Available online at www.sciencedirect.com
ScienceDirect
Mathematics and Computers in Simulation 143 (2018) 78–88
MATHEMATICS AND COMPUTERS IN SIMULATION
www.elsevier.com/locate/matcom

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.

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 $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}$ of N points in $[0, 1]^s$ is the star-discrepancy D_N^*, defined by

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

where $x_n^{(i)}$ and $y^{(i)}$ denote the ith components of $\boldsymbol{x}_n$ and $\boldsymbol{y}$. For an infinite sequence $(\boldsymbol{x}_n)_{n\ge 0}$ 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

$$N D_N^* \le c \log^s N + O(\log^{s-1} N) \tag{1}$$

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

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

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 nth 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 $\varphi_b : \mathbb{N}_0 \to [0, 1]$ is given by

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

where

$$n = n_0 + n_1 b + n_2 b^2 + \cdots \quad \text{with } n_r \in \{0, 1, \ldots, b-1\} \tag{2}$$

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 $b_1, b_2, \ldots, b_s$. Such a sequence $(\varphi_{b_1}(n), \varphi_{b_2}(n), \ldots, \varphi_{b_s}(n))_{n\geq 0}$ is well-known as *Halton sequence in bases* $(b_1, b_2, \ldots, b_s)$. 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 $n_0, n_1, \ldots$ before inserting them in the radical inverse function. An example utilizes a permutation on $\{0, 1, \ldots, b-1\}$ 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 $(n_0, n_1, n_2, \ldots)$, 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 overviewing 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 as $(v_1, \ldots, v_s)$, or $(x_n^{(1)}, \ldots, x_n^{(s)})$ in $\mathbb{R}^s$ are often abbreviated by bold symbols as $\boldsymbol{v}$ or $\boldsymbol{x}_n$.

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

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