ACTA ARITHMETICA
138.4 (2009)

On the discrepancy of some hybrid sequences

by

Harald Niederreiter (Linz and Salzburg)

To the memory of 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 [8], [9], [17], [18] for accounts of the classical theory and [21] for a recent survey. The stochastic counterparts of quasi-Monte Carlo methods, namely Monte Carlo methods, work with sequences of pseudorandom numbers. The theoretical analysis of sequences of pseudorandom numbers also involves tools from the theory of uniform distribution modulo 1 (see [10, Chapter 3], [17], [18]).

The relative effectiveness of quasi-Monte Carlo methods and Monte Carlo methods for multidimensional numerical integration depends on the nature and the dimensionality of the integrand. As a general rule of thumb, quasi-Monte Carlo methods are more effective in low dimensions. On the other hand, Monte Carlo methods work reasonably well in arbitrarily high dimensions as long as the variance of the integrand is under control. This has led to the idea, first proposed by Spanier [32], of combining the advantages of quasi-Monte Carlo methods and Monte Carlo methods by using *hybrid sequences*. The principle here is to sample a relatively small number of "dominating" variables of the integrand by low-discrepancy sequences and the remaining variables by sequences of pseudorandom numbers. Thus, in effect, one works with sequences of points in a high-dimensional unit cube that are obtained by "mixing" low-discrepancy sequences and sequences of pseudorandom numbers, in the sense that certain coordinates of the points stem from low-discrepancy sequences and the remaining coordinates stem

2000 *Mathematics Subject Classification*: Primary 11K38, 11K45, 11L07; Secondary 65C05, 65C10, 65D30.

Key words and phrases: discrepancy, hybrid sequence, Halton sequence, $n\boldsymbol{\alpha}$ sequence, linear congruential sequence, inversive sequence, quasi-Monte Carlo method.

DOI: 10.4064/aa138-4-8

from sequences of pseudorandom numbers. Various successful applications of hybrid sequences to challenging computational problems have been reported in the literature (see e.g. [29], [30], [32], [33]).

In view of the well-known Koksma–Hlawka inequality (see [7], [11, Section 2.5]), the analysis of numerical integration methods based on hybrid sequences requires the study of the discrepancy of hybrid sequences. So far, only two papers have been devoted to the discrepancy of hybrid sequences (see [28], [30]), and both of them prove only probabilistic results on this discrepancy.

In this paper, we establish the first nontrivial deterministic discrepancy bounds for various hybrid sequences. We consider four families of basic sequences which can be classified into two types. The first type consists of sequences that are used in quasi-Monte Carlo methods: (i) Halton sequences; (ii) $n\boldsymbol{\alpha}$ sequences. The second type consists of sequences of pseudorandom numbers: (iii) linear congruential sequences; (iv) inversive sequences. The detailed definitions of these sequences are reviewed in Section 2. We consider all five possibilities of "mixing" different families of basic sequences such that at least one basic sequence belongs to the first type.

The organization of this paper is straightforward. In Section 2 we collect some definitions and basic facts. Each of the following five sections is devoted to one of the five cases of "mixed" sequences mentioned above. Some concluding remarks are given in Section 8.

2. Definitions and basic facts. For an arbitrary integer $m \geq 1$, 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

$$D_L = \sup_J \left| \frac{A(J;L)}{L} - \lambda_m(J) \right|, \tag{1}$$

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

$$A(J;L) = \#\{0 \leq n \leq L-1 : \mathbf{y}_n \in J\}. \tag{2}$$

Note that we always have $LD_L \geq 1$ (see [11, p. 93]) and $D_L \leq 1$. The *star discrepancy* D_L^* of $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{L-1}$ is obtained by letting the supremum in (1) run only over the half-open intervals $J \subseteq [0,1)^m$ with one vertex at the origin. According to [18, Proposition 2.4] we have

$$D_L \leq 2^m D_L^*. \tag{3}$$

For any integer $B \geq 1$ and any $\mathbf{z} \in \mathbb{R}^m$, put $\mathbf{z}_n = \{B\mathbf{y}_n + \mathbf{z}\} \in [0,1)^m$ for $n = 0, 1, \ldots, L-1$, where $\{\mathbf{u}\}$ denotes the fractional part of $\mathbf{u} \in \mathbb{R}^m$. Let $D_L^{(B,\mathbf{z})}$ be the discrepancy of the points $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{L-1}$.

