

METRICAL STAR DISCREPANCY BOUNDS FOR LACUNARY SUBSEQUENCES OF DIGITAL KRONECKER-SEQUENCES AND POLYNOMIAL TRACTABILITY

MARIO NEUMÜLLER — FRIEDRICH PILLICHSHAMMER

ABSTRACT. The star discrepancy $D_N^*(\mathcal{P})$ is a quantitative measure for the irregularity of distribution of a finite point set \mathcal{P} in the multi-dimensional unit cube which is intimately related to the integration error of quasi-Monte Carlo algorithms. It is known that for every integer $N \geq 2$ there are point sets \mathcal{P} in $[0, 1]^d$ with $|\mathcal{P}| = N$ and $D_N^*(\mathcal{P}) = O((\log N)^{d-1}/N)$. However, for small N compared to the dimension d this asymptotically excellent bound is useless (e.g., for $N \leq e^{d-1}$).

In 2001 it has been shown by Heinrich, Novak, Wasilkowski and Woźniakowski that for every integer $N \geq 2$ there exist point sets \mathcal{P} in $[0, 1]^d$ with $|\mathcal{P}| = N$ and $D_N^*(\mathcal{P}) \leq C\sqrt{d/N}$. Although not optimal in an asymptotic sense in N , this upper bound has a much better (and even optimal) dependence on the dimension d .

Unfortunately the result by Heinrich et al. and also later variants thereof by other authors are pure existence results and until now no explicit construction of point sets with the above properties is known. Quite recently Löbke studied lacunary subsequences of Kronecker's $(n\alpha)$ -sequence and showed a metrical discrepancy bound of the form $C\sqrt{d(\log d)/N}$ with implied absolute constant $C > 0$ independent of N and d .

In this paper we show a corresponding result for digital Kronecker sequences, which are a non-archimedean analog of classical Kronecker sequences.

Communicated by Werner G. Nowak

2010 Mathematics Subject Classification: 11K38, 11K31, 11K45.

Keywords: star discrepancy, digital Kronecker-sequence, polynomial tractability, quasi-Monte Carlo.

The authors are supported by the Austrian Science Fund (FWF): Projects F5505-N26 (M.N.) and F5509-N26 (F.P.), which are parts of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

1. Introduction

For an N -element point set $\mathcal{P} = \{\mathbf{x}_1, \dots, \mathbf{x}_N\}$ in the d -dimensional unit cube $[0, 1]^d$ the *star discrepancy* D_N^* is defined as

$$D_N^*(\mathcal{P}) = \sup_J \left| \frac{A(J, \mathcal{P})}{N} - \lambda(J) \right|,$$

where the supremum is extended over all intervals of the form $J = [\mathbf{0}, \mathbf{t}) = \prod_{j=1}^d [0, t_j)$ with $t_j \in [0, 1]$, $\mathbf{t} = (t_1, \dots, t_d)$, $A(J, \mathcal{P})$ is the number of indices $n \in \{1, 2, \dots, N\}$ for which \mathbf{x}_n belongs to J and $\lambda(J)$ is the Lebesgue measure of J .

The star discrepancy is a quantitative measure for irregularity of distribution of a point set \mathcal{P} . It is also intimately related to the integration error of a quasi-Monte Carlo (QMC) algorithm via the celebrated Koksma-Hlawka inequality. More information about star discrepancy and its relation to uniform distribution theory and numerical integration can be found in the books [9, 11, 16, 20, 22].

Let $\text{disc}^*(N, d) = \inf_{\mathcal{P}} D_N^*(\mathcal{P})$, where the infimum is extended over all N -element point sets \mathcal{P} in $[0, 1]^d$, be the *minimal star discrepancy* and let, for $\varepsilon \in (0, 1]$, the *inverse of the star discrepancy* be defined as

$$N^*(\varepsilon, d) = \min\{N \in \mathbb{N} : \text{disc}^*(N, d) \leq \varepsilon\}.$$

For fixed dimension $d \geq 2$ it is known that there exist $0 < c_d < C_d$ and $\eta_d \in (0, \frac{1}{2})$ such that

$$c_d \frac{(\log N)^{\frac{d-1}{2} + \eta_d}}{N} \leq \text{disc}^*(N, d) \leq C_d \frac{(\log N)^{d-1}}{N} \quad \text{for all } N \geq 2.$$

The lower bound was shown by Bilyk, Lacey and Vagharyshakyan [5] and for the upper bound there are several explicit constructions of point sets which achieve such a star discrepancy (see, for example, [9, 22] and the references therein). For growing d the exponent η_d in the lower bound tends to zero (approximately with order d^{-2}). It should be mentioned that the exact determination of the power in the $\log N$ -term of the minimal star discrepancy is a very famous and difficult open problem.

In this paper we consider a different view point. It was pointed out in several discussions that the excellent asymptotic behavior of the minimal star discrepancy of N -element point sets is not very useful for practical applications, especially when the dimension d is not small. For example it should be noted that $N \mapsto (\log N)^{d-1}/N$ does not start to decrease until $N \geq \exp(d-1)$ and this number is huge already for moderately large d . In applications of QMC-algorithms however the dimension d could be in the hundreds (see [8], [20]).

Since the last one and a half decades a lot of effort has been put into the analysis of the star discrepancy with respect to dimensions d tending to infinity. In a seminal work by Heinrich, Novak, Waskowski and Woźniakowski [14] it has been shown that there exists an absolute constant $C > 0$ such that

$$\text{disc}^*(N, d) \leq C \sqrt{\frac{d}{N}} \quad \text{for all } d, N \in \mathbb{N} \quad (1)$$

(see [14, Theorem 3]). Later Aistleitner [1, Theorem 1] showed that the constant C can be chosen as $C = 10$. From this we obtain

$$N^*(\varepsilon, d) \leq 100d\varepsilon^{-2}.$$

In the language of “Information Based Complexity” one says that the star discrepancy is *polynomially tractable*, see [23, 24].

On the other hand, Hinrichs [15] showed that $N^*(\varepsilon, d) \geq cd\varepsilon^{-1}$ for all $d \in \mathbb{N}$ and for sufficiently small $\varepsilon > 0$. Hence *the inverse of the star discrepancy depends linearly on the dimension*, which is also the programmatic title of [14].

The proof in [1] and also the proof of the slightly weaker bound

$$\text{disc}^*(N, s) \leq C \sqrt{\frac{d}{N}} (\log d + \log N)^{1/2} \quad (2)$$

in [14, Theorem 1] (which still implies that $N^*(\varepsilon, d) \leq Cd\varepsilon^{-2} \log(d/\varepsilon)$) use the probabilistic method. The main ingredient is the fact that one can obtain extremely small probabilities for the deviation from the mean for sums of independent random variables. This probability can be quantified with the help of Bernstein’s (in [1]) or Hoeffding’s (in [14]) inequality, respectively. In fact, the point sets in [1], [14] consist of N independently chosen random points from the unit cube $[0, 1]^d$. So far no explicit construction of point sets whose star discrepancy satisfies a bound like (1) or (2) is known.

Some authors, initiated in [10], presented algorithmic constructions of point sets with star discrepancy of order (2). We refer to the survey [13] for more information and references in this direction. However, all these constructions have the disadvantage that their run times are too large in order to be applied in practical applications with large dimension d . So there is still need for a really explicit construction.

In 2014 Löbbe [21] studied lacunary subsequences of Kronecker-sequences $(\{n\alpha\})_{n \geq 0}$, where $\alpha \in \mathbb{R}^d$ and where $\{\cdot\}$ denotes the fractional part applied component-wise to a vector (until now the paper is only available via arXiv.org). Based on the work of Aistleitner, Löbbe was able to prove the following remarkable metrical result which can be interpreted as a semi-probabilistic (or semi-constructive) version of (2).

For $\alpha \in [0, 1)^d$ let $\mathcal{P}_N(\alpha) = \{\mathbf{x}_1, \dots, \mathbf{x}_N\}$ be the point set consisting of the first N elements of the infinite sequence $(\mathbf{x}_n)_{n \geq 1}$ in $[0, 1)^d$ with $\mathbf{x}_n = \{2^{n-1}\alpha\}$ for $n \in \mathbb{N}$.

THEOREM 1 (Löb b e [21, Theorem 1.1]). *Let $N \geq 1$ and $d \geq 2$ be integers. Then for every $\varepsilon \in (0, 1)$ there is a quantity $C(\varepsilon) > 0$ such that the star discrepancy of the point set $\mathcal{P}_N(\alpha)$ satisfies*

$$D_N^*(\mathcal{P}_N(\alpha)) \leq C(\varepsilon) \sqrt{\frac{d \log d}{N}}$$

with probability at least $1 - \varepsilon$. The quantity $C(\varepsilon)$ is of order $C(\varepsilon) \asymp \log \varepsilon^{-1}$.

