

Original articles

Halton-type sequences in rational bases in the ring of rational integers and in the ring of polynomials over a finite field

Roswitha Hofer

Institute of Financial Mathematics, Johannes Kepler University Linz, Altenbergerstr. 69, 4040 Linz, Austria

Received 22 January 2016; received in revised form 13 July 2016; accepted 14 July 2016

Available online 5 August 2016

Abstract

The aim of this paper is to generalize the well-known Halton sequences from integer bases to rational number bases and to translate this concept of *Halton-type sequences in rational bases* from the ring of integers to the ring of polynomials over a finite field. These two new classes of Halton-type sequences are low-discrepancy sequences. More exactly, the first class, based on the ring of integers, satisfies the discrepancy bounds that were recently obtained by Atanassov for the ordinary Halton sequence, and the second class, based on the ring of polynomials over a finite field, satisfies the discrepancy bounds that were recently introduced by Tezuka and by Faure & Lemieux for the generalized Niederreiter sequences.

© 2016 International Association for Mathematics and Computers in Simulation (IMACS). Published by Elsevier B.V. All rights reserved.

Keywords: Low-discrepancy sequences; Halton-type sequences; Digital sequences

1. Introduction

For applications – for instance in finance, physics, or digital imaging – one relies on point distributions in the multidimensional unit cube that are uniformly spread. One important measure for the uniformity of a point set $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ of N points in $[0, 1]^s$ is the star-discrepancy D_N^* , defined by

$$D_N^*(\mathbf{x}_0, \dots, \mathbf{x}_{N-1}) = \sup_{\mathbf{y} \in (0, 1]^s} \left| \frac{\#\{0 \leq n < N : x_n^{(i)} < y^{(i)}, i = 1, \dots, s\}}{N} - \prod_{i=1}^s y^{(i)} \right|,$$

where $x_n^{(i)}$ and $y^{(i)}$ denote the i th components of \mathbf{x}_n and \mathbf{y} . For an infinite sequence $(\mathbf{x}_n)_{n \geq 0}$ in $[0, 1]^s$, the star-discrepancy D_N^* is defined via the first N elements of the sequence. The star-discrepancy appears as one main factor in the celebrated Koksma–Hlawka inequality. This inequality gives an upper bound of the integration error of a quadrature rule that heavily depends on the star-discrepancy of the sampling points. Hence, the smaller the discrepancy the better the approximation of the integral. Concerning this measure of uniformity the best explicit examples of sequences in dimension s satisfy discrepancy bounds in the style of

$$ND_N^* \leq c \log^s N + O(\log^{s-1} N) \quad (1)$$

E-mail address: roswitha.hofer@jku.at.

<http://dx.doi.org/10.1016/j.matcom.2016.07.005>

0378-4754/© 2016 International Association for Mathematics and Computers in Simulation (IMACS). Published by Elsevier B.V. All rights reserved.

where both constants $-c$ and the implied one $-$ are independent of N . We call sequences that satisfy (1) *low-discrepancy sequences*. (For further details on numerical integration and discrepancy we refer the reader to the excellent monographs [5,13].)

The probably most basic one-dimensional low-discrepancy sequence is the well-known *van der Corput sequence* in an integer base b greater than 1. The n th point x_n of the sequence is obtained by applying the b -adic Monna map φ_b , which is often called the radical inverse function in base b , to the nonnegative integer n . The function $\varphi_b : \mathbb{N}_0 \rightarrow [0, 1]$ is given by

$$n \mapsto \frac{n_0}{b} + \frac{n_1}{b^2} + \frac{n_2}{b^3} + \dots$$

where

$$n = n_0 + n_1b + n_2b^2 + \dots \quad \text{with } n_r \in \{0, 1, \dots, b - 1\} \tag{2}$$

is the b -adic expansion of n . One interesting property of this sequence is that one can easily build multidimensional low-discrepancy sequences by concatenating van der Corput sequences in pairwise coprime bases b_1, b_2, \dots, b_s . Such a sequence $(\varphi_{b_1}(n), \varphi_{b_2}(n), \dots, \varphi_{b_s}(n))_{n \geq 0}$ is well-known as *Halton sequence in bases* (b_1, b_2, \dots, b_s) . In the literature varied generalizations of the van der Corput sequences and their multidimensional forms were investigated. The majority of them can be categorized in the following three types.

1. Generalizations by applying operations on the digits n_0, n_1, \dots before inserting them in the radical inverse function. An example utilizes a permutation on $\{0, 1, \dots, b - 1\}$ to each digit. This generalization was introduced by Faure and its multidimensional versions are known as *generalized Halton sequences*. Another example allows linear operations on the digit vector (n_0, n_1, n_2, \dots) , before its entries are inserted in the radical inverse function. This way *linearly scrambled van der Corput (or Halton) sequences* are obtained.
2. Generalizations by using different expansions for the non-negative integer n and defining a proper radical inverse function. In [6] (see also [4]) a radical inverse function based on so-called Cantor expansions was introduced and investigated. In several papers van der Corput sequences based on so-called β -expansions were introduced and studied (see for example [3,16,17,19]).
3. Generalizations by changing the domain \mathbb{N}_0 of the Monna map. In [15] Niederreiter and Yeo introduced so-called Halton-type sequences from global function fields by defining a proper Monna map in a special subring of a global function field. Corresponding Halton-type sequences in algebraic number fields were introduced and investigated by Levin [11].

For details on previous generalizations of van der Corput and Halton sequences, particularly for the first two items above, the reader is referred to the overviews article [7] and the references therein.

In this paper we extend the family of generalized van der Corput sequences in two directions. Firstly we introduce a generalization of Halton sequences in the sense of item 2 by using expansions of integers in rational bases. Secondly we work out the corresponding framework for this Halton sequences in rational bases when switching the domain of the corresponding Monna map from \mathbb{Z} to the ring of polynomials over a finite field, which represents a generalization in the sense of item 3. The paper is organized as follows. We start with introducing proper expansions in the style of (2) for integers and for polynomials in rational bases in Section 2, before we define the radical inverse function in rational bases and the new Halton-type sequences in Section 3. This section also gives discrepancy bounds for the new sequences in Theorems 3 and 4 as well as short discussions on the discrepancy of the new Halton-type sequences in rational bases.

