ACTA ARITHMETICA
155.1 (2012)

Improved discrepancy bounds for hybrid sequences involving Halton sequences

by

Harald Niederreiter (Linz and Dhahran)

Dedicated to Professor Andrzej Schinzel on his 75th birthday

1. Introduction. A *hybrid sequence* is a sequence of points in an m-dimensional unit cube that is obtained by "mixing" two different types of lower-dimensional sequences, in the sense that certain coordinates of the m-dimensional points stem from the first type of sequence and the remaining coordinates of the m-dimensional points stem from the second type of sequence. In many cases of practical interest, one lower-dimensional sequence is a low-discrepancy sequence and the other is a sequence of pseudorandom numbers (or vectors). Hybrid sequences go back to a proposal of Spanier [15] in the context of multidimensional numerical integration by Monte Carlo and quasi-Monte Carlo methods (see [11] for a recent survey of these methods).

A classical family of low-discrepancy sequences is formed by Halton sequences (see Section 2 for the definition). It is therefore of great interest to study hybrid sequences involving Halton sequences as one constituent. Discrepancy bounds for hybrid sequences involving Halton sequences have been established in [9], [10], and [13]. In the present paper, we introduce a new method for dealing with hybrid sequences involving Halton sequences which leads in several cases to substantial improvements on the previous discrepancy bounds for such sequences.

For an integer $m \geq 1$, let λ_m denote the m-dimensional Lebesgue measure. For arbitrary points $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1} \in [0,1)^m$, their *discrepancy* D_N is defined by

$$D_N = \sup_J \left| \frac{A(J;N)}{N} - \lambda_m(J) \right|,$$

where the supremum is extended over all half-open subintervals J of $[0,1)^m$

2010 *Mathematics Subject Classification*: 11K38, 11K45, 65C05, 65C10.
Key words and phrases: discrepancy, hybrid sequence, Halton sequence, Kronecker sequence, pseudorandom numbers.

DOI: 10.4064/aa155-1-7 © Instytut Matematyczny PAN, 2012

and the counting function $A(J;N)$ is given by

$$A(J;N) = \#\{0 \le n \le N-1 : \mathbf{y}_n \in J\}. \tag{1}$$

Note that we always have $ND_N \ge 1$ (see [5, p. 93]) and $D_N \le 1$. Throughout the paper, we use the convention that the parameters on which the implied constant in a Landau symbol O depends are written in the subscript of O. A symbol O without a subscript indicates an absolute implied constant.

In Section 2 we review Halton sequences and prove the basic lemmas for our new method. In Section 3 we apply the new method to hybrid sequences obtained by "mixing" Halton sequences and Kronecker sequences. We also prove a multidimensional version of the classical lower bound of Behnke [2] for the discrepancy of one-dimensional Kronecker sequences. In Sections 4 to 6 we establish improved discrepancy bounds for hybrid sequences obtained by "mixing" Halton sequences with various types of sequences of pseudorandom numbers.

2. Halton sequences. 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 digit expansion of the integer $n \ge 0$ in base b. The *radical-inverse function* ϕ_b in base b is defined by

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

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

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

It is a classical low-discrepancy sequence (see [7, Section 3.1]).

LEMMA 1. *Let $b \ge 2$ be an integer and let v and f be positive integers with $v \le b^f$. Then for any integer $n \ge 0$, we have $\phi_b(n) \in [0, vb^{-f})$ if and only if $n \in \bigsqcup_{k=1}^{m} Q_k$, where $1 \le m \le bf$, each Q_k is a residue class in $\mathbb{Z}$, and $Q_1, \ldots, Q_m$ are disjoint. The moduli of the residue classes are powers b^j with $1 \le j \le f$. The sets $Q_1, \ldots, Q_m$ depend only on b, v, and f.*

Proof. We write $(v-1)b^{-f} = \sum_{j=1}^{f} d_j b^{-j}$ with $d_j \in \mathbb{Z}_b$ for $1 \le j \le f$. Then $\phi_b(n) \in [0, vb^{-f})$ if and only if

$$\sum_{j=1}^{f} a_j(n) b^{-j} \le \sum_{j=1}^{f} d_j b^{-j}.$$

This condition holds if and only if one of the following f mutually exclusive conditions is satisfied: (C_1) $a_1(n) \le d_1 - 1$; (C_2) $a_1(n) = d_1$ and $a_2(n) \le$

$d_2 - 1$; (C_3) $a_1(n) = d_1$, $a_2(n) = d_2$, and $a_3(n) \le d_3 - 1$;...; (C_f) $a_1(n) = d_1, \dots, a_{f-1}(n) = d_{f-1}$, and $a_f(n) \le d_f$. These conditions can be translated into the following congruence conditions on n: (C'_1) $n \equiv r_1 \pmod b$ for some $0 \le r_1 \le d_1 - 1$; (C'_2) $n \equiv d_1 + r_2 b \pmod{b^2}$ for some $0 \le r_2 \le d_2 - 1$; (C'_3) $n \equiv d_1 + d_2 b + r_3 b^2 \pmod{b^3}$ for some $0 \le r_3 \le d_3 - 1$;...; (C'_f) $n \equiv d_1 + d_2 b + \cdots + d_{f-1} b^{f-2} + r_f b^{f-1} \pmod{b^f}$ for some $0 \le r_f \le d_f$. This yields disjoint residue classes $Q_1, \dots, Q_m$ in which n must lie. The number m of residue classes satisfies $m = \sum_{j=1}^{f-1} d_j + d_f + 1 \le (b-1)f + 1 \le bf$, whence the result. ∎

The following multidimensional version of Lemma 1 is obtained by combining the Chinese remainder theorem with Lemma 1.

