Mathematica Balkanica

New Series Vol. 18, 2004, Fasc. 1-2

On the Discrepancy of the Halton Sequences

Emanouil I. Atanassov

Presented by Bl. Sendov

In this paper some estimates of the discrepancy of the Halton sequences are presented. It is known that for given pairwise relatively prime integers $p_1, \ldots, p_s$ the discrepancy of the Halton sequence $\sigma(p_1, \ldots, p_s)$ satisfies $ND_N(\sigma) < c_s(p_1, \ldots, p_s) \ln^s N + O(\ln^{s-1} N)$. We prove that this estimate holds with $c_s = \frac{1}{s!} \prod_{i=1}^{s} \frac{p_i - 1}{\ln p_i}$, improving well known results of Halton, Meijer, Faure and Niederreiter. It is shown that if the integers $p_1, \ldots, p_s$ are the first s primes then $\lim_{s\to\infty} c_s = 0$. It is also proven that if the prime numbers $p_1, \ldots, p_s$ satisfy certain condition the same inequality holds with

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

For every distinct primes $p_1, \ldots, p_s$, a modified Halton sequence $\sigma(p_1, \ldots, p_s)$ is constructed, so that the same estimate for its discrepancy holds unconditionally.

AMS Sibject Classification: 11K38, 11K31, 11J71

Key words: bution modulo one, low-discrepancy sequences, irregularities of distribution.

1. Introduction

Perhaps the most important measures of the irregularity of distribution of a sequence are its discrepancy and star-discrepancy.

Definition 1.1. For every s -dimensional interval $J = \prod_{i=1}^{s} [c_i, d_i) \subseteq \mathbb{E}^s$, where $\mathbb{E}^s$ is the unit cube $[0,1)^s$, let $A_N(J)$ be the number of terms of the sequence $\sigma = \{x_j\}$ 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 σ is equal to

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

The star-discrepancy of the sequence $D_N^{\star}(\sigma)$ is obtained when the supremum is taken only over intervals $J \subseteq \mathbb{E}^s$ of the kind $J = \prod_{i=1}^{s} [0, d_i')$.

Van der Corput in [9] introduced a one-dimensional infinite sequence with very small discrepancy. A generalization of the Van der Corput sequence to s dimensions was proposed by Halton in [6]. H. Faure in [4] proposed a further generalization of the one-dimensional Van der Corput - Halton sequence in order to construct infinite sequences with small discrepancy.

Definition 1.2. Let $p \geq 2$ be a fixed integer, and let $\tau = \{\tau_j\}_{j=0}^{\infty}$ be a sequence of substitutions of the numbers $\{0, \ldots, p-1\}$. The terms of the corresponding generalized Van der Corput sequence are obtained by representing n as $n = \sum_{j=0}^{k} a_j p^j, \quad a_j \in \{0, \ldots, p-1\}$, and putting $x_n = \sum_{j=0}^{k} \tau_j(a_j) p^{-j-1}$. The one-dimensional Van der Corput - Halton sequence in base p is obtained by setting $\tau_j(i) = i$.

Definition 1.3. Let $p_1, \ldots, p_s$ be pairwise relatively prime integers, $p_i \geq 2$. The Halton sequence $\sigma(p_1, \ldots, p_s) = \left\{\left(x_n^{(1)}, \ldots, x_n^{(s)}\right)\right\}_{n=0}^{\infty}$ is constructed by setting each sequence $\left\{x_n^{(i)}\right\}_{n=0}^{\infty}$ to be a Van der Corput - Halton sequence in base p_i.

The following estimate of Halton [6] (see also Sobol [15], p. 176) had the smallest constant before the leading term (for infinite sequence) for many years.

Theorem 1.1. *Let $p_1, \ldots, p_s$ be pairwise relatively prime numbers. The discrepancy of the Halton sequence $\sigma(p_1, \ldots, p_s) = \{x_n\}_{n=0}^{\infty}$ satisfies*

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

with

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

Meijer in [8] showed that the term $\mathrm{O}(\ln^{s-1} N)$ in the previous estimate might be replaced with $\mathrm{O}(1)$. The estimate (1) was improved by H. Faure ([3], [5]) and a different proof can be seen from Niederreiter ([11]). The best known bound of the type (1) for the Halton sequence in more than 1 dimension has the constant

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

It is believed, that the order $N^{-1} \ln^s N$ is the best possible for an infinite sequence, and W.M. Schmidt ([14]) proved this in the case $s = 1$. For $s > 1$ the question remains open. K.F. Roth in [13] proved a lower bound of $\Omega(N^{-1}\ln^{\frac{s}{2}} N)$, and this result was slightly improved by R.C. Baker in [1]. The question how small the constant c_s in an estimate

$$ND_N(\sigma) < c_s \ln^s N + \mathrm{O}(\ln^{s-1} N) \tag{2}$$

can be, is interesting from theoretical and practical viewpoint. See for example the book of Niederreiter ([11], p. 95). Nowadays there are many families of sequences , for which estimates of the type (2) were proven. For some of them the constant c_s has been shown to tend to zero super-exponentially, when s tends to infinity. For the Halton sequences however, the results presented above do not show such behavior. On the contrary, the constant c_s tends to infinity super-exponentially, when s tends to infinity.

2. Results

In this paper the following estimate of the discrepancy of the Halton sequences is established:

Theorem 2.1. *Let $p_1, \ldots, p_s$ be pairwise relatively prime integers, $p_i \geq 2$. The discrepancy of the Halton sequence $\sigma(p_1, \ldots, p_s)$ satisfies*

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

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

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

if p_r is the even number among them. Therefore the estimate (2) holds with constant

$$c_s = \frac{1}{s!}\prod_{i=1}^{s}\frac{p_i - 1}{\ln p_i}. \tag{3}$$

The improvement in the constant c_s is with a factor of $s!$. We also prove:

Corollary 2.1. *When $p_1, \ldots, p_s$ are the first s primes,*

$$\lim_{s\to\infty} c_s(p_1, \ldots, p_s) = 0.$$

The next estimate is valid only when the numbers $p_1, \dots, p_s$ are distinct primes and satisfy certain condition, which is defined below.