Throughout the paper q always denotes a prime power p^r with $p \in \mathbb{P}$ and $r \in \mathbb{N}_0$, \mathbb{F}_q stands for the finite field with q elements, $\mathbb{F}_q[X]$ for the set of polynomials in X with coefficients in \mathbb{F}_q . Vectors (v_1, \dots, v_s) , or $(x_n^{(1)}, \dots, x_n^{(s)})$ in \mathbb{R}^s are often abbreviated by bold symbols as \mathbf{v} or \mathbf{x}_n .

2. An expansion in rational bases

Let $b \geq 2$ be a rational integer. It is well-known that every rational integer z has a b -adic expansion of the form

$$z = \sum_{r=0}^{\infty} a_r b^r \quad \text{with } a_r \in \{0, 1, \dots, b - 1\} \text{ for } r \in \mathbb{N}_0. \tag{3}$$

There is an analogue of (3) in the ring of polynomials $\mathbb{F}_q[X]$ over a finite field \mathbb{F}_q with q elements. Let $b(X) \in \mathbb{F}_q[X]$ with $\deg b(X) =: e \geq 1$. Then every polynomial $f(X) \in \mathbb{F}_q[X]$ has a $b(X)$ -adic expansion of the form

$$f(X) = \sum_{r=0}^{\infty} a_r(X)b(X)^r \quad \text{with } a_r(X) \in \mathbb{F}_q[X] \text{ with } \deg a_r(X) < e \text{ for } r \in \mathbb{N}_0. \tag{4}$$

Note that $\deg 0$ is set $-\infty$. In Eqs. (3) and (4) the coefficients a_r and $a_r(X)$ are computed by the following algorithms.

\mathbb{Z} : Set $z_0 := z$ and for each $r \geq 1$ set $z_r = (z_{r-1} - a_{r-1})/b$, where a_{r-1} is the unique element in $\{0, 1, \dots, b-1\}$ such that $b|(z_{r-1} - a_{r-1})$.

$\mathbb{F}_q[X]$: Set $f_0(X) := f(X)$ and for each $r \geq 1$ set $f_r(X) = (f_{r-1}(X) - a_{r-1}(X))/b(X)$ where $a_{r-1}(X)$ is the unique polynomial in $\mathbb{F}_q[X]$ with $\deg a_{r-1}(X) < e$ such that $b(X)|(f_{r-1}(X) - a_{r-1}(X))$.

First we generalize those two algorithms to rational numbers $b = u/v$ with coprime integers $u \geq 2, v \geq 1$ and to rational functions $b(X) = u(X)/v(X)$ with coprime polynomials $u(X), v(X) \in \mathbb{F}_q[X]$ with $\deg u(X) =: e \geq 1$ and $v(X) \neq 0$.

\mathbb{Z} : Set $z_0 := z$ and for each $r \geq 1$ set $z_r = (vz_{r-1} - a_{r-1})/u$ where a_{r-1} is the unique element in $\{0, 1, \dots, u-1\}$ such that $u|(vz_{r-1} - a_{r-1})$.

$\mathbb{F}_q[X]$: Set $f_0(X) := f(X)$ and for each $r \geq 1$ set $f_r(X) = (v(X)f_{r-1}(X) - a_{r-1}(X))/u(X)$ where $a_{r-1}(X)$ is the unique polynomial in $\mathbb{F}_q[X]$ with $\deg a_{r-1}(X) < e$ such that $u(X)|(v(X)f_{r-1}(X) - a_{r-1}(X))$.

Note that z_r is an integer for every $r \geq 0$ and $f_r(X)$ is an element of $\mathbb{F}_q[X]$ for every $r \geq 0$. Application of these algorithms produces the following formal u/v -adic expansion of z

$$\sum_{r=0}^{\infty} \frac{a_r}{v} \left(\frac{u}{v}\right)^r =: (a_0, a_1, \dots)_{u/v}, \tag{5}$$

and the formal $u(X)/v(X)$ -adic expansion of $f(X)$

$$\sum_{r=0}^{\infty} \frac{a_r(X)}{v(X)} \left(\frac{u(X)}{v(X)}\right)^r =: (a_0(x), a_1(X), \dots)_{u(X)/v(X)}. \tag{6}$$

The expansions (5) and (6) coincide with the non-rational ones in (3) and (4) if $v = 1$ and $u = b$, and if $v(X) = 1$ and $u(X) = b(X)$ respectively.

Remark 1. Note that we speak of *formal* expansions and do not take care about convergence of the series. Using induction we deduce for $j \in \mathbb{N}_0$ the following identities

$$z = \sum_{r=0}^{j-1} \frac{a_r}{v} \left(\frac{u}{v}\right)^r + z_j \left(\frac{u}{v}\right)^j \tag{7}$$

and

$$f(X) = \sum_{r=0}^{j-1} \frac{a_r(X)}{v(X)} \left(\frac{u(X)}{v(X)}\right)^r + f_j(X) \left(\frac{u(X)}{v(X)}\right)^j. \tag{8}$$

Taking a prime p with $p|u$, taking a monic irreducible polynomial $p(X)$ with $p(X)|u(X)$, bearing in mind that $(z_r)_{r \geq 0}$ is a sequence in \mathbb{Z} , and that $(f_r(X))_{r \geq 0}$ is a sequence in $\mathbb{F}_q[X]$, we obtain convergence of the formal series with respect to the p -adic and $p(X)$ -adic absolute values and their limits are indeed z and $f(x)$.

Remark 2. We call an expansion of the form (5) or (6) *finite* if there are only finitely many nonzero a_r or nonzero $a_r(X)$ respectively.

If $u > v$ then (5) is finite for every nonnegative rational integer z and it coincides with the rational base number system for \mathbb{N}_0 considered by Akiyama et al. in [1]. Analogously, if $\deg u(X) > \deg v(X)$ then (6) is finite. It coincides with the number system considered by Loquias et al. in [12].

