

COMPONENT-BY-COMPONENT CONSTRUCTION OF SHIFTED HALTON SEQUENCES

PETER KRITZER—FRIEDRICH PILLICHSHAMMER

Dedicated to Professor Harald Niederreiter on the occasion of his 70th birthday

ABSTRACT. We study quasi-Monte Carlo integration in a weighted anchored Sobolev space. As the underlying integration nodes we consider Halton sequences in prime bases $\mathbf{p} = (p_1, \dots, p_s)$ which are shifted with a \mathbf{p} -adic shift based on \mathbf{p} -adic arithmetic. The error is studied in the worst-case setting. In a recent paper, Hellekalek together with the authors of this article proved optimal error bounds in the root mean square sense, where the mean was extended over the uncountable set of all possible \mathbf{p} -adic shifts. Here we show that candidates for good shifts can in fact be chosen from a finite set and can be found by a component-by-component algorithm.

Communicated by Arne Winterhof

1. Introduction

We study the problem of approximating the value of the integral $I_s(f) := \int_{[0,1]^s} f(\mathbf{x}) \, d\mathbf{x}$ of functions f belonging to a reproducing kernel Hilbert space $\mathcal{H}(K)$ of functions $f : [0, 1]^s \rightarrow \mathbb{R}$. One way of numerically approximating $I_s(f)$ is to employ a quasi-Monte Carlo (QMC) rule,

$$Q_{N,s}(f) := \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n),$$

where $P_{N,s} = \{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}\}$ is a set of N deterministically chosen points in $[0, 1]^s$. It is well known (see, e. g., [3, 4, 10, 12, 15]) that point sets which are

2010 Mathematics Subject Classification: 65D30, 65C05, 11K38, 11K45.

Keywords: Quasi-Monte Carlo integration, shifted Halton sequences, worst-case error.

The authors are supported by the Austrian Science Fund (FWF): Projects F5506-N26 (Kritzer) and F5509-N26 (Pillichshammer), respectively, which are part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

in some way evenly distributed in the unit cube yield a low integration error when applying the corresponding QMC rules for approximating $I_s(f)$.

We study the error of QMC rules in the worst-case setting. The worst-case error of an algorithm $Q_{N,s}$ based on nodes $P_{N,s}$ is defined as the worst integration error over the unit ball of $\mathcal{H}(K)$, i. e.,

$$e_{N,s}(P_{N,s}, K) = \sup_{\substack{f \in \mathcal{H}(K) \\ \|f\|_K \leq 1}} |I_s(f) - Q_{N,s}(f)|.$$

An essential question in the theory of QMC methods is how the sample nodes $P_{N,s}$ of a QMC rule $Q_{N,s}$ should be chosen.

Shifted Halton sequences. In this paper we focus on a special kind of point sequences underlying a QMC rule, namely Halton sequences (cf. [5]) whose definition is based on the radical inverse function. Let $p \geq 2$ be an integer, $\mathbb{N} = \{1, 2, 3, \dots\}$, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $n \in \mathbb{N}_0$, let $n = n_0 + n_1p + n_2p^2 + \dots$ be the base p expansion of n (which is of course finite) with digits $n_i \in \{0, 1, \dots, p-1\}$ for $i \geq 0$. The radical inverse function $\phi_p : \mathbb{N}_0 \rightarrow [0, 1)$ in base p is defined by

$$\phi_p(n) := \sum_{r=0}^{\infty} \frac{n_r}{p^{r+1}}.$$

Halton sequences can be defined for any dimension $s \in \mathbb{N}$. Let $p_1, \dots, p_s \geq 2$ be s integers, and let $\mathbf{p} = (p_1, \dots, p_s)$. Then the s -dimensional Halton sequence $H_{\mathbf{p}}$ in bases p_1, \dots, p_s is defined to be the sequence $H_{\mathbf{p}} = (\mathbf{x}_n)_{n \geq 0} \subseteq [0, 1)^s$, where

$$\mathbf{x}_n = (\phi_{p_1}(n), \phi_{p_2}(n), \dots, \phi_{p_s}(n)), \quad \text{for } n \in \mathbb{N}_0.$$

It is well known (see, e.g., [3, 12]) that Halton sequences have good distribution properties if and only if the bases p_1, \dots, p_s are mutually relatively prime, and for the sake of simplicity we assume throughout the rest of the paper that $\mathbf{p} = (p_1, \dots, p_s)$ consists of s mutually different prime numbers.

We also introduce a method of randomizing the elements of the Halton sequence which is referred to as a \mathbf{p} -adic shift. This special case of randomization is based on arithmetic over the p -adic numbers and is perfectly suited for Halton sequences $H_{\mathbf{p}}$.

Let p be a prime number. We define the set of p -adic numbers as the set of formal sums

$$\mathbb{Z}_p = \left\{ z = \sum_{r=0}^{\infty} z_r p^r : z_r \in \{0, 1, \dots, p-1\} \text{ for all } r \in \mathbb{N}_0 \right\}.$$

Clearly $\mathbb{N}_0 \subseteq \mathbb{Z}_p$. For two nonnegative integers $y, z \in \mathbb{N}_0 \subseteq \mathbb{Z}_p$, the sum $y+z \in \mathbb{Z}_p$ is defined as the usual sum of integers. The addition can be extended to all p -adic numbers. The set \mathbb{Z}_p with this addition, which we denote by $+\mathbb{Z}_p$, then forms an abelian group.

As an extension of the radical inverse function defined above, we define the so-called Monna map

$$\phi_p : \mathbb{Z}_p \rightarrow [0, 1) \text{ by } \phi_p(z) := \sum_{r=0}^{\infty} \frac{z_r}{p^{r+1}} \pmod{1}$$

whose restriction to \mathbb{N}_0 is exactly the radical inverse function in base p . In order to keep the used notation at a minimum we denote both, the Monna map and the radical inverse function, by ϕ_p . We also define the inverse

$$\phi_p^+ : [0, 1) \rightarrow \mathbb{Z}_p \text{ by } \phi_p^+ \left(\sum_{r=0}^{\infty} \frac{x_r}{p^{r+1}} \right) := \sum_{r=0}^{\infty} x_r p^r,$$

where we always use the finite p -adic representation for p -adic rationals in $[0, 1)$. By a p -adic rational, we understand a number in $[0, 1)$ that can be represented by a finite p -adic expansion.

For a prime number p and for $x \in [0, 1)$ we consider the following p -adic shifts:

- **p -adic shift:** for $\sigma \in [0, 1)$, we define $x \oplus_p \sigma \in [0, 1)$ to be

$$x \oplus_p \sigma = \phi_p(\phi_p^+(x) +_{\mathbb{Z}_p} \phi_p^+(\sigma)).$$

- **simplified p -adic shift:** for $m \in \mathbb{N}$ and $\sigma \in [0, 1)$, we write $x \oplus_{p,m}^{\text{smp}} \sigma$ to be the truncation of $x \oplus_p \sigma$ to the m most significant digits, i.e., if $\phi_p^+(x) +_{\mathbb{Z}_p} \phi_p^+(\sigma) = \sum_{r=0}^{\infty} y_r p^r \in \mathbb{Z}_p$, then

$$x \oplus_{p,m}^{\text{smp}} \sigma = \phi_p \left(\sum_{r=0}^{m-1} y_r p^r \right).$$

- **mid-simplified p -adic shift:** for $m \in \mathbb{N}$ and $\sigma \in [0, 1)$, we write

$$x \oplus_{p,m}^{\text{mid}} \sigma = (x \oplus_{p,m}^{\text{smp}} \sigma) + \frac{1}{2p^m}.$$

If the choice of m is clear from the context, we may often omit m in the notation $\oplus_{p,m}^{\text{smp}}$ and $\oplus_{p,m}^{\text{mid}}$ and write \oplus_p^{smp} and \oplus_p^{mid} instead.

