Uniform Distribution Theory **6** (2011), no.1, 33–56

uniform distribution theory

DISCREPANCY BOUNDS FOR HYBRID SEQUENCES INVOLVING DIGITAL EXPLICIT INVERSIVE PSEUDORANDOM NUMBERS

Harald Niederreiter — Arne Winterhof

ABSTRACT. We consider hybrid sequences, that is, sequences in a multidimensional unit cube that are composed from low-discrepancy sequences and sequences of pseudorandom numbers. We establish the first nontrivial deterministic discrepancy bounds for three kinds of hybrid sequences that are obtained by "mixing" low-discrepancy sequences and digital explicit inversive sequences. Such hybrid sequences are of interest for high-dimensional numerical integration since they combine the advantages of Monte Carlo methods and quasi-Monte Carlo methods.

Communicated by Reinhard Winkler

1. Introduction

Monte Carlo methods and quasi-Monte Carlo methods are important techniques for multidimensional numerical integration. Monte Carlo methods have the advantage that they allow statistical error estimation, whereas quasi-Monte Carlo methods offer the advantage of faster convergence under mild regularity assumptions on the integrand. It was a proposal of Spanier [29] to combine the advantages of Monte Carlo methods and quasi-Monte Carlo methods 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

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

the remaining coordinates stem from the sequence of pseudorandom numbers (or vectors).

It is an interesting issue, both for the theory of uniform distribution and for the applications to numerical integration, to establish discrepancy bounds for hybrid sequences. Probabilistic results on the discrepancy of hybrid sequences were shown in [6], [26], [27]. The first deterministic discrepancy bounds for various types of hybrid sequences were proved in [18], [19], [20].

In the present paper, we consider hybrid sequences that are obtained by "mixing" either Halton sequences or Kronecker sequences with two types of digital explicit inversive sequences. The definitions of these sequences are given in later sections. The case where a Kronecker sequence is "mixed" with a digital explicit inversive sequence in the sense of Section 2 was already treated in [19]. For the remaining three cases, deterministic discrepancy bounds are established below.

In Section 2 we describe the digital explicit inversive sequences of period q, with q a prime power, introduced by Niederreiter and Winterhof [21]. Section 3 collects some auxiliary results on the discrepancy. A crucial bound for character sums over finite fields is proved in Section 4. This bound is used in Section 5 to establish a discrepancy bound for hybrid sequences produced by "mixing" Halton sequences and digital explicit inversive sequences in the sense of Section 2. In Section 6 we describe the second type of digital explicit inversive sequences, namely those of order T with T a divisor of $q-1$, where q is again a prime power. Sections 7 and 8 contain discrepancy bounds for hybrid sequences obtained by "mixing" these digital explicit inversive sequences with Halton sequences and Kronecker sequences, respectively.

2. Digital explicit inversive sequences of period q

We describe the digital explicit inversive sequences introduced by Niederreiter and Winterhof [21]. These sequences have attracted considerable interest in the area of pseudorandom number generation (see [1], [2], [11], [13], [21], [22], [23], [28]).

Let $q = p^k$ with a prime 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 uniquely determined $c_{n,l} \in \mathbb{F}_p = \mathbb{Z}_p$. 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 [17]. Because of its periodicity, it is meaningful to consider only the first $N \leqslant q$ terms of a digital explicit inversive sequence.

3. Basic facts on the discrepancy

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

$$D_L := \sup_J \left| \frac{A(J; L)}{L} - \lambda_m(J) \right|, \tag{4}$$

where the supremum is extended over all half-open subintervals J of $[0, 1)^m$ and the counting function $A(J; L)$ is given by

$$A(J; L) := \#\{0 \leqslant n \leqslant L-1 : \mathbf{y}_n \in J\}. \tag{5}$$

Note that we always have $LD_L \geqslant 1$ (see [9, p. 93]) and $D_L \leqslant 1$. The *star discrepancy* D_L^* of $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{L-1}$ is obtained by letting the supremum in (4)

run only over the half-open intervals $J \subseteq [0,1)^m$ with one vertex at the origin. According to [16, Proposition 2.4] we have

$$D_L \leqslant 2^m D_L^*. \tag{6}$$

For a dimension $t \geqslant 1$, we consider now points $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{N-1} \in [0,1)^t$ with the property that all their coordinates are rational numbers with denominator b^k, where $b \geqslant 2$ and $k \geqslant 1$ are fixed integers. 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

$$Q_b(h_1, \ldots, h_k) := \begin{cases} 1 & \text{if } (h_1, \ldots, h_k) = \mathbf{0}, \\ b^{-d} \csc(\pi \, |h_d| \, / b) & \text{if } (h_1, \ldots, h_k) \neq \mathbf{0}, \end{cases} \tag{7}$$

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

$$W_b(\mathcal{H}) := \prod_{j=1}^{t} Q_b(h_{j,1}, \ldots, h_{j,k}). \tag{8}$$

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

$$\mathcal{H} \otimes \mathbf{z} := \sum_{j=1}^{t} \sum_{l=1}^{k} h_{j,l} \, w_l^{(j)}. \tag{9}$$

The operation in (9) 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.

We write

$$\mathrm{e}(u) = \mathrm{e}^{2\pi \mathrm{i} u} \quad \text{for } u \in \mathbb{R}.$$

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. Now we recall the following discrepancy bound which is an immediate consequence of [16, Theorem 3.12].