Remark 3. Switching from the integer base b to a rational base u/v with coprime u and v is different from taking a digital permutation. Consider for example $u/v = 3/2$. By Remark 2 each $n \in \mathbb{N}_0$ has a finite expansion. For the sake of simplicity we write $(a_0, a_1, \dots, a_k)_{u/v}$ where k is maximal such that $a_k \neq 0$ instead of $(a_0, a_1, \dots)_{u/v}$. The number 0 is denoted by $(0)_{u/v}$. In detail we obtain

n	0	1	2	3
$(a_0, a_1, \dots)_3$	$(0)_3$	$(1)_3$	$(2)_3$	$(0, 1)_3$
$(a_0, a_1, \dots)_{\frac{3}{2}}$	$(0)_{\frac{3}{2}}$	$(2)_{\frac{3}{2}}$	$(1, 2)_{\frac{3}{2}}$	$(0, 1, 2)_{\frac{3}{2}}$
n	4	5	6	7
$(a_0, a_1, \dots)_3$	$(1, 1)_3$	$(2, 1)_3$	$(0, 2)_3$	$(1, 2)_3$
$(a_0, a_1, \dots)_{\frac{3}{2}}$	$(2, 1, 2)_{\frac{3}{2}}$	$(1, 0, 1, 2)_{\frac{3}{2}}$	$(0, 2, 1, 2)_{\frac{3}{2}}$	$(2, 2, 1, 2)_{\frac{3}{2}}$
n	8	9	10	11
$(a_0, a_1, \dots)_3$	$(2, 2)_3$	$(0, 0, 1)_3$	$(1, 0, 1)_3$	$(2, 0, 1)_3$
$(a_0, a_1, \dots)_{\frac{3}{2}}$	$(1, 1, 0, 1, 2)_{\frac{3}{2}}$	$(0, 0, 2, 1, 2)_{\frac{3}{2}}$	$(2, 0, 2, 1, 2)_{\frac{3}{2}}$	$(1, 2, 2, 1, 2)_{\frac{3}{2}}$

For instance, the behavior of the lengths of the finite expansions shows that switching from base 3 to base $3/2$ cannot be described by digital permutations. This behavior also ensures that those different expansions cannot be obtained from each other by a linear map on the vector space $\mathbb{F}_3^{\mathbb{N}_0}$.

The example in Remark 3 indicates some nice properties of the expansion $(a_0, a_1, \dots)_{3/2}$ which are similar to some properties of the expansion $(a_0, a_1, \dots)_3$. For example, if n varies between 0 and $3^j - 1$, then both sets of tuples

$$\{(a_0, a_1, \dots, a_{j-1})_3, 0 \leq n < 3^j\} \quad \text{and} \quad \{(a_0, a_1, \dots, a_{j-1})_{3/2}, 0 \leq n < 3^j\}$$

span the set $\{0, 1, 2\}^j$. Furthermore, the starting sequence $(a_0, a_1, \dots, a_{j-1})_3$ (or $(a_0, a_1, \dots, a_{j-1})_{3/2}$ resp.) of $n \in \mathbb{N}_0$ coincides with the starting sequence $(a_0, a_1, \dots, a_{j-1})_3$ (or $(a_0, a_1, \dots, a_{j-1})_{3/2}$ resp.) of $m \in \mathbb{N}_0$ if n is congruent to m modulo 3^j . Properties like these between the expansions of different integers or polynomials respectively are ensured by the subsequent lemmas.

Lemma 1. Let $u, v, j \in \mathbb{N}$, satisfying $u \geq 2$ and $\gcd(u, v) = 1$. For $i \in \{1, 2\}$ let $z^{(i)}$ be an integer and $(a_0^{(i)}, a_1^{(i)}, a_2^{(i)}, \dots)_{u/v}$ be the u/v -adic expansion of $z^{(i)}$. Then $a_r^{(1)} = a_r^{(2)}$ for every $0 \leq r \leq j - 1$ if and only if $z^{(1)}$ is congruent to $z^{(2)}$ modulo u^j .

Proof. Suppose $a_r^{(1)} = a_r^{(2)}$ for every $0 \leq r \leq j - 1$, then by (7) we have for $i \in \{1, 2\}$

$$z^{(i)} = \sum_{r=0}^{j-1} \frac{a_r^{(i)}}{v} \left(\frac{u}{v}\right)^r + z_j^{(i)} \left(\frac{u}{v}\right)^j.$$

Hence,

$$z^{(1)} - z^{(2)} = (z_j^{(1)} - z_j^{(2)}) \left(\frac{u}{v}\right)^j.$$

Since $z_j^{(1)}, z_j^{(2)} \in \mathbb{Z}$ and $\gcd(u, v) = 1$ we know $v^j | (z_j^{(1)} - z_j^{(2)})$ and the desired result $u^j | (z^{(1)} - z^{(2)})$ follows.

Conversely, suppose $u^j | (z^{(1)} - z^{(2)})$. Using (7) we deduce

$$u^j | \sum_{r=0}^{j-1} v^{j-r-1} (a_r^{(1)} - a_r^{(2)}) u^r.$$

This relation immediately yields $a_r^{(1)} = a_r^{(2)}$ for every $0 \leq r \leq j - 1$.

Lemma 2. Let j be a positive integer, and let $u(X), v(X) \in \mathbb{F}_q[X]$ be coprime and satisfying $\deg u(X) \geq 1$ and $v(X) \neq 0$. For $i \in \{1, 2\}$ let $f^{(i)}(X) \in \mathbb{F}_q[X]$ and $(a_0^{(i)}(X), a_1^{(i)}(X), a_2^{(i)}(X), \dots)_{u(X)/v(X)}$ denote the $u(X)/v(X)$ -adic expansion of $f^{(i)}(X)$. Then $a_r^{(1)}(X) = a_r^{(2)}(X)$ for every $0 \leq r \leq j - 1$ if and only if $f^{(1)}(X)$ is congruent to $f^{(2)}(X)$ modulo $u(X)^j$.

Proof. The proof is carried out by analogous arguments as the ones used in the proof of Lemma 1.