In the s -variate case, for given bases $\mathbf{p} = (p_1, \dots, p_s)$, a given point $\mathbf{x} = (x_1, \dots, x_s) \in [0, 1)^s$, and given $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_s) \in [0, 1)^s$ and $\mathbf{m} = (m_1, \dots, m_s) \in \mathbb{N}^s$, the above shifts are defined component-wise and we write $\mathbf{x} \oplus_{\mathbf{p}} \boldsymbol{\sigma} \in [0, 1)^s$, $\mathbf{x} \oplus_{\mathbf{p}, \mathbf{m}}^{\text{smp}} \boldsymbol{\sigma}$ and $\mathbf{x} \oplus_{\mathbf{p}, \mathbf{m}}^{\text{mid}} \boldsymbol{\sigma}$, respectively.

For a point set $Y = \{\mathbf{y}_n : n = 0, \dots, N-1\}$ we write

$Y \oplus \boldsymbol{\sigma} := \{\mathbf{y}_n \oplus \boldsymbol{\sigma} : n = 0, \dots, N-1\}$ where \oplus is either $\oplus_{\mathbf{p}}$, $\oplus_{\mathbf{p}, \mathbf{m}}^{\text{smp}}$, or $\oplus_{\mathbf{p}, \mathbf{m}}^{\text{mid}}$.

A weighted Sobolev space. In this paper, we are going to consider the problem of numerical integration of functions f that belong to a weighted anchored Sobolev space. Before we give the definition we introduce some notation which we require for the following: assume that $\gamma = (\gamma_j)_{j=1}^\infty$ is a non-increasing sequence of positive weights, where $1 \geq \gamma_1 \geq \gamma_2 \geq \dots$. These weights are used in order to model the influence of the different variables of the integrands, an idea which was introduced by Sloan and Woźniakowski [17]. For $s \in \mathbb{N}$ let $[s] := \{1, \dots, s\}$. For $\mathbf{u} \subseteq [s]$, $\mathbf{x}_\mathbf{u}$ denotes the projection of $\mathbf{x} \in [0, 1]^s$ onto $[0, 1]^{|\mathbf{u}|}$ consisting of the components whose indices are contained in \mathbf{u} . Furthermore we write $(\mathbf{x}_\mathbf{u}, \mathbf{1}) \in [0, 1]^s$ for the point where those components of \mathbf{x} whose indices are not in \mathbf{u} are replaced by 1.

We consider a weighted anchored Sobolev space $\mathcal{H}(K_{s,\gamma})$ with anchor $\mathbf{1} = (1, 1, \dots, 1)$ consisting of functions on $[0, 1]^s$ whose first mixed partial derivatives are square integrable. This space is a reproducing kernel Hilbert space with kernel function

$$K_{s,\gamma}(\mathbf{x}, \mathbf{y}) = \prod_{j=1}^s (1 + \gamma_j \min(1 - x_j, 1 - y_j)) \quad \text{for } \mathbf{x}, \mathbf{y} \in [0, 1]^s, \quad (1)$$

where $\mathbf{x} = (x_1, x_2, \dots, x_s)$ and $\mathbf{y} = (y_1, y_2, \dots, y_s)$. The inner product is given by

$$\langle f, g \rangle_{K_{s,\gamma}} = \sum_{\mathbf{u} \subseteq [s]} \gamma_\mathbf{u}^{-1} \int_{[0,1]^{|\mathbf{u}|}} \frac{\partial^{|\mathbf{u}|}}{\partial \mathbf{x}_\mathbf{u}} f(\mathbf{x}_\mathbf{u}, \mathbf{1}) \frac{\partial^{|\mathbf{u}|}}{\partial \mathbf{x}_\mathbf{u}} g(\mathbf{x}_\mathbf{u}, \mathbf{1}) d\mathbf{x}_\mathbf{u}.$$

Here $\gamma_\mathbf{u} = \prod_{j \in \mathbf{u}} \gamma_j$; in particular $\gamma_\emptyset = 1$. Furthermore, we denote by $\frac{\partial^{|\mathbf{u}|}}{\partial \mathbf{x}_\mathbf{u}} h$ the derivative of a function h with respect to the x_j with $j \in \mathbf{u}$. The norm in $\mathcal{H}(K_{s,\gamma})$ is given by $\|f\|_{K_{s,\gamma}} = \sqrt{\langle f, f \rangle_{K_{s,\gamma}}}$. The Sobolev space $\mathcal{H}(K_{s,\gamma})$ has been studied frequently in the literature (see, among many references, e. g., [1, 2, 7, 9, 11, 13, 17, 18]).

It is well known that the squared worst-case integration error in a reproducing kernel Hilbert space can be expressed in terms of the kernel function. In the particular case of the kernel $K_{s,\gamma}$, it is easily derived with the help of [3, Proposition 2.11] that for $P_{N,s} = \{\mathbf{x}_0, \dots, \mathbf{x}_{N-1}\}$ in $[0, 1]^s$, where $\mathbf{x}_n = (x_{n,1}, \dots, x_{n,s})$ for $n = 0, 1, \dots, N-1$, we have

$$\begin{aligned} e_{N,s}^2(P_{N,s}, K_{s,\gamma}) &= \prod_{i=1}^s \left(1 + \frac{\gamma_i}{3}\right) - \frac{2}{N} \sum_{n=0}^{N-1} \prod_{i=1}^s \left(1 + \frac{\gamma_i}{2}(1 - x_{n,i}^2)\right) \\ &\quad + \frac{1}{N^2} \sum_{n,h=0}^{N-1} \prod_{i=1}^s (1 + \gamma_i \min(1 - x_{n,i}, 1 - x_{h,i})). \quad (2) \end{aligned}$$

Hence the worst-case error can be computed at a cost of $O(sN^2)$ arithmetic operations.

In [7] the authors studied the root mean square worst-case error in $\mathcal{H}(K_{s,\gamma})$ of the \mathbf{p} -adically shifted Halton sequence extended over all \mathbf{p} -adic shifts, i.e.,

$$\widehat{e}_{N,s}(H_{\mathbf{p}}, K_{s,\gamma}) := \sqrt{\mathbb{E}_{\sigma}[e_{N,s}^2(H_{\mathbf{p}} \oplus_{\mathbf{p}} \sigma, K_{s,\gamma})]}.$$

We remark that there are some relations of $\widehat{e}_{N,s}$ to other figures of merit like the weighted L_2 -discrepancy or the worst-case error in a certain reproducing kernel Hilbert space which is based on the so-called \mathbf{p} -adic function system (see [7] for more information). The latter one is a generalization of the \mathbf{p} -adic diaphony which was introduced by Hellekalek [6] (see also [14]).

The following result is the main result of [7].

