Uniform Distribution Theory **8** (2013), no.1, 31–45

uniform distribution theory

A GENERAL DISCREPANCY BOUND FOR HYBRID SEQUENCES INVOLVING HALTON SEQUENCES

Domingo Gómez-Pérez, Roswitha Hofer, and Harald Niederreiter

ABSTRACT. Niederreiter initiated the study of the discrepancy of hybrid sequences that are built from Halton sequences and sequences of pseudorandom numbers. The aims of this paper are multiple: we provide a general discrepancy bound for such hybrid sequences, we derive from it the results obtained by Niederreiter for concrete examples, and we apply this bound to two further examples that are related to recursive generators and were not considered so far. Finally, we briefly discuss the main tasks for the investigation of hybrid sequences that are built from digital sequences and pseudorandom number sequences.

Communicated by Werner Georg Nowak

1. Motivation and introduction

Many applications, such as simulation, digital imaging, or financial mathematics, require accurate numerical approximation of the integral of a function $F : [0,1]^s \to \mathbb{R}$, $I(F) := \int_{[0,1]^s} F(\boldsymbol{x})\mathrm{d}\boldsymbol{x}$, where the integration domain may be very high-dimensional, having perhaps hundreds of dimensions. One way of accomplishing this task is to approximate $I(F)$ by the following average

$$Q_N(F) := \frac{1}{N}\sum_{n=0}^{N-1} F(\boldsymbol{x}_n)$$

of function values, where $(\boldsymbol{x}_n)_{n=0}^{N-1}$ is a finite sequence of points in $[0,1)^s$ (or a point set, as one also says). As the function F is given by the problem, one can influence the quality of the approximation only by intelligent choices of the sequence $(\boldsymbol{x}_n)_{n=0}^{N-1}$. We mainly distinguish between the following two algorithms:

2010 Mathematics Subject Classification: 11K38, 11K45, 65C05, 65C10.
Keywords: Discrepancy, hybrid sequence, Halton sequence, pseudorandom numbers.
The first author was supported by the Spanish Government by Research Grant MTM2011-24678 and TIN2011-27479-C04-04. The second author was supported by the Austrian Science Fund (FWF), Project P21943.

- a Monte Carlo (MC) rule uses a sequence of independent and uniformly distributed random samples;
- a quasi-Monte Carlo (QMC) rule is based on a deterministic point set (or the initial segment of a deterministic infinite sequence).

Both algorithms have advantages and disadvantages. For example, for an MC rule we know a probabilistic bound for the integration error $I(F)-Q_N(F)$ which depends on the variance of the function F and the number N of points that are used, but is more or less independent of the dimensionality of the problem. For a QMC rule we have a deterministic bound for the integration error which depends on two aspects, the function F and the discrepancy of the point set, and this bound tends to be much smaller than the MC bound for low dimensions and a judicious choice of the point set. In a nutshell — of course under certain conditions on the function F — one can say: QMC rules are very effective in low dimensions, whereas MC rules work reasonably well in high dimensions. (The interested reader is referred, e.g., to [1, 12, 13] for more details on MC and QMC rules.)

Spanier [25] was the first to suggest combining the advantages of both rules by using hybrid sequences. The idea is to use a low-discrepancy sequence to sample the "dominating" variables of the integrand and the remaining variables are sampled by random sequences. Recently, the first nontrivial deterministic discrepancy bounds for hybrid sequences were established by Niederreiter [14]. Several papers considered hybrid sequences that are built from low-discrepancy Halton sequences and certain pseudorandom number sequences, see [14, 16, 17, 18, 20]. Previously, only probabilistic results on the discrepancy of hybrid sequences were known (see, e.g., [3, 21, 22]).

2. Preliminaries

From now on, we use the Landau symbol $h(N) = O(H(N))$ to express $|h(N)| \le CH(N)$ for some positive constant C independent of N and a function $H : \mathbb{N} \to \mathbb{R}^+$. If the implied constant C depends on some parameters, then these parameters will appear as a subscript in the Landau symbol. A symbol O without a subscript indicates an absolute implied constant. Also, we denote $\log x$ as the natural logarithm and $\operatorname{Log} x := \max(1, \log x)$ for real numbers $x > 0$.

For an integer $b \ge 2$, let $\mathbb{Z}_b = \{0, 1, \ldots, b-1\}$ denote the least residue system modulo b. Let $n = \sum_{j=1}^{\infty} a_j(n) b^{j-1}$ with all $a_j(n) \in \mathbb{Z}_b$ and $a_j(n) = 0$ for all sufficiently large j be the unique digit expansion of the integer $n \ge 0$ in base b.

The *radical-inverse function* $\phi_b : \mathbb{N}_0 \to [0,1)$ in base b is defined by

$$\phi_b(n) = \sum_{j=1}^{\infty} a_j(n) b^{-j}.$$

For pairwise coprime integers $b_1, \ldots, b_s \geq 2$, the *Halton sequence* (in the bases $b_1, \ldots, b_s$) is given by

$$\boldsymbol{y}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n)) \in [0,1)^s, \quad n = 0, 1, \ldots.$$

The *discrepancy* of the first N terms of any sequence $(\boldsymbol{z}_n)_{n\geq 0}$ of points in $[0,1)^s$ is defined by

$$D_N(\boldsymbol{z}_n) = \sup_J \left| \frac{A(J,N)}{N} - \lambda_s(J) \right|,$$

where the supremum is extended over all half-open subintervals J of $[0,1)^s$, λ_s denotes the s-dimensional Lebesgue measure, and the counting function $A(J,N)$ is given by

$$A(J,N) = \#\{0 \leq n \leq N-1 \ : \ \boldsymbol{z}_n \in J\}.$$

For the sake of simplicity, we will sometimes write D_N instead of $D_N(\boldsymbol{z}_n)$.

