

$$k = m\bigl(qx(m+x)\bigr)^{p-2}. \tag{11}$$

Now, if there was a parameter resp. column $\tilde{a}_0$ such that for every $x \in \{1, \dots, q\}$ we get $x' \in \{q+1, \dots, 2q\}$, then there must be a second parameter $-\tilde{a}_0$ for which all $x \in \{q+1, \dots, 2q\}$ are mapped to $\{q+1, \dots, 2q\}$. This can be seen from the symmetry

$$(a_0 x)^{p-2} = \big(-a_0(-x)\big)^{p-2}. \tag{12}$$

However, this means that we see $q$ of the values $\{0, 1, \dots, q\}$ in column $-\tilde{a}_0$ for $x \in \{1, \dots, q\}$.

To conclude, we know that the column for $a_0 = 0$ contains the value $x$ in row $x$. Moreover, assuming their exists a special parameter $\tilde{a}_0$, column $\tilde{a}_0$ always contains all values $q < y \leq 2q$ for $x \in \{1, \dots, q\}$, whereas column $-\tilde{a}_0$ contains all but one of the values $0 \leq z \leq q$. Thus, in each row such a value $y$ lies $\tilde{k} = \tilde{a}_0$ columns away of the value $x$, whereas such a value $z$ is $-\tilde{k} = -\tilde{a}_0$ columns away from $x$. This fixes the position of all elements in the shift permutation; i.e., this determines all shifts observed in (11) when going from the permutation in row $x$ to the permutation in row $x+1$. All values $z$ come at distance $-\tilde{k}$, thus implying that the shift permutation has a linear structure, i.e., turning from row $x$ to $x+1$ has to result in a shift by a multiple of $-\tilde{k}$, which contradicts our observation in (11). Therefore, there can not exist a special parameter $\tilde{a}_0$.

In the case $a_1 \neq 0$, we observe that since $(a_0 x + a_1)^{p-2}$ is a permutation of $\mathbb{F}_p$, there exists an $x^* \in \{1, \dots, p-1\}$ such that

$$a_0 x^* + a_1 = 0.$$

Therefore,

$$a_0 x + a_1 = a_0 x^* + a_1 + a_0(x - x^*) = a_0(x - x^*)$$

and

$$(a_0 x + a_1)^{p-2} = \big(a_0(x - x^*)\big)^{p-2}.$$

The proof of the corresponding assertion follows now along the same lines as in the case $a_1 = 0$ and is omitted for the sake of brevity. $\square$

**Remark 4.2.** This proof shows nicely the difference between affine and fractional affine permutations. Applying the same argument to affine permutations, we get $x' = x - q a_0^{p-2}$ in (9). Now we see that the rows of the corresponding matrix are not shifted versions of each other, but are obtained via incrementing each row by 1 when going from $x$ to $x+1$. Thus, if two elements in row 1 have a certain distance $k$, this row-wise increment ensures that we find $q$ different pairs of numbers with the same distance $k$. Therefore a special parameter $\tilde{a}_0$ can indeed exist for linear permutations; for example $\tilde{a}_0 = 1$.

Thus, we conclude that

$$\max_{1 \leq k \leq p} \psi_b^{\pi}(k/p) < \max_{1 \leq k \leq p} \psi_p^{id}(k/p), \quad \text{for all } \ \pi = \pi_{a_0, a_1, a_2} \in \mathcal{F}_p^{(f)}. \tag{13}$$

P r o o f o f T h e o r e m 1.3. Since we know that $\psi_p^\pi(x) \le \psi_p^{id}(x)$ for all $x \in [0,1]$ we have that

$$\alpha_p^\pi = \inf_{n\ge1} \sup_{y\in\mathbb{R}} \left( \frac{1}{n} \sum_{j=1}^{n} \psi_p^\pi \left( \frac{y}{p^j} \right) \right) \le \alpha_p^{id},$$

for all $y \in \mathbb{R}$. However, we get from the result of Faure and by the periodicity of $\psi_p^{id}$ that

$$\alpha_{p,n}^{id} = \frac{1}{n} \left( \psi_p^{id} \left( \frac{p-1}{2p} \right) + \sum_{j=2}^{n} \psi_p^{id} \left( \frac{\tilde{x}_n}{p^j} \right) \right),$$

for the above stated $\tilde{x}$. We set

$$\alpha_{p,n}^\pi := \sup_{y\in\mathbb{R}} \left( \frac{1}{n} \sum_{j=1}^{n} \psi_p^\pi \left( \frac{y}{p^j} \right) \right).$$

By Lemma 4.1 resp. (13) we know that $\max_{1\le k\le p} \psi_p^\pi(k/p) < \psi_p^{id}\big((p-1)/(2p)\big)$ and hence

$$\alpha_{p,n}^\pi < \alpha_{p,n}^{id},$$

for all $n$ from which the result follows. □

## 5. Extending the family of fractional permutations

The aim of this section is to show how fractional affine permutations can be related in a natural way to permutations with similar distribution properties of an even larger family by interchanging two elements in a systematic way.