LEMMA 2. *Let $b_1, \dots, b_s \ge 2$ be pairwise coprime integers and let $v_1, \dots, v_s$ and $f_1, \dots, f_s$ be positive integers with $v_i \le b_i^{f_i}$ for $1 \le i \le s$. Then for any integer $n \ge 0$, we have*

$$(\phi_{b_1}(n), \dots, \phi_{b_s}(n)) \in \prod_{i=1}^{s} [0, v_i b_i^{-f_i})$$

if and only if $n \in \bigsqcup_{k=1}^{M} R_k$, 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 $R_1, \dots, R_M$ are disjoint. The moduli of the residue classes are of the form $b_1^{j_1} \cdots b_s^{j_s}$ with $1 \le j_i \le f_i$ for $1 \le i \le s$. The sets $R_1, \dots, R_M$ depend only on $b_1, \dots, b_s, v_1, \dots, v_s, f_1, \dots, f_s$.

3. Mixing Halton sequences and Kronecker sequences. A *Kronecker sequence* is a sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \dots$, of fractional parts, where $\boldsymbol{\alpha} \in \mathbb{R}^t$ for an arbitrary dimension $t \ge 1$. The discrepancy of this sequence depends on the (simultaneous) diophantine approximation character of $\boldsymbol{\alpha}$. The following definition is relevant here (see e.g. [6, Definition 6.1]). We write $\|u\| = \min(\{u\}, 1 - \{u\})$ for the distance from $u \in \mathbb{R}$ to the nearest integer. Furthermore, we put

$$r(\mathbf{h}) = \prod_{j=1}^{t} \max(|h_j|, 1) \quad \text{for } \mathbf{h} = (h_1, \dots, h_t) \in \mathbb{Z}^t$$

and we use $\cdot$ for the standard inner product in $\mathbb{R}^t$.

DEFINITION 1. Let τ be a real number. Then $\boldsymbol{\alpha} \in \mathbb{R}^t$ is *of finite type τ* if τ is the infimum of all real numbers σ for which there exists a constant $c = c(\sigma, \boldsymbol{\alpha}) > 0$ such that

$$r(\mathbf{h})^\sigma \|\mathbf{h} \cdot \boldsymbol{\alpha}\| \ge c \quad \text{for all } \mathbf{h} \in \mathbb{Z}^t \setminus \{\mathbf{0}\}.$$

REMARK 1. It is well known that we always have $\tau \ge 1$. There are interesting examples of points $\boldsymbol{\alpha} \in \mathbb{R}^t$ with $\tau = 1$, for instance: (i) $\boldsymbol{\alpha} =$

$(\alpha_1, \ldots, \alpha_t)$ with real algebraic numbers $\alpha_1, \ldots, \alpha_t$ such that $1, \alpha_1, \ldots, \alpha_t$ are linearly independent over $\mathbb{Q}$ (see [14]); (ii) $\boldsymbol{\alpha} = (e^{q_1}, \ldots, e^{q_t})$ with distinct nonzero rational numbers $q_1, \ldots, q_t$ (see [1]).

Now we choose dimensions $s \geq 1$ and $t \geq 1$, pairwise coprime integers $b_1, \ldots, b_s \geq 2$, and $\boldsymbol{\alpha} \in \mathbb{R}^t$. Then we define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), \{n\boldsymbol{\alpha}\}) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots. \tag{2}$$

The following discrepancy bound is an improvement on [9, Theorem 2].

THEOREM 1. *If $b_1, \ldots, b_s \geq 2$ are pairwise coprime integers and $\boldsymbol{\alpha} \in \mathbb{R}^t$ is of finite type τ, then for any integer $N \geq 1$ the discrepancy D_N of the first N terms of the sequence* (2) *satisfies*

$$D_N = O_{b_1,\ldots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{(\tau-1)(st^2-st+t)+st+1}+\varepsilon}) \quad \text{for all } \varepsilon > 0.$$

Proof. The result is trivial for $N = 1$, and so we can assume that $N \geq 2$. Let $A(J; N)$ be the counting function in (1), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in (2). We introduce the positive integers

$$f_i = \left\lceil \frac{1}{(\tau-1)(st^2-st+t)+st+1} \log_{b_i} N \right\rceil \quad \text{for } 1 \leq i \leq s. \tag{3}$$

We first consider an interval $J \subseteq [0,1)^{s+t}$ of the form

$$J = \prod_{i=1}^{s} [0, v_i b_i^{-f_i}) \times \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}) \tag{4}$$

with $v_1, \ldots, v_s \in \mathbb{Z}$, $1 \leq v_i \leq b_i^{f_i}$ for $1 \leq i \leq s$, and $0 \leq w_j^{(1)} < w_j^{(2)} \leq 1$ for $1 \leq j \leq t$. We apply Lemma 2 to a point $\mathbf{x}_n$ in (2). Then we have $\mathbf{x}_n \in J$ if and only if

$$n \in \bigsqcup_{k=1}^{M} R_k \quad \text{and} \quad \{n\boldsymbol{\alpha}\} \in \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}),$$

where M and $R_1, \ldots, R_M$ are as in Lemma 2. Hence we obtain $A(J; N) = \sum_{k=1}^{M} S_k$, where

$$S_k = \#\Big\{0 \leq n \leq N-1 : n \equiv r_k \pmod{m_k} \text{ and } \{n\boldsymbol{\alpha}\} \in \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)})\Big\}$$

with suitable moduli $m_1, \ldots, m_M$ and $0 \leq r_k < m_k$ for $1 \leq k \leq M$.

