Extensions of Atanassov's methods for Halton sequences

Henri Faure, Christiane Lemieux, and Xiaoheng Wang

Abstract We extend Atanassov's methods for Halton sequences in two different directions: (1) in the direction of Niederreiter $(t,s)-$sequences, (2) in the direction of generating matrices for Halton sequences. It is quite remarkable that Atanassov's method for *classical* Halton sequences applies almost "word for word" to $(t,s)-$sequences and gives an upper bound quite comparable to those of Sobol', Faure, and Niederreiter. But Atanassov also found a way to improve further his bound for classical Halton sequences by means of a clever scrambling producing sequences which he named *modified* Halton sequences. We generalize his method to nonsingular upper triangular matrices in the last part of this article.

1 Introduction

Halton sequences and their generalizations are a popular class of low-discrepancy sequences. Their relevance in practical settings has been enhanced by various improvements that have been proposed over the years (see [8] for a survey). But it is the remarkable result published by E. Atanassov in 2004 [1] that has increased their appeal from a theoretical point of view. In Theorem 2.1 of this paper, Atanassov reduced by a factor of $s!$ the value of the hidden constant c_s in the discrepancy bound of these sequences. His proof relies on a result from diophantine geometry, and as such, provides a new approach to study the behavior of low-discrepancy sequences. The purpose of this paper is to explore how this approach can be extended to other constructions.

Henri Faure
Institut de Mathématiques de Luminy, Marseille, France, e-mail: faure@iml.univ-mrs.fr

Christiane Lemieux
University of Waterloo, Waterloo, Canada, e-mail: clemieux@uwaterloo.ca

Xiaoheng Wang
Harvard University, Cambridge, MA, USA, e-mail: xwang@math.harvard.edu

Our contribution is to first extend Atanassov's methods to $(t,s)-$sequences, including Sobol' and Faure sequences, and then to a more general class of Halton sequences which makes use of generating matrices.

It is quite remarkable that Atanassov's method for the original Halton sequences applies almost "word for word" to $(t,s)-$sequences in the narrow sense (as defined in [16]) and gives an upper bound that is comparable to those of Sobol', Faure, and Niederreiter, with the same leading term. The details are provided in Section 3, after first reviewing Halton and (t,s)-sequences in Section 2. This method also applies to extensions of these sequences introduced by Tezuka [17, 18]) and Niederreiter–Xing [16] as shown in our recently submitted work [9].

In [1], Atanassov also introduces a family of sequences called *modified Halton sequences*, and proves that an even better behavior for the constant c_s holds in that case. So far, this approach has no equivalent for $(t,s)-$sequences. In fact, this method works for Halton sequences and gives asymptotic improvements thanks to the structure of these sequences, which is completely different from the structure of $(t,s)-$sequences.

However, what we propose to do here is to extend these modified Halton sequences, which rely on so-called *admissible integers*, by using what we call *admissible matrices*. As shown later in Section 4, the same improved behavior holds for this more general construction.

Another direction for generalizations would be to consider a larger family including both Halton and $(t,s)-$sequences. Until now, attempts in this direction have been disappointing, except in the almost trivial case of $(0,s)-$sequences in variable base which, in fact, are very close to original Halton sequences (see [7] and [11] more recently, where many other references are given).

We end the introduction with a review of the notion of discrepancy, which will be used throughout the paper. Various types exist but here, for short, we only consider the so-called *extreme discrepancy*, which corresponds to the worst case error in the domain of complexity of multivariate problems. Assume we have a point set $\mathscr{P}_N = \{X_1,\dots,X_N\} \subseteq I^s = [0,1]^s$ and denote $\mathscr{J}$ (resp $\mathscr{J}^*$) the set of intervals J of I^s of the form $J = \prod_{j=1}^s [y_j, z_j)$, where $0 \le y_j < z_j \le 1$ (resp. $J = \prod_{j=1}^s [0, z_j)$). Then the *discrepancy function* of $\mathscr{P}_N$ on J is the difference

$$E(J;N) = A(J;\mathscr{P}_N) - NV(J),$$

where $A(J;\mathscr{P}_N) = \#\{n; 1 \le n \le N, X_n \in J\}$ is the number of points in $\mathscr{P}_N$ that fall in the subinterval J, and $V(J) = \prod_{j=1}^s (z_j - y_j)$ is the volume of J.

Then, the *star (extreme) discrepancy* D^* and the *(extreme) discrepancy* D of $\mathscr{P}_N$ are defined by

$$D^*(\mathscr{P}_N) = \sup_{J\in\mathscr{J}^*} |E(J;N)| \quad \text{and} \quad D(\mathscr{P}_N) = \sup_{J\in\mathscr{J}} |E(J;N)|.$$

It is well known that $D^*(\mathscr{P}_N) \le D(\mathscr{P}_N) \le 2^s D^*(\mathscr{P}_N)$. For an infinite sequence X, we denote by $D(N,X)$ and $D^*(N,X)$ the discrepancies of its first N points. Note that several authors have a $1/N$ factor when defining the above quantities.

A sequence satisfying $D^*(N,X) \in O((\log N)^s)$ is typically considered to be a *low-discrepancy sequence*. But the constant hidden in the O notation needs to be made explicit to make comparisons possible across sequences. This is achieved in many papers with an inequality of the form

$$D^*(N,X) \leq c_s(\log N)^s + O((\log N)^{s-1}). \tag{1}$$

As mentioned before, the constant c_s in this inequality is the main object of study in [1], as well as in the present paper.

2 Review of Halton and $(t,s)-$sequences

2.1 Generalized Halton sequences

Halton sequences are s-dimensional sequences, with values in the hybercube I^s. They are obtained using one-dimensional van der Corput sequences S_b in base b for each coordinate, defined as follows: For any integer $n \geq 1$

$$S_b(n) = \sum_{r=0}^{\infty} \frac{a_r(n)}{b^{r+1}}, \text{ where } n-1 = \sum_{r=0}^{\infty} a_r(n)\, b^r \text{ (b-adic expansion of } n-1).$$

An s-dimensional *Halton sequence* [10] $X_1, X_2, \ldots$ in I^s is defined as

$$X_n = (S_{b_1}(n), \ldots, S_{b_s}(n)), n \geq 1, \tag{2}$$

where the b_j's, for $j = 1, \ldots, s$, are pairwise coprime.

A *generalized van der Corput sequence* [4] is obtained by scrambling the digits with a sequence $\Sigma = (\sigma_r)_{r\geq 0}$ of permutations of $\mathbb{Z}_b = \{0, 1, \ldots, b-1\}$:

$$S_b^{\Sigma}(n) = \sum_{r=0}^{\infty} \frac{\sigma_r\big(a_r(n)\big)}{b^{r+1}}. \tag{3}$$

If the same permutation σ is used for all digits, (i.e., if $\sigma_r = \sigma$ for all $r \geq 0$), then we use the notation S_b^{σ} to denote S_b^{Σ}. The van der Corput sequence S_b is obtained by taking $\sigma_r = id$ for all $r \geq 0$, where id stands for the identity permutation over $\mathbb{Z}_b$.

A *generalized Halton sequence* [6] $X_1, X_2, \ldots$ in I^s is defined by choosing s generalized van der Corput sequences:

$$X_n = (S_{b_1}^{\Sigma_1}(n), \ldots, S_{b_s}^{\Sigma_s}(n)),\ n \geq 1, \tag{4}$$

where the b_j's are pairwise coprime bases. In applications, these b_j's are usually chosen as the first s prime numbers. In this case, we denote the jth base as p_j.