Interchanging two elements of a permutation does in general not change the asymptotic constant of the corresponding van der Corput sequence too much. This follows from the fact that for $1 \le N \le p$, the value of the discrepancy function of all intervals that are affected by the interchange, will change by at most 1, since the number of points in the interval either increases or decreases by one. Writing $\sigma$ for the original permutation and $\sigma'$ for the modified permutation, we immediately see from the definition that

$$\alpha_p^{\sigma'} \le \alpha_p^\sigma + 1$$

and hence (5) implies

$$t\left(S_p^{\sigma'}\right) \le \frac{\alpha_p^\sigma}{\log p} + \frac{1}{\log p}.$$

### 5.1. Fractional linear transformations

First, we consider fractional linear transformations

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

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

$$\pi(x) = \pi_{a_0,a_1,a_2}(x) = (a_0 x + a_1)^{p-2} + a_2\,, \tag{14}$$

where $a_0 \neq 0, \alpha_1 = a_0, \beta_1 = a_1, \alpha_2 = a_0 a_2, \beta_2 = a_1 a_2 + 1$. Similarly, we consider permutations

$$\tau(x) = \tau_{A_0,A_1,A_2,A_3}(x) = \big((A_0 x + A_1)^{p-2} + A_2\big)^{p-2} + A_3 \tag{15}$$

for $A_0, A_2 \in \mathbb{F}_p^*$ and $A_1, A_3 \in \mathbb{F}_p$, and the fractional transformations

$$R_2(x) = \frac{\alpha_3 x + \beta_3}{\alpha_2 x + \beta_2},$$

where $\alpha_2, \beta_2$ 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 $X_1 = -A_1/A_0$, $X_2 = -(A_1A_2 + 1)/(A_0A_2)$, and set $\tau(X_1) = \alpha_3/\alpha_2$, $\tau(X_2) = R_2(X_1)$.

### 5.2. Interchanging elements

The following result shows that for every permutation $\pi$ there exists a permutation $\tau$ such that $\pi(x) = \tau(x)$ for all $x \in \mathbb{F}_p \setminus \{X_1, X_2\}$.

**Theorem 5.1.** *Fix $a_0, a_1, a_2 \in \mathbb{F}_p$, with $a_0, a_2 \neq 0$ and set (in $\mathbb{F}_p$)*

$$A_0 = -a_0 a_2^2, \quad A_1 = -a_1 a_2^2 - a_2, \quad A_2 = 1/a_2.$$

*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 $\pi(X_2) = \tau(X_1)$.*

Proof. Plugging into the above fractional linear transformations, we see that $\pi$ and $\tau$ have the same transformations

$$R_2(x) = \frac{A_0 x + A_1}{A_0 A_2 x + A_1 A_2 + 1} = \frac{-a_2(a_0 a_2 x + a_1 a_2 + 1)}{-a_2(a_0 x + a_1)} = R_1(x).$$

for all $x$ but $X_1, X_2$, with

$$X_1 = -\frac{A_1}{A_0} = -\frac{a_1 a_2 + 1}{a_0 a_2} \quad \text{and} \quad X_2 = -\frac{A_2 A_1 + 1}{A_2 A_0} = -\frac{a_1}{a_0}.$$

For $X_1$ and $X_2$ we obtain

$$\pi(X_1) = R_1(X_1) = 0 = \tau(X_2),$$
$$\pi(X_2) = \pi(-a_1/a_0) = a_2 = 1/A_2 = \tau(X_1). \qquad \square$$

From the last lines of the proof we see that $\tau$ is obtained from $\pi$ by swapping 0 and $a_2$. In this way, we associate a permutation $\tau_{A_0,A_1,A_2,0}$ to each permutation $\pi_{a_0,a_1,a_2}$. Note that by Lemma 2.1 the parameters $a_2, A_3$ have no importance for the discrepancy of $S_p^\pi$ resp. $S_p^\tau$ . Hence we can replace $a_2$ by zero to conclude the following. To each $\pi_{a_0,a_1,0}$ we can associate $p-1$ permutations $\tau_{A_0,A_1,A_2,-a_2}$, for $a_2 \in \{1,\dots,p-1\}$ such that the image of $\tau$ is obtained from the image of $\pi$ by swapping 0 and $-a_2$. We illustrate this with an example. To emphasize how different permutations are related, we represent a permutation $\sigma = \binom{0\ 1\ 2\ 3\ 4}{0\ 4\ 3\ 2\ 1}$ as $\sigma = (0,4,3,2,1)$, meaning that 0 is mapped to 0, 1 is mapped to 4 and so on.