THEOREM 1 ([7, Theorem 1]). *Let $N \geq 2$. We have*

$$\begin{aligned} & [\widehat{e}_{N,s}(H_{\mathbf{p}}, K_{s,\gamma})]^2 \\ & \leq \frac{1}{N^2} \left[\prod_{j=1}^s \left(1 + \gamma_j (\log N) \frac{p_j^2}{\log p_j} \right) + \prod_{j=1}^s \left(1 + \frac{\gamma_j}{2} \right) \prod_{j=1}^s \left(1 + \frac{\gamma_j p_j}{6} \right) \right]. \end{aligned} \quad (3)$$

In particular, if $\sum_{j=1}^{\infty} \gamma_j \frac{p_j^2}{\log p_j} < \infty$, then for any $\delta > 0$ we have

$$\widehat{e}_{N,s}(H_{\mathbf{p}}, K_{s,\gamma}) \ll_{\delta,\gamma,\mathbf{p}} \frac{1}{N^{1-\delta}},$$

where the implied constant is independent of the dimension s .

The bound (3) is, up to log-factors, optimal. For a further discussion of the result, especially with respect to the dependence on the dimension s we refer to [7]. Theorem 1 can also be interpreted in the “deterministic” sense that for every fixed $N \geq 2$ there exists a \mathbf{p} -adic shift $\sigma \in [0, 1]^s$ such that the squared worst-case error of the initial N elements of the corresponding \mathbf{p} -adically shifted Halton sequence satisfies the bound (3). The problem with this interpretation is that the \mathbf{p} -adic shift has to be chosen from an uncountable set, namely the s -dimensional unit cube. This is a big drawback if one wants to effectively find good \mathbf{p} -adic shifts.

It is the aim of this short paper to show that it suffices to choose the \mathbf{p} -adic shifts, which yield an upper bound of the form (3), from a finite set. This set of possible candidates has size N^s which is of course huge already for moderately large s or N . However we also show that in principle good shifts can be found by a component-by-component (CBC) algorithm. This idea is borrowed from the construction of good lattice point sets which goes back to Korobov [8] and

to Sloan and Reztsov [16], and which is nowadays used in a multitude of papers. With this “adaptive search” the search space is only of a size of order $O(sN)$.

The rest of the paper is structured as follows: In Section 2 we prove some auxiliary results. The CBC construction of p -adic shifts as well as the statement and proof of the main results of this paper are presented in Section 3.

2. Auxiliary results

We use the following notation: for $p \in \mathbb{N}$ and $m \in \mathbb{N}_0$ let

$$\mathbb{Q}(p^m) := \{ap^{-m} : a = 0, 1, \dots, p^m - 1\}.$$

We now show the following lemma.

LEMMA 1. *Let $H_{p,N}$ be the point set consisting of the first N elements of H_p and let $m \in \mathbb{N}$ be minimal such that $N < p^m$. Furthermore, let $\sigma_m \in \mathbb{Q}(p^m)$. Then it is true that*

$$e_{N,1}^2(H_{p,N} \oplus_p^{\text{mid}} \sigma_m, K_{1,\gamma_1}) \leq p^m \int_0^{p^{-m}} e_{N,1}^2(H_{p,N} \oplus_p(\sigma_m + \delta), K_{1,\gamma_1}) d\delta.$$

Proof. Let $H_{p,N} = \{h_0, h_1, \dots, h_{N-1}\}$. From (2) we obtain

$$\begin{aligned} & p^m \int_0^{p^{-m}} e_{N,1}^2(H_{p,N} \oplus_p(\sigma_m + \delta), K_{1,\gamma_1}) d\delta \\ &= \left(1 + \frac{\gamma_1}{3}\right) - \frac{2}{N} \sum_{n=0}^{N-1} p^m \int_0^{p^{-m}} \left(1 + \frac{\gamma_1}{2} \left(1 - (h_n \oplus_p(\sigma_m + \delta))^2\right)\right) d\delta \\ &+ \frac{1}{N^2} \sum_{n=0}^{N-1} p^m \int_0^{p^{-m}} \left(1 + \gamma_1 \left(1 - (h_n \oplus_p(\sigma_m + \delta))\right)\right) d\delta \\ &+ \frac{1}{N^2} \sum_{\substack{n,k=0 \\ n \neq k}}^{N-1} p^m \int_0^{p^{-m}} \left(1 + \gamma_1 \min\{1 - (h_n \oplus_p(\sigma_m + \delta)), \right. \\ &\qquad \qquad \qquad \left. 1 - (h_k \oplus_p(\sigma_m + \delta))\}\right) d\delta. \end{aligned}$$

For given $n \in \{0, 1, \dots, N-1\}$, let us now analyze the quantity

$$h_n \oplus_p(\sigma_m + \delta) = \phi_p(\phi_p^+(h_n) +_{\mathbb{Z}_p} \phi_p^+(\sigma_m + \delta)).$$

The base p expansion of h_n is of the form $h_n = \sum_{r=1}^m \frac{h_n^{(r)}}{p^r}$, since $N < p^m$. Furthermore, the base p expansions of σ_m and δ , respectively, are of the form

$$\sigma_m = \sum_{r=0}^{m-1} \frac{\sigma^{(r)}}{p^{r+1}} \quad \text{and} \quad \delta = \sum_{r=m}^{\infty} \frac{\delta^{(r)}}{p^{r+1}},$$

due to the assumptions on σ_m and δ . Consequently,

$$\phi_p^+(h_n) = \sum_{r=0}^{m-1} h_n^{(r)} p^r$$

and

$$\phi_p^+(\sigma_m + \delta) = \phi_p^+(\sigma_m) +_{\mathbb{Z}_p} \phi_p^+(\delta) = \sum_{r=0}^{m-1} \sigma^{(r)} p^r +_{\mathbb{Z}_p} \sum_{r=m}^{\infty} \delta^{(r)} p^r.$$

Let

$$\phi_p^+(h_n) +_{\mathbb{Z}_p} \phi_p^+(\sigma_m) = \sum_{r=0}^m y_r p^r$$

with $y_r \in \{0, 1, \dots, p-1\}$. Then we obtain

$$\phi_p^+(h_n) +_{\mathbb{Z}_p} \phi_p^+(\sigma_m + \delta) = \sum_{r=0}^{m-1} y_r p^r +_{\mathbb{Z}_p} y_m p^m +_{\mathbb{Z}_p} \phi_p^+(\delta).$$

Note that $\sum_{r=0}^{m-1} y_r p^r$ is the truncation of the p -adic sum $\phi_p^+(h_n) +_{\mathbb{Z}_p} \phi_p^+(\sigma_m)$ to the first m digits. Hence

$$\phi_p \left(\sum_{r=0}^{m-1} y_r p^r \right) = h_n \oplus_p^{\text{smp}} \sigma_m.$$

For short we write

$$\xi(h_n, \sigma_m) := \phi_p(y_{m+1} p^m).$$

Note that $\phi_p^+(\xi(h_n, \sigma_m)) = y_{m+1} p^m$. Hence we can write

$$h_n \oplus_p (\sigma_m + \delta) = \phi_p(\phi_p^+(h_n) +_{\mathbb{Z}_p} \phi_p^+(\sigma_m + \delta)) = (h_n \oplus_p^{\text{smp}} \sigma_m) + (\xi(h_n, \sigma_m) \oplus_p \delta).$$