Lemma 1. *Let $b \geqslant 2$, $k \geqslant 1$, and $t \geqslant 1$ be integers. Let the points*

$$\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{N-1} \in [0,1)^t$$

be such that all their coordinates are rational numbers with denominator b^k. Then for the discrepancy D_N of these points we have

$$D_N = O_t\left(\frac{1}{b^k} + \frac{1}{N}\sum_{\mathcal{H} \in C(b)^{t\times k}}^{*} W_b(\mathcal{H}) \left|\sum_{n=0}^{N-1} \mathrm{e}\left(\frac{1}{b}\mathcal{H} \otimes \mathbf{z}_n\right)\right|\right),$$

where $W_b(\mathcal{H})$ is given by (7) *and* (8) *and where the asterisk signifies that the zero matrix is omitted from the range of summation.*

Next we recall the Erdős-Turán-Koksma inequality for hybrid sequences which was shown in [20]. For any $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$, we put

$$M(\mathbf{h}) := \max_{1 \leqslant i \leqslant s} |h_i|, \qquad r(\mathbf{h}) := \prod_{i=1}^{s} \max\bigl(|h_i|, 1\bigr). \tag{10}$$

We use $\cdot$ to denote the standard inner product in $\mathbb{R}^s$.

Lemma 2. *Let $b \geqslant 2$, $k \geqslant 1$, $s \geqslant 1$, and $t \geqslant 1$ be integers. Let the points*

$$\mathbf{x}_n = (\mathbf{y}_n, \mathbf{z}_n) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots, N-1,$$

be such that $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1} \in [0,1)^s$ are arbitrary and the coordinates of all points $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{N-1} \in [0,1)^t$ are rational numbers with denominator b^k. Let D_N be the discrepancy of $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$. 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 (10) *and $W_b(\mathcal{H})$ is given by* (7) *and* (8)*. The asterisk signifies that the pair $(\mathbf{h}, \mathcal{H}) = (\mathbf{0}, 0)$ is omitted from the range of summation.*

4. A bound for additive character sums

Let $q = p^k$ with a prime p and an integer $k \geqslant 1$. For $n = 0, 1, \ldots$, let $\xi_n \in \mathbb{F}_q$ and $\gamma_n \in \mathbb{F}_q$ be as in Section 2. For integers $1 \leqslant N \leqslant q$, $1 \leqslant t \leqslant q$, $1 \leqslant B < p$, and $0 \leqslant d_1 < d_2 < \cdots < d_t < q$, and for $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_t) \in \mathbb{F}_q^t$, we introduce the character sum

$$S_N(\boldsymbol{\mu}, B) := \sum_{n=0}^{N-1} \chi\left(\sum_{j=1}^{t} \mu_j \gamma_{Bn+d_j}\right),$$

where χ is a nontrivial additive character of $\mathbb{F}_q$.

Theorem 1. *If $\boldsymbol{\mu} \neq \mathbf{0}$ and the conditions above hold, then we have*

$$|S_N(\boldsymbol{\mu}, B)| = O\left(2^k (B+1)^{(k-1)t} t q^{1/2} (1 + \log p)^k\right).$$

Proof. For fixed j with $1 \leqslant j \leqslant t$ and integers $0 \leqslant d_j < q$, $0 \leqslant n < q$, let

$$d_j = d_{1,j} + d_{2,j} p + \cdots + d_{k,j} p^{k-1}, \quad 0 \leqslant d_{1,j}, d_{2,j}, \ldots, d_{k,j} < p,$$

and

$$n = n_1 + n_2 p + \cdots + n_k p^{k-1}, \qquad 0 \leqslant n_1, n_2, \ldots, n_k < p,$$

be the digit expansions of d_j and n, respectively, in base p.

Put

$$w_{1,j} = 0 \quad \text{and} \quad w_{i+1,j} = \left\lfloor \frac{d_{i,j} + B n_i + w_{i,j}}{p} \right\rfloor, \quad i = 1, 2, \ldots, k.$$

Then we have

$$B n + d_j \equiv z_{1,j} + z_{2,j} p + \cdots + z_{k,j} p^{k-1} \pmod{q}, \quad 0 \leqslant z_{1,j}, z_{2,j}, \ldots, z_{k,j} < p,$$

with

$$z_{i,j} = B n_i + d_{i,j} + w_{i,j} - w_{i+1,j} p, \qquad i = 1, 2, \ldots, k,$$

and

$$\xi_{Bn+d_j} = B \xi_n + \xi_{d_j} + \omega_j,$$

where

$$\omega_j = w_{2,j} \beta_2 + w_{3,j} \beta_3 + \cdots + w_{k,j} \beta_k.$$

Since

$$0 \leqslant w_{i,j} \leqslant B \quad \text{for} \quad i = 2, 3, \ldots, k,$$

we have at most $(B+1)^{k-1}$ possible choices for ω_j and $(B+1)^{(k-1)t}$ possible choices for $(\omega_1, \omega_2, \ldots, \omega_t)$.

We define

$$S_{\omega_j}(d_j) = \{\xi_n : 0 \leqslant n < N,\ \xi_{Bn+d_j} = B\xi_n + \xi_{d_j} + \omega_j\},$$

$$S_{\omega_1,\dots,\omega_k} = S_{\omega_1}(d_1) \cap \ldots \cap S_{\omega_k}(d_k),$$

and note that the latter sets define a partition of $\{\xi_0, \xi_1, \dots, \xi_{N-1}\}$.

For a fixed ordered basis $\{\beta'_1, \dots, \beta'_k\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, we call a set of the form

$$\mathcal{B} = \{\nu + n_1\beta'_1 + \cdots + n_k\beta'_k : 0 \leqslant n_i < N_i,\ i = 1, \dots, k\}$$

for some integers $0 \leqslant N_1, \dots, N_k \leqslant p$ and an element $\nu \in \mathbb{F}_q$ a *box* (including the empty set). Note that $S_{\omega_j}(d_j)$ is a box with respect to the ordered basis $\{\beta'_1, \dots, \beta'_k\} = \{B\beta_1, \dots, B\beta_k\}$ and that the intersection of a family of boxes is the union of at most 2^k boxes. So we can split $S_N(\boldsymbol{\mu}, B)$ into at most

$$2^k(B+1)^{(k-1)t}$$

sums over boxes

$$S_{\mathcal{B}} := \sum_{\xi\in\mathcal{B}} \chi\left(\sum_{j=1}^{t} \mu_j \overline{\alpha\xi + \delta_j}\right)$$

with $\delta_j = \alpha(\xi_{d_j} + \omega_j) + \delta$ for $1 \leqslant j \leqslant t$.