Definition 2.1. Let $p_1, \dots, p_s$ be distinct primes. The integers $k_1, \dots, k_s$ are called "admissible" for them, if $p_i \nmid k_i$ and for each set of integers $b_1, \dots, b_s, p_i \nmid b_i$, there exists a set of integers $\alpha_1, \dots, \alpha_s$, satisfying the congruences

$$k_i^{\alpha_i} \prod_{1 \le j \le s, j \ne i} p_j^{\alpha_j} \equiv b_i \,(\operatorname{mod} p_i)\,, \quad i = 1, \dots, s. \tag{4}$$

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

In Section 4 we prove the existence of such "admissible" integers for each set of distinct primes. An algorithm for checking if given integers $k_1, \dots, k_s$ are "admissible" was developed and tested. It was discovered that if $p_1, \dots, p_s$ are the first s primes, Condition $\mathcal{R}$ is satisfied for all $s \le 10$ and for 58 values of s between 11 and 100.

Now we formulate an estimate of the discrepancy of the Halton sequences with better constant before the leading term, which is true when the numbers p_i are prime and satisfy the condition $\mathcal{R}$.

Theorem 2.2. *If the prime numbers $p_1, \dots, p_s$ fulfill Condition $\mathcal{R}$, then the discrepancy of the Halton sequence $\sigma(p_1, \dots, p_s)$ satisfies (2) with constant*

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

Definition 2.2. Let $p_1, \dots, p_s$ be distinct primes, and let $k_1, \dots, k_s$ be "admissible" for them. The modified Halton sequence $\sigma\left(p_1, \dots, p_s; k_1, \dots, k_s\right) = \left\{\left(x_n^{(1)}, \dots, x_n^{(s)}\right)\right\}_{n=0}^{\infty}$ is constructed by setting each sequence $\left\{x_n^{(i)}\right\}_{n=0}^{\infty}$ to be a generalized Van der Corput-Halton sequence in base p_i (see Definition 1.2.), with the sequence of substitutions $\tau^{(i)}$ defined by taking $\tau_j^{(i)}(t)$ to be the remainder of tk_i^j modulo p_i, $\tau_j^{(i)}(t) \in \{0, \dots, p_i - 1\}$.

In this paper the following estimate of the discrepancy of the modified Halton sequences is proven:

Theorem 2.3. *Let $p_1, \dots, p_s$ be distinct primes and the integers $k_1, \dots, k_s$ are "admissible" for them. The modified Halton sequence $\sigma(p_1, \dots, p_s; k_1, \dots, k_s)$ satisfies (2) with the same constant as in Theorem 2.2., i.e. with*

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

When the Condition $\mathcal{R}$ is fulfilled, the Halton sequence $\sigma(p_1, \dots, p_s)$ can be considered as a modified Halton sequence $\sigma(p_1, \dots, p_s; 1, \dots, 1)$, and therefore Theorem 2.2. follows from Theorem 2.3..

3. Proof of Theorem 2.1.

For brevity we are going to use notations as $\mathbf{j}$ for $j_1, \dots, j_s$, $\mathbf{b}$ for $b_1, \dots, b_s$ etc. The next Lemma is used extensively in the proofs:

Lemma 3.1. *Let $\sigma\,(p_1, \dots, p_s) = \{x_n\}_{n=0}^{\infty}$ be a Halton or modified Halton sequence and let J be an interval of the form $J = \prod_{i=1}^{s} [b_i p_i^{-\alpha_i}, c_i p_i^{-\alpha_i})$. Then*

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

for every 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. Let $n = \sum_{j=0}^{n_i} n_{ij} p_i^j$, be the expansions of n in the number systems with base p_i. Select some $\mathbf{l} = (l_1, \dots, l_s)$ such that $b_i \leq l_i < c_i$, and let $l_i = \sum_{j=0}^{\infty} l_{ij} p_i^j$, be the respective expansion. From Definition 1.2. it follows that the condition $x_n^{(i)} \in \left[l_i p_i^{-\alpha_i}, (l_i + 1)\, p_i^{-\alpha_i}\right)$ is equivalent to $\tau_j^{(i)}(n_{ij}) = l_{ij}$ for all $j = 0, \dots, \alpha_i - 1, i = 1, \dots, s$. Since $\tau_j^{(i)}$ are bijections and p_i are pairwise relatively prime, from the Chinese remainder theorem we obtain that in every $p_1^{\alpha_1} \dots p_s^{\alpha_s}$ consecutive integers exactly 1 has these properties. Therefore $A_{tp_1^{\alpha_1} \dots p_s^{\alpha_s}}(J) = t(c_1 - b_1) \dots (c_s - b_s)$, which completes the proof. ■

Definition 3.1. Let $p_1, \dots, p_k$ be a possibly empty set of integers, $p_i \geq 2$ and let N be any positive number. By $d(p_1, \dots, p_k; N)$ we denote the number of positive integers $(j_1, \dots, j_k)$, such that $p_1^{j_1} \dots p_s^{j_k} \leq N$. If $k = 0$, then $d(N) = 1$.

In the next Lemma a simple estimate of the function d is established. Functions of this kind are extensively studied, and if one is interested, he or she might look at [2] for more information on the subject.