From this we obtain

$$\begin{aligned} & p^m \int_0^{p^{-m}} 1 + \frac{\gamma_1}{2} \left(1 - (h_n \oplus_p (\sigma_m + \delta))^2 \right) d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \frac{\gamma_1}{2} \left(1 - \left((h_n \oplus_p^{\text{smp}} \sigma_m) + (\xi(h_n, \sigma_m) \oplus_p \delta) \right)^2 \right) d\delta. \end{aligned}$$

We now use [7, Lemma 3], which states that for any $f \in L_2([0, 1])$ and any $y \in [0, 1)$, we have

$$\int_0^1 f(x) \, dx = \int_0^1 f(x \oplus_p y) \, dx. \quad (4)$$

This yields

$$\begin{aligned} & p^m \int_0^{p^{-m}} 1 + \frac{\gamma_1}{2} \left(1 - (h_n \oplus_p (\sigma_m + \delta))^2\right) \, d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \frac{\gamma_1}{2} \left(1 - ((h_n \oplus_p^{\text{smp}} \sigma_m) + \delta)^2\right) \, d\delta \\ &= 1 + \frac{\gamma_1}{2} (1 - (h_n \oplus_p^{\text{smp}} \sigma_m)^2) - \frac{1}{p^m} \frac{\gamma_1}{2} (h_n \oplus_p^{\text{smp}} \sigma_m) - \frac{1}{p^{2m}} \frac{\gamma_1}{6}. \end{aligned}$$

Furthermore, in a similar fashion,

$$\begin{aligned} & p^m \int_0^{p^{-m}} 1 + \gamma_1 \left(1 - (h_n \oplus_p (\sigma_m + \delta))\right) \, d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \gamma_1 \left(1 - ((h_n \oplus_p^{\text{smp}} \sigma_m) + (\xi(h_n, \sigma_m) \oplus_p \delta))\right) \, d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \gamma_1 \left(1 - ((h_n \oplus_p^{\text{smp}} \sigma_m) + \delta)\right) \, d\delta \\ &= -\frac{\gamma_1}{2} \frac{1}{p^m} + 1 + \gamma_1 - \gamma_1 (h_n \oplus_p^{\text{smp}} \sigma_m). \end{aligned}$$

Finally, let us deal with the expression

$$p^m \int_0^{p^{-m}} 1 + \gamma_1 \min \{1 - (h_n \oplus_p (\sigma_m + \delta)), 1 - (h_k \oplus_p (\sigma_m + \delta))\} \, d\delta \quad (5)$$

with $k \neq n$. Note that, as $k \neq n$, we cannot have $h_n \oplus_p (\sigma_m + \delta) = h_k \oplus_p (\sigma_m + \delta)$. Suppose that

$$h_n \oplus_p (\sigma_m + \delta) < h_k \oplus_p (\sigma_m + \delta). \quad (6)$$

Using the notation introduced above, we can rewrite (6) as

$$(h_n \oplus_p^{\text{smp}} \sigma_m) + (\xi(h_n, \sigma_m) \oplus_p \delta) < (h_k \oplus_p^{\text{smp}} \sigma_m) + (\xi(h_k, \sigma_m) \oplus_p \delta).$$

Again, since $k \neq n$, we cannot have

$$(h_n \oplus_p^{\text{smp}} \sigma_m) = (h_k \oplus_p^{\text{smp}} \sigma_m),$$

as this would also imply $\xi(h_n, \sigma_m) = \xi(h_k, \sigma_m)$, and so would yield a contradiction to (6). Furthermore, it cannot be the case that

$$(h_n \oplus_p^{\text{smp}} \sigma_m) > (h_k \oplus_p^{\text{smp}} \sigma_m),$$

since $\xi(h_n, \sigma_m), \xi(h_k, \sigma_m) \in [0, p^{-m})$, and so we would also end up with a contradiction to (6). Therefore, we see that (6) automatically implies

$$(h_n \oplus_p^{\text{smp}} \sigma_m) < (h_k \oplus_p^{\text{smp}} \sigma_m). \quad (7)$$

Suppose now, on the other hand, that (7) holds. Then, since $\xi(h_n, \sigma_m)$ and $\xi(h_k, \sigma_m)$ are in $[0, p^{-m})$, also (6) must hold. We have thus shown that (6) and (7) are equivalent.

Suppose now in the analysis of (5) that (6) holds, i. e.,

$$\begin{aligned} & p^m \int_0^{p^{-m}} 1 + \gamma_1 \min \left\{ 1 - (h_n \oplus_p (\sigma_m + \delta)), 1 - (h_k \oplus_p (\sigma_m + \delta)) \right\} d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \gamma_1 (1 - (h_k \oplus_p (\sigma_m + \delta))) d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \gamma_1 \left(1 - \left((h_k \oplus_p^{\text{smp}} \sigma_m) + (\xi(h_k, \sigma_m) \oplus_p \delta) \right) \right) d\delta. \end{aligned}$$

Using the equivalence between (6) and (7), and again (4), we see that the latter expression equals

$$\begin{aligned} & p^m \int_0^{p^{-m}} \left(1 + \gamma_1 \left(\min \{ 1 - (h_n \oplus_p^{\text{smp}} \sigma_m), 1 - (h_k \oplus_p^{\text{smp}} \sigma_m) \} - (\xi(h_k, \sigma_m) \oplus_p \delta) \right) \right) d\delta \\ &= p^m \int_0^{p^{-m}} 1 + \gamma_1 \left(\min \{ 1 - (h_n \oplus_p^{\text{smp}} \sigma_m), 1 - (h_k \oplus_p^{\text{smp}} \sigma_m) \} - \delta \right) d\delta \\ &= -\frac{\gamma_1}{2} \frac{1}{p^m} + 1 + \gamma_1 \min \{ 1 - (h_n \oplus_p^{\text{smp}} \sigma_m), 1 - (h_k \oplus_p^{\text{smp}} \sigma_m) \}. \end{aligned}$$

A similar argument holds if the converse of (6) holds.

Putting all of these observations together, we obtain

$$\begin{aligned} & p^m \int_0^{p^{-m}} e_{N,1}^2(H_{p,N} \oplus_p (\sigma_m + \delta), K_{1,\gamma_1}) d\delta = \left(1 + \frac{\gamma_1}{3} \right) \\ & - \frac{2}{N} \sum_{n=0}^{N-1} \left(1 + \frac{\gamma_1}{2} (1 - (h_n \oplus_p^{\text{smp}} \sigma_m)^2) - \frac{\gamma_1}{2} \frac{1}{p^m} (h_n \oplus_p^{\text{smp}} \sigma_m) - \frac{1}{p^{2m}} \frac{\gamma_1}{6} \right) \\ & + \frac{1}{N^2} \sum_{n=0}^{N-1} \left(-\frac{\gamma_1}{2} \frac{1}{p^m} + 1 + \gamma_1 - \gamma_1 (h_n \oplus_p^{\text{smp}} \sigma_m) \right) \\ & + \frac{1}{N^2} \sum_{\substack{n,k=0 \\ n \neq k}}^{N-1} \left(-\frac{\gamma_1}{2} \frac{1}{p^m} + 1 + \gamma_1 \min \{ 1 - (h_n \oplus_p^{\text{smp}} \sigma_m), 1 - (h_k \oplus_p^{\text{smp}} \sigma_m) \} \right) \end{aligned}$$