We consider S_k for a fixed k with $1 \leq k \leq M$. For an n counted by S_k, we have $n = lm_k + r_k$ for some integer l, and the condition $0 \leq n \leq N-1$ is

equivalent to $0 \le l \le \lfloor (N - r_k - 1)/m_k \rfloor$. Assume first that $N \ge m_k$. Then

$$\begin{aligned} S_k &= \#\Big\{0 \le l \le \Big\lfloor \frac{N - r_k - 1}{m_k} \Big\rfloor : \{l m_k \boldsymbol{\alpha} + r_k \boldsymbol{\alpha}\} \in \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)})\Big\} \\ &= \Big\lfloor \frac{N - r_k - 1 + m_k}{m_k} \Big\rfloor \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) \\ &\quad + O\Big(\Big\lfloor \frac{N - r_k - 1 + m_k}{m_k} \Big\rfloor D^{(k)}_{\lfloor (N - r_k - 1 + m_k)/m_k \rfloor} \Big), \end{aligned}$$

where $D_L^{(k)}$ denotes the discrepancy of the L points $\{l m_k \boldsymbol{\alpha} + r_k \boldsymbol{\alpha}\}$, $l = 0, 1, \ldots, L-1$. Since

$$\Big\lfloor \frac{N - r_k - 1 + m_k}{m_k} \Big\rfloor \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) = \frac{N}{m_k} \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) + O(1),$$

it follows that

$$\begin{aligned} S_k &= \frac{N}{m_k} \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) \\ &\quad + O\Big(\Big\lfloor \frac{N - r_k - 1 + m_k}{m_k} \Big\rfloor D^{(k)}_{\lfloor (N - r_k - 1 + m_k)/m_k \rfloor} \Big). \end{aligned} \tag{5}$$

Now fix an $\varepsilon > 0$. Then by [9, Lemmas 1 and 6] we have

$$L D_L^{(k)} = O_{\boldsymbol{\alpha}, \varepsilon}(m_k^t L^{1 - 1/((\tau-1)t+1) + \varepsilon/2}) \quad \text{for all } L \ge 1.$$

With $L = \lfloor (N - r_k - 1 + m_k)/m_k \rfloor = O(m_k^{-1} N)$ this yields

$$S_k = \frac{N}{m_k} \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) + O_{\boldsymbol{\alpha}, \varepsilon}(m_k^{t - 1 + 1/((\tau-1)t+1)} N^{1 - 1/((\tau-1)t+1) + \varepsilon/2}). \tag{6}$$

This is trivial for $N < m_k$ since then $S_k = 0$ or 1, and so (6) holds in all cases.

By inserting (6) in the identity $A(J; N) = \sum_{k=1}^{M} S_k$, we get

$$\begin{aligned} A(J; N) &= N \Big(\prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) \Big) \sum_{k=1}^{M} \frac{1}{m_k} \\ &\quad + O_{\boldsymbol{\alpha}, \varepsilon}\Big(N^{1 - 1/((\tau-1)t+1) + \varepsilon/2} \sum_{k=1}^{M} m_k^{t - 1 + 1/((\tau-1)t+1)} \Big). \end{aligned}$$

Since the Halton sequence in the bases $b_1, \ldots, b_s$ is uniformly distributed in

$[0,1]^s$ (see [7, Theorem 3.6]), we deduce in conjunction with Lemma 2 that

$$\prod_{i=1}^{s} v_i b_i^{-f_i} = \lim_{N\to\infty} \frac{1}{N} \#\Big\{0 \le n \le N-1 : (\phi_{b_1}(n), \ldots, \phi_{b_s}(n)) \in \prod_{i=1}^{s} [0, v_i b_i^{-f_i})\Big\}$$

$$= \lim_{N\to\infty} \frac{1}{N} \#\Big\{0 \le n \le N-1 : n \in \bigsqcup_{k=1}^{M} R_k\Big\}$$

$$= \sum_{k=1}^{M} \lim_{N\to\infty} \frac{1}{N} \#\{0 \le n \le N-1 : n \equiv r_k \pmod{m_k}\} = \sum_{k=1}^{M} \frac{1}{m_k}.$$

Therefore

$$A(J;N) = N\lambda_{s+t}(J) + O_{\boldsymbol{\alpha},\varepsilon}\Big(N^{1-1/((\tau-1)t+1)+\varepsilon/2} \sum_{k=1}^{M} m_k^{t-1+1/((\tau-1)t+1)}\Big),$$

and so

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| = O_{\boldsymbol{\alpha},\varepsilon}\Big(N^{-1/((\tau-1)t+1)+\varepsilon/2} \sum_{k=1}^{M} m_k^{t-1+1/((\tau-1)t+1)}\Big). \tag{7}$$

Next we note that Lemma 2 yields $M \le b_1 \cdots b_s f_1 \cdots f_s$ and $m_k \le b_1^{f_1} \cdots b_s^{f_s}$ for $1 \le k \le M$. From the choice of the integers f_i in (3), it follows that

$$m_k \le b_1 \cdots b_s N^{\frac{s}{(\tau-1)(st^2-st+t)+st+1}} \quad \text{for } 1 \le k \le M.$$

Using these bounds in (7), we obtain

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| = O_{b_1,\ldots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{(\tau-1)(st^2-st+t)+st+1}+\varepsilon}) \tag{8}$$

with an implied constant independent of J.

