Publ. Math. Debrecen
79/3-4 (2011), 589–603
DOI: 10.5486/PMD.2011.5092

Discrepancy bounds for hybrid sequences involving matrix-method pseudorandom vectors

By HARALD NIEDERREITER (Dhahran)

Dedicated to Professor K. Győry on the occasion of his 70th birthday

Abstract. We establish the first nontrivial deterministic discrepancy bounds for sequences that are obtained by "mixing" either Halton sequences or Kronecker sequences with sequences of matrix-method pseudorandom vectors.

1. Introduction

In recent years, a series of papers (see [9], [10], [11], [13]) has been written on so-called hybrid sequences. These papers established the first nontrivial deterministic discrepancy bounds for various types of hybrid sequences. Previously, only probabilistic results on the discrepancy of hybrid sequences were known (see [3], [14], [15]). We recall that a *hybrid sequence* is a sequence of points in a (usually high-dimensional) unit cube that is obtained by "mixing" a low-discrepancy sequence and a sequence of pseudorandom numbers (or vectors), in the sense that certain coordinates of the points stem from the low-discrepancy sequence and the remaining coordinates stem from the sequence of pseudorandom numbers (or vectors). Hybrid sequences go back to a proposal of Spanier [17] in the context of multidimensional numerical integration by Monte Carlo and quasi-Monte Carlo

Mathematics Subject Classification: 11K38, 11K45, 65C05, 65C10.
Key words and phrases: discrepancy, hybrid sequence, Halton sequence, Kronecker sequence, pseudorandom vectors, matrix method.

methods (see [12] for a recent survey of these methods). In practice, the "pseudorandom" constituent of a hybrid sequence should be of high dimension, and an efficient way to achieve this is to consider methods that generate pseudorandom vectors directly. The most popular method for this purpose is the matrix method (see [8, Section 10.1]). In the present paper, we consider hybrid sequences that are obtained by "mixing" either Halton sequences or Kronecker sequences with sequences of matrix-method pseudorandom vectors.

We review some basic facts on the discrepancy. 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 $[0,1)^m$ and the counting function $A(J;N)$ is given by

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

Note that we always have $ND_N \geq 1$ (see [4, p. 93]) and $D_N \leq 1$. Next we recall the Erdős–Turán–Koksma inequality (see [2, Theorem 1.21]). For any $\mathbf{h} = (h_1, \ldots, h_m) \in \mathbb{Z}^m$, we put

$$M(\mathbf{h}) := \max_{1 \leq i \leq m} |h_i|, \qquad r(\mathbf{h}) := \prod_{i=1}^{m} \max(|h_i|, 1). \tag{2}$$

We use $\cdot$ to denote the standard inner product in $\mathbb{R}^m$ and we write $\mathrm{e}(u) = \mathrm{e}^{2\pi \mathrm{i} u}$ for $u \in \mathbb{R}$. We adopt 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.

Lemma 1. *The discrepancy D_N of the points $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1} \in [0,1)^m$ satisfies*

$$D_N = O_m\Big(\frac{1}{H} + \frac{1}{N} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^m \\ 0 < M(\mathbf{h}) \leq H}} \frac{1}{r(\mathbf{h})} \Big| \sum_{n=0}^{N-1} \mathrm{e}\left(\mathbf{h} \cdot \mathbf{y}_n\right) \Big| \Big)$$

for any integer $H \geq 1$, where $M(\mathbf{h})$ and $r(\mathbf{h})$ are as in (2).

In Section 2, respectively Section 3, we provide background and auxiliary results on matrix-method pseudorandom vectors, respectively Halton sequences. Sections 4 and 5 contain discrepancy bounds for hybrid sequences obtained by "mixing" Halton sequences, respectively Kronecker sequences, and matrix-method pseudorandom vectors.