$$\begin{aligned}
 &\geq \left(1 + \frac{\gamma_1}{3}\right) \\
 &\quad - \frac{2}{N} \sum_{n=0}^{N-1} \left(1 + \frac{\gamma_1}{2} \left(1 - (h_n \oplus_p^{\text{smp}} \sigma_m)^2\right) - \frac{\gamma_1}{2} \frac{1}{2p^m} 2(h_n \oplus_p^{\text{smp}} \sigma_m) - \frac{\gamma_1}{2} \frac{1}{4p^{2m}}\right) \\
 &\quad + \frac{1}{N^2} \sum_{n=0}^{N-1} \left(1 + \gamma_1 \left(1 - \left(h_n \oplus_p^{\text{smp}} \sigma_m + \frac{1}{2p^m}\right)\right)\right) \\
 &\quad + \frac{1}{N^2} \sum_{\substack{n,k=0 \\ n \neq k}}^{N-1} \left(1 + \gamma_1 \min \left\{1 - \left(h_n \oplus_p^{\text{smp}} \sigma_m + \frac{1}{2p^m}\right), \right. \right. \\
 &\quad \quad \quad \left. \left. 1 - \left(h_k \oplus_p^{\text{smp}} \sigma_m + \frac{1}{2p^m}\right)\right\}\right) \\
 &= \left(1 + \frac{\gamma_1}{3}\right) - \frac{2}{N} \sum_{n=0}^{N-1} \left(1 + \frac{\gamma_1}{2} \left(1 - (h_n \oplus_p^{\text{mid}} \sigma_m)^2\right)\right) \\
 &\quad + \frac{1}{N^2} \sum_{n,k=0}^{N-1} \left(1 + \gamma_1 \min \left\{1 - (h_n \oplus_p^{\text{mid}} \sigma_m), 1 - (h_k \oplus_p^{\text{mid}} \sigma_m)\right\}\right) \\
 &= e_{N,1}^2(H_{p,N} \oplus_p^{\text{mid}} \sigma_m, K_{1,\gamma_1}).
 \end{aligned}$$

The result follows. \square

For two point sets

$$X = \{\mathbf{x}_0, \dots, \mathbf{x}_{N-1}\} \text{ in } [0, 1]^{s_1} \quad \text{and} \quad Y = \{\mathbf{y}_0, \dots, \mathbf{y}_{N-1}\} \text{ in } [0, 1]^{s_2}$$

we write (X, Y) to denote the point set consisting of the concatenated points

$$(\mathbf{x}_k, \mathbf{y}_k) = (x_{k,1}, \dots, x_{k,s_1}, y_{k,1}, \dots, y_{k,s_2}) \in [0, 1]^{s_1+s_2} \quad \text{for } k = 0, 1, \dots, N-1.$$

Using this notation, we have the following result.

LEMMA 2. *Let $P_{s,N}$ be a point set of N points in $[0, 1]^s$. Let $H_{p,N}$ be as in Lemma 1 and let $m \in \mathbb{N}$ be minimal such that $N < p^m$. Furthermore, let $\sigma_m \in \mathbb{Q}(p^m)$. Then it is true that*

$$\begin{aligned}
 &e_{N,s+1}^2((P_{s,N}, H_{p,N} \oplus_p^{\text{mid}} \sigma_m), K_{s+1,\gamma}) \\
 &\quad \leq p^m \int_0^{p^{-m}} e_{N,s+1}^2((P_{s,N}, H_{p,N} \oplus_p(\sigma_m + \delta)), K_{s+1,\gamma}) \, d\delta.
 \end{aligned}$$

Proof. The proof is similar to that of Lemma 1. \square

3. The CBC construction

In this section, we analyze the following CBC construction of a mid-simplified \mathbf{p} -adic shift to obtain \mathbf{p} -adically shifted Halton sequences with a low integration error.

Throughout this section, let $s, N \in \mathbb{N}$ be given and let $\mathbf{p} = (p_1, \dots, p_s)$ with pairwise distinct prime components p_j . For $j \in [s]$ let $m_j \in \mathbb{N}$ be minimal such that $N < p_j^{m_j}$. Let $H_{\mathbf{p}, N}$ be the point set consisting of the first N elements of $H_{\mathbf{p}}$. To stress the dependence of the worst-case error on the \mathbf{p} -adic shift we write in the following

$$e_{N,s}(\boldsymbol{\sigma}) := e_{N,s}(H_{\mathbf{p}, N} \oplus_{\mathbf{p}}^{\text{mid}} \boldsymbol{\sigma}, K_{s,\gamma}) \quad \text{for } \boldsymbol{\sigma} \in \mathbb{Q}(p_1^{m_1}) \times \dots \times \mathbb{Q}(p_s^{m_s}).$$

We propose the following algorithm.

ALGORITHM 1.

- (1) Choose $\sigma_1 \in \mathbb{Q}(p_1^{m_1})$ to minimize $e_{N,1}^2(\sigma)$ as a function of σ .
- (2) For $1 \leq d \leq s-1$, assume that $\sigma_1, \dots, \sigma_d$ have already been found. Choose

$$\sigma_{d+1} \in \mathbb{Q}(p_{d+1}^{m_{d+1}})$$

to minimize

$$e_{N,d+1}^2((\sigma_1, \dots, \sigma_d, \sigma)) \tag{8}$$

as a function of σ .

- (3) If $d \leq s-1$ increase d by 1 and go to Step 2, otherwise stop.

REMARK 1. We remark that Algorithm 1 makes the main result in [7] much more explicit, as the algorithm only needs to check a countable number of possible candidates for the \mathbf{p} -adic shift. A slight drawback of our method is that the effective CBC construction of good \mathbf{p} -adic shifts has a cost of $O(s^2 N^3)$ operations, which is still large. Using a probabilistic version of Algorithm 1 leads to a reduction of a factor N in the construction cost, see Algorithm 2. Further improvements with respect to the construction cost are a demanding problem for future research.

The following theorem states that Algorithm 1 yields \mathbf{p} -adically shifted Halton sequences with a low integration error. Note that the error bound is of the same order as the one in Theorem 1.

THEOREM 2. *Let the notation be as above, and let $d \in [s]$. Assume that*

$$\boldsymbol{\sigma}_s = (\sigma_1, \dots, \sigma_s)$$

has been constructed according to Algorithm 1. Then

$$e_{N,d}(\boldsymbol{\sigma}_d) \leq \frac{1}{N} \left(\prod_{j=1}^d \left(1 + 2\gamma_j(\log N) \frac{p_j^2}{\log p_j} \right) + \prod_{j=1}^d (1 + \gamma_j) \prod_{j=1}^d \left(1 + \frac{\gamma_j p_j}{6} \right) \right)^{1/2},$$

where $\boldsymbol{\sigma}_d := (\sigma_1, \dots, \sigma_d)$.