Next we consider an interval $J \subseteq [0,1)^{s+t}$ of the form

$$J = \prod_{i=1}^{s} [0, w_i) \times \prod_{j=1}^{t} [w_j^{(1)}, w_j^{(2)}) \tag{9}$$

with $0 < w_i \le 1$ for $1 \le i \le s$ and $0 \le w_j^{(1)} < w_j^{(2)} \le 1$ for $1 \le j \le t$. By approximating the w_i from below and above by the nearest fractions of the form $v_i/b_i^{f_i}$ with $v_i \in \mathbb{Z}$, we deduce from (8) that

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| \le \sum_{i=1}^{s} b_i^{-f_i} + O_{b_1,\ldots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{(\tau-1)(st^2-st+t)+st+1}+\varepsilon}). \tag{10}$$

Using again the expression for the f_i in (3), we derive from (10) that

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| = O_{b_1,\ldots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{(\tau-1)(st^2-st+t)+st+1}+\varepsilon})$$

with an implied constant still independent of J. The standard method of moving from intervals of the form (9) to arbitrary half-open subintervals of $[0,1)^{s+t}$ (see [5, p. 93, Example 1.2]) produces an additional factor 2^s in the discrepancy bound. ∎

REMARK 2. In the special case where $\boldsymbol{\alpha} \in \mathbb{R}^t$ is of finite type $\tau = 1$ (compare with Remark 1), we obtain the simpler bound

$$D_N = O_{b_1,\dots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-1/(st+1)+\varepsilon}) \qquad \text{for all } \varepsilon > 0.$$

There is an even more special case where $t = 1$ and $\alpha \in \mathbb{R}$ is of constant type c (see [9, Section 3]). In this case, the method in the proof of Theorem 1 yields

$$D_N = O_{b_1,\dots,b_s}(c^{1/(s+1)} N^{-1/(s+1)} (\log(c^{-1}N + 3))^{s/(s+1)}).$$

This is an improvement on [9, Theorem 1].

REMARK 3. A probabilistic result on the discrepancy D_N of the first N terms of the hybrid sequence (2) was shown in [4], namely that for almost all $\boldsymbol{\alpha} \in [0,1)^t$ in the sense of Lebesgue measure we have

$$D_N = O_{b_1,\dots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-1}(\log(N+1))^{s+t+1+\varepsilon}) \quad \text{for all } \varepsilon > 0.$$

This result was extended in [3] to a more general family of hybrid sequences.

There is a classical lower bound on the discrepancy of one-dimensional Kronecker sequences, due to Behnke [2]. A multidimensional version of this lower bound has not been established so far. We present such a generalization in Theorem 2 below. In the case $t = 1$, Theorem 2 reduces to Behnke's result. It is clear that Theorem 2 yields also a lower bound on the discrepancy of the hybrid sequence (2) when $\boldsymbol{\alpha}$ is of finite type.

THEOREM 2. *Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be of finite type τ. Then the discrepancy D_N of the first N terms of the Kronecker sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \dots$, satisfies*

$$D_N = \Omega(N^{-1/\tau-\varepsilon}) \quad \textit{for all } \varepsilon > 0.$$

Proof. Fix $\varepsilon > 0$ and put $\delta = \tau^2\varepsilon/(2\tau\varepsilon + 2)$. Since $\delta > 0$, it follows from Definition 1 that for any $c > 0$ there is $\mathbf{h} \in \mathbb{Z}^t \setminus \{\mathbf{0}\}$ with $r(\mathbf{h})^{\tau-\delta}\|\mathbf{h}\cdot\boldsymbol{\alpha}\| < c$. Consequently, there exist infinitely many $\mathbf{h} \in \mathbb{Z}^t \setminus \{\mathbf{0}\}$ such that $\|\mathbf{h}\cdot\boldsymbol{\alpha}\| < r(\mathbf{h})^{-\tau+\delta}$. Fix such an $\mathbf{h}$ for the moment. Then there exists $v \in \mathbb{Z}$ with $|\mathbf{h}\cdot\boldsymbol{\alpha} - v| < r(\mathbf{h})^{-\tau+\delta}$. Put $\beta = \tau - 2\delta = \tau/(\tau\varepsilon+1)$ and $N = \lceil r(\mathbf{h})^{\beta}\rceil$. Then for $0 \le n \le N-1$ we get $|\mathbf{h}\cdot(n\boldsymbol{\alpha}) - nv| < r(\mathbf{h})^{\beta-\tau+\delta} = r(\mathbf{h})^{-\delta}$, and so

$$\|\mathbf{h}\cdot\{n\boldsymbol{\alpha}\}\| < r(\mathbf{h})^{-\delta} \quad \text{for } 0 \le n \le N-1. \tag{11}$$

Since we have infinitely many $\mathbf{h}$, we can assume that $r(\mathbf{h})^{-\delta} \le 1/3$. It follows from (11) that none of the points $\{n\boldsymbol{\alpha}\}$, $n = 0, 1, \dots, N-1$, is in the set $K(\mathbf{h}) = \{\mathbf{x} \in [0,1)^t : \|\mathbf{h}\cdot\mathbf{x}\| \ge 1/3\}$. For any half-open subinterval J of $K(\mathbf{h})$, we then have $D_N \ge \lambda_t(J)$.