Lemma 3.2. *The number $d(p_1,\dots,p_s;N)$ satisfies the inequality*

$$d(p_1,\dots,p_k;N) \le \frac{1}{k!}\prod_{i=1}^{k}\frac{\ln N}{\ln p_i}. \tag{5}$$

P r o o f. If the positive integers $j_1,\dots,j_k$ satisfy $\prod_{i=1}^{k} p_i^{j_i} \le N$, then the cube $\prod_{i=1}^{k}[j_i-1,j_i)$ is entirely contained in the simplex

$$\{x_1\ln p_1+\cdots+x_k\ln p_k \le \ln N,\, x_i\ge 0\}\,.$$

Such cubes do not intersect and therefore their number is not more than the volume of the simplex, which is exactly the right-hand-side of (5). ■

Lemma 3.3. *Let N and $p_1,\dots,p_k$ be integers, $p_i \ge 2$. Let some numbers $c_j^{(i)} \ge 0$ be given, such that $c_0^{(i)} \le 1$ and $c_j^{(i)} \le f_i(p_i)$ for $j\ge 1$. Then*

$$\sum_{(j_1,\dots,j_k)\,|\,p_1^{j_1}\dots p_k^{j_k}\le N}\ \prod_{i=1}^{k} c_{j_i}^{(i)} \le \frac{1}{k!}\prod_{i=1}^{k}\left(f_i(p_i)\frac{\ln N}{\ln p_i}+k\right). \tag{6}$$

P r o o f. Fix some possibly empty subset $L=\{i_1,\dots,i_m\}$ of $\{1,\dots,k\}$. Consider the contributions of all the m-tupples $\mathbf{j}$, such that $j_r>0$ for $r\in L$, $j_r=0$ for $r\notin L$, and $\prod_{i\in L} p_i^{j_i} \le N$. The number of such m-tupples is $d(p_{i_1},\dots,p_{i_m},N) \le \frac{1}{m!}\prod_{i\in L}\frac{\ln N}{\ln p_i}$ and each one contributes at most $\prod_{i\in L} f_i(p_i)$. Now the estimate (6) is obtained by expanding its right-hand-side and using $\frac{k^{k-m}}{k!} \ge \frac{1}{m!}$. ■

Definition 3.2. Consider an interval $J \subseteq \mathbb{E}^s$. We call "signed splitting" of the interval J any collection of intervals $J_1,\dots,J_n$ and respective signs $\varepsilon_1,\dots,\varepsilon_n$ equal to ± 1, such that for any additive function ν on the intervals in $\mathbb{E}^s$

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

E x a m p l e 3.1. *For the interval* $[0,0.5)\times[0,0.5)$ *a "signed splitting" can be given by the intervals:* $J_1=[0,1)\times[0,1)$, $J_2=[0,1)\times[0.5,1)$, $J_3=[0.5,1)\times[0,1)$, $J_4=[0.5,1)\times[0.5,1)$, *and the signs:* $\varepsilon_1=1,\varepsilon_2=-1,\varepsilon_3=-1,\varepsilon_4=1$.

Our ability to construct such "signed splittings" is based upon the following trivial Lemma.

Lemma 3.4. *Let the interval* $J = \prod_{i=1}^{s}[a_i, b_i) \subseteq \mathbb{E}^s$ *be given. Fix a dimension* k *and a number* $c \in [0, 1)$*. The intervals* $I_1 = [\min(a_k, c), \max(a_k, c))$ *and* $I_2 = [\min(c, b_k), \max(c, b_k))$ *and the signs* $\varepsilon_1 = \mathrm{sgn}(c - a_k), \varepsilon_2 = \mathrm{sgn}(b_k - c)$*, define a "signed splitting" of the interval* $[a_k, b_k)$*. Multiplying correspondingly, we obtain the collection of intervals*

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

which together with the same signs $\varepsilon_1, \varepsilon_2$*, provide a "signed splitting" of the interval* J*.*

Lemma 3.5. *Let* $J = \prod_{i=1}^{s}[0, z^{(i)}) \subseteq \mathbb{E}^s$ *be an* s*-dimensional interval, and let for each* j *some numbers* $(z_j^{(i)})_{j=1}^{n_i} \subseteq [0, 1]$ *be given. 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 collections of intervals*

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

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

Proof. The splitting is constructed by applying Lemma 3.4. iteratively. ∎

Proof of Theorem 2.1. Let $N \ge 1$ be a sufficiently large integer and $\mathbf{z} = (z^{(1)}, \ldots, z^{(s)})$ be a point of $E^s = [0, 1)^s$. When p_i is odd, $z^{(i)}$ can be expanded as $z^{(i)} = \sum_{j=0}^{\infty} a_j^{(i)} p_i^{-j}$, with $\left|a_j^{(i)}\right| \le \frac{p_i - 1}{2}$. The expansion is obtained by induction, choosing the digit $a_k^{(i)}$ to be the smallest in absolute value integer, such that the distance $|z^{(i)} - \sum_{j=0}^{k} a_j^{(i)} p_i^{-j}|$ is less than $\frac{p^{-k}}{2}$. At most one of the integers p_r can be even. For such an index r an expansion of $z^{(r)}$ of the same type is possible, with the integers $a_j^{(r)}$ satisfying instead the inequalities $\left|a_j^{(r)}\right| \le \frac{p_r}{2}$

and $\left|a_j^{(r)}\right| + \left|a_{j+1}^{(r)}\right| \le p_r - 1$. Such an expansion is obtained again by induction, choosing the digit $a_k^{(r)}$ to be the smallest in absolute value integer, so that the distance $|z^{(r)} - \sum_{j=0}^{k} a_j^{(i)} p_i^{-j}|$ is less than

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

For all i denote $n_i = \left[\frac{\ln N}{\ln p_i}\right]$, and consider the numbers $z_k^{(i)} = \sum_{j=0}^{k-1} a_j^{(i)} p_i^{-j}$ for $k = 1, \dots, n_i$. Let $z_0^{(i)} = 0$ and $z_{n_i+1}^{(i)} = z^{(i)}$. Following Lemma 3.5. we expand the interval $\prod_{i=1}^{s}[0, z^{(i)})$, using the numbers $(z_j^{(i)})_{j=1}^{n_i}$. We obtain the collection of intervals