2. Matrix-method pseudorandom vectors

The *matrix method* is a standard technique for the generation of uniform pseudorandom vectors. We refer to [8, Section 10.1] for background on the matrix method. Let $t \geq 1$ be a given dimension and choose a (large) prime p. We identify the finite prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with the set $\{0, 1, \dots, p-1\}$ of integers. Choose a nonsingular $t \times t$ matrix A over $\mathbb{F}_p$, called the *generating matrix.* Now select an initial row vector $\mathbf{z}_0 \in \mathbb{F}_p^t$ with $\mathbf{z}_0 \neq \mathbf{0}$ and generate further row vectors $\mathbf{z}_1, \mathbf{z}_2, \dots \in \mathbb{F}_p^t$ by the recursion

$$\mathbf{z}_{n+1} = \mathbf{z}_n A \quad \text{for } n = 0, 1, \dots . \tag{3}$$

The sequence $\mathbf{z}_0, \mathbf{z}_1, \dots$ is called a *matrix-method generator.* Finally, we get *matrix-method pseudorandom vectors* by the normalization

$$\mathbf{u}_n = \frac{1}{p}\mathbf{z}_n \in [0,1)^t \quad \text{for } n = 0, 1, \dots . \tag{4}$$

It is trivial that the sequences $\mathbf{z}_0$, $\mathbf{z}_1, \dots$ and $\mathbf{u}_0, \mathbf{u}_1, \dots$ are purely periodic with the same least period $\leq p^t - 1$. We get the maximum period $p^t - 1$ if and only if the characteristic polynomial $g \in \mathbb{F}_p[x]$ of the matrix A is primitive over $\mathbb{F}_p$ (see [8, Theorem 10.2]). Recall that g is said to be *primitive* over $\mathbb{F}_p$ if each root of g is a primitive element of the finite field $\mathbb{F}_q$ with $q = p^t$ elements, i.e., each root of g generates the cyclic group $\mathbb{F}_q^*$. We need the following discrepancy bound.

Proposition 1. *Let $p \geq 19$ be a prime and let $t \geq 1$ be an integer. Let $\mathbf{u}_0, \mathbf{u}_1, \dots$ be a sequence of t-dimensional matrix-method pseudorandom vectors with maximum period $p^t - 1$. Then the discrepancy D_N of $\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_{N-1}$ satisfies*

$$D_N = O\left(tp^{-1} + N^{-1}p^{t/2}(\log p)^{t+1}\right) \quad \textit{for } 1 \leq N \leq p^t - 1$$

with an absolute implied constant.

Proof. For fixed $\mathbf{h} \in \mathbb{F}_p^t$ with $\mathbf{h} \neq \mathbf{0}$, we consider the exponential sum

$$\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{u}_n) = \sum_{n=0}^{N-1} \mathrm{e}\left(\frac{1}{p}\mathbf{h} \cdot \mathbf{z}_n\right).$$

Let $y_n \in \mathbb{F}_p$ be given by $y_n \equiv \mathbf{h} \cdot \mathbf{z}_n \pmod{p}$ for $n = 0, 1, \dots$, then

$$\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{u}_n) = \sum_{n=0}^{N-1} \mathrm{e}\left(\frac{1}{p}y_n\right). \tag{5}$$

If $g(x) = x^t - a_{t-1}x^{t-1} - \ldots - a_0 \in \mathbb{F}_p[x]$ is the characteristic polynomial of A, then $g(A) = 0$ by the Cayley–Hamilton theorem. Left multiplying by $\mathbf{z}_n$ and using (3), we obtain

$$\mathbf{z}_{n+t} = a_{t-1}\mathbf{z}_{n+t-1} + \cdots + a_0\mathbf{z}_n \quad \text{for } n = 0, 1, \ldots .$$

Form the inner product with $\mathbf{h}$, then in $\mathbb{F}_p$ we have

$$y_{n+t} = a_{t-1}y_{n+t-1} + \cdots + a_0y_n \quad \text{for } n = 0, 1, \ldots .$$

Hence $y_0, y_1, \ldots$ is a linear recurring sequence in $\mathbb{F}_p$ with characteristic polynomial g.

We claim that $y_0, y_1, \ldots$ is not the zero sequence. Since $\mathbf{h} \not\equiv \mathbf{0} \pmod p$, there exists a nonzero vector $\mathbf{b} \in \mathbb{F}_p^t$ with $\mathbf{h} \cdot \mathbf{b} \not\equiv 0 \pmod p$. Furthermore, $\mathbf{z}_0, \mathbf{z}_1, \ldots$ run through all nonzero vectors in $\mathbb{F}_p^t$ (see [8, p. 207]), and so there exists an integer $k \geq 0$ with $\mathbf{z}_k = \mathbf{b}$. Then

$$y_k \equiv \mathbf{h} \cdot \mathbf{z}_k \equiv \mathbf{h} \cdot \mathbf{b} \not\equiv 0 \pmod p,$$

and so $y_0, y_1, \ldots$ is not the zero sequence.