Proof. We show the result by induction on d . For $d = 1$ we have

$$\begin{aligned} & \int_0^1 e_{N,1}^2(H_{p_1,N} \oplus_{p_1} \sigma, K_{1,\gamma_1}) \, d\sigma \\ &= \frac{1}{p_1^{m_1}} \sum_{\ell=0}^{p_1^{m_1}-1} p_1^{m_1} \int_{\ell/p_1^{m_1}}^{(\ell+1)/p_1^{m_1}} e_{N,1}^2 \left(H_{p_1,N} \oplus_{p_1} \left(\frac{\ell}{p_1^{m_1}} + \delta \right), K_{1,\gamma_1} \right) \, d\delta \\ &\geq \frac{1}{p_1^{m_1}} \sum_{\ell=0}^{p_1^{m_1}-1} e_{N,1}^2 \left(\frac{\ell}{p_1^{m_1}} \right), \end{aligned}$$

where we applied Lemma 1. Hence there exists a $\sigma'_1 \in \mathbb{Q}(p_1^{m_1})$ such that

$$\begin{aligned} e_{N,1}^2(\sigma'_1) &\leq \int_0^1 e_{N,1}^2(H_{p_1,N} \oplus_{p_1} \sigma, K_{1,\gamma_1}) \, d\sigma \\ &\leq \frac{1}{N^2} \left(1 + 2\gamma_1(\log N) \frac{p_1^2}{\log p_1} + (1 + \gamma_1) \left(1 + \frac{\gamma_1 p_1}{6} \right) \right), \end{aligned}$$

where we used [7, Theorem 1] for the second inequality. Since σ_1 is chosen by Algorithm 1 to minimize $e_{N,1}^2(\sigma)$, it follows that the result holds for $d = 1$.

Suppose the result has already been shown for some fixed $d \in [s-1]$. Assume that $\boldsymbol{\sigma}_d = (\sigma_1, \dots, \sigma_d)$ has been obtained by the CBC algorithm. Since σ_{d+1} is chosen in order to minimize the squared error (8), we have (where we write with some abuse of notation $(\boldsymbol{\sigma}_d, \sigma_{d+1}) := (\sigma_1, \dots, \sigma_d, \sigma_{d+1})$)

$$e_{N,d+1}^2((\boldsymbol{\sigma}_d, \sigma_{d+1})) \leq \frac{1}{p_{d+1}^{m_{d+1}}} \sum_{v=0}^{p_{d+1}^{m_{d+1}}-1} e_{N,d+1}^2 \left(\left(\boldsymbol{\sigma}_d, \frac{v}{p_{d+1}^{m_{d+1}}} \right) \right).$$

Using Lemma 2, we now see that, for any $v \in \{0, \dots, p_{d+1}^{m_{d+1}} - 1\}$,

$$\begin{aligned} & \frac{1}{p_{d+1}^{m_{d+1}}} e_{N,d+1}^2 \left(\left(\sigma_d, \frac{v}{p_{d+1}} \right) \right) \\ & \leq \int e_{N,d+1}^2 \left(\left(H_{\mathbf{p}_d, N} \oplus_{\mathbf{p}}^{\text{mid}} \sigma_d, H_{p_{d+1}, N} \oplus_{p_{d+1}} \left(\frac{v}{p_{d+1}} + \delta \right) \right), K_{d+1, \gamma} \right) d\delta, \end{aligned}$$

where the integral is between 0 and $p_{d+1}^{-m_{d+1}}$ and where $\mathbf{p}_d := (p_1, \dots, p_d)$. Hence

$$e_{N,d+1}^2((\sigma_d, \sigma_{d+1})) \leq \int_0^1 e_{N,d+1}^2((H_{\mathbf{p}_d, N} \oplus_{\mathbf{p}}^{\text{mid}} \sigma_d, H_{p_{d+1}, N} \oplus_{p_{d+1}} \sigma), K_{d+1, \gamma}) d\sigma.$$

We denote the points of $H_{\mathbf{p}_d, N} \oplus_{\mathbf{p}}^{\text{mid}} \sigma_d$ by $\mathbf{x}_n = (x_{n,1}, \dots, x_{n,d})$, and the points of $H_{p_{d+1}, N}$ by h_n . Due to (2), we obtain

$$\begin{aligned} & \int_0^1 e_{N,d+1}^2((H_{\mathbf{p}_d, N} \oplus_{\mathbf{p}}^{\text{mid}} \sigma_d, H_{p_{d+1}, N} \oplus_{p_{d+1}} \sigma), K_{d+1, \gamma}) d\sigma = \prod_{j=1}^{d+1} \left(1 + \frac{\gamma_j}{3} \right) \\ & \quad - \frac{2}{N} \sum_{n=0}^{N-1} \left[\prod_{j=1}^d \left(1 + \frac{\gamma_j}{2} (1 - x_{n,j}^2) \right) \right] \int_0^1 \left(1 + \frac{\gamma_{d+1}}{2} (1 - (h_n \oplus_{p_{d+1}} \sigma)^2) \right) d\sigma \\ & \quad + \frac{1}{N^2} \sum_{n,k=0}^{N-1} \left[\prod_{j=1}^d (1 + \gamma_j \min\{1 - x_{n,j}, 1 - x_{k,j}\}) \right] \\ & \quad \times \int_0^1 (1 + \gamma_{d+1} \min\{1 - (h_n \oplus_{p_{d+1}} \sigma), 1 - (h_k \oplus_{p_{d+1}} \sigma)\}) d\sigma. \end{aligned}$$

Let now

$$I_1 := \int_0^1 \left(1 + \frac{\gamma_{d+1}}{2} (1 - (h_n \oplus_{p_{d+1}} \sigma)^2) \right) d\sigma,$$

and

$$I_2 := \int_0^1 (1 + \gamma_{d+1} \min\{1 - (h_n \oplus_{p_{d+1}} \sigma), 1 - (h_k \oplus_{p_{d+1}} \sigma)\}) d\sigma.$$

Using (4), we obtain

$$I_1 = \int_0^1 \left(1 + \frac{\gamma_{d+1}}{2} (1 - \sigma^2) \right) d\sigma = 1 + \frac{\gamma_{d+1}}{3}.$$

Let us now deal with I_2 . Applying Proposition 2 in [7] yields that

$$I_2 = \sum_{\ell=0}^{\infty} r_{p_{d+1}, \gamma_{d+1}}(\ell) \beta_{\ell}(h_n) \overline{\beta_{\ell}(h_k)},$$

where for $\ell = \ell_{a-1}p_{d+1}^{a-1} + \cdots + \ell_1 p_{d+1} + \ell_0$ with $\ell_{a-1} \neq 0$ we have

$$r_{p_{d+1}, \gamma_{d+1}} = \begin{cases} 1 + \frac{\gamma_{d+1}}{3} & \text{if } \ell = 0, \\ \frac{\gamma_{d+1}}{2p_{d+1}^a} \left(\frac{1}{\sin^2(\ell_{a-1}\pi/p_{d+1})} - \frac{1}{3} \right) & \text{if } \ell \neq 0. \end{cases}$$