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

and signs $\varepsilon(\mathbf{j}) = \prod_{i=1}^{s} \operatorname{sgn}(z_{j_i+1}^{(i)} - z_{j_i}^{(i)})$. Since μ and A_N are additive, $A_N(J) - N\,\mu(J)$ may be expanded as

$$\sum_{j_1=0}^{n_1} \dots \sum_{j_s=0}^{n_s} \varepsilon(\mathbf{j})\ (A_N(I(\mathbf{j})) - N\,\mu(I(\mathbf{j}))) = \sum\nolimits_1 + \sum\nolimits_2 . \tag{7}$$

We rearrange the terms, so that in Σ_1 we put the terms with $p_1^{j_1} ... p_s^{j_s} \le N$ and in Σ_2 - the rest. We need to prove

$$\left|\sum\nolimits_1\right| \le \frac{1}{s!}\prod_{i=1}^{s}\left(\frac{(p_i-1)\ln N}{2\ln p_i} + s\right) + u, \tag{8}$$

where u was defined in the statement of the Theorem. According to Lemma 3.1.,

$$|A_N(I(\mathbf{j})) - N\,\mu(I(\mathbf{j}))| \le \prod_{i=1}^{s}\left|a_{j_i}^{(i)}\right|.$$

If all the p_i are odd, we apply Lemma 3.3. with $f_i(p_i) = \frac{p_i-1}{2}$ and obtain exactly (8), since $u = 0$ in this case. Suppose now that some p_r is even. Let the numbers $p'_1, \dots, p'_s$ be defined by $p'_i = p_i$ for $i \ne r$, $p'_r = p_r^2$. Define $c_0^{(i)} = 1$, $c_j^{(i)} = |a_j^{(i)}|$ for $i \ne r$, $c_j^{(r)} = |a_{2j-1}^{(r)}| + |a_{2j}^{(r)}|$ for $j \ge 1$. By Lemma 3.3., applied to $\mathbf{p}'$, with

$f_i(p) = \frac{p-1}{2}$ for $i \neq r$, and $f_r(p) = \sqrt{p} - 1$, we have

$$\sum_{\mathbf{j}' \mid \prod_{i=1}^s {p'_i}^{j'_i} \leq N} \prod_{i=1}^s c_{j_i}^{(i)} \leq \frac{1}{s!} \prod_{i=1}^s \left(\frac{(p_i - 1) \ln N}{2 \ln p_i} + s \right).$$

Thus we obtain an estimate for the terms of Σ_1, which come from $\mathbf{j}$ such that $j_r = 0$ or $\prod_{i=1}^s {p_i}^{j_i} \leq p_r N$. The only terms which are not accounted for come from $\mathbf{j}$ satisfying $N p_r < \prod_{i=1}^s {p_i}^{j_i} \leq N$. Obviously $\prod_{1 \leq i \leq s, i \neq r} {p_i}^{j_i} \leq N$ and j_r is uniquely determined if the other j_i are fixed. Thus for estimating the contribution of these additional terms we apply again Lemma 3.3. and obtain that it is not more than

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

and the estimate (8) is proven.

The s-tupples $\mathbf{j} = (j_1, \ldots j_s)$, for which $p_1^{j_1} \ldots p_s^{j_s} > N$ are divided into s disjoint sets $B_0, \ldots, B_{s-1,}$ where

$$B_k = \{\mathbf{j} : p_1^{j_1} \ldots p_k^{j_k} \leq N,\, p_1^{j_1} \ldots p_k^{j_k} p_{k+1}^{j_{k+1}} \; > \; N\}.$$

By B_0 we denote the set $\{\mathbf{j} : p_1^{j_1} > N\}$. Fix $k \leq s - 1$. Fix one of the k-tupples $(j_1, \ldots, j_k)$ with $p_1^{j_1} \ldots p_k^{j_k} \leq N$ and let r be the biggest integer such that $p_{k+1}^{r-1} \prod_{i=1}^k p_i^{j_i} \leq N$. If $j_{k+1}, \ldots, j_s$ are such that $j_1, \ldots, j_k, j_{k+1}, \ldots, j_s \in B_k$, then $j_{k+1} \geq r$ and $j_{k+2}, \ldots, j_s$ may be arbitrary. Therefore

$$\sum_{\{(j_{k+1}, \ldots, j_s) | \mathbf{j} \in B_k\}} \varepsilon(\mathbf{j})(A_N(I(\mathbf{j})) - N\,\mu(I(\mathbf{j}))) = \pm\left(A_N(\kappa) - N\,\mu(\kappa)\right),$$

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

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

From $\mathbf{j} \in B_k$ it follows that the interval $[\min(z_r^{(k+1)}, z^{(k+1)}), \max(z_r^{(k+1)}, z^{(k+1)}))$ is inside some interval $[m_1 p_{k+1}^{-r}, m_2 p_{k+1}^{-r})$, so that $m_2 - m_1 \leq p_{k+1}$. Therefore κ is inside $\kappa' = \prod_{i=1}^k [\min(z_{j_i}, z_{j_i+1}), \max(z_{j_i}, z_{j_i+1})) \times [m_1 p_{k+1}^{-r}, m_2 p_{k+1}^{-r}) \times \prod_{i=k+2}^s [0, 1)$. Applying Lemma 3.1. to the interval κ', we obtain

$$A_N(\kappa) \leq A_N(\kappa') \leq p_{k+1} \prod_{i=1}^k \left| a_{j_i}^{(i)} \right|.$$

On the other hand, $N\,\mu(\kappa) \le p_{k+1}\prod_{i=1}^{k}\left|a_{j_i}^{(i)}\right|$. We have $\left|a_j^{(i)}\right| \le \left[\frac{p_i}{2}\right]$ for $i \le k$. In this way the intervals in B_i are combined into larger intervals, and applying Lemma 3.3. to estimate the contribution of these larger intervals, we obtain

$$\left|\sum\nolimits_2\right| \le \sum_{k=0}^{s-1}\frac{p_{k+1}}{k!}\prod_{i=1}^{k}\left(\left[\frac{p_i}{2}\right]\frac{\ln N}{\ln p_i}+k\right). \tag{9}$$