Throughout the paper, we denote respectively by H and GH the Halton and generalized Halton sequence defined by (2) and (4), in which case, to avoid some dif-

ficulties, for $1 \le j \le s$, the sequence $\Sigma_j = (\sigma_{j,r})_{r\ge 0}$ satisfies $\sigma_{j,r}(0) \ne b_j - 1$ for infinitely many r. Various bounds for the discrepancy of Halton sequences have been obtained since their introduction by Halton — by Meijer, Faure, Niederreiter — all of them by refinements of the same idea. But the major theoretical improvement goes back to Atanassov [1, Theorem 2.1], with a completely different proof using an argument of diophantine geometry:

$$D^*(N,GH) \le \frac{1}{s!}\prod_{j=1}^{s}\left(\frac{(b_j-1)\log N}{2\log b_j}+s\right)+\sum_{k=0}^{s-1}\frac{b_{k+1}}{k!}\prod_{j=1}^{k}\left(\left\lfloor\frac{b_j}{2}\right\rfloor\frac{\log N}{\log b_j}+k\right)+u, \tag{5}$$

where $u = 0$ when all bases b_j are odd, and

$$u = \frac{b_j}{2(s-1)!}\prod_{1\le i\le s, i\ne j}\left(\frac{(b_i-1)\log N}{2\log b_i}+s-1\right)$$

if b_j is the even number among them. Therefore estimate (1) holds with constant

$$c_s = \frac{1}{s!}\prod_{j=1}^{s}\frac{b_j-1}{2\log b_j}. \tag{6}$$

By making the constant c_s smaller by a factor $s!$ compared to previously established bounds, it is going to 0, instead of infinity, as s goes to infinity!

2.2 $(t,s)-$*sequences*

The concept of $(t,s)-$sequences has been introduced by Niederreiter to give a general framework for various constructions including Sobol' and Faure sequences.

Definition 1. Given an integer $b \ge 2$, an *elementary interval* in I^s is an interval of the form $\prod_{i=1}^{s}[a_i b^{-d_i},(a_i+1)b^{-d_i})$ where a_i, d_i are nonnegative integers with $0 \le a_i < b^{d_i}$ for $1 \le i \le s$.
Given integers t, m with $0 \le t \le m$, a $(t,m,s)-$*net in base* b is an s-dimensional set with b^m points such that any elementary interval in base b with volume b^{t-m} contains exactly b^t points of the set.
An s-dimensional sequence $X_1, X_2, \ldots$ in I^s is a $(t,s)-$*sequence* if the subset $\{X_n : kb^m < n \le (k+1)b^m\}$ is a $(t,m,s)-$net in base b for all integers $k \ge 0$ and $m \ge t$.

Further generalizations by Niederreiter and Xing would require an extension of that definition with the so-called truncation operator. To avoid the additional developments required to explain these, we leave them out. Issues related to the construction of these sequences and the optimization of the quality parameter t are not relevant for our purpose in Section 3. But since we will use the digital method with generating matrices for Halton sequences in Section 4, we now briefly recall that method for constructing $(t,s)-$sequences in base b.

A *linearly scrambled* van der Corput sequence is obtained by choosing an $\infty \times \infty$ matrix $C = (C_{r,l})_{r\geq 0, l\geq 0}$ with elements in $\mathbb{Z}_b$, and then defining the nth term of this one-dimensional sequence as

$$S_b^C(n) = \sum_{r=0}^{\infty} y_{n,r} b^{-(r+1)} \quad \text{with} \quad y_{n,r} = \sum_{l=0}^{\infty} C_{r,l} a_l(n) \bmod b, \tag{7}$$

where $a_r(n)$ is the r-th digit of the b-adic expansion of $n-1 = \sum_{r=0}^{\infty} a_r(n)\, b^r$.

Then, in arbitrary dimension s, one has to choose s linearly scrambled van der Corput sequences with generating matrices $C_1, \ldots, C_s$ to define the so-called *digital sequence* $(S_b^{C_1}, \ldots, S_b^{C_s})$ as proposed by Niederreiter in [14]. Of course the generating matrices must satisfy strong properties to produce low-discrepancy sequences. Special cases are the Sobol' sequences — defined in base $b = 2$ and making use of primitive polynomials to construct the non-singular upper triangular (NUT) C_i recursively — and the Faure sequences — defined in a prime base $b \geq s$ and taking C_i as the NUT Pascal matrix in $\mathbb{Z}_b$ raised to the power $i-1$.

As to bounds for the star discrepancy, $(t,s)-$sequences satisfy estimate (1) with constant c_s (see for instance [3, 14])

$$c_s = \frac{b^t}{s!} \frac{b-1}{2\lfloor \frac{b}{2} \rfloor} \left(\frac{\lfloor \frac{b}{2} \rfloor}{\log b} \right)^s. \tag{8}$$

Note that Kritzer [12] recently improved constants c_s in (8) by a factor $1/2$ for odd $b \geq 3$ and $s \geq 2$, and by a factor $1/3$ for $b = 2$ and $s \geq 5$ (a similar result holds for even b).

3 Atanassov's method applied to $(t,s)-$sequences

In this section, we apply Atanassov's method to $(t,s)-$sequences and obtain a new proof for estimate (1) and constant (8). To do so, we need to recall an important property of $(t,s)-$sequences and lemmas used in [1], reformulated here for convenience with base b instead of bases p_i (in brackets we recall the corresponding lemmas in [1] with label A). In what follows, $\mathscr{P}_N$ denotes the set containing the first N points of a sequence X.

Property 1. (**Lemma A.3.1.**) Let X be a $(t,s)-$sequence. Let $J = \prod_{i=1}^{s} [b_i b^{-d_i}, c_i b^{-d_i})$ where b_i, c_i are integers satisfying $0 \leq b_i < c_i \leq b^{d_i}$. Then

$$A(J;\mathscr{P}_N) = k b^t (c_1 - b_1) \cdots (c_s - b_s) \text{ where } N = k b^t b^{d_1} \cdots b^{d_s} \ (k \geq 0) \quad \text{and}$$

$$|A(J;\mathscr{P}_N) - NV(J)| \leq b^t \prod_{i=1}^{s} (c_i - b_i), \text{ for any integer } N \geq 1.$$

This property directly follows from the definition of $(t,s)-$sequences and is left for the reader to verify.

Lemma 1. ***(Lemma A.3.3.)*** *Let $N \geq 1, k \geq 1$ and $b \geq 2$ be integers. For integers $j \geq 0, 1 \leq i \leq k$, let some numbers $c_j^{(i)} \geq 0$ be given, satisfying $c_0^{(i)} \leq 1$ and $c_j^{(i)} \leq c$ for $j \geq 1$, for some fixed number c. Then*

$$\sum_{(j_1,\ldots,j_k)|b^{j_1}\cdots b^{j_k}\leq N} \prod_{i=1}^{k} c_{j_i}^{(i)} \leq \frac{1}{k!}\left(c\frac{\log N}{\log b}+k\right)^k. \tag{9}$$

For convenience, all the j_i's are nonnegative unless otherwise stated.