Altogether, we obtain

$$\begin{aligned} & e_{N, d+1}^2((\boldsymbol{\sigma}_d, \boldsymbol{\sigma}_{d+1})) \\ & \leq \prod_{j=1}^{d+1} \left(1 + \frac{\gamma_j}{3} \right) - \frac{2}{N} \sum_{n=0}^{N-1} \left[\prod_{j=1}^d \left(1 + \frac{\gamma_j}{2} (1 - x_{n,j}^2) \right) \right] \left(1 + \frac{\gamma_{d+1}}{3} \right) \\ & \quad + \frac{1}{N^2} \sum_{n,k=0}^{N-1} \left[\prod_{j=1}^d (1 + \gamma_j \min\{1 - x_{n,j}, 1 - x_{k,j}\}) \right] \\ & \quad \quad \quad \times \sum_{\ell=0}^{\infty} r_{p_{d+1}, \gamma_{d+1}}(\ell) \beta_\ell(h_n) \overline{\beta_\ell(h_k)} \\ & = \left(1 + \frac{\gamma_{d+1}}{3} \right) \left[\prod_{j=1}^d \left(1 + \frac{\gamma_j}{3} \right) - \frac{2}{N} \sum_{n=0}^{N-1} \prod_{j=1}^d \left(1 + \frac{\gamma_j}{2} (1 - x_{n,j}^2) \right) \right. \\ & \quad \quad \quad \left. + \frac{1}{N^2} \sum_{n,k=0}^{N-1} \prod_{j=1}^d (1 + \gamma_j \min\{1 - x_{n,j}, 1 - x_{k,j}\}) \right] \\ & \quad + \frac{1}{N^2} \sum_{n,k=0}^{N-1} \left(\prod_{j=1}^d (1 + \gamma_j \min\{1 - x_{n,j}, 1 - x_{k,j}\}) \right) \\ & \quad \quad \quad \times \sum_{\ell=1}^{\infty} r_{p_{d+1}, \gamma_{d+1}}(\ell) \beta_\ell(h_n) \overline{\beta_\ell(h_k)} \\ & = \left(1 + \frac{\gamma_{d+1}}{3} \right) e_{N,d}^2(\boldsymbol{\sigma}_d) + T, \end{aligned} \tag{9}$$

where

$$\begin{aligned} T := & \frac{1}{N^2} \sum_{n,k=0}^{N-1} \left(\prod_{j=1}^d (1 + \gamma_j \min\{1 - x_{n,j}, 1 - x_{k,j}\}) \right) \\ & \quad \quad \quad \times \sum_{\ell=1}^{\infty} r_{p_{d+1}, \gamma_{d+1}}(\ell) \beta_\ell(h_n) \overline{\beta_\ell(h_k)}. \end{aligned}$$

Since $\min\{1 - x_{n,j}, 1 - x_{k,j}\} \leq 1$ we obviously have

$$T \leq \left(\prod_{j=1}^d (1 + \gamma_j) \right) \sum_{\ell=1}^{\infty} r_{p_{d+1}, \gamma_{d+1}}(\ell) \left| \frac{1}{N} \sum_{n=0}^{N-1} \beta_\ell(h_n) \right|^2. \tag{10}$$

From the proof of [7, Theorem 1], it can easily be derived that

$$\sum_{\ell=1}^{\infty} r_{p_{d+1}, \gamma_{d+1}}(\ell) \left| \frac{1}{N} \sum_{n=0}^{N-1} \beta_{\ell}(h_n) \right|^2 \leq \frac{1}{N^2} \frac{\gamma_{d+1} g p_{d+1}^2}{2} + \frac{\gamma_{d+1}}{6 p_{d+1}^g} \left(1 + \frac{\gamma_{d+1}}{2} \right),$$

for arbitrarily chosen $g \in \mathbb{N}_0$. By choosing $g = \lfloor 2 \log_{p_{d+1}} N \rfloor$ and inserting into (10), we arrive at

$$\begin{aligned} T &\leq \frac{1}{N^2} \prod_{j=1}^d (1 + \gamma_j) \left(\left(\gamma_{d+1} (\log N) \frac{p_{d+1}^2}{\log p_{d+1}} \right) + \frac{\gamma_{d+1} p_{d+1}}{6} \left(1 + \frac{\gamma_{d+1}}{2} \right) \right) \\ &\leq \frac{1}{N^2} \left(\left(\gamma_{d+1} (\log N) \frac{p_{d+1}^2}{\log p_{d+1}} \right) \prod_{j=1}^d \left(1 + 2\gamma_j (\log N) \frac{p_j^2}{\log p_j} \right) \right. \\ &\quad \left. + \frac{\gamma_{d+1} p_{d+1}}{6} \prod_{j=1}^{d+1} (1 + \gamma_j) \prod_{j=1}^d \left(1 + \frac{\gamma_j p_j}{6} \right) \right). \end{aligned} \quad (11)$$

On the other hand, we have, using the induction assumption,

$$\begin{aligned} &\left(1 + \frac{\gamma_{d+1}}{3} \right) e_{N,d}^2(\boldsymbol{\sigma}_d) \\ &\leq \left(1 + \frac{\gamma_{d+1}}{3} \right) \frac{1}{N^2} \\ &\quad \left(\prod_{j=1}^d \left(1 + 2\gamma_j (\log N) \frac{p_j^2}{\log p_j} \right) + \prod_{j=1}^d (1 + \gamma_j) \prod_{j=1}^d \left(1 + \frac{\gamma_j p_j}{6} \right) \right) \\ &\leq \frac{1}{N^2} \left(\left(1 + \gamma_{d+1} (\log N) \frac{p_{d+1}^2}{\log p_{d+1}} \right) \prod_{j=1}^d \left(1 + 2\gamma_j (\log N) \frac{p_j^2}{\log p_j} \right) \right. \\ &\quad \left. + \prod_{j=1}^{d+1} (1 + \gamma_j) \prod_{j=1}^d \left(1 + \frac{\gamma_j p_j}{6} \right) \right). \end{aligned} \quad (12)$$

Combining equations (11) and (12), and inserting into (9), we obtain

$$\begin{aligned} &e_{N,d+1}^2((\boldsymbol{\sigma}_d, \sigma_{d+1})) \\ &\leq \frac{1}{N^2} \left(\prod_{j=1}^{d+1} \left(1 + 2\gamma_j (\log N) \frac{p_j^2}{\log p_j} \right) + \prod_{j=1}^{d+1} (1 + \gamma_j) \prod_{j=1}^{d+1} \left(1 + \frac{\gamma_j p_j}{6} \right) \right). \end{aligned}$$

Taking the square root we obtain the result for $d+1$, and the theorem is shown. \square

We also propose the following randomized algorithm.

ALGORITHM 2. Let $c \in \mathbb{N}$ such that $c \leq p_i^{m_i}$ for all $i \in [s]$.

- (1) Randomly choose c shifts $\tilde{\sigma}_1, \dots, \tilde{\sigma}_c \in \mathbb{Q}(p_1^{m_1})$, where $\tilde{\sigma}_1, \dots, \tilde{\sigma}_c$ are uniformly i.i.d. Set $\sigma_1 = \tilde{\sigma}_u$, where $u \in \{1, 2, \dots, c\}$ is the value of w which minimizes $e_{N,1}^2(\tilde{\sigma}_w)$ over $w \in \{1, 2, \dots, c\}$.
- (2) For $1 \leq d \leq s - 1$, assume that $\sigma_1, \dots, \sigma_d$ have already been found. Randomly choose c shifts $\tilde{\sigma}_1, \dots, \tilde{\sigma}_c \in \mathbb{Q}(p_{d+1}^{m_{d+1}})$, where $\tilde{\sigma}_1, \dots, \tilde{\sigma}_c$ are uniformly i.i.d. Set $\sigma_{d+1} = \tilde{\sigma}_u$, where $u \in \{1, 2, \dots, c\}$ is the value of w which minimizes

$$e_{N,d+1}^2((\sigma_1, \dots, \sigma_d, \tilde{\sigma}_w))$$

over $w \in \{1, 2, \dots, c\}$.

- (3) If $d \leq s - 1$ increase d by 1 and go to Step 2, otherwise stop.

REMARK 2. We remark that Algorithm 2 has a reduced construction cost of $O(cs^2N^2)$ operations. This means, if c is fixed and small compared to N we save a factor of N in the construction cost compared to Algorithm 1. This reduction is penalized by a slightly worse error estimate which now only holds with a certain probability. This is the essence of the following theorem.

