# A NOTE ON ATANASSOV'S DISCREPANCY BOUND FOR THE HALTON SEQUENCE

by Xiaoheng WANG and Christiane LEMIEUX * and Henri FAURE

ABSTRACT. In this note, we provide a complete proof of the results presented by E. Atanassov in a 2004 paper about the discrepancy of the Halton sequence. Our proof addresses an inaccuracy found in the original proof, and fills in some non-trivial gaps.

## 1. INTRODUCTION

The Halton sequence is the oldest multidimensional low-discrepancy sequence [12]. Its star-discrepancy is in $O(\log^s N/N)$, and for about 40 years, the best bounds that were proved for the implicit constant $c_s$ in this $O$ notation were growing superexponentially fast with the dimension $s$. However, a few years ago, Atanassov published a paper [1] establishing that the constant $c_s$ was actually going to 0 with $s$ superexponentially. Furthermore, in this paper he showed (in his Theorem 2.3) that the behavior of this constant could be improved by using so-called "admissible integers" to permute the digits of the Halton sequence, thereby obtaining a form of *modified Halton sequence*.

The purpose of this note is to provide a complete, more detailed proof of Atanassov's important contributions, based on [1]. In particular, we give details for some non-trivial gaps that appear in the proofs given in [1], and make several important remarks regarding the essence of these proofs. In addition, we found there is a subtle inaccuracy in the proof of one of the intermediate results (Proposition 4.1) used in [1]. This inaccuracy can be rectified in different ways, and does not affect the end result, given in Theorem 2.3. The simplest way to deal with it is to make use of asymptotic notation in the

* The second author acknowledges the support of the National Sciences and Engineering Council of Canada.

bound given in that proposition. However, if we still want a precise bound and no asymptotic notation, then Proposition 4.1 needs to be modified, and we propose two ways of doing so. In both cases, we show how to adapt the proof of Theorem 2.3 so that the modification to Proposition 4.1 is correctly handled.

This note is organized as follows. In Section 2, we recall the definitions and main results proved in [1]. We discuss in Section 3 how the proofs of these results are organized. Sections 4 and 5 contain our detailed and corrected proofs of these results. We discuss two alternative approaches to cover the inaccuracy in the proof of Proposition 4.1 in [1] in Section 6.

*Foreword.* The results in this note are not new, but the work presented here has led to further generalizations of these results, showing the vitality of methods initiated by Atanassov. Readers interested in this subsequent works are referred to [8, 9, 10, 11, 18]. See also [6] for an updated survey to appear in 2014 relating the various aspects of Atanassov's methods and their extensions.

This note was first released in 2008 as a technical report. It has been updated first in September 2012 to overcome a small inaccuracy in the proof of Lemma 4.4 and then in November 2013 to overcome another small inaccuracy in the proof of Theorem 2.1 (Claim 3) and to add the recent related references above.

## 2. Definitions and results given in Atanassov's paper

In this section we state the results proved by Atanassov in [1] and give the required definitions and notation. For convenience, we use the same numbering as in [1] for definitions and results. The reader is referred to [2, 4, 13, 14, 16, 17] for more information on the concept of discrepancy and irregularities of distributions. A recent, comprehensive survey of low-discrepancy sequences can be found in [3], and [7] gives up-to-date results on generalized Halton sequences.

**Definition 1.1.** For every $s$-dimensional interval $J = \prod_{i=1}^{s} [c_i, d_i) \subseteq \mathbf{E}^s$ where $\mathbf{E}^s$ is the unit cube $[0,1)^s$, let $A_N(J)$ be the number of terms of the sequence $\sigma = \{x_j\}_{j=0}^{\infty}$ among the first $N$ such that $x_j \in J$, and let $\mu(J)$ be the volume of $J$. The *discrepancy* $D_N(\sigma)$ of the sequence $\sigma$ is defined to be

$$\sup_{J \subseteq \mathbf{E}^s} \left| \frac{A_N(J)}{N} - \mu(J) \right| .$$

The *star-discrepancy* $D_N^*(\sigma)$ of the sequence $\sigma$ is obtained when the supremum is taken over intervals $J \subseteq \mathbf{E}^s$ of the kind $J = \prod_{i=1}^s \left[0, d_i'\right)$. In what follows, we will always be working with $ND_N(\sigma)$ and $ND_N^*(\sigma)$. We will also reserve $s$ for the dimension.

**Definition 1.2.** Let $p \geq 2$ be a fixed integer, and let $\tau = \{\tau_j\}_{j=0}^\infty$ be a sequence of permutations of the numbers $\{0, \dots, p-1\}$. The terms of the corresponding *generalized van der Corput sequence* are obtained by representing nonnegative integers $n$ as $n = \sum_{j=0}^k a_j p^j$, $a_j \in \{0, \dots, p-1\}$, and putting

$$x_n = \sum_{j=0}^{k} \tau_j(a_j) p^{-j-1}.$$

The one-dimensional van der Corput sequence in base $p$ is obtained by setting $\tau_j(i) = i$ for $i = 0, \dots, p-1$, $j \geq 0$.

**Definition 1.3.** Let $p_1, \dots, p_s$ be pairwise relatively prime integers with $p_i \geq 2$. The *Halton sequence*

$$\sigma(p_1, \dots, p_s) = \left\{ \left(x_n^{(1)}, \dots, x_n^{(s)}\right) \right\}_{n=0}^\infty$$

is constructed by setting each sequence $\{x_n^{(i)}\}_{n=0}^\infty$ to be a van der Corput sequence in base $p_i$, for $i = 1, \dots, s$.

Before Atanassov's result, the best known upper bound on the discrepancy of the Halton sequence was as follows.

**Theorem 1.1.** Let $p_1, \dots, p_s$ be pairwise relatively prime numbers. The discrepancy of the Halton sequence $\sigma(p_1, \dots, p_s)$ satisfies

$$ND_N(\sigma) < c_s \ln^s N + O(\ln^{s-1} N), \tag{2.1}$$

with

$$c_s = 2^s \prod_{i=1}^{s} \frac{p_i - 1}{\ln p_i}.$$

This was later improved to [5]

$$c_s = \prod_{i=1}^{s} \frac{p_i - 1}{\ln p_i}.$$

The following theorem describes how Atanassov was able to further improve this result.

**Theorem 2.1.** Let $p_1, \dots, p_s$ be pairwise relatively prime numbers. The discrepancy of the Halton sequence $\sigma(p_1, \dots, p_s)$ satisfies

$$ND_N(\sigma) \leq \frac{2^s}{s!} \prod_{i=1}^{s} \left( \frac{(p_i - 1)\ln N}{2 \ln p_i} + s \right) + 2^s \sum_{k=0}^{s-1} \frac{p_{k+1}}{k!} \prod_{i=1}^{k} \left( \left\lfloor \frac{p_i}{2} \right\rfloor \frac{\ln N}{\ln p_i} + k \right) + 2^s u,$$

where $u$ is 0 when all numbers $p_i$ are odd, and

$$u = \frac{p_r}{2(s-1)!} \prod_{1 \le i \le s, i \ne r} \left( \frac{(p_i - 1) \ln N}{2 \ln p_i} + s - 1 \right)$$

if $p_r$ is the only even number among them. Therefore the estimate (2.1) holds with constant

$$c_s = \frac{1}{s!} \prod_{i=1}^{s} \frac{p_i - 1}{\ln p_i}.$$

By making the constant $c_s$ smaller by a factor $s!$, it is now going to 0 as $s$ goes to infinity, whereas the bound previously known was such that $c_s$ was tending to infinity super-exponentially with $s$.

Furthermore, Atanassov was able to make this constant even smaller in two cases, both of which make use of the concept of *admissible integers*:

**Definition 2.1.** Let $p_1, \ldots, p_s$ be distinct primes. The integers $k_1, \ldots, k_s$ are called *admissible* for them, if $p_i \not| k_i$ and for each set of integers $b_1, \ldots, b_s$, $p_i \not| b_i$, there exists a set of integers $\alpha_1, \ldots, \alpha_s$, satisfying the congruences

$$k_i^{\alpha_i} \prod_{1 \le j \le s, j \ne i} p_j^{\alpha_j} \equiv b_i \pmod{p_i}, \qquad i = 1, \ldots, s. \tag{2.2}$$

If a sequence of $s$ ones is admissible for the prime numbers $p_1, \ldots, p_s$, we say that $p_1, \ldots, p_s$ *satisfy Condition* $\mathcal{R}$.

A quantity that is used repeatedly when dealing with admissible integers is the following:

$$P_i(k_i; (\alpha_1, \ldots, \alpha_s)) = k_i^{\alpha_i} \prod_{1 \le j \le s, j \ne i} p_j^{\alpha_j} \bmod p_i \ \in \{0, \ldots, p_i - 1\}, \ i = 1, \ldots, s. \tag{2.3}$$

We chose to introduce this here just so that the reader can see the relation between this quantity and the definition of admissible integers.

The two cases where a smaller value for $c_s$ are proved are as follows: (1) for a Halton sequence with prime integers $p_1, \ldots, p_s$ satisfying Condition $\mathcal{R}$; (2) for a *modified Halton sequence*, which uses a generalized van der Corput sequence $\{x_n^{(i)}\}_{n=0}^{\infty}$ for its $i$th coordinate, based on permutations of the form

$$\tau_j^{(i)}(a) = a k_i^j \bmod p_i \ \in \{0, \ldots, p_i - 1\}, \qquad j = 0, \ldots, k, i = 1, \ldots, s, \tag{2.4}$$

and where $k_1, \ldots, k_s$ are admissible integers for the prime numbers $p_1, \ldots, p_s$.

The two corresponding results are as follows:

**Theorem 2.2.** If the prime numbers $p_1, \ldots, p_s$ fulfill Condition $\mathcal{R}$, then the discrepancy of the Halton sequence $\sigma(p_1, \ldots, p_s)$ satisfies (2.1) with constant

$$c_s(p_1,\dots,p_s) = \frac{2^s}{s!}\sum_{i=1}^{s}\ln p_i \prod_{i=1}^{s}\frac{p_i(1+\ln p_i)}{(p_i-1)\ln p_i}.$$

**Theorem 2.3.** Let $p_1,\dots,p_s$ be distinct primes and the integers $k_1,\dots,k_s$ be admissible for them. The modified Halton sequence $\sigma(p_1,\dots,p_s;k_1,\dots,k_s)$ satisfies (2.1) with the same constant as in Theorem 2.2, i.e., with

$$c_s(p_1,\dots,p_s) = \frac{2^s}{s!}\sum_{i=1}^{s}\ln p_i \prod_{i=1}^{s}\frac{p_i(1+\ln p_i)}{(p_i-1)\ln p_i}.$$

As pointed out by Atanassov, when Condition $\mathcal{R}$ is fulfilled, the corresponding Halton sequence can be thought of as a special case of the modified Halton sequence. Thus Theorem 2.2 follows from Theorem 2.3.

## 3. Organization of the proof

The two results that need to be proved are Theorem 2.1, which improved the best known upper bound $c_s$ on the Halton sequence, and Theorem 2.3, which shows an even better bound for the modified Halton sequence.

To prove Theorem 2.1, Atanassov relies on five lemmas (Lemmas 3.1 to 3.5). Lemma 3.1 gives a bound on the difference $|A_N(J)-N\mu(J)|$ for intervals $J$ whose endpoints are given by multiples of some powers of the $p_i$'s. That is, for $J$ of the form

$$J = \prod_{i=1}^{s}[b_i p_i^{-\alpha_i}, c_i p_i^{-\alpha_i}).$$

When $c_i - b_i = 1$, such intervals are typically referred to as "elementary intervals".

Lemmas 3.4 and 3.5 have to do with how one can rewrite an arbitrary interval $J$ of the form

$$J = \prod_{i=1}^{s}[0, z_i)$$

(as used in the computation of the star-discrepancy) into something called a "signed splitting". In the proof of Theorem 2.1, the idea is then to break down $A_N(J) - N\mu(J)$ into two parts $\Sigma_1$ and $\Sigma_2$, with $\Sigma_1$ dealing with the coarser parts of the signed splitting for $J$, and $\Sigma_2$ dealing with the finer parts. What determines whether an interval is coarse or fine has to do with the value $N$, and Lemmas 3.2 and 3.3 provide results on this aspect.

The proof of Theorem 2.1 found in [1] is correct. What we do below is to reproduce these proofs but we correct a few notation problems found in [1], and give more details.

As for Theorem 2.3, its proof relies on the following proposition:

**Proposition 4.1.** The star-discrepancy of the modified Halton sequence $\sigma = \sigma(p_1, \ldots, p_s, k_1, \ldots, k_s)$ satisfies [1]:

$$ND_N^*(\sigma) \leq \sum_{\mathbf{j} \in T(N)} \left( 1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^s (l_i/p_i) P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})} \right) + \sum_{k=0}^{s-1} \frac{p_{k+1}}{k!} \prod_{i=1}^{k} \left( \left\lfloor \frac{p_i}{2} \right\rfloor \frac{\ln N}{\ln p_i} + k \right),$$

where $\lfloor \cdot \rfloor$ denotes the floor function, $\| \cdot \|$ denotes the "distance to the nearest integer" function, $\mathbf{j} = (j_1, \ldots, j_s)$, with each $j_i$ a nonnegative integer, $\mathbf{p} = (p_1, \ldots, p_s)$, and

$$\begin{aligned} T(N) &= \{\mathbf{j} : p_1^{j_1} \cdots p_s^{j_s} \leq N, j_1, \ldots, j_s \geq 0\}, \\ M(\mathbf{p}) &= \{\mathbf{j} \mid 0 \leq j_i \leq p_i - 1, j_1 + \cdots + j_s > 0\}, \\ R(\mathbf{j}) &= \prod_{i=1}^{s} r_i(j_i), \\ \text{with } r_i(m) &= \max(1, \min(2m, 2(p_i - m))), \end{aligned} \tag{3.1}$$

and the quantity $P_i(k_i; \mathbf{j})$ is defined in (2.3). In addition, we introduce some additional notation that will be useful in the proof of future results:

$$\begin{aligned} T^*(N) &= \{\mathbf{j} : p_1^{j_1} \cdots p_s^{j_s} \leq N, j_1, \ldots, j_s > 0\} = \{\mathbf{j} \in T(N) : \mathbb{z}(\mathbf{j}) = 0\}, \\ T_z(N) &= \{\mathbf{j} : p_1^{j_1} \cdots p_s^{j_s} \leq N, \text{ some } j_i = 0\} = \{\mathbf{j} \in T(N) : \mathbb{z}(\mathbf{j}) > 0\}. \end{aligned} \tag{3.2}$$

That is, $T^*(N) = T(N) \setminus T_z(N)$ and $\mathbb{z}(\mathbf{j})$ is the number of zero entries in $\mathbf{j}$.

To prove this proposition, Atanassov relies on three lemmas (Lemmas 4.1 to 4.3). Lemma 4.1 establishes the existence of admissible integers. Lemma 4.3 gives an upper bound on $A_N(J) - N\mu(J)$ for elementary intervals, and relies on Lemma 4.2, which relates the distance $A_N(J) - N\mu(J)$ in a certain setting with exponential sums. It should be noted that this Lemma 4.2 is a special case of [15, Satz 2].

The proof of these lemmas found in [1] are also correct (again, modulo some problems in the notation). However, we believe that the proof of

[1] The term $(l_i/p_i)$ in the sum over $\mathbf{l} \in M(\mathbf{p})$ above is instead just $l_i$ in [1], which is a typo.