It is well known (see [12, Theorem 3.6]) that the discrepancy of the Halton sequence in pairwise coprime bases $b_1, \ldots, b_s \geq 2$ satisfies a low-discrepancy bound, i.e.,

$$D_N(\boldsymbol{y}_n) = O_{b_1,\ldots,b_s}\left((\operatorname{Log} N)^s/N\right) \qquad \text{for all } N \geq 1. \tag{1}$$

The specific construction algorithm implies special regularities in the distribution of the Halton sequence. In Section 3 these regularities are exploited to prove a general discrepancy bound that relates the discrepancy of the hybrid sequence to the discrepancy of arithmetic subsequences of the sequence that is mixed with the Halton sequence. This bound is then applied to the hybrid sequences that were considered in [14, 16, 17, 18, 20] and to some more hybrid sequences that involve recursive pseudorandom number generators. Finally, in Section 4 we briefly discuss possible generalizations for hybrid sequences that are related to recursive generators and we work out the main tasks for the investigation of hybrid sequences that are built from digital sequences and pseudorandom number sequences.

3. Results for hybrid sequences involving Halton sequences

Combining two sequences to obtain a new higher-dimensional one is a sensitive task. Two single sequences can have really good uniform distribution properties, but their mixing can be a catastrophe. Take the easy example where a higher-dimensional sequence is constructed by taking any pseudorandom number sequence and combining it with the same sequence. More subtle examples can be given, for example, in the form of Halton sequences with bases that are not pairwise coprime (see [4, Corollary 2.18]). In this section, we will prove a theorem on hybrid sequences built from a Halton sequence and any other sequence. It states a sufficient condition on the distribution of the sequence that is mixed with a Halton sequence, to get a discrepancy bound for the hybrid sequence.

3.1. A discrepancy bound

For given dimensions s and t, we consider a hybrid sequence $(\boldsymbol{x}_n)_{n\geq 0}$ of points in $[0,1)^{s+t}$ with

$$\boldsymbol{x}_n = (\boldsymbol{y}_n, \boldsymbol{z}_n) \qquad \text{for } n = 0, 1, \ldots, \tag{2}$$

where $(\boldsymbol{y}_n)_{n\geq 0}$ is the s-dimensional Halton sequence in the pairwise coprime bases $b_1, \ldots, b_s \geq 2$ and $(\boldsymbol{z}_n)_{n\geq 0}$ is a sequence of points in $[0,1)^t$.

Theorem 1. *Let T be a positive integer and let $b_1, \ldots, b_s \geq 2$ be pairwise coprime integers. Let $(\boldsymbol{z}_n)_{n\geq 0}$ be a sequence of points in $[0,1)^t$. Suppose that the discrepancy $D_L^{(m,r)}(\boldsymbol{z}_n)$ of the first L terms of every arithmetic subsequence of the form $(\boldsymbol{z}_{mk+r})_{k\geq 0}$, where $m = b_1^{j_1} \cdots b_s^{j_s}$ with integers $j_1, \ldots, j_s \geq 0$ and $0 \leq r < m \leq N$, can be bounded by*

$$LD_L^{(m,r)}(\boldsymbol{z}_n) = O_P(NH(N))$$

for all $1 \leq N \leq T$. Here the implied constant may depend on a set P of some parameters, but is independent of N, m, and r, and $H : \mathbb{N} \to \mathbb{R}^+$ is a suitable function. Furthermore, L stands for

$$L = \left\lfloor \frac{N-r-1}{m} + 1 \right\rfloor.$$

Then the discrepancy of the hybrid sequence $((\boldsymbol{y}_n, \boldsymbol{z}_n))_{n\geq 0}$ satisfies

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s,P}\left(H(N)\left(\operatorname{Log}\frac{1}{H(N)}\right)^s\right) \tag{3}$$

for all $1 \leq N \leq T$, where $(\boldsymbol{y}_n)_{n\geq 0}$ is the s-dimensional Halton sequence in the bases $b_1, \ldots, b_s$.

P r o o f. For a fixed integer N with $1 \le N \le T$, put

$$f_i := \left\lceil \frac{1}{\log b_i} \mathrm{Log} \frac{1}{H(N)} \right\rceil \quad \text{for } 1 \le i \le s. \tag{4}$$

The first aim in the proof is to compute or estimate the counting function $A(J,N)$ relative to the points $\boldsymbol{x}_n$ in (2), where $J \subseteq [0,1)^{s+t}$ is an interval of the form

$$J = \prod_{i=1}^{s} [0, v_i b_i^{-f_i}) \times \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}) \tag{5}$$

with $v_1, \ldots, v_s \in \mathbb{Z}$, $1 \le v_i \le b_i^{f_i}$ for $1 \le i \le s$, and $0 \le w_j^{(1)} < w_j^{(2)} \le 1$ for $1 \le j \le t$.