We claim that if $\delta_i = \delta_j$ for some $i \neq j$, then there is no n with $0 \leqslant n < q$ and $\xi = B\xi_n \in \mathcal{B}$, i.e.,

$$\xi_{Bn+d_i} = B\xi_n + \xi_{d_i} + \omega_i \quad \text{and} \quad \xi_{Bn+d_j} = B\xi_n + \xi_{d_j} + \omega_j.$$

Otherwise, suppose n_0 is such a value. Then $\delta_i = \delta_j$ implies $\xi_{d_i} + \omega_i = \xi_{d_j} + \omega_j$ and thus $\xi_{Bn_0+d_i} = \xi_{Bn_0+d_j}$, which leads to $d_i \equiv d_j \pmod q$, a contradiction. So for $\delta_i = \delta_j$ with $i \neq j$,

$$B^{-1}\mathcal{B} \subseteq S_{\omega_i}(d_i) \cap S_{\omega_j}(d_j) = \varnothing,$$

where B^{-1} denotes the inverse of B modulo p.

Using the standard method for completing exponential sums (see [3] or [8, Chapter 12]), we get

$$S_{\mathcal{B}} = \frac{1}{q} \sum_{\varrho\in\mathbb{F}_q} \sum_{\xi\in\mathbb{F}_q} \chi\left(\sum_{j=1}^{t} \mu_j \overline{\alpha\xi + \delta_j} + \varrho\xi\right) \sum_{\zeta\in\mathcal{B}} \chi(-\varrho\zeta).$$

Note that for $\varrho \in \mathbb{F}_q$ the rational functions

$$\sum_{j=1}^{t} \mu_j(\alpha X + \delta_j)^{-1} + \varrho X$$

are not of the form $A^p - A$ with $A \in \overline{\mathbb{F}_q}(X)$ by [21, Lemma 2], and so we can apply the character sum bound in [14] to obtain

$$\left| \sum_{\xi \in \mathbb{F}_q} \chi \left(\sum_{j=1}^{t} \mu_j \, \overline{\alpha\xi + \delta_j} + \varrho\xi \right) \right| = O\left(tq^{1/2}\right).$$

From the proof of [3, Theorem 2] we see that

$$\sum_{\varrho \in \mathbb{F}_q} \left| \sum_{\zeta \in \mathcal{B}} \chi(-\varrho\zeta) \right| \leqslant q(1 + \log p)^k,$$

which completes the proof. □

5. Mixing Halton sequences and digital explicit inversive sequences

We recall the definition of the Halton sequences (see [7], [16, Chapter 3]). For integers $b \geqslant 2$ and $n \geqslant 0$, let

$$n = \sum_{j=0}^{\infty} a_j(n) b^j$$

be the digit expansion of n in base b, where $a_j(n) \in \{0, 1, \ldots, b-1\}$ for all $j \geqslant 0$ and $a_j(n) = 0$ for all sufficiently large j. Then we define the *radical-inverse function* ϕ_b in base b by

$$\phi_b(n) = \sum_{j=0}^{\infty} a_j(n) b^{-j-1}.$$

For a given dimension $s \geqslant 1$, let $b_1, \ldots, b_s$ be pairwise coprime integers $\geqslant 2$. Then the *Halton sequence* (in the bases $b_1, \ldots, b_s$) is given by

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

It is a classical low-discrepancy sequence.

We consider now hybrid sequences that are obtained by "mixing" Halton sequences and digital explicit inversive sequences. As above, we choose a dimension $s \geqslant 1$ and pairwise coprime integers $b_1, \ldots, b_s \geqslant 2$. Furthermore, let $z_0, z_1, \ldots$ be the digital explicit inversive sequence in (3) with least period $q = p^k$, where p is a prime and k is a positive integer. We choose a dimension t with $1 \leqslant t \leqslant q$ and integers $0 \leqslant d_1 < d_2 < \cdots < d_t < q$. Then we define the hybrid sequence

$$\mathbf{x}_n = \left(\phi_{b_1}(n), \ldots, \phi_{b_s}(n), z_{n+d_1}, \ldots, z_{n+d_t}\right) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots \tag{11}$$

We establish the following discrepancy bound for this hybrid sequence.

Theorem 2. *Let $q = p^k$ with a prime p and an integer $k \geqslant 1$. Let $b_1, \ldots, b_s$ be pairwise coprime integers $\geqslant 2$. Then for $1 \leqslant N \leqslant q$ the discrepancy D_N of the first N terms of the sequence* (11) *satisfies*

$$D_N = O_{b_1,\ldots,b_s,t}\left(\left(2^k q^{1/2}(1+\log p)^k (\log q)^t N^{-1}\right)^{1/(s(k-1)t+s+1)}\right)$$

with an implied constant depending only on $b_1, \ldots, b_s$, and t.

P r o o f. Clearly, we can assume that $q \geqslant 3$. We take an integer N with $1 \leqslant N \leqslant q$ and we can assume that

$$N \geqslant 2^{s(k-1)t+s+k+1} q^{1/2}(1+\log p)^k (\log q)^t, \tag{12}$$

for otherwise we have

$$\left(\frac{N}{2^k q^{1/2}(1+\log p)^k (\log q)^t}\right)^{\frac{1}{s(k-1)t+s+1}} < 2,$$

that is,

$$\left(2^k q^{1/2}(1+\log p)^k (\log q)^t N^{-1}\right)^{1/(s(k-1)t+s+1)} > \frac{1}{2},$$

and the discrepancy bound in the theorem is trivial.