We now construct a special interval J. We can assume without loss of generality that all coordinates of $\mathbf{h} = (h_1, \ldots, h_t)$ are nonzero and that, moreover, $h_i > 0$ for $1 \le i \le m$ and $h_i < 0$ for $m+1 \le i \le t$, with some integer m satisfying $1 \le m \le t$. Put

$$J = \prod_{i=1}^{m} \left[\frac{1}{2mh_i}, \frac{2}{3mh_i}\right) \times \prod_{i=m+1}^{t} \left[0, \frac{1}{6(t-m)|h_i|}\right) \subseteq [0,1)^t.$$

Then for any $\mathbf{x} = (x_1, \ldots, x_t) \in J$ we have

$$\mathbf{h} \cdot \mathbf{x} = \sum_{i=1}^{t} h_i x_i \le \sum_{i=1}^{m} h_i x_i \le \frac{2}{3},$$

$$\mathbf{h} \cdot \mathbf{x} = \sum_{i=1}^{m} h_i x_i - \sum_{i=m+1}^{t} |h_i| x_i \ge \frac{1}{2} - \frac{1}{6} = \frac{1}{3}.$$

Hence $J \subseteq K(\mathbf{h})$, and so $D_N \ge \lambda_t(J) \ge (6t)^{-t} r(\mathbf{h})^{-1}$. Recalling that $N = \lceil r(\mathbf{h})^{\beta} \rceil$, we conclude that

$$D_N \ge (6t)^{-t} N^{-1/\beta} = (6t)^{-t} N^{-1/\tau - \varepsilon}. \tag{12}$$

Since there are infinitely many choices for $\mathbf{h}$, there are infinitely many values of N for which (12) holds. ∎

4. Mixing Halton sequences and explicit nonlinear congruential sequences. A standard nonlinear method for the generation of uniform pseudorandom numbers is the *explicit nonlinear congruential method* (see [7, Section 8.1]). In this section we consider hybrid sequences obtained by "mixing" Halton sequences and sequences of explicit nonlinear congruential pseudorandom numbers. We choose dimensions $s \ge 1$ and $t \ge 1$, pairwise coprime integers $b_1, \ldots, b_s \ge 2$, and a prime $p \ge 3$. We identify the finite prime field $\mathbb{F}_p$ of characteristic p with the set $\{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}$. Now we choose polynomials $g_1, \ldots, g_t \in \mathbb{F}_p[X]$, view their function values as elements of $\mathbb{F}_p$, and define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), g_1(n)/p, \ldots, g_t(n)/p) \in [0,1)^{s+t} \tag{13}$$

for $n = 0, 1, \ldots$. The following discrepancy bound is a substantial improvement on [10, Theorem 2]. We put $\operatorname{Log} u = \max(1, \log u)$ for $u \in \mathbb{R}$, $u > 0$.

THEOREM 3. *Let $b_1, \ldots, b_s \ge 2$ be pairwise coprime integers. Let $p \ge 3$ be a prime and assume that $\gcd(b_i, p) = 1$ for $1 \le i \le s$. Let $g_1, \ldots, g_t \in \mathbb{F}_p[X]$ with $\deg(g_j) < p$ for $1 \le j \le t$ and assume that the polynomials $1, X, g_1(X), \ldots, g_t(X)$ are linearly independent over $\mathbb{F}_p$. Put $G = \max(\deg(g_1), \ldots, \deg(g_t))$. Then for $1 \le N \le p$ the discrepancy D_N of*

the first N terms of the sequence (13) *satisfies*

$$D_N = O_{b_1,\dots,b_s,t}\left(\frac{Gp^{1/2}(\log p)^{t+1}}{N}\left(\operatorname{Log}\frac{N}{Gp^{1/2}(\log p)^{t+1}}\right)^s\right).$$

Proof. For a fixed integer N with $1 \le N \le p$, we introduce the positive integers

$$f_i = \left\lceil \frac{1}{\log b_i} \operatorname{Log}\frac{N}{Gp^{1/2}(\log p)^{t+1}} \right\rceil \quad \text{for } 1 \le i \le s. \tag{14}$$

Let $A(J;N)$ be the counting function in (1), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ in (13). We put

$$\mathbf{u}_n = (g_1(n)/p, \dots, g_t(n)/p) \in [0,1)^t, \qquad n = 0, 1, \dots.$$

For an interval $J \subseteq [0,1)^{s+t}$ of the form (4), we then deduce as in the proof of Theorem 1 that $A(J;N) = \sum_{k=1}^{M} S_k$, where now

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

with suitable moduli $m_1, \dots, m_M$ and $0 \le r_k < m_k$ for $1 \le k \le M$.