Proof. The proof proceeds very closely to the one given for Lemma 3.3 in [1], except that here we work with a single base b rather than with s different bases. For each $m \in \{0,1,\ldots,k\}$, fix a subset $L = \{i_1,\ldots,i_m\}$ of $\{1,\ldots,k\}$ and consider the contributions of all the k-tuples $\mathbf{j}$ with $j_r > 0$ for $r \in L$, and $j_r = 0$ for $r \notin L$, with $\prod_{i=1}^{k} b^{j_i} = \prod_{i\in L} b^{j_i} \leq N$. One can verify as in [1, Lemma A.3.2] that there are $\frac{1}{m!}\left(\frac{\log N}{\log b}\right)^m$ such k-tuples, each having a contribution of

$$\prod_{i=1}^{k} c_{j_i}^{(i)} = \prod_{i\in L} c_{j_i}^{(i)} \prod_{i\notin L} c_{j_i}^{(i)} \leq \prod_{i\in L} c \prod_{i\notin L} 1 = c^m.$$

Expanding both sides of (9), the result now follows since $\frac{1}{m!} \leq \frac{1}{k!}k^{k-m}$. □

Definition 2. (**Definition A.3.2.**) Consider an interval $J \subseteq I^s$. We call a *signed splitting* of J any collection of intervals $J_1,\ldots,J_n$ and respective signs $\varepsilon_1,\ldots,\varepsilon_n$ equal to ± 1, such that for any (finitely) additive function ν on the intervals in I^s, we have $\nu(J) = \sum_{i=1}^{n} \varepsilon_i \nu(J_i)$.

The following lemma is taken from [1], in a slightly modified form.

Lemma 2. ***(Lemma A.3.5.)*** *Let $J = \prod_{i=1}^{s}[0, z^{(i)})$ be an s-dimensional interval and, for each $1 \leq i \leq s$, let $n_i \geq 0$ be given integers. Set $z_0^{(i)} = 0$, $z_{n_i+1}^{(i)} = z^{(i)}$ and, if $n_i \geq 1$, let $z_j^{(i)} \in [0,1]$ be arbitrary given numbers for $1 \leq j \leq n_i$. Then the collection of intervals $\prod_{i=1}^{s}[\min(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}), \max(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}))$, with signs $\varepsilon(j_1,\ldots,j_s) = \prod_{i=1}^{s} sgn(z_{j_i+1}^{(i)} - z_{j_i}^{(i)})$, for $0 \leq j_i \leq n_i$, is a signed splitting of J.*

Now we have all the ingredients to prove the following theorem:

Theorem 1. *The discrepancy bound for a $(t,s)-$sequence X in base b satisfies*

$$D^*(N,X) \leq \frac{b^t}{s!}\left(\left\lfloor\frac{b}{2}\right\rfloor\frac{\log N}{\log b}+s\right)^s + b^t\sum_{k=0}^{s-1}\frac{b}{k!}\left(\left\lfloor\frac{b}{2}\right\rfloor\frac{\log N}{\log b}+k\right)^k. \tag{10}$$

Proof. As in [5] and [1], we will use special numeration systems in base b — using signed digits a_j bounded by $\lfloor \frac{b}{2} \rfloor$— to expand reals in $[0,1)$. That is, we write $z \in [0,1)$ as

$$z = \sum_{j=0}^{\infty} a_j b^{-j} \begin{cases} \text{with } |a_j| \le \frac{b-1}{2} \text{ if } b \text{ is odd} \\ \text{with } |a_j| \le \frac{b}{2} \text{ and } |a_j| + |a_{j+1}| \le b-1 \text{ if } b \text{ is even.} \end{cases} \tag{11}$$

The existence and unicity of such expansions are obtained by induction, see [1, p. 21–22] or [19, p. 12–13] where more details are given. For later use, it is worth pointing out that the expansion starts at b^0 and as a result, it is easy to see that a_0 is either 0 or 1.

Now we can begin the proof: Pick any $\mathbf{z} = (z^{(1)}, \dots, z^{(s)}) \in [0,1)^s$. Expand each $z^{(i)}$ as $\sum_{j=0}^{\infty} a_j^{(i)} b^{-j}$ according to our numeration systems (11) above.
Let $n := \left\lfloor \frac{\log N}{\log b} \right\rfloor$ and define $z_0^{(i)} = 0$ and $z_{n+1}^{(i)} = z^{(i)}$. Consider the numbers $z_k^{(i)} = \sum_{j=0}^{k-1} a_j^{(i)} b^{-j}$ for $k = 1, \dots, n$. Applying Lemma 2 with $n_i = n$, we expand $J = \prod_{i=1}^{s} [0, z^{(i)})$ using $(z_j^{(i)})_{j=1}^{n+1}$, obtaining a signed splitting

$$I(\mathbf{j}) = \prod_{i=1}^{s} [\min(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}), \max(z_{j_i}^{(i)}, z_{j_i+1}^{(i)})), \qquad 0 \le j_i \le n, \tag{12}$$

and signs $\varepsilon(j_1, \dots, j_s) = \prod_{i=1}^{s} \operatorname{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)})$, where $\mathbf{j} = (j_1, \dots, j_s)$.
Since V and $A(\,.\,; \mathscr{P}_N)$ are both additive, so is any scalar linear combination of them, and hence $A(J; \mathscr{P}_N) - NV(J)$ may be expanded as

$$A(J; \mathscr{P}_N) - NV(J) = \sum_{j_1=0}^{n} \cdots \sum_{j_s=0}^{n} \varepsilon(\mathbf{j}) \left(A(I(\mathbf{j}); \mathscr{P}_N) - NV(I(\mathbf{j})) \right) =: \Sigma_1 + \Sigma_2 \tag{13}$$

where we rearrange the terms so that in Σ_1 we put the terms $\mathbf{j}$ such that $b^{j_1} \cdots b^{j_s} \le N$ (that is $j_1 + \cdots + j_s \le n$) and in Σ_2 the rest. Notice that in Σ_1, the j_i's are small, so the corresponding $I(\mathbf{j})$ is bigger. Hence, Σ_1 deals with the coarser part whereas Σ_2 deals with the finer part.

It is easy to deal with Σ_1: from Property 1 and since $z_{k+1}^{(i)} - z_k^{(i)} = a_k^{(i)} b^{-k}$, we have that

$$|A(I(\mathbf{j}); \mathscr{P}_N) - NV(I(\mathbf{j}))| \le b^t \prod_{i=1}^{s} |z_{j_i+1}^{(i)} - z_{j_i}^{(i)}| \, b^{j_i} = b^t \prod_{i=1}^{s} |a_{j_i}^{(i)}|. \tag{14}$$

Hence, applying Lemma 1 with $k = s$, $c_j^{(i)} = |a_j^{(i)}|$ and $c = \lfloor \frac{b}{2} \rfloor$, we obtain

$$|\Sigma_1| \le \sum_{\mathbf{j} | b^{j_1} \cdots b^{j_s} \le N} |A(I(\mathbf{j}); \mathscr{P}_N) - NV(I(\mathbf{j}))| \le \frac{b^t}{s!} \left(\left\lfloor \frac{b}{2} \right\rfloor \frac{\log N}{\log b} + s \right)^s$$

which is the first part of the bound of Theorem 1.