Lemma 1. *We have*

$$D_L^{(B,\mathbf{z})} \le 2^m B^m D_L.$$

Proof. For $0 \le y < 1$, $z \in \mathbb{R}$, and a fixed half-open subinterval J_1 of $[0,1)$, we have the following equivalences: $\{By+z\} \in J_1 \Leftrightarrow \{By\}$ is in one of at most two disjoint half-open subintervals of $[0,1) \Leftrightarrow By$ is in one of at most $2B$ disjoint half-open subintervals of $[0,B) \Leftrightarrow y$ is in one of at most $2B$ disjoint half-open subintervals of $[0,1)$. In the m-dimensional case, for a fixed half-open subinterval J of $[0,1)^m$ we have: $\mathbf{z}_n = \{B\mathbf{y}_n + \mathbf{z}\} \in J \Leftrightarrow \mathbf{y}_n$ is in one of at most $(2B)^m$ disjoint half-open subintervals of $[0,1)^m$. This implies the desired inequality. ■

A standard tool for estimating the discrepancy is the Erdős–Turán–Koksma inequality, which provides an upper bound on the discrepancy in terms of exponential sums. First we introduce the following two functions on $\mathbb{Z}^m$.

Definition 1. For any $\mathbf{h} = (h_1, \ldots, h_m) \in \mathbb{Z}^m$, put

$$M(\mathbf{h}) = \max_{1\le j\le m} |h_j|, \qquad r(\mathbf{h}) = \prod_{j=1}^{m} \max(|h_j|, 1).$$

Now we state the Erdős–Turán–Koksma inequality (compare with [3, Theorem 1.21] and [11, p. 116]). In the following, we use $\cdot$ to denote the standard inner product in $\mathbb{R}^m$. We write $\mathrm{e}(u) = e^{2\pi i u}$ 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.

Lemma 2. *Let $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{L-1}$ be arbitrary points in $[0,1)^m$ and let D_L be their discrepancy. Then for any integer $K \ge 1$ we have*

$$D_L = O_m\biggl(\frac{1}{K} + \frac{1}{L} \sum_{\substack{\mathbf{h}\in\mathbb{Z}^m \\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1} \biggl|\sum_{n=0}^{L-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{y}_n)\biggr|\biggr).$$

We now recall the definitions of the specific sequences on which we focus in this paper. We start with the Halton sequences (see [6], [18, Chapter 3]). For integers $b \ge 2$ and $n \ge 0$, let

$$n = \sum_{k=0}^{\infty} a_k(n) b^k$$

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

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

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

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

It is a classical low-discrepancy sequence.

Our second family of sequences is that of $n\boldsymbol{\alpha}$ *sequences*, also called *Kronecker sequences*. Let $t \geq 1$ be a given dimension and let $\boldsymbol{\alpha} \in \mathbb{R}^t$. Then we consider the sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \dots,$ of fractional parts. If $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_t)$, then this sequence is uniformly distributed if and only if $1, \alpha_1, \dots, \alpha_t$ are linearly independent over $\mathbb{Q}$ (see [3, Theorem 1.76]). If $\boldsymbol{\alpha}$ is badly approximable in the sense of diophantine approximations, then this sequence has a small discrepancy (compare also with Lemmas 5 and 6 below).

Next we recall the linear congruential sequences which go back to Lehmer [13] and are classical sequences of pseudorandom numbers. Let p be a prime (in practice, p will be large) and let g and a be integers with $\gcd(g,p) = \gcd(a,p) = 1$. Then a *linear congruential sequence* is given as the sequence $(\{g^n a/p\})$, $n = 0, 1, \dots,$ of fractional parts. This sequence is purely periodic with least period $\tau = \mathrm{ord}_p(g)$, where here and in the following $\mathrm{ord}_p(g)$ denotes the multiplicative order of g modulo p. Therefore it is meaningful to study only the first $N \leq \tau$ terms of the sequence. The maximum period $\tau = p - 1$ is attained if and only if g is a primitive root modulo p. Without loss of generality, we can assume that $1 \leq g < p$ and $1 \leq a < p$. Linear congruential sequences have been intensively investigated in the area of uniform pseudorandom number generation (see e.g. [5, Chapter 1], [10, Chapter 3], [18, Chapter 7]).