Let α be a fixed root of g in the finite field $\mathbb{F}_q$ with $q = p^t$ elements. Then by [5, Theorem 6.24] there exists $\beta \in \mathbb{F}_q$ such that

$$y_n = \mathrm{Tr}(\beta\alpha^n) \quad \text{for } n = 0, 1, \ldots,$$

where Tr is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. We observe that $\beta \neq 0$ since $y_0, y_1, \ldots$ is not the zero sequence. Using (5), we can write

$$\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{u}_n) = \sum_{n=0}^{N-1} \mathrm{e}\left(\frac{1}{p}\,\mathrm{Tr}(\beta\alpha^n)\right) = \sum_{n=0}^{N-1} \chi(\beta\alpha^n), \tag{6}$$

where χ is the canonical additive character of $\mathbb{F}_q$ (see [5, p. 170]). Note that α is an element of order $q-1$ in the group $\mathbb{F}_q^*$ since the polynomial g is primitive. Hence (6) and [7, Lemma 3] show that for $1 \leq N \leq q-1$ we have

$$\left|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{u}_n)\right| < q^{1/2}\left(\frac{4}{\pi^2}\log q + 0.41 + \frac{0.61}{q-1}\right) + \frac{N}{q-1} = O\left(q^{1/2}\log q\right). \tag{7}$$

We remark that [7, Lemma 3] has the condition $N < q-1$, but (7) is trivial for $N = q-1$ since then the character sum in (6) has the value -1. Now we apply [8, Corollary 3.11] to obtain

$$D_N = O\left(\frac{t}{p} + \frac{q^{1/2}\log q}{N}\left(\frac{4}{\pi^2}\log p + 1.72\right)^t\right).$$

Since $p \geq 19$ by assumption, we have

$$1.72 \leq \left(1 - \frac{4}{\pi^2} - c\right) \log p$$

for some $c > 0$, and so we arrive at the desired result. □

3. Halton sequences

For an integer $b \geq 2$, let $\mathbb{Z}_b = \{0, 1, \dots, b-1\}$ 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 $n \geq 0$ 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 $b_1, \dots, b_s \geq 2$, the *Halton sequence* (in the bases $b_1, \dots, b_s$) is given by

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

It is a classical low-discrepancy sequence (see [8, Section 3.1]).

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

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

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') $n \equiv d_1 + d_2 b + \dots + d_{f-1} b^{f-2} + r_f b^{f-1} \pmod{b^f}$ 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 2 is obtained by combining the Chinese remainder theorem with Lemma 2.

Lemma 3. *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 $n \in \sqcup_{k=1}^{M} R_k$, 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 $b_1, \dots, b_s, v_1, \dots, v_s, f_1, \dots, f_s$.

4. Mixing Halton sequences and matrix-method pseudorandom vectors

We consider hybrid sequences that are obtained by "mixing" Halton sequences and matrix-method pseudorandom vectors. We choose dimensions $s \ge 1$ and $t \ge 1$. Let $b_1, \dots, b_s \ge 2$ be pairwise coprime integers. Furthermore, let $\mathbf{u}_0, \mathbf{u}_1, \dots$ be a sequence of t-dimensional matrix-method pseudorandom vectors generated by (3) and (4). Then we define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \dots, \phi_{b_s}(n), \mathbf{u}_n) \in [0,1)^{s+t}, \quad n = 0, 1, \dots . \tag{8}$$

Under suitable conditions, we show the following discrepancy bound for this hybrid sequence. We write $\operatorname{Log} u := \max(1, \log u)$ for $u \in \mathbb{R}$, $u > 0$.

Theorem 1. *Let $p \geq 19$ be a prime and let $s \geq 1$ and $t \geq 1$ be given dimensions. Let $b_1, \dots, b_s \geq 2$ be pairwise coprime integers with $\gcd(b_i, p^t - 1) = 1$ for $1 \leq i \leq s$. Let $\mathbf{u}_0, \mathbf{u}_1, \dots$ 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 D_N of the first N terms of the sequence* (8) *satisfies*

$$D_N = O\left(\frac{2^s t}{p}\right) + O_{b_1,\dots,b_s}\left(\frac{p^{t/2}(\log p)^{t+1}}{N}\left(\operatorname{Log}\frac{N}{p^{t/2}(\log p)^{t+1}}\right)^s\right), \tag{9}$$

where the first implied constant is absolute and the second implied constant depends only on $b_1, \dots, b_s$.