Proposition 4.1 given in [1] contains an inaccuracy. More precisely, here Atanassov breaks down $A_N(J) - N\mu(J)$ into two parts $\Sigma_1$ and $\Sigma_2$ again, but we think the bound he gets for $\Sigma_1$ is incorrect. We find that $\Sigma_1$ needs to be splitted up into two parts, with one part that can be bounded as in [1], but with the other part contributing an extra term in the bound, which behaves in $O(\ln^{s-1} N)$. That is, we modify Proposition 4.1 as follows:

**(Modified) Proposition 4.1.** The star-discrepancy of the modified Halton sequence $\sigma = \sigma(p_1, \dots, p_s, k_1, \dots, k_s)$ satisfies:

$$ND_N^*(\sigma) \leq \sum_{\mathbf{j} \in T^*(N)} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^s \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})}\right) + \sum_{k=0}^{s-1} \frac{p_{k+1}}{k!} \prod_{i=1}^{k} \left( \left\lfloor \frac{p_i}{2} \right\rfloor \frac{\ln N}{\ln p_i} + k \right) + \sum_{i=1}^{s} \frac{1}{(s-1)!} \prod_{\substack{k=1 \\ k \neq i}}^{s} \left( \frac{p_k}{2} \frac{\ln N}{\ln p_k} + s - 1 \right).$$

Our proof of this modified Proposition 4.1 contains a remark (Remark 5.1) that explain precisely where this extra term comes from. The fact that the new term is $O(\ln^{s-1} N)$ will also be quickly proved in this note.

Alternatively, as we will show in Section 6, another version of Proposition 4.1 also holds. Namely, we have:

**(Modified$^2$) Proposition 4.1.** The star-discrepancy of the modified Halton sequence $\sigma = \sigma(p_1, \dots, p_s, k_1, \dots, k_s)$ satisfies:

$$ND_N^*(\sigma) \leq \sum_{\mathbf{j} \in T(N)} 2^{\mathbb{z}(\mathbf{j})} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^s \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})}\right) + \sum_{k=0}^{s-1} \frac{p_{k+1}}{k!} \prod_{i=1}^{k} \left( \left\lfloor \frac{p_i}{2} \right\rfloor \frac{\ln N}{\ln p_i} + k \right),$$

where $\mathbb{z}(\mathbf{j}) = \#\{i = 1, \dots, s : j_i = 0\}$.

In turn, in [1] Theorem 2.3 is proved using Proposition 4.1 and another lemma (Lemma 4.4). Although, as we show, Proposition 4.1 does not hold as in [1], we are able to also prove Theorem 2.3 using either our modified Proposition 4.1 or a slightly weaker version of modified$^2$ Proposition 4.1, and an approach similar to the one used by Atanassov. We find however that the proof of Theorem 2.3 in [1] omits some non-trivial steps, which we provide below.

Note that the bound in our modified Proposition 4.1 could presumably be improved, but since in its current form we are still able to prove the main result—given by Theorem 2.3—for now we have not attempted to perform such improvements.

A last note: for the sake of completeness, we have included in our proof a few very easy intermediate results, and have numbered them using hyphens referring to the more important results to which they relate. For instance, Lemma 3.2.-1 is a very easy lemma used as an intermediate result for Lemma 3.2.

## 4. Proofs Leading to Theorem 2.1

**Lemma 3.1.** Let $\sigma(p_1, \dots, p_s) = \{x_n\}_{n=0}^{\infty}$ be a Halton or modified Halton sequence (based on any permutations $\tau_j^{(i)}$) and let $J$ be an interval of the form

$$J = \prod_{i=1}^{s} [b_i p_i^{-\alpha_i}, c_i p_i^{-\alpha_i}).$$

where $b_i, c_i \geq 0$ are integers for all $i$. Then

$$|A_N(J) - N\mu(J)| \leq \prod_{i=1}^{s} (c_i - b_i)$$

for every positive integer $N$ and $A_N(J) \leq \prod_{i=1}^{s} (c_i - b_i)$ for $N \leq \prod_{i=1}^{s} p_i^{\alpha_i}$.

*Proof.* For each nonnegative integer $n$, write $n = \sum_{j=0}^{\infty} n_{ij} p_i^j$ in base $p_i$. Fix some $\mathbf{l} = (l_1, \dots, l_s)$ such that $b_i \leq l_i < c_i \leq p_i^{\alpha_i}$. Fix some $i = 1, \dots, s$, write $l_i = \sum_{j=0}^{\infty} l_{ij} p_i^j$ in base $p_i$. Recall that $x_n^{(i)} = \sum_{j=0}^{\infty} \tau_j^{(i)}(n_{ij}) p_i^{-j-1}$. Thus, we have

$$\begin{aligned} x_n^{(i)} \in [l_i p_i^{-\alpha_i}, (l_i+1) p_i^{-\alpha_i}) &\Leftrightarrow \sum_{j=0}^{\infty} \tau_j^{(i)}(n_{ij}) p_i^{\alpha_i - j - 1} \in [\sum_{j=0}^{\alpha_i - 1} l_{ij} p_i^j, \sum_{j=0}^{\alpha_i - 1} l_{ij} p_i^j + 1) \\ &\Leftrightarrow \tau_j^{(i)}(n_{ij}) = l_{i, \alpha_i - j - 1}, \text{ for all } j = 0, 1, \dots, \alpha_i - 1. \end{aligned} \tag{4.1}$$

Since each $\tau_j^{(i)}$ is a bijection, we see that for each $l_i$ and each $j$, there is a unique $n_{ij}$ satisfying (4.1). That is, the first $\alpha_i$ digits of $n$ in base $p_i$ are uniquely determined by (4.1). More precisely, there exists $a_i \in \{1, \dots, p_i^{\alpha_i}\}$ such that

$$x_n^{(i)} \in [l_i p_i^{-\alpha_i}, (l_i+1)p_i^{-\alpha_i}) \Leftrightarrow n \equiv a_i \pmod{p_i^{\alpha_i}}.$$

Since the $p_i$'s are coprime, by the Chinese Remainder Theorem, we see that

$$(x_n^{(1)}, \ldots, x_n^{(s)}) \in J_1 = \prod_{i=1}^{s} [l_i p_i^{-\alpha_i}, (l_i+1)p_i^{-\alpha_i}) \Leftrightarrow n \equiv b \pmod{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}$$

for some $b$ with $b \equiv a_i \pmod{p_i^{\alpha_i}}$, for $i = 1, \ldots, s$. In other words, exactly one term out of every $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ consecutive terms falls into $J_1$.

Since each $l_i$ can take $c_i - b_i$ values, we have for any positive integer $t$,

$$A_{tp_1^{\alpha_1}\cdots p_s^{\alpha_s}}(J) = t(c_1 - b_1)\cdots(c_s - b_s). \tag{4.2}$$

The last statement follows by taking $t = 1$ and the trivial fact that $A_N(J)$ is increasing in $N$.

For an arbitrary $N$, find a $t$ such that $tp_1^{\alpha_1} \cdots p_s^{\alpha_s} \le N < (t+1)p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, we have

$$A_N(J) - N\mu(J) \le A_{(t+1)p_1^{\alpha_1}\cdots p_s^{\alpha_s}}(J) - tp_1^{\alpha_1} \cdots p_s^{\alpha_s} \prod_{i=1}^{s} \frac{(c_i - b_i)}{p_i^{\alpha_i}} = \prod_{i=1}^{s} (c_i - b_i).$$

Similarly, $N\mu(J) - A_N(J) \le \prod_{i=1}^{s}(c_i - b_i)$. The result now follows. □

The next lemma uses the following definition:

**Definition 3.1.** Let $p_1, \ldots, p_s$ be a possibly empty set of integers, $p_i \ge 2$ and let $N$ be any positive number. We denote by $d(p_1, \ldots, p_k; N)$ the number of positive integer vectors $\mathbf{j} = (j_1, \ldots, j_k)$ such that $p_1^{j_1} \cdots p_k^{j_k} \le N$. If $k = 0$ then we let $d(N) = 1$.

We will need to following result from Euclidean geometry to prove Lemma 3.2:

**Lemma 3.2.-1.** The volume of the *simplex* $\{x_1a_1 + \cdots + x_ka_k \le b, x_i \ge 0\}$ with $b, k \ge 0, a_i > 0$ is $\frac{1}{k!} b^k / \prod_{i=1}^{k} a_i$.

*Proof.* An easy integration shows that $\mathrm{Vol}\{x_1 + \cdots + x_k \le 1, x_i \ge 0\} = \frac{1}{k!}$, where $\mathrm{Vol}(S)$ represents the volume of the set $S$. Now the case when $b = 0$ is trivial, so let us assume that $b \neq 0$.

Let $T$ be the linear transformation with matrix representation

$$T = \begin{pmatrix} a_1/b & 0 & \cdots & 0 \\ 0 & a_2/b & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_k/b \end{pmatrix}.$$

Then, we have

$$\begin{aligned}\frac{1}{k!} &= |\det(T)|\,\mathrm{Vol}\{x_1,\ldots,x_s : T(x_1,\ldots,x_s)\in S\}\\ &= \frac{1}{b^k}\left(\prod_{i=1}^{k} a_i\right)\mathrm{Vol}\{x_1a_1+\cdots x_ka_k\le b, x_i\ge 0\}.\end{aligned}$$

Rearranging gives the result. □

**Lemma 3.2.** The number $d(p_1,\ldots,p_k;N)$ satisfies

$$d(p_1,\ldots,p_k;N)\le \frac{1}{k!}\prod_{i=1}^{k}\frac{\ln N}{\ln p_i}.$$

*Proof.* If positive integers $j_1,\ldots,j_s$ satisfy $\prod_{i=1}^{k} p_i^{j_i} \le N$, then by taking natural logarithm, we see that $\sum_{i=1}^{k} j_i \ln p_i \le \ln N$. Then the cube $\prod_{i=1}^{k}[j_i-1,j_i)$ is contained in the simplex $S=\{\sum_{i=1}^{k} x_i\ln p_i\le \ln N, x_i\ge 0\}$. Clearly, for distinct vectors $(j_1,\ldots,j_s)$, the corresponding cubes as defined above, each having volume 1, do not intersect and

$$\dot{\bigcup_{j_1,\ldots,j_k>0\,|p_1^{j_1}\cdots p_k^{j_k}\le N}}\ \prod_{i=1}^{k}[j_i-1,j_i)\subseteq S,$$

where $\dot\cup$ represents a disjoint union. Therefore, we have

$$\begin{aligned}d(p_1,\ldots,p_k;N) &= \mathrm{Vol}\left(\dot{\bigcup_{j_1,\ldots,j_k>0\,|p_1^{j_1}\cdots p_k^{j_k}\le N}}\ \prod_{i=1}^{k}[j_i-1,j_i)\right)\\ &\le \mathrm{Vol}(S)=\frac{1}{k!}\prod_{i=1}^{k}\frac{\ln N}{\ln p_i},\end{aligned}$$

where the last equality follows from Lemma 3.2.-1. □

**Lemma 3.3.** Let $N$ and $p_1,\ldots,p_k$ be integers, $p_i\ge 2$. Let some numbers $c_j^{(i)}\ge 0$ be given, for $j\ge 0, i=1\ldots,k$, satisfying $c_0^{(i)}\le 1$ and $c_j^{(i)}\le f_i(p_i)$ for $j\ge 1$, where $f_1(p_1),\ldots,f_k(p_k)$ are some numbers (possibly depending on the $p_i$'s). Then

$$\sum_{(j_1,\ldots,j_k)|p_1^{j_1}\ldots p_k^{j_k}\le N}\ \prod_{i=1}^{k} c_{j_i}^{(i)}\le \frac{1}{k!}\prod_{i=1}^{k}\left(f_i(p_i)\frac{\ln N}{\ln p_i}+k\right). \tag{4.3}$$

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

*Proof.* First notice that each $f_i(p_i) \geq 0$, and hence we could multiply them on both side of any equation without changing the inequality sign. Now, for each $m = \{0, 1, \ldots, k\}$, fix a subset $L = \{i_1, \ldots, i_m\}$ of $\{1, \ldots, k\}$. 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 $\prod_{i=1}^{k} p_i^{j_i} = \prod_{i \in L} p_i^{j_i} \leq N$. There are $d(p_{i_1}, \ldots, p_{i_m}; N) = \frac{1}{m!} \prod_{i \in L} \frac{\ln N}{\ln p_i}$ such $k$-tuples, by Lemma 3.2, each having a contribution of

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

So by expanding the two sides of (4.3), we have,

$$\begin{aligned}
\text{Left hand side} &= \sum_m \sum_L (\text{number of such } k\text{-tuples}) \cdot (\text{amount of each} \\
&\qquad \text{contribution}) \\
&\leq \sum_{m=0}^{k} \sum_{\substack{L \subseteq \{1,\ldots,k\} \\ |L|=m}} \frac{1}{m!} \prod_{i \in L} \frac{\ln N}{\ln p_i} \prod_{i \in L} f_i(p_i) \\
\text{Right hand side} &= \frac{1}{k!} \sum_{\substack{\text{all subset } L \\ \text{of } \{1,\ldots,k\}}} \left( \prod_{i \in L} f_i(p_i) \frac{\ln N}{\ln p_i} \cdot \prod_{i \notin L} k \right) \\
&= \frac{1}{k!} \sum_{m=0}^{k} \sum_{\substack{L \subseteq \{1,\ldots,k\} \\ |L|=m}} \left( \prod_{i \in L} f_i(p_i) \frac{\ln N}{\ln p_i} \cdot k^{k-m} \right)
\end{aligned}$$

The result now follows since $\frac{1}{m!} \leq \frac{1}{k!} k^{k-m}$ as

$$\overbrace{k \cdot k \cdots k}^{(k-m)\, k\text{'s}} \geq \overbrace{k(k-1) \cdots (m+1)}^{k-m \text{ terms}}. \qquad \square$$

The next two easy lemmas use the following definition:

**Definition 3.2.** Consider an interval $J \subseteq \mathbf{E}^s$. We call a *signed splitting* of $J$ any collection of intervals $J_1, \ldots, J_n$ and respective signs $\epsilon_1, \ldots, \epsilon_n$ equal to $\pm 1$, such that for any (finitely) additive function $\nu$ on the intervals in $\mathbf{E}^s$, we have

$$\nu(J) = \sum_{i=1}^{n} \epsilon_i \nu(J_i).$$

**Lemma 3.4.** Let the interval $J = \prod_{i=1}^{s}[a_i, b_i) \subseteq \mathbf{E}^s$ be given. Fix a dimension $k$ and a number $c \in (0,1)$. The intervals

$$\begin{aligned} I_1 &= [\min(a_k, c), \max(a_k, c)) \\ \text{and } I_2 &= [\min(c, b_k), \max(c, b_k)) \end{aligned}$$

and the signs $\epsilon_1 = \operatorname{sgn}(c - a_k)$, $\epsilon_2 = \operatorname{sgn}(b_k - c)$ define a signed splitting of the interval $[a_k, b_k)$. Multiplying correspondingly, we obtain the collection of intervals

$$\begin{aligned} J_1 &= \prod_{i=1}^{k-1}[a_i, b_i) \times I_1 \times \prod_{i=k+1}^{s}[a_i, b_i), \\ J_2 &= \prod_{i=1}^{k-1}[a_i, b_i) \times I_2 \times \prod_{i=k+1}^{s}[a_i, b_i), \end{aligned}$$

which, together with the same signs $\epsilon_1$, $\epsilon_2$, provide a signed splitting of the interval $J$.