The main problem in the proof of this result is to prove independence of certain random variables in order to be able to apply Bernstein's inequality. Of course, the elements of the classical Kronecker-sequence are not independent. For this reason the author studied lacunary subsequences of the form $(\{2^{n-1}\alpha\})_{n \geq 1}$ which led then to the desired independence properties.

Theorem 1 makes an assertion for fixed N , i.e., for finite point sets. In 2007 Dick [7] considered the problem of the dependence of star discrepancy on the dimension d also for infinite sequences and he gave an existence result. Compared to the bound (1) for finite point sets the generalization is penalized with an extra $\sqrt{\log N}$ -factor in the discrepancy estimate. Later Aistleitner [2] improved this further and got rid of the $\sqrt{\log N}$ -term. In contrast to the probabilistic approaches in, e.g., [14, 7], the proof in [2] is, like in [21], also of a semi-probabilistic nature in the sense that certain coordinates of the points are deterministic others are chosen randomly. This once more shows the relevance of semi-probabilistic construction in this context.

The following corollary to Theorem 1 addresses a metrical result for infinite sequences:

COROLLARY 2. *Let $d \in \mathbb{N}$ with $d \geq 2$. Then for every $\delta \in (0, 1)$ there is a quantity $C(\delta) > 0$ such that the star discrepancy of $\mathcal{P}_N(\alpha)$ satisfies*

$$D_N^*(\mathcal{P}_N(\alpha)) \leq C(\delta)(\log N) \sqrt{\frac{d \log d}{N}} \quad \text{for all } N \geq 2$$

with probability at least $1 - \delta$. We have $C(\delta) \asymp \log \delta^{-1}$.

Concerning the proof of Corollary 2 we will refer to Section 3.5.

There is an interesting connection of Corollary 2 to the theory of normal numbers which is worth to be mentioned: it is well-known that a real number α is normal to base 2, if and only if the sequence $(\{2^{n-1}\alpha\})_{n \geq 1}$ is uniformly

distributed modulo one (see [16, Chapter 1, Theorem 8.1]). Hence the α 's which satisfy the discrepancy estimate in Corollary 2 are d -tuples of normal numbers to base 2. (By another well-known result due to Borel [6] almost all numbers $\alpha \in [0, 1]$ are normal to every base $b \geq 2$.)

It should also be mentioned, that metrical bounds on the star-discrepancy of classical Kronecker-sequences for fixed d have been given by Beck in [3].

In this paper we study digital Kronecker-sequences. These sequences are a “non-archimedean analog” to classical Kronecker-sequences which fit into the class of digital (t, s) -sequences. This concept was introduced by Niederreiter [22, Section 4] and further investigated by Larcher and Niederreiter [18]. We will give a digital analog of Theorem 1.

In the next section we provide the necessary definitions and we formulate the metrical discrepancy estimate. The proof of our result will be presented in Section 3.

2. Digital Kronecker-sequences and formulation of the main result

Let q be a prime number and let $\mathbb{Z}_q = \{0, \dots, q-1\}$ be the finite field of order q with the usual arithmetic operations modulo q . We denote the field of formal Laurent series over \mathbb{Z}_q in the variable t^{-1} by $\mathbb{Z}_q((t^{-1}))$. Elements of $\mathbb{Z}_q((t^{-1}))$ are of the form

$$g = \sum_{i=w}^{\infty} g_i t^{-i}, \quad (3)$$

where w is an arbitrary integer and all $g_i \in \mathbb{Z}_q$ with $g_w \neq 0$. Note that $\mathbb{Z}_q((t^{-1}))$ contains the polynomial ring $\mathbb{Z}_q[t]$ over \mathbb{Z}_q .

For a formal Laurent series g of the form (3) we define its “fractional part” by

$$\{g\} := \sum_{i=\max(1, w)}^{\infty} g_i t^{-i}.$$

Let

$$\begin{aligned} \overline{\mathbb{Z}}_q((t^{-1})) &:= \{\{g\} : g \in \mathbb{Z}_q((t^{-1}))\} \\ &= \{g \in \mathbb{Z}_q((t^{-1})) : g \text{ of the form (3) with } w \geq 1\} \end{aligned}$$

and define further

$$\phi : \overline{\mathbb{Z}}_q((t^{-1})) \rightarrow [0, 1), \quad \sum_{i=1}^{\infty} g_i t^{-i} \mapsto \sum_{i=1}^{\infty} g_i q^{-i}.$$

Applied to vectors the operations $\{\cdot\}$ and ϕ are understood component-wise.

We associate a nonnegative integer n with q -adic expansion $n = n_0 + n_1q + \cdots + n_rq^r$, where $n_0, \dots, n_r \in \mathbb{Z}_q$ with the polynomial $n(t) = n_0 + n_1t + \cdots + n_rt^r$ in $\mathbb{Z}_q[t]$ and vice versa.

DEFINITION 1. For a given d -tuple $\mathbf{f} = (f_1, \dots, f_d)$ of elements of $\mathbb{Z}_q((t^{-1}))$ the sequence $\mathcal{S}(\mathbf{f}) = (\mathbf{y}_n)_{n \geq 0}$ given by

$$\mathbf{y}_n = \phi(\{n\mathbf{f}\}) = (\phi(\{nf_1\}), \dots, \phi(\{nf_d\})) \quad \text{for all } n \in \mathbb{N}_0$$

is called a *digital Kronecker-sequence* over \mathbb{Z}_q . Note that the multiplication of the polynomial n and the Laurent series f_j is carried out in $\mathbb{Z}_q((t^{-1}))$. (Obviously, it suffices to choose $\mathbf{f} \in (\overline{\mathbb{Z}_q}((t^{-1})))^d$.)

In order to prove a metrical result for digital Kronecker-sequences we need to introduce a suitable probability measure on $(\overline{\mathbb{Z}_q}((t^{-1})))^d$.

DEFINITION 2. By μ we denote the normalized Haar-measure on $\overline{\mathbb{Z}_q}((t^{-1}))$ and by μ_d the d -fold product measure on $(\overline{\mathbb{Z}_q}((t^{-1})))^d$.

REMARK 1. The measure μ has the following rather simple shape: If we identify the elements $\sum_{k=1}^{\infty} g_k t^{-k}$ of $\overline{\mathbb{Z}_q}((t^{-1}))$ where $g_k \neq q-1$ for infinitely many k in the natural way with the real numbers $\sum_{k=1}^{\infty} g_k q^{-k} \in [0, 1)$, then, by neglecting the countably many elements where $g_k \neq q-1$ only for finitely many k , μ corresponds to the Lebesgue measure λ on $[0, 1)$. For example, the “cylinder set” $C(c_1, \dots, c_m)$ consisting of all elements $g = \sum_{k=1}^{\infty} g_k t^{-k}$ from $\overline{\mathbb{Z}_q}((t^{-1}))$ with $g_k = c_k$ for $k = 1, \dots, m$ and arbitrary $g_k \in \mathbb{Z}_q$ for $k \geq m+1$ has measure $\mu(C(c_1, \dots, c_m)) = q^{-m}$.

Metrical results for the star discrepancy of digital Kronecker-sequences for fixed dimension d can be found in [17, 19]. In the following we provide a non-archimedean version of the result of Löbke [21].

For $\mathbf{f} \in (\overline{\mathbb{Z}_q}((t^{-1})))^d$ let $\mathcal{P}_N(\mathbf{f}) = \{\mathbf{x}_1, \dots, \mathbf{x}_N\}$ be the point set consisting of the first N elements of the infinite sequence $(\mathbf{x}_n)_{n \geq 1}$ in $[0, 1)^d$ with $\mathbf{x}_n = \phi(\{t^{n-1}\mathbf{f}\})$ for $n \in \mathbb{N}$.

THEOREM 3. Let q be a prime number and let $N, d \in \mathbb{N}$ with $N, d \geq 2$. Then for every $\varepsilon \in (0, 1)$ there is a quantity $C(q, \varepsilon) > 0$ such that the star discrepancy of the point set $\mathcal{P}_N(\mathbf{f})$ satisfies

$$D_N^*(\mathcal{P}_N(\mathbf{f})) \leq C(q, \varepsilon) \sqrt{\frac{d \log d}{N}}$$

with probability at least $1 - \varepsilon$. The quantity $C(q, \varepsilon)$ is of order $C(q, \varepsilon) \asymp \log \varepsilon^{-1}$.

The proof of this result will be presented in the next section. It should be mentioned that with some more effort the quantity $C(q, \varepsilon)$ could be given explicitly.