Our last family of sequences is that of *inversive sequences*. These are sequences of pseudorandom numbers that are generated by an algorithm which involves the multiplicative inverse in residue class rings of $\mathbb{Z}$ or in finite fields (see [4], [20], [25] for surveys of inversive sequences). The family of inversive sequences is quite large, and so we consider only the inversive sequences with the currently strongest pseudorandomness properties, namely those introduced recently by Niederreiter and Rivat [22]; see also [23], [24], [26] for further results on these sequences. Here it is convenient to work with the finite field $\mathbb{F}_p$ of prime order p which can be identified with the set $\{0, 1, \dots, p-1\} \subseteq \mathbb{Z}$. In practice, p will again be large. Fix $a, b \in \mathbb{F}_p^*$ and define the sequence $R_0, R_1, \dots$ of rational functions over $\mathbb{F}_p$ by

$$R_0(X) = X, \qquad R_n(X) = R_{n-1}(aX^{-1} + b) \quad \text{for } n = 1, 2, \dots.$$

The sequence $R_0, R_1, \dots$ is purely periodic with least period $T \le p+1$. For $1 \le n \le T-1$, each R_n has a unique pole $e_n \in \mathbb{F}_p$. Now choose $c_0 \in \mathbb{F}_p$ with $c_0^2 \ne bc_0 + a$. Then for $1 \le n \le T-1$ we put

$$c_n = \begin{cases} R_n(c_0) & \text{if } c_0 \ne e_n, \\ b - e_n & \text{if } c_0 = e_n. \end{cases}$$

By extending with period T, we get a sequence $c_0, c_1, \dots$ of elements of $\mathbb{F}_p$ which is called an *inversive generator*. This sequence has least period T according to [22, Lemma 2]. A simple sufficient condition for obtaining the maximum period $T = p+1$ is given in [22, Theorem 1], and for any p there are always choices of $a, b \in \mathbb{F}_p^*$ such that this maximum period is attained (see [22, p. 255]). The inversive sequence that we want to consider is the normalized sequence (c_n/p), $n = 0, 1, \dots$, of numbers in $[0, 1)$. Because of its periodicity, it is meaningful to study only the first $N \le T$ terms of this sequence.

3. Mixing Halton sequences and $n\boldsymbol{\alpha}$ sequences

3.1. *Preliminaries.* We consider sequences that are obtained by "mixing" Halton sequences and $n\boldsymbol{\alpha}$ sequences. Let $s \ge 1$ and $t \ge 1$ be given dimensions. For an integer $b \ge 2$, let ϕ_b denote the radical-inverse function in base b (see Section 2). Let $b_1, \dots, b_s$ be pairwise coprime integers ≥ 2 and let $\boldsymbol{\alpha} \in \mathbb{R}^t$. Define

$$\mathbf{x}_n = (\phi_{b_1}(n), \dots, \phi_{b_s}(n), \{n\boldsymbol{\alpha}\}) \in [0,1)^{s+t}, \quad n = 0, 1, \dots. \tag{4}$$

Since we want the sequence $\mathbf{x}_0, \mathbf{x}_1, \dots$ to be uniformly distributed in $[0,1)^{s+t}$, we assume that $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_t)$ is such that $1, \alpha_1, \dots, \alpha_t$ are linearly independent over $\mathbb{Q}$. In fact, it is easily seen that this is the necessary and sufficient condition on $\boldsymbol{\alpha}$ for the uniform distribution of the sequence (4); compare with the first few steps of the proofs of Theorems 1 and 2 below.

We write $\|u\| = \min(\{u\}, 1 - \{u\})$ for the distance from $u \in \mathbb{R}$ to the nearest integer. Note that if $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_t)$ is such that $1, \alpha_1, \dots, \alpha_t$ are linearly independent over $\mathbb{Q}$, then $\|\mathbf{h} \cdot \boldsymbol{\alpha}\| > 0$ for all $\mathbf{h} \in \mathbb{Z}^t \setminus \{\mathbf{0}\}$. In the following lemma, we use the notation of Definition 1.

LEMMA 3. *Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be such that there exist real numbers $\sigma \ge 1$ and $c > 0$ with*

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

Then for any integers $K \ge 1$ and $N \ge 1$ we have

$$\sum_{\substack{\mathbf{h} \in \mathbb{Z}^t \\ 0 < M(\mathbf{h}) \le K}} r(\mathbf{h})^{-1} \Big| \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h} \cdot \boldsymbol{\alpha})) \Big| = O_{\boldsymbol{\alpha},\varepsilon}(K^{(\sigma-1)t+\varepsilon}) \quad \textit{for all } \varepsilon > 0.$$

Proof. We follow the method in the proof of [14, Theorem 9]. We fix the positive integers K and N. For any $\mathbf{h} \in \mathbb{Z}^t \setminus \{\mathbf{0}\}$, we have

$$\Big|\sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}\cdot\boldsymbol{\alpha}))\Big| \le \frac{2}{|\mathrm{e}(\mathbf{h}\cdot\boldsymbol{\alpha})-1|} = \frac{1}{\sin \pi \|\mathbf{h}\cdot\boldsymbol{\alpha}\|} \le \frac{1}{2\|\mathbf{h}\cdot\boldsymbol{\alpha}\|}.$$