Proof. Fix N with $1 \leq N \leq p^t - 1$. We introduce the positive integers

$$f_i := \left\lceil \frac{1}{\log b_i} \operatorname{Log} \frac{N}{p^{t/2}(\log p)^{t+1}} \right\rceil \quad \text{for } 1 \leq i \leq s. \tag{10}$$

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

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

with $v_1, \dots, v_s \in \mathbb{Z}$, $1 \leq v_i \leq b_i^{f_i}$ 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 3 to a point $\mathbf{x}_n$ in (8). Then we have $\mathbf{x}_n \in J$ if and only if

$$n \in \bigsqcup_{k=1}^{M} R_k \quad \text{and} \quad \mathbf{u}_n \in \prod_{j=1}^{t} \left[w_j^{(1)}, w_j^{(2)}\right),$$

where M and $R_1, \dots, R_M$ are as in Lemma 3. With $A(J; N)$ as in (1), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$, we obtain

$$A(J; N) = \sum_{k=1}^{M} T_k, \tag{11}$$

where

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

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

We consider T_k for a fixed k with $1 \leq k \leq M$. For an n counted by T_k, we have $n = m_k l + r_k$ for some integer l, and the condition $0 \le n \le N-1$ is equivalent to $0 \le l \le \lfloor (N - r_k - 1)/m_k \rfloor$. Assume first that $N \ge r_k + 1$. Then

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

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

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

it follows that

$$T_k = \frac{N}{m_k} \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) + O\left(\left\lfloor \frac{N - r_k - 1 + m_k}{m_k} \right\rfloor D^{(k)}_{\lfloor (N - r_k - 1 + m_k)/m_k \rfloor} \right). \quad (12)$$

To bound $D_L^{(k)}$, we note that by Section 2 we have $\mathbf{u}_{m_k l + r_k} = p^{-1} \mathbf{z}_{m_k l + r_k}$ and

$$\mathbf{z}_{m_k l + r_k} = \mathbf{z}_0 A^{m_k l + r_k} = \left(\mathbf{z}_0 A^{r_k} \right) \left(A^{m_k} \right)^l \qquad \text{for } l = 0, 1, \ldots .$$

This is a matrix-method generator with initial vector $\mathbf{z}_0 A^{r_k} \ne \mathbf{0}$ (since A is nonsingular) and generating matrix A^{m_k}. We can thus bound $D_L^{(k)}$ by Proposition 1 if we can show that the characteristic polynomial of A^{m_k} is primitive over $\mathbb{F}_p$. Let

$$g(x) = \prod_{j=1}^{t} \left(x - \alpha^{p^{j-1}} \right) \in \mathbb{F}_p[x]$$

be the characteristic polynomial of A, with α a primitive element of $\mathbb{F}_{p^t}$ by hypothesis. The characteristic polynomial of A^{m_k} is given by

$$g_{m_k}(x) = \prod_{j=1}^{t} \left(x - \alpha^{m_k p^{j-1}} \right).$$

Note that m_k is of the form $b_1^{j_1} \cdots b_s^{j_s}$ by Lemma 3, and so a hypothesis in the theorem implies that $\gcd(m_k, p^t - 1) = 1$. It follows that α^{m_k} is a primitive element of $\mathbb{F}_{p^t}$, and so the characteristic polynomial g_{m_k} of A^{m_k} is indeed primitive over $\mathbb{F}_p$. Thus, Proposition 1 yields

$$LD_L^{(k)} = O\left(Ltp^{-1} + p^{t/2}(\log p)^{t+1}\right) \quad \text{for } 1 \le L \le p^t - 1.$$

This bound is now used in (12) to obtain

$$T_k = \frac{N}{m_k} \prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)}) + O\left(\frac{tN}{pm_k} + p^{t/2}(\log p)^{t+1}\right). \tag{13}$$

Note that if $N \le r_k$, then $T_k = 0$ and $N < m_k$, and so the bound (13) is trivial. Thus, (13) holds in all cases.