Again Theorem 3 makes an assertion for fixed N , i.e., for finite point sets. From this we can again deduce a metrical result for infinite sequences:

COROLLARY 4. *Let q be a prime number and let $d \in \mathbb{N}$ with $d \geq 2$. Then for every $\delta \in (0, 1)$ there is a quantity $C(q, \delta) > 0$ such that the star discrepancy of $\mathcal{P}_N(\mathbf{f})$ satisfies*

$$D_N^*(\mathcal{P}_N(\mathbf{f})) \leq C(q, \delta)(\log N) \sqrt{\frac{d \log d}{N}} \quad \text{for all } N \geq 2$$

with probability at least $1 - \delta$.

The proof of Corollary 4 will be presented in Section 3.5.

3. The proof of Theorem 3

The proof of Theorem 3 is inspired by the techniques used in [21]. The difficulty here is that we are concerned with polynomial arithmetic over finite fields instead of the usual integer arithmetic.

Throughout the proof we tacitly assume that all components of \mathbf{f} belong to the class of Laurent series $\sum_{k=1}^{\infty} g_k t^{-k}$ of $\overline{\mathbb{Z}}_q((t^{-1}))$ where $g_k \neq q-1$ for infinitely many k . Let

$$\mathcal{C} = \{g \in \overline{\mathbb{Z}}_q((t^{-1})) : g_k = q-1 \text{ for all but finitely many } k \geq 1\}.$$

Note that \mathcal{C} is a countable set and therefore $\mu(\mathcal{C}) = 0$. We denote $\overline{\mathbb{Z}}_q^*((t^{-1})) := \overline{\mathbb{Z}}_q((t^{-1})) \setminus \mathcal{C}$. Hence we assume that $\mathbf{f} \in (\overline{\mathbb{Z}}_q^*((t^{-1})))^d$.

3.1. Some auxiliary results

As in [1, 21] the proof will be based on Bernstein's inequality for sums of independent random variables.

LEMMA 5 ([4], The Bernstein inequality). *Let $N \in \mathbb{N}$ and X_1, \dots, X_N be independent random variables with $\mathbb{E}(X_i) = 0$ and $|X_i| \leq C$ for $i \in \{1, \dots, N\}$ and some $C > 0$. Then we have for any $t > 0$*

$$\mathbb{P} \left(\left| \sum_{i=1}^N X_i \right| > t \right) \leq 2 \exp \left(- \frac{t^2}{2 \sum_{i=1}^N \mathbb{E}(X_i^2) + \frac{2Ct}{3}} \right).$$

Another very important tool in our analysis are bracketing covers whose definition is recalled below. As usual, for $\mathbf{a} = (a_1, \dots, a_d)$ and $\mathbf{b} = (b_1, \dots, b_d)$ in $[0, 1]^d$ we write $\mathbf{a} \leq \mathbf{b}$ if and only if $a_i \leq b_i$ for all $i \in \{1, \dots, d\}$.

DEFINITION 3. Let $\delta > 0$. A subset $\tau \subseteq [0, 1]^d \times [0, 1]^d$ is called a δ -bracketing cover if for every $\mathbf{x} \in [0, 1]^d$ there exists $(\mathbf{v}, \mathbf{w}) \in \tau$ such that $\mathbf{v} \leq \mathbf{x} \leq \mathbf{w}$ and $\lambda([0, \mathbf{w}) \setminus [0, \mathbf{v})) \leq \delta$.

The following result about the number of elements of a δ -bracketing cover is due to Gnewuch:

LEMMA 6 (Gnewuch [12, Theorem 1.15]). *For any $d \in \mathbb{N}$ and any $\delta > 0$ there exists a δ -bracketing cover τ with*

$$|\tau| \leq \frac{1}{2}(2e)^d(\delta^{-1} + 1)^d.$$

From this result Löbbeck deduced the following corollary:

COROLLARY 7 (Löbbeck [21, Corollary 2.3]). *Let $d, h \in \mathbb{N}$ and $q \geq 2$, then there exists a q^{-h} -bracketing cover τ_h with*

- (1) $|\tau_h| \leq \frac{1}{2}(2e)^d(q^{h+2} + 1)^d$, and
- (2) for $(\mathbf{v}, \mathbf{w}) \in \tau_h$ and $i \in \{1, \dots, d\}$ there exist $a_i \in \{0, 1, \dots, q^{h+1+\lceil \log_q d \rceil}\}$ and $b_i \in \{0, 1, \dots, q^{h+2+\lceil \log_q d \rceil}\}$ such that

$$v_i = \frac{a_i}{q^{h+1+\lceil \log_q d \rceil}} \quad \text{and} \quad w_i = \frac{b_i}{q^{h+2+\lceil \log_q d \rceil}}.$$

3.2. Preliminaries

Let $N, d \in \mathbb{N}$ and fix some $H \in \mathbb{N}$. For $h \in \{1, \dots, H\}$ let τ_h be a q^{-h} -bracketing cover of $[0, 1]^d$ with elements described as in Corollary 7. Let $\mathbf{y} \in [0, 1]^d$. We are going to define inductively a finite sequence of points $\beta_h(\mathbf{y}) \in [0, 1]^d$ for $h \in \{0, \dots, H+1\}$ in the following way:

- (1) Let $\beta_H(\mathbf{y}), \beta_{H+1}(\mathbf{y}) \in [0, 1]^d$ with $\beta_H(\mathbf{y}) \leq \mathbf{y} \leq \beta_{H+1}(\mathbf{y})$ and $(\beta_H(\mathbf{y}), \beta_{H+1}(\mathbf{y})) \in \tau_H$.
- (2) For $h \in \{1, \dots, H-1\}$ let $\beta_h(\mathbf{y}) \in [0, 1]^d$ be such that there exists a point $\mathbf{w} \in [0, 1]^d$ with $\beta_h(\mathbf{y}) \leq \beta_{h+1}(\mathbf{y}) \leq \mathbf{w}$ and $(\beta_h(\mathbf{y}), \mathbf{w}) \in \tau_h$.
- (3) Set $\beta_0(\mathbf{y}) = \mathbf{0} = (0, \dots, 0)$, the d -dimensional zero-vector.
- (4) Additionally we choose the points β_h such that the following property is fulfilled. For $\mathbf{x}, \mathbf{y} \in [0, 1]^d$ and $h \in \{0, \dots, H-1\}$ we have that

$$\beta_{h+1}(\mathbf{y}) = \beta_{h+1}(\mathbf{x}) \Rightarrow \beta_h(\mathbf{y}) = \beta_h(\mathbf{x}).$$

Note that the sequence of points $\beta_h(\mathbf{y})$ is well defined for $h \in \{0, \dots, H+1\}$ since we choose τ_h to be a q^{-h} -bracketing cover. For $\mathbf{y} \in [0, 1)^d$ we observe the following properties for the finite sequence $\beta_h(\mathbf{y})$:

We have

- (1) $\mathbf{0} = \beta_0(\mathbf{y}) \leq \beta_1(\mathbf{y}) \leq \dots \leq \beta_H(\mathbf{y}) \leq \mathbf{y} \leq \beta_{H+1}(\mathbf{y}) \leq \mathbf{1}$;
- (2) for all $h \in \{0, \dots, H-1\}$ there exists $\mathbf{w} \in [0, 1)^d$ such that $\beta_h(\mathbf{y}) \leq \beta_{h+1}(\mathbf{y}) \leq \mathbf{w}$ and $(\beta_h(\mathbf{y}), \mathbf{w}) \in \tau_h$. Note that $(\beta_H(\mathbf{y}), \beta_{H+1}(\mathbf{y})) \in \tau_H$;
- (3) for all $h \in \{0, \dots, H\}$ and $i \in \{1, \dots, d\}$ we have that

$$(\beta_h(\mathbf{y}))_i = q^{-(h+1+\lceil \log_q d \rceil)} a_{h,i}$$

and

$$(\beta_{H+1}(\mathbf{y}))_i = q^{-(H+2+\lceil \log_q d \rceil)} b_{H+1,i}$$

for $a_{h,i} \in \{0, 1, \dots, q^{h+1+\lceil \log_q d \rceil}\}$ and $b_{H+1,i} \in \{0, 1, \dots, q^{H+2+\lceil \log_q d \rceil}\}$.

The properties 1. and 2. are an immediate consequence of the definition of the $\beta_h(\mathbf{y})$ and property 3. follows directly by Corollary 7.

