Uniform Distribution Theory **5** (2010), no.1, 53–63

uniform distribution theory

A DISCREPANCY BOUND FOR HYBRID SEQUENCES INVOLVING DIGITAL EXPLICIT INVERSIVE PSEUDORANDOM NUMBERS

Harald Niederreiter

ABSTRACT. We establish the first nontrivial deterministic discrepancy bound for hybrid sequences composed of Kronecker sequences and sequences of digital explicit inversive pseudorandom numbers.

Communicated by Reinhard Winkler

Dedicated to the memory of Professor Edmund Hlawka

1. Introduction

This work is motivated by applications of the theory of uniform distribution modulo 1 to numerical analysis. The applications of low-discrepancy sequences to quasi-Monte Carlo methods for multidimensional numerical integration are classical and well known; see [7], [8], [12], [13] for accounts of the classical theory and [15] for a more recent survey. The stochastic counterparts of quasi-Monte Carlo methods, namely Monte Carlo methods, work with sequences of pseudorandom numbers. It was an idea of Spanier [22] to combine the advantages of quasi-Monte Carlo methods (faster convergence) and Monte Carlo methods (statistical error estimation) by using so-called hybrid sequences. 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).

2010 Mathematics Subject Classification: 11K38, 11K45, 65C05, 65C10.
Keywords: Discrepancy, hybrid sequence, Kronecker sequence, inversive sequence, quasi-Monte Carlo method.

The Koksma-Hlawka inequality (see [6], [9, Section 2.5]) provides an error bound for numerical integration in terms of the discrepancy of the integration nodes. It is therefore an important issue for the numerical practice to establish discrepancy bounds for hybrid sequences. Probabilistic results on the discrepancy of hybrid sequences were shown in [5], [19], [20]. The first deterministic discrepancy bounds for various types of hybrid sequences were proved in [16] and in the follow-up paper [17].

In the present paper, we establish a deterministic discrepancy bound for a type of hybrid sequence of practical interest that was not considered previously. In detail, we study hybrid sequences obtained by "mixing" Kronecker sequences and sequences of digital explicit inversive pseudorandom numbers (or digital explicit inversive sequences, for short). In Section 2 we recall the construction of the latter sequences. Some auxiliary results are collected in Section 3. The main result, namely a deterministic discrepancy bound for hybrid sequences composed of Kronecker sequences and digital explicit inversive sequences, is presented in Section 4.

2. Digital explicit inversive sequences

We describe the digital explicit inversive sequences introduced by Niederreiter and Winterhof [18]. Let $q = p^k$ with a prime number p and an integer $k \geqslant 1$. Let $\mathbb{F}_q$ denote the finite field of order q and let $\{\beta_1, \ldots, \beta_k\}$ be an ordered basis of $\mathbb{F}_q$ as a vector space over its prime subfield $\mathbb{F}_p$. Define $\xi_n \in \mathbb{F}_q$, $n = 0, 1, \ldots$, by

$$\xi_n := \sum_{l=1}^{k} n_l \, \beta_l$$

if

$$n \equiv \sum_{l=1}^{k} n_l \, p^{l-1} \pmod{q} \quad \text{with } n_l \in \mathbb{Z}_p \text{ for } 1 \leqslant l \leqslant k,$$

where $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is the least residue system modulo p. For $\varrho \in \mathbb{F}_q$, we put $\overline{\varrho} := \varrho^{-1} \in \mathbb{F}_q$ if $\varrho \neq 0$ and $\overline{\varrho} := 0 \in \mathbb{F}_q$ if $\varrho = 0$. Now we choose $\alpha \in \mathbb{F}_q^*$ and $\delta \in \mathbb{F}_q$. Then we define

$$\gamma_n := \overline{\alpha \xi_n + \delta} \in \mathbb{F}_q \qquad \text{for } n = 0, 1, \ldots. \tag{1}$$