By inserting (13) in (11) and recalling that $M \le b_1 \cdots b_s f_1 \cdots f_s$ by Lemma 3, we get

$$\begin{aligned} A(J;N) = N \left(\prod_{j=1}^{t} (w_j^{(2)} - w_j^{(1)})\right) \sum_{k=1}^{M} \frac{1}{m_k} + O\left(\frac{tN}{p} \sum_{k=1}^{M} \frac{1}{m_k}\right) \\ + O_{b_1,\ldots,b_s}\left(f_1 \cdots f_s p^{t/2}(\log p)^{t+1}\right). \end{aligned}$$

Since the Halton sequence in the bases $b_1, \ldots, b_s$ is uniformly distributed in $[0,1]^s$ (see [8, Theorem 3.6]), we obtain in conjunction with Lemma 3 that

$$\begin{aligned} \prod_{i=1}^{s} v_i b_i^{-f_i} &= \lim_{N\to\infty} \frac{1}{N} \# \left\{ 0 \le n \le N-1 : (\phi_{b_1}(n), \ldots, \phi_{b_s}(n)) \in \prod_{i=1}^{s} [0, v_i b_i^{-f_i}) \right\} \\ &= \lim_{N\to\infty} \frac{1}{N} \# \left\{ 0 \le n \le N-1 : n \in \bigsqcup_{k=1}^{M} R_k \right\} \\ &= \sum_{k=1}^{M} \lim_{N\to\infty} \frac{1}{N} \# \{ 0 \le n \le N-1 : n \equiv r_k \pmod{m_k} \} = \sum_{k=1}^{M} \frac{1}{m_k}. \end{aligned}$$

Therefore

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

and so

$$\left| \frac{A(J;N)}{N} - \lambda_{s+t}(J) \right| = O\left(tp^{-1}\right) + O_{b_1,\ldots,b_s}\left(f_1 \cdots f_s N^{-1} p^{t/2}(\log p)^{t+1}\right) \tag{14}$$

with implied constants independent of J.

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

$$J = \prod_{i=1}^{s} [0, w_i) \times \prod_{j=1}^{t} \left[w_j^{(1)}, w_j^{(2)}\right) \tag{15}$$

with $0 < w_i \leq 1$ for $1 \leq i \leq s$ and $0 \leq w_j^{(1)} < w_j^{(2)} \leq 1$ for $1 \leq j \leq t$. 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 (14) that

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

Using the expression for the f_i in (10), this yields

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

with implied constants still independent of J. The standard method of moving from intervals of the form (15) to arbitrary half-open subintervals of $[0,1)^{s+t}$ (see [4, p. 93, Example 1.2]) produces an additional factor 2^s in the discrepancy bound. □

Remark 1. A term of the order of magnitude p^{-1}, like the first term on the right-hand side of (9), is needed in the bound on D_N. Consider the interval

$$J_\delta = [0,1)^s \times [0, 1 - p^{-1} + \delta)^t \subseteq [0,1)^{s+t}$$

with $0 < \delta \leq p^{-1}$. Then all points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in (8) belong to J_δ, and so

$$D_N \geq \left|\frac{A(J_\delta;N)}{N} - \lambda_{s+t}(J_\delta)\right| = 1 - (1 - p^{-1} + \delta)^t.$$

Letting $\delta \to 0+$ we get $D_N \geq 1 - (1 - p^{-1})^t \geq c_t p^{-1}$ with a constant $c_t > 0$ depending only on t.

Remark 2. The special case $t = 1$ of Theorem 1, in which the matrix method reduces to the classical linear congruential method for pseudorandom number generation, was already treated in [9, Theorem 3]. The result there, for the case where the multiplier is a primitive root modulo p, says that

$$D_N = O_{b_1,\ldots,b_s}\left(\left(N^{-1} p^{1/2} (\log p)^2\right)^{1/(s+1)}\right) \qquad \text{for } 1 \leq N \leq p-1.$$

It is clear that Theorem 1 provides a substantial improvement on the discrepancy bound above. This improvement is due to the refined method in the present paper based on Lemma 3. Further improved discrepancy bounds for hybrid sequences that are based on Lemma 3 will be established in future work of the author.

5. Mixing Kronecker sequences and matrix-method pseudorandom vectors

A *Kronecker sequence* is a sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \dots$, of fractional parts, where $\boldsymbol{\alpha} \in \mathbb{R}^s$ for an arbitrary dimension $s \geq 1$. 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.

Definition 1. Let τ be a real number. Then $\boldsymbol{\alpha} \in \mathbb{R}^s$ 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

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

where $r(\mathbf{h})$ is as in (2).

It is well known that we always have $\tau \geq 1$ and that there are interesting examples of points $\boldsymbol{\alpha} \in \mathbb{R}^s$ with $\tau = 1$ (see Remark 3 below). The following auxiliary result was shown in [9, Lemma 3].