*Proof.* This lemma is an easy case analysis. Notice that there are only three cases: $J_1 \dot{\cup} J_2 = J; J_1 \dot{\cup} J = J_2; J_2 \dot{\cup} J = J_1$. The signs tell us which case are we dealing with. □

**Lemma 3.5.** Let $J = \prod_{i=1}^{s}[0, z^{(i)})$ be an $s$-dimensional interval, and let for each $i$ some numbers $(z_j^{(i)})_{j=1}^{n_i} \subseteq [0,1]$ be given, where $n_i \geq 1$. Denote $z_0^{(i)} = 0$ and $z_{n_i+1}^{(i)} = z^{(i)}$. A signed splitting of $J$, induced by the numbers $(z_j^{(i)})$, is given by the collection of intervals

$$\prod_{i=1}^{s}[\min(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}), \max(z_{j_i}^{(i)}, z_{j_i+1}^{(i)})), \qquad 0 \leq j_i \leq n_i,$$

and signs $\epsilon(j_1, \ldots, j_s) = \prod_{i=1}^{s} \operatorname{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)})$.

*Proof.* Apply Lemma 3.4 inductively. □

Notice that the above lemma also holds for intervals of the form $J = \prod_{i=1}^{s}[y^{(i)}, z^{(i)})$ by requiring $z_0^{(i)} = y^{(i)} \leq z^{(i)}$.

**Proof of Theorem 2.1.**
Pick any $\mathbf{z} = (z^{(1)}, \ldots, z^{(s)}) \in \mathbf{E}^s = [0,1)^s$. Expand each $z^{(i)}$ as $\sum_{j=0}^{\infty} a_j^{(i)} p_i^{-j}$.

**Claim 1:** If $p_i$ is odd, we can choose $a_j^{(i)}$ so that $|a_j^{(i)}| \le \frac{p_i-1}{2}$, for all $j \le M$ where $M$ is an arbitrary positive integer.

*Proof.* We can first write $z^{(i)} = \sum_{j=0}^{\infty} b_j^{(i)} p_i^{-j}$ with $b_0 = 0, b_j^{(i)} \in \{0, 1, \ldots, p_i - 1\}$ for $j > 0$. Consider $z_M^{(i)} = \sum_{j=0}^{M} b_j^{(i)} p_i^{-j}$, let us start from $b_M^{(i)}$ and proceed backwards inductively so that if $b_j^{(i)} > p_i/2$ for $j > 0$, i.e. $b_j^{(i)} \ge (p_i+1)/2$, replace $b_j^{(i)}$ by $b_j^{(i)} - p_i$, and $b_{j-1}^{(i)}$ by $b_{j-1}^{(i)} + 1$. It is easy to see that the resulting expression satisfies the condition given in Claim 1. The claim now follows by defining $a_j^{(i)} := b_j^{(i)}$ (see Remark 4.1 on page 18). Notice that after the above operations, $a_0^{(i)} = b_0^{(i)}$ which remains 0 if $b_1^{(i)} \le \lfloor p_i/2 \rfloor$, and was incremented to 1 otherwise. □

Since $p_1, \ldots, p_s$ are coprime, at most one of them, say $p_r$, could be even. In that case, we appeal to the following claim:

**Claim 2:** If $p_r$ is even, we can choose $a_j^{(r)}$ so that $|a_j^{(r)}| \le \frac{p_r}{2}$, and $|a_j^{(r)}| + |a_{j+1}^{(r)}| \le p_r - 1$, for all $j \le M$ where $M$ is an arbitrary positive integer.

**Proof:** We can use the same trick as above, except that we start with $z_{M+1}^{(r)}$ and when $b_j^{(r)} = p_r/2$: we do nothing if $b_{j-1}^{(r)} \ne p_r/2$; we replace $b_j^{(r)}$ by $-p_r/2$, and $b_{j-1}$ by $b_{j-1} + 1$ if $b_{j-1} = p_r/2$. (See Remark 4.2 on page 18.) □

For each $i = 1, \ldots, s$, write $n_i = \left\lfloor \frac{\ln N}{\ln p_i} \right\rfloor + 1$ and consider the numbers $z_k^{(i)} = \sum_{j=0}^{k-1} a_j^{(i)} p_i^{-j}$ for $k = 1, \ldots, n_i$ satisfying the conditions in Claims 1 and 2 with $M$ big enough, say $n_i + 1$. (Notice that the $z_k^{(i)}$ defined here is different from what it was above.) Define $z_0^{(i)} = 0$ and $z_{n_i+1}^{(i)} = z^{(i)}$. Applying Lemma 3.5, we expand $J = \prod_{i=1}^{s} [0, z^{(i)})$ using $(z_j^{(i)})_{j=1}^{n_i}$, obtaining a collection of intervals

$$I(\mathbf{j}) = \prod_{i=1}^{s} [\min(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}), \max(z_{j_i}^{(i)}, z_{j_i+1}^{(i)})), \qquad 0 \le j_i \le n_i, \tag{4.4}$$

and signs $\epsilon(j_1, \ldots, j_s) = \prod_{i=1}^{s} \mathrm{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)})$.

Since $\mu$ and $A_N$ are both additive, so is any scalar linear combination of them, and hence $A_N(J) - N\mu(J)$ may be expanded as

$$A_N(J) - N\mu(J) = \sum_{j_1=0}^{n_1} \cdots \sum_{j_s=0}^{n_s} \epsilon(\mathbf{j})(A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))) = \sum\nolimits_1 + \sum\nolimits_2. \tag{4.5}$$

We rearrange the terms so that in $\sum_1$, we put the terms with $p_1^{j_1} \cdots p_s^{j_s} \le N$ (i.e. $\mathbf{j} \in T(N)$) and in $\sum_2$ the rest. Notice that in $\sum_1$, the $j_i$'s are small, so the corresponding $I(\mathbf{j})$ is bigger. Hence, as we stated earlier, $\sum_1$ deals with the coarser part whereas $\sum_2$ deals with the finer part. Notice that if $j_i = n_i$ for some $i$, then $p_1^{j_1}\cdots p_s^{j_s} \geq p_i^{n_i} > N$. That is, any $\mathbf{j}$ with $j_i$ being its maximum will not be accounted for in $\sum_1$. In other words, all $I(\mathbf{j})$ included in $\sum_1$ are "regular" in the sense that Lemma 3.1 applies.

**Claim 3:**

$$|\sum\nolimits_1| \leq \sum_{\mathbf{j}|p_1^{j_1}\cdots p_s^{j_s}\leq N} |A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))| \leq \frac{1}{s!}\prod_{i=1}^{s}\left(\frac{(p_i-1)\ln N}{2\ln p_i} + s\right) + u, \tag{4.6}$$

where $u$ is defined in the statement of Theorem 2.1.

**Proof:** By Lemma 3.1, we have, for $j_i < n_i, \forall i$, that

$$|A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))| \leq \prod_{i=1}^{s} |z_{j_i+1}^{(i)} - z_{j_i}^{(i)}|p_i^{j_i} = \prod_{i=1}^{s}|a_{j_i}^{(i)}|. \tag{4.7}$$

If all the $p_i$'s are odd, applying Lemma 3.3 with $f_i(p_i) = (p_i-1)/2$ gives exactly (4.6).

Suppose now some $p_r$ is even. Consider the numbers $p_1', \ldots, p_s'$ defined by $p_i' = p_i$ for $i \neq r$, and $p_r' = p_r^2$. Define $c_0^{(i)} = 1$ (observe that $a_0^{(i)} = 0$ or $1$, by definition), $c_j^{(i)} = |a_j^{(i)}|$ for $i \neq r$, and $c_j^{(r)} = |a_{2j-1}^{(r)}| + |a_{2j}^{(r)}|$ for all $j \geq 1$. Applying Lemma 3.3 on $(p_1', \ldots, p_s')$ with $f_i(p_i') = (p_i'-1)/2$ for $i \neq r$ and $f_r(p_r') = \sqrt{p_r'} - 1$, we have

$$\begin{aligned}
\sum_{\mathbf{j}'|\prod_{i=1}^{s} p_i'^{j_i'}\leq N}\prod_{i=1}^{s} c_{j_i'}^{(i)} &\leq \frac{1}{s!}\left(\frac{(\sqrt{p_r^2}-1)\ln N}{\ln p_r^2} + s\right)\prod_{\substack{i=1\\ i\neq r}}^{s}\left(\frac{(p_i-1)\ln N}{2\ln p_i} + s\right) \\
&= \frac{1}{s!}\prod_{i=1}^{s}\left(\frac{(p_i-1)\ln N}{2\ln p_i} + s\right).
\end{aligned} \tag{4.8}$$

Let us see what has been covered and what is missing in $\sum_1$:

- First, all vectors $\mathbf{j}$ with $j_r = 0$ are covered: $a_{j_r}^{(r)} = a_0^{(r)} = 0$ or $1$ and $c_{j_r}^{(r)} = c_0^{(r)} = 1$ while $c_{j_i}^{(i)} = |a_{j_i}^{(i)}|$ if $i \neq r$. Hence $\prod_{i=1}^{s}|a_{j_i}^{(i)}| \leq \prod_{i\neq r}|a_{j_i}^{(i)}| = \prod_{i=1}^{s} c_{j_i}^{(i)} = \prod_{i=1}^{s} c_{j_i'}^{(i)}$.
- For vectors $\mathbf{j}$ with $j_r \neq 0$, consider two consecutive $s$-tuples $(j_1, \ldots, j_{r-1}, 2h_r - 1, j_{r+1}, \ldots, j_s)$ and $(j_1, \ldots, j_{r-1}, 2h_r, j_{r+1}, \ldots, j_s)$ in $\sum_1$: we have

$$\prod_{i=1,i\neq r}^{s} |a_{j_i}^{(i)}| \cdot |a_{2h_r-1}^{(r)}| + \prod_{i=1,i\neq r}^{s} |a_{j_i}^{(i)}| \cdot |a_{2h_r}^{(r)}| =$$

$$\prod_{i=1,i\neq r}^{s} |a_{j_i}^{(i)}| \cdot \left(|a_{2h_r-1}^{(r)}| + |a_{2h_r}^{(r)}|\right) = \prod_{i=1,i\neq r}^{s} c_{j_i}^{(i)} \cdot c_{j'_r}^{(r)} = \prod_{i=1}^{s} c_{j'_i}^{(i)}, \qquad (4.9)$$

with $j'_i = j_i$ if $i \neq r$ and $j'_r = h_r$, according to the definition of integers $c_j^{(i)}$ for all $j \leq 1$. Moreover, since $j'_r = h_r = (j_r+1)/2$, we have

$$\prod_{\substack{i=1\\ i\neq r}}^{s} p_i'^{j'_i} \cdot (p_r^2)^{j'_r} = \begin{cases} \prod_{i=1}^{s} p_i^{j_i} & \text{if } j_r \text{ is even} \\ \prod_{i=1}^{s} p_i^{j_i} \cdot p_r & \text{if } j_r \text{ is odd.} \end{cases}$$

So terms with $\prod_{i=1}^{s} p_i^{j_i} \leq N/p_r$ have also been covered.
This is the correct version for item 2 above. In the former version of this note, it was written as $\prod_{i=1}^{s} |a_{j_i}^{(i)}| \leq \prod_{i=1,i\neq r}^{s} |c_{j_i}^{(i)}| \cdot |c_{\lfloor j_r/2 \rfloor}^{(r)}|$ instead of (4.9) and we see that for two consecutive $s$-tuples $\mathbf{j}$ with $j_r \neq 0$ occurring in $\sum_1$, we only get one integer $j'_r$ in the LHS of this inequality, i.e., $j'_r := j_r/2$ if $j_r$ is even or $j'_r := (j_r+1)/2$ if $j_r$ is odd. Hence, with the LHS of this inequality, we only recover one product in $\sum_1$ instead of two. This omission is of the same kind as the one that motivated the Corrigendum [9]. Notice that the corresponding passage in the original paper from Atanassov is so terse that it is impossible to infer anything about this tricky point.

The missing terms are contained in $S' = \{\mathbf{j} : N/p_r < \prod_{i=1}^{s} p_i^{j_i} \leq N\}$. Obviously, for any $\mathbf{j} \in S'$, we have that $\prod_{i=1,i\neq r}^{s} p_i^{j_i} \leq N$ and that $j_r$ is uniquely determined given all other $j_i$'s. Their total contribution $\sum'_1$ is

$$\begin{aligned} \sum\nolimits'_1 \quad &\leq \sum_{\mathbf{j} \mid \prod_{i=1,i\neq r}^{s} p_i^{j_i} \leq N} \frac{p_r}{2} \prod_{i=1,i\neq r}^{s} |a_{j_i}^{(i)}| \\ &\leq \frac{p_r}{2} \frac{1}{(s-1)!} \prod_{i=1,i\neq r}^{s} \left(\frac{(p_i-1)\ln N}{2\ln p_i} + s - 1\right) = u \end{aligned}$$

where the second inequality follows from Lemma 3.3 with $k = s-1$. Combining this result with (4.8), we have proved Claim 3. $\square$

Let us now examine $|\sum_2|$: recall that in $\sum_2$, we are summing over all vectors $\mathbf{j}$ in $Q = \{\mathbf{j} \,|\, p_1^{j_1} \cdots p_s^{j_s} > N\}$. Divide $Q$ into $s$ disjoint sets $B_0, \ldots, B_{s-1}$, where $B_k = \{\mathbf{j} : p_1^{j_1} \cdots p_k^{j_k} \leq N, p_1^{j_1} \cdots p_k^{j_k} p_{k+1}^{j_{k+1}} > N\}$ for $k > 0$ and $B_0 = \{\mathbf{j} : p_1^{j_1} > N\}$.

Fix any $k \le s-1$ and one $k$-tuple $(j_1, \dots, j_k)$ with $p_1^{j_1} \cdots p_k^{j_k} \le N$. Let $r$ be the biggest integer such that $p_1^{j_1} \cdots p_k^{j_k} p_{k+1}^{r-1} \le N$. Hence, if $j_{k+1}, \dots, j_s$ are any nonnegative integers satisfying $j_1, \dots, j_s \in B_k$, then $j_{k+1} \ge r$ and $j_{k+2}, \dots, j_s$ can be arbitrary.

For convenience, write $K_1 = \prod_{i=1}^{k} [\min(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}), \max(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}))$. [2] Obviously, by Lemma 3.5,

$$\left\{ K_1 \times \prod_{i=k+1}^{s} [\min(z_{j_i}^{(i)}, z_{j_i+1}^{(i)}), \max(z_{j_i}^{(i)}, z_{j_i+1}^{(i)})) \right\}$$

with signs

$$\left\{ \prod_{i=k+1}^{s} \operatorname{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)}) \right\}$$

is a "signed splitting" of

$$K_2 = K_1 \times \prod_{i=k+1}^{s} [0, z^{(i)}),$$

whereas the same sets and same signs restricted to $j_{k+1} < r$ is a "signed splitting" of

$$K_3 = K_1 \times [0, z_r^{(k+1)}) \times \prod_{i=k+2}^{s} [0, z^{(i)}).$$

Note that $\prod_{i=k+1}^{s} \operatorname{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)}) = \epsilon(j_1, \dots, j_s) \cdot \delta$, where $\delta = \prod_{i=1}^{k} \operatorname{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)})$ and $\epsilon$ was defined as in Lemma 3.5. Define

$$K = K_1 \times [\min(z_r^{(k+1)}, z^{(k+1)}), \max(z_r^{(k+1)}, z^{k+1})) \times \prod_{i=k+2}^{s} [0, z^{(i)}).$$

Then we see that either $K_2 = K_3 \dot{\cup} K$ when $z^{k+1} > z_r^{k+1}$, or $K_3 = K_2 \dot{\cup} K$ when $z^{k+1} \le z_r^{k+1}$. So a simple case analysis implies that

$$\begin{aligned} \pm(A_N(K) - N\mu(K)) &= (A_N(K_2) - N\mu(K_2)) - (A_N(K_3) - N\mu(K_3)) \\ &= \delta \cdot \sum_{\substack{j_{k+1}, \dots j_s \\ \mathbf{j} = (j_1, \dots, j_s) \in B_k}} \epsilon(\mathbf{j})(A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))) \quad (4.10) \end{aligned}$$

where the $\pm = \operatorname{sgn}(z^{(k+1)} - z_r^{(k+1)})$, and the last equality follows from the definition of signed splitting.