This estimate together with (8) yields

$$ND_N^{\star}(\sigma) \le \frac{1}{s!}\prod_{i=1}^{s}\left(\frac{(p_i-1)\ln N}{2\ln p_i}+s\right)+\sum_{k=0}^{s-1}\frac{p_{k+1}}{k!}\prod_{i=1}^{k}\left(\left[\frac{p_i}{2}\right]\frac{\ln N}{\ln p_i}+k\right)+u$$

The inequality $D_N(\sigma) \le 2^s D_N^*(\sigma)$ (see e.g. [7], Chapter 2) accomplishes the proof. ∎

Proof of Corollary 2.1. For sufficiently large x the number of primes less than or equal to x satisfies $\pi(x) > x\ln^{-1} x$. This inequality can be derived from the following estimate for $\pi(x)$ (see [16], [12] p. 56,[10] p. 382):

$$\pi(x) = \mathrm{li}(x) + \mathrm{O}\left(x\exp\left(\frac{-0.009(\ln x)^{\frac{3}{5}}}{(\ln\ln x)^{\frac{1}{5}}}\right)\right),$$

expanding $\mathrm{li}(x)$ as $x((\ln x)^{-1}+(\ln x)^{-2}+\mathrm{O}((\ln x)^{-3}))$. Substituting p_n-1 for x, for sufficiently large n we get $n-1 \ge \dfrac{p_n-1}{\ln(p_n-1)}$ and consequently $\dfrac{p_n-1}{n\ln p_n} \le \dfrac{n-1}{n}$. Therefore $c_s = \mathrm{O}(s^{-1})$. ∎

4. Proof of Theorems 2.2. and 2.3.

As we noted before, Theorem 2.2. is obtained as a corollary of Theorem 2.3.. In the following proposition we formulate an estimate of the star-discrepancy, which is the basis for our proof of Theorem 2.3.. It can also be used for computational estimation of $D_N^{\star}(\sigma)$, if performing $\mathrm{O}(\ln^s N)$ operations is not a problem.

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

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

where $T(N) = \left\{ \mathbf{j} \mid p_1^{j_1} ... p_s^{j_s} \le N \right\}$, $M(\mathbf{p}) = \{\mathbf{j} \mid 0 \le j_i \le p_i - 1,\ j_1 + \cdots + j_s > 0\}$, $R(\mathbf{j}) = \prod_{i=1}^{s} r_i(j_i)$, *with* $r_i(m) = \max(1, \min(2m, 2(p_i - m)))$.

The existance of modified Halton sequences is established in

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

P r o o f. Let g_i be some fixed primitive root modulo p_i, $i = 1, \ldots, s$. For any positive integers a and b, a prime p and a primitive root g modulo p, if $a \equiv g^m \pmod{p}$ and $b \equiv g^n \pmod{p}$ (therefore $p \nmid a$, $p \nmid b$), the congruence $a \equiv b \pmod{p}$ is equivalent to $m \equiv n \pmod{p-1}$. Therefore the congruences (4) lead to the system

$$a_{1i}x_1 + \cdots + a_{is}x_s \equiv m_i \pmod{p_i - 1}, \quad i = 1, \ldots, s, \tag{10}$$

where a_{ij} are such that $g_i^{a_{ij}} \equiv p_j \pmod{p_i}$ for $j \ne i$, $g_i^{a_{ii}} \equiv k_i \pmod{p_i}$, $g_i^{m_i} \equiv b_i \pmod{p_i}$. We introduce s integer variables $y_1, \ldots, y_s$, in order to change the congruences into a system of Diophantine equations:

$$a_{1i}x_1 + \cdots + a_{is}x_s + y_i(p_i - 1) = m_i, \quad i = 1, \ldots, s. \tag{11}$$

The determinant of the matrix $C = (c_{ij})$, where $c_{ij} = a_{ij}$ for $i \ne j$, $c_{ii} = r_i$, can be made 1 by a suitable choice of the numbers r_i , for any fixed integers $a_{ij}, i \ne j$. This claim follows by induction, expanding the determinant of the matrix C along the last column, C_{is} being the cofactors:

$$|C| = r_s C_{1s} + a_{2s}C_{2s} + \cdots + a_{ss}C_{ss},$$

By the induction hypothesis $C_{ss} = (-1)^{s+s}1 = 1$ and setting

$$r_s = 1 - (a_{1s}C_{1s} + \cdots + a_{s-1\,1}C_{s-1\,1})$$

yields $|C| = 1$. Setting k_i to be the remainders of $g_i^{r_i}$ modulo p_i makes $k_1, \ldots, k_s$ "admissible" for the prime numbers $p_1, \ldots, p_s$. ∎

Lemma 4.2. *Let* $\mathbf{p} = p_1, \ldots, p_s$ *be distinct prime numbers and* $\omega = (w_n)_{n=0}^{K-1}$ *be a sequence in* $\mathbb{Z}^s$. *Let* $\mathbf{b}$ *and* $\mathbf{c}$ *be fixed integer* s*-tupples, such that* $0 \le b_i < c_i \le p_i$. *Denote by* $a_K(\mathbf{b}, \mathbf{c})$ *the number of terms of* ω *among the first* K, *such that for all* $i = 1, \ldots, s$ *the remainder of* $w_n^{(i)}$ *modulo* p_i *is among the numbers* $b_i, \ldots, c_i - 1$. *Then*

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

where

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

with the usual notation $e(x)=\exp(2\pi \mathrm{i}x)$.