We introduce the integers

$$f_i := \left\lfloor \frac{1}{\log b_i} \log\left(\left(\frac{N}{2^k q^{1/2}(1+\log p)^k (\log q)^t}\right)^{\frac{1}{s(k-1)t+s+1}} - 1\right)\right\rfloor \quad \text{for } 1 \leqslant i \leqslant s. \tag{13}$$

The condition (12) guarantees that $f_i \geqslant 0$ for $1 \leqslant i \leqslant s$. Furthermore, we define the positive integer

$$B := b_1^{f_1} \cdots b_s^{f_s}.$$

We assume next that $N \geqslant B$. We first consider an interval $J \subseteq [0,1)^{s+t}$ of the form

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

with $v_1, \ldots, v_s \in \mathbb{Z}$, $0 \leqslant v_i < b_i^{f_i}$ for $1 \leqslant i \leqslant s$, and $0 < w_j \leqslant 1$ for $1 \leqslant j \leqslant t$. By the construction of the Halton sequence, we have $\mathbf{x}_n \in J$ if and only if

$$n \equiv d \pmod{B} \quad \text{and} \quad (z_{n+d_1}, \ldots, z_{n+d_t}) \in \prod_{j=1}^{t}[0, w_j),$$

where d is an integer with $0 \leqslant d < B$ which depends only on J. Thus, $n = B\ell + d$ for some integer ℓ, and the condition $0 \leqslant n \leqslant N-1$ is equivalent to

$$0 \leqslant \ell \leqslant \lfloor (N-d-1)/B \rfloor .$$

Recall that $N \geqslant B \geqslant d+1$. With $A(J;N)$ as in (5), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in (11), we obtain

$$A(J;N) = \# \left\{ 0 \leqslant \ell \leqslant \left\lfloor \frac{N-d-1}{B} \right\rfloor : (z_{B\ell+d+d_1}, \ldots, z_{B\ell+d+d_t}) \in \prod_{j=1}^{t} [0, w_j) \right\}.$$

It follows that

$$A(J;N) = \left\lfloor \frac{N-d-1+B}{B} \right\rfloor \prod_{j=1}^{t} w_j + O\left(\left\lfloor \frac{N-d-1+B}{B} \right\rfloor D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor} \right),$$

where $D^{(B)}_L$ denotes the discrepancy of the L points

$$(z_{B\ell+d+d_1}, \ldots, z_{B\ell+d+d_t}) \in [0,1)^t, \qquad \ell = 0, 1, \ldots, L-1.$$

Therefore

$$A(J;N) = N\lambda_{s+t}(J) + O\left(\left\lfloor \frac{N-d-1+B}{B} \right\rfloor D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor} \right). \tag{14}$$

Now we bound $D^{(B)}_L$ for $1 \leqslant L \leqslant q$. We put

$$\mathbf{z}_n := (z_{Bn+d+d_1}, \ldots, z_{Bn+d+d_t}) \qquad \text{for } n = 0, 1, \ldots$$

and

$$E_L(\mathcal{H}) := \sum_{n=0}^{L-1} \mathrm{e}\left(\frac{1}{p} \mathcal{H} \otimes \mathbf{z}_n \right)$$

for a nonzero $t \times k$ matrix $\mathcal{H} = (h_{j,l}) \in C(p)^{t \times k}$.

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 $\mathbb{F}_p$. By the $\mathbb{F}_p$-linearity of the trace we have

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

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

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

Therefore we can write

$$E_L(\mathcal{H}) = \sum_{n=0}^{L-1} \chi\left(\sum_{j=1}^{t} \mu_j\, \gamma_{Bn+d+d_j}\right).$$

Since the matrix $\mathcal{H}$ is nonzero, the elements $\mu_1, \ldots, \mu_t$ are not all 0. Note that the subscripts of γ can be considered modulo q since the sequence $\gamma_0, \gamma_1, \ldots$ has period q. In order to apply Theorem 1, we need to verify that $B < p$. Since $B = b_1^{f_1} \cdots b_s^{f_s}$ with the f_i as in (13), it suffices to show that

$$\left(\frac{N}{2^k q^{1/2} (1+\log p)^k (\log q)^t}\right)^{\frac{s}{s(k-1)t+s+1}} \leqslant p.$$

Since $N \leqslant q$, it suffices to verify that

$$q^{1/2} \leqslant p^{(k-1)t+1+1/s}.$$

Taking into account that $q = p^k$ and $t \geqslant 1$, it is straightforward to check the above inequality. Thus, we have shown that $B < p$, and so we are now in a position to apply Theorem 1. This yields

$$|E_L(\mathcal{H})| = O_t\left(2^k (B+1)^{(k-1)t} q^{1/2} (1+\log p)^k\right).$$

Then Lemma 1 with $b = p$ implies that

$$LD_L^{(B)} = O_t\left(\frac{L}{q} + 2^k (B+1)^{(k-1)t} q^{1/2} (1+\log p)^k \sum_{\mathcal{H} \in C(p)^{t\times k}}^{*} W_p(\mathcal{H})\right).$$

By [16, Lemma 3.13] we have

$$\sum_{\mathcal{H} \in C(p)^{t\times k}}^{*} W_p(\mathcal{H}) = O_t\left((\log q)^t\right). \tag{15}$$

Hence for $1 \leqslant L \leqslant q$,

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

Together with (14) this yields

$$A(J;N) = N\lambda_{s+t}(J) + O_t\left(2^k (B+1)^{(k-1)t} q^{1/2} (1+\log p)^k (\log q)^t\right). \tag{16}$$

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

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

with

$$v_1, \ldots, v_s \in \mathbb{Z},\ 1 \leqslant v_i \leqslant b_i^{f_i} \quad \text{for } 1 \leqslant i \leqslant s, \quad \text{and} \quad 0 < w_j \leqslant 1 \quad \text{for } 1 \leqslant j \leqslant t.$$