The crucial step is to exploit special properties of the Halton sequence. By [17, Lemma 3], for any integer $n \ge 0$ we have

$$(\phi_{b_1}(n), \ldots, \phi_{b_s}(n)) \in \prod_{i=1}^{s} [0, v_i b_i^{-f_i}) \text{ if and only if } n \in \bigcup_{k=1}^{M} R_k,$$

where $1 \le M \le b_1 \cdots b_s f_1 \cdots f_s$, each R_k is a residue class in $\mathbb{Z}$, and $R_1, \ldots, R_M$ are (pairwise) disjoint. The moduli m_k of the residue classes R_k are of the form $b_1^{j_1} \cdots b_s^{j_s}$ with integers $1 \le j_i \le f_i$ for $1 \le i \le s$. The sets $R_1, \ldots, R_M$ depend only on $b_1, \ldots, b_s, v_1, \ldots, v_s, f_1, \ldots, f_s$ and are thus independent of n. Furthermore, one can easily prove for the Lebesgue measure of $\prod_{i=1}^{s} [0, v_i b_i^{-f_i})$ that

$$\lambda_s \left(\prod_{i=1}^{s} [0, v_i b_i^{-f_i}) \right) = \prod_{i=1}^{s} v_i b_i^{-f_i} = \sum_{k=1}^{M} \frac{1}{m_k},$$

by applying the uniform distribution of the Halton sequence and the disjointness of $R_1, \ldots, R_M$ (see [17, Proof of Theorem 1]). Now we split up the counting function $A(J,N)$ into M parts as follows: $A(J,N) = \sum_{k=1}^{M} S_k$, where

$$S_k = \# \left\{ 0 \le n \le N-1 : n \equiv r_k \pmod{m_k} \text{ and } \boldsymbol{z}_n \in \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}) \right\}$$

with moduli $m_1, \ldots, m_M$ and residues $0 \le r_k < m_k$ for $1 \le k \le M$. The next step uses the assumption on the discrepancy of the arithmetic subsequences of $(\boldsymbol{z}_n)_{n \ge 0}$. We fix k with $1 \le k \le M$ for the moment. Assume first that $N \ge m_k$. We can write S_k as follows:

$$S_k = \# \left\{ 0 \le l \le \left\lfloor \frac{N - r_k - 1}{m_k} \right\rfloor \ : \ \boldsymbol{z}_{m_k l + r_k} \in \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}) \right\}$$

$$= \left\lfloor \frac{N - r_k - 1 + m_k}{m_k} \right\rfloor \left(\prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) \right) + O\left(\left\lfloor \frac{N - r_k - 1 + m_k}{m_k} \right\rfloor D^{(m_k, r_k)}_{\lfloor (N - r_k - 1 + m_k)/m_k \rfloor}(\boldsymbol{z}_n) \right).$$

Note that if $N < m_k$, then $S_k = 0$ or 1, and so in this case the above identity holds with an error term $O(1)$. Hence with $L_k = \lfloor (N - r_k - 1 + m_k)/m_k \rfloor$ for $1 \le k \le M$ we obtain

$$\begin{aligned} A(J,N) &= N \left(\prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) \right) \sum_{k=1}^{M} \frac{1}{m_k} + O(M) \\ &\quad + O\left(\sum_{\substack{k=1 \\ N \ge m_k}}^{M} L_k D^{(m_k, r_k)}_{L_k}(\boldsymbol{z}_n) \right) \\ &= N \left(\prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) \right) \prod_{i=1}^{s} v_i b_i^{-f_i} + O_P\left(NH(N)M\right) \\ &= N\lambda_{s+t}(J) + O_P\left(NH(N) b_1 \cdots b_s f_1 \cdots f_s\right). \end{aligned}$$

Substituting the values of the f_i from (4), we arrive at

$$|A(J,N) - N\lambda_{s+t}(J)| = O_{b_1,\ldots,b_s,P}\left(NH(N) \left(\operatorname{Log} \frac{1}{H(N)} \right)^{s} \right). \tag{6}$$

An arbitrary interval $I \subseteq [0,1)^{s+t}$ of the form

$$I = \prod_{i=1}^{s} [0, w_i) \times \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}) \tag{7}$$

with $0 < w_i \le 1$ for $1 \le i \le s$ and $0 \le w_j^{(1)} < w_j^{(2)} \le 1$ for $1 \le j \le t$ can be approximated from below and above by an interval J of the form (5), by taking the nearest fraction to the left and to the right, respectively, of w_i of the form $v_i b_i^{-f_i}$ with $v_i \in \mathbb{Z}$. We easily get

$$|A(I,N) - N\lambda_{s+t}(I)| \le N \sum_{i=1}^{s} b_i^{-f_i} + |A(J,N) - N\lambda_{s+t}(J)|.$$

The definition of the f_i in (4) yields $f_i \geq \log_{b_i}(1/H(N))$. Therefore $Nb_i^{-f_i} \leq NH(N)$, and using (6) we obtain

$$|A(I,N) - N\lambda_{s+t}(I)| = O_{b_1,\ldots,b_s,P}\left(NH(N)\left(\mathrm{Log}\frac{1}{H(N)}\right)^s\right).$$

Finally, we use the standard method of moving from intervals of the form (7) to arbitrary half-open subintervals of $[0,1)^{s+t}$ (see [7, p. 93, Example 1.2]). This produces an additional factor 2^s in the discrepancy bound and yields the desired result. □

Remark 1. Using the trivial bound $\frac{1}{N} \leq D_N(\boldsymbol{z}_n) \leq CH(N)$, we get $\frac{1}{H(N)} \leq CN$. Applying this inequality to (3), we obtain

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s,P}\left(H(N)(\mathrm{Log}N)^s\right).$$

This bound is usually as strong as the bound in (3) and easier to understand.