The terms gathered in Σ_2 give the second part of the bound of Theorem 1, i.e., the part in $O((\log N)^{s-1})$. The idea of Atanassov for his proof of Theorem 2.1 for Halton sequences is to divide the set of s-tuples $\mathbf{j}$ in Σ_2 into s disjoint sets included in larger ones for which Lemma 1 applies and gives the desired upper bound. His proof is very terse. It has been rewritten in detail in [19] and we refer the reader to this note for further information. Following the same approach, we can adapt the proof to $(t,s)-$sequences and get the second part of the bound of Theorem 1. $\square$

From Theorem 1 we can derive the constant c_s, which for the case where b is odd is the same as in the known bound (8), and for b even is larger than (8) by a factor $b/(b-1)$ (this has recently been improved, together with the extension to Niederreiter–Xing sequences suggested in Section 1, in our submitted work [9]).

Corollary 1. *The discrepancy of a $(t,s)-$sequence X in base b satisfies (1) with*

$$c_s = \begin{cases} \frac{b^t}{s!}\left(\frac{b-1}{2\log b}\right)^s & \text{if } b \text{ is odd} \\ \frac{b^t}{s!}\left(\frac{b}{2\log b}\right)^s & \text{if } b \text{ is even.} \end{cases}$$

4 Scrambling Halton sequences with matrices

In this section, we generalize Atanassov's methods from [1] to Halton sequences scrambled with matrices, especially the method where he uses *admissible integers* to get a smaller constant c_s. We start by the simplest case of Theorem 2.1 from [1] extended with matrices.

4.1 Halton sequences scrambled with lower triangular matrices

Our idea of scrambling Halton sequences with matrices goes back to the scrambling of Faure $(0,s)$-sequences in [18]: to improve the initial portions of these sequences that tend to not spread uniformly over $[0,1)^s$, Tezuka suggested to apply linear transformations to the generating matrices of the original sequences by mean of non-singular lower triangular (NLT) matrices $A_1,\ldots,A_s$. That is, he introduced the idea of *generalized Faure sequences*, which are based on generating matrices of the form $C_i = A_i P_i$, where P_i is the NUT Pascal matrix in $\mathbb{Z}_b$ raised to the power $i-1$. Now, going back to Halton sequences, it seems natural to use similar ideas to scramble Halton sequences, as described in the following definition (see also [13, App. B]).

Definition 3. The *linearly scrambled* Halton (LSH) sequence $(X_n)_{n\geq 1}$, based on NLT matrices $A_1,\ldots,A_s$, where A_i has entries in $\mathbb{Z}_{p_i}$, is obtained as

$$X_n = (S_{p_1}^{A_1}(n),\ldots,S_{p_s}^{A_s}(n)),\ n \geq 1,$$

where $S_b^C(n)$ was defined in (7).

Theorem 2. *An LSH sequence satisfies the discrepancy bound (1) with c_s given by (6) (the same constant as for GH sequences).*

This theorem results from an analog of [1, Lemma 3.1]. But here, the use of NLT matrices A_i implies that there might be infinitely many $y_{n,r} = b-1$ in (7). This introduces disruptions in the proof (when using elementary intervals), as it does for $(t,s)-$sequences generalized with linear scramblings [18] or with global function fields [16]. Hence, as in [16, 18], we must introduce the *truncation operator* to overcome this difficulty.
Truncation: Let $x = \sum_{r=0}^{\infty} x_r b^{-(r+1)}$ be a b–adic expansion of $x \in [0,1]$, with the possibility that $x_r = b-1$ for all but finitely many r. For every integer $m \geq 1$, we define the m-truncation of x by $[x]_{b,m} = \sum_{r=0}^{m} x_r b^{-(r+1)}$ (depending on x via its expansion). In the multi-dimensional case, the truncation is defined coordinate-wise.
Next, we define an *elementary interval in bases* $p_1, \ldots, p_s$, i. e., an interval of the form

$$\prod_{i=1}^{s} [l_i p_i^{-d_i}, (l_i+1) p_i^{-d_i}), \text{ where } d_i \geq 0 \text{ and } 0 \leq l_i < p_i^{d_i} \text{ are given integers.} \quad (15)$$

In order to establish our discrepancy bound for an LSH sequence, we first need to work with the truncated version of the sequence, and to do so the following definition is useful.

Definition 4. Let $(S_{p_1}^{A_1}, \ldots, S_{p_s}^{A_s})$ be an LSH sequence. We define

$$[\mathscr{P}_N] = \{([S_{p_1}^{A_1}(n)]_{p_1,D_1}, \ldots, [S_{p_s}^{A_s}(n)]_{p_s,D_s}), 1 \leq n \leq N\}, \text{ where } D_i = \lceil \log N / \log p_i \rceil.$$

We refer to $[\mathscr{P}_N]$ as the first N points of a truncated version of the sequence.

The next result, about $A(J;[\mathscr{P}_N])$ viewed as a function of N, would be trivial without the truncation operator.

Lemma 3. *Let $(S_{p_1}^{A_1}, \ldots, S_{p_s}^{A_s})$ be an LSH sequence and J be an interval of the form $\prod_{i=1}^{s} [b_i p_i^{-d_i}, c_i p_i^{-d_i})$ with integers b_i, c_i satisfying $0 \leq b_i < c_i \leq p_i^{d_i}$. Then for $N \geq p_1^{d_1} \cdots p_s^{d_s}$, $A(J;[\mathscr{P}_N])$ is an increasing function of N.*

Proof. Let $D_i = \lceil \log N / \log p_i \rceil$. If $N \geq p_1^{d_1} \cdots p_s^{d_s}$, then $D_i \geq d_i$ for all i. Therefore as N increases, there can only be more points (from the truncated sequence) inside a particular interval J. The reason why we have to make sure $D_i \geq d_i$ for all i is that otherwise, as N increases some points could leave the interval J as more precision is added on their digital expansion, but once the precision D_i is greater than the precision d_i used to define the interval, then this can no longer happen. □

We then establish the following lemma, analog of [1, Lemma 3.1] and Property 1.

Lemma 4. *Let $(S_{p_1}^{A_1},\dots,S_{p_s}^{A_s})$ be an LSH sequence. Then for any integer $k\geq 0$, any elementary interval as in (15) contains exactly one point of the point set*

$$\left\{\left([S_{p_1}^{A_1}(n)]_{p_1,d_1},\dots,[S_{p_s}^{A_s}(n)]_{p_s,d_s}\right)\ ;\ kp_1^{d_1}\cdots p_s^{d_s}+1\leq n\leq (k+1)p_1^{d_1}\cdots p_s^{d_s}\right\}.$$

Moreover, for all intervals of the form $J=\prod_{i=1}^s[b_ip_i^{-d_i},c_ip_i^{-d_i})$ with integers b_i,c_i satisfying $0\leq b_i<c_i\leq p_i^{d_i}$, we have for all $k\geq 0$

$$A(J;[\mathscr{P}_N])=k(c_1-b_1)\cdots(c_s-b_s),\ \textit{where } N=kp_1^{d_1}\cdots p_s^{d_s}.$$

Proof. For short, write $X_n^{(i)}:=S_{p_i}^{A_i}(n)$ for all $1\leq i\leq s$. First, the condition on n implies that the digits $a_r(n)$ from the expansion of $n-1$ are uniquely determined for $r\geq p_1^{d_1}\cdots p_s^{d_s}$.
Then, it is easy to see that the digits $y_{n,r}^{(i)}$ $(0\leq r<d_i)$ defining $[X_n^{(i)}]_{p_i,d_i}$ are uniquely determined by the integers d_i,l_i describing a given elementary interval.
Now, since A_i is an NLT matrix, the $d_i\times d_i$ linear system in the unknowns $a_r(n)$ $(0\leq r<d_i)$ given by

$$A_i\left(a_0(n),\dots,a_{d_i-1}(n)\right)^T=(y_{n,0}^{(i)},\dots,y_{n,d_i-1}^{(i)})^T,$$

also has a unique solution and hence the digits $a_r(n)$ $(0\leq r<d_i)$ are uniquely determined, which means that n is unique modulo $p_i^{d_i}$ for all $1\leq i\leq s$.
Finally, applying the Chinese remainder theorem, we obtain that n is unique modulo $p_1^{d_1}\cdots p_s^{d_s}$. Together with the condition $kp_1^{d_1}\cdots p_s^{d_s}+1\leq n\leq(k+1)p_1^{d_1}\cdots p_s^{d_s}$, all digits $a_r(n)$ $(r\geq 0)$ are unique and so is n, which ends the proof of the first part of Lemma 4. The second part simply results from the fact that J splits into $(c_1-b_1)\cdots(c_s-b_s)$ disjoint elementary intervals. □

We also need the following lemma, another result that would be trivial without the truncation.