By adding at most B identities of the form (16), we obtain

$$A(J;N) = N\lambda_{s+t}(J) + O_t\left(2^k (B+1)^{(k-1)t+1} q^{1/2} (1+\log p)^k (\log q)^t\right). \tag{17}$$

Finally, we consider an arbitrary half-open interval $J \subseteq [0,1)^{s+t}$ with one vertex at the origin, i.e.,

$$J = \prod_{i=1}^{s}[0, u_i) \times \prod_{j=1}^{t}[0, w_j)$$

with

$$0 < u_i \leqslant 1 \quad \text{for } 1 \leqslant i \leqslant s \quad \text{and} \quad 0 < w_j \leqslant 1 \quad \text{for } 1 \leqslant j \leqslant t.$$

By approximating the u_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 (17) that

$$D_N^* \leqslant \sum_{i=1}^{s} b_i^{-f_i} + O_t\left(2^k (B+1)^{(k-1)t+1} q^{1/2} (1+\log p)^k (\log q)^t N^{-1}\right), \tag{18}$$

where D_N^* is the star discrepancy of the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$. The bound (18) is trivial for $N < B$, and so it holds for all integers $N \leqslant q$ satisfying (12).

By (13) and (12) we have

$$\begin{aligned} b_i^{f_i+1} &> \left(\frac{N}{2^k q^{1/2}(1+\log p)^k(\log q)^t}\right)^{\frac{1}{s(k-1)t+s+1}} - 1 \\ &\geqslant \frac{1}{2}\left(\frac{N}{2^k q^{1/2}(1+\log p)^k(\log q)^t}\right)^{\frac{1}{s(k-1)t+s+1}}. \end{aligned}$$

Thus,

$$\begin{aligned} \sum_{i=1}^{s} b_i^{-f_i} &< \sum_{i=1}^{s} 2b_i \left(2^k q^{1/2}(1+\log p)^k(\log q)^t N^{-1}\right)^{1/(s(k-1)t+s+1)} \\ &= O_{b_1,\ldots,b_s}\left(\left(2^k q^{1/2}(1+\log p)^k(\log q)^t N^{-1}\right)^{1/(s(k-1)t+s+1)}\right). \end{aligned}$$

Furthermore,

$$\begin{aligned} B+1 &\leqslant (b_1^{f_1}+1)\cdots(b_s^{f_s}+1) \\ &\leqslant \left(\frac{N}{2^k q^{1/2}(1+\log p)^k(\log q)^t}\right)^{\frac{s}{s(k-1)t+s+1}}. \end{aligned}$$

Using these bounds in (18), we obtain

$$D_N^* = O_{b_1,\ldots,b_s,t}\left(\left(2^k q^{1/2}(1+\log p)^k(\log q)^t N^{-1}\right)^{1/(s(k-1)t+s+1)}\right).$$

An application of (6) completes the proof. □

Remark 1. It is clear that the proof of Theorem 2 works in the same way if in (11) the s-dimensional Halton sequence is replaced by an s-dimensional generalized Halton sequence in the sense of [5]. This means that in the ith coordinate ($1 \leqslant i \leqslant s$) the jth digit ($j \geqslant 1$) in base b_i can be scrambled by a permutation

$$\pi_{i,j} \text{ of } \{0,1,\ldots,b_i-1\}.$$

The discrepancy bound in Theorem 2 thus holds also if Halton sequences are replaced by generalized Halton sequences.

6. Explicit inversive generators of order T

We recall the definition of the explicit inversive generators that were introduced by Meidl and Winterhof [12] and further analyzed in [1], [13], [24], [25], [30]. Let the finite field $\mathbb{F}_q$ be as in Section 2. Choose $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ and assume that γ has order $T \geqslant 2$ in the multiplicative group $\mathbb{F}_q^*$. Note that T is a divisor of $q-1$, hence $T \leqslant q-1$. Now we define

$$\varrho_n := \overline{\alpha\gamma^n + \beta} \in \mathbb{F}_q \qquad \text{for } n = 0, 1, \ldots, \tag{19}$$

where the bar has the same meaning as in (1). The sequence $\varrho_0, \varrho_1, \ldots$ is periodic with least period T. This sequence is called an *explicit inversive generator of order* T. The maximum period $T = q-1$ is attained if and only if γ is a primitive element of $\mathbb{F}_q$ (i.e., γ is a generator of the cyclic group $\mathbb{F}_q^*$).

We derive pseudorandom numbers from this sequence by proceeding as in Winterhof [30]. As in Section 2, let $\{\beta_1, \ldots, \beta_k\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. We write

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

with uniquely determined $c_{n,l} \in \mathbb{F}_p = \mathbb{Z}_p$. Then we define

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

The sequence $z_0, z_1, \ldots$ is called a *digital explicit inversive sequence of order* T. It is periodic with least period T. Because of its periodicity, it is meaningful to consider only the first $N \leqslant T$ terms of this sequence. Again, we obtain the maximum period $T = q-1$ if and only if γ is a primitive element of $\mathbb{F}_q$.

We note the following bound on character sums which is obtained from [30, Theorems 1 and 2].

Lemma 3. *Let χ be a nontrivial additive character of $\mathbb{F}_q$ and let m be an integer with $1 \leqslant m \leqslant q-1$. Let $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_q^*$ be distinct and choose $\beta, \gamma \in \mathbb{F}_q^*$ such that γ has order $T \geqslant 2$ in the group $\mathbb{F}_q^*$. If $\mu_1, \ldots, \mu_m \in \mathbb{F}_q$ are not all 0, then*

$$\left| \sum_{n=0}^{N-1} \chi\left(\sum_{j=1}^{m} \mu_j \overline{\alpha_j \gamma^n + \beta} \right) \right| = O\left(m q^{1/2} \log T \right) \qquad \textit{for } 1 \leqslant N \leqslant T.$$

7. Mixing Halton sequences and digital explicit inversive sequences of order T

Halton sequences were introduced in Section 5. We consider now hybrid sequences that are obtained by "mixing" Halton sequences and the digital explicit inversive sequences of order T introduced in Section 6.