In the next subsection, we apply Theorem 1 to various hybrid sequences involving Halton sequences.

3.2. Applications of Theorem 1

The probably most basic example of a hybrid sequence as treated in Theorem 1 is an $(s+1)$-dimensional Halton sequence in the pairwise coprime bases $b_1,\ldots,b_{s+1} \geq 2$. We interpret this sequence as a combination of an s-dimensional Halton sequence in the pairwise coprime bases $b_1,\ldots,b_s$ with a one-dimensional Halton sequence in base b_{s+1}, satisfying $\gcd(b_{s+1}, b_i) = 1$ for all $1 \leq i \leq s$. It follows from (1) that the one-dimensional Halton sequence in base b_{s+1} satisfies $ND_N = O_{b_{s+1}}(\mathrm{Log}N)$ for all $N \geq 1$. In [6] it was proved that any subsequence $(\phi_{b_{s+1}}(b_1^{j_1}\cdots b_s^{j_s}l + r))_{l\geq 0}$ satisfies $LD_L = O_{b_{s+1}}(\mathrm{Log}\, L)$. Now we can apply Theorem 1 and we obtain for the $(s+1)$-dimensional Halton sequence the well-known discrepancy bound

$$ND_N = O_{b_1,\ldots,b_s,b_{s+1}}\left((\mathrm{Log}N)\left(\mathrm{Log}\frac{N}{\mathrm{Log}N}\right)^s\right) = O_{b_1,\ldots,b_s,b_{s+1}}\left((\mathrm{Log}N)^{s+1}\right).$$

The following examples overview the results obtained by Niederreiter for different hybrid sequences that can be proved by applying Theorem 1, once the assumption on the discrepancy of arithmetic subsequences is verified. Throughout the remainder of the paper, $\mathbb{F}_p$ denotes the finite field with p elements, where p is a prime number. We can identify $\mathbb{F}_p$ with the least residue system $\mathbb{Z}_p$ modulo p. Some of the sequences are defined using polynomials with coefficients in $\mathbb{F}_p$; we denote for short $\mathbb{F}_p[X]$ the ring of univariate polynomials with coefficients in $\mathbb{F}_p$. In the first examples, we are going to review results given in [17, 18].

Example 1 (Linear recursive pseudorandom sequence)**.** Let $p \geq 3$ be a prime, let $g \in \mathbb{Z}$ with $2 \leq g < p$, and let $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. We set $\boldsymbol{z}_n := \{g^n a/p\}$. Suppose $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$, where τ is the multiplicative order of g modulo p and therefore the period of the sequence $(\boldsymbol{z}_n)_{n \geq 0}$. Then for $1 \leq N \leq \tau$ the discrepancy $D_N((\boldsymbol{y}_n, \boldsymbol{z}_n))$ satisfies

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s}\left(\frac{p^{1/2}(\log p)\log \tau}{N}\left(\mathrm{Log}\frac{N}{p^{1/2}(\log p)\log \tau}\right)^s\right).$$

The bound on the discrepancy of this pseudorandom generator, namely

$$N D_N(\boldsymbol{z}_n) = O(p^{1/2}(\log p)\log \tau),$$

also holds for the arithmetic subsequences

$$\boldsymbol{z}_{ml+r} = \{a g^{ml+r}/p\} = \{a g^r (g^m)^l/p\} =: \boldsymbol{z}'_l \qquad \text{for } l = 0, 1, \ldots,$$

i.e.,

$$L D_L(\boldsymbol{z}'_l) = O\left(p^{1/2}(\log p)\log \tau\right)$$

(see the proof of [14, Theorem 3]), and the result follows from Theorem 1. Notice that the bound for the discrepancy of the subsequence holds because $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$, therefore $\gcd(m, \tau) = 1$ and the multiplicative order of g^m modulo p is also τ.

Example 2 (Inversive pseudorandom sequence)**.** Let $p \geq 3$ be a prime, let $(c_n)_{n \geq 0}$ be an inversive generator in $\mathbb{F}_p$ (modified in the sense of Niederreiter and Rivat [19]) with least period τ, and set $\boldsymbol{z}_n := c_n/p$. In the proof of [14, Theorem 5] the following bound was given for the discrepancy of the arithmetic subsequences,

$$D_L^{(m,r)}(\boldsymbol{z}_n) = O\left(\frac{p^{1/4}\log p}{L^{1/2}}\right).$$

This bound and Theorem 1 yield for $1 \leq N \leq \tau$,

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s}\left(\frac{p^{1/4}\log p}{N^{1/2}}\left(\mathrm{Log}\frac{N^{1/2}}{p^{1/4}\log p}\right)^s\right).$$

Example 3 (Nonlinear congruential pseudorandom sequence)**.** Assume $p \geq 3$ prime, $\gcd(b_i, p) = 1$ for $1 \leq i \leq s$, and choose polynomials $g_1, \ldots, g_t \in \mathbb{F}_p[X]$ such that $\deg(g_j) < p$ for $1 \leq j \leq t$ and $1, X, g_1(X), \ldots, g_t(X)$ are linearly independent over $\mathbb{F}_p$. We put $G := \max(\deg(g_1), \ldots, \deg(g_t))$ and define $\boldsymbol{z}_n := (g_1(n)/p, \ldots, g_t(n)/p)$. Then for $1 \leq N \leq p$,

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s,t}\left(\frac{G p^{1/2}(\log p)^{t+1}}{N}\left(\mathrm{Log}\frac{N}{G p^{1/2}(\log p)^{t+1}}\right)^s\right).$$

The bound for the discrepancy of the arithmetic subsequences was given in [16, Proof of Theorem 2], i.e., $LD_L^{(m,r)}(\boldsymbol{z}_n) = O_t\left(Gp^{1/2}(\log p)^{t+1}\right)$.