Moreover, for $h \in \{0, \dots, H\}$ we define $K_h(\mathbf{y}) := [\mathbf{0}, \beta_{h+1}(\mathbf{y})) \setminus [\mathbf{0}, \beta_h(\mathbf{y}))$ and observe that the $K_h(\mathbf{y})$ are pairwise disjoint sets and by the definition respectively property 2. of $\beta_h(\mathbf{y})$ we obtain

$$\bigcup_{h=0}^{H-1} K_h(\mathbf{y}) \subseteq [\mathbf{0}, \mathbf{y}) \subseteq \bigcup_{h=0}^H K_h(\mathbf{y}) \quad \text{and} \quad \lambda(K_h(\mathbf{y})) \leq q^{-h}. \quad (4)$$

Finally, for $\{0, \dots, H\}$ define $S_h := \{K_h(\mathbf{y}) : \mathbf{y} \in [0, 1)^d\}$. Note that by definition of the $\beta_h(\mathbf{y})$ and Corollary 7 we have

$$|S_H| = |\{(\beta_H(\mathbf{y}), \beta_{H+1}(\mathbf{y})) : \mathbf{y} \in [0, 1)^d\}| \leq |\tau_H| \leq \frac{1}{2}(2e)^d(q^{H+2} + 1)^d.$$

With point 4. in the definition of the $\beta_h(\mathbf{y})$ we get for $h \in \{0, \dots, H-1\}$ that

$$|S_h| = |\{\beta_{h+1}(\mathbf{y}) : \mathbf{y} \in [0, 1)^d\}| \leq |\tau_{h+1}| \leq \frac{1}{2}(2e)^d(q^{h+3} + 1)^d.$$

Fix $\mathbf{y} \in [0, 1)^d$. In order to simplify the notation from now on, we will write β_h and K_h instead of $\beta_h(\mathbf{y})$ and $K_h(\mathbf{y})$, respectively. Then by (4) we get that

$$\begin{aligned} \sum_{n=1}^N \mathbf{1}_{[\mathbf{0}, \mathbf{y})}(\mathbf{x}_n) &\geq \sum_{n=1}^N \mathbf{1}_{[\mathbf{0}, \beta_H)}(\mathbf{x}_n) \\ &= \sum_{h=0}^{H-1} \sum_{n=1}^N \left(\mathbf{1}_{K_h}(\mathbf{x}_n) - \lambda(K_h) \right) + N \sum_{h=0}^{H-1} \lambda(K_h) \end{aligned} \quad (5)$$

and

$$\begin{aligned} \sum_{n=1}^N \mathbf{1}_{[0, \mathbf{y})}(\mathbf{x}_n) &\leq \sum_{n=1}^N \mathbf{1}_{[0, \beta_{H+1})}(\mathbf{x}_n) \\ &= \sum_{h=0}^H \sum_{n=1}^N \left(\mathbf{1}_{K_h}(\mathbf{x}_n) - \lambda(K_h) \right) + N \sum_{h=0}^H \lambda(K_h). \end{aligned} \quad (6)$$

Let us define the functions $\Delta_{K_h} : [0, 1]^d \rightarrow [-1, 1]$, $\Delta_{K_h}(\mathbf{x}) := \mathbf{1}_{K_h}(\mathbf{x}) - \lambda(K_h)$ for $h \in \{0, \dots, H\}$. A crucial step for the proof of the main result will be to use Bernstein's inequality to give a lower bound on the probability that the inequality

$$\left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| \leq t_h$$

holds simultaneously for all $h \in \{0, \dots, H\}$ and for some $t_h > 0$ to be specified later. First of all observe that

$$\mathbb{E}(\Delta_{K_h}(\mathbf{x}_n)) = 0, \quad \mathbb{E}^2(\Delta_{K_h}(\mathbf{x}_n)) = \lambda(K_h)(1 - \lambda(K_h)) \quad \text{and} \quad |\Delta_{K_h}(\mathbf{x}_n)| \leq 1$$

$$\text{for all } h \in \{0, \dots, H\} \quad \text{and} \quad n \in \{1, \dots, N\}.$$

Unfortunately for $h \in \{0, \dots, H\}$ the random variables $\Delta_{K_h}(\mathbf{x}_1), \Delta_{K_h}(\mathbf{x}_2), \dots, \Delta_{K_h}(\mathbf{x}_N)$ are not independent in general. We will see how to overcome this problem in the next section.

3.3. Independence of $\Delta_{K_h}(\mathbf{x}_n)$

Before we begin we point out the following easy algebraic characterization of Laurent series whose image under ϕ belongs to a certain type of intervals: for $p \in \overline{\mathbb{Z}}_q^*((t^{-1}))$ of the form $p = p_1 t^{-1} + p_2 t^{-2} + p_3 t^{-3} + \dots$, for $r \in \mathbb{N}$ and $k \in \{0, \dots, q^r - 1\}$ with q -adic expansion $k = k_0 + k_1 q + \dots + k_{r-1} q^{r-1}$ we have that

$$\phi(p) \in \left[\frac{k}{q^r}, \frac{k+1}{q^r} \right) \Leftrightarrow p_1 = k_{r-1}, p_2 = k_{r-2}, \dots, p_r = k_0.$$

Throughout the proof the underlying probability measure is the measure μ_d from Definition 2. However, out of habit we will in the following denote the probability by \mathbb{P} .

LEMMA 8. *Let $\kappa_h := \log_2(h+2 + \lceil \log_q d \rceil)$ and let $\gamma \in \{0, \dots, 2^{\kappa_h} - 1\}$. Moreover, let*

$$Q(N, \kappa_h, \gamma) := \{n \in \{1, \dots, N\} : n \equiv \gamma \pmod{2^{\kappa_h}}\}.$$

Then for $n_1, \dots, n_l \in Q(N, \kappa_h, \gamma)$ and $l \in \{1, \dots, |Q(N, \kappa_h, \gamma)|\}$ the random variables $\Delta_{K_h}(\mathbf{x}_{n_1}), \Delta_{K_h}(\mathbf{x}_{n_2}), \dots, \Delta_{K_h}(\mathbf{x}_{n_l})$ are independent, i.e.,

$$\mathbb{P}(\Delta_{K_h}(\mathbf{x}_{n_1}) = c_1, \dots, \Delta_{K_h}(\mathbf{x}_{n_l}) = c_l) = \prod_{r=1}^l \mathbb{P}(\Delta_{K_h}(\mathbf{x}_{n_r}) = c_r).$$

Proof. The proof is based on the ideas from [21]. We will show the case $l = 2$. The general case follows by induction. Let $h \in \{0, \dots, H\}$, $\gamma \in \{0, \dots, 2^{\kappa_h} - 1\}$ and $n, m \in Q(N, \kappa_h, \gamma)$ with $n > m$. We want to show that $\Delta_{K_h}(\mathbf{x}_n), \Delta_{K_h}(\mathbf{x}_m)$ are independent. To this end we consider the following decomposition of $[0, 1]^d$:

$$\Sigma_{n-1} := \left\{ \prod_{i=1}^d \left[\frac{a_i}{q^{n-1}}, \frac{a_i + 1}{q^{n-1}} \right) : a_i \in \{0, \dots, q^{n-1} - 1\} \right\}.$$

Since the underlying structure of the sequence $(\mathbf{x}_k)_{k \geq 1}$ is $\overline{\mathbb{Z}}_q((t^{-1}))$ we are considering the preimage of Σ_{n-1} .

$$\Lambda_{n-1} := \left\{ \phi^{-1}(S) \cap \left(\overline{\mathbb{Z}}_q^*((t^{-1})) \right)^d : S \in \Sigma_{n-1} \right\},$$

For $A = (a_{i,j})_{i=1,j=1}^{d,n-1} \in \mathbb{Z}_q^{d \times (n-1)}$ let us define

$$B_A := \prod_{i=1}^d \left\{ g \in \overline{\mathbb{Z}}_q^*((t^{-1})) : (g_1, \dots, g_{n-1}) = (a_{i,1}, \dots, a_{i,n-1}) \right\}.$$

where $(a_{i,1}, \dots, a_{i,n-1})$ is the i -th row of A . One can easily check that

$$\Lambda_{n-1} = \left\{ B_A : A \in \mathbb{Z}_q^{d \times (n-1)} \right\}.$$

For matrices $A_1, A_2 \in \mathbb{Z}_q^{d \times (n-1)}$, $A_j = (a_{j,i,k})_{i=1,k=1}^{d,n-1}$ for $j \in \{1, 2\}$ we define

$$\begin{aligned} \alpha_{A_1, A_2} : \left(\overline{\mathbb{Z}}_q((t^{-1})) \right)^d &\rightarrow \left(\overline{\mathbb{Z}}_q((t^{-1})) \right)^d, \\ \left(g^{(1)}, \dots, g^{(d)} \right) &\mapsto \left(g^{(1)} + u_{A_1 A_2}^{(1)}, \dots, g^{(d)} + u_{A_1 A_2}^{(d)} \right), \end{aligned}$$

where for $i \in \{1, \dots, d\}$, $u_{A_1 A_2}^{(i)} = \sum_{k=1}^{\infty} u_{A_1 A_2, k}^{(i)} t^{-k} \in \overline{\mathbb{Z}}_q((t^{-1}))$ and

$$u_{A_1 A_2, k}^{(i)} = \begin{cases} a_{2,i,k} - a_{1,i,k} & \text{if } 1 \leq k \leq n-1, \\ 0 & \text{if } k > n-1. \end{cases}$$