Lemma 5. *Let $(S_{p_1}^{A_1},\dots,S_{p_s}^{A_s})$ be an LSH sequence and J be an interval of the form $J=\prod_{i=1}^s[b_ip_i^{-d_i},c_ip_i^{-d_i})$ with integers b_i,c_i satisfying $0\leq b_i<c_i\leq p_i^{d_i}$. If $N<p_1^{d_1}\cdots p_s^{d_s}$ then $A(J;[\mathscr{P}_N])\leq(c_1-b_1)\cdots(c_s-b_s)$.*

Proof. Define $\tilde{d}_i=\min(D_i,d_i)$. Let $[J]$ be defined as the smallest interval of the form $\prod_{i=1}^s[\tilde{b}_ip_i^{-\tilde{d}_i},\tilde{c}_ip_i^{-\tilde{d}_i})$ with $0\leq\tilde{b}_i<\tilde{c}_i\leq p_i^{\tilde{d}_i}$ and such that $J\subseteq[J]$. We can see that $[J]$ is obtained by using $\tilde{c}_i=\lceil c_i/p_i^{\tilde{d}_i-d_i}\rceil$ and $\tilde{b}_i=\lfloor b_i/p_i^{\tilde{d}_i-d_i}\rfloor$. Using the same arguments as in the proof of the previous lemma, we have that each interval of the form $\prod_{i=1}^s[l_ip_i^{-\tilde{d}_i},(l_i+1)p_i^{-\tilde{d}_i})$ has at most one point from $[\mathscr{P}_N]$. Hence

$$A(J;[\mathscr{P}_N])\leq A([J];[\mathscr{P}_N])\leq\prod_{i=1}^s(\tilde{c}_i-\tilde{b}_i)\leq\prod_{i=1}^s(c_i-b_i),$$

where the last inequality follows from the definition of $\tilde{b}_i$ and $\tilde{c}_i$. □

Now, we can give the proof of Theorem 2.

Proof. From Lemma 3 and the second part of Lemma 4, we obtain that for every $N \geq p_1^{d_1} \cdots p_s^{d_s}$ and $J = \prod_{i=1}^{s} [b_i p_i^{-d_i}, c_i p_i^{-d_i})$

$$|A(J;[\mathscr{P}_N]) - NV(J)| \leq (c_1 - b_1) \cdots (c_s - b_s). \tag{16}$$

Further, Lemma 5 proves that (16) also holds when $N < p_1^{d_1} \cdots p_s^{d_s}$.

The inequality (16) is similar to the result stated in Lemma A.3.1 from [1], but note that here it applies to the truncated sequence. From that point, we can proceed as in Atanassov's proof of his Theorem 2.1, which consists in breaking down $A(J;[\mathscr{P}_N]) - NV(J)$ into a sum $\Sigma_1 + \Sigma_2$ as done in (13), and then bound each term separately. Note however that in our case, the obtained bound applies to the truncated version of the sequence. But as discussed in [15, 16], it is easy to show that if a bound of the form (1) applies to the truncated version of a sequence, it applies to the untruncated version as well (with the same constant c_s). □

4.2 Scrambling Halton sequences with admissible matrices

In this section, we show that by using admissible integers to construct the matrices A_i of an LSH sequence, we obtain sequences satisfying the same improved discrepancy bound as in [1, Theorem 2.3], obtained there for modified Halton sequences, which use permutations based on admissible integers. We first need a few definitions, including that of admissible integers and the "generating–matrices" analog of these integers, which we call "admissible matrices".

Definition 5. Given non-negative integers $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_s$ and $k_1, \ldots, k_s$, we define the quantity

$$P_i^{(\beta_i)}(k_i;(\alpha_1,\ldots,\alpha_s)) := k_i^{\alpha_i+\beta_i} \prod_{1\leq j\leq s, j\neq i} p_j^{\alpha_j} \bmod p_i, \qquad i = 1,\ldots,s. \tag{17}$$

Definition 6. We say that $k_1, \ldots, k_s$ are *admissible* for the primes $p_1, \ldots, p_s$ if $p_i \nmid k_i$ and for each set of integers $(b_1, \ldots, b_s)$, $p_i \nmid b_i$, there exists a set of integers $(\alpha_1, \ldots, \alpha_s)$ such that

$$P_i^{(0)}(k_i;(\alpha_1,\ldots,\alpha_s)) \equiv b_i \bmod p_i, \quad i = 1,\ldots,s.$$

Lemma A.4.1. Let $p_1, \ldots, p_s$ be distinct primes. Then there exist admissible integers $k_1, \ldots, k_s$.

Definition 7. Let $A_1, \ldots, A_s$ be NLT matrices in distinct prime bases $p_1, \ldots, p_s$ and let $k_1, \ldots, k_s$ be admissible integers for these bases. Then the matrices $A_i, i = 1, \ldots, s$ are *admissible* if the jth entry on their diagonal has the form $k_i^{\beta_i+j}$, $j \geq 1$, where

$\beta_1,\ldots,\beta_s$ are non-negative integers. An LSH sequence based on admissible matrices $A_1,\ldots,A_s$ is called a *modified linearly scrambled Halton* (MLSH) sequence.

Atanassov's modified Halton sequence corresponds to the case where A_i is diagonal and $\beta_i = 0$ for all i, while if we take A_i diagonal and $\beta_i = 1$, then we obtain the sequences used in the experiments in [2] (where the authors also apply digital shifts chosen independently $(\bmod p_i)$). It is important to take $\beta_i \geq 1$ for applications in QMC methods, otherwise the sequences behave like original Halton sequences in the usual ranges of sample sizes [8, Section 3, Paragraph 2].

We can now state the main result of this section.

Theorem 3. *The discrepancy of an MLSH sequence based on distinct primes bases $p_1,\ldots,p_s$, non-negative integers $\beta_1,\ldots,\beta_s$ and admissible integers $k_1,\ldots,k_s$ satisfies the bound (1) with constant*

$$c_s(p_1,\ldots,p_s) = \frac{1}{s!}\sum_{i=1}^{s}\log p_i \prod_{i=1}^{s}\frac{p_i(1+\log p_i)}{(p_i-1)\log p_i}.$$

The proof of Theorem 3 follows closely that of [1, Theorem 2.3], which in turn essentially proceeds through an intermediate result called *Proposition 4.1* in [1]. Here this result must be adapted to the more general setting of admissible matrices, and is described in a slightly different version in the following proposition.