Example 4 (Explicit inversive pseudorandom sequence)**.** Let $p \geq 5$ be a prime, assume $\gcd(b_i, p) = 1$ for $1 \leq i \leq s$, and let $a_1, \ldots, a_t$ be nonzero elements of $\mathbb{F}_p$ and $d_1, \ldots, d_t \in \mathbb{F}_p$ be such that $d_1 a_1^{p-2}, \ldots, d_t a_t^{p-2}$ are distinct elements of $\mathbb{F}_p$. Defining $\boldsymbol{z}_n := (e_n^{(1)}/p, \ldots, e_n^{(t)}/p)$, where $e_n^{(j)} = (a_j n + d_j)^{p-2}$, the following holds for all $1 \leq N \leq p$,

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s,t}\left(\frac{p^{1/2}(\log p)^{t+1}}{N}\left(\mathrm{Log}\frac{N}{p^{1/2}(\log p)^{t+1}}\right)^s\right).$$

The bound for the discrepancy of the arithmetic subsequences was given in [16, Proof of Theorem 4], i.e., $LD_L^{(m,r)}(\boldsymbol{z}_n) = O_t\left(p^{1/2}(\log p)^{t+1}\right)$.

Example 5 (Digital explicit inversive sequence)**.** Let $q = p^k \geq 3$, where p is a prime and k is a positive integer. We choose digital explicit inversive pseudorandom numbers $z_0, z_1, \ldots$ of order $T \geq 2$ defined in [8]. Assume that $\gcd(b_i, T) = 1$ for $1 \leq i \leq s$. For a dimension t such that $1 \leq t \leq T$, choose integers $0 \leq d_1 < d_2 < \cdots < d_t < T$ and set $\boldsymbol{z}_n := (z_{n+d_1}, \ldots, z_{n+d_t})$. Then for $1 \leq N \leq T$ the discrepancy of the first N terms of the sequence $((\boldsymbol{y}_n, \boldsymbol{z}_n))_{n\geq 0}$ satisfies

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s,t}\left(\frac{q^{1/2}(\log q)^t \log T}{N}\left(\mathrm{Log}\frac{N}{q^{1/2}(\log q)^t \log T}\right)^s\right).$$

The bound for the discrepancy of the arithmetic subsequences was given in [20, Proof of Theorem 3], i.e., $LD_L^{(m,k)}(\boldsymbol{z}_n) = O_t\left(q^{1/2}(\log q)^t \log T\right)$.

Remark 2. In some cases the bound known for the discrepancy of the arithmetic subsequences is of a different nature, and then the method of proof of Theorem 1 can be adapted depending on the specific bound. This is the case, for example, for hybrid sequences involving matrix-method pseudorandom vectors, see [17, Theorem 1] and its proof. Let $p \geq 19$ be a prime and let $t \geq 1$ be a given dimension such that $\gcd(b_i, p^t - 1)$ for all $1 \leq i \leq s$. Let $(\boldsymbol{z}_n)_{n\geq 0}$ be a sequence of t-dimensional matrix-method pseudorandom vectors of maximum period $p^t - 1$. Then for $1 \leq N \leq p^t - 1$ the discrepancy of the corresponding hybrid sequence satisfies

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O\left(\frac{2^s t}{p}\right) + O_{b_1,\ldots,b_s}\left(\frac{p^{t/2}(\log p)^{t+1}}{N}\left(\mathrm{Log}\frac{N}{p^{t/2}(\log p)^{t+1}}\right)^s\right).$$

The discrepancy of the arithmetic subsequences satisfies

$$LD_L^{(m,r)}(\boldsymbol{z}_n) = O\left(Ltp^{-1} + p^{t/2}(\log p)^{t+1}\right).$$

In the following two examples, we consider hybrid sequences of Halton sequences and one-dimensional sequences that are related to recursive pseudorandom number generators and that have not been considered before.