---

[2] Strickly speaking, $K_1$ is a function of $\mathbf{j}$, but we will simply write $K_1$ to save space. The same goes for other $K_i$ to be defined later.

Notice that

$$| z_r^{(k+1)} - z^{(k+1)} | = | \sum_{j=r}^{\infty} a_j^{(k+1)} p_{k+1}^{-j} | < \frac{p_{k+1}}{2} \frac{p_{k+1}^{-r}}{1 - p_{k+1}} \le p_{k+1}^{-r} p_{k+1},$$

where the first inequality follows since by Claims 1 and 2, each $a_j^{(k+1)} \le p_{k+1}/2$ and not all of them are equal to $p_{k+1}/2$; whereas the last inequality follows since $2(1 - p_{k+1}^{-1}) \ge 1$ as $p_{k+1} \ge 2$. Since $p_{k+1}^r z_r^{(k+1)} \in \mathbf{Z}$, it follows that

$$[\min(z_r^{(k+1)}, z^{(k+1)}), \max(z_r^{(k+1)}, z^{(k+1)})) \subseteq [m_1 p_{k+1}^{-r}, m_2 p_{k+1}^{-r})$$

for some nonnegative integers $m_1, m_2$ satisfying $0 \le m_2 - m_1 < p_{k+1}$. Hence, we have that $K \subseteq K_4 = K_1 \times [m_1 p_{k+1}^{-r}, m_2 p_{k+1}^{-r}) \times \prod_{i=k+2}^{s} [0, 1)$. Applying Lemma 3.1 on $K_4$, since $N \le p_1^{j_1} \cdots p_k^{j_k} p_{k+1}^r$ by definition of $r$, we get:

$$A_N(K) \le A_N(K_4) \le (m_2 - m_1) \prod_{i=1}^{k} p_i^{j_i} | z_{j_i+1}^{(i)} - z_{j_i}^{(i)} | \le p_{k+1} \prod_{i=1}^{k} | a_{j_i}^{(i)} |.$$

On the other hand,

$$N\mu(K) \le p_1^{j_1} \cdots p_k^{j_k} p_{k+1}^r \cdot \mu(K_4) = (m_2 - m_1) \prod_{i=1}^{k} | a_{j_i}^{(i)} | \le p_{k+1} \prod_{i=1}^{k} | a_{j_i}^{(i)} |.$$

Therefore,

$$|A_N(K) - N\mu(K)| \le p_{k+1} \prod_{i=1}^{k} | a_{j_i}^{(i)} |. \tag{4.11}$$

Since $| a_j^{(i)} | \le \lfloor \frac{p_i}{2} \rfloor$ for $i \le k$, applying Lemma 3.3, we have

$$\begin{aligned}
\left| \sum\nolimits_2 \right| &= \left| \sum_{k=0}^{s-1} \sum_{\substack{(j_1,\ldots,j_k) \\ p_1^{j_1} \cdots p_k^{j_k} \le N}} \sum_{\substack{(j_{k+1},\ldots,j_s) \\ \mathbf{j}=(j_1,\ldots,j_s)\in B_k}} \epsilon(\mathbf{j})(A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))) \right| \\
&= \left| \sum_{k=0}^{s-1} \sum_{\substack{(j_1,\ldots,j_k) \\ p_1^{j_1} \cdots p_k^{j_k} \le N}} \pm (A_N(K) - N\mu(K)) \right| \qquad \text{by (4.10)} \\
&\le \sum_{k=0}^{s-1} p_{k+1} \sum_{\substack{(j_1,\ldots,j_k) \\ p_1^{j_1} \cdots p_k^{j_k} \le N}} \prod_{i=1}^{k} | a_{j_i}^{(i)} | \quad \text{by (4.11)} \\
&\le \sum_{k=0}^{s-1} \frac{p_{k+1}}{k!} \prod_{i=1}^{k} \left( \left\lfloor \frac{p_i}{2} \right\rfloor \frac{\ln N}{\ln p_i} + k \right).
\end{aligned} \tag{4.12}$$

The result now follows by combining (4.6), (4.12) and the fact that $D_N(\sigma) \le 2^s D_N^*(\sigma)$. $\square$

REMARK 4.1. The original paper by Atanassov gives a different proof for Claim 1:
Inductively, choose $a_k^{(i)}$ to be the smallest integer in absolute value such that $|z^{(i)} - \sum_{j=0}^{k} a_j^{(i)} p_i^{-j}| < p_i^{-k}/2$. Such $a_k^{(i)}$ satisfies $|a_k^{(i)}| \le (p_i - 1)/2$ since

$$\frac{p_i^{-(k-1)}}{2} - \frac{p_i - 1}{2} p_i^{-k} = \frac{p_i^{-k}}{2}.$$

REMARK 4.2. The original paper by Atanassov also contains a different proof for Claim 2:
Inductively, choose $a_k^{(i)}$ to be the smallest integer in absolute value such that

$$|z^{(i)} - \sum_{j=0}^{k} a_j^{(i)} p^{-j}| < p^{-k-1} \left( \frac{p}{2} + \frac{p-2}{2p} + \frac{p}{2p^2} + \frac{p-2}{2p^3} + \cdots \right) = \frac{p^{-k}(p+2)}{2(p+1)},$$

where $p = p_r$ for convenience.
Such $a_k^{(i)}$ satisfies $|a_k^{(i)}| \le p/2$ since

$$\frac{p^{-(k-1)}(p+2)}{2(p+1)} - \frac{p^{-k}(p+2)}{2(p+1)} < \frac{p}{2} p^{-k},$$

and $|a_k^{(r)}| + |a_{k+1}^{(r)}| \le p - 1$ since

$$p^{-k} \left( \frac{p}{2} + \frac{p-2}{2p} + \frac{p}{2p^2} + \frac{p-2}{2p^3} + \cdots \right) - \frac{p}{2} p^{-k} - (\frac{p}{2} - 1) p^{-k-1}$$
$$= p^{-k-2} \left( \frac{p}{2} + \frac{p-2}{2p} + \frac{p}{2p^2} + \frac{p-2}{2p^3} + \cdots \right).$$

REMARK 4.3. The fact that $D_N(\sigma) \le 2^s D_N^*(\sigma)$ can be seen from:
Take any $J = \prod_{i=1}^{s} [a_i, b_i)$. For each $i$, define $z_1^{(i)} = a_i, n_i = 1$. Then by Lemma 3.5, $(z_1^{(i)})$ induces a "signed splitting"

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

for $\prod_{i=1}^{s} [0, b_i)$, with signs $\epsilon(\mathbf{j}) = 1$ for all $\mathbf{j}$.

Thus, $A_N(\prod_{i=1}^s [0,b_i)) - N\mu(\prod_{i=1}^s [0,b_i)) = \sum_{\mathbf{j}} A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))$. Therefore, we have

$$\begin{aligned} |A_N(J) - N\mu(J)| &= |(A_N - N\mu)\prod_{i=1}^s [0,b_i) - \sum_{\mathbf{j}\neq(1,\ldots,1)} (A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j})))| \\ &\leq 2^s D_N^*(\sigma) \quad \text{since there are } 2^s \text{ terms each } \leq D_N^*(\sigma) \end{aligned}$$

Taking sup over $J$ yields $D_N(\sigma) \leq 2^s D_N^*(\sigma)$.

REMARK 4.4. It is now worthwhile to look at the proof again to see what is essential to the Halton sequences. Doing so is very important in applying the same proof to other types of sequences.

The proof begins with two number theoretical claims, from which a signed splitting of a particular interval is obtained. Then by using Lemma 3.1 and careful case analysis, an estimate for $|\sum_1|$ is obtained in Claim 3. To obtain the desired upper bound for $|\sum_2|$, some set theoretical manipulations were applied to get the containment $K \subseteq K_4$. By applying Lemma 3.1 on $K_4$, upper bounds of $A_N(K)$ and $N\mu(K)$ were obtained. The proof concludes by applying Lemma 3.3 on the sum of products of the upper bounds for each $K$.

In other words, in order to prove Theorem 2.1, all that is needed about the Halton sequences is Lemma 3.1. As Lemma 3.1 also holds for the modified Halton sequences (based on any permutations $\tau_j^{(i)}$), so does Theorem 2.1. It is also not hard to see that Lemma 3.1 holds for those sequences because equation (4.2) is true.

REMARK 4.5. The estimate for $c_s$ holds as advertised since:

First off, by expanding, we see that

$$\begin{aligned} \prod_{i=1}^s \left(\frac{(p_i-1)\ln N}{2\ln p_i} + s\right) &= \frac{\ln^s N}{2^s}\left(\prod_{i=1}^s \frac{p_i - 1}{\ln p_i}\right) + \text{ remaining terms all} \\ &\quad\ \text{dominated by } O(\ln^{s-1} N) \\ &= \frac{\ln^s N}{2^s}\left(\prod_{i=1}^s \frac{p_i - 1}{\ln p_i}\right) + O(\ln^{s-1} N). \end{aligned}$$

Now, for $N$ large, $\lfloor \frac{p_i}{2} \rfloor \frac{\ln N}{\ln p_i} \gg k$, hence,

$$2^s \sum_{k=0}^{s-1} \frac{p_{k+1}}{k!} \prod_{i=1}^k \left(\left\lfloor \frac{p_i}{2} \right\rfloor \frac{\ln N}{\ln p_i} + k\right) \sim 2^s \sum_{k=0}^{s-1} d_k \ln^k N = O(\ln^{s-1} N),$$

where $\sim$ denotes "on the same order" and $d_k = \frac{p_{k+1}}{k!} \prod_{i=1}^{k} \left\lfloor \frac{p_i}{2} \right\rfloor \frac{1}{\ln p_i}$ is some constant. Similar treatment on $u$ implies that $u = O(\ln^{s-1} N)$. Thus,

$$ND_N(\sigma) < \left( \frac{1}{s!} \prod_{i=1}^{s} \frac{p_i - 1}{\ln p_i} \right) \ln^s N + O(\ln^{s-1} N).$$

Strictly speaking, we get from Theorem 2.1 only $\leq$. However, because of the presence of $O(\ln^{s-1} N)$, we could replace $\leq$ by $<$.

As claimed before, we now have the following result:
**Corollary 2.1:** $\lim_{s\to\infty} c_s(p_1, \ldots, p_s) = 0$, where $p_1, \ldots, p_s$ are the first $s$ primes.

*Proof.* For sufficiently large $x$, say $x > M$, we know from Analytic Number Theory that $\pi(x) > x \ln^{-1} x$, where $\pi(x)$ is the number of prime numbers less than or equal to $x$. So for large $n$, we have

$$n - 1 = \pi(p_n - 1) > \frac{p_n - 1}{\ln(p_n - 1)} > \frac{p_n - 1}{\ln(p_n)}$$
$$\Rightarrow \frac{p_n - 1}{n \ln p_n} < \frac{n-1}{n}.$$

Thus, for $s > M$

$$\begin{aligned} c_s &= \frac{1}{s!} \prod_{i=1}^{s} \frac{p_i - 1}{\ln p_i} = \prod_{i=1}^{M} \frac{p_i - 1}{i \ln p_i} \prod_{i=M+1}^{s} \frac{p_i - 1}{i\colon \ln p_i} \\ &\leq \prod_{i=1}^{M} \frac{p_i - 1}{i\colon \ln p_i} \cdot \prod_{i=M+1}^{s} \frac{i-1}{i} \\ &= \prod_{i=1}^{M} \frac{p_i - 1}{i\colon \ln p_i} \cdot \frac{M}{s} \\ &\to 0 \text{ as } s \to \infty. \qquad \square \end{aligned}$$

## 5. Proofs Leading to Theorem 2.3

After proving the first main result, Atanassov turned to improve the bounds even more for the so-called "modified Halton sequence". To start, he proved the existence of admissible integers which are vital in the construction of the modified Halton sequence.

**Lemma 4.1.** Let $p_1, \dots, p_s$ be distinct primes. There exist admissible integers $k_1, \dots, k_s$.

*Proof.* Observe that given any positive integers $a, b,$ a prime number $p$ and a primitive root $g \bmod p$, if $a \equiv g^m \pmod{p}, b \equiv g^n \pmod{p}$, then by Fermat's Little Theorem, we see that $a \equiv b \pmod{p}$ if and only if $m \equiv n \pmod{p-1}$. Back to the proof, for each $i = 1, \dots, s,$ let $g_i$ be a fixed primitive root mod $p_i$. Write $p_j \equiv g_i^{a_{ij}} \pmod{p_i}$ for $j \neq i$. We also write $k_i \equiv g_i^{a_{ii}} \pmod{p_i}$ and $b_i \equiv g_i^{m_i} \pmod{p_i}$. We need to prove that we can find integers $k_1, \dots, k_s$ so that for any integers $b_1, \dots, b_s$, the defining congruence (2.2) for admissible integers can always be satisfied. By the above observation, we see that (2.2) is equivalent to

$$a_{i1}x_1 + \cdots + a_{is}x_s \equiv m_i \pmod{p_i - 1}, \qquad i = 1, \dots, s, \tag{5.1}$$

where $x_1, \dots, x_s$ are integer variables representing $\alpha_1, \dots, \alpha_s$. We show that for some suitable choice of the numbers $r_i = a_{ii}$, (5.1) can always be solved for integers $x_1, \dots, x_s$ given any $m_1, \dots, m_s$.

We shall show by induction that the determinant of the matrix $C = (c_{ij})$, where $c_{ij} = a_{ij}, c_{ii} = a_{ii} = r_i$ can be made 1 for some $r_1, \dots, r_s$ given any $a_{ij}, j \neq i$. The base case when $s = 1$ is obvious. In general when $s > 1$, applying cofactor expansion along the last column of $C$ with cofactors $C_{ij}$ gives

$$\det(C) = a_{1s}C_{1s} + \cdots + r_sC_{ss}.$$

By induction hypothesis, choose $r_1, \dots, r_{s-1}$ given $(a_{ij})_{1 \le i \le s-1, 1 \le j \le s-1}$ so that $C_{ss} = (-1)^{s+s} \cdot 1 = 1$. Take $r_s = 1 - (a_{1s}C_{1s} + \cdots + a_{s-1,s}C_{s-1,s})$, then $\det(C) = 1$.

Now, $C^{-1} = \frac{1}{\det(C)} \operatorname{adj}(C) = \operatorname{adj}(C) \in M_s(\mathbf{Z})$ where $\operatorname{adj}(C)$ is the adjugate matrix of $C$. That is, $C^{-1}$ is an $s \times s$ matrix with integer entries. Multiplying $C^{-1}$ by $(m_1, \dots, m_s)^T$ on the right gives an $s$-vector whose (integer) entries solve (5.1), where $^T$ denotes the transpose operator. Actually, they solve (5.1) with congruences replaced by equalities.