Proposition 1. *For an MLSH sequence based on distinct primes $p_1,\ldots,p_s$, non-negative integers $\beta_1,\ldots,\beta_s$ and admissible integers $k_1,\ldots,k_s$, we have that*

$$\sum_{\mathbf{j}\in T(N)} |A(I(\mathbf{j});[\mathscr{P}_N]) - NV(I(\mathbf{j}))| \leq \sum_{\mathbf{j}\in T(N)}\left(1+\sum_{\mathbf{l}\in M(\mathbf{p})}\frac{\|\sum_{i=1}^{s}(l_i/p_i)P_i^{(\beta_i)}(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) + O((\log N)^{s-1}),$$

where $T(N) = \{\mathbf{j}|p_1^{j_1}\cdots p_s^{j_s} \leq N, j_1,\ldots,j_s \geq 0\}$, $M(\mathbf{p}) = \{\mathbf{j}|0 \leq j_i \leq p_i - 1, j_1 + \cdots + j_s > 0\}$, $R(\mathbf{j}) = \prod_{i=1}^{s} r_i(j_i)$, with $r_i(m) = \max(1,\min(2m,2(p_i-m)))$ and $\|\cdot\|$ denotes the "distance to the nearest integer" function.

Before presenting the proof of this result, we first need to recall a technical lemma from [1] and an adapted version of a key lemma used in the proof of [1, Prop. 4.1].

Lemma A.4.2. Let $\mathbf{p} = (p_1,\ldots,p_s)$ and let $\omega = (\omega_n^{(1)},\ldots,\omega_n^{(s)})_{n=0}^{\infty}$ be a sequence in $\mathbb{Z}^s$. Let $\mathbf{b},\mathbf{c}$ be fixed elements in $\mathbb{Z}^s$, such that $0 \leq b_i < c_i \leq p_i$, for $1 \leq i \leq s$. For $C \geq 1$, denote by $a_C(\mathbf{b},\mathbf{c})$ the number of terms of ω among the first C such that for all $1 \leq i \leq s$, we have $b_i \leq \omega_n^{(i)} \bmod p_i < c_i$. Then

$$\sup_{\mathbf{b},\mathbf{c}}\left|a_C(\mathbf{b},\mathbf{c}) - C\prod_{i=1}^{s}\frac{c_i-b_i}{p_i}\right| \leq \sum_{\mathbf{j}\in M(\mathbf{p})}\frac{|S_C(\mathbf{j},\omega)|}{R(\mathbf{j})}, \tag{18}$$

where $S_C(\mathbf{j},\omega) = \sum_{n=0}^{C-1} e\left(\sum_{k=1}^{s}\frac{j_k\omega_n^{(k)}}{p_k}\right)$ and $e(x) = \exp(2i\pi x)$.

This result is applied in Lemma 6 below, but to the counting function $A(J;[\mathscr{P}_N])$ in place of $a_C(\mathbf{b},\mathbf{c})$. Hence, the discrepancy function will be estimated by means of a trigonometrical sum, which in turn will give the part $\|\sum_{i=1}^s (l_i/p_i)P_i^{(\beta_i)}(k_i;\mathbf{j})\|^{-1}$ in the upper bound of Proposition 1.

Lemma 6. *Let X be an MLSH sequence in bases $p_1,\dots,p_s$ as in Definition 7. Fix some elementary interval $I=\prod_{i=1}^s [a_i p_i^{-\alpha_i},(a_i+1)p_i^{-\alpha_i})$ with $0\le a_i<p_i^{\alpha_i}$, and a subinterval $J=\prod_{i=1}^s [a_i p_i^{-\alpha_i}+b_i p_i^{-\alpha_i-1},a_i p_i^{-\alpha_i}+c_i p_i^{-\alpha_i-1})$ with $0\le b_i<c_i\le p_i$. Let $N>\prod_{i=1}^s p_i^{\alpha_i}$ and let n_0 (whose existence will be proved) be the smallest integer such that $[X_{n_0}]\in I$ (the notation $[X_n]=([X_n^{(1)}]_{p_1,D_1},\dots,[X_n^{(s)}]_{p_s,D_s})$ has been introduced in Definition 4). Suppose that $[X_{n_0}]$ belongs to*

$$\prod_{i=1}^s [a_i p_i^{-\alpha_i}+d_i p_i^{-\alpha_i-1},a_i p_i^{-\alpha_i}+(d_i+1)p_i^{-\alpha_i-1}),$$

and let $\omega=\{\omega_t\}_{t=0}^\infty$ in $\mathbb{Z}^s$ be defined by $\omega_t^{(i)}=d_i+tP_i^{(\beta_i)}(k_i;(\alpha_1,\dots,\alpha_s))$. Then

1. *We have that $n_0<\prod_{i=1}^s p_i^{\alpha_i}$ and the indices n of the terms $[X_n]$ of $[\mathscr{P}_N]$ that belong to I are of the form $n=n_0+t\prod_{i=1}^s p_i^{\alpha_i}$.*
2. *For these n, $[X_n]\in J$ if and only if for some integers $(l_1,\dots,l_s)$, $l_i\in\{b_i,\dots,c_i-1\}$, the following system of congruences is satisfied by t:*

$$\omega_t^{(i)}=d_i+tP_i^{(\beta_i)}(k_i;(\alpha_1,\dots,\alpha_s))\equiv l_i \bmod p_i,\quad i=1,\dots,s. \tag{19}$$

3. *If C is the largest integer with $n_0+(C-1)\prod_{i=1}^s p_i^{\alpha_i}<N$, then*

$$|A(J;[\mathscr{P}_N])-NV(J)|<1+\sum_{\mathbf{l}\in M(\mathbf{p})}\frac{|S_C(\mathbf{l},\omega)|}{R(\mathbf{l})}.$$

Proof. We consider each of the three claims one by one.

1. This has been dealt with in the proof of Lemma 4 (first part with $k=t$), which applies here since an MLSH sequence is a special case of an LSH sequence.
2. We first note that for $[X_n]$ to be in J, for each fixed i the (α_i+1)st digit of $[X_n^{(i)}]$ must be in $\{b_i,\dots,c_i-1\}$. Hence we need to show that this digit is given by (19). By the definition of n_0, we know that $A_i\left(a_0(n_0),\dots,a_{d_i-1}(n_0)\right)^T=(*,\dots,*,d_i,*,\dots)^T$ (where d_i is the (α_i+1)st digit), $(a_0(n_0),\dots,a_{d_i-1}(n_0))$ coming from the expansion of n_0-1 in base p_i. For brevity, let $P_i:=\prod_{j=1,j\ne i}^s p_j^{\alpha_j}$ mod p_i. Since the (α_i+1)st digit of $\prod_{j=1}^s p_j^{\alpha_j}$ in base p_i is tP_i, we have that $(a_0(n),\dots,a_{d_i-1}(n))=(a_0(n_0),\dots,a_{d_i-1}(n_0))+(0,\dots,0,tP_i,*,\dots)$. Note that possible carries to higher order digits are absorbed in the stars $*$. Now,

$$\begin{aligned}A_i(a_0(n),\dots,a_{d_i-1}(n))^T&=A_i(a_0(n_0),\dots,a_{d_i-1}(n_0))^T+A_i(0,\dots,0,tP_i,*,\dots)^T\\&=(*,\dots,*,d_i,*,\dots)^T+(0,\dots,0,tk_i^{\alpha_i+\beta_i}P_i,*,\dots)\end{aligned}$$

by definition of A_i. Therefore, the first α_i digits of $[X_n^{(i)}]$ and $[X_{n_0}^{(i)}]$ are equal and the (α_i+1)st digit of $[X_n^{(i)}]$ is $d_i + tk_i^{\alpha_i+\beta_i} P_i \equiv d_i + tP_i^{(\beta_i)}(k_i;\alpha) \bmod p_i$, as desired.