With this definition we have

$$\alpha_{A_1, A_2}(B_{A_1}) = B_{A_2}.$$

Before we can prove the independence of $\Delta_{K_h}(\mathbf{x}_n)$ and $\Delta_{K_h}(\mathbf{x}_m)$, we need to show four claims:

CLAIM 1. *Let $c \in \mathbb{R}$, $A_1, A_2 \in \mathbb{Z}_q^{d \times (n-1)}$, $\mathbf{f} \in B_{A_1}$ and $(\mathbf{y}_n)_{n \geq 1}$ in $[0, 1)^d$ with $\mathbf{y}_n = \phi(\{t^{n-1} \bar{\mathbf{f}}\})$ with $\bar{\mathbf{f}} = \alpha_{A_1 A_2}(\mathbf{f})$. Then we have that*

$$\mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c \mid \mathbf{f} \in B_{A_1}) = \mathbb{P}(\Delta_{K_h}(\mathbf{y}_n) = c \mid \bar{\mathbf{f}} \in B_{A_2}).$$

Proof of Claim 1. For $i \in \{1, \dots, d\}$ we have that

$$y_{n,i} = \phi\left(\left\{t^{n-1} \bar{f}^{(i)}\right\}\right) = \phi\left(\left\{t^{n-1} f^{(i)} + \left(t^{n-1} u_{A_1 A_2}^{(i)}\right)\right\}\right) = \phi\left(\left\{t^{n-1} f^{(i)}\right\}\right) = x_{n,i}.$$

Note that the second last equality is true because $u_{A_1 A_2, k}^{(i)} = 0$ for $k \geq n$. Additionally it holds that $\mathbf{f} \in B_{A_1} \Leftrightarrow \bar{\mathbf{f}} \in B_{A_2}$. Therefore the claim follows. \square

CLAIM 2. *Let $h \in \{0, \dots, H\}$ and $\mathbf{p} = (p^{(1)}, \dots, p^{(d)}) \in (\overline{\mathbb{Z}}_q^*((t^{-1})))^d$ with $p^{(i)} = \sum_{j=1}^{\infty} p_j^{(i)} t^{-j}$. Then the $d(h+2+\lceil \log_q d \rceil)$ coefficients $p_1^{(i)}, \dots, p_{h+2+\lceil \log_q d \rceil}^{(i)}$ for $i \in \{1, \dots, d\}$ determine if $\phi(\mathbf{p}) \in K_h$.*

Proof of Claim 2. For $\mathbf{p} = (p^{(1)}, \dots, p^{(d)}) \in (\overline{\mathbb{Z}}_q^*((t^{-1})))^d$, we have that

$$\begin{aligned} \phi(\mathbf{p}) \in K_h &\Leftrightarrow \phi(\mathbf{p}) \in [\mathbf{0}, \beta_{h+1}) \setminus [\mathbf{0}, \beta_h) \\ &\Leftrightarrow \forall i \in \{1, \dots, d\} : \phi(p^{(i)}) \in [0, \beta_{h+1}^{(i)}) \end{aligned}$$

and

$$\exists j \in \{1, \dots, d\} : \phi(p^{(j)}) \in [\beta_h^{(j)}, 1),$$

(7)

where $\beta_{h+1} = (\beta_{h+1}^{(1)}, \dots, \beta_{h+1}^{(d)})$ with

$$\beta_{h+1}^{(i)} = \frac{b_i}{q^{h+2+\lceil \log_q d \rceil}} \quad \text{for some } b_i \in \{0, 1, \dots, q^{h+2+\lceil \log_q d \rceil} - 1\},$$

and similarly, $\beta_h = (\beta_h^{(1)}, \dots, \beta_h^{(d)})$ with

$$\beta_h^{(i)} = \frac{\bar{b}_i}{q^{h+1+\lceil \log_q d \rceil}} \quad \text{for some } \bar{b}_i \in \{0, 1, \dots, q^{h+1+\lceil \log_q d \rceil} - 1\}.$$

We can write

$$[0, \beta_{h+1}^{(i)}) = \bigcup_{k=0}^{b_i-1} \left[\frac{k}{q^{h+2+\lceil \log_q d \rceil}}, \frac{k+1}{q^{h+2+\lceil \log_q d \rceil}} \right).$$

Hence $\phi(p^{(i)}) \in [0, \beta_{h+1}^{(i)})$ if and only if there exists a $k \in \{0, \dots, b_i - 1\}$ such that

$$\phi(p^{(i)}) \in \left[\frac{k}{q^{h+2+\lceil \log_q d \rceil}}, \frac{k+1}{q^{h+2+\lceil \log_q d \rceil}} \right).$$

Since $\phi(p^{(i)}) = \sum_{j=1}^{\infty} p_j^{(i)} q^{-j}$ the last condition is satisfied if and only if

$$p_1^{(i)} = k_{h+1+\lceil \log_q d \rceil}, p_2^{(i)} = k_{h+\lceil \log_q d \rceil}, \dots, p_{h+2+\lceil \log_q d \rceil}^{(i)} = k_0,$$

whenever k has q -adic expansion $k = k_0 + k_1 q + \dots + k_{h+1+\lceil \log_q d \rceil} q^{h+1+\lceil \log_q d \rceil}$.

In the same vein we can write

$$[\beta_h^{(j)}, 1) = \bigcup_{\ell=\bar{b}_j}^{q^{h+1+\lceil \log_q d \rceil}-1} \left[\frac{\ell}{q^{h+1+\lceil \log_q d \rceil}}, \frac{\ell+1}{q^{h+1+\lceil \log_q d \rceil}} \right).$$

Hence $\phi(p^{(j)}) \in [\beta_h^{(j)}, 1)$ if and only if there exists a $\ell \in \{\bar{b}_j, q^{h+1+\lceil \log_q d \rceil} - 1\}$ such that

$$\phi(p^{(j)}) \in \left[\frac{\ell}{q^{h+1+\lceil \log_q d \rceil}}, \frac{\ell+1}{q^{h+1+\lceil \log_q d \rceil}} \right).$$

Since $\phi(p^{(j)}) = \sum_{k=1}^{\infty} p_k^{(j)} q^{-k}$ the last condition is satisfied if and only if

$$p_1^{(j)} = l_{h+\lceil \log_q d \rceil}, p_2^{(j)} = l_{h+\lceil \log_q d \rceil-1}, \dots, p_{h+1+\lceil \log_q d \rceil}^{(j)} = l_0,$$

whenever ℓ has q -adic expansion $\ell = l_0 + l_1 q + \dots + l_{h+\lceil \log_q d \rceil} q^{h+\lceil \log_q d \rceil}$.

Together with (7) it follows that the coefficients $p_1^{(i)}, \dots, p_{h+2+\lceil \log_q d \rceil}^{(i)}$ for $i \in \{1, \dots, d\}$ determine whether or not $\phi(\mathbf{p})$ belongs to K_h . This proves the second claim. \square

Recall that $m \in Q(N, \kappa_h, \gamma)$ and $m < n$. Define

$$\delta_m : \overline{\mathbb{Z}}_q((t^{-1})) \rightarrow \overline{\mathbb{Z}}_q((t^{-1})), p \mapsto \{t^{m-1}p\}.$$

CLAIM 3. For all $h \in \{0, \dots, H\}$ and for all $A \in \mathbb{Z}_q^{d \times (n-1)}$ we have that Δ_{K_h} is constant on $\phi(\delta_m(B_A))$.

Proof of Claim 3. Let $\mathbf{p} = (p^{(1)}, \dots, p^{(d)}) \in B_A$ with $p^{(i)} = \sum_{j=1}^{\infty} p_j^{(i)} t^{-j}$. Note that for each $i \in \{1, \dots, d\}$ the first $n-1$ coefficients $p_1^{(i)}, \dots, p_{n-1}^{(i)}$ of $p^{(i)}$ are equal to the entries in the i -th row of A . Now we have

$$\delta_m \left(\sum_{j=1}^{\infty} p_j^{(i)} t^{-j} \right) = \left\{ \sum_{j=1}^{\infty} p_j^{(i)} t^{m-1-j} \right\} = \sum_{j=1}^{\infty} p_{m-1+j}^{(i)} t^{-j}.$$

Because of Claim 2, the coefficients $p_m^{(i)}, \dots, p_{m+h+1+\lceil \log_q d \rceil}^{(i)}$ for $i \in \{1, \dots, d\}$ determine if $\phi(\delta_m(\mathbf{p})) \in K_h$. Since $n - m \geq h + 2 + \lceil \log_q d \rceil$ these coefficients are fixed by the choice of B_A . Hence it follows that $\phi(\delta_m(B_A)) \cap K_h \in \{\emptyset, \phi(\delta_m(B_A))\}$. Therefore the function $\Delta_{K_h}(\mathbf{x}) = \mathbf{1}_{K_h}(\mathbf{x}) - \lambda(K_h)$ is constant on $\phi(\delta_m(B_A))$. This proves the claim. \square

Define for $c \in \mathbb{R}$,

$$\Lambda_{K_h, c} := \left\{ B_A \in \Lambda_{n-1} : \Delta_{K_h}(\phi(\delta_m(B_A))) = c \right\}.$$

Note that $\Lambda_{K_h, c}$ is well-defined according to Claim 3.