We consider S_k for fixed k with $1 \le k \le M$ and we assume first that $N \ge m_k$. In analogy with (5), we get

$$\begin{aligned} S_k = {} & \frac{N}{m_k}\prod_{j=1}^{t}(w_j^{(2)} - w_j^{(1)}) \\ & + O\left(\left\lfloor \frac{N - r_k - 1 + m_k}{m_k} \right\rfloor D^{(k)}_{\lfloor (N-r_k-1+m_k)/m_k \rfloor}\right), \end{aligned} \tag{15}$$

where $D_L^{(k)}$ denotes the discrepancy of the L points $\mathbf{u}_{lm_k+r_k}$, $l = 0, 1, \dots, L-1$. Note that $\gcd(m_k, p) = 1$. It was shown in the proof of [10, Theorem 2] that

$$LD_L^{(k)} = O_t(Gp^{1/2}(\log p)^{t+1}) \quad \text{for } 1 \le L \le p.$$

Together with (15) this yields

$$S_k = \frac{N}{m_k}\prod_{j=1}^{t}(w_j^{(2)} - w_j^{(1)}) + O_t(Gp^{1/2}(\log p)^{t+1}). \tag{16}$$

This is trivial for $N < m_k$ since then $S_k = 0$ or 1, and so (16) holds in all cases.

By continuing to follow the arguments in the proof of Theorem 1, we obtain

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| = O_{b_1,\dots,b_s,t}(f_1 \cdots f_s N^{-1} G p^{1/2}(\log p)^{t+1})$$

with an implied constant independent of J. Furthermore, for an interval $J \subseteq [0,1)^{s+t}$ of the form (9) we derive in analogy with (10) that

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| \le \sum_{i=1}^{s} b_i^{-f_i} + O_{b_1,\ldots,b_s,t}(f_1 \cdots f_s N^{-1} G p^{1/2} (\log p)^{t+1}).$$

Using the expression for the f_i in (14), we get

$$\left|\frac{A(J;N)}{N} - \lambda_{s+t}(J)\right| = O_{b_1,\ldots,b_s,t}\left(\frac{G p^{1/2}(\log p)^{t+1}}{N}\left(\mathrm{Log}\,\frac{N}{G p^{1/2}(\log p)^{t+1}}\right)^s\right)$$

with an implied constant still independent of J. The proof is completed like the proof of Theorem 1. ∎

REMARK 4. The conditions on $g_1, \ldots, g_t \in \mathbb{F}_p[X]$ in Theorem 3 are satisfied if $2 \le \deg(g_j) < p$ for $1 \le j \le t$ and $\deg(g_1), \ldots, \deg(g_t)$ are distinct.

An interesting special case of the explicit nonlinear congruential method is the *explicit inversive method* (see [8, Section 3.3]). In this case, the hybrid sequence corresponding to (13) is obtained as follows. Let $s \ge 1$ and $t \ge 1$ be given dimensions, let $b_1, \ldots, b_s \ge 2$ be pairwise coprime integers, and let $p \ge 5$ be a prime. Choose $a_1, \ldots, a_t \in \mathbb{F}_p^*$ and $c_1, \ldots, c_t \in \mathbb{F}_p$. For $1 \le j \le t$, we introduce the sequence

$$e_n^{(j)} = (a_j n + c_j)^{p-2} \in \mathbb{F}_p, \quad n = 0, 1, \ldots,$$

of period p. Then we define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), e_n^{(1)}/p, \ldots, e_n^{(t)}/p) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots. \tag{17}$$

The following discrepancy bound is a substantial improvement on [10, Theorem 4].

THEOREM 4. *Let $b_1, \ldots, b_s \ge 2$ be pairwise coprime integers. Let $p \ge 5$ be a prime and assume that $\gcd(b_i, p) = 1$ for $1 \le i \le s$. Let $a_1, \ldots, a_t \in \mathbb{F}_p^*$ and $c_1, \ldots, c_t \in \mathbb{F}_p$ be such that $c_1 a_1^{-1}, \ldots, c_t a_t^{-1}$ are distinct elements of $\mathbb{F}_p$. Then for $1 \le N \le p$ the discrepancy D_N of the first N terms of the sequence* (17) *satisfies*

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

Proof. A comparison with the proof of [10, Theorem 4] shows that we can formally proceed as in the proof of Theorem 3 with $G = 1$. ∎

5. Mixing Halton sequences and digital explicit inversive sequences. Let $q \ge 3$ be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. Choose $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ with γ of order $T \ge 2$ in the cyclic group $\mathbb{F}_q^*$. Put $\varrho_n = (\alpha\gamma^n + \beta)^{q-2} \in \mathbb{F}_q$, $n = 0, 1, \ldots$. Let $\{\beta_1, \ldots, \beta_e\}$ be an ordered

basis of $\mathbb{F}_q$ over its prime subfield $\mathbb{F}_p$. Then we can write $\varrho_n = \sum_{l=1}^{e} c_{n,l}\,\beta_l$, $n = 0, 1, \ldots$, with uniquely determined $c_{n,l} \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$. A sequence of *digital explicit inversive pseudorandom numbers of order* T is then defined by

$$z_n = \sum_{l=1}^{e} c_{n,l}\, p^{-l} \in [0,1), \qquad n = 0, 1, \ldots. \tag{18}$$

These sequences were introduced in [16]. They are purely periodic with least period T.