Putting each $k_i$ to be the remainder of $g_i^{r_i} \bmod p_i$ gives admissible integers $k_1, \dots, k_s$. □

To prove the next lemma, we need an easy result from Calculus:

**Lemma 4.2.-1** $|e(-x) - 1| = 2\sin(\pi\,\|x\|) \ge 4\,\|x\|$, where $e(x) = \exp(2\pi i x)$ with $i = \sqrt{-1}$.

*Proof.* We have that

$$\begin{aligned} |\,e(-x)-1| &= |\cos 2\pi x - i\sin 2\pi x - 1| = |-2\sin^2\pi x - i\,2\cos\pi x\sin\pi x| \\ &= 2|\sin\pi x| = 2\sin\pi\,\|x\| \quad \text{by a simple case analysis} \\ &\geq 2\cdot \underbrace{\frac{1-0}{1/2-0}(\|x\|-0)}_{\substack{\text{equation of line segment joining} \\ (0,\sin(\pi 0)) \text{ and } (1/2,\sin(\pi/2))}} = 4\,\|x\| \end{aligned}$$

since $\sin\pi y$ is convex on $[0,1/2]$. □

**Lemma 4.2.** Let $\mathbf{p}=(p_1,\ldots,p_s)$ be a vector of distinct prime numbers and $\omega=\{\omega_n\}_{n=0}^{\infty}$ be a sequence with $\omega_n=(\omega_n^{(1)},\ldots,\omega_n^{(s)})\in\mathbf{Z}^s$. Let $\mathbf{b}$ and $\mathbf{c}$ be fixed elements in $\mathbf{Z}^s$, such that $0\leq b_i<c_i\leq p_i$, for $i=1,\ldots,s$. Denote by $a_K(\mathbf{b},\mathbf{c})$ the number of terms of $\omega$ among the first $K$ such that for all $i=1,\ldots,s$, we have $b_i\leq\omega_n^{(i)} \bmod p_i<c_i$. Then

$$\sup_{\mathbf{b},\mathbf{c}}\left|a_K(\mathbf{b},\mathbf{c})-K\prod_{i=1}^{s}\frac{c_i-b_i}{p_i}\right|\leq\sum_{\mathbf{j}\in M(\mathbf{p})}\frac{|S_K(\mathbf{j},\omega)|}{R(\mathbf{j})}, \tag{5.2}$$

where

$$S_K(\mathbf{j},\omega)=\sum_{n=0}^{K-1}e\left(\sum_{k=1}^{s}\frac{j_k\omega_n^{(k)}}{p_k}\right),$$

and $R(\mathbf{j})$ is defined as in (3.1).
As already noted in Section 3, we mention that Lemma 4.2 is a special case of [15, Satz 2].

*Proof.* Observe that

$$\frac{1}{p_i}\sum_{j=0}^{p_i-1}e\left(j\frac{m}{p_i}\right)=\begin{cases}1 & \text{if } p_i|m\\ 0 & \text{if } p_i\not|\,m,\end{cases} \tag{5.3}$$

for any integer $p_i$, which could easily be proven as a geometric sum.
By multiplying a few sums as in (5.3) together, we see that for integers $l_1,\ldots,l_s$, and $w_n^{(1)},\ldots,w_n^{(s)}$ :

$$\sum_{\substack{\mathbf{j}\,|0\leq j_i<p_i\\ i=1,\ldots,s}}\frac{e\left(j_1\frac{w_n^{(1)}-l_1}{p_1}+\cdots+j_s\frac{w_n^{(s)}-l_s}{p_s}\right)}{p_1\cdots p_s}=\begin{cases}1 & \text{if } w_n^{(i)}\equiv l_i \pmod{p_i}\\ & \text{for all } i=1,\ldots,s\\ 0 & \text{otherwise.}\end{cases}$$

Therefore, we have

$$
\begin{aligned}
a_K(\mathbf{b},\mathbf{c}) &= \sum_{\text{all } w_n} \sum_{\substack{\text{possible values } l_i \\ \text{for } w_n^{(i)} \bmod p_i}} \begin{cases} 1 & \text{if } w_n^{(i)} \equiv l_i \pmod{p_i} \text{ for all } i = 1,\dots,s \\ 0 & \text{otherwise} \end{cases} \\
&= \sum_{n=0}^{K-1} \sum_{l_1=b_1}^{c_1-1} \cdots \sum_{l_s=b_s}^{c_s-1} \sum_{\mathbf{j}\in M(\mathbf{p})\cup\{\mathbf{0}\}} \frac{e\left(j_1 \frac{w_n^{(1)}-l_1}{p_1} + \cdots + j_s \frac{w_n^{(s)}-l_s}{p_s}\right)}{p_1 \cdots p_s} \\
&= \sum_{\mathbf{j}\in M(\mathbf{p})\cup\{\mathbf{0}\}} \left[ \sum_{n=0}^{K-1} e\left(j_1 \frac{w_n^{(1)}}{p_1} + \cdots + j_s \frac{w_n^{(s)}}{p_s}\right) \cdot \prod_{i=1}^{s} \frac{1}{p_i} \sum_{l_i=b_i}^{c_i-1} e\left(-j_i \frac{l_i}{p_i}\right) \right].
\end{aligned}
$$

Observe that the term corresponding to $\mathbf{j} = \mathbf{0}$ is

$$
\sum_{n=0}^{K-1} e(0) \cdot \prod_{i=1}^{s} \frac{1}{p_i} \sum_{l_i=b_i}^{c_i-1} e(0) = K \prod_{i=1}^{s} \frac{c_i - b_i}{p_i},
$$

so,

$$
a_K(\mathbf{b},\mathbf{c}) - K \prod_{i=1}^{s} \frac{c_i - b_i}{p_i} = \sum_{\mathbf{j}\in M(\mathbf{p})} S_K(\mathbf{j},\omega) \cdot \prod_{i=1}^{s} \frac{1}{p_i} \sum_{l_i=b_i}^{c_i-1} e\left(-j_i \frac{l_i}{p_i}\right). \tag{5.4}
$$

Comparing (5.4) and (5.2), we see that it suffices to establish:

$$
\frac{1}{p_i} \left| \sum_{l_i=b_i}^{c_i-1} e\left(-j_i \frac{l_i}{p_i}\right) \right| \le \frac{1}{r_i(j_i)}.
$$

When $j_i = 0$, the left hand side $LHS = (c_i - b_i)/p_i \le 1 = RHS$ the right hand side. For $j_i \neq 0$, we have that $e(-j_i/p_i) \neq 1$ and so:

$$
\begin{aligned}
\frac{1}{p_i} \left| \sum_{l_i=b_i}^{c_i-1} e\left(-j_i \frac{l_i}{p_i}\right) \right| &= \frac{1}{p_i} \left| \frac{e\left(-j_i \frac{b_i}{p_i}\right) - e\left(-j_i \frac{c_i}{p_i}\right)}{1 - e\left(-\frac{j_i}{p_i}\right)} \right| \\
&\le \frac{1}{p_i} \frac{\left| e\left(-j_i \frac{b_i}{p_i}\right) \right| + \left| e\left(-j_i \frac{c_i}{p_i}\right) \right|}{\left| e\left(-\frac{j_i}{p_i}\right) - 1 \right|} \\
&\le \frac{1}{p_i} \frac{2}{4\,\|j_i/p_i\|} \text{ by Lemma 4.2.-1 and since } |\,e(\cdot)| = 1 \\
&\le \max\left\{ \frac{1}{p_i} \frac{2}{4(j_i/p_i)}, \frac{1}{p_i} \frac{2}{4(1 - j_i/p_i)} \right\} \\
&= \max\left\{ \frac{1}{2j_i}, \frac{1}{2(p_i - j_i)} \right\} = \frac{1}{\min\{2j_i, 2(p_i - j_i)\}} \\
&= \frac{1}{r_i(j_i)},
\end{aligned}
$$

since $0 < j_i < p_i$, so $\min\{2j_i, 2(p_i - j_i)\} > 1$ and hence $r_i(j_i) = \min\{2j_i, 2(p_i - j_i)\}$

According to the above discussion, the proof is now complete. □

**Lemma 4.3.** Let $\sigma = \sigma(p_1, \dots, p_s, k_1, \dots, k_s) = \{x_n\}_{n=0}^{\infty}$ be a modified Halton sequence. Fix some elementary interval

$$I = \prod_{i=1}^{s} [a_i p_i^{-\alpha_i}, (a_i + 1) p_i^{-\alpha_i}), \qquad 0 \le a_i < p_i^{\alpha_i},$$

and a subinterval

$$J = \prod_{i=1}^{s} [a_i p_i^{-\alpha_i} + b_i p_i^{-\alpha_i - 1}, a_i p_i^{-\alpha_i} + c_i p_i^{-\alpha_i - 1}), \qquad 0 \le b_i < c_i \le p_i.$$

Let $n_0$ be the smallest integer such that $x_{n_0} \in I$ (whose existence will be proved). Suppose that $x_{n_0}$ belongs to

$$J_1 = \prod_{i=1}^{s} [a_i p_i^{-\alpha_i} + d_i p_i^{-\alpha_i - 1}, a_i p_i^{-\alpha_i} + (d_i + 1) p_i^{-\alpha_i - 1}),$$

and consider the sequence $\omega = \{y_t\}_{t=0}^{\infty}$ with $y_t \in \mathbf{Z}^s$ defined by

$$y_t^{(i)} = d_i + t P_i(k_i; (\alpha_1, \dots, \alpha_s)).$$

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 $\sigma$ that belong to $I$ are of the form $n = n_0 + t \prod_{i=1}^{s} p_i^{\alpha_i}$.
2. For these $n$, the relation $x_n \in J$ is possible 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 $t$:

$$d_i + t P_i(k_i; (\alpha_1, \dots, \alpha_s)) \equiv l_i \pmod{p_i}, \qquad i = 1, \dots, s. \tag{5.5}$$

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

$$|A_N(J) - N\mu(J)| < 1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{|S_K(\mathbf{l}, \omega)|}{R(\mathbf{l})}.$$

*Proof.*

1. Done in the proof for Lemma 3.1 with $n_0 = b$ for the same $b$ defined there.

2. Fix any $i = 1, \ldots, s$, look at the next digit (the $\alpha_i + 1^{\text{st}}$ digit) of $n = n_0 + t\prod_{j=1}^{s} p_j^{\alpha_j}$ in base $p_i$ : The coefficient for $p_i^{\alpha_i}$ in $n$ in base $p_i$, call it $s_i$, satisfies

$$s_i \equiv k_i^{-\alpha_i} d_i + t \prod_{\substack{j=1 \\ j \neq i}}^{s} p_j^{\alpha_j} \pmod{p_i},$$

since $k_i^{\alpha_i}$(such coefficient for $n_0$) $\equiv d_i \pmod{p_i}$, as $x_{n_0} \in J_1$. Thus, the coefficient of $p_i^{-\alpha_i - 1}$ in $x_n$, say $l_i$, satisfy

$$l_i \equiv k_i^{\alpha_i} s_i \equiv d_i + tP_i(k_i; (\alpha_1, \ldots, \alpha_s)) \pmod{p_i}.$$

Now the result follows immediately.

3. By part (2), we see that

$$\begin{pmatrix} \text{number of } w_n \text{ accounted} \\ \text{towards } a_K(\mathbf{b}, \mathbf{c}) \end{pmatrix} = \begin{pmatrix} \text{number of} \\ \text{solutions to (5.5)} \end{pmatrix} = A_N(J),$$

that is, $A_N(J) = a_K(\mathbf{b}, \mathbf{c})$. The given condition also implies that

$$(K-1)\prod_{i=1}^{s} p_i^{\alpha_i} \leq n_0 + (K-1)\prod_{i=1}^{s} p_i^{\alpha_i} < N \leq n_0 + K\prod_{i=1}^{s} p_i^{\alpha_i} < (K+1)\prod_{i=1}^{s} p_i^{\alpha_i}.$$

Multiplying by $\mu(J) = \prod_{i=1}^{s} \frac{c_i - b_i}{p_i^{\alpha_i + 1}} \geq 0$, we get:

$$(K-1)\prod_{i=1}^{s} \frac{c_i - b_i}{p_i} < N\mu(J) < (K+1)\prod_{i=1}^{s} \frac{c_i - b_i}{p_i}$$

and hence

$$-1 + K\prod_{i=1}^{s} \frac{c_i - b_i}{p_i} < N\mu(J) < K\prod_{i=1}^{s} \frac{c_i - b_i}{p_i} + 1$$

since $c_i - b_i \leq p_i$. Therefore,

$$\begin{aligned} |A_N(J) - N\mu(J)| &< \left| a_K(\mathbf{b}, \mathbf{c}) - K\prod_{i=1}^{s} \frac{c_i - b_i}{p_i} \right| + 1 \\ &\leq 1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{|S_K(\mathbf{l}, \omega)|}{R(\mathbf{l})} \quad \text{by Lemma 4.2.} \qquad \square \end{aligned}$$

**Proof of modified Proposition 4.1.**

*Proof.* We expand an arbitrary $\mathbf{z} = (z^{(1)}, \dots, z^{(s)}) \in \mathbf{E}^s$ in the same way as in the proof of Theorem 2.1. Using the same idea, and same notation, there we obtain a "signed splitting" and equality (4.5), that is, $A_N(J) - N\mu(J) = \sum_1 + \sum_2$ where $J = \prod_{i=1}^s [0, z^{(i)})$. The estimates for $\sum_1, \sum_2$ in the proof for Theorem 2.1 use only Lemma 3.1, 3.3 and 3.5 all of which work here. We will use the same estimate for $\sum_2$ but will reevaluate $|\sum_1| \le \sum_{\mathbf{j} \in T(N)} |A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))|$ for a tighter bound.

Fix some $\widetilde{\mathbf{j}} = (\widetilde{j}_1, \dots, \widetilde{j}_s) \in T(N)$.

**Case 1:** $\widetilde{j}_i \ge 1$ for all $i = 1, \dots, s$. That is, $\widetilde{\mathbf{j}} \in T^*(N)$.

Write $\mathbf{1} = (1, \dots, 1)$, we define $\mathbf{j} = \widetilde{\mathbf{j}} - \mathbf{1}$, then obviously, each $j_i \ge 0$ and $\mathbf{j} \in T(N)$. The interval $I(\widetilde{\mathbf{j}})$—see Equation (4.4) on page 13—is contained inside some elementary interval

$$G = \prod_{i=1}^s [c_i p_i^{-j_i}, (c_i + 1) p_i^{-j_i})$$

since $|z^{(i)}_{\widetilde{j}_i} - z^{(i)}_{\widetilde{j}_i+1}| = |a^{(i)}_{\widetilde{j}_i}| p_i^{-\widetilde{j}_i} \le p_i^{-\widetilde{j}_i+1} = p_i^{-j_i}$, and $p_i^{j_i} z^{(i)}_{\widetilde{j}_i} = p_i^{\widetilde{j}_i - 1} z^{(i)}_{\widetilde{j}_i} \in \mathbf{Z}$, for each $i$.

Consider the sequence $\omega = \{\omega_n\}_{n=0}^{\infty} \subseteq \mathbf{Z}^s$, defined as in Lemma 4.3, that is, $w_n^{(i)} = d_i + nP_i(k_i; \mathbf{j})$ where the integers $d_i$ are determined by the condition that the first term of the sequence $\sigma$ that falls in $G$ fits into the interval

$$\prod_{i=1}^s [c_i p_i^{-j_i} + d_i p_i^{-j_i - 1}, c_i p_i^{-j_i} + (d_i + 1) p_i^{-j_i - 1}). \tag{5.6}$$

From part (3) in Lemma 4.3 (where (5.6), $I(\widetilde{\mathbf{j}})$ and $G$ above correspond respectively to $J_1$, $J$ and $I$ there), it follows that

$$|A_N(I(\widetilde{\mathbf{j}})) - N\mu(I(\widetilde{\mathbf{j}}))| < 1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{|S_K(\mathbf{l}, \omega)|}{R(\mathbf{l})}, \tag{5.7}$$

where $K$ is the number of terms of $\sigma$ among the first $N$ terms that fall into $G$. Note that we can apply Lemma 4.3 to obtain the above because the end points of $I(\widetilde{\mathbf{j}})$ are of the form $m/p_i^{\widetilde{j}_i} = m/p_i^{j_i+1}$ for some integer $m$.