CLAIM 4. *Let $c \in \mathbb{R}$ and $h \in \{0, \dots, H\}$. Then we have*

$$\Delta_{K_h}(\mathbf{x}_m) = c \Leftrightarrow \exists B_A \in \Lambda_{K_h, c} \text{ such that } \mathbf{f} \in B_A.$$

Proof of Claim 4. Let $c \in \mathbb{R}$ and suppose that there exists $B_A \in \Lambda_{K_h, c}$ such that $\mathbf{f} \in B_A$. Since $\mathbf{x}_m = \phi(\delta_m(\mathbf{f}))$ we have

$$\Delta_{K_h}(\mathbf{x}_m) = \Delta_{K_h}(\phi(\delta_m(\mathbf{f}))).$$

Since $\delta_m(\mathbf{f}) \in \delta_m(B_A)$ we get that $\Delta_{K_h}(\mathbf{x}_m) = c$.

Now assume that $\Delta_{K_h}(\mathbf{x}_m) = c$ which is equivalent to $\Delta_{K_h}(\phi(\delta_m(\mathbf{f}))) = c$. Now there exists $A' \in \mathbb{Z}_q^{d \times (n-1)}$ such that $B_{A'} \in \Lambda_{K_h, c}$ and $\delta_m(\mathbf{f}) \in \delta_m(B_{A'})$ and we get that

$$(f_{m+1}^{(i)}, \dots, f_{n-1}^{(i)}) = (a'_{i, m+1}, \dots, a'_{i, n-1}) \quad \text{for } i \in \{1, \dots, d\}.$$

On the other hand, there exists $A \in \mathbb{Z}_q^{d \times (n-1)}$ with $\mathbf{f} \in B_A$. We obtain that

$$(f_{m+1}^{(i)}, \dots, f_{n-1}^{(i)}) = (a_{i, m+1}, \dots, a_{i, n-1}) \quad \text{for } i \in \{1, \dots, d\}.$$

Altogether we have that

$$(a'_{i, m+1}, \dots, a'_{i, n-1}) = (a_{i, m+1}, \dots, a_{i, n-1}) \quad \text{for } i \in \{1, \dots, d\}.$$

Now it follows by Claim 2 that

$$\Delta_{K_h}(\phi(\delta_m(B_A))) = \Delta_{K_h}(\phi(\delta_m(B_{A'}))) = c.$$

This means that $B_A \in \Lambda_{K_h, c}$ and $\mathbf{f} \in B_A$ and this proves the claim. \square

Now we can prove the independence of $\Delta_{K_h}(\mathbf{x}_n)$ and $\Delta_{K_h}(\mathbf{x}_m)$ for $n, m \in Q(N, \kappa_h, \gamma)$ with $n > m$. For $c \in \mathbb{R}$ and $B_{A'} \in \Lambda_{n-1}$ we have

$$\begin{aligned} \mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c) &= \sum_{B_A \in \Lambda_{n-1}} \mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c \mid \mathbf{f} \in B_A) \mathbb{P}(\mathbf{f} \in B_A) \\ &= \mathbb{P}(\Delta_{K_h}(\mathbf{y}_n) = c \mid \overline{\mathbf{f}} \in B_{A'}) \sum_{B_A \in \Lambda_{n-1}} \mathbb{P}(\mathbf{f} \in B_A) \\ &= \mathbb{P}(\Delta_{K_h}(\mathbf{y}_n) = c \mid \overline{\mathbf{f}} \in B_{A'}), \end{aligned} \quad (8)$$

where we used Claim 1 with $A_1 = A$ and $A_2 = A'$. By Claim 4 and (8) we get for $c_1, c_2 \in \mathbb{R}$ and $A' \in \mathbb{Z}_q^{d \times (n-1)}$ that

$$\begin{aligned} \mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c_2 \mid \Delta_{K_h}(\mathbf{x}_m) = c_1) &= \frac{\mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c_2, \Delta_{K_h}(\mathbf{x}_m) = c_1)}{\mathbb{P}(\Delta_{K_h}(\mathbf{x}_m) = c_1)} \\ &= \frac{\sum_{B_A \in \Lambda_{n-1}} \mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c_2, \Delta_{K_h}(\mathbf{x}_m) = c_1 \mid \mathbf{f} \in B_A) \mathbb{P}(\mathbf{f} \in B_A)}{\mathbb{P}(\Delta_{K_h}(\mathbf{x}_m) = c_1)} \\ &= \sum_{B_A \in \Lambda_{K_h, c_1}} \mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c_2 \mid \mathbf{f} \in B_A) \frac{\mathbb{P}(\mathbf{f} \in B_A)}{\mathbb{P}(\Delta_{K_h}(\mathbf{x}_m) = c_1)} \\ &= \mathbb{P}(\Delta_{K_h}(\mathbf{y}_n) = c_2 \mid \overline{\mathbf{f}} \in B_{A'}) \frac{\sum_{B_A \in \Lambda_{K_h, c_1}} \mathbb{P}(\mathbf{f} \in B_A)}{\mathbb{P}(\Delta_{K_h}(\mathbf{x}_m) = c_1)} \\ &= \mathbb{P}(\Delta_{K_h}(\mathbf{y}_n) = c_2 \mid \overline{\mathbf{f}} \in B_{A'}) \\ &= \mathbb{P}(\Delta_{K_h}(\mathbf{x}_n) = c_2). \end{aligned}$$

This implies the desired result. \square

3.4. Applying Bernstein's inequality and finalizing the proof of Theorem 3

Proof. We may assume that $N \geq d \log_q d$ since otherwise the discrepancy bound is trivial. First of all we set

$$H = \left\lceil \frac{1}{2} \log_q \left(\frac{N}{d \log_q d} \right) \right\rceil \in \mathbb{N}. \quad (9)$$

With this choice we obtain

$$\frac{1}{q^H} \leq \sqrt{\frac{d \log_q d}{N}} \quad \text{and} \quad q^{2H} \leq q^2 \frac{N}{d \log_q d}.$$

Recall the definition of $Q(N, \kappa_h, \gamma) = \{n \in \{1, \dots, N\} : n \equiv \gamma \pmod{2^{\kappa_h}}\}$ and note that $Q(N, \kappa_h, \gamma)$ for $\gamma \in \{0, \dots, 2^{\kappa_h} - 1\}$ are a partition of $\{1, \dots, N\}$

and that

$$|Q(N, \kappa_h, \gamma)| \leq \left\lfloor \frac{N}{2^{\kappa_h}} \right\rfloor + \xi \quad \text{for some } \xi \in \{0, 1\}.$$

With the help of Lemma 8 we are able to apply Bernstein's inequality (Lemma 5). For $h \in \{0, \dots, H\}$ we get that

$$\begin{aligned} \mathbb{P} \left(\left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| > t_h \right) &\leq \sum_{\gamma=0}^{2^{\kappa_h}-1} \mathbb{P} \left(\left| \sum_{n \in Q(N, \kappa_h, \gamma)} \Delta_{K_h}(\mathbf{x}_n) \right| > \frac{t_h}{2^{\kappa_h}} \right) \\ &\leq 2 \sum_{\gamma=0}^{2^{\kappa_h}-1} \exp \left(- \frac{t_h^2 / 2^{2\kappa_h}}{2|Q(N, \kappa_h, \gamma)|\lambda(K_h)(1 - \lambda(K_h)) + 2t_h / (3 \cdot 2^{\kappa_h})} \right) \\ &\leq 2^{\kappa_h+1} \exp \left(- \frac{t_h^2 / 2^{\kappa_h}}{2(1 + 2^{\kappa_h}/N)Nq^{-h} + 2t_h/3} \right). \end{aligned}$$

Since

$$\begin{aligned} \frac{2^{\kappa_h}}{N} &= \frac{h + 2 + \lceil \log_q d \rceil}{N} \leq \frac{1}{N} \left(\frac{1}{2} \log_q \left(\frac{N}{d \log_q d} \right) + 4 + \log_q d \right) \\ &\leq \frac{1}{2} \frac{\log_q N}{N} + 4 + \frac{1}{d} \leq 5, \end{aligned}$$

we obtain

$$\mathbb{P} \left(\left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| > t_h \right) \leq 2^{\kappa_h+1} \exp \left(- \frac{t_h^2 / 2^{\kappa_h}}{12Nq^{-h} + \frac{2}{3}t_h} \right). \quad (10)$$

For the choice of t_h we will distinguish two cases

$$t_h := \begin{cases} C_1 \sqrt{Ndhq^{-h}2^{\kappa_h}} & \text{if } h \in \{1, \dots, H\}, \\ C_2 \sqrt{Nd2^{\kappa_0}} & \text{if } h = 0 \end{cases} \quad (11)$$

for constants $C_1, C_2 > 0$ to be specified later.