We choose a dimension $s \geqslant 1$ and pairwise coprime integers $b_1, \ldots, b_s \geqslant 2$. Furthermore, let $z_0, z_1, \ldots$ be a digital explicit inversive sequence of order $T \geqslant 2$ with parameters $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ as in Section 6. We assume that

$$\gcd(b_i, T) = 1 \quad \text{for} \quad 1 \leqslant i \leqslant s.$$

For a dimension t with $1 \leqslant t \leqslant T$, we choose integers $0 \leqslant d_1 < d_2 < \cdots < d_t < T$. Then we define the hybrid sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), z_{n+d_1}, \ldots, z_{n+d_t}) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots \tag{20}$$

We establish the following discrepancy bound for this hybrid sequence.

Theorem 3. *Under the conditions above, the discrepancy D_N of the first N terms of the sequence* (20) *satisfies*

$$D_N = O_{b_1,\ldots,b_s,t}\left(\left(N^{-1} q^{1/2} (\log q)^t \log T\right)^{1/(s+1)}\right) \qquad \text{for} \quad 1 \leqslant N \leqslant T$$

with an implied constant depending only on $b_1, \ldots, b_s$, and t.

P r o o f. We proceed in analogy with the proof of Theorem 2. We take an integer N with $1 \leqslant N \leqslant T$ and we can assume that

$$N > q^{1/2} (\log q)^t \log T,$$

for otherwise the discrepancy bound in the theorem is trivial. We introduce the positive integers

$$f_i := \left\lceil \frac{1}{(s+1)\log b_i} \log \frac{N}{q^{1/2} (\log q)^t \log T} \right\rceil \qquad \text{for} \quad 1 \leqslant i \leqslant s \tag{21}$$

and we put

$$B := b_1^{f_1} \cdots b_s^{f_s}.$$

We assume next that $N \geqslant B$. We first consider an interval $J \subseteq [0,1)^{s+t}$ of the form

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

with

$$v_1, \ldots, v_s \in \mathbb{Z}, \ 0 \leqslant v_i < b_i^{f_i} \quad \text{for} \quad 1 \leqslant i \leqslant s, \quad \text{and} \quad 0 < w_j \leqslant 1 \quad \text{for} \quad 1 \leqslant j \leqslant t.$$

In analogy with (14) we obtain

$$A(J;N) = N\lambda_{s+t}(J) + O\left(\left\lfloor \frac{N-d-1+B}{B} \right\rfloor D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor}\right), \qquad (22)$$

where $A(J;N)$ is the counting function relative to the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in (20) and $D^{(B)}_L$ denotes the discrepancy of the L points

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

Furthermore, d is an integer with $0 \leqslant d < B$ which depends only on J.

Now we bound $D^{(B)}_L$ for $1 \leqslant L \leqslant T$. For a nonzero $t \times k$ matrix

$$\mathcal{H} = (h_{j,l}) \in C(p)^{t \times k}$$

we put

$$E_L(\mathcal{H}) := \sum_{n=0}^{L-1} \mathrm{e}\left(\frac{1}{p}\mathcal{H} \otimes \mathbf{z}_n\right).$$

By the same arguments as in the proof of Theorem 2, we obtain

$$E_L(\mathcal{H}) = \sum_{n=0}^{L-1} \chi\left(\sum_{j=1}^{t} \mu_j \varrho_{Bn+d+d_j}\right),$$

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

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

In view of (19), this yields

$$\begin{aligned} E_L(\mathcal{H}) &= \sum_{n=0}^{L-1} \chi\left(\sum_{j=1}^{t} \mu_j \overline{\alpha\gamma^{Bn+d+d_j} + \beta}\right) \\ &= \sum_{n=0}^{L-1} \chi\left(\sum_{j=1}^{t} \mu_j \overline{\alpha\gamma^{d+d_j}\delta^n + \beta}\right) \end{aligned}$$

with $\delta = \gamma^B$. The condition $\gcd(b_i, T) = 1$ for $1 \leqslant i \leqslant s$ implies that $\gcd(B, T) = 1$, and so δ has order T in the group $\mathbb{F}_q^*$. Since the matrix $\mathcal{H}$ is nonzero, the elements $\mu_1, \ldots, \mu_t$ are not all 0. The condition on the integers $d_1, \ldots, d_t$ implies that the elements $\alpha\gamma^{d+d_j}$, $j = 1, \ldots, t$, are distinct. Thus, we can apply Lemma 3 to obtain

$$|E_L(\mathcal{H})| = O\left(tq^{1/2} \log T\right).$$

Now Lemma 1 with $b = p$ and (15) yield

$$LD_L^{(B)} = O_t\left(q^{1/2}(\log q)^t \log T\right) \qquad \text{for } 1 \leqslant L \leqslant T.$$

We deduce from (22) that

$$A(J;N) = N\lambda_{s+t}(J) + O_t\left(q^{1/2}(\log q)^t \log T\right).$$

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

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

with $v_1, \ldots, v_s \in \mathbb{Z}$, $1 \leqslant v_i \leqslant b_i^{f_i}$ for $1 \leqslant i \leqslant s$, and $0 < w_j \leqslant 1$ for $1 \leqslant j \leqslant t$. In analogy with (17) we obtain

$$A(J;N) = N\lambda_{s+t}(J) + O_t\left(Bq^{1/2}(\log q)^t \log T\right).$$

Finally, the analog of (18) is

$$D_N^* \leqslant \sum_{i=1}^{s} b_i^{-f_i} + O_t\left(BN^{-1}q^{1/2}(\log q)^t \log T\right), \tag{23}$$

where D_N^* is the star discrepancy of the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in (20). This bound is trivial for $N < B$, and so it holds for all integers N with $q^{1/2}(\log q)^t \log T < N \leqslant T$. By the definition of the f_i in (21), we have

$$\left(\frac{N}{q^{1/2}(\log q)^t \log T}\right)^{1/(s+1)} \leqslant b_i^{f_i} \leqslant b_i\left(\frac{N}{q^{1/2}(\log q)^t \log T}\right)^{1/(s+1)} \quad \text{for } 1 \leqslant i \leqslant s,$$

and so

$$B \leqslant b_1 \cdots b_s\left(\frac{N}{q^{1/2}(\log q)^t \log T}\right)^{s/(s+1)}.$$

From (23) we get then

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

An application of (6) completes the proof. □

Remark 2. As in Remark 1, we observe that the discrepancy bound in Theorem 3 holds also if in (20) the s-dimensional Halton sequence is replaced by an s-dimensional generalized Halton sequence.