Note that the sequence $\gamma_0, \gamma_1, \ldots$ is periodic with least period q. Next we identify $\mathbb{F}_p$ with $\mathbb{Z}_p$ and we write

$$\gamma_n = \sum_{l=1}^{k} c_{n,l}\, \beta_l \qquad \text{for } n = 0, 1, \ldots, \tag{2}$$

with all $c_{n,l} \in \mathbb{F}_p = \mathbb{Z}_p$. Then a *digital explicit inversive sequence* is defined by

$$z_n := \sum_{l=1}^{k} c_{n,l}\, p^{-l} \in [0,1) \qquad \text{for } n = 0, 1, \ldots. \tag{3}$$

It is clear that the sequence $z_0, z_1, \ldots$ is periodic with least period q. In the special case $k = 1$ we obtain an *explicit inversive congruential sequence* as introduced by Eichenauer-Herrmann [4] and further studied in [14]. Because of its periodicity, it is meaningful to consider only the first $N \leqslant q$ terms of a digital explicit inversive sequence.

3. Auxiliary results

First of all, we recall the definition of discrepancy. For an arbitrary dimension $m \geqslant 1$, let $[0,1)^m$ be the m-dimensional half-open unit cube. Given N points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1} \in [0,1)^m$ and a subinterval J of $[0,1)^m$, we write $A(J; N)$ for the number of integers n with $0 \leqslant n \leqslant N-1$ such that $\mathbf{x}_n \in J$. Then the *discrepancy* D_N of these points 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 λ_m denotes the m-dimensional Lebesgue measure.

Next we recall the Erdös-Turán-Koksma inequality for hybrid sequences which was shown in [17]. For integers $s \geqslant 1$ and $t \geqslant 1$, we consider points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1} \in [0,1)^{s+t}$ which we write in the form $\mathbf{x}_n = (\mathbf{y}_n, \mathbf{z}_n)$ with $\mathbf{y}_n \in [0,1)^s$ and $\mathbf{z}_n \in [0,1)^t$ for $0 \leqslant n \leqslant N-1$. The points $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1}$ are arbitrary. The points $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{N-1}$ are such that all their coordinates are rational numbers with denominator b^k, where $b \geqslant 2$ and $k \geqslant 1$ are fixed integers. The version of the Erdös-Turán-Koksma inequality in [17] provides an upper bound on the discrepancy of the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in terms of exponential sums.

Before we can state this inequality, we need further notation. With $b \geqslant 2$ as above, we use the complete residue system modulo b given by

$$C(b) := (-b/2, b/2] \cap \mathbb{Z}.$$

For $k \geqslant 1$ as above, let $C(b)^k$ be the set of k-tuples of elements of $C(b)$. For $(h_1, \ldots, h_k) \in C(b)^k$, we put

$$Q_b(h_1, \ldots, h_k) := \begin{cases} 1 & \text{if } (h_1, \ldots, h_k) = \mathbf{0}, \\ b^{-d} \csc(\pi \, |h_d| \, / b) & \text{if } (h_1, \ldots, h_k) \neq \mathbf{0}, \end{cases} \tag{4}$$

where $d = d(h_1, \ldots, h_k)$ is the largest l with $h_l \neq 0$. We write $C(b)^{t \times k}$ for the set of $t \times k$ matrices with entries from $C(b)$. For $\mathcal{H} = (h_{j,l}) \in C(b)^{t \times k}$, we define

$$W_b(\mathcal{H}) := \prod_{j=1}^{t} Q_b(h_{j,1}, \ldots, h_{j,k}). \tag{5}$$

Let again $\mathcal{H} = (h_{j,l}) \in C(b)^{t \times k}$ and let $\mathbf{z} = \left(z^{(1)}, \ldots, z^{(t)}\right) \in [0,1)^t$ be a point for which each coordinate is a rational number with fixed denominator b^k. For each $j = 1, \ldots, t$, we have a unique representation

$$z^{(j)} = \sum_{l=1}^{k} w_l^{(j)} \, b^{-l} \qquad \text{with all } w_l^{(j)} \in \{0, 1, \ldots, b-1\}.$$

Then we define

$$\mathcal{H} \otimes \mathbf{z} := \sum_{j=1}^{t} \sum_{l=1}^{k} h_{j,l} \, w_l^{(j)}. \tag{6}$$

This operation depends of course on the base b, but for the sake of simplicity we suppress this dependence in the notation. The value of b will always be clear from the context.