Example 6 (Nonlinear recursive pseudorandom number generator)**.** Let $p \geq 3$ be a prime and $f(X) \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. We define $(\boldsymbol{z}_n) := (u_n/p)$, where

$$u_n = f(u_{n-1}) \qquad \text{for } n = 1, 2, \ldots$$

and $u_0 \in \mathbb{F}_p$ is an arbitrary element called the seed. The sequence $(u_n)_{n\geq 0}$ is called a nonlinear recursive pseudorandom number generator. We denote by τ the period of the sequence and we assume that the sequence is purely periodic. Let $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$. Then the discrepancy of the hybrid sequence satisfies

$$\begin{aligned} &D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) \\ &\quad = \quad O_{b_1,\ldots,b_s}\left((\log d)^{1/2}\frac{p^{1/2}\log\log p}{N^{1/2}(\log p)^{1/2}}\left(\mathrm{Log}\frac{N^{1/2}(\log p)^{1/2}}{(\log d)^{1/2}p^{1/2}\log\log p}\right)^s\right) \end{aligned}$$

for $1 \leq N \leq \tau$. To prove this result, we note that for the discrepancy of the pseudorandom component we find in [26, Theorem 4.1] and its proof that for $1 \leq N \leq \tau$ we have

$$D_N(\boldsymbol{z}_n) = O\left((\log d)^{1/2}\frac{p^{1/2}\log\log p}{N^{1/2}(\log p)^{1/2}}\right)$$

with an absolute implied constant. Now an arithmetic subsequence of a purely periodic sequence is obviously purely periodic as well. Furthermore, the assumption $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$ ensures that the subsequences $(\boldsymbol{z}_{ml+r})_{l\geq 0}$ have the same period τ. Only the degree of the polynomial $g(X) \in \mathbb{F}_p[X]$, the polynomial obtained by composing $f(X)$ m times with itself, differs and it is d^m. Therefore

$$\begin{aligned} LD_L^{(m,r)}(\boldsymbol{z}_n) &= O\left(L(\log d^m)^{1/2}\frac{p^{1/2}\log\log p}{L^{1/2}(\log p)^{1/2}}\right) \\ &= O\left(L^{1/2}m^{1/2}(\log d)^{1/2}\frac{p^{1/2}\log\log p}{(\log p)^{1/2}}\right) \\ &= O\left(N^{1/2}(\log d)^{1/2}\frac{p^{1/2}\log\log p}{(\log p)^{1/2}}\right) = O(NH(N)). \end{aligned}$$

The rest follows by applying Theorem 1.

The class of nonlinear recursive pseudorandom number generators is very general, which is the reason why the discrepancy bound in Example 6 is very

weak. Nevertheless, for small degree d and period $\tau \approx p$ and $N \approx p$, we obtain nontrivial bounds in p of the form $(\log\log p)^{s+1}/(\log p)^{1/2}$. The bound can be improved for specific choices of the polynomial $f(X)$. For the formulation of the following example, we make use of the multiplicative order of an integer a modulo $q \geq 2$, which we abbreviate by $t_q(a)$.

Example 7 (Power generator)**.** We take $f(X) = X^e \in \mathbb{F}_p[X]$, with $e \geq 2$ and a seed $u_0 \in \{2, \ldots, p-1\}$. We assume that the sequence $(e^n)_{n\geq 0}$ is purely periodic modulo $T = t_p(u_0)$ with period $\tau = t_T(e)$. Furthermore, let $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$ and let $\gcd(e, T) = 1$. Let $(\boldsymbol{z}_n)_{n\geq 0} = (u_0^{e^n}/p)_{n\geq 0}$ be the sequence of pseudorandom numbers obtained by this power generator. Then for every positive integer ν, the discrepancy of the hybrid sequence satisfies

$$D_N((\boldsymbol{y}_n, \boldsymbol{z}_n)) = O_{b_1,\ldots,b_s,\nu}\left(N^{-(2\nu+1)/(2\nu(\nu+1))}T^{1/(2\nu)}p^{1/(4\nu+4)+o(1)}\right)$$

for $1 \leq N \leq \tau$, where $o(1)$ denotes the small o of Landau. For the proof, we note that in [24, Corollary 3] a bound for the discrepancy of the power generator was given:

$$D_N(\boldsymbol{z}_n) = O_\nu\left(N^{-(2\nu+1)/(2\nu(\nu+1))}T^{1/(2\nu)}p^{1/(4\nu+4)+o(1)}\right).$$

Next we verify that $T = t_p(u_0) = t_p(u_0^{e^r})$ for any integer $r \geq 0$. Suppose that for $k \in \mathbb{N}$ we have $u_0^{e^r k} \equiv 1 \pmod{p}$. From $\gcd(e, T) = \gcd(e^r, T) = 1$ we find $x, y \in \mathbb{Z}$ and $x > 0$ satisfying $xe^r + yT = 1$. Now

$$1 \equiv u_0^{e^r k} \equiv u_0^{e^r kx} = u_0^{k-yTk} \equiv u_0^k \pmod{p}$$

and therefore $t_p(u_0)|t_p(u_0^{e^r})$. For $k \in \mathbb{N}$ such that $u_0^k \equiv 1 \pmod{p}$, we trivially have $u_0^{e^r k} \equiv 1 \pmod{p}$ and $t_p(u_0^{e^r})|t_p(u_0)$. Hence indeed $t_p(u_0^{e^r}) = T$. Furthermore, $\gcd(e^m, T) = 1$ since $\gcd(e, T) = 1$. Finally, the assumption $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$ ensures that the subsequence $(\boldsymbol{z}_{ml+r})_{l\geq 0} = (u_0^{e^r(e^m)^l}/p)_{l\geq 0}$ is again a purely periodic power generator with the same period τ as the sequence $(\boldsymbol{z}_n)_{n\geq 0}$. Altogether we have

$$LD_L^{(m,r)}(\boldsymbol{z}_n) = O_\nu\left(N^{1-(2\nu+1)/(2\nu(\nu+1))}T^{1/(2\nu)}p^{1/(4\nu+4)+o(1)}\right).$$

An application of Theorem 1 yields the desired result. Note that the term $(\mathrm{Log}(1/H(N)))^s$ can be bounded by p^ε for p big enough and can therefore be absorbed into the term $p^{o(1)}$.