Lemma 4. *Let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be such that there exist real numbers $\sigma \geq 1$ and $c > 0$ with*

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

Then for any integers $H \geq 1$ and $N \geq 1$ we have

$$\sum_{\substack{\mathbf{h} \in \mathbb{Z}^s \\ 0 < M(\mathbf{h}) \leq H}} \frac{1}{r(\mathbf{h})} \left| \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h} \cdot \boldsymbol{\alpha})) \right| = O_{\boldsymbol{\alpha}, \varepsilon}\left(H^{(\sigma-1)s+\varepsilon}\right) \quad \textit{for all } \varepsilon > 0,$$

where $M(\mathbf{h})$ and $r(\mathbf{h})$ are as in (2).

We now choose a dimension $t \geq 1$ and let $\mathbf{u}_0, \mathbf{u}_1, \dots$ be a sequence of t-dimensional matrix-method pseudorandom vectors generated by (3) and (4) of maximum period $p^t - 1$. Then for $\boldsymbol{\alpha} \in \mathbb{R}^s$ with $s \geq 1$ arbitrary, we define the hybrid sequence

$$\mathbf{x}_n = (\{n\boldsymbol{\alpha}\}, \mathbf{u}_n) \in [0, 1)^{s+t}, \quad n = 0, 1, \dots. \tag{16}$$

For $\mathbf{h}_1 \in \mathbb{Z}^s$ and $\mathbf{h}_2 \in \mathbb{Z}^t$, we introduce the exponential sum

$$E_N(\mathbf{h}_1, \mathbf{h}_2) := \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + \mathbf{h}_2 \cdot \mathbf{u}_n). \tag{17}$$

Lemma 5. *Let p be a prime, let $\mathbf{h}_1 \in \mathbb{Z}^s$, and let $\mathbf{h}_2 \in \mathbb{Z}^t$ with $\mathbf{h}_2 \not\equiv \mathbf{0}$* (mod p)*. Then for the exponential sum $E_N(\mathbf{h}_1, \mathbf{h}_2)$ in* (17) *we have*

$$|E_N(\mathbf{h}_1, \mathbf{h}_2)| = O\left(t^{1/2} N^{1/2} p^{t/4} (\log p)^{1/2}\right) \quad \text{for } 1 \le N \le p^t - 1.$$

Proof. For $1 \le N \le p^t - 1$ we have

$$\begin{aligned} |E_N(\mathbf{h}_1, \mathbf{h}_2)|^2 &= \sum_{k,n=0}^{N-1} \mathrm{e}((k-n)(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + \mathbf{h}_2 \cdot (\mathbf{u}_k - \mathbf{u}_n)) \\ &\le N + 2 \left| \sum_{\substack{k,n=0 \\ k>n}}^{N-1} \mathrm{e}((k-n)(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + \mathbf{h}_2 \cdot (\mathbf{u}_k - \mathbf{u}_n)) \right| \\ &= N + 2 \left| \sum_{d=1}^{N-1} \sum_{n=0}^{N-1-d} \mathrm{e}(d(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + \mathbf{h}_2 \cdot (\mathbf{u}_{n+d} - \mathbf{u}_n)) \right| \\ &\le N + 2 \sum_{d=1}^{N-1} \left| \sum_{n=0}^{N-1-d} \mathrm{e}(\mathbf{h}_2 \cdot (\mathbf{u}_{n+d} - \mathbf{u}_n)) \right| . \end{aligned}$$

For fixed d with $1 \le d \le N - 1 < p^t - 1$, we consider

$$\sum_{n=0}^{N-1-d} \mathrm{e}(\mathbf{h}_2 \cdot (\mathbf{u}_{n+d} - \mathbf{u}_n)) = \sum_{n=0}^{N-1-d} \mathrm{e}\left(\frac{1}{p}\, \mathbf{h}_2 \cdot (\mathbf{z}_{n+d} - \mathbf{z}_n)\right).$$

In view of (3) we have $\mathbf{z}_{n+d} - \mathbf{z}_n = \mathbf{z}_n(A^d - I)$, where I is the $t \times t$ identity matrix over $\mathbb{F}_p$. Thus,

$$\mathbf{h}_2 \cdot (\mathbf{z}_{n+d} - \mathbf{z}_n) = [\mathbf{h}_2 (A^d - I)^{\mathrm{T}}] \cdot \mathbf{z}_n,$$

and so

$$\sum_{n=0}^{N-1-d} \mathrm{e}(\mathbf{h}_2 \cdot (\mathbf{u}_{n+d} - \mathbf{u}_n)) = \sum_{n=0}^{N-1-d} \mathrm{e}\big([\mathbf{h}_2 (A^d - I)^{\mathrm{T}}] \cdot \mathbf{u}_n\big). \tag{18}$$