Therefore

$$(5) \qquad \sum_{\substack{\mathbf{h}\in\mathbb{Z}^t \\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1}\Big|\sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}\cdot\boldsymbol{\alpha}))\Big| = O\Big(\sum_{\substack{\mathbf{h}\in\mathbb{Z}^t \\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1}\|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1}\Big).$$

Put $f(n) = 1/(n(n+1))$ for $1 \le n < K$ and $f(K) = 1/K$. For $(n_1,\dots,n_t) \in \mathbb{Z}^t$ with $1 \le n_j \le K$ for $1 \le j \le t$, put

$$F(n_1,\dots,n_t) = \prod_{j=1}^{t} f(n_j).$$

Then we claim that

$$(6) \qquad \sum_{\substack{\mathbf{h}\in\mathbb{Z}^t \\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1}\|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1} = \sum_{n_1,\dots,n_t=1}^{K} F(n_1,\dots,n_t) \sum_{\substack{\mathbf{h}\in\mathbb{Z}^t\setminus\{\mathbf{0}\} \\ |h_j|\le n_j}} \|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1},$$

where we write $\mathbf{h} = (h_1,\dots,h_t)$. To prove (6), we compute, for fixed $\mathbf{h} \in \mathbb{Z}^t$ with $0 < M(\mathbf{h}) \le K$, the total coefficient of $\|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1}$ on the right-hand side of (6). Since $r(h) = \max(|h|,1)$ for $h \in \mathbb{Z}$, this coefficient is given by

$$\sum_{n_1=r(h_1)}^{K} \cdots \sum_{n_t=r(h_t)}^{K} F(n_1,\dots,n_t) = \prod_{j=1}^{t}\Big(\sum_{n_j=r(h_j)}^{K} f(n_j)\Big) = \prod_{j=1}^{t} r(h_j)^{-1} = r(\mathbf{h})^{-1},$$

and so it is equal to the coefficient of $\|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1}$ on the left-hand side of (6). Thus, (6) is shown.

The next step is the estimation of the inner sum on the right-hand side of (6). Let $\mathbf{n} = (n_1,\dots,n_t) \in \mathbb{Z}^t$ with $n_j \ge 1$ for $1 \le j \le t$ be given. Consider two lattice points $\mathbf{h},\mathbf{h}' \in \mathbb{Z}^t \setminus \{\mathbf{0}\}$ with $\mathbf{h}' \ne \pm\mathbf{h}$ which belong to the range of summation of the inner sum on the right-hand side of (6). Then

$$\|\mathbf{h}\cdot\boldsymbol{\alpha} \pm \mathbf{h}'\cdot\boldsymbol{\alpha}\| = \|(\mathbf{h}\pm\mathbf{h}')\cdot\boldsymbol{\alpha}\| \ge c r(\mathbf{h}\pm\mathbf{h}')^{-\sigma} \ge c r(2\mathbf{n})^{-\sigma} =: \delta.$$

Using simple properties of the function $\|u\|$, we then conclude that

$$\big|\|\mathbf{h}\cdot\boldsymbol{\alpha}\| - \|\mathbf{h}'\cdot\boldsymbol{\alpha}\|\big| \ge \delta.$$

Since we also have $\|\mathbf{h}\cdot\boldsymbol{\alpha}\| \ge \delta$, it follows that in each of the intervals $[0,\delta), [\delta,2\delta), \dots, [k\delta,(k+1)\delta)$, where $k = \lfloor 1/(2\delta)\rfloor$, there are at most two numbers of the form $\|\mathbf{h}\cdot\boldsymbol{\alpha}\|$, with no such number lying in the first interval.

Therefore

$$\sum_{\substack{\mathbf{h}\in\mathbb{Z}^t\setminus\{\mathbf{0}\}\\ |h_j|\le n_j}} \|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1} \le 2\sum_{m=1}^{k}\frac{1}{m\delta} \le \frac{2}{\delta}(1+\log k) = O_{\boldsymbol{\alpha},\varepsilon}(r(\mathbf{n})^{\sigma+\varepsilon/t})$$

for all $\varepsilon > 0$.