For any $\mathbf{h} = (h_1, \ldots, h_t) \in \mathbb{Z}^t$, we put

$$M(\mathbf{h}) := \max_{1 \leqslant j \leqslant t} |h_j|, \qquad r(\mathbf{h}) := \prod_{j=1}^{t} \max(|h_j|, 1). \tag{7}$$

We write $\mathrm{e}(u) = \mathrm{e}^{2\pi i u}$ for $u \in \mathbb{R}$. We also 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. Now we can state the version of the Erdös-Turán-Koksma inequality in [17].

Lemma 1. *Let $b \geqslant 2$, $k \geqslant 1$, $s \geqslant 1$, and $t \geqslant 1$ be integers. Let the points $\mathbf{x}_n = (\mathbf{y}_n, \mathbf{z}_n) \in [0,1)^{s+t}$, $n = 0, 1, \ldots, N-1$, be as above and let D_N be their discrepancy. Then for any integer $H \geqslant 1$ we have*

$$D_N = O_{s,t}\left(\frac{1}{b^k} + \frac{1}{H} + \frac{1}{N} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^s, \ \mathcal{H} \in C(b)^{t \times k} \\ M(\mathbf{h}) \leqslant H}}^{*} \frac{W_b(\mathcal{H})}{r(\mathbf{h})} \left| \sum_{n=0}^{N-1} \mathrm{e}\left(\mathbf{h} \cdot \mathbf{y}_n + \frac{1}{b} \mathcal{H} \otimes \mathbf{z}_n\right) \right| \right),$$

where $M(\mathbf{h})$ and $r(\mathbf{h})$ are as in (7) and $W_b(\mathcal{H})$ is given by (4) and (5). The asterisk signifies that the pair $(\mathbf{h}, \mathcal{H}) = (\mathbf{0}, 0)$ is omitted from the range of summation.

The following lemma was shown in [16]. We again use the notation in (7). We write also $\|u\| = \min(\{u\}, 1 - \{u\})$ for the distance from $u \in \mathbb{R}$ to the nearest integer. Note that if $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_s) \in \mathbb{R}^s$ is such that $1, \alpha_1, \dots, \alpha_s$ are linearly independent over $\mathbb{Q}$, then $\|\mathbf{h} \cdot \boldsymbol{\alpha}\| > 0$ for all $\mathbf{h} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

Lemma 2. *Let s be an arbitrary positive integer and let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be such that there exist real numbers $\sigma \geqslant 1$ and $c > 0$ with*

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

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

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

The following is a standard definition regarding the simultaneous diophantine approximation character of $\boldsymbol{\alpha} \in \mathbb{R}^s$ (see e.g. [11, Definition 6.1]).

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

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

Remark 1. As noted in [11, p. 164], it is an easy consequence of Minkowski's linear forms theorem that we always have $\eta \geqslant 1$. Well-known examples of points $\boldsymbol{\alpha} \in \mathbb{R}^s$ of finite type $\eta = 1$ are the following: (i) $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_s)$ with real algebraic numbers $\alpha_1, \dots, \alpha_s$ such that $1, \alpha_1, \dots, \alpha_s$ are linearly independent over $\mathbb{Q}$ (see [21]); (ii) $\boldsymbol{\alpha} = (\mathrm{e}^{r_1}, \dots, \mathrm{e}^{r_s})$ with distinct nonzero rational numbers $r_1, \dots, r_s$ (see [1]).

Next we state a bound on character sums which is shown in the proof of [2, Theorem 1].