THEOREM 3. Let $t \geq 1$. The probability that the vector $\boldsymbol{\sigma}_s = (\sigma_1, \dots, \sigma_s)$ constructed by Algorithm 2 satisfies

$$e_{N,d}(\boldsymbol{\sigma}_d) \leq \frac{t}{N} \left(\prod_{j=1}^d \left(1 + 2\gamma_j(\log N) \frac{p_j^2}{\log p_j} \right) + \prod_{j=1}^d (1 + \gamma_j) \prod_{j=1}^d \left(1 + \frac{\gamma_j p_j}{6} \right) \right)^{1/2}$$

for all $d \in [s]$, where $\boldsymbol{\sigma}_d := (\sigma_1, \dots, \sigma_d)$, is at least

$$\left(1 - \frac{1}{t^{2c}} \right)^s \geq 1 - \frac{s}{t^{2c}}.$$

Proof. For $d \in [s]$ let

$$L_{d,N} := \prod_{j=1}^d \left(1 + 2\gamma_j(\log N) \frac{p_j^2}{\log p_j} \right) + \prod_{j=1}^d (1 + \gamma_j) \prod_{j=1}^d \left(1 + \frac{\gamma_j p_j}{6} \right).$$

According to the proof of Theorem 2 we have

$$\frac{1}{p_1^{m_1}} \sum_{\ell=0}^{p_1^{m_1}-1} e_{N,1}^2 \left(\frac{\ell}{p_1^{m_1}} \right) \leq \frac{1}{N^2} L_{1,N}.$$

Using Markov's inequality we obtain that for all $t \geq 1$ we have

$$\frac{1}{p_1^{m_1}} \left| \left\{ \sigma \in \mathbb{Q}(p_1^{m_1}) : e_{N,1}^2(\sigma) \leq \frac{t}{N^2} L_{1,N} \right\} \right| \geq 1 - \frac{1}{t},$$

which can be re-written as

$$\frac{1}{p_1^{m_1}} \left| \left\{ \sigma \in \mathbb{Q}(p_1^{m_1}) : e_{N,1}(\sigma) \leq \frac{t}{N} L_{1,N}^{1/2} \right\} \right| \geq 1 - \frac{1}{t^2}.$$

Hence the probability that at least one of $\tilde{\sigma}_1, \dots, \tilde{\sigma}_c$ satisfies

$$e_{N,1}(\tilde{\sigma}_w) \leq \frac{t}{N} L_{1,N}^{1/2}$$

is at least $1 - t^{-2c}$.

Furthermore it was shown in the proof of Theorem 2 that under the assumption

$$e_{n,d}^2(\boldsymbol{\sigma}_d) \leq \frac{1}{N^2} L_{d,N}$$

we have

$$\frac{1}{p_{d+1}^{m_{d+1}}} \sum_{v=0}^{p_{d+1}^{m_{d+1}}-1} e_{N,d+1}^2 \left(\left(\boldsymbol{\sigma}_d, \frac{v}{p_{d+1}} \right) \right) \leq \frac{1}{N^2} L_{d+1,N}.$$

Using Markov's inequality again we obtain for $t \geq 1$

$$\frac{1}{p_{d+1}^{m_{d+1}}} \left| \left\{ \sigma \in \mathbb{Q}(p_{d+1}^{m_{d+1}}) : e_{N,d+1}(\boldsymbol{\sigma}_d, \sigma) \leq \frac{t}{N} L_{d+1,N}^{1/2} \right\} \right| \geq 1 - \frac{1}{t^2}.$$

Hence the probability that at least one of $\tilde{\sigma}_1, \dots, \tilde{\sigma}_c$ satisfies

$$e_{N,d+1}(\boldsymbol{\sigma}_d, \tilde{\sigma}_w) \leq \frac{t}{N} L_{d+1,N}^{1/2}$$

is at least $1 - t^{-2c}$. Hence the result follows. \square

REFERENCES

- [1] DICK, J.—KUO, F. Y.—PILLICHSHAMMER, F.—SLOAN, I. H.: *Construction algorithms for polynomial lattice rules for multivariate integration*, Math. Comp. **74** (2005), 1895–1921.
- [2] DICK, J.—PILLICHSHAMMER, F.: *Multivariate integration in weighted Hilbert spaces based on Walsh functions and weighted Sobolev spaces*, J. Complexity **21** (2005), 149–195.
- [3] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, 2010.
- [4] DRMOTA, M.—TICHY, R. F.: *Sequences, Discrepancies and Applications*, Springer-Verlag, Berlin, 1997.

- [5] HALTON, J. H.: *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*, Numer. Math. **2** (1960), 84–90.
- [6] HELLEKALEK, P.: *A notion of diaphony based on p -adic arithmetics*, Acta Arith. **139** (2010), 117–129.
- [7] HELLEKALEK, P.—KRITZER, P.—PILLICHSHAMMER, F.: *Open type quasi-Monte Carlo integration based on Halton sequences in weighted Sobolev spaces*, (2014), (submitted).
- [8] KOROBOV, N. M.: *Number-theoretic methods in approximate analysis*, Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1963. (In Russian)
- [9] KRITZER, P.—PILLICHSHAMMER, F.: *On the component by component construction of polynomial lattice point sets for numerical integration in weighted Sobolev spaces*. Unif. Distrib. Theory **6** (2011), 79–100.
- [10] KUIPERS, L.—NIEDERREITER, H.: *Uniform Distribution of Sequences*, John Wiley, New York, 1974.
- [11] KUO, F. Y.: *Component-by-component constructions achieve the optimal rate of convergence for multivariate integration in weighted Korobov and Sobolev spaces*, J. Complexity **19** (2003), 301–320.
- [12] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*. In: CBMS-NSF Series in Applied Mathematics Vol. 63. SIAM, Philadelphia, 1992.
- [13] NOVAK, E.—WOŹNIAKOWSKI, H.: *Tractability of Multivariate Problems. Volume I: Linear Information*. In: EMS Tracts in Mathematics, Vol. 6. European Mathematical Society (EMS), Zürich, 2008.
- [14] PILLICHSHAMMER, F.: *The p -adic diaphony of the Halton sequence*. Funct. Approx. Comment. Math. **49** (2013), 91–102.
- [15] SLOAN, I. H.—JOE, S.: *Lattice Methods for Multiple Integration*. Oxford University Press, New York and Oxford, 1994.
- [16] SLOAN, I. H.—REZTSOV, A. V.: *Component-by-component construction of good lattice rules*, Math. Comp. **71** (2002), 263–273.
- [17] SLOAN, I. H.—WOŹNIAKOWSKI, H.: *When are quasi-Monte Carlo algorithms efficient for high-dimensional integrals?* J. Complexity **14**, (1998), 1–33.
- [18] WANG, X.: *A constructive approach to strong tractability using quasi-Monte Carlo algorithms*, J. Complexity **18** (2002), 683–701.

Received January 29, 2015

Accepted April 16, 2015

Peter Kritzer

Friedrich Pillichshammer

Institut für Finanzmathematik und

angewandte Zahlentheorie

Johannes Kepler Universität Linz

Altenbergerstraße 69

A-4040 Linz

AUSTRIA

E-mail: peter.kritzer(at)jku.at

friedrich.pillichshammer(at)jku.at