We now consider hybrid sequences obtained by "mixing" Halton sequences and sequences of digital explicit inversive pseudorandom numbers of order T. For a dimension $s \geq 1$, we choose pairwise coprime integers $b_1, \ldots, b_s \geq 2$. For a dimension t with $1 \leq t \leq T$, we choose integers $0 \leq d_1 < d_2 < \cdots < d_t < T$. Then with $z_0, z_1, \ldots$ as in (18), we define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), z_{n+d_1}, \ldots, z_{n+d_t}) \in [0,1)^{s+t}, \qquad n = 0, 1, \ldots. \tag{19}$$

The following discrepancy bound is a substantial improvement on [13, Theorem 3].

THEOREM 5. *Let $b_1, \ldots, b_s \geq 2$ be pairwise coprime integers. Let $q \geq 3$ be a prime power and let the sequence $z_0, z_1, \ldots$ in* (18) *have least period $T \geq 2$. Assume that $\gcd(b_i, T) = 1$ for $1 \leq i \leq s$. Then for $1 \leq N \leq T$ the discrepancy D_N of the first N terms of the sequence* (19) *satisfies*

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

Proof. For a fixed integer N with $1 \leq N \leq T$, we introduce the positive integers

$$f_i = \left\lceil \frac{1}{\log b_i} \operatorname{Log} \frac{N}{q^{1/2}(\log q)^t \log T} \right\rceil \quad \text{for } 1 \leq i \leq s.$$

Let $A(J; N)$ be the counting function in (1), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in (19). We put

$$\mathbf{z}_n = (z_{n+d_1}, \ldots, z_{n+d_t}) \in [0,1)^t, \qquad n = 0, 1, \ldots.$$

For an interval $J \subseteq [0,1)^{s+t}$ of the form (4), we deduce as in the proof of Theorem 1 that $A(J; N) = \sum_{k=1}^{M} S_k$, where now

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

with suitable moduli $m_1, \ldots, m_M$ and $0 \leq r_k < m_k$ for $1 \leq k \leq M$.

For $N \ge m_k$, we derive in analogy with (15) that

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

where $D_L^{(k)}$ denotes the discrepancy of the L points $\mathbf{z}_{lm_k+r_k}$, $l = 0, 1, \ldots, L-1$. Note that $\gcd(m_k, T) = 1$. It was shown in the proof of [13, Theorem 3] that

$$LD_L^{(k)} = O_t(q^{1/2} (\log q)^t \log T) \quad \text{for } 1 \le L \le T.$$

The proof of the theorem is completed in the same way as that of Theorem 3. ∎

REMARK 5. The paper [13] studied also the "mixing" of Halton sequences with sequences of so-called digital explicit inversive pseudorandom numbers of period q. The method of the present paper can be applied also to this case, but it yields only a tiny improvement on the earlier discrepancy bound in [13, Theorem 2].

6. Mixing Halton sequences and recursive inversive sequences. We consider the recursive inversive sequences introduced in [12]. Let $p \ge 3$ be a prime. As in Section 4, we identify $\mathbb{F}_p$ with the set $\{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}$. Fix $a, b \in \mathbb{F}_p^*$ and define the sequence $h_0, h_1, \ldots$ of rational functions over $\mathbb{F}_p$ by $h_0(X) = X$ and $h_n(X) = h_{n-1}(aX^{-1} + b)$ for $n = 1, 2, \ldots$. The sequence $h_0, h_1, \ldots$ is purely periodic with least period $T \le p+1$. For $1 \le n \le T-1$, each h_n has a unique pole $e_n \in \mathbb{F}_p$. Now choose $c_0 \in \mathbb{F}_p$ with $c_0^2 \ne bc_0 + a$. Then for $1 \le n \le T-1$ we put $c_n = h_n(c_0)$ if $c_0 \ne e_n$ and $c_n = b - e_n$ if $c_0 = e_n$. By extending with period T, we get a sequence $c_0, c_1, \ldots$ of elements of $\mathbb{F}_p$ which is called an *inversive generator* and has least period T according to [12, Lemma 2]. A simple sufficient condition for obtaining the maximum period $T = p+1$ is given in [12, Theorem 1], and for any p there are always choices of $a, b \in \mathbb{F}_p^*$ such that this maximum period is attained (see [12, p. 255]).

For a dimension $s \ge 1$, we choose pairwise coprime integers $b_1, \ldots, b_s \ge 2$. Then we define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), c_n/p) \in [0,1)^{s+1}, \quad n = 0, 1, \ldots. \tag{20}$$

The following discrepancy bound is a substantial improvement on [9, Theorem 5].