**Example 5.2.**

Let $p = 11$ with $a_0 = 2, a_1 = 3$ and $a_2 = 5$. Then

$$\pi_{2,3,0} = (4,9,8,5,\mathbf{0},6,3,2,7,10,1)$$

and

$$\pi_{2,3,5} = (9,3,2,10,5,\mathbf{0},8,7,1,4,6).$$

Consequently, $A_0 = 5$, $A_1 = 8$ and $A_2 = 9$, such that

$$\tau_{5,8,9,-5} = (4,9,8,5,\mathbf{6},\mathbf{0},3,2,7,10,1)$$

and

$$\tau_{5,8,9,0} = (9,3,2,10,\mathbf{0},\mathbf{5},8,7,1,4,6).$$

Now choose $a_2' = 3$. Then

$$\pi_{2,3,3} = (7,1,\mathbf{0},8,3,9,6,5,10,2,4)$$

and $A_0' = 4, A_1' = 3, A_2' = 4$, such that

$$\tau_{4,3,4,-3} = (4,9,\mathbf{0},5,\mathbf{8},6,3,2,7,10,1)$$

and

$$\tau_{4,3,4,0} = (7,1,\mathbf{3},8,\mathbf{0},9,6,5,10,2,4).$$

## 6. Concluding remarks

### 6.1. Hammersley point sets and Halton sequences

Permuted Hammersley point sets are two dimensional point sets. Let $b \geq 2$ be an integer and let $S_b^\sigma$ be a permuted van der Corput sequence in base $b$. The *permuted two-dimensional Hammersley point set in base* $b$ consisting of $b^n$ points for $n \geq 0$ is defined by

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

In [10, Theorem 1] Faure proved a general formula for the star discrepancy $D_N^*(\mathcal{H}_{b,n}^\sigma)$ of Hammersley point sets generated from arbitrary permutations. Furthermore, he showed that the identity permutations generate up to a small constant the worst point sets in a given base. He derived asymptotic results [10, Theorem 3] that are similar to the one-dimensional case. His general formula reduces the study of two-dimensional Hammersley point sets to the study of one-dimensional van der Corput sequences and therefore all our results can be immediately applied to Hammersley point sets.

A *generalized Halton sequence* is a multi-dimensional sequence, whose $i$-th coordinate is a permuted van der Corput sequence. Halton sequences are uniformly distributed if the bases of the generating van der Corput sequences are coprime. The paper [21] as well as our results sharpen and confirm some of the observations and suggestions derived from the numerical results of [9, 12], where various selection criteria for good (and bad) multipliers $a_0$ (or $f$ in the notation of these papers) were stated. Our main contribution in this context is to give a concrete criterion how to identify good and bad multipliers based on continued fraction expansions. Moreover, we give a formal proof — relying on the Conjecture of Zaremba — that, indeed, there always exist good multipliers as observed in [9, Section 7].

### 6.2. Carlitz rank

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

$$P_n(x) = \Big( \dots \big( (a_0 x + a_1)^{p-2} + a_2 \big)^{p-2} \dots + a_n \Big)^{p-2} + a_{n+1}, \quad n \geq 0 \qquad (16)$$

for $a_0 a_2 \cdots a_n \neq 0$, with an associated fractional transformation

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

where $\alpha_i, \beta_i,\ i \geq 2$ can be described recursively. This is due to a well-known result of Carlitz [2], and leads to the concept of the *Carlitz rank* of permutations. For details we refer the reader to [23] and the references therein.

The Carlitz rank is a particular measure of the complexity of a permutation. The results of our paper 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 $n$.

### 6.3. Numerical results and open problem

We conclude this paper with numerical results on the discrepancy of sequences generated from permutations in $\mathcal{F}_p^{(a)}$ and $\mathcal{F}_p^{(f)}$. As described in Section 2, we can upper bound $t(S_p^\sigma)$ with $\alpha_0/\log p$, where $\alpha_0 = \max_{1\leq k\leq p} \psi_b^\sigma(k/p)$. In Table 2 we collect the parameters $a_0$ resp. pairs $a_0, a_1$ generating affine resp. fractional affine permutations in a given base $p$ with minimal and maximal value for $\alpha_0/\log p$.