Proof. Since the sum $\frac{1}{p_i}\sum_{j=0}^{p_i-1} e\left(j\frac{m}{p_i}\right)$ is equal to 1 if p divides the integer m, and zero otherwise, we obtain

$$a_K(\mathbf{b},\mathbf{c})=\sum_{n=0}^{K-1}\sum_{l_1=b_1}^{c_1-1}\cdots\sum_{l_s=b_s}^{c_s-1}\sum_{\mathbf{j}\in M(\mathbf{p})\cup\mathbf{0}}\frac{e\left(j_1\frac{w_n^{(1)}-l_1}{p_1}+\cdots+j_s\frac{w_n^{(s)}-l_s}{p_s}\right)}{p_1\dots p_s}$$
$$=\sum_{\mathbf{j}\in M(\mathbf{p})\cup\mathbf{0}}\sum_{n=0}^{N-1}\frac{1}{p_1\dots p_s}e\left(j_1\frac{w_n^{(1)}}{p_1}+\cdots+j_s\frac{w_n^{(s)}}{p_s}\right)\times$$
$$\sum_{l_1=b_1}^{c_1-1}\cdots\sum_{l_s=b_s}^{c_s-1}e\left(-j_1\frac{l_1}{p_1}-\cdots-j_s\frac{l_s}{p_s}\right).$$

Observe that the term corresponding to $\mathbf{j}=\mathbf{0}$ is $K\prod_{i=1}^{s}\frac{c_i-b_i}{p_i}$, therefore

$$a_K(\mathbf{b},\mathbf{c})-K\prod_{i=1}^{s}\frac{c_i-b_i}{p_i}=\sum_{\mathbf{j}\in M(\mathbf{p})}\sum_{n=0}^{K-1}e\left(j_1\frac{w_n^{(1)}}{p_1}+\cdots+j_s\frac{w_n^{(s)}}{p_s}\right)\frac{1}{p_1\dots p_s}\times$$
$$\sum_{l_1=b_1}^{c_1-1}\cdots\sum_{l_s=b_s}^{c_s-1}e\left(-j_1\frac{l_1}{p_1}-\cdots-j_s\frac{l_s}{p_s}\right).$$

In order to finish the proof, we need the inequality

$$\frac{1}{p_k}\left|\sum_{l_k=b_k}^{c_k-1}e\left(j_k\frac{-l_k}{p_k}\right)\right|\le\frac{1}{r_k\left(j_k\right)}. \tag{12}$$

For $j_k=0$ it is trivial, and for $j_k\neq 0$ it follows from the estimate $|e(-x)-1|=2\left|\sin\left(\pi\|x\|\right)\right|\ge 4\|x\|$. ∎

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 interval (such intervals are usually called* elementary*)* $I=\prod_{i=1}^{s}\left[a_i p_i^{-\alpha_i},(a_i+1)\,p^{-\alpha_i}\right),\quad a_i\in\{0,\dots,p_i^{\alpha_i}-1\}$ *and a subinterval* $J=\prod_{i=1}^{s}\left[a_i p_i^{-\alpha_i}+b_i p_i^{-\alpha_i-1},a_i p_i^{-\alpha_i}+c_i p_i^{-\alpha_i-1}\right),\quad 0\le b_i<c_i\in\{0,\dots,p_i\}$. *Let*

n_0 be the smallest integer with $x_{n_0} \in I$ (we are going to prove that such integer exists). Suppose that x_{n_0} drops into

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

and consider the sequence $\omega = (y_t) \subset \mathbb{Z}^s$, such that $y_t^{(i)} = d_i + tP_i(k_i; \alpha_1, \ldots, \alpha_s)$, with $P_i(k_i; \alpha_1, \ldots, \alpha_s)$ the remainder of $k_i^{\alpha_i} \prod_{1 \le j \le s, j \ne i} p_j^{\alpha_j}$ modulo p_i.

1. *$n_0 < \prod_{i=1}^{s} p_i^{\alpha_i}$ and the indices of the terms of σ that drop into I are of the kind $n = n_0 + t \prod_{i=1}^{s} p_i^{\alpha_i}$.*
2. *For these n the relation $x_n \in J$ is possible if and only if for some integers $(l_1, \ldots, l_s)$, $l_i \in \{b_i, \ldots, c_i - 1\}$, the following system of congruences is satisfied:*
$$d_i + tP_i(k_i; \alpha_1, \ldots, \alpha_s) \equiv l_i (\operatorname{mod} p_i).$$
3. *If K is the largest integer with $n_0 + (K - 1) \prod_{i=1}^{s} p_i^{\alpha_i} < N$:*
$$|A_N(J) - N\mu(J)| < 1 + \sum_{\mathbf{l} \in M(\mathbf{p})} \frac{|S_K(\mathbf{l}, \omega)|}{R(\mathbf{l})},$$

P r o o f. We expand n and a_i in p_i-adic number system, for each i:

$$n = \sum_{j=0}^{\infty} n_{ij} p_i^j, n_{ij} \in \{0, \ldots, p_i - 1\}, \quad a_i = \sum_{j=0}^{\infty} a_{ij} p_i^j, a_{ij} \in \{0, \ldots, p_i - 1\}, \tag{13}$$

From Definitions 1.2. and 2.2. it follows that $x_n \in I$ if and only if the congruences

$$k_i^j n_{ij} \equiv a_{ij} (\operatorname{mod} p_i), j \le \alpha_i, i = 1, \ldots, s \tag{14}$$

are satisfied. Since $p_i \nmid k_i$, and p_i are distinct primes, (14) are satisfied for exactly one n_0 such that $0 \le n_0 < p_1^{\alpha_1} \ldots p_s^{\alpha_s}$. The first α_i digits of $n_0 + t \prod_{i=1}^{s} p_i^{\alpha_i}$ in p_i-adic number system are the same as that of n, and $x_n \in I$ is equivalent to

$$n = n_0 + t \prod_{i=1}^{s} p_i^{\alpha_i}. \tag{15}$$

Now we prove the second property by looking at the next digits of n, defined by (15). The digit before $p_i^{-\alpha_i - 1}$ in x_n is determined by the remainder of $t \prod_{1 \le j \le s, j \ne i} p_j^{\alpha_j}$ modulo p_i by the formula $l_i \equiv d_i + t \prod_{1 \le j \le s, j \ne i} p_j^{\alpha_j} (\operatorname{mod} p_i)$. Obviously