The eigenvalues of A are the conjugates $\alpha, \alpha^p, \ldots, \alpha^{p^{t-1}}$ over $\mathbb{F}_p$ of a primitive element $\alpha \in \mathbb{F}_q$ with $q = p^t$. Then the eigenvalues of A^d are $\alpha^d, \alpha^{dp}, \ldots, \alpha^{dp^{t-1}}$. Since $1 \le d < p^t - 1$, it follows that $1 \in \mathbb{F}_q$ is not an eigenvalue of A^d, and so the matrix $A^d - I$ is nonsingular. For $\mathbf{h}_2 \not\equiv \mathbf{0}$ (mod p) we can thus apply the bound (7) to the exponential sum in (18) to obtain

$$\left| \sum_{n=0}^{N-1-d} \mathrm{e}(\mathbf{h}_2 \cdot (\mathbf{u}_{n+d} - \mathbf{u}_n)) \right| = O\left(q^{1/2} \log q\right).$$

Finally, we get

$$|E_N(\mathbf{h}_1,\mathbf{h}_2)|^2 \le N + O\left(tNp^{t/2}\log p\right) = O\left(tNp^{t/2}\log p\right),$$

which yields the desired result. □

In the following discrepancy bound, we use the notion of finite type introduced in Definition 1.

Theorem 2. *Let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be of finite type τ and let $\mathbf{u}_0, \mathbf{u}_1, \dots$ be a sequence of t-dimensional matrix-method pseudorandom vectors of maximum period $p^t - 1$. Then for $1 \le N \le p^t - 1$ the discrepancy D_N of the first N terms of the sequence* (16) *satisfies*

$$D_N = O_{\boldsymbol{\alpha},t,\varepsilon}\left(\max\left(p^{-1},\ N^{-1/((\tau-1)s+1)+\varepsilon},\ N^{-1/2}p^{t/4}(\log p)^{1/2}(\log N)^{s+t}\right)\right)$$

for all $\varepsilon > 0$, where the implied constant depends only on $\boldsymbol{\alpha}$, t, and ε.

Proof. Since the discrepancy bound is trivial if either $N = 1$ or $p = 2$, we can assume that $2 \le N \le p^t - 1$ and $p \ge 3$. We apply Lemma 1 with

$$H = \min\left(\left\lceil N^{1/((\tau-1)s+1)}\right\rceil,\ p-1\right). \tag{19}$$

Then $2 \le H \le N$ and

$$D_N = O_{s,t}\left(\frac{1}{H} + \frac{1}{N}\sum_{\substack{\mathbf{h}\in\mathbb{Z}^{s+t}\\ 0<M(\mathbf{h})\le H}} \frac{1}{r(\mathbf{h})}\left|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\right|\right). \tag{20}$$

We write $\mathbf{h} = (\mathbf{h}_1, \mathbf{h}_2)$ with $\mathbf{h}_1 \in \mathbb{Z}^s$ and $\mathbf{h}_2 \in \mathbb{Z}^t$. If $\mathbf{h}_2 = \mathbf{0}$, then the contribution to the sum over $\mathbf{h}$ in (20) is

$$\sum_{\substack{\mathbf{h}_1\in\mathbb{Z}^{s}\\ 0<M(\mathbf{h}_1)\le H}} \frac{1}{r(\mathbf{h}_1)}\left|\sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}_1\cdot\boldsymbol{\alpha}))\right| = O_{\boldsymbol{\alpha},\varepsilon}\left(H^{(\tau-1)s+\varepsilon}\right) \tag{21}$$

for any fixed $\varepsilon > 0$ by Lemma 4. For the remaining $\mathbf{h}$ we have $\mathbf{h}_2 \ne \mathbf{0}$ and $M(\mathbf{h}_2) \le H < p$, hence $\mathbf{h}_2 \not\equiv \mathbf{0} \pmod p$. Now by Lemma 5,

$$\left|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\right| = |E_N(\mathbf{h}_1,\mathbf{h}_2)| = O_t\left(N^{1/2}p^{t/4}(\log p)^{1/2}\right),$$