Table 2. Comparison of approximations to the asymptotic discrepancy constants for affine permutations (left) and fractional affine permutations (right). Columns 2 and 4 contain the parameters $a_0$ generating an affine permutation with minimal resp. maximal value $\alpha_0/\log p$ within $\mathcal{F}_p^{(a)}$. Column 6 and 8 contain the parameters $a_0, a_1$ for the fractional affine permutations having minimal resp. maximal value $\alpha_0/\log p$ within $\mathcal{F}_p^{(f)}$.

| $p$ | $a_0$ | $\frac{\alpha_0}{\log p}$ | $a_0$ | $\frac{\alpha_0}{\log p}$ | $a_0, a_1$ | $\frac{\alpha_0}{\log p}$ | $a_0, a_1$ | $\frac{\alpha_0}{\log p}$ |
|---|---|---|---|---|---|---|---|---|
| 13 | 5 | 0.4798 | 1 | 1.2596 | $4, 2$ | 0.5098 | $1, 2$ | 1.1996 |
| 17 | 5 | 0.5813 | 1 | 1.4949 | $6, 3$ | 0.6436 | $5, 8$ | 1.3288 |
| 19 | 7 | 0.5005 | 1 | 1.6087 | $2, 1$ | 0.5362 | $5, 11$ | 1.5730 |
| 23 | 5 | 0.5546 | 1 | 1.8303 | $10, 13$ | 0.7071 | $4, 6$ | 1.4282 |
| 29 | 8 | 0.5120 | 1 | 2.1505 | $13, 18$ | 0.7065 | $12, 0$ | 1.5975 |
| 31 | 12 | 0.4884 | 1 | 2.2545 | $2, 1$ | 0.6575 | $4, 0$ | 1.6720 |
| 37 | 8 | 0.5389 | 1 | 2.5598 | $4, 19$ | 0.7035 | $3, 16$ | 1.9161 |
| 41 | 16 | 0.5122 | 1 | 2.7585 | $2, 5$ | 0.7618 | $7, 15$ | 2.0229 |
| 43 | 12 | 0.5193 | 1 | 2.8565 | $2, 9$ | 0.7605 | $5, 7$ | 1.9662 |
| 47 | 13 | 0.4973 | 1 | 3.0504 | $14, 29$ | 0.7626 | $2, 17$ | 2.2215 |
| 53 | 14 | 0.5417 | 1 | 3.3361 | $4, 15$ | 0.7080 | $25, 27$ | 2.3096 |
| 59 | 25 | 0.5320 | 1 | 3.6163 | $4, 28$ | 0.8188 | $16, 25$ | 2.2612 |
| 61 | 22 | 0.5263 | 1 | 3.7086 | $21, 0$ | 0.7417 | $5, 1$ | 2.1295 |
| 67 | 18 | 0.5111 | 1 | 3.9827 | $9, 38$ | 0.6992 | $14, 19$ | 2.4066 |
| 71 | 26 | 0.5022 | 1 | 4.1632 | $27, 12$ | 0.8689 | $1, 15$ | 2.6168 |
| 73 | 27 | 0.4853 | 1 | 4.2528 | $33, 53$ | 0.8844 | $2, 37$ | 2.3882 |
| 79 | 29 | 0.4693 | 1 | 4.5193 | $16, 8$ | 0.8806 | $20, 7$ | 2.9085 |
| 83 | 30 | 0.5344 | 1 | 4.9651 | $33, 37$ | 0.9515 | $3, 0$ | 2.4320 |
| 89 | 34 | 0.4505 | 1 | 4.9563 | $35, 62$ | 0.8636 | $30, 37$ | 2.6233 |
| 97 | 35 | 0.5047 | 1 | 5.3003 | $20, 42$ | 0.9802 | $16, 31$ | 2.4743 |

While there is an absolute constant $K$ such that we can find a parameter $a_0$ for infinitely many $p$ with $t(S_p^\sigma) < K$, $\sigma \in \mathcal{F}_p^{(a)}$, we conjecture that such a result does not hold for affine fractional permutations. That is, even if $t(S_p^\pi) < t(S_p^{id})$ for all $\pi$ we conjecture that there exists a constant $\kappa(p)$ that depends on $p$ such that $\kappa(p) < t(S_p^\pi)$ for all affine fractional permutations $\pi$ with $\kappa(p) \to \infty$ when $p \to \infty$; see also the numerical values in Table 2. A result of this kind was shown in [21] for the particular set of affine permutations for which $a_0$ either divides $p-1$ or $p+1$.