Lemma 3. *Let $q = p^k$ with a prime p and an integer $k \geqslant 1$ and let χ be the canonical additive character of the finite field $\mathbb{F}_q$. Let $\gamma_0, \gamma_1, \dots$ be the sequence defined by (1). Then for any integers $0 \leqslant f_1 < f_2 < \cdots < f_m < q$, for any $\mu_1, \dots, \mu_m \in \mathbb{F}_q$ not all 0, and for $1 \leqslant N \leqslant q$, we have*

$$\left| \sum_{n=0}^{N-1} \chi\left(\sum_{i=1}^{m} \mu_i \gamma_{n+f_i} \right) \right| = O_m\left(2^{(k-1)m+k} k q^{1/2} (1 + \log p)^k\right).$$

4. The main result

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{R}^s$ for an arbitrary dimension $s \geqslant 1$. The corresponding Kronecker sequence is the sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \ldots$, of fractional parts. It is uniformly distributed if and only if $1, \alpha_1, \ldots, \alpha_s$ are linearly independent over $\mathbb{Q}$ (see [3, Theorem 1.76]). If $\boldsymbol{\alpha}$ is of small finite type η, then the Kronecker sequence has a small discrepancy (see [9, p. 132, Exercise 3.17] and [16, Lemma 6]).

Let $z_0, z_1, \ldots$ be a digital explicit inversive sequence as defined in (3). Let $q = p^k$ be as in Section 2. For a given integer t with $1 \leqslant t \leqslant q$, we choose integers $0 \leqslant d_1 < d_2 < \cdots < d_t < q$. Now we consider the hybrid sequence

$$\mathbf{x}_n = (\{n\boldsymbol{\alpha}\}, z_{n+d_1}, \ldots, z_{n+d_t}) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots. \tag{8}$$

We establish an upper bound on the discrepancy of this hybrid sequence by using Lemma 1 with $b = p$. For this purpose, we employ the same notation as in Section 3. In particular, we put

$$\mathbf{z}_n = (z_{n+d_1}, \ldots, z_{n+d_t}) \in [0,1)^t, \quad n = 0, 1, \ldots. \tag{9}$$

For $\mathbf{h} \in \mathbb{Z}^s$, a $t \times k$ matrix $\mathcal{H} \in C(p)^{t \times k}$, and an integer $N \geqslant 1$, we introduce the exponential sum

$$E_N(\mathbf{h}, \mathcal{H}) := \sum_{n=0}^{N-1} \mathrm{e}\left(n(\mathbf{h} \cdot \boldsymbol{\alpha}) + \frac{1}{p}\mathcal{H} \otimes \mathbf{z}_n\right). \tag{10}$$

Lemma 4. *Let $q = p^k$ with a prime p and an integer $k \geqslant 1$. Let $\boldsymbol{\alpha} \in \mathbb{R}^s$, $\mathbf{h} \in \mathbb{Z}^s$, and let the matrix $\mathcal{H} \in C(p)^{t \times k}$ be nonzero. Then for the exponential sum $E_N(\mathbf{h}, \mathcal{H})$ in (10) we have*

$$|E_N(\mathbf{h}, \mathcal{H})| = O_t\left(2^{(k-1)t+k/2} k^{1/2} N^{1/2} q^{1/4} (1 + \log p)^{k/2}\right) \qquad \text{for } 1 \leqslant N \leqslant q.$$

Proof. Let $\{\beta_1, \ldots, \beta_k\}$ be the ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ as in Section 2 and let $\{\sigma_1, \ldots, \sigma_k\}$ be its dual basis. Then it is well known (see [10, p. 58]) that the coefficients $c_{n,l}$ in (2) can be represented as

$$c_{n,l} = \mathrm{Tr}(\sigma_l \gamma_n),$$

where Tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Now for a nonzero matrix $\mathcal{H} = (h_{j,l}) \in C(p)^{t \times k}$ and a point $\mathbf{z}_n$ in (9), we obtain by the $\mathbb{F}_p$-linearity of the