4. Discussions

This paper concentrates on hybrid sequences where the QMC component sequence is a Halton sequence. A very interesting question is the following: what happens if other QMC component sequences are used together with various pseudorandom number sequences to build a hybrid sequence? Niederreiter considered also hybrid sequences that are built from Kronecker sequences and pseudorandom number generators, see [14, 15, 16, 20]. Another interesting class of hybrid sequences can be built by combining different examples of digital (u, s)-sequences, as the ones introduced in [2, 9, 10, 11], and various pseudorandom number generators. It is well known that a digital (u, s)-sequence $(\boldsymbol{z}_n)_{n\geq 0}$ over $\mathbb{F}_p$ satisfies $ND_N(\boldsymbol{z}_n) = O_{s,u,p}((\mathrm{Log}N)^s)$. It is natural to apply a method similar to the one in the proof of Theorem 1 to investigate the discrepancy of such hybrid sequences. Within this method, the main task will be to get good discrepancy bounds on certain subsequences of the pseudorandom number sequence. For the Halton component sequence, these subsequences are special arithmetic ones. For a digital (u, s)-sequence over a finite prime field $\mathbb{F}_p$, these subsequences $(\boldsymbol{z}_{k_l})_{l\geq 0}$ will be based on index sequences $(k_l)_{l\geq 0}$ that are solutions of systems of congruences in increasing order as described in the following.

Let $z \in \mathbb{N}$ and let $\mathbb{F}_p^{\mathbb{N}_0}$ be the direct product of denumerably many copies of $\mathbb{F}_p$. For every integer i with $1 \leq i \leq z$, we are given the following congruence over $\mathbb{F}_p^{\mathbb{N}_0}$,

$$(\rho_0^{(i)}, \rho_1^{(i)}, \ldots) \cdot (x_0, x_1, \ldots)^{\mathrm{T}} = b^{(i)}$$

with fixed $b^{(i)} \in \mathbb{F}_p$ and fixed $\rho_h^{(i)} \in \mathbb{F}_p$ for all $h \geq 0$. We call a nonnegative integer n a "solution" of this system of congruences if the base p digit vector $(n_0, n_1, n_2, \ldots)^{\mathrm{T}}$ of n solves all the z given congruences over $\mathbb{F}_p^{\mathbb{N}_0}$. Bearing in mind that the system of congruences is related to the digital (u, s)-sequence over $\mathbb{F}_p$, we can assume that if we regard a set of p^{z+u} consecutive integers of the form $\{mp^{z+u}, mp^{z+u} + 1, \ldots, mp^{z+u} + p^{z+u} - 1\}$, where m is a nonnegative integer, then exactly p^u elements of this set solve the system of congruences. Now we give some examples of such systems and the corresponding subsequence.

(1) If $z = 1$ and if $(\rho_0^{(1)}, \rho_1^{(1)}, \ldots) = (1, 0, 0, \ldots)$ then the subsequence $(\boldsymbol{z}_{k_l})_{l\geq 0}$ is given by $(\boldsymbol{z}_{pl+b^{(1)}})_{l\geq 0}$, which is an arithmetic subsequence.

(2) If $z = 1$, if $(\rho_0^{(1)}, \rho_1^{(1)}, \ldots) = (1, 1, 1, \ldots)$, and if $b^{(1)} = 0$, then the subsequence $(\boldsymbol{z}_{k_l})_{l\geq 0}$ is indexed by all integers k_l for which the base p sum of digits is a multiple of p.

(3) If $z = 1$ and if $b^{(1)} = 0$, then the subsequence $(\boldsymbol{z}_{k_l})_{l\geq 0}$ is indexed by all integers k_l for which the weighted base p sum of digits is a multiple of p, where the weights are given by the sequence $(\rho_r^{(1)})_{r\geq 0}$.

The distribution properties of arithmetic subsequences are, in some cases, not too difficult to study. But subsequences that are indexed by solutions of systems of congruences are much more involved. Such subsequences were studied, for example, for Niederreiter-Halton sequences [5], but rarely for pseudorandom number generators.

Another challenging problem is to extend the results given in Examples 6 and 7 to multidimensional versions of the pseudorandom component sequences. To obtain results on the discrepancy of such hybrid sequences, it is necessary to give bounds on the discrepancy of sequences of the form

$$(\boldsymbol{z}_{ml+d_1}, \ldots, \boldsymbol{z}_{ml+d_t}) \qquad \text{for } 1 \leq l \leq L,$$

where $d_1, \ldots, d_t$ are distinct nonnegative integers. The values $d_1, \ldots, d_t$ are called lags, and without any restriction on the lags a bound is difficult to obtain. One possibility is to repeat the proof of Theorem 1 and select the f_i small enough such that $d_1, \ldots, d_t$ are bounded, but this will increase the upper bound for the hybrid sequence. Another way to treat general values for the dimension t is to consider multidimensional versions of the pseudorandom number sequences proposed in Examples 6 and 7. A generalization for the nonlinear recursive pseudorandom number sequence is given in [23] and a multidimensional generalization for the power generator can be found in [24], but the discrepancy bounds for those generators are weaker compared to other multidimensional generators.