3. Halton-type sequences in rational bases

In this section we introduce Halton-type sequences in rational bases in \mathbb{Z} and in $\mathbb{F}_q[X]$ and show low-discrepancy bounds for these sequences. We use the following notations. We set $Z_u = \{0, 1, \dots, u - 1\}$, where u is an integer greater than 1. For a polynomial $u(X)$ in $\mathbb{F}_q[X]$ with degree $e \geq 1$, $Z_{u(X)}$ denotes the set $\{f(X) \in \mathbb{F}_q[X] : \deg f(X) < e\}$.

3.1. Halton-type sequences in rational bases in \mathbb{Z}

Let $u, v \in \mathbb{N}$, satisfying $u \geq 2$ and $\gcd(u, v) = 1$. Let $\Sigma = (\sigma_r)_{r \geq 0}$ be a sequence of permutations on Z_u . We define the u/v -adic Monna map $\varphi_{u/v}^\Sigma : \mathbb{Z} \rightarrow [0, 1]$ by

$$z \mapsto \sum_{r \geq 0} \frac{\sigma_r(a_r)}{u^{r+1}}$$

where

$$\sum_{r \geq 0} \frac{a_r}{v} \left(\frac{u}{v}\right)^r$$

is the formal u/v -adic expansion of z .

Remark 4. One may suggest the alternative and probably more natural generalization of the Monna map from an integer base to a rational base of the form $z \mapsto \sum_{r \geq 0} \frac{\sigma_r(a_r)}{v} \left(\frac{u}{v}\right)^{r+1}$. In the case where $v > u$ the sum in this alternative definition may not converge. Furthermore, the Monna map is planned to serve for the definition of a van der Corput type sequence in a rational base and therefore its range should be a subset of $[0, 1]$. Taking the example in Remark 3 we know that 7 in base $3/2$ is $(2, 2, 1, 2)_{3/2}$. Now if all σ_r are chosen to be the identity then the alternative definition maps 7 to $118/81$ which is greater than 1, while the definition above yields $77/81$.

We are now in a position to define generalized Halton sequences in rational bases.

Definition 1. Let s be a dimension. Let $u_1, v_1, u_2, v_2, \dots, u_s, v_s \in \mathbb{N}$ satisfying $u_i \geq 2, \gcd(u_i, v_i) = 1$ for $1 \leq i \leq s$, and $\gcd(u_i, u_j) = 1$ for all $1 \leq i < j \leq s$. For each $i \in \{1, 2, \dots, s\}$ let $\Sigma^{(i)} = (\sigma_r^{(i)})$ be a sequence of permutations on Z_{u_i} . Then the sequence $\omega = (\mathbf{x}_n)_{n \geq 0}$ in $[0, 1]^s$ where the n th element \mathbf{x}_n is given by

$$\mathbf{x}_n = (\varphi_{u_1/v_1}^{\Sigma^{(1)}}(n), \varphi_{u_2/v_2}^{\Sigma^{(2)}}(n), \dots, \varphi_{u_s/v_s}^{\Sigma^{(s)}}(n))$$

is called an s -dimensional generalized Halton sequence in bases $(u_1/v_1, u_2/v_2, \dots, u_s/v_s)$.

If $v_1 = v_2 = \dots = v_s = 1$ then the sequences in Definition 1 coincide with generalized Halton sequences, which were mentioned in item 1 in Section 1. If, furthermore, $\sigma_r^{(i)}$ is the identity map on Z_{u_i} for every $r \geq 0$ and $i = 1, \dots, s$ then Definition 1 gives the ordinary Halton sequence in pairwise coprime bases (u_1, \dots, u_s) . Remark 3 ensures that generalized Halton sequences in integer bases form a strict subset of generalized Halton sequence in rational bases and that the latter are in general different from linearly scrambled Halton sequences. Fig. 1 shows the first 500 points of the Halton sequences in bases $(2, 3)$ and in bases $(2/3, 3/2)$, where all permutations $\sigma_r^{(i)}$ are chosen to be identities. Both point sets are evenly spread in the unit square.

As generalized Halton-sequences in pairwise coprime integer bases are low-discrepancy sequences, an aim is that the generalization to rational bases preserves the low-discrepancy property. The conservation of this property is ensured by the following theorem.

Theorem 3. The star-discrepancy of the s -dimensional generalized Halton sequence $(\mathbf{x}_n)_{n \geq 0}$ in bases $(u_1/v_1, u_2/v_2, \dots, u_s/v_s)$ in Definition 1 satisfies for all $N > 1$

$$ND_N^*(\mathbf{x}_0, \dots, \mathbf{x}_{N-1}) \leq c \log^s N + O(\log^{s-1} N) \tag{9}$$

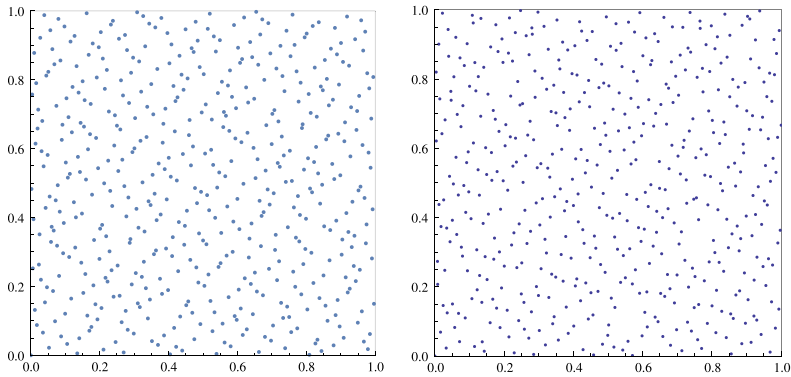


Fig. 1. First 500 points of the Halton sequences in bases (2, 3) (to the left) and (2/3, 3/2) (to the right), $\sigma_r^{(i)}$ are all identities.

where

$$c = \frac{1}{s!} \prod_{i=1}^s \left(\frac{u_i - 1}{2 \log u_i} \right)$$

and the implied constant is independent of N .