3. We apply Lemma A.4.2 with $a_C(\mathbf{b},\mathbf{c}) = A(J;[\mathscr{P}_N])$ and use the inequalities

$$C\prod_{i=1}^{s}\frac{c_i-b_i}{p_i} - 1 \le NV(J) \le (1+C)\prod_{i=1}^{s}\frac{c_i-b_i}{p_i} \le 1 + C\prod_{i=1}^{s}\frac{c_i-b_i}{p_i}$$

resulting from the hypothesis of item 3. □

Proof. (**Proposition 1**) As in [19] we first consider the case where $j_i \ge 1$ for all i, as this allows use to use Lemma 6. The interval $I(\mathbf{j})$ is contained inside some elementary interval $G = \prod_{i=1}^{s}[c_i p_i^{-j_i}, (c_i+1)p_i^{-j_i})$. We define a sequence ω as in Lemma 6, where the integers d_i are determined by the condition that the first term of the sequence σ that falls in G fits into the interval

$$\prod_{i=1}^{s}[c_i p_i^{-j_i} + d_i p_i^{-j_i-1}, c_i p_i^{-j_i} + (d_i+1)p_i^{-j_i-1}). \tag{20}$$

Hence $\omega_n^{(i)} = d_i + nP_i^{(\beta_i)}(k_i,\mathbf{j})$. From part (3) of Lemma 6, it follows that

$$|A(I(\mathbf{j});[\mathscr{P}_N]) - NV(I(\mathbf{j}))| < 1 + \sum_{\mathbf{l}\in M(\mathbf{p})}\frac{|S_K(\mathbf{l},\omega)|}{R(\mathbf{l})}, \tag{21}$$

where K is the number of terms of the MLSH sequence among the first N terms that fall into G. Since the p_i's are coprime, we see that $P_i^{(\beta_i)}(k_i,\mathbf{j}) \neq 0$, in particular, it is not divisible by p_i and hence coprime to p_i. For any $\mathbf{l} \in M(\mathbf{p})$, by definition, there is an l_t, with $1 \le t \le s$ such that $l_t \neq 0$, and so $p_t \not| l_t$. These properties imply that $\alpha = \sum_{i=1}^{s}\frac{l_i}{p_i}P_i^{(\beta_i)}(k_i;\mathbf{j})$ is not an integer. Thus we have

$$\begin{aligned}|S_K(\mathbf{l},\omega)| &= \left|\sum_{n=0}^{K-1} e\left(\sum_{i=1}^{s}\frac{l_i}{p_i}(d_i + nP_i^{(\beta_i)}(k_i;\mathbf{j}))\right)\right| = \left|\sum_{n=0}^{K-1} e(n\alpha + \sum_{i=1}^{s} l_i d_i/p_i)\right| \\ &= \frac{|e(K\alpha)-1|}{|e(\alpha)-1|} \le \frac{1}{2}\left\|\sum_{i=1}^{s}\frac{l_i}{p_i}P_i^{(\beta_i)}(k_i;\mathbf{j})\right\|^{-1},\end{aligned}$$

where the last inequality is obtained by noticing that $|e(\alpha)-1| \ge 2\pi|\alpha|2/\pi = 4|\alpha|$ for $-1/2 \le \alpha \le 1/2$. Combining this result with (21), we obtain

$$\sum_{\substack{\mathbf{j}\in T(N),\\ j_i\ge 1}} |(A(I(\mathbf{j});[\mathscr{P}_N]) - NV(I(\mathbf{j}))| \le \sum_{\substack{\mathbf{j}\in T(N),\\ j_i\ge 1}}\left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})}\frac{\|\sum_{i=1}^{s}\frac{l_i}{p_i}P_i^{(\beta_i)}(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right). \tag{22}$$

In the second case, the fact that at least one j_i is 0 implies that we can use a similar approach to the one used to bound Σ_1 in Theorem 1, and the obtained bound in $O(\log^{s-1} N)$ as we are essentially working in at most $s-1$ dimensions. Observing that $T(N)$ contains the vectors $\mathbf{j}$ such that $j_i \geq 1$ for all i completes the proof.

We still need two more technical lemmas before proceeding to the proof of Theorem 2.3. The first one is directly from [1], and is useful to bound the upper bound derived in Proposition 1.

Lemma A.4.4. Let $\mathbf{p} = (p_1, \ldots, p_s)$, then

$$\sum_{\mathbf{j} \in M(\mathbf{p})} \sum_{m_1=1}^{p_1-1} \cdots \sum_{m_s=1}^{p_s-1} \frac{\| \frac{j_1 m_1}{p_1} + \ldots + \frac{j_s m_s}{p_s} \|^{-1}}{2R(\mathbf{j})} \leq \sum_{i=1}^{s} \log p_i \prod_{i=1}^{s} p_i \left(\prod_{j=1}^{s} (1 + \log p_j) - 1 \right).$$

The next one is useful to count the vectors $\mathbf{j} \in T(N)$, over which the sum that is bounded in Proposition 1 is defined. In [1, p. 30–31], this is achieved in the text of the proof but, for the sake of clarity, we prefer to state it as a last lemma.

Lemma 7. *Let $\mathbf{a} \in \mathbb{Z}^s$ be a vector of non-negative integers and let $U(\mathbf{a}) := \{\mathbf{j}\,;\, a_i K \leq j_i < (a_i+1)K$ for all $1 \leq i \leq s\}$, where $K = \prod_{i=1}^{s} (p_i - 1)$. The s functions $P_i^{(\beta_i)}(k_i;\mathbf{j})$, $1 \leq i \leq s$, are such that for each $\mathbf{b} = (b_1, \ldots, b_s) \in \mathbb{Z}^s$, with $1 \leq b_i \leq p_i - 1$ for all $1 \leq i \leq s$, there are exactly K^{s-1} s-tuples $\mathbf{j} \in U(\mathbf{a})$ such that $P_i^{(\beta_i)}(k_i;\mathbf{j}) \equiv b_i \bmod p_i$ for all $1 \leq i \leq s$.*

Proof. The proof essentially follows from the fact that the s functions $P_i^{(0)}(k_i;\mathbf{j})$ satisfy the property described in this Lemma 7 (see [1, p. 30]), and then the observation that $P_i^{(\beta_i)}(k_i;\mathbf{j}) \equiv b_i \bmod p_i$ if and only if $P_i^{(0)}(k_i;\mathbf{j}) \equiv k_i^{-\beta_i} b_i \bmod p_i$. □

We are now ready to prove Theorem 3.