8. Mixing Kronecker sequences and digital explicit inversive sequences of order T

A *Kronecker sequence* is a sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \ldots$, of fractional parts, where $\boldsymbol{\alpha} \in \mathbb{R}^s$ for an arbitrary dimension $s \geqslant 1$. The discrepancy of this sequence depends on the simultaneous diophantine approximation character of $\boldsymbol{\alpha}$. The following definition is relevant here (see e.g. [15, 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

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

where $r(\mathbf{h})$ is as in (10).

It is well known that we always have $\tau \geqslant 1$ and that there are many examples of

$$\boldsymbol{\alpha} \in \mathbb{R}^s \qquad \text{with } \ \tau = 1$$

(compare with [19, Remark 1]). The following auxiliary result was shown in [18, Lemma 3].

Lemma 4. *Let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be such that there exist real numbers*

$$\sigma \geqslant 1 \qquad \text{and} \quad c > 0$$

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

$$H \geqslant 1 \qquad \text{and} \quad N \geqslant 1$$

we have

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

where $M(\mathbf{h})$ and $r(\mathbf{h})$ are as in (10).

Let $z_0, z_1, \ldots$ be a digital explicit inversive sequence of order $T \geqslant 2$ with parameters $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ as in Section 6. Here $q = p^k$ with a prime p and an integer $k \geqslant 1$. For a dimension t with $1 \leqslant t \leqslant T$, we choose integers

$$0 \leqslant d_1 < d_2 < \cdots < d_t < T.$$

For $\boldsymbol{\alpha} \in \mathbb{R}^s$ we consider the hybrid sequence

$$\mathbf{x}_n = \big(\{n\boldsymbol{\alpha}\}, z_{n+d_1}, \ldots, z_{n+d_t}\big) \in [0,1)^{s+t}, \quad n = 0, 1, \ldots \tag{24}$$

We establish an upper bound on the discrepancy of this hybrid sequence by using Lemma 2 with $b = p$. We employ the same notation as in Lemma 2. In particular, we put

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

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

$$E_N(\mathbf{h}, \mathcal{H}) := \sum_{n=0}^{N-1} \mathrm{e}\left(n(\mathbf{h} \cdot \boldsymbol{\alpha}) + \frac{1}{p}\mathcal{H} \otimes \mathbf{z}_n\right). \tag{25}$$

Lemma 5. *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 (25) we have*

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

Proof. As in the proofs of Theorems 2 and 3, we obtain

$$\mathrm{e}\left(\frac{1}{p}\mathcal{H} \otimes \mathbf{z}_n\right) = \chi\left(\sum_{j=1}^{t} \mu_j \varrho_{n+d_j}\right),$$

where χ is the canonical additive character of $\mathbb{F}_q$ and $\mu_1, \ldots, \mu_t \in \mathbb{F}_q$ are not all 0. Therefore,

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

Then for $1 \leqslant N \leqslant T$ we get

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

Now we consider the character sum inside the last absolute value bars. Note that $1 \leqslant d < N \leqslant T$. If d is such that $d \equiv d_j - d_\ell \pmod{T}$ for some $1 \leqslant j, \ell \leqslant t$ with $j \neq \ell$, then we bound the absolute value of the character sum trivially by N. There are $O(t^2)$ such values of d. If d is not of the above form, then using (19) we write the character sum as

$$\sum_{n=0}^{N-1-d}\chi\left(\sum_{j=1}^{t}\mu_j\left(\overline{\alpha\gamma^{d+d_j}\gamma^n+\beta}-\overline{\alpha\gamma^{d_j}\gamma^n+\beta}\right)\right).$$

We can now apply Lemma 3 with $m = 2t$, and this shows that the absolute value of the character sum is $O_t\left(q^{1/2}\log T\right)$. Altogether, we obtain

$$|E_N(\mathbf{h},\mathcal{H})|^2 \leqslant N + O_t(N) + O_t\left(Nq^{1/2}\log T\right) = O_t\left(Nq^{1/2}\log T\right),$$

which yields the desired result. □

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

Theorem 4. *Let $q = p^k$ with a prime p and an integer $k \geqslant 1$. Let $z_0, z_1, \ldots$ be a digital explicit inversive sequence of order $T \geqslant 2$ with parameters $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ as in Section 6. Let $\boldsymbol{\alpha} \in \mathbb{R}^s$ be of finite type τ. Then for $1 \leqslant N \leqslant T$ the discrepancy D_N of the first N terms of the sequence (24) satisfies*

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

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

P r o o f. Since the discrepancy bound is trivial for $N = 1$, we can assume that $2 \leqslant N \leqslant T$. We apply Lemma 2 with $b = p$ and

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

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

$$D_N = O_{s,t}\left(\frac{1}{H} + \frac{1}{N} \sum_{\substack{\mathbf{h}\in\mathbb{Z}^s,\ \mathcal{H}\in C(p)^{t\times k}\\ M(\mathbf{h})\leqslant H}}^{*} \frac{W_p(\mathcal{H})}{r(\mathbf{h})}\,|E_N(\mathbf{h},\mathcal{H})|\right), \tag{26}$$

where $E_N(\mathbf{h},\mathcal{H})$ is given by (25).