REMARK 5.1. In [1], the above treatment is applied to *any* $\widetilde{\mathbf{j}} \in T(N)$; this is where we believe there is a mistake, because the application of Lemma 4.3 as done above requires $\widetilde{\mathbf{j}}$ to be such that $\widetilde{j}_i - 1 \geq 0$ for all $i$, which is why we use a two-case analysis here. Alternatively, we could define $\mathbf{j} = \max\{\widetilde{\mathbf{j}} - \mathbf{1}, \mathbf{0}\}$ where the "max" operation of vectors is a component-wise operation, and $\mathbf{0} = (0, \dots, 0)$. However, such a definition would lead to a new form of Proposition 4.1 which will be discussed in more details in Section 6.

We now digress a little to prove a result about exponential sums: for $\alpha \notin \mathbf{Z}$ and so $e(\alpha) \neq 1$, we have

$$\begin{aligned} \left| \sum_{k=0}^{K-1} e(k\alpha + \beta) \right| &= \left| \frac{e(\beta)(1 - e(K\alpha))}{1 - e(\alpha)} \right| \quad \text{as a geometric sum} \\ &= \frac{|\, e(\beta)| \sin(\pi \, \|K\alpha\|)}{\sin \pi \, \|\alpha\|} \leq \frac{1}{2\,\|\alpha\|} \end{aligned}$$

by Lemma 4.2.-1 and the fact that $\sin(\cdot) \leq 1$.
Since the $p_i$'s are coprime, we see that $P_i(k_i, \mathbf{j}) \neq 0$, 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 $1 \leq t \leq s$ such that $l_t \neq 0$, and so $p_t \nmid l_t$. Define $\widetilde{\alpha} = \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \mathbf{j})$. Putting the summands in $\widetilde{\alpha}$ into common denominator $p_1 \cdots p_s$, we see that $p_t$ divides every summand in the numerator except for the term $l_t P_t(k_t; \mathbf{j}) p_1 \cdots p_{t-1} p_{t+1} \cdots p_s$, as $p_t$, being a prime, does not divide any term in that product. Since $p_t$ divides the denominator, it follows that $\widetilde{\alpha} \notin \mathbf{Z}$. Thus, by the above digression, we have

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

Combining this result with (5.7), we obtain

$$\begin{aligned} &\sum_{\widetilde{\mathbf{j}} \in T^*(N)} |A_N(I(\widetilde{\mathbf{j}})) - N\mu(I(\widetilde{\mathbf{j}}))| \\ &\qquad \leq \sum_{\widetilde{\mathbf{j}} \in T^*(N)} \left( 1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})} \right) \end{aligned} \tag{5.8}$$

which is the first piece as in the result of the proposition . As we will see later, we can still prove Theorem 2.3 using our modified Proposition 4.1.

**Case 2:** $\widetilde{j}_i = 0$ for some $i$. That is, $\widetilde{\mathbf{j}} \in T_z(N)$.

We shall use a similar estimate as (4.7), which was used in the proof of Theorem 2.1. Remember that as $T_z(N) \subset T(N)$, none of the $\widetilde{\mathbf{j}} \in T_z(N)$ has any $\tilde{j}_i = n_i$. So Lemma 3.1 applies and we get:

$$\begin{aligned} \sum_{\widetilde{\mathbf{j}} \in T_z(N)} |A_N(I(\widetilde{\mathbf{j}})) - N\mu(I(\widetilde{\mathbf{j}}))| &\leq \sum_{i=1}^{s} \sum_{\widetilde{\mathbf{j}} \in T(N), \widetilde{j}_i = 0} \prod_{\substack{k=1 \\ k \neq i}}^{s} \left| a^{(k)}_{\widetilde{j}_k} \right| \\ &\leq \sum_{i=1}^{s} \frac{1}{(s-1)!} \prod_{\substack{k=1 \\ k \neq i}}^{s} \left( \frac{p_k}{2} \frac{\ln N}{\ln p_k} + s - 1 \right) \\ &= O(\ln^{s-1} N), \end{aligned} \tag{5.9}$$

since each summand is $O(\ln^{s-1} N)$ and there is $s$, which does not depend on $N$, such summands. Above, we recalled the fact that $a_0^{(i)} \in \{0, 1\}$ by definition. Note that the first inequality above is quite conservative, in the sense that vectors with at least one zero component are counted more than once. But the bound is good enough to get the desired result (Theorem 2.3), and thus we haven't tried to make it tighter.

Combining (5.9) and the estimate (4.12) for $\sum_2$, we get the remaining two pieces in the desired result.

Combining Case 1 and Case 2, we see that the proof is complete now. □

The following lemma will be used twice in the proof for Lemma 4.4:

**Lemma 4.4.-1** Let $m$ be any positive integer, then

$$\sum_{j=1}^{m-1} \frac{1}{\min(j, m-j)} \leq 2 \ln m.$$

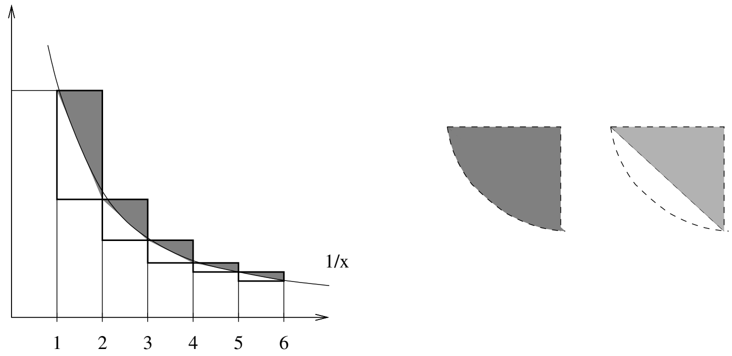
*Proof.* Now,

$$\sum_{k=1}^{n} \frac{1}{k} = 1 + \int_1^n \frac{1}{x} dx + \text{shaded area on Fig. 1} - \sum_{k=1}^{n-1} \underbrace{1 \cdot \left( \frac{1}{k} - \frac{1}{k+1} \right)}_{\substack{\text{area of each little rectangle} \\ \text{with thick boundary}}} .$$

Also, looking at Figure 1, we have that

$$\text{shaded area} \leq \gamma - \sum_{k=n}^{\infty} \frac{1}{2} \left( \frac{1}{k} - \frac{1}{k+1} \right)$$

FIGURE 1
Left: integrating $1/x$; Right: comparison of regions




where $\gamma$ is the Euler constant, and is equal to the sum of all the surfaces in shaded area. The inequality holds because $\ln x$ is a convex function, and therefore the surface area of each shaded region is at least as large as the corresponding triangle (see right-hand-side of Figure 1), whose area is given by

$$\frac{1}{2}\left(\frac{1}{k}-\frac{1}{k+1}\right).$$

Combining these facts gives

$$\begin{aligned}\sum_{k=1}^{n}\frac{1}{k} &\leq 1+\ln n+\gamma-\sum_{k=n}^{\infty}\frac{1}{2}\left(\frac{1}{k}-\frac{1}{k+1}\right)-\sum_{k=1}^{n-1}1\cdot\left(\frac{1}{k}-\frac{1}{k+1}\right)\\ &= 1+\ln n+\gamma-\frac{1}{2n}-(1-\frac{1}{n})\\ &= \ln n+\gamma+\frac{1}{2n}.\end{aligned}$$

For $2n \geq 9$, we see that

$$\ln n+\gamma+\frac{1}{2n} \leq \ln n+0.5773+\frac{1}{9}=\ln n+0.6884\bar{1}<\ln n+\ln 2=\ln 2n,$$

where we used the fact that $\gamma = 0.5772...$ and $\ln 2 = 0.693147....$ So for $m \geq 10$, we have that

$$\begin{aligned}
\sum_{j=1}^{m-1} \frac{1}{\min(j, m-j)} &= \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{\lfloor m/2 \rfloor} + \ldots + \frac{1}{2} + 1 \\
&\leq 2 \sum_{j=1}^{\lfloor m/2 \rfloor} \frac{1}{j} \quad \left( \begin{matrix} \text{with equality iff } m \text{ is odd so} \\ \text{there were an even number of terms} \end{matrix} \right) \\
&\leq 2 \ln \left( \lfloor \frac{m}{2} \rfloor \right) \qquad (\text{since } 2\lfloor m/2 \rfloor \geq 2 \cdot 5 = 10 \geq 9) \\
&\leq 2 \ln \left( 2 \frac{m}{2} \right) = 2 \ln m \qquad (\text{as } \lfloor m/2 \rfloor \leq (m/2)).
\end{aligned}$$

One can easily check that $\sum_{j=1}^{m-1} \min(j, m-j)^{-1} \leq 2 \ln m$ for $m \leq 9$ as well. In fact,

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $\sum_{j=1}^{m-1} \min(j, m-j)^{-1}$ | 0 | 1 | 2 | 2.5 | 3 | $3.\bar{3}$ | $3.\bar{6}$ | $3.91\bar{6}$ | $4.1\bar{6}$ |
| $2 \ln m$ (to 2 decimals) | 0 | 1.3 | 2.1 | 2.7 | 3.2 | 3.5 | 3.8 | 4.1 | 4.3 |

So

$$\sum_{j=1}^{m-1} \min(j, m-j)^{-1} \leq 2 \ln m \qquad \text{for all } m \geq 1. \qquad \square$$

**Lemma 4.4.** Let $p_1, \ldots, p_s$ be distinct prime numbers. Then

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

*Proof.* Write $P = p_1 \cdots p_s$. Fix some $\mathbf{j} \in M(\mathbf{p})$, then for each $i = 1, \ldots, s$, we have that $1 \leq j_i \leq p_i - 1$. Let $I$ denote the subset of indices for which $j_i = 0$ and let $J$ denote its complement. Let $G(\mathbf{j})$ denote the contribution to the above sum from $\mathbf{j}$. We wish to prove,

$$G(\mathbf{j}) \leq \frac{P \ln P}{R(\mathbf{j})}.$$

Without loss of generality, assume $I = \{1, \ldots, k\}$ for some $k$. For each $i = k+1, \ldots, s$, write $j_i^* = j_i p_{k+1} \cdots p_s / p_i$. The map

$$\begin{aligned}
(\mathbf{Z}/p_{k+1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_s\mathbf{Z})^\times &\rightarrow (\mathbf{Z}/p_{k+1} \cdots p_s \mathbf{Z})^\times \\
(m_{k+1}, \ldots, m_s) &\mapsto j_{k+1}^* m_{k+1} + \cdots + j_s^* m_s
\end{aligned}$$

is an isomorphism by the Chinese Remainder Theorem since

$$\gcd(j^*_{k+1},\ldots,j^*_s,p_{k+1}\cdots p_s)=1.$$

In other words, for each $t=1,\ldots,p_{k+1}\cdots p_s$ coprime to $p_{k+1}\cdots p_s$, there exists a unique tuple $(m_{k+1},\ldots,m_s)$ with $1\le m_i\le p_i-1$ such that

$$\frac{j_{k+1}m_{k+1}}{p_{k+1}}+\cdots+\frac{j_s m_s}{p_s}-\frac{t}{p_{k+1}\cdots p_s}\in\mathbf{Z}.$$

Therefore,

$$\begin{aligned}
G(\mathbf{j}) &= \frac{1}{2R(\mathbf{j})}\sum_{\substack{1\le t\le p_{k+1}\cdots p_s\\ gcd(t,p_{k+1}\cdots p_s)=1}}||\frac{t}{p_{k+1}\cdots p_s}||^{-1}\\
&\le \frac{p_1\cdots p_k}{2R(\mathbf{j})}\sum_{t=1}^{p_{k+1}\cdots p_s-1}\frac{1}{\min(\frac{t}{p_{k+1}\cdots p_s},1-\frac{t}{p_{k+1}\cdots p_s})}\\
&= \frac{P}{2R(\mathbf{j})}\sum_{t=1}^{p_{k+1}\cdots p_s-1}\frac{1}{\min(t,p_{k+1}\cdots p_s-t)}\\
&\le \frac{P}{2R(\mathbf{j})}\cdot 2\ln(p_{k+1}\cdots p_s) \quad \text{by Lemma 4.4.-1}\\
&\le \frac{P\ln P}{R(\mathbf{j})}.
\end{aligned}$$

Summing everything up, we get what we want:

$$\begin{aligned}
G &= \sum_{\mathbf{j}\in M(\mathbf{p})}G(\mathbf{j})\le\sum_{\mathbf{j}\in M(\mathbf{p})}\frac{P\ln P}{R(\mathbf{j})}\\
&= P\ln P\left(-\frac{1}{R(\mathbf{0})}+\sum_{m_1=1}^{p_1-1}\cdots\sum_{m_s=1}^{p_s-1}\prod_{k=1}^{s}\frac{1}{r_k(j_k)}\right) \quad \text{since } \mathbf{0}\notin M(\mathbf{p})\\
&= P\ln P\left(-1+\prod_{k=1}^{s}\sum_{j_k=0}^{p_k-1}\frac{1}{r_k(j_k)}\right) \quad \text{by associativity}\\
&= P\ln P\left[-1+\prod_{k=1}^{s}\left(\frac{1}{r_k(0)}+\sum_{j_k=1}^{p_k-1}\frac{1}{2\min(j_k,p_k-j_k)}\right)\right]\\
&\le P\ln P\left[-1+\prod_{k=1}^{s}\left(1+\frac{1}{2}2\ln p_k\right)\right] \quad \text{by Lemma 4.4.-1}\\
&= \sum_{i=1}^{s}\ln p_i\prod_{i=1}^{s}p_i\left(-1+\prod_{j=1}^{s}(1+\ln p_i)\right) \quad \text{by definition of } P.
\end{aligned}$$

□

Theorem 2.3 can now be proved:

**Proof of Theorem 2.3.**

*Proof.* The proof relies on (modified) Proposition 4.1. Take $J = \prod_{i=1}^{s} [0, z_i)$ and form $I(\mathbf{j})$ as before.
Write $K = \prod_{i=1}^{s}(p_i - 1)$. For each nonnegative vectors $\mathbf{a} = (a_1, \dots, a_s) \in \mathbf{Z}^s$, we consider the box of integers $U(\mathbf{a}) = \{(j_1, \dots, j_s) |\ a_i K \leq j_i < (a_i + 1)K,$ for all $i = 1, \dots, s\}$.