REFERENCES

[1] DICK, J. – PILLICHSHAMMER, F.: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, Cambridge, 2010.

[2] FAURE, H.: *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. **41** (1982), 337–351.

[3] GNEWUCH, M.: *On probabilistic results for the discrepancy of a hybrid-Monte Carlo sequence*, J. Complexity **25** (2009), 312–317.

[4] HELLEKALEK, P. – NIEDERREITER, H.: *Constructions of uniformly distributed sequences using the* **b***-adic method*, Unif. Distrib. Theory **6** (2011), 185–200.

[5] HOFER, R.: *On subsequences of Niederreiter-Halton sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 2008 (Pierre L' Ecuyer and Art B. Owen, eds.), pp. 423–438, Springer, Berlin, Heidelberg, 2009.

[6] HOFER, R. – KRITZER, P. – LARCHER, G. – PILLICHSHAMMER, F.: *Distribution properties of generalized van der Corput-Halton sequences and their subsequences*, Int. J. Number Theory **5** (2009), 719–746.

[7] KUIPERS, L. – NIEDERREITER, H.: *Uniform Distribution of Sequences*, Wiley, New York, 1974; reprint, Dover Publications, Mineola, NY, 2006.
[8] MEIDL, W. – WINTERHOF, A.: *On the linear complexity profile of some new explicit inversive pseudorandom numbers*, J. Complexity **20** (2004), 350–355.
[9] NIEDERREITER, H.: *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273–337.
[10] NIEDERREITER, H.: *Low-discrepancy and low-dispersion sequences*, J. Number Theory **30** (1988), 51–70.
[11] NIEDERREITER, H.: *Quasi-Monte Carlo methods for multidimensional numerical integration*, in: Proc. Conf. Oberwolfach/FRG 1987, ISNM Vol. 85, pp. 157–171, Birkhäuser, Basel, 1988.
[12] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.
[13] NIEDERREITER, H.: *High-dimensional numerical integration*, in: Applied Mathematics Entering the 21st Century. Papers from the 5th International Congress on Industrial and Applied Mathematics (ICIAM 2003) (James M. Hill, ed.), pp. 337–351, Society for Industrial and Applied Mathematics (SIAM), 2004.
[14] NIEDERREITER, H.: *On the discrepancy of some hybrid sequences*, Acta Arith. **138** (2009), 373–398.
[15] NIEDERREITER, H.: *A discrepancy bound for hybrid sequences involving digital explicit inversive pseudorandom numbers*, Unif. Distrib. Theory **5** (2010), 53–63.
[16] NIEDERREITER, H.: *Further discrepancy bounds and an Erdős-Turán-Koksma inequality for hybrid sequences*, Monatsh. Math. **161** (2010), 193–222.
[17] NIEDERREITER, H.: *Discrepancy bounds for hybrid sequences involving matrix-method pseudorandom vectors*, Publ. Math. Debrecen **79** (2011), 589–603.
[18] NIEDERREITER, H.: *Improved discrepancy bounds for hybrid sequences involving Halton sequences*, Acta Arith. **155** (2012), 71–84.
[19] NIEDERREITER, H. – RIVAT, J.: *On the correlation of pseudorandom numbers generated by inversive methods*, Monatsh. Math. **153** (2008), 251–264.
[20] NIEDERREITER, H. – WINTERHOF, A.: *Discrepancy bounds for hybrid sequences involving digital explicit inversive pseudorandom numbers*, Unif. Distrib. Theory **6** (2011), 33–56.
[21] ÖKTEN, G.: *A probabilistic result on the discrepancy of a hybrid-Monte Carlo sequence and applications*, Monte Carlo Methods Appl. **2** (1996), 255–270.
[22] ÖKTEN, G. – TUFFIN, B. – BURAGO, V.: *A central limit theorem and improved error bounds for a hybrid-Monte Carlo sequence with applications in computational finance*, J. Complexity **22** (2006), 435–458.
[23] OSTAFE, A. – PELICAN, E. – SHPARLINSKI, I.: *On pseudorandom numbers from multivariate polynomial systems*, Finite Fields Appl. **16** (2010), 320–328.
[24] OSTAFE, A. – SHPARLINSKI, I.: *On the power generator and its multivariate analogue*, J. Complexity **28** (2012), 238-249.
[25] SPANIER, J.: *Quasi-Monte Carlo methods for particle transport problems*, in: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing (H. Niederreiter and P.J.-S. Shiue, eds.), Lecture Notes in Statistics, Vol. **106**, pp. 121–148, Springer, New York, 1995.

[26] TOPUZOĞLU, A. – WINTERHOF, A.: *Pseudorandom sequences*, in: Topics in geometry, coding theory and cryptography (Garcia, Arnaldo et al., eds.), Algebra and Applications Vol. **6**, pp. 135–166, Springer, Dordrecht, 2007.

Received May 29, 2012
Accepted June 16, 2012

Domingo Gómez-Pérez
University of Cantabria,
Avd. de los Castros s/n,
Santander, SPAIN
E-mail: domingo.gomez@unican.es

Roswitha Hofer
Institute of Financial Mathematics,
University of Linz,
Altenbergerstr. 69,
A-4040 Linz, AUSTRIA.
E-mail: roswitha.hofer@jku.at

Harald Niederreiter
Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences,
Altenbergerstr. 69,
A-4040 Linz, AUSTRIA.
E-mail: ghnied@gmail.com