The constant in Theorem 3 equals the one that was obtained by Atanassov [2] for the ordinary Halton sequence in bases u_1, u_2, \dots, u_s . If we choose u_1, \dots, u_s as the first s prime numbers and v_1, \dots, v_s satisfying $\gcd(u_i, v_i) = 1$ for $i = 1, \dots, s$ then the constant in Theorem 3 is of the same behavior in s as the best known constant for the Halton sequence in prime bases. Atanassov additionally identified special digital permutations for the Halton sequence in prime bases (u_1, \dots, u_s) which allows an asymptotical improvement in the constant. When using for the r th digit of the i th component the permutation $\sigma_{i,r}$ defined by $\sigma_{i,r}(x) = k_i^r x \pmod{u_i}$ where k_1, \dots, k_s are admissible positive integers for the prime numbers u_1, \dots, u_s . That is: $\gcd(u_i, k_i) = 1$ for $i = 1, \dots, s$, and for each set of integers a_1, \dots, a_s satisfying $\gcd(u_i, a_i) = 1$ for $i = 1, \dots, s$ there exists a set of integers $\alpha_1, \dots, \alpha_s$ satisfying the congruences

$$k_i^{\alpha_i} \prod_{1 \leq j \leq s, j \neq i} p_j^{\alpha_j} \equiv a_i \pmod{u_i} \quad i = 1, \dots, s.$$

For such generalized Halton sequences Atanassov improved the leading constant in the discrepancy bound to

$$\frac{1}{s!} \sum_{i=1}^s \log u_i \prod_{j=1}^s \frac{u_j(1 + \log u_j)}{(u_j - 1) \log u_j}. \tag{10}$$

It is an interesting question if it is possible to identify proper denominators v_1, \dots, v_s for the Halton sequences in bases $(u_1/v_1, \dots, u_s/v_s)$ such that an improvement for the leading constant similar to (10) may be achieved.

3.2. Halton-type sequences in rational bases in $\mathbb{F}_q[X]$

Let $u(X), v(X) \in \mathbb{F}_q[X]$ be coprime, satisfying $e := \deg u(X) \geq 1$ and $v(X) \neq 0$. Let $\Sigma = (\sigma_r)_{r \geq 0}$ be a sequence of bijections between $Z_{u(X)}$ and Z_{q^e} . We define the $u(X)/v(X)$ -adic Monna map $\varphi_{u(X)/v(X)}^\Sigma : \mathbb{F}_q[X] \rightarrow [0, 1]$ by

$$f(X) \mapsto \sum_{r \geq 0} \frac{\sigma_r(a_r(X))}{q^{e(r+1)}}$$

where

$$\sum_{r \geq 0} \frac{a_r(X)}{v(X)} \left(\frac{u(X)}{v(X)} \right)^r$$

is the formal $u(X)/v(X)$ -adic expansion of $f(X)$.

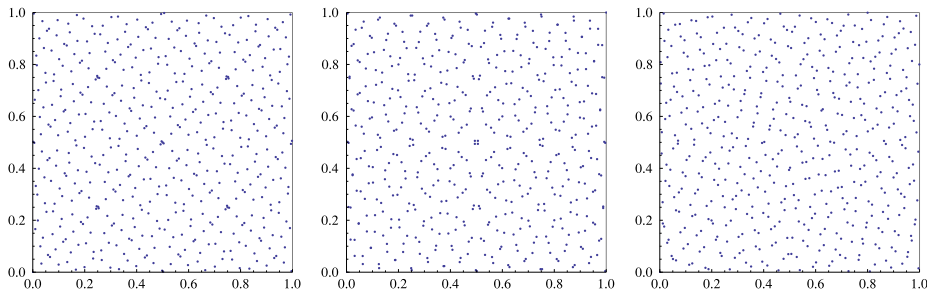


Fig. 2. First 512 points of the Halton sequence in bases $(X, X + 1)$ (to the left), $(X/(X + 1), (X + 1)/X)$ (in the middle), and $(X/(X^2 + X + 1), (X + 1)/(X^2 + X + 1))$ (to the right); $\sigma_r^{(i)}, \mu_j$ are all identities, $p_j(X) = X^j$.

In order to define a sequence $(\mathbf{x}_n)_{n \geq 0}$ we first have to associate with every $n \in \mathbb{N}_0$ a polynomial $n(X) \in \mathbb{F}_q[X]$. We use the ordinary q -adic expansion (3) of n , which we denote by

$$n = \sum_{j \geq 0} n_j q^j.$$

Note that only finitely many n_j are nonzero since $n \geq 0$. Let $(p_j(X))_{j \geq 0}$ be a sequence in $\mathbb{F}_q[X]$ satisfying $\deg p_j(X) = j$ for $j \geq 0$, and let $(\mu_j)_{j \geq 0}$ be a sequence of bijections between Z_q and \mathbb{F}_q that map 0 to 0. We set

$$n(X) := \sum_{\substack{j \geq 0 \\ n_j \neq 0}} \mu_j(n_j) p_j(X).$$

We are now ready to define Halton-type sequences in rational bases in $\mathbb{F}_q[X]$.

Definition 2. Let s be a dimension. Let $u_1(X), v_1(X), u_2(X), v_2(X), \dots, u_s(X), v_s(X) \in \mathbb{F}_q[X]$ satisfying $\deg u_i(X) := e_i \geq 1, v_i(X) \neq 0$, and $v_i(X)$ is coprime with $u_i(X)$ for $1 \leq i \leq s$. Furthermore, let the polynomials $u_1(X), u_2(X), \dots, u_s(X)$ be pairwise coprime. For each $i \in \{1, 2, \dots, s\}$ let $\Sigma^{(i)} = (\sigma_r^{(i)})$ be a sequence of bijections between $Z_{u_i(X)}$ and $Z_{q^{e_i}}$. Let $(p_j(X))_{j \geq 0}$ be a sequence in $\mathbb{F}_q[X]$ satisfying $\deg p_j(X) = j$ for $j \geq 0$, and let $(\mu_j)_{j \geq 0}$ be a sequence of bijections between Z_q and \mathbb{F}_q that map 0 to 0. Then the sequence $\omega = (\mathbf{x}_n)_{n \geq 0}$ where the n th element \mathbf{x}_n is given by

$$\mathbf{x}_n := (\varphi_{u_1(X)/v_1(X)}^{\Sigma^{(1)}}(n(X)), \varphi_{u_2(X)/v_2(X)}^{\Sigma^{(2)}}(n(X)), \dots, \varphi_{u_s(X)/v_s(X)}^{\Sigma^{(s)}}(n(X)))$$

is called s -dimensional generalized Halton sequence in bases

$$(u_1(X)/v_1(X), u_2(X)/v_2(X), \dots, u_s(X)/v_s(X)).$$

If, $v_i(X) = 1$ for all i in $\{1, \dots, s\}$ then the Halton sequences in Definition 2 are non-digital generalizations of the sequences introduced in [9]. If, furthermore, $u_i(X)$ is an irreducible polynomial for every $i \in \{1, \dots, s\}$ then these sequences can be viewed as special examples of the Niederreiter–Yeo sequences [15], which are different of the so-called polynomial arithmetic analogues of Halton sequences [20].