trace that

$$\begin{aligned}
\mathrm{e}\left(\frac{1}{p}\mathcal{H} \otimes \mathbf{z}_n\right) &= \mathrm{e}\left(\frac{1}{p}\sum_{j=1}^{t}\sum_{l=1}^{k} h_{j,l}\, c_{n+d_j,l}\right) \\
&= \mathrm{e}\left(\frac{1}{p}\sum_{j=1}^{t}\sum_{l=1}^{k} h_{j,l}\, \mathrm{Tr}(\sigma_l\, \gamma_{n+d_j})\right) \\
&= \mathrm{e}\left(\frac{1}{p}\mathrm{Tr}\left(\sum_{j=1}^{t}\sum_{l=1}^{k} h_{j,l}\, \sigma_l\, \gamma_{n+d_j}\right)\right) \\
&= \chi\left(\sum_{j=1}^{t} \mu_j\, \gamma_{n+d_j}\right),
\end{aligned}$$

where χ is the canonical additive character of $\mathbb{F}_q$ and

$$\mu_j = \sum_{l=1}^{k} h_{j,l}\, \sigma_l \in \mathbb{F}_q \qquad \text{for } 1 \leqslant j \leqslant t.$$

Since the matrix $\mathcal{H}$ is nonzero, the elements $\mu_1, \ldots, \mu_t$ are not all 0. By what we have just shown, we can write

$$E_N(\mathbf{h}, \mathcal{H}) = \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h} \cdot \boldsymbol{\alpha}))\chi\left(\sum_{j=1}^{t} \mu_j\, \gamma_{n+d_j}\right).$$

Then for $1 \leqslant N \leqslant q$ we obtain

$$\begin{aligned}
|E_N(\mathbf{h}, \mathcal{H})|^2 &= \sum_{m,n=0}^{N-1} \mathrm{e}((m-n)(\mathbf{h} \cdot \boldsymbol{\alpha}))\chi\left(\sum_{j=1}^{t} \mu_j \left(\gamma_{m+d_j} - \gamma_{n+d_j}\right)\right) \\
&\leqslant N + 2\left|\sum_{\substack{m,n=0 \\ m>n}}^{N-1} \mathrm{e}((m-n)(\mathbf{h} \cdot \boldsymbol{\alpha}))\chi\left(\sum_{j=1}^{t} \mu_j \left(\gamma_{m+d_j} - \gamma_{n+d_j}\right)\right)\right| \\
&= N + 2\left|\sum_{d=1}^{N-1}\sum_{n=0}^{N-1-d} \mathrm{e}(d(\mathbf{h} \cdot \boldsymbol{\alpha}))\chi\left(\sum_{j=1}^{t} \mu_j \left(\gamma_{n+d+d_j} - \gamma_{n+d_j}\right)\right)\right| \\
&\leqslant N + 2\sum_{d=1}^{N-1}\left|\sum_{n=0}^{N-1-d} \chi\left(\sum_{j=1}^{t} \mu_j \left(\gamma_{n+d+d_j} - \gamma_{n+d_j}\right)\right)\right|.
\end{aligned}$$

Next we consider the character sum inside the last absolute value bars. Recall that $1 \leqslant N \leqslant q$, and so $1 \leqslant d < q$. Suppose that d is such that $d \equiv d_j - d_\ell \pmod q$ for some $1 \leqslant j, \ell \leqslant t$ with $j \neq \ell$. There are $O(t^2)$ such values of d. For these values of d, we bound the absolute value of the character sum trivially by N. If d is not of the above form, then the absolute value of the character sum is

$$O_t\left(2^{2(k-1)t+k} k q^{1/2} (1+\log p)^k\right)$$

according to Lemma 3 with $m = 2t$. Altogether, we obtain

$$\begin{aligned} |E_N(\mathbf{h}, \mathcal{H})|^2 &\leqslant N + O_t(N) + O_t\left(2^{2(k-1)t+k} k N q^{1/2} (1+\log p)^k\right) \\ &= O_t\left(2^{2(k-1)t+k} k N q^{1/2} (1+\log p)^k\right), \end{aligned}$$

which yields the desired result. □

Now we use the notion of finite type introduced in Definition 1.