Proof. As in the proof of Theorems 1 and 2, we first write the discrepancy function of $[\mathscr{P}_N]$ on J using (13) and similarly get

$$A(J;[\mathscr{P}_N]) - NV(J) = \Sigma_1 + \Sigma_2.$$

The terms gathered in Σ_2 are still in $O((\log N)^{s-1})$ and those in Σ_1 are divided in two sums bounded separately as follows:

$$\left|\sum\nolimits_1\right| \leq \sum_{\substack{\mathbf{j} \in T(N) \\ j_i > 0}} t(\mathbf{j}) + \sum_{\substack{\mathbf{j} \in T(N) \\ \text{some } j_i = 0}} t(\mathbf{j}). \tag{23}$$

Now, using Proposition 1 and the fact that each $\mathbf{j} \in T(N)$ is inside a box $U(\mathbf{a})$ such that the s-tuples $\mathbf{a}$ satisfy $\prod_{i=1}^{s} p_i^{a_i K} \leq \prod_{i=1}^{s} p_i^{j_i} \leq N$, we get that the first term on the right-hand side of (23) is bounded by

$$\sum_{\mathbf{a} \mid \prod_{i=1}^{s} p_i^{a_i \cdot K} \leq N} \sum_{\mathbf{j} \in U(\mathbf{a})} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i^{(\beta_i)}(k_i;\mathbf{j}) \|^{-1}}{2R(\mathbf{l})} \right). \tag{24}$$

We also note that the second term on the right-hand side of (23) is in $O(\log^{s-1} N)$.

We then apply Lemma A.3.3 (whose base b version is given in Lemma 1) with $c = 1$ and $p_i' = p_i^K$ and get the bound $\frac{1}{s!}\prod_{i=1}^{s}\left(\frac{\log N}{K\log p_i}+s\right)$ for the number of s-tuples $\mathbf{a}$ enumerated in the first sum of (24). Next we use Lemma 7 to enumerate and count the number of vectors $\mathbf{j}$ in $U(\mathbf{a})$ considered in the inner sum of (24). These two results together with Lemma A.4.4 give us the bound

$$\frac{1}{s!}\prod_{i=1}^{s}\left(\frac{\log N}{K\log p_i}+s\right)K^{s-1}\left(K+\sum_{i=1}^{s}\log p_i\prod_{i=1}^{s}p_i\left(-1+\prod_{i=1}^{s}(1+\log p_i)\right)\right)$$

for Σ_1. The final result can then be obtained after a few further simplifications and using the fact that, as explained in [15], a discrepancy bound holding for the truncated version of the sequence also applies to the untruncated version. □

Remark 1. The reader interested in the unfolding of the original proof by Atanassov has the choice between the text in [1, Theorem 2.3] (very terse) and its careful analysis in [19] (very detailed). With our proof of Theorem 3 in hand, we now have the opportunity to present an overview of Atanassov's proof and thus make it accessible to readers who do not wish to go over [1] or [19].

Atanassov's modified Halton sequences in bases $p_1,\ldots,p_s$, with admissible integers $k_1,\ldots,k_s$, are generalized Halton sequences in which the sequences of permutations $\Sigma_i = (\sigma_{i,r})_{r\geq 0}$ are defined by

$$\sigma_{i,r}(a) := ak_i^r \bmod p_i \quad \text{for all } 0 \leq a < p_i,\ r \geq 0,\ i = 1,\ldots,s.$$

Of course they are a special case of MLSH sequences (see definitions and comments just before Theorem 3).

The basis of the proof of Theorem A.2.3 is Proposition A.4.1 which essentially reads as Proposition 1 where $\beta_i = 0$.

Lemma A.4.1, which establishes the existence of admissible integers (using primitive roots modulo p_i), and Lemma A.4.2 have already been stated.

Lemma A.4.3 is the core of the proof. It reads as Lemma 6 where brackets have been removed, i.e., where the truncation is unnecessary, since Atanassov deals with diagonal matrices only.

Now, Lemma A.4.2 is applied in Lemma A.4.3 to the counting function $A(J;\mathscr{P}_N)$ in place of $a_C(\mathbf{b},\mathbf{c})$. Hence, as already noted, the discrepancy function is estimated by means of a trigonometrical sum, which gives the part $\|\sum_{i=1}^{s}(l_i/p_i)P_i^{(0)}(k_i;\mathbf{j})\|^{-1}$ in the upper bound of Proposition A.4.1. The end of the proof of Proposition A.4.1 together with the proof of Theorem A.2.3 are mainly the same as that of Proposition 1 and Theorem 3, respectively, where the brackets have to be removed and where $\beta_i = 0$. The only subtle difference is in the split into two cases, $j_i \geq 1$ for all i or not. This distinction was ignored by Atanassov whereas it appears crucial at a stage of the proof (see [19] for complete details).

Acknowledgements We wish to thank the referee for his/her detailed comments, which were very helpful to improve the presentation of this manuscript. The second author acknowledges the support of NSERC for this work.

References

1. E. I. Atanassov, On the discrepancy of the Halton sequences, *Math. Balkanica, New Series* **18.1-2** (2004), 15–32.
2. E. I. Atanassov and M. Durchova, Generating and testing the modified Halton sequences. In *Fifth International Conference on Numerical Methods and Applications, Borovets 2002*, Springer-Verlag (Berlin), Lecture Notes in Computer Science **2542** (2003), 91–98.
3. J. Dick and F. Pillichshammer, Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration, Cambridge University Press, UK (2010).
4. H. Faure, Discrépance de suites associées à un système de numération (en dimension *un*), *Bull. Soc. math. France* **109** (1981), 143–182.
5. H. Faure, Discrépance de suites associées à un système de numération (en dimension s), *Acta Arith.* **61** (1982), 337–351.
6. H. Faure, On the star-discrepancy of generalized Hammersley sequences in two dimensions, *Monatsh. Math.* **101** (1986), 291–300.
7. H. Faure, Méthodes quasi-Monte Carlo multidimensionnelles, *Theoretical Computer Science* **123** (1994), 131–137.
8. H. Faure and C. Lemieux, Generalized Halton sequences in 2008: A comparative study, *ACM Trans. Model. Comp. Sim.* **19** (2009), Article 15.
9. H. Faure and C. Lemieux, Improvements on the star discrepancy of $(t,s)-$sequences. Submitted for publication, 2011.
10. J. H. Halton, On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals, *Numer. Math.* **2** (1960), 184–90.
11. R. Hofer and G. Larcher, On the existence and discrepancy of certain digital Niederreiter–Halton sequences, *Acta Arith.* **141** (2010), 369–394.
12. P. Kritzer, Improved upper bounds on the star discrepancy of (t,m,s)-nets and (t,s)-sequences, *J. Complexity* **22** (2006), 336–347.
13. C. Lemieux, Monte Carlo and Quasi-Monte Carlo Sampling, Springer Series in Statistics, Springer, New York (2009).
14. H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* **104** (1987), 273–337.
15. H. Niederreiter and F. Özbudak, Low-discrepancy sequences using duality and global function fields, *Acta Arith.* **130** (2007), 79–97.
16. H. Niederreiter and C. P. Xing, Quasirandom points and global function fields, *Finite Fields and Applications*, S. Cohen and H. Niederreiter (Eds), London Math. Soc. Lectures Notes Series **233** (1996), 269–296.
17. S. Tezuka, Polynomial arithmetic analogue of Halton sequences, *ACM Trans. Modeling and Computer Simulation* **3** (1993), 99–107.
18. S. Tezuka, A generalization of Faure sequences and its efficient implementation, Technical Report RT0105, IBM Research, Tokyo Research Laboratory (1994).
19. X. Wang, C. Lemieux, H. Faure, A note on Atanassov's discrepancy bound for the Halton sequence, Technical report, University of Waterloo, Canada (2008). Available at $s$as.uwaterloo.ca/stats_navigation/techreports/08techreports.shtml.