$x_n \in J$ is equivalent to $l_i \in \{b_i, \dots, c_i - 1\}$, which proves the second property. For the last property we observe that only the subsequence of σ, defined by (15) is important. Therefore $A_N(J) = a_K(\mathbf{b}, \mathbf{c})$. Now the inequality

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

together with Lemma 4.2. accomplishes the proof. ■

Proof of Proposition 4.1. We expand $\mathbf{z} = (z^{(1)}, \dots, z^{(s)},) \in \mathbb{E}^s$ in the same way as in Theorem 2.1., and obtain the equality (7) for $A_N\,(J) - N\,\mu\,(J)$. The estimate (9) for Σ_2 depends only on Lemma 3.1., so we can use it here too. We investigate

$$\sum\nolimits_1 = \sum_{\mathbf{j} \in T(N)} A_N(I(\mathbf{j})) - N\,\mu(I(\mathbf{j})).$$

Fix some $\mathbf{j} \in T(N)$. The interval $I(\mathbf{j})$ is contained inside some *elementary* interval $G = \prod_{i=1}^{s} [c_i p_i^{-j_i+1}, (c_i+1) p_i^{-j_i+1})$. Consider the sequence $\omega = \{w_n\}_{n=0}^{\infty} \subset \mathbb{Z}^s$, defined as in Lemma 4.3., i.e. $w_n^{(i)} = d_i + nP_i(k_i; \mathbf{j})$, where the integers d_i are determined by the condition that the first term of the sequence σ that drops into the interval G fits into the smaller interval

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

From the last property in Lemma 4.3. it follows that

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

K being the number of terms of σ among the first N that drop into the interval G. In order to accomplish the proof, we use the inequality

$$|S_K(\mathbf{l}, \omega)| < \frac{1}{2} \left\| \sum_{i=1}^{s} \frac{l_i}{p_i} P_i(k_i; \mathbf{j}) \right\|^{-1},$$

which follows from $\left| \sum_{k=0}^{K-1} e\,(k\alpha + \beta) \right| = \dfrac{|\sin \pi K \alpha|}{|\sin \pi \alpha|} < \dfrac{1}{2\,\|\alpha\|}$, used for $\alpha = \sum_{i=1}^{s} \dfrac{l_i}{p_i} P_i(k_i; \mathbf{j}) \neq 0$, since p_i are pairwise relatively prime and $p_i \nmid P_i(k_i; \mathbf{j})$.

■

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

$$G = \sum_{\mathbf{j} \in M(\mathbf{p})} \sum_{m_1=1}^{p_1-1} \cdots \sum_{m_s=1}^{p_s-1} \frac{\left\| \frac{j_1 m_1}{p_1} + \cdots + \frac{j_s m_s}{p_s} \right\|^{-1}}{2R(\mathbf{j})} \leq$$

$$\sum_{i=1}^{s} \ln p_i \prod_{i=1}^{s} p_i \left(-1 + \prod_{i=1}^{s} (1 + \ln p_i) \right).$$

P r o o f. Denote $P = p_1 \dots p_s$. Fix some $\mathbf{j} \in M(\mathbf{p})$. Let I be the subset of $\{1, \dots, s\}$ of all i, for which $j_i = 0$, and let $J = \{1, \dots, s\} \setminus I$. Fix some integer l between 1 and $P - 1$ and consider the congruence

$$\frac{j_1 m_1 P}{p_1} + \cdots + \frac{j_s m_s P}{p_s} \equiv l \,(\operatorname{mod} P). \tag{16}$$

It follows that p_i divides l for $i \in I$, and that the m_i are uniquely determined by l when $i \in J$. For simplicity suppose that $I = \{1, \dots, k\}$. Then $l = p_1 \dots p_k t$ and t uniquely determines $m_{k+1}, \dots, m_s$. Therefore the contribution to G of all the terms which satisfy the congruence (16) is estimated by

$$G(\mathbf{j}) = \frac{P}{2R(\mathbf{j})} \sum_{t=1}^{\frac{P}{p_1 \cdots p_k}-1} \frac{1}{\min\left(t, \frac{P}{p_1 \cdots p_k} - t\right)}.$$

We are going to use the inequality

$$\sum_{j=1}^{m-1} \frac{1}{\min(j, m-j)} \leq 2 \ln m, \tag{17}$$

for every $m \geq 2$. It easily follows from the estimate $\sum_{k=1}^{n} \frac{1}{k} - \ln n + \gamma \leq \frac{1}{2n}$, (see e.g. [17]) since $2\gamma - 2\ln 2 < 0$ (γ is the Euler constant). Therefore

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

Since $\mathbf{0}$ is not in $M(\mathbf{p})$, we have

$$G \leq \sum_{\mathbf{j} \in M(\mathbf{p})} \frac{P \ln P}{R(\mathbf{j})} \leq P \ln P \left(-1 + \prod_{i=1}^{s} \left(1 + \sum_{j_i=1}^{p_i-1} \frac{1}{2\min(j_i, p_i - j_i)} \right) \right) \leq$$

$$P \ln P \left(-1 + \prod_{i=1}^{s} (1 + \ln p_i) \right).$$

■

Proof of Theorem 2.3. Our proof is based upon Proposition 4.1.. Denote $K = \prod_{i=1}^{s} (p_i - 1)$. For each non-negative integers $\mathbf{a} = a_1, \dots, a_s$ we consider the box of integers $U(\mathbf{a}) = \{(j_1, \dots, j_s) \mid a_i K \leq j_i < (a_i + 1)K\}$. We first prove that for each integer s-tupple $\mathbf{b}$ such that $1 \leq b_i \leq p_i - 1$, there are exactly $\prod_{i=1}^{s} (p_i - 1)^{s-1}$ s-tupples $\mathbf{j} \in U(\mathbf{a})$ such that