We first consider the pairs $(\mathbf{h},\mathcal{H})$ in the summation in (26) with $\mathbf{h} \neq \mathbf{0}$, $M(\mathbf{h}) \leqslant H$, and $\mathcal{H} = 0$. Then $W_p(\mathcal{H}) = 1$ by (7) and (8). Furthermore by (25),

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

Now fix an $\varepsilon > 0$. Then the contribution of these pairs to the sum in (26) is

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

$$= O_{\boldsymbol{\alpha},\varepsilon}\left(N^{(\tau-1)s/\left((\tau-1)s+1\right)+\varepsilon}\right) \tag{27}$$

according to Lemma 4.

The remaining pairs $(\mathbf{h},\mathcal{H})$ in the summation in (26) satisfy $M(\mathbf{h}) \leqslant H$ and $\mathcal{H} \neq 0$. For these pairs we can apply Lemma 5 to obtain

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

Using (15) and

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

we get

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

By combining this bound with (26) and (27), we complete the proof. □

Corollary 1. *Consider the special case of Theorem 4 where $\boldsymbol{\alpha} \in \mathbb{R}^s$ is of finite type $\tau = 1$. Then for $2 \leqslant N \leqslant T$ the discrepancy D_N of the first N terms of the sequence* (24) *satisfies*

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

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

REFERENCES

[1] CHEN, Z.X.: *Finite binary sequences constructed by explicit inversive methods*, Finite Fields Appl. **14** (2008), 579–592.

[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, A.B. Owen, eds.), Springer, Berlin, 2009, pp. 249–258,.

[3] DAVENPORT, H. – LEWIS, D.J.: *Character sums and primitive roots in finite fields*, Rend. Circ. Mat. Palermo (2) **12** (1963), 129–136.

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

[5] FAURE, H. – LEMIEUX, C.: *Generalized Halton sequences in 2008: A comparative study*, ACM Trans. Modeling Computer Simulation **19** (2009), no. 4, article 15.

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

[7] HALTON, J.H.: *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*, Numer. Math. **2** (1960), 84–90; Berichtigung, ibid. **2** (1960), 196.

[8] IWANIEC, H. – KOWALSKI, E.: *Analytic Number Theory*, Amer. Math. Soc, Providence, RI, 2004.

[9] KUIPERS, L. – NIEDERREITER, H.: *Uniform Distribution of Sequences*, *Pure and Applied Mathematics*, Wiley-Interscience [John Wiley & Sons], New York, 1974; reprint, Dover Publications, Mineola, NY, 2006.

[10] LIDL, R. – NIEDERREITER, H.: *Finite Fields. Encyclopedia of Mathematics and Its Applications* **20**, Cambridge University Press, Cambridge, 1997.

[11] MEIDL, W. – WINTERHOF, A.: *On the linear complexity profile of explicit nonlinear pseudorandom numbers*, Information Processing Letters **85** (2003), 13–18.

[12] MEIDL, W. – WINTERHOF, A.: *On the linear complexity profile of some new explicit inversive pseudorandom numbers*, J. Complexity **20** (2004), 350–355.

[13] MEIDL, W. – WINTERHOF, A.: *On the joint linear complexity profile of explicit inversive multisequences*, J. Complexity **21** (2005), 324–336.

[14] MORENO, C.J. – MORENO, O.: *Exponential sums and Goppa codes: I*, Proc. Amer. Math. Soc. **111** (1991), 523–531.

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

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

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

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

[19] NIEDERREITER, H.: *A discrepancy bound for hybrid sequences involving digital explicit inversive pseudorandom numbers*, Uniform Distribution Theory **5** (2010), 53–63.

[20] NIEDERREITER, H.: *Further discrepancy bounds and an Erdős-Turán-Koksma inequality for hybrid sequences*, Monatsh. Math. **161** (2010), 193–222.

[21] 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.

[22] NIEDERREITER, H. – WINTERHOF, A.: *On the lattice structure of pseudorandom numbers generated over arbitrary finite fields*, Applicable Algebra Engrg. Comm. Comput. **12** (2001), 265–272.

[23] NIEDERREITER, H. – WINTERHOF, A.: *On a new class of inversive pseudorandom numbers for parallelized simulation methods*, Periodica Math. Hungarica **42** (2001), 77–87.

[24] NIEDERREITER, H. – WINTERHOF, A.: *On the distribution of some new explicit nonlinear congruential pseudorandom numbers*, in: *Sequences and Their Applications — SETA 2004* (T. Helleseth, D. Sarwate, H.-Y. Song, K. C. Yang, eds.), Lecture Notes in Computer Science, **3486**, Springer, Berlin, 2005, pp. 266–274.

[25] NIEDERREITER, H. – WINTERHOF, A.: *On the structure of inversive pseudorandom number generators*, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (S. Boztaş, H. F. Lu, eds.), Lecture Notes in Computer Science, **4851**, Springer, Berlin, 2007, pp. 208–216.

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

[27] 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.

[28] PIRSIC, G. – WINTERHOF, A.: *On the structure of digital explicit nonlinear and inversive pseudorandom number generators*, J. Complexity **26** (2010), 43–50.

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

[30] WINTERHOF, A.: *On the distribution of some new explicit inversive pseudorandom numbers and vectors*, in: *Monte Carlo and Quasi-Monte Carlo Methods 2004* (H. Niederreiter. D. Talay, eds.), Springer, Berlin, 2006, pp. 487–499.

Received September 3 2010
Accepted December 22, 2010

Harald Niederreiter
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz
AUSTRIA

Department of Mathematics and Statistics
King Fahd University of Petroleum & Minerals
P.O. Box 5046
Dhahran 31261
SAUDI ARABIA
E-mail: ghnied@gmail.com

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz
AUSTRIA
E-mail: arne.winterhof@oeaw.ac.at