THEOREM 6. *Let $b_1, \ldots, b_s \ge 2$ be pairwise coprime integers. Let $p \ge 3$ be a prime, let $c_0, c_1, \ldots \in \mathbb{F}_p$ be an inversive generator, and let T be the least period of this sequence. Then for $1 \le N \le T$ the discrepancy D_N of*

the first N terms of the sequence (20) *satisfies*

$$D_N = O_{b_1,\dots,b_s}\left(\frac{p^{1/4}\log p}{N^{1/2}}\left(\operatorname{Log}\frac{N^{1/2}}{p^{1/4}\log p}\right)^s\right).$$

Proof. For a fixed integer N with $1 \le N \le T$, we introduce the positive integers

$$f_i = \left\lceil \frac{1}{\log b_i}\operatorname{Log}\frac{N^{1/2}}{p^{1/4}\log p}\right\rceil \quad \text{for } 1 \le i \le s.$$

Let $A(J;N)$ be the counting function in (1), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ in (20). For an interval $J \subseteq [0,1)^{s+1}$ of the form (4) with $t = 1$, we deduce as in the proof of Theorem 1 that $A(J;N) = \sum_{k=1}^{M} S_k$, where now

$$S_k = \#\{0 \le n \le N-1 : n \equiv r_k \pmod{m_k} \text{ and } c_n/p \in [w_1^{(1)}, w_1^{(2)})\}$$

with suitable moduli $m_1, \dots, m_M$ and $0 \le r_k < m_k$ for $1 \le k \le M$.

For $N \ge m_k$, we derive in analogy with (15) that

$$S_k = \frac{N}{m_k}(w_1^{(2)} - w_1^{(1)}) + O\left(\left\lfloor \frac{N - r_k - 1 + m_k}{m_k}\right\rfloor D^{(k)}_{\lfloor (N-r_k-1+m_k)/m_k\rfloor}\right),$$

where $D_L^{(k)}$ is the discrepancy of the L points $c_{lm_k+r_k}\, p^{-1}$, $l = 0, 1, \dots, L-1$. With $L = \lfloor (N - r_k - 1 + m_k)/m_k\rfloor$ we have

$$m_k(L-1) + r_k \le N - r_k - 1 + m_k - m_k + r_k = N - 1 < T,$$

and so we deduce as in the proof of [9, Theorem 5] that

$$LD_L^{(k)} = O(L^{1/2}p^{1/4}\log p).$$

Since $L < 2N$, this yields

$$S_k = \frac{N}{m_k}(w_1^{(2)} - w_1^{(1)}) + O(N^{1/2}p^{1/4}\log p). \tag{21}$$

This is trivial for $N < m_k$ since then $S_k = 0$ or 1, and so (21) holds in all cases. The proof of the theorem is completed in the same way as the proof of Theorem 3. ∎

References

[1] A. Baker, *On some Diophantine inequalities involving the exponential function*, Canad. J. Math. 17 (1965), 616–626.

[2] H. Behnke, *Zur Theorie der diophantischen Approximationen. I, II*, Abh. Math. Sem. Univ. Hamburg 3 (1924), 261–318; 4 (1926), 33–46.

[3] R. Hofer and P. Kritzer, *On hybrid sequences built from Niederreiter–Halton sequences and Kronecker sequences*, Bull. Austral. Math. Soc. 84 (2011), 238–254.

[4] R. Hofer and G. Larcher, *Metrical results on the discrepancy of Halton–Kronecker sequences*, Math. Z. 271 (2012), 1–11.

[5] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974; reprint, Dover Publ., Mineola, NY, 2006.
[6] H. Niederreiter, *Application of diophantine approximations to numerical integration*, in: Diophantine Approximation and Its Applications, C. F. Osgood (ed.), Academic Press, New York, 1973, 129–199.
[7] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.
[8] H. Niederreiter, *New developments in uniform pseudorandom number and vector generation*, in: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, H. Niederreiter and P. J.-S. Shiue (eds.), Lecture Notes in Statist. 106, Springer, New York, 1995, 87–120.
[9] H. Niederreiter, *On the discrepancy of some hybrid sequences*, Acta Arith. 138 (2009), 373–398.
[10] H. Niederreiter, *Further discrepancy bounds and an Erdős–Turán–Koksma inequality for hybrid sequences*, Monatsh. Math. 161 (2010), 193–222.
[11] H. Niederreiter, *Quasi-Monte Carlo methods*, in: Encyclopedia of Quantitative Finance, R. Cont (ed.), Wiley, Chichester, 2010, 1460–1472.
[12] H. Niederreiter and J. Rivat, *On the correlation of pseudorandom numbers generated by inversive methods*, Monatsh. Math. 153 (2008), 251–264.
[13] H. Niederreiter and A. Winterhof, *Discrepancy bounds for hybrid sequences involving digital explicit inversive pseudorandom numbers*, Unif. Distrib. Theory 6 (2011), no. 1, 33–56.
[14] W. M. Schmidt, *Simultaneous approximation to algebraic numbers by rationals*, Acta Math. 125 (1970), 189–201.
[15] J. Spanier, *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 Statist. 106, Springer, New York, 1995, 121–148.
[16] A. Winterhof, *On the distribution of some new explicit inversive pseudorandom numbers and vectors*, in: Monte Carlo and Quasi-Monte Carlo Methods 2004, H. Niederreiter and D. Talay (eds.), Springer, Berlin, 2006, 487–499.

Harald Niederreiter
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz, Austria
and
Department of Mathematics and Statistics
King Fahd University of Petroleum & Minerals
P.O. Box 5046
Dhahran 31261, Saudi Arabia
E-mail: ghnied@gmail.com

Received on 16.5.2011
and in revised form on 4.11.2011 (6697)