**Claim:** For each $\mathbf{b} = (b_1, \dots, b_s) \in \mathbf{Z}^s$ with $1 \leq b_i \leq p_i - 1$ for each $i$, there are exactly $K^{s-1}$ $s$-tuples $\mathbf{j} \in U(\mathbf{a})$ such that

$$P_i(k_i; \mathbf{j}) = b_i \qquad \text{for all } i = 1, \dots, s. \tag{5.10}$$

**Proof:** Observe that there are $K^s$ vectors in $U(\mathbf{a})$ with only $K$ distinct such vectors $\mathbf{b} = (b_1, \dots, b_s)$. By the Pigeonhole principle, there is a $\mathbf{b}_0$ so that (5.10) has at least $K^{s-1}$ solutions. Now write $\mathbf{b}_0 = (b_1, \dots, b_s)$ with $1 \leq b_i \leq p_i - 1$. Since $p_i \not| b_i$, there exists $m_i \in \mathbf{Z}$ such that $b_i \equiv g_i^{m_i}$ $(\bmod\ p_i)$ where $g_i$ is some primitive root $\bmod p_i$.
Then by definition of $P_i(k_i; \mathbf{j})$ and the proof of Lemma 4.1, we see that $\mathbf{j}$ satisfies (5.10) if and only if:

$$a_{i1} j_1 + \cdots + a_{is} j_s \equiv m_i \pmod{p_i - 1}, \tag{5.11}$$

where $p_j \equiv g_i^{a_{ij}}$ $(\bmod\ p_i)$ for $j \neq i$, and $k_i = g_i^{a_{ii}}$ $(\bmod\ p_i)$ for all $i$. Notice that if the vector $j_1, \dots, j_s$ satisfies (5.11), then so does $\tilde{j}_1, \dots, \tilde{j}_s$ where $\tilde{j}_i = j_i + c_i \prod_{i=1}^{s}(p_i - 1)$ for some integer $c_i$ for all $i$. In what follows, we will not write "for all $i$" just to save some space, but it should be understood that the statements are true for all $i = 1, \dots, s$.
Fix $\mathbf{j}' \in U(\mathbf{a})$, a solution to (5.10) with right-hand side (RHS) equals $\mathbf{b}_0$. Now, given any solution $\mathbf{j}'' \in U(\mathbf{a})$ to (5.10) with RHS $= \mathbf{b}_0$, then from (5.11), we see that $(j_1''', \dots, j_s''')$ satisfies the corresponding homogeneous equation, that is (5.10) with RHS $= \mathbf{b} = (1, \dots, 1)$, (i.e, (5.11) with $m_i = 0$) where $j_i''' = j_i' - j_i''$. Since $j_i', j_i'' \in [a_i K, (a_i + 1)K)$, we have that each $j_i''' \in (-K, K)$. By adding $K = \prod_{i=1}^{s}(p_i - 1)$ to $j_i'''$ if necessary, we get a vector $\mathbf{j}^{(\mathrm{iv})} = (j_1^{(\mathrm{iv})}, \dots, j_s^{(\mathrm{iv})}) \in U(\mathbf{0})$ satisfying the homogeneous equation.
Note that if $\mathbf{j}''^{(2)} = (j_1''^{(2)}, \dots, j_s''^{(2)}) \in U(\mathbf{a})$ is also a solution to (5.10) with RHS $= \mathbf{b}_0$ but with the same resulting vector $\mathbf{j}^{iv}$, then $|(j_i' - j_i'') - (j_i' - j''^{(2)}_i)| = 0$ or $K$. In particular, we see that $K | (j_i'' - j_i''^{(2)})$. However, similar to $j_i'''$, we know that $|(j_i'' - j_i''^{(2)})| < K$. Therefore, $j_i'' = j_i''^{(2)}$ and hence $\mathbf{j}''^{(2)} = \mathbf{j}''$. Since there are at least $K^{s-1}$ distinct

solutions in $U(\mathbf{a})$ to (5.10) with RHS $= \mathbf{b}_0$, there must also be at least $K^{s-1}$ distinct solutions in $U(\mathbf{0})$ to the homogeneous equation.
Now, select an arbitrary RHS $\mathbf{b}'$. Since $k_1, \ldots, k_s$ are admissible, then by Definition 2.1, a particular solution $\mathbf{j}$ to (5.10) with RHS $= \mathbf{b}'$ exists. If $\mathbf{j}'$ is any solution to the homogeneous equation, then from (5.11), we see that $\mathbf{j}+\mathbf{j}'$ is a solution to (5.10) with RHS $= \mathbf{b}'$. As $j_i + j_i' \in [a_iK, (a_i+2)K)$, by subtracting by $K$ if necessary, we get a solution $\mathbf{j}'' \in U(\mathbf{a})$ to (5.10) with RHS $= \mathbf{b}'$. By the same argument as above, distinct such $\mathbf{j}'$ yields distinct such $\mathbf{j}''$. So there are at least $K^{s-1}$ solutions for each RHS $\mathbf{b}'$. By an easy "number-of-elements" argument, one sees that there are *exactly* $K^{s-1}$ solutions for each RHS $\mathbf{b}'$. (See Remark 5.3). □

Obviously, since $\bigcup_{\mathbf{a}\in\mathbf{Z}^s} U(\mathbf{a}) = \mathbf{Z}^s$, each $\mathbf{j} \in T(N)$ is inside some box $U(\mathbf{a})$ with $\prod_{i=1}^s p_i^{a_iK} \le \prod_{i=1}^s p_i^{j_i} \le N$. So

$$\left|\{\mathbf{a} : \prod_{i=1}^{s} p_i^{a_iK} \le N\}\right| = \sum_{\mathbf{a}|\prod_{i=1}^s p_i^{K\cdot a_i} \le N} 1 \le \frac{1}{s!}\prod_{i=1}^{s}\left(1\cdot\frac{\ln N}{\ln p_i^K} + s\right),$$

by Lemma 3.3 with $p_i' = p_i^K, f_i(p_i') = 1$.

For convenience, let us write $t(\mathbf{j})$ for $|A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))|$, we now have:

$$\begin{aligned}\left|\sum\nolimits_1\right| &\le \sum_{\mathbf{j}\in T(N)} t(\mathbf{j}) = \sum_{\mathbf{j}\in T^*(N)} t(\mathbf{j}) + \sum_{\mathbf{j}\in T_z(N)} t(\mathbf{j}) = \sum_{\mathbf{j}\in T^*(N)} t(\mathbf{j}) + O(\ln^{s-1} N)\\ &\le \sum_{\mathbf{a}|\prod_{i=1}^s p_i^{K\cdot a_i}\le N}\ \sum_{\mathbf{j}\in U(\mathbf{a})}\left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})}\frac{\|\sum_{i=1}^s \frac{l_i}{p_i}P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) + O(\ln^{s-1} N)\end{aligned} \tag{5.12}$$

by the proof of (modified) Proposition 4.1 and also the fact that $T^*(N) \subseteq T(N) \subseteq \bigcup\{U(\mathbf{a}) : \prod_{i=1}^s p_i^{a_iK} \le N\}$.

Further, we have, up to a $O(\ln^{s-1} N)$ term whose constant depends only on the primes $p_1, \ldots, p_s$ :

$$
\begin{aligned}
(5.12) \le\ & \underbrace{\left[\frac{1}{s!}\prod_{i=1}^{s}\left(\frac{\ln N}{K\ln p_i}+s\right)\right]}_{\#\mathbf{a}\ \text{with}\ \prod_{i=1}^{s} p_i^{Ka_i}\le N} \\
& \times \underbrace{\sum_{b_1=1}^{p_1-1}\cdots\sum_{b_s=1}^{p_s-1}}_{\substack{\text{enumerate } U(\mathbf{a})\\ \text{according to (5.10)}}} K^{s-1}\left(1+\sum_{\mathbf{l}\in M(\mathbf{p})}\frac{\|l_1\frac{b_1}{p_1}+\cdots+l_s\frac{b_s}{p_s}\|^{-1}}{2R(\mathbf{l})}\right) \\
=\ & \left[\frac{1}{s!}\left(\prod_{i=1}^{s}\frac{\ln N}{K\ln p_i}\right)+O(\ln^{s-1}N)\right]K^{s-1} \\
& \times\left(K+\sum_{\mathbf{l}\in M(\mathbf{p})}\sum_{\mathbf{b}}\frac{\|l_1\frac{b_1}{p_1}+\cdots+l_s\frac{b_s}{p_s}\|^{-1}}{2R(\mathbf{l})}\right) \\
\le\ & \left[\frac{K^{s-1}}{s!}\,\frac{\ln^s N}{K^s\prod_{i=1}^{s}\ln p_i}\right]\left(K+\sum_{i=1}^{s}\ln p_i\prod_{i=1}^{s}p_i\left(-1+\prod_{j=1}^{s}(1+\ln p_i)\right)\right) \\
=\ & \frac{1}{s!}\,\frac{\ln^s N}{\prod_{i=1}^{s}\ln p_i}\left(1-\left(\sum_{i=1}^{s}\ln p_i\right)\prod_{i=1}^{s}\frac{p_i}{p_i-1}\right. \\
& \left.+\left(\sum_{i=1}^{s}\ln p_i\right)\prod_{i=1}^{s}\frac{p_i(1+\ln p_i)}{p_i-1}\right) \\
<\ & \frac{1}{s!}\left(\sum_{i=1}^{s}\ln p_i\prod_{i=1}^{s}\frac{p_i(1+\ln p_i)}{(p_i-1)\ln p_i}\right)\ln^s N
\end{aligned}
\tag{5.13}
$$

where the $K^{s-1}$ in the second line represents the number of $\mathbf{j}\in U(\mathbf{a})$ with $P_i(k_i;\mathbf{j})=b_i$, as in the above Claim; the first equality follows by expanding the product on the first line as in Remark 4.5 on page 19, and the second $K$ comes from summing 1 over all suitable $\mathbf{b}$; the second inequality follows from Lemma 4.4, and by remembering that we are trying to get a bound valid up to $O(\ln^{s-1}N)$ terms; the second equality follows from some cancellation and rearrangement while recalling the definition of $K$ as $\prod_{i=1}^{s}(p_i-1)$; and finally, the last inequality follows by some further rearrangement and a simple case analysis (whether $2\in\{p_1,\ldots,p_s\}$ or not) which yields $(\sum\ln p_i)(\prod_{i=1}^{s}\frac{p_i}{p_i-1})>1$.

The result now follows by combining the estimate for $|\sum_1|$ as in (5.12) and (5.13), the estimate for $|\sum_2|$ as in (4.12), taking sup over $J$, and finally the fact that $D_N(\sigma)\le 2^s D_N^*(\sigma)$. □

REMARK 5.2. As at the end of the proof of Theorem 2.1, we discuss the essential steps in the proof of Theorem 2.3.

The proof begins with the definition of $U(\mathbf{a})$ and a claim that will be used later to partition the sum of all $\mathbf{j} \in T(N)$. The proof of the claim is purely number theoretical with the fact that equations (5.10) and (5.11) are equivalent. Therefore, it is essential that we define $P_i(k_i; \mathbf{j})$ in a certain way.

By using the estimate of $t(\mathbf{j})$ as in the proof of (modified) Proposition 4.1, the next milestone, equation (5.12), is obtained. From there, along with another number theoretical result (Lemma 4.4), we obtain our targeted upper bound for $|\sum_1|$. To finish the proof, the estimate of $|\sum_2|$ as in the proof of Theorem 2.1 is needed. That is, we also need Lemma 3.1 to hold (See Remark 4.4).

The proof of (modified) Proposition 4.1 consists of three parts. The first part is to apply Lemma 4.3 on $I(\widetilde{\mathbf{j}})$ for $\widetilde{\mathbf{j}} \in T^*(N)$. The second part uses the fact that $p_i \nmid P_i(k_i; \mathbf{j})$ to obtain an upper bound for $|S_K(\mathbf{l}, \omega)|$ and then the equation (5.8). The last part is to apply Lemma 3.1 on $\widetilde{\mathbf{j}} \in T_z(N)$ to complete the estimate of $|\sum_1|$.

To summarize, we see that the proof of Theorem 2.3 replies on and only on Lemma 3.1 (so in fact equation (4.2)), a proper definition of $P_i(k_i; \mathbf{j})$ (so that (5.10) and (5.11) are equivalent), and also Lemma 4.3. It is not hard to see that Lemma 4.3(3) follows from part (2). Therefore, the whole Lemma 4.3 holds if the first two parts hold.

REMARK 5.3. The original paper by Atanassov gives another way of getting $\mathbf{j}^{(iv)}$ and another way of obtaining new solutions to (5.10) with RHS $= \mathbf{b}'$ from a particular solution and a general solution to the homogeneous equations. Namely,

$$j_i^{(iv)} = j_i' - j_i'' - \left( \left\lfloor \frac{j_i' - j_i''}{(p_1 - 1) \cdots (p_s - 1)} \right\rfloor \right) (p_1 - 1) \cdots (p_s - 1) \quad (5.14)$$

$$j_i'' = j_i + j_i' - \left( \left\lfloor \frac{j_i + j_i'}{(p_1 - 1) \cdots (p_s - 1)} \right\rfloor - a_i \right) (p_1 - 1) \cdots (p_s - 1) \quad (5.15)$$

In fact, these two equations are in the same vein as the construction given in our proof, since in (5.14), $\left\lfloor \frac{j_i' - j_i''}{(p_1-1)\cdots(p_s-1)} \right\rfloor = -1$ or $0$, whereas in (5.15), $\left\lfloor \frac{j_i + j_i'}{(p_1-1)\cdots(p_s-1)} \right\rfloor - a_i = 0$ or $1$.

## 6. Proposition 4.1 Revisited

As we discussed before, the inaccuracy in the proof of Proposition 4.1 from [1] is quite subtle. There are three ways to fix this and still be able to prove Theorem 2.3. The first one has been presented in the previous section, where we have separated $T(N)$ into $T^*(N)$ and $T_z(N)$. Then we used Lemma 4.3 on vectors in $T^*(N)-\mathbf{1}$, while the approach in Theorem 2.1 to estimate $\sum_2$ was used on elements of $T_z(N)$.

The second one is to prove our modified[2] Proposition 4.1, stated again below for convenience, and then show that Theorem 2.3 will also hold. This is what we do next. A third approach is discussed at the end of the section, which is a simplified version of our first approach, but where we replace the second term of the bound in the original Proposition 4.1 by a $O((\ln N)^{s-1})$ term. The proof of Theorem 2.3 given in the previous section then carries through.

**(Modified[2]) Proposition 4.1.** The star-discrepancy of the modified Halton sequence $\sigma=\sigma(p_1,\ldots,p_s,k_1,\ldots,k_s)$ satisfies:

$$ND_N^*(\sigma) \le \sum_{\mathbf{j}\in T(N)} 2^{\mathbb{z}(\mathbf{j})}\left(1+\sum_{\mathbf{l}\in M(\mathbf{p})}\frac{\|\sum_{i=1}^{s}\frac{l_i}{p_i}P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) + \sum_{k=0}^{s-1}\frac{p_{k+1}}{k!}\prod_{i=1}^{k}\left(\left\lfloor\frac{p_i}{2}\right\rfloor\frac{\ln N}{\ln p_i}+k\right),$$

where $\mathbb{z}(\mathbf{j})=\#\{i=1,\ldots,s : j_i=0\}$.

*Proof.*
We will repeat or rephrase part of the proof of modified Proposition 4.1, in particular from the beginning of Case 1 to the beginning of Remark 5.1, for convenience.

Same setup as before to get the signed splittings with intervals

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

where $z_k^{(i)}=\sum_{j=0}^{k-1}a_j^{(i)}p_i^{-j}$. Notice that $z_1^{(i)}=\sum_{j=0}^{0}a_j^{(i)}p_i^{-j}=a_0^{(i)}$ which is either 0 or 1. Therefore, if $j_i=0$, then the $i^{\text{th}}$ coordinate-projection of $I(\mathbf{j})$ is either empty or $[0,1)$.