and so

$$\sum_{\substack{\mathbf{h}\in\mathbb{Z}^{s+t},\mathbf{h}_2\neq\mathbf{0}\\ 0<M(\mathbf{h})\leq H}} \frac{1}{r(\mathbf{h})}\left|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\right| = O_t\Bigg(N^{1/2}p^{t/4}(\log p)^{1/2} \sum_{\substack{\mathbf{h}\in\mathbb{Z}^{s+t},\,\mathbf{h}_2\neq\mathbf{0}\\ 0<M(\mathbf{h})\leq H}} \frac{1}{r(\mathbf{h})}\Bigg)$$

$$= O_{s,t}\left(N^{1/2}p^{t/4}(\log p)^{1/2}(\log H)^{s+t}\right).$$

By combining this bound with (20) and (21) and using the expression for H in (19), we complete the proof. □

Corollary 1. *Consider the special case of Theorem 2 where $\boldsymbol{\alpha} \in \mathbb{R}^s$ is of finite type $\tau = 1$. Then for $2 \leq N \leq p^t - 1$ the discrepancy D_N of the first N terms of the sequence* (16) *satisfies*

$$D_N = O_{\boldsymbol{\alpha},t}\left(\max\left(p^{-1},\ N^{-1/2}p^{t/4}(\log p)^{1/2}(\log N)^{s+t}\right)\right)$$

with an implied constant depending only on $\boldsymbol{\alpha}$ and t.

Remark 3. Well-known examples of points $\boldsymbol{\alpha} \in \mathbb{R}^s$ of finite type $\tau = 1$ are the following: (i) $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ with real algebraic numbers $\alpha_1, \ldots, \alpha_s$ such that $1, \alpha_1, \ldots, \alpha_s$ are linearly independent over $\mathbb{Q}$ (see [16]); (ii) $\boldsymbol{\alpha} = (\mathrm{e}^{q_1}, \ldots, \mathrm{e}^{q_s})$ with distinct nonzero rational numbers $q_1, \ldots, q_s$ (see [1]).

Remark 4. It is obvious that Remark 1 applies also to Theorem 2, and so the term of order of magnitude p^{-1} is needed in the bounds on D_N in Theorem 2 and Corollary 1.

References

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

[2] M. Drmota and R. F. Tichy, Sequences, Discrepancies and Applications, Vol. 1651, Lecture Notes in Math., *Springer, Berlin*, 1997.

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

[4] L. Kuipers and H. Niederreiter, Uniform Distribution of Sequences, *Wiley, New York*, 1974, reprint, *Dover Publications, Mineola, NY*, 2006.

[5] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, *Cambridge University Press, Cambridge*, 1994.

[6] H. Niederreiter, Application of diophantine approximations to numerical integration, Diophantine Approximation and Its Applications, (C. F. Osgood, ed.), *Academic Press, New York*, 1973, 129–199.

[7] H. Niederreiter, Statistical independence properties of pseudorandom vectors produced by matrix generators, *J. Comp. Applied Math.* **31** (1990), 139–151.

[8] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, *SIAM, Philadelphia*, 1992.

[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, A discrepancy bound for hybrid sequences involving digital explicit inversive pseudorandom numbers, *Unif. Distrib. Theory* **5** (2010), 53–63.

[12] H. Niederreiter, Quasi-Monte Carlo methods, Encyclopedia of Quantitative Finance, (R. Cont, ed.), *Wiley, Chichester*, 2010, 1460–1472.

[13] H. Niederreiter and A. Winterhof, Discrepancy bounds for hybrid sequences involving digital explicit inversive pseudorandom numbers, *Unif. Distrib. Theory* **6** (2011), 33–56.

[14] G. Ökten, A probabilistic result on the discrepancy of a hybrid-Monte Carlo sequence and applications, *Monte Carlo Methods Appl.* **2** (1996), 255–270.

[15] G. Ökten, B. Tuffin and V. Burago, 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.

[16] W. M. Schmidt, Simultaneous approximation to algebraic numbers by rationals, *Acta Math.* **125** (1970), 189–201.

[17] J. Spanier, Quasi-Monte Carlo methods for particle transport problems, Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Vol. 106, Lecture Notes in Statistics, (H. Niederreiter and P. J.-S. Shiue, eds.), *Springer, New York*, 1995, 121–148.

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 January 10, 2011)