Theorem 1. *Let $q = p^k$ with a prime p and an integer $k \geqslant 1$. Let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be of finite type η. Then for $1 \leqslant N \leqslant q$ the discrepancy D_N of the first N terms of the sequence* (8) *satisfies*

$$D_N = O_{\boldsymbol{\alpha},t,\varepsilon}\Bigg(\max\big(N^{-1/((\eta-1)s+1)+\varepsilon}, \\ 2^{(k-1)t+k/2} k^{1/2} N^{-1/2} (\log N)^s q^{1/4} (\log q)^t (1+\log p)^{k/2}\big)\Bigg)$$

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

Proof. Since the discrepancy bound is trivial for $N = 1$, we can assume that $2 \leqslant N \leqslant q$. We apply Lemma 1 with $b = p$ and

$$H = \left\lceil N^{1/((\eta-1)s+1)} \right\rceil.$$

Then $2 \leqslant H \leqslant N \leqslant q$ and

$$D_N = O_{s,t}\left(\frac{1}{H} + \frac{1}{N} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^s,\ \mathcal{H} \in C(p)^{t \times k} \\ M(\mathbf{h}) \leqslant H}}^{*} \frac{W_p(\mathcal{H})}{r(\mathbf{h})} |E_N(\mathbf{h}, \mathcal{H})|\right). \tag{11}$$

We first consider the pairs $(\mathbf{h}, \mathcal{H})$ in the summation in (11) with $\mathbf{h} \neq \mathbf{0}$, $M(\mathbf{h}) \leqslant H$, and $\mathcal{H} = 0$. Then $W_p(\mathcal{H}) = 1$ by (4) and (5). Furthermore by (10),

$$E_N(\mathbf{h}, \mathcal{H}) = \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h} \cdot \boldsymbol{\alpha})).$$

Now fix an $\varepsilon > 0$. Then the contribution of these pairs to the sum in (11) is

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

$$= O_{\boldsymbol{\alpha},\varepsilon}\left(N^{(\eta-1)s/((\eta-1)s+1)+\varepsilon}\right) \tag{12}$$

according to Lemma 2.

The remaining pairs $(\mathbf{h},\mathcal{H})$ in the summation in (11) satisfy $M(\mathbf{h}) \leqslant H$ and $\mathcal{H} \neq 0$. For these pairs we can apply Lemma 4 to obtain

$$\sum_{\substack{\mathbf{h}\in\mathbb{Z}^s,\ \mathcal{H}\in C(p)^{t\times k}\\ M(\mathbf{h})\leqslant H,\ \mathcal{H}\neq 0}} \frac{W_p(\mathcal{H})}{r(\mathbf{h})}\,|E_N(\mathbf{h},\mathcal{H})|$$

$$= O_t\left(2^{(k-1)t+k/2}k^{1/2}N^{1/2}q^{1/4}(1+\log p)^{k/2}\sum_{\substack{\mathbf{h}\in\mathbb{Z}^s,\ \mathcal{H}\in C(p)^{t\times k}\\ M(\mathbf{h})\leqslant H,\ \mathcal{H}\neq 0}} \frac{W_p(\mathcal{H})}{r(\mathbf{h})}\right).$$

Now clearly

$$\sum_{\substack{\mathbf{h}\in\mathbb{Z}^s\\ M(\mathbf{h})\leqslant H}} r(\mathbf{h})^{-1} = O_s\left((\log H)^s\right) = O_s\left((\log N)^s\right).$$

Moreover, by [13, Lemma 3.13] we have

$$\sum_{\substack{\mathcal{H}\in C(p)^{t\times k}\\ \mathcal{H}\neq 0}} W_p(\mathcal{H}) = O_t\left((\log q)^t\right),$$

and so

$$\sum_{\substack{\mathbf{h}\in\mathbb{Z}^s,\ \mathcal{H}\in C(p)^{t\times k}\\ M(\mathbf{h})\leqslant H,\ \mathcal{H}\neq 0}} \frac{W_p(\mathcal{H})}{r(\mathbf{h})}\,|E_N(\mathbf{h},\mathcal{H})|$$