Fig. 2 shows the first 512 points of the Halton sequence in bases $(X, X + 1)$ over \mathbb{F}_2 , in bases $(X/(X + 1), (X + 1)/X)$ over \mathbb{F}_2 , and in bases $(X/(X^2 + X + 1), (X + 1)/(X^2 + X + 1))$ where all mappings $\sigma_r^{(i)}$ and μ_j are identities, and where $p_j(X) = X^j$ for $j \geq 0$.

The following theorem guarantees the low-discrepancy property for the sequences in Definition 2.

Theorem 4. The star-discrepancy of the s -dimensional generalized Halton sequence $(\mathbf{x}_n)_{n \geq 0}$ in bases

$$(u_1(X)/v_1(X), u_2(X)/v_2(X), \dots, u_s(X)/v_s(X))$$

in Definition 2 satisfies for all $N > 1$

$$ND_N^*(\mathbf{x}_0, \dots, \mathbf{x}_{N-1}) \leq c \log^s N + O(\log^{s-1} N) \tag{11}$$

where

$$c = \frac{1}{s!} \prod_{i=1}^s \left(\frac{q^{e_i} - 1}{2e_i \log q} \right)$$

and the implied constant is independent of N .

The constant c in Theorem 4 actually is the same as the one that was recently proved by Faure and Lemieux [8] and by Tezuka [22] for example for the generalized Niederreiter sequences based on the polynomials $u_1(X), u_2(X), \dots, u_s(X)$. When choosing $u_1(X), u_2(X), \dots, u_s(X)$ as the first s monic irreducible polynomials in $\mathbb{F}_q[X]$ with smallest possible degrees both constants the one for the Niederreiter sequence as well as the Halton-type sequences in bases

$$(u_1(X)/v_1(X), u_2(X)/v_2(X), \dots, u_s(X)/v_s(X))$$

with arbitrary $v_i(X)$ coprime with $u_i(X), i = 1, \dots, s$ are equal. An interesting question is: whether admissible bijections $\sigma_r^{(i)}$ exist for the Halton-type concept in rational function bases such that the leading constant in the discrepancy bound can be improved similarly in the generalized Halton case in (10). This question is supported by for example the different patterns in Fig. 2, which are not distinguished by the discrepancy bound in Theorem 4. Another interesting aspect is the following. It is known that the L_2 -discrepancy of the digitally permuted van der Corput sequence in base 2 is of order $\log N/N$ in N (see [10]). The one-dimensional Halton-type sequence in base $X \in \mathbb{F}_2[X]$ with underlying polynomials $p_j(X) = X^j, j \geq 0$ in $\mathbb{F}_2[X]$ corresponds with the case of digitally permuted van der Corput sequences in base 2. An interesting question is: are there choices of base functions $u(X)/v(X)$ and of polynomials $p_j(X) = X^j$ in $\mathbb{F}_2(X)$ such that the L_2 -discrepancy is optimal in N , i.e., of the form $O(\sqrt{\log N}/N)$. This question is particularly motivated by positive results in [18] for special linearly scrambled van der Corput sequences in base 2.

3.3. Proofs of Theorems 3 and 4

To derive the discrepancy bounds of Theorems 3 and 4 we use a concept of truncation.

Let s be a nonnegative integer. Let b_1, \dots, b_s be s nonnegative integers greater or equal to 2. Let $\omega = (x_n)_{n \geq 0}$ be an s -dimensional sequence in $[0, 1]^s$ satisfying that for every $i \in \{1, 2, \dots, s\}$ the i th component has prescribed digit expansion in base b_i , where the case with almost all digits equal to $b_i - 1$ is admissible.

We introduce the truncation operator $[x]_N$ depending on $N \in \mathbb{N}$ that applies for every $i \in \{1, \dots, s\}$ in the i th component $x^{(i)}$ of \mathbf{x} the base b_i digits truncation of length $\lfloor \log_{b_i} N \rfloor + 1 =: l_i$, i.e., x with prescribed digit expansion $\sum_{r=1}^{\infty} x_r b_i^{-r}$ maps to $\sum_{r=1}^{l_i} x_r b_i^{-r}$. In the sequel $\mathcal{P}_N(\omega)$ denotes the set $\{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}\}$ and $[\mathcal{P}_N(\omega)]$ the set $\{[\mathbf{x}_0]_N, [\mathbf{x}_1]_N, \dots, [\mathbf{x}_{N-1}]_N\}$.

Proof of Theorem 3. We apply the truncation operator with $b_i = u_i, i = 1, \dots, s$ and prove the subsequent two inequalities. The first,

$$|A_N(I, [\mathcal{P}_N(\omega)]) - N \text{vol}(I)| \leq 1 \tag{12}$$

with

$$I := I(\mathbf{u}, \mathbf{j}, \mathbf{d}) = \prod_{i=1}^s \left[\frac{d_i}{u_i^{j_i}}, \frac{d_i + 1}{u_i^{j_i}} \right) \tag{13}$$

for all choices of \mathbf{j}, \mathbf{d} , and N , where $j_i \in \{0, 1, \dots, \lfloor \log_{u_i} N \rfloor + 1\}$ and $d_i \in [0, u_i^{j_i}) \cap \mathbb{Z}$ for $i = 1, \dots, s$. The second, if, additionally, $N < \prod_{i=1}^s u_i^{j_i}$ then

$$A_N(I, [\mathcal{P}_N(\omega)]) \leq 1. \tag{14}$$

Thanks to the truncation operator $[\cdot]_N$, we see that, whether a point $[\mathbf{x}_n]_N$ is included in I or not, is completely determined by $(a_0^{(i)}, a_1^{(i)}, \dots, a_{j_i-1}^{(i)})_{u_i/v_i}$, where the $a_r^{(i)}$ are given by the u_i/v_i -adic expansion of n

$$n = \sum_{r=0}^{j_i-1} \frac{a_r^{(i)}}{v_i} \left(\frac{u_i}{v_i} \right)^r.$$