## REFERENCES


[1] BOURGAIN, J.—KONTOROVICH, A.: *On Zaremba's conjecture*, Ann. of Math. **180** (2014), no. 2. 1–6

[2] CARLITZ, L.: *Permutations in a finite field*, Proc. Amer. Math. Soc. **4** (1953), 538.

[3] CHAIX, H.—FAURE, H.: *Discrépance et diaphonie en dimension un*, Acta Arith. **63** (1993), 103–141.

[4] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences*. Cambridge Univ. Press, Cambridge, England, 2010.

[5] DRMOTA, M.—TICHY, R. F.: *Sequences, Discrepancies and Applications*. In: Lecture Notes in Math. Vol. 1651. Springer-Verlag, Berlin, 1997.

[6] FAURE, H.: *Discrépance de suites associées à un système de numération (en dimension un)*, Bull. Soc. Math. France **109** (1981), no 2, 143–182.

[7] ______ *Good permutations for extreme discrepancy*, J. Number Theory **42** (1992), 47–56.

[8] ______ Irregularities of distribution of digital $(0,1)$-sequences in prime base, Integers **5** (2005), no. 3, A7, 12 pages.

[9] ______ *Selection criteria for (random) generation of digital $(0,s)$-sequences*. In: Monte Carlo and Quasi-Monte Carlo Methods 2004, (H. Niederreiter and D. Talay, eds.), Springer-Verlag, Berlin (2006), pp. 113–126.

[10] ______ *Star extreme discrepancy of generalized two-dimensional Hammersley point sets*, Unif. Distrib. Theory **3** (2008), no. 2, 45–65.

[11] FAURE, H—KRITZER, P.—PILLICHSHAMMER, F.: *From van der Corput to modern constructions of sequences for quasi-Monte Carlo rules*, Indag. Math. **26** (2015), 760–822.

[12] FAURE, H.—LEMIEUX, C.: *Generalized Halton Sequences in 2008: A Comparative Study*, ACM Trans. Model. Comp. Sim. **19** (2009), no. 15, 1–31.

[13] HUANG, S.: *An Improvement to Zaremba's Conjecture*. Geometric and Functional Analysis **25** (2015), 860–914.

[14] KHINCHIN, A. YA.: *Continued Fractions*. The University of Chicago Press, Chicago, Ill.-London, 1964.

[15] KUIPERS, L.—NIEDERREITER, H.: *Uniform Distribution of Sequences*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974.

[16] LARCHER, G.: *On the discrepancy of sequences in the unit-interval*, Indag. Math., New Series **27** (2016), 546–558.

[17] MATOUŠEK, J.: *On the $L_2$-discrepancy for anchored boxes*, J. Complexity **14** (1998), 527–556.

[18] NIEDERREITER, H.: *Applications of diophantine approximations to numerical integration*, In: Diophantine Approximation and Its Applications, (C.F. Osgood, ed.), Academic Press, New York, 1973, pp. 129–199.

[19] ______ *Random Number Generation and Quasi-Monte Carlo Methods*. In: CBMS-NSF Regional Conference Series in Applied Mathematics, Vol. 63, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[20] 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, (P. L'Ecuyer, and A. B. Owen, eds.), Springer-Verlag, Berlin, 2009, pp. 561–572.

[21] PAUSINGER, F.: *Weak multipliers for generalized van der Corput sequences*, J. Théor. Nombres Bordeaux **24** (2012), no. 3, 729–749.

[22] SCHMIDT,W. M.: *Irregularities of distribution VII*, Acta Arith. **21** (1972), 45–50.

[23] TOPUZOĞLU, A.: *The Carlitz rank of permutations of finite fields: a survey*, J. Symb. Comput. **64** (2014), 53–66.

[24] ZAREMBA, S. K.: *La méthode des bons treillis pour le calcul des intégrals multiples*. In: Applications of Number Theory to Numerical Analysis, (S. K. Zaremba, ed.), (Proc. Sympos., Univ. Montreal, Montreal, Que., 1971), Academic Press, New York, 1972, pp. 39–119.

Received March 31, 2017
Accepted July 10, 2017

**Florian Pausinger**
*Technical University of Munich*
*Zentrum Mathematik (M10)*
*Boltzmannstr. 3*
*85748 Garching*
*Germany*
*E-mail*: florian.pausinger@gmx.at

**Alev Topuzoğlu**
*Sabancı University*
*MDBF, Orhanlı*
*34965 Tuzla, Istanbul*
*TURKEY*
*E-mail*: alev@sabanciuniv.edu