Let us consider first the case $h \in \{1, \dots, H\}$. By $\kappa_h = \log_2(h + 2 + \lceil \log_q d \rceil)$ we get that

$$\begin{aligned} 2^{\kappa_h} q^h h &\leq 2^{\kappa_H} q^H H \leq H^2 q^H (4 + \log_q d) \leq 2q^{2H} (4 + \log_q d) \\ &\leq 2q^2 \frac{N}{d} \left(1 + \frac{4}{\log_q d} \right) \leq c(q) \frac{N}{d}, \end{aligned}$$

where $c(q) = 2q^2 \left(1 + \frac{4}{\log_q d} \right)$. Thus we obtain for $h \in \{1, \dots, H\}$,

$$t_h = C_1 \sqrt{Ndhq^{-h}2^{\kappa_h}} \leq C_1 \sqrt{c(q)} q^{-h} N.$$

Furthermore, we get

$$\frac{t_h^2/2^{\kappa_h}}{12q^{-h}N + \frac{2}{3}t_h} \geq \frac{C_1^2 N d h q^{-h}}{12q^{-h}N + \frac{2}{3}C_1 \sqrt{c(q)} q^{-h}N} = \frac{C_1^2 d h}{12 + \frac{2}{3}C_1 \sqrt{c(q)}}. \quad (12)$$

Combining (10) and (12) we get

$$\begin{aligned} \mathbb{P} \left(\left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| > C_1 \sqrt{N h q^{-h} 2^{\kappa_h} d} \right) \\ \leq 2 \exp \left(\kappa_h \log 2 - \frac{C_1^2}{12 + \frac{2}{3}C_1 \sqrt{c(q)}} d h \right). \end{aligned} \quad (13)$$

Consider the case $h = 0$, i.e., $t_0 = C_2 \sqrt{N 2^{\kappa_0} d}$. We have

$$2^{\kappa_0} d \leq (3 + \log_q d) d \leq N c(q).$$

After continuing with the same steps as in the first case we end up with

$$\begin{aligned} \mathbb{P} \left(\left| \sum_{n=1}^N \Delta_{K_0}(\mathbf{x}_n) \right| > C_2 \sqrt{N 2^{\kappa_0} d} \right) \\ \leq 2 \exp \left(\kappa_0 \log 2 - \frac{C_2^2}{12 + \frac{2}{3}C_2 \sqrt{c(q)}} d \right). \end{aligned} \quad (14)$$

Recall that β_h and K_h are dependent on a point $\mathbf{y} \in [0, 1]^d$, respectively. Moreover, we defined

$$S_h = \{K_h(\mathbf{y}) : \mathbf{y} \in [0, 1]^d\} \quad \text{with} \quad |S_h| \leq \frac{1}{2}(2e)^d (q^{h+3} + 1)^d.$$

Additionally we define

$$A_{K_h, N, d} := \left\{ \mathbf{f} \in (\overline{\mathbb{Z}}_q^*((t^{-1})))^d : \left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| > t_h \right\}$$

with t_h defined as in (11) and set

$$C_3 := \frac{C_1^2}{12 + \frac{2}{3}C_1 \sqrt{c(q)}}, \quad \text{and} \quad C_4 := \frac{C_2^2}{12 + \frac{2}{3}C_2 \sqrt{c(q)}}. \quad (15)$$

Then with (13) and (14) we have

$$\begin{aligned}
 & \mathbb{P} \left(\bigcap_{h=0}^H \bigcap_{K_h \in S_h} \left\{ \left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| \leq t_h \right\} \right) = 1 - \mathbb{P} \left(\bigcup_{h=0}^H \bigcup_{K_h \in S_h} A_{K_h, N, d} \right) \\
 & \geq 1 - \sum_{K_0 \in S_0} \mathbb{P}(A_{K_0, N, d}) - \sum_{h=1}^H \sum_{K_h \in S_h} \mathbb{P}(A_{K_h, N, d}) \\
 & \geq 1 - |S_0| 2e^{\kappa_0 \log 2 - C_4 d} - \sum_{h=1}^H |S_h| 2e^{\kappa_h \log 2 - C_3 d h} \\
 & \geq 1 - (2q^3 + 2)^d e^{d(1-C_4) + \kappa_0 \log 2} - \sum_{h=1}^H (2q^{h+3} + 2)^d e^{d(1-C_3 h) + \kappa_h \log 2}. \quad (16)
 \end{aligned}$$

We will now choose $C_1 = C_1(\varepsilon)$ and $C_2 = C_2(\varepsilon)$ such that

$$(2q^3 + 2)^d e^{d(1-C_4) + \kappa_0 \log 2} \leq \frac{\varepsilon}{2} \quad (17)$$

and

$$(2q^{h+3} + 2)^d e^{d(1-C_3 h) + \kappa_h \log 2} \leq \frac{\varepsilon}{2^{h+1}}. \quad (18)$$

From (16), (17) and (18) we then obtain that

$$\mathbb{P} \left(\bigcap_{h=0}^H \bigcap_{K_h \in S_h} \left\{ \left| \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) \right| \leq t_h \right\} \right) \geq 1 - \varepsilon.$$

Inequality (17) is equivalent to

$$C_4 \geq \frac{1}{d} \left(d \log(2q^3 + 2) + d + \log(2 + \lceil \log_q d \rceil) + \log \frac{2}{\varepsilon} \right).$$

This is certainly satisfied for the choice

$$C_4 = \log(2q^3 + 2) + 2 + \log \frac{2}{\varepsilon} = \log \left(\frac{4(q^3 + 1)e^2}{\varepsilon} \right).$$

With (15) it follows that we choose

$$C_2 = C_4 \frac{1}{3} \sqrt{c(q)} + \sqrt{C_4^2 \frac{1}{9} c(q) + 12C_4} \asymp \log \frac{1}{\varepsilon}.$$

Inequality (18) is equivalent to

$$C_3 \geq \frac{1}{dh} \left(d \log(2q^{h+3} + 2) + d + \log(h + 2 + \lceil \log_q d \rceil) + \log 2^h + \log \frac{2}{\varepsilon} \right).$$

This is certainly satisfied for the choice

$$C_3 = \log(2(q^4 + 1)) + 2 + \frac{\log 2}{2} + \log \frac{2}{\varepsilon} = \log \left(\frac{4\sqrt{2}(q^4 + 1)e^2}{\varepsilon} \right).$$

With (15) it follows that we choose

$$C_1 = C_3 \frac{1}{3} \sqrt{c(q)} + \sqrt{C_3^2 \frac{1}{9} c(q) + 12C_3} \asymp \log \frac{1}{\varepsilon}.$$

Finally, by (6), (13), (14) we obtain with probability at least $1 - \varepsilon$

$$\begin{aligned} \sum_{n=1}^N \mathbf{1}_{[\mathbf{0}, \mathbf{y})}(\mathbf{x}_n) &\leq \sum_{n=1}^N \sum_{h=0}^H \Delta_{K_h}(\mathbf{x}_n) + N\lambda([\mathbf{0}, \beta_{H+1})) \\ &\leq \sum_{n=1}^N \Delta_{K_0}(\mathbf{x}_n) + \sum_{h=1}^H \sum_{n=1}^N \Delta_{K_h}(\mathbf{x}_n) + N\lambda([\mathbf{0}, \mathbf{y})) + \\ &\quad N(\lambda([\mathbf{0}, \beta_{H+1})) - \lambda([\mathbf{0}, \mathbf{y}))) \\ &\leq \sqrt{Nd} \left(C_2 \sqrt{2^{\kappa_0}} + \sum_{h=1}^H C_1 \sqrt{2^{\kappa_h}} \sqrt{hq^{-h}} \right) + N(\lambda([\mathbf{0}, \mathbf{y})) + q^{-H}) \\ &\leq \sqrt{Nd} \left(C_2 \sqrt{2^{\kappa_0}} + \sum_{h=1}^{\infty} C_1 \sqrt{2^{\kappa_h}} \sqrt{hq^{-h}} \right) + \sqrt{Nd \log_q d} + N\lambda([\mathbf{0}, \mathbf{y})) \\ &\leq \sqrt{Nd} \left(C_2 \sqrt{2^{\kappa_0}} + \sum_{h=1}^{\infty} C_1 \sqrt{(h+3)hq^{-h}} + \sqrt{\log_q d} \sum_{h=1}^{\infty} C_1 \sqrt{hq^{-h}} \right) \\ &\quad + \sqrt{Nd \log_q d} + N\lambda([\mathbf{0}, \mathbf{y})), \end{aligned} \tag{19}$$

where we used that

$$\lambda([\mathbf{0}, \beta_{H+1})) - \lambda([\mathbf{0}, \mathbf{y})) \leq \lambda(K_H(y)) \leq q^{-H}.$$

By the choices for C_1 and C_2 we obtain that

$$\frac{1}{N} \sum_{n=1}^N \mathbf{1}_{[\mathbf{0}, \mathbf{y})}(\mathbf{x}_n) - \lambda([\mathbf{0}, \mathbf{y})) \leq C_5(q, \varepsilon) \sqrt{\frac{d \log d}{N}}, \tag{20}$$

where $C_5(q, \varepsilon) \asymp \log \frac{1}{\varepsilon}$.