Indeed, for fixed j_1, \dots, j_s there is a one-to-one correspondence between the set $\mathbb{Z} \cap [0, u_i^{j_i})$ and $Z_{u_i}^{j_i}$. Application of Lemma 1 yields

$$[\mathbf{x}_n]_N \in I \quad \text{if and only if} \quad n \equiv R_i \pmod{u_i^{j_i}} \quad \text{for } i = 1, \dots, s,$$

where the $R_i \in Z_{u_i}^{j_i}$ are determined by the interval I . Application of the Chinese Remainder theorem yields

$$[\mathbf{x}_n]_N \in I \quad \text{if and only if} \quad n \equiv R \pmod{\prod_{i=1}^s u_i^{j_i}}$$

and, therefore,

$$A_N(I, [\mathcal{P}_N(\omega)]) \leq 1.$$

as long $N < \prod_{i=1}^s u_i^{j_i}$ and

$$\begin{aligned} |A_N(I, [\mathcal{P}_N(\omega)]) - N \text{vol}(I)| &= \left| \left\lfloor \frac{N}{\prod_{i=1}^s u_i^{j_i}} \right\rfloor + \delta_{N,I} - \frac{N}{\prod_{i=1}^s u_i^{j_i}} \right| \\ &= \left| \delta_{N,I} - \left\{ \frac{N}{\prod_{i=1}^s u_i^{j_i}} \right\} \right| \leq 1. \end{aligned}$$

Here $\delta_{N,I} \in \{0, 1\}$ is depending on N and I . Note that furthermore if $N = k \prod_{i=1}^s u_i^{j_i}$ with $k \in \mathbb{N}$ then $|A_N(I, [\mathcal{P}_N(\omega)]) - N \text{vol}(I)| = 0$ is even true.

Atanassov’s proof for the discrepancy bound on the Halton sequences [2] is based on properties (12) and (14), which are obviously valid for the ordinary Halton sequence. Hence the bound in Theorem 3 is valid for $[\mathcal{P}_N(\omega)]$.

So far the desired discrepancy bound is proved only for the truncated version of the sequence $[\mathcal{P}_N(\omega)]$. In order to show it for the point set $\mathcal{P}_N(\omega)$ we follow an idea of Niederreiter and Özbudak (cf. [14, Proof of Lemma 4.2]). For $n = 0, 1, \dots, N - 1$ we can write

$$\mathbf{x}_n = [\mathbf{x}_n]_N + \mathbf{z}_n \quad \text{with } \mathbf{z}_n \in \prod_{i=1}^s [0, u_i^{-\lfloor \log_{u_i} N \rfloor} - 1].$$

Now let $0 < \varepsilon \leq 1$ be given and let $\mathcal{P}_N(\omega; \varepsilon)$ be the point set consisting of

$$\mathbf{x}_n(\varepsilon) = [\mathbf{x}_n]_N + (1 - \varepsilon)\mathbf{z}_n, \quad n = 0, 1, \dots, N - 1.$$

From the definition of the digit-truncation operator and I in (13) it is clear that

$$A_N(I, [\mathcal{P}_N(\omega)]) = A_N(I, \mathcal{P}_N(\omega; \varepsilon)).$$

Hence, if (12) and (14) hold for $[\mathcal{P}_N(\omega)]$ then they remain true for $\mathcal{P}_N(\omega; \varepsilon)$. Since, as already mentioned, these inequalities are the only assumptions on the point set that are used to deduce the discrepancy bound in Theorem 3, it holds also for $\mathcal{P}_N(\omega; \varepsilon)$.

Finally, by using a general principle of [13, proof of Lemma 2.5] we observe that

$$|ND_N^*(\mathcal{P}_N(\omega)) - ND_N^*(\mathcal{P}_N(\omega; \varepsilon))| \leq s\varepsilon,$$

and we are done.

Proof of Theorem 4. Analogously to the proof of Theorem 3 we make use of the truncation operator with base q^{e_i} . First we prove the following two inequalities. The first,

$$|A_N(I, [\mathcal{P}_N(\omega)]) - N \text{vol}(I)| \leq 1 \tag{15}$$

with

$$I := I(\mathbf{b}, \mathbf{j}, \mathbf{d}) = \prod_{i=1}^s \left[\frac{d_i}{q^{e_i j_i}}, \frac{d_i + 1}{q^{e_i j_i}} \right) \tag{16}$$

for all choices of \mathbf{j}, \mathbf{d} , and N , where $j_i \in \{0, 1, \dots, \lfloor \log_{q^{e_i}} N \rfloor + 1\}$ and $d_i \in [0, q^{e_i j_i}) \cap \mathbb{Z}$ for $i = 1, \dots, s$. Note that \mathbf{b} denotes $(q^{e_1}, \dots, q^{e_s})$. The second,

$$A_N(I, [\mathcal{P}_N(\omega)]) \leq 1 \tag{17}$$

if, additionally, $N < \prod_{i=1}^s q^{e_i j_i}$.