Fix some $\widetilde{\mathbf{j}}=(\widetilde{j}_1,\ldots,\widetilde{j}_s)\in T(N)$, define $\mathbf{j}=\lambda(\widetilde{\mathbf{j}}):=\max\{\widetilde{\mathbf{j}}-\mathbf{1},\mathbf{0}\}$. Obviously, if $\widetilde{j}_i=0$, then $j_i=0$. Therefore, we have

$$|z^{(i)}_{\widetilde{j}_i} - z^{(i)}_{\widetilde{j}_i+1}| = \begin{cases} |a^{(i)}_{\widetilde{j}_i}|p_i^{-\widetilde{j}_i} \le p_i^{-\widetilde{j}_i+1} = p_i^{-j_i} & \text{if } j_i \ge 1 \\ |z^{(i)}_0 - z^{(i)}_1| \le 1 = p_i^{-j_i} & \text{if } j_i = 0 \end{cases}. \tag{6.1}$$

Therefore, the interval $I(\widetilde{\mathbf{j}})$ is contained inside some elementary interval

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

Now we can apply Lemma 4.3 as in the proof of modified Proposition 4.1 to get (5.7). Using the same inequality regarding $|S_K(\mathbf{l}, \omega)|$, we get

$$|\textstyle\sum_1| \le \displaystyle\sum_{\widetilde{\mathbf{j}} \in T(N)} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})}\right). \tag{6.2}$$

Notice now that the sum in RHS(6.2) is indexed by $\widetilde{\mathbf{j}}$ whereas the summands are in terms of $\mathbf{j} = \lambda(\widetilde{\mathbf{j}})$. Moreover, the function $\lambda$ is not one-to-one. Namely, different $\widetilde{\mathbf{j}}$ may lead to the same $\mathbf{j} = \max\{\widetilde{\mathbf{j}} - \mathbf{1}, \mathbf{0}\}$. In other words, if we use $\mathbf{j}$ as the index of the sum in RHS(6.2), then some $\mathbf{j}$'s are summed multiple times.

If a particular $\mathbf{j}$ has $\mathbb{z}(\mathbf{j})$ zero entries, then those entries could be coming from either 1 or 0 in the corresponding entry of $\widetilde{\mathbf{j}}$. The nonzero entries uniquely determine the corresponding entries of $\widetilde{\mathbf{j}}$ by adding 1. Therefore, $\#\{\widetilde{\mathbf{j}} : \lambda(\widetilde{\mathbf{j}}) = \mathbf{j}\} = 2^{\mathbb{z}(\mathbf{j})}$. Also, since $\lambda(T(N)) \subset T(N)$, taking inverse gives

$$T(N) \subset \bigcup_{\mathbf{j} \in T(N)} \lambda^{-1}(\mathbf{j}).$$

Hence, we have

$$\begin{aligned} |\textstyle\sum_1| &\le \displaystyle\sum_{\widetilde{\mathbf{j}} \in T(N)} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})}\right) \\ &\le \sum_{\mathbf{j} \in T(N)} \sum_{\widetilde{\mathbf{j}} \in \lambda^{-1}(\mathbf{j})} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \lambda(\widetilde{\mathbf{j}})) \|^{-1}}{2R(\mathbf{l})}\right) \\ &= \sum_{\mathbf{j} \in T(N)} 2^{\mathbb{z}(\mathbf{j})} \left(1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \|^{-1}}{2R(\mathbf{l})}\right). \end{aligned} \tag{6.3}$$

The result now follows by combining (6.3) with the estimates (4.12) of $\sum_2$ in the proof of Theorem 2.1. □

Even though this new upper bound seems a lot larger than the one in modified Proposition 4.1, we can still prove Theorem 2.3. In fact, we shall use an even weaker result, namely,

$$
\begin{aligned}
ND_N^*(\sigma) \leq \sum_{\mathbf{j}\in T(N)} \left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) + O(\ln^{s-1} N) \\
+ \sum_{\mathbf{j}\in T_z(N)} 2^s \left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right).
\end{aligned} \tag{6.4}
$$

It is not hard to see that (6.4) comes right out of modified[2] Proposition 4.1. The fact that the estimate (4.12) for $\sum_2$ is $O(\ln^{s-1} N)$ was proven and used many times already. From the definition, we know that $2^{\mathbb{z}(\mathbf{j})} = 1$ for $\mathbf{j} \in T^*(N)$ and $\mathbb{z}(\mathbf{j}) \leq s$ for all $\mathbf{j}$. Finally, since we are looking for an upper bound, it does not hurt to sum over $T(N)$ in the first sum in RHS(6.4) where it suffices to sum over $T^*(N)$.

The following lemma provides the key why the extra term in (6.4) does not create much trouble as far as proving Theorem 2.3 is concerned. Namely, we did not add too much.

**Lemma 5.1.** $\text{card}(T_z(N)) \in O(\ln^{s-1} N)$, where card(.) denotes the cardinality of a set.

*Proof.*

We will first introduce some set-theoretic notations, not because the proof is complicated, but to make it easier for us to explain.

Let $\mathcal{P}^*$ be the set of all proper subsets of $\{1, 2, \ldots, s\}$. For any set $S = \{a_1, \ldots, a_m\} \in \mathcal{P}^*$, define

$$T_S(N) = \text{card}\{(j_1, \ldots, j_m) : p_{a_1}^{j_1} \cdots p_{a_m}^{j_m} \leq N, j_1, \ldots, j_m \in \mathbf{Z}^+\},$$

and $d_S(N) = \text{card}(T_S(N)) = d(p_{a_1}, \ldots, p_{a_m}; N)$ which was defined in Definition 3.1.

Take any $\mathbf{j} \in T_z(N)$, it will have none-zero entries with indices in a proper subset of $\{1, \ldots, s\}$, say $S$ for some set $S \in \mathcal{P}^*$, and hence $\mathbf{j} \in T_S(N)$. Obviously, $T_S(N) \subset T(N)$ and $T_{S_1}(N) \cap T_{S_2}(N) = \varnothing$ if $S_1 \neq S_2$. Therefore,

$$T_z(N) = \dot{\bigcup}_{S\in\mathcal{P}^*} T_S(N)$$

Taking card gives, for N large, in fact bigger than 2:

$$
\begin{aligned}
\mathrm{card}(T_z(N)) = \sum_{S\in\mathcal{P}^*} d_S(N) &= \sum_{k=1}^{s-1} \sum_{S=\{a_1,\ldots,a_k\}\in\mathcal{P}^*} d(p_{a_1},\ldots,p_{a_m};N) \\
&\le \sum_{k=1}^{s-1} \sum_{S=\{a_1,\ldots,a_k\}\in\mathcal{P}^*} \frac{1}{k!}\prod_{i=1}^{k}\frac{\ln N}{\ln p_{a_i}} \quad \text{by Lemma 3.2} \\
&\le \frac{1}{\ln 2}\sum_{k=1}^{s-1} \sum_{S=\{a_1,\ldots,a_k\}\in\mathcal{P}^*} \frac{1}{k!}\ln^k N \\
&\le \frac{\ln^{s-1} N}{\ln 2}\sum_{k=1}^{s-1} \sum_{S=\{a_1,\ldots,a_k\}\in\mathcal{P}^*} 1 \\
&= \frac{\ln^{s-1} N}{\ln 2}\cdot \mathrm{card}(\mathcal{P}^*) = \ln^{s-1} N\frac{2^s-1}{\ln 2} \\
&\in O(\ln^{s-1} N),
\end{aligned} \tag{6.5}
$$

where the upper limit of $k$ is $s-1$ since $\mathcal{P}^*$ does not contain the full $\{1,\ldots,s\}$; the third line follows because all but possibly one $p_{a_i} \ge 3$ and $\ln 3 > 1$; the fourth line follows as $\ln^k N \le \ln^{s-1} N$ and $1/k! \le 1$. □

Next, we prove a nearly trivial and seemingly useless corollary of Lemma 4.4.

**Lemma 5.2.** For arbitrary $\mathbf{j}$ (distinctive primes $p_1,\ldots,p_s$ and their admissible integers $p_1,\ldots,p_k$ as always),

$$
\sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\|\sum_{i=1}^{s}(l_i/p_i)P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})} \le \sum_{i=1}^{s}\ln p_i \prod_{i=1}^{s} p_i \left(-1+\prod_{j=1}^{s}(1+\ln p_j)\right) =: \xi \tag{6.6}
$$

*Proof.*
For each $i$, $P_i(k_i;\mathbf{j}) \in \{1,2,\ldots,p_i-1\}$. Thus,

$$
\begin{aligned}
\sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\|\sum_{i=1}^{s}(l_i/p_i)P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})} &\le \sum_{\mathbf{l}\in M(\mathbf{p})}\sum_{m_1=1}^{p_1-1}\cdots\sum_{m_s=1}^{p_s-1} \frac{\left\|\frac{l_1m_1}{p_1}+\ldots+\frac{l_sm_s}{p_s}\right\|^{-1}}{2R(\mathbf{l})} \\
&\le \sum_{i=1}^{s}\ln p_i \prod_{i=1}^{s} p_i \left(-1+\prod_{j=1}^{s}(1+\ln p_j)\right),
\end{aligned}
$$

as required. □

Now we are in shape to finish the proof of Theorem 2.3 using modified[2] Proposition 4.1. Remember that we are showing that the extra term in the new Proposition 4.1 is small enough. Therefore, we will use the same setup/approach involving $U(\mathbf{a})$.

Going directly to (5.12), we have, up to $O(\ln^{s-1} N)$,

$$\begin{aligned}
\left|\sum\nolimits_1\right| &\leq \sum_{\mathbf{j}\in T(N)} \left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) \\
&\quad + \sum_{\mathbf{j}\in T_z(N)} 2^s \left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) \\
&\leq \sum_{\mathbf{a}|\prod_{i=1}^{s} p_i^{K\cdot a_i}\leq N} \sum_{\mathbf{j}\in U(\mathbf{a})} \left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) \\
&\quad + \sum_{\mathbf{j}\in T_z(N)} 2^s(1+\xi) \\
&< \frac{1}{s!}\left(\sum_{i=1}^{s} \ln p_i \prod_{i=1}^{s} \frac{p_i(1+\ln p_i)}{(p_i-1)\ln p_i}\right) \ln^s N \\
&\quad + O(\ln^{s-1} N)\cdot 2^s(1+\xi) \qquad (6.7) \\
&= \frac{1}{s!}\left(\sum_{i=1}^{s} \ln p_i \prod_{i=1}^{s} \frac{p_i(1+\ln p_i)}{(p_i-1)\ln p_i}\right) \ln^s N, \qquad (6.8)
\end{aligned}$$

where we refer to (5.13) to get the estimate in the fourth line. As in the proof of Theorem 2.3 in the previous section, equation (6.7) is essentially Theorem 2.3. □

As a summary, we used a more straightforward approach to Proposition 4.1 to get a seemingly bad upper bound, which in turns requires some extra lemmas, though not difficult, so that Theorem 2.3 still carries through.

As mentioned at the beginning of this section, yet another way to address the inaccuracy found in the proof of Proposition 4.1 given in [1] is to use asymptotic notation to replace the second term of the bound given in that result. More precisely, we have:

**(Simplified) Proposition 4.1.** The star-discrepancy of the modified Halton sequence $\sigma = \sigma(p_1, \ldots, p_s, k_1, \ldots, k_s)$ satisfies:

$$ND_N^*(\sigma) \leq \sum_{\mathbf{j}\in T(N)} \left(1 + \sum_{\mathbf{l}\in M(\mathbf{p})} \frac{\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i;\mathbf{j})\|^{-1}}{2R(\mathbf{l})}\right) + O((\ln N)^{s-1}).$$

*Proof.*
The proof is almost the same as in [1], except that on p.28, line 12, after "Fix some $\mathbf{j} \in T(N)$.", we have to say "Without loss of generality we can assume that all $j_i \geq 1$ because if some $j_i = 0$ then $A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j})) \in O((\ln N)^{s-1})$. This is because if at least one $j_i = 0$, then it means that at least one projection of $I(\mathbf{j})$ is equal to $[0, 1)$ or the empty set, and consequently when we compute $A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j}))$, we only need to consider a (strict) subset of the coordinates of the first $N$ points of the sequence. Hence we deal with modified Halton sequences in dimension no larger than $s - 1$, and can thus apply Theorem 2.1 to show that $A_N(I(\mathbf{j})) - N\mu(I(\mathbf{j})) \in O((\ln N)^{s-1})$, since this theorem also applies to modified Halton sequences (see end of Remark 4)". Note that a similar argument is used in [16, Thm 4.49, p. 90]. □

The proof of Theorem 2.3 follows in the same way as in Section 5 after the proof of (modified) Proposition 4.1.

## Acknowledgements

We wish to thank Shu Tezuka for pointing out a small inaccuracy in our original proof of Lemma 4.4, which has been corrected in a preceding version. We also thank Harald Niederreiter and Shu Tezuka for pointing out another small inacurracy in [8], which was present too in the proof of Theorem 2.1, Claim 3 and has been corrected in this newer version.

## References

[1] E. Atanassov. On the discrepancy of the Halton sequences. *Mathematica Balkanica*, 18 : 15–32, 2004.

[2] J. Beck and W.W.L. Chen. *Irregularities of Distribution*. Cambridge University Press, UK,1987.

[3] J. Dick and F. Pillichshammer. *Digital Nets and Sequences : Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, UK, 2010.

[4] M. Drmota, R.F. Tichy. *Sequences, Discrepancies and Applications.* Lecture Notes in Mathematics 1651. Springer, Berlin, 1997.

[5] H. Faure. Discrépance des suites associées à un système de numération (en dimension $s$). *Acta Arith*, 41 : 337–351, 1982.

[6] H. Faure. On Atanassov methods for discrepancy bounds of low-discrepancy sequences. In *Uniform Distribution and Quasi-Monte Carlo Methods: Discrepancy, Integration and Applications*, P. Kritzer, H. Niederreiter, F. Pillichshammer, A. Winterhof (Eds.), to appear.

[7] H. Faure and C. Lemieux. Generalized Halton sequence in 2009 : a comparative study. *ACM Transactions on Modeling and Computer Simulation*, 19(Article 15), 2009.

[8] H. Faure and C. Lemieux. Improvements on the star discrepancy of $(t,s)$-sequences. *Acta Arith*, 154(1) : 61–78, 2012.

[9] H. Faure and C. Lemieux. Corrigendum to : Improvements on the star discrepancy of $(t,s)$-sequences, *Acta Arith.* **154.1** (2012), 61–78. *Acta Arith*, 159(3) : 299–300, 2013.

[10] H. Faure and C. Lemieux. A variant of Atanassov's methods for $(t,s)$-sequences and $(t,\mathbf{e},s)$-sequences. Submitted to *J. Complexity*.

[11] H. Faure, C. Lemieux, and X. Wang. Extensions of Atanassov's methods for Halton sequences. In *Monte Carlo and Quasi-Monte Carlo Methods 2010*, L. Plastoka and H. Wozniakowski, (Eds.), 345–362, 2012.

[12] J. H. Halton. On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals. *Numerische Mathematik*, 2 : 84–90, 1960.

[13] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*. John Wiley, New York, 1974.

[14] J. Matoušek. *Geometric Discrepancy*. Springer, 1999.

[15] H. Niederreiter. *Pseudozufallszahlen und die Theorie der Gleichverteilung, Sitzungsber.* Österr. Akad. Wiss. Math.-Naturw. Kl. (II) 195, 109–138, 1986.

[16] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*, volume 63 of *SIAM CBMS-NSF Regional Conference Series in Applied Mathematics*. SIAM, Philadelphia, 1992.

[17] S. Tezuka. *Uniform Random Numbers : Theory and Practice*. Kluwer Academic Publishers, Norwell, Mass., 1995.

[18] S. Tezuka. On the discrepancy of generalized Niederreiter sequences. *J. Complexity*, 29 : 240–247, 2013.