If we use (5) instead of (6) and the fact that

$$\lambda([\mathbf{0}, \mathbf{y})) - \lambda([\mathbf{0}, \beta_H)) \leq \lambda(K_H(y)) \leq q^{-H},$$

we get that

$$\frac{1}{N} \sum_{n=1}^N \mathbf{1}_{[\mathbf{0}, \mathbf{y})}(\mathbf{x}_n) - \lambda([\mathbf{0}, \mathbf{y})) \geq -C_5(q, \varepsilon) \sqrt{\frac{d \log d}{N}} \quad (21)$$

with $C_5(q, \varepsilon)$ as before.

Finally, (20) and (21) imply

$$\left| \frac{1}{N} \sum_{n=1}^N \mathbf{1}_{[\mathbf{0}, \mathbf{y})}(\mathbf{x}_n) - \lambda([\mathbf{0}, \mathbf{y})) \right| \leq C_5(q, \varepsilon) \sqrt{\frac{d \log d}{N}}.$$

Since $\mathbf{y} \in [0, 1]^d$ was arbitrary we get that

$$D_N^*(\mathcal{P}_N(\mathbf{f})) \leq C_5(q, \varepsilon) \sqrt{\frac{d \log d}{N}}$$

holds with probability at least $1 - \varepsilon$. This finishes the proof. \square

3.5. The proof of Corollaries 2 and 4

P r o o f. Since the proofs of the two corollaries are very similar we only present the proof of Corollary 4.

Let $c(q) > 0$ be such that $C(q, \varepsilon)$ from Theorem 3 satisfies

$$C(q, \varepsilon) \leq c(q) \log \varepsilon^{-1}.$$

For $\delta \in (0, 1)$ and $N \geq 2$ let $\varepsilon_N = 6\delta/(\pi N)^2$ and

$$A_N := \left\{ \mathbf{f} \in (\overline{\mathbb{Z}}_q((t^{-1})))^d : D_N^*(\mathcal{P}_N(\mathbf{f})) \leq c(q) \log \varepsilon_N^{-1} \sqrt{\frac{d \log d}{N}} \right\}.$$

According to Theorem 3 we have $\mathbb{P}(A_N) \geq 1 - \varepsilon_N$.

Set

$$A := \left\{ \mathbf{f} \in (\overline{\mathbb{Z}}_q((t^{-1})))^d : D_N^*(\mathcal{P}_N(\mathbf{f})) \leq c(q) \log \varepsilon_N^{-1} \sqrt{\frac{d \log d}{N}} \text{ for all } N \geq 2 \right\}.$$

Then obviously, $A = \bigcap_{N \geq 2} A_N$ and hence

$$\mathbb{P}(A^c) = \mathbb{P} \left(\bigcup_{N \geq 2} A_N^c \right) \leq \sum_{N \geq 2} \mathbb{P}(A_N^c) \leq \sum_{N \geq 2} \varepsilon_N \leq \delta,$$

where A^c is the complement of A in $(\overline{\mathbb{Z}}_q((t^{-1})))^d$ and similarly for A_N^c . Hence $\mathbb{P}(A) \geq 1 - \delta$ and the result follows. \square

REFERENCES

- [1] AISTLEITNER, CH.: *Covering numbers, dyadic chaining and discrepancy*, J. Complexity **27** (2011), 531–540.
- [2] ———: *On the inverse of the discrepancy for infinite dimensional infinite sequences*, J. Complexity **29** (2013), 182–194.
- [3] BECK, J.: *Probabilistic diophantine approximation, I. Kronecker-sequences*, Ann. Math. **140** (1994), 451–502.
- [4] BERNSTEIN, S. N.: *The Theory of Probabilities*. Gastehizdat Publishing House, Moscow, 1946.
- [5] BILYK, D.—LACEY, M. T.—VAGHARSHAKYAN, A.: *On the small ball inequality in all dimensions*, J. Funct. Anal. **254** (2008), 2470–2502.
- [6] BOREL, É.: *Les probabilités denombrables et leurs applications arithmétiques*, Rend. Circ. Mat. Palermo **27** (1909), 247–271.
- [7] DICK, J.: *A note on the existence of sequences with small star discrepancy*, J. Complexity **23** (2007), 649–652.
- [8] DICK, J.—KUO, F. Y.—SLOAN, I. H.: *High-dimensional integration: the quasi-Monte Carlo way*, Acta Numer. **22** (2013), 133–288.
- [9] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.
- [10] DOERR, B.—GNEWUCH, M.—SRIVASTAV, A.: *Bounds and constructions for the star-discrepancy via δ -covers*, J. Complexity **21** (2005), 691–709.
- [11] DRMOTA, M.—TICHY, R. F.: *Sequences, Discrepancies and Applications*. In: Lecture Notes in Math. Vol. 1651, Springer-Verlag, Berlin, 1997.
- [12] GNEWUCH, M.: *Bracketing numbers for axis-parallel boxes and applications to geometric discrepancy*, J. Complexity **24** (2008), 154–172.
- [13] ———: Gnewuch, M. *Entropy, randomization, derandomization, and discrepancy*. In: Monte Carlo and Quasi-Monte Carlo Methods 2010. Springer Proc. Math. Stat. Vol. 23, Springer-Verlag, Heidelberg, 2012, pp. 43–78.
- [14] HEINRICH, S.—NOVAK, E.—WASILKOWSKI, G. W.—WOŹNIAKOWSKI, H.: *The inverse of the star discrepancy depends linearly on the dimension*, Acta Arith. **96** (2001), 279–302.
- [15] HINRICHS, A.: *Covering numbers, Vapnik-Červonenkis classes and bounds on the star-discrepancy*, J. Complexity **20** (2004), 477–483.
- [16] KUIPERS, L.—NIEDERREITER, H.: *Uniform Distribution of Sequences*. John Wiley, New York (1974). Reprint, Dover Publications, Mineola, NY, 2006.
- [17] LARCHER, G.: *On the distribution of an analog to classical Kronecker-sequences*, J. Number Theory **52** (1995), 198–215.
- [18] LARCHER, G.—NIEDERREITER, H.: *Kronecker-type sequences and nonarchimedean diophantine approximation*, Acta Arith. **63** (1993), 380–396.
- [19] LARCHER, G.—PILLICHSHAMMER, F.: *Metrical lower bounds on the discrepancy of digital Kronecker-sequences*, J. Number Th. **135** (2014), 262–283.
- [20] LEOBACHER, G.—PILLICHSHAMMER, F.: *Introduction to Quasi-Monte Carlo Integration and Applications*. In: Compact Textbooks in Mathematics, Birkhäuser, 2014.
- [21] LÖBBE, TH.: *Probabilistic star discrepancy bounds for lacunary point sets* (2014), see arXiv:1408.2220.

- [22] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*. In: CBMS-NSF Series in Applied Mathematics Vol. 63, SIAM, Philadelphia, 1992.
- [23] NOVAK, E.—WOŹNIAKOWSKI, H.: *Tractability of Multivariate Problems, Volume I: Linear Information*. EMS, Zürich, 2008.
- [24] ——— *Tractability of Multivariate Problems, Volume II: Standard Information for Functionals*. EMS, Zürich, 2010.

Received September 28, 2016

Accepted November 9, 2017

Mario Neumüller

Friedrich Pillichshammer

*Department of Financial Mathematics
and Applied Number Theory*

Johannes Kepler University Linz

Altenbergerstr. 69

4040 Linz

AUSTRIA

E-mail: mario.neumueller@jku.at

friedrich.pillichshammer@jku.at