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

By combining this bound with (11) and (12), we complete the proof. □

Corollary 1. *Let $q = p^k$ with a prime p and an integer $k \geqslant 1$. Let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be of finite type $\eta = 1$. Then for $2 \leqslant N \leqslant q$ the discrepancy D_N of the first N terms of the sequence* (8) *satisfies*

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

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

Remark 2. Fix $\boldsymbol{\alpha} \in \mathbb{R}^s$ of finite type and the integers $k \geqslant 1$ and $t \geqslant 1$. For each prime p, choose an integer N_p such that there exist constants $C > 0$ and $\varepsilon > 0$ with $C(p^k)^{1/2+\varepsilon} \leqslant N_p \leqslant p^k$ for all p. Then for each prime p, we can consider a corresponding hybrid sequence (8) and the discrepancy D_{N_p} of its first N_p terms. Theorem 1 implies then that $D_{N_p} \to 0$ as $p \to \infty$, and so in this sense we get asymptotic uniform distribution. In view of the Koksma-Hlawka inequality, the corresponding quasi-Monte Carlo method yields a convergent numerical integration scheme for integrands of bounded variation in the sense of Hardy and Krause.

REFERENCES

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

[2] CHEN, Z.X. – GOMEZ, D. – WINTERHOF, A.: *Distribution of digital explicit inversive pseudorandom numbers and their binary threshold sequence*, in: *Monte Carlo and Quasi-Monte Carlo Methods 2008* (P. L'Ecuyer and A. Owen, eds.), pp. 249–258, Springer, Berlin, 2009.

[3] DRMOTA, M. – TICHY, R.F.: *Sequences, Discrepancies and Applications*, Lecture Notes in Mathematics, Vol. **1651**, Springer, Berlin, 1997.

[4] EICHENAUER-HERRMANN, J.: *Statistical independence of a new class of inversive congruential pseudorandom numbers*, Math. Comp. **60** (1993), 375–384.

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

[6] HLAWKA, E.: *Funktionen von beschränkter Variation in der Theorie der Gleichverteilung*, Ann. Mat. Pura Appl. (IV) **54** (1961), 325–333.

[7] HLAWKA, E.: *Uniform distribution modulo 1 and numerical analysis*, Compositio Math. **16** (1964), 92–105.

[8] HUA, L.K. – WANG, Y.: *Applications of Number Theory to Numerical Analysis*, Springer, Berlin, 1981.

[9] KUIPERS, L. – NIEDERREITER, H.: *Uniform Distribution of Sequences*, Wiley, New York, 1974; reprint, Dover Publications, Mineola, NY, 2006.

[10] LIDL, R. – NIEDERREITER, H.: *Finite Fields*, Cambridge University Press, Cambridge, 1997.

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

[12] NIEDERREITER, H.: *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.

[13] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[14] NIEDERREITER, H.: *On a new class of pseudorandom numbers for simulation methods*, J. Comp. Appl. Math. **56** (1994), 159–167.

[15] NIEDERREITER, H.: *High-dimensional numerical integration*, in: *Applied Mathematics Entering the 21st Century—Invited Talks from the ICIAM 2003 Congress* (J.M. Hill and R. Moore, eds.), pp. 337–351, SIAM, Philadelphia, 2004.

[16] NIEDERREITER, H.: *On the discrepancy of some hybrid sequences*, Acta Arith. **138** (2009), 373–398.

[17] NIEDERREITER, H.: *Further discrepancy bounds and an Erdös-Turán-Koksma inequality for hybrid sequences*, Monatsh. Math., to appear.

[18] NIEDERREITER, H. – WINTERHOF, A.: *Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators*, Acta Arith. **93** (2000), 387–399.

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

[20] 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.

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

[22] 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.

Received November 19, 2009
Accepted January 22, 2010

Harald Niederreiter
RICAM, Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz
and
Department of Mathematics
University of Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg
AUSTRIA
E-mail: ghnied@gmail.com