Thanks to the truncation operator $[\cdot]_N$ again, we know that, whether a point $[\mathbf{x}_n]_N$ is included in I or not, is determined by $(a_0^{(i)}(X), a_1^{(i)}(X), \dots, a_{j_i-1}^{(i)}(X))_{u_i/v_i}$, where the $a_r^{(i)}(X)$ are given by the $u_i(X)/v_i(X)$ -adic expansion of $n(X)$

$$n(X) = \sum_{r \geq 0} \frac{a_r^{(i)}(X)}{v_i(X)} \left(\frac{u_i(X)}{v_i(X)} \right)^r.$$

Indeed, for fixed j_1, \dots, j_s there is a one-to-one relation between the set of integers $d_i \in [0, q^{e_i j_i})$ and $(a_0^{(i)}(X), a_1^{(i)}(X), \dots, a_{j_i-1}^{(i)}(X)) \in Z_{u_i(X)}^{j_i}$. Application of Lemma 2 yields

$$[\mathbf{x}_n]_N \in I \quad \text{if and only if} \quad n(X) \equiv R_i(X) \pmod{u_i(X)^{j_i}} \quad \text{for } i = 1, \dots, s,$$

where the $R_i(X) \in Z_{(u_i(X))^{j_i}}$ depend on the d_i . Application of the Chinese Remainder theorem yields

$$[\mathbf{x}_n]_N \in I \quad \text{if and only if} \quad n(X) \equiv R(X) \pmod{\prod_{i=1}^s (u_i(X))^{j_i}}$$

where $R(X)$ takes a value in $Z_{\prod_{i=1}^s (u_i(X))^{j_i}}$ depending on d_1, \dots, d_s . Finally, we consider the set of polynomials

$$\mathcal{M}(k) = \left\{ n(X) : n = k \prod_{i=1}^s q^{e_i j_i} + m \text{ with } m \in Z_{\prod_{i=1}^s q^{e_i j_i}} \right\}$$

and it is easily seen that for any $k \in \mathbb{N}_0$, $\mathcal{M}(k)$ forms a complete set of representatives of $\mathbb{F}_q[X]$ modulo $\prod_{i=1}^s (u_i(X))^{j_i}$. Hence, exactly one point out of $\mathbf{x}_k \prod_{i=1}^s q^{e_i j_i} + m$, $m = 0, 1, \dots, \prod_{i=1}^s q^{e_i j_i} - 1$ is contained in I . It is not so hard to see that this property implies that the sequence is a $(0, \mathbf{e}, s)$ -sequence in base q , which were introduced by Tezuka [22, Definition 2].

Analogously to the proof of Theorem 3 both inequalities (15) and (17) immediately follow, which are exactly the crucial properties of $(0, \mathbf{e}, s)$ -sequences in base q that were used by Tezuka [22], confer the Lemma 1 therein. Hence, the discrepancy bound in Theorem 4 is valid for the truncated point set $[\mathcal{P}_N(\omega)]$. Using the same arguments as in the proof of Theorem 3 we generalize the discrepancy bound to the untruncated point set $\mathcal{P}_N(\omega)$ and the proof is complete.

Remark 5. Since the important inequalities (12), (14), (15) and (17) hold, one could derive stronger versions of the discrepancy bounds (9) and (11) as, for instance, the ones that can be found in [22,21,8].

Acknowledgment

The author is partially supported by the Austrian Science Fund (FWF): Project F5505-N26, which is a part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

References

[1] S. Akiyama, C. Frougny, J. Sakarovitch, Powers of rationals modulo 1 and rational base number systems, *Israel J. Math.* 168 (2008) 53–91.
 [2] E.I. Atanassov, On the discrepancy of the Halton sequences, *Math. Balkanica (N.S.)* 18 (2004) 15–32.
 [3] G. Barat, P.J. Grabner, Distribution properties of G -additive functions, *J. Number Theory* 60 (1996) 103–123.
 [4] H. Chaix, H. Faure, Discr pance et diaphonie en dimension un, *Acta Arith.* 63 (1993) 103–141 (in French).
 [5] J. Dick, F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, Cambridge, 2010.
 [6] H. Faure, Discr pances de suites associ es a un syst me de num ration (en dimension un), *Bull. Soc. Math. France* 109 (1981) 143–182 (in French).

- [7] H. Faure, P. Kritzer, F. Pillichshammer, From van der Corput to modern constructions of sequences for quasi-Monte Carlo rules, *Indag. Math.* 26 (2015) 760–822.
- [8] H. Faure, C. Lemieux, A variant of Atanassov’s method for (t, s) -sequences and (t, e, s) -sequences, *J. Complexity* 30 (2014) 620–633.
- [9] R. Hofer, A construction of low-discrepancy sequences involving finite-row digital (t, s) -sequences, *Math. Monatsh.* 171 (2013) 77–89.
- [10] P. Kritzer, F. Pillichshammer, Improvements of the discrepancy of the van der Corput sequence, *Math. Pannon.* 16 (2005) 179–198.
- [11] M.B. Levin, Adelic constructions of low discrepancy sequences, *Online J. Anal. Comb.* (5) (2010) 27.
- [12] M.J.C. Loquias, M. Mkaouar, K. Scheicher, J.M. Thuswaldner, Rational digit systems over finite fields and Christol’s Theorem, 2015 (submitted for publication).
- [13] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.
- [14] H. Niederreiter, F. Özbudak, Low-discrepancy sequences using duality and global function fields, *Acta Arith.* 130 (2007) 79–97.
- [15] H. Niederreiter, A.S. Yeo, Halton-type sequences from global function fields, *Sci. China Math.* 56 (2013) 1467–1476.
- [16] S. Ninomiya, Constructing a new class of low-discrepancy sequences by using the β -adic transformation, *Math. Comput. Simulation* 47 (1998) 403–418.
- [17] S. Ninomiya, On the discrepancy of the β -adic van der Corput sequence, *J. Math. Sci. Univ. Tokyo* 5 (1998) 345–366.
- [18] F. Pillichshammer, Digital sequences with best possible order of L_2 -discrepancy, *Mathematika* 53 (2006) 149–160.
- [19] W. Steiner, Regularities of the distribution of β -adic van der Corput sequences, *Monatsh. Math.* 149 (2006) 67–81.
- [20] S. Tezuka, Polynomial arithmetic analogue of Halton sequences, *ACM Trans. Model. Comput. Simul.* 3 (1993) 99–107.
- [21] S. Tezuka, On the discrepancy of generalized Niederreiter sequences, *J. Complexity* 29 (2013) 240–247.
- [22] S. Tezuka, Improvement on the discrepancy of (t, e, s) -sequences, *Tatra Mt. Math. Publ.* 59 (2014) 27–38.