$$P_i(k_i, \mathbf{j}) = b_i. \tag{18}$$

Observe that there are K^s elements in $U(\mathbf{a})$ and only K distinct right-hand-sides, therefore for some right-hand-side we have at least K^{s-1} distinct solutions. For each prime p_i we fix some primitive root g_i. Since $p_i \nmid b_i$, for some integers m_i the congruences $b_i \equiv g_i^{m_i} (\operatorname{mod} p_i)$ are fulfilled. The equalities (18) are possible if and only if $\mathbf{j}$ together with some integers $\mathbf{y}$ form a solution to the system (11). We conclude, that if $\mathbf{j}', \mathbf{j}'' \in U(\mathbf{a})$ are two (possibly equal) solutions of (18) for the same right-hand-side $\mathbf{b}$, then the s-tupple $\mathbf{j}'''$ defined by

$$j_i''' = j_i' - j_i'' + \left(\left[\frac{j_i' - j_i''}{(p_1 - 1) \dots (p_s - 1)} \right] \right) (p_1 - 1) \dots (p_s - 1).$$

is a (possibly trivial) solution of the "homogenious" equation (i.e. with righ-hand-side $\mathbf{m} = \mathbf{0}$, $\mathbf{b} = (1, \dots, 1)$) and it is in $U(\mathbf{0})$. It follows that there are at least K^{s-1} solutions of the "homogenious" equation in $U(\mathbf{0})$. Now select an arbitrary right-hand-side $\mathbf{b}$. Since the numbers $k_1, \dots, k_s$ are 'admissible" (see Definition 2.1.), a solution $\mathbf{j}$ of (18) exists. If $\mathbf{j}'$ is any solution of the "homogenious" equation, which is in $U(\mathbf{0})$, the next formula yeilds a solution of (18) in $U(\mathbf{a})$:

$$j_i'' = j_i + j_i' - \left(\left[\frac{j_i + j_i'}{(p_1 - 1) \dots (p_s - 1)} \right] \right) (p_1 - 1) \dots (p_s - 1) + a_i (p_1 - 1) \dots (p_s - 1).$$

Therefore in $U(\mathbf{a})$ there are at least K^{s-1} solutions for any right-hand-side, and now it easily follows that this number is exactly K^{s-1}.

Each $\mathbf{j} \in T(N)$ is inside some box $U(\mathbf{a})$, such that the integer s-tupples $\mathbf{a}$ satisfy $\prod_{i=1}^{s} p_i^{a_i K} \leq N$. We apply Lemma 3.3. for the integers $p_i' = p_i^K$ and the functions $f_i(p) = 1$ and obtain that the number of these s-tupples $\mathbf{a}$ is not more than

$$\frac{1}{s!}\prod_{i=1}^{s}\left(\frac{\ln N}{K\ln p_i}+s\right). \tag{19}$$

Since the contribution $t(\mathbf{j})$ of each $\mathbf{j}\in U(\mathbf{a})$ is non-negative, we can write

$$\sum_{\mathbf{j}\in T(N)} t(\mathbf{j}) \leq \sum_{\mathbf{a}\mid\prod_{i=1}^{s}p_i^{a_iK}\leq N}\ \sum_{\mathbf{j}\in U(\mathbf{a})} t(\mathbf{j}) \leq$$
$$\frac{1}{s!}\prod_{i=1}^{s}\left(\frac{\ln N}{K\ln p_i}+s\right)K^s\left(1+\frac{1}{K}\sum_{i=1}^{s}\ln p_i\prod_{i=1}^{s}p_i\left(-1+\prod_{i=1}^{s}(1+\ln p_i)\right)\right),$$

using Proposition 4.1., Lemma 4.4. and (19). Since $\sum_{i=1}^{s}\ln p_i\prod_{i=1}^{s}\frac{p_i}{p_i-1}\geq 1$ the proof is finished. ∎

References

[1] R. C. Baker, On irregularities of distribution II, *J. London Math. Soc.* (**2**) 59 (1999), 50–64

[2] E. Ehrhart, Sur un problème de géométrie diophantienne linéaire II, *J. Reine Angew. Math.*, **227** (1967), 25–49.

[3] H. Faure, Suites à faible discrépance dans T^s, *Publ.Dép.Math.*, Université de Limoges, France (1980)

[4] H. Faure, Discrépance de suites associées à un système de numéracion (en dimension un), *H. Bull. Soc. Math. France*, **109** (1981), 143–182

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

[6] J. H. Halton, On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals, *Numer. math.*, **2** (1960), 84–90

[7] L. Kuipers, H. Niederreiter, *Uniform distribution of sequences,* John Wiley & sons, New York, 1974.

[8] H.G. Meijer, The discrepancy of a g - adic sequence. *Indag. Math.*, **30** (1968), 54–66.

[9] J.G. Van der Corput, Verteilungsfunktionen, I–VIII, Proc. Akad. Amsterdam, **38** (1935), S. 813–821, 1058–1066, **39** (1936), S. 10–19, 19–26, 149–153, 339–344, 489–494, 579–590.

[10] Knuth, D. E. *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, 3rd ed. Reading, MA: Addison-Wesley, 1998.

[11] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, *SIAM Conf.Ser.Appl.Math.Vol.63* (1992)

[12] Riesel, H. *The Remainder Term in the Prime Number Theorem.* Prime Numbers and Computer Methods for Factorization, 2nd ed. Boston, MA: Birkhüser, 1994.

[13] K. F. Roth, On irregularities of distribution, *Mathematika*, **1** (1954), 73–79.

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

[15] I. M. Sobol, *Multi-dimensional quadrature formulae and Haar functions*, (in Russian), Nauka, Moskwa, 1969.

[16] Walfisz, A. *Ch. 5 in Weyl'sche Exponentialsummen in der neueren Zahlentheorie.* Deutscher Verlag der Wissenschaften, 1963.

[17] R. M. Young, Euler's Constant, *Math. Gaz.*, **75** (1991), 187–190.

Institute for Parallel Processing,
Bulgarian Academy of Sciences
1113 Sofia, BULGARIA
e-mail: emanouil@parallel.bas.bg

Received 27.02.2002