Now we return to (6). Using the estimate that we have just obtained, we get

$$\begin{aligned}\sum_{\substack{\mathbf{h}\in\mathbb{Z}^t\\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1}\|\mathbf{h}\cdot\boldsymbol{\alpha}\|^{-1} &= O_{\boldsymbol{\alpha},\varepsilon}\Big(\sum_{n_1,\dots,n_t=1}^{K} F(n_1,\dots,n_t)(n_1\cdots n_t)^{\sigma+\varepsilon/t}\Big)\\ &= O_{\boldsymbol{\alpha},\varepsilon}\Big(\sum_{n_1,\dots,n_t=1}^{K}\prod_{j=1}^{t} f(n_j)n_j^{\sigma+\varepsilon/t}\Big)\\ &= O_{\boldsymbol{\alpha},\varepsilon}\Big(\Big(\sum_{n=1}^{K} f(n)n^{\sigma+\varepsilon/t}\Big)^t\Big) = O_{\boldsymbol{\alpha},\varepsilon}(K^{(\sigma-1)t+\varepsilon})\end{aligned}$$

for all $\varepsilon > 0$. The result of the lemma now follows from (5). ∎

3.2. *An interesting special case.* We first consider the special case of the sequence (4) where $t = 1$ and the irrational number α is of constant type according to the following standard definition (see e.g. [11, p. 121]).

Definition 2. Let $c \ge 2$ be a real number. The irrational number α is *of constant type* c if

$$h\|h\alpha\| \ge \frac{1}{c} \quad \text{for all integers } h \ge 1.$$

Lemma 4. *If α is of constant type c and*

$$\alpha = [a_0; a_1, a_2, \dots] \tag{7}$$

is the continued fraction expansion of α, then $a_i < c$ for all $i \ge 1$.

Proof. If p_i/q_i, $i = 0, 1, \dots$, are the convergents to α, then by the theory of continued fractions,

$$q_{i-1}\|q_{i-1}\alpha\| \le q_{i-1}|q_{i-1}\alpha - p_{i-1}| < \frac{q_{i-1}}{q_i} \quad \text{for all } i \ge 1.$$

On the other hand, $q_{i-1}\|q_{i-1}\alpha\| \ge 1/c$ by Definition 2, and so $q_i < cq_{i-1}$ for all $i \ge 1$. Now $q_i = a_iq_{i-1} + q_{i-2}$ (with $q_{-1} = 0$), hence

$$a_iq_{i-1} \le a_iq_{i-1} + q_{i-2} = q_i < cq_{i-1},$$

and so $a_i < c$ for all $i \ge 1$. ∎

Remark 1. The converse of Lemma 4 is also true, in the sense that if α has bounded partial quotients, then α is of constant type (see [12, Chapter II, Theorem 6]).

The following result was shown in [18, Corollary 3.5].

Lemma 5. *Let α be an irrational number for which there exists a positive integer K such that in the continued fraction expansion* (7) *of α we have $a_i \le K$ for all $i \ge 1$. Then for any integer $L \ge 1$ the discrepancy D_L of the first L terms of the sequence $(\{n\alpha\})$, $n = 0, 1, \dots,$ satisfies*

$$LD_L = O\biggl(\frac{K \log(L+1)}{\log(K+1)}\biggr).$$

Let the irrational number α be of constant type c and consider the special case of the sequence (4) given by

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

Theorem 1. *If $b_1, \dots, b_s$ are pairwise coprime integers ≥ 2 and α is of constant type c, then for any integer $N \ge 1$ the discrepancy D_N of the first N terms of the sequence* (8) *satisfies*

$$D_N = O_{b_1,\dots,b_s}(c^{1/(2s+1)} N^{-1/(2s+1)})$$

with an implied constant depending only on $b_1, \dots, b_s$.

Proof. We introduce the integers

$$f_i := \biggl\lceil \frac{\log(N/c)}{(2s+1)\log b_i} \biggr\rceil \quad \text{for } 1 \le i \le s.$$

We claim that we can assume $f_i \ge 2$ for $1 \le i \le s$. Indeed, otherwise

$$\frac{\log(N/c)}{(2s+1)\log b_i} \le 1$$

for some i, hence

$$\biggl(\frac{c}{N}\biggr)^{1/(2s+1)} \ge \frac{1}{b_i}$$

for some i, and the discrepancy bound is trivial.

We put

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

Since $f_i \ge 2$ for $1 \le i \le s$, the definition of the f_i implies that

$$\biggl(\frac{N}{c}\biggr)^{1/(2s+1)} \ge b_i^{f_i - 1} \ge b_i^{f_i/2} \quad \text{for } 1 \le i \le s.$$

Multiplying together these inequalities, we get $(N/c)^{s/(2s+1)} \ge B^{1/2}$, and so $N \ge cB^{(2s+1)/2s} \ge B$.

Let $A(J; N)$ be the counting function in (2), but relative to the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ in (8). We first choose an interval $J \subseteq [0,1)^{s+1}$ of the form

$$J = \prod_{i=1}^{s} \biggl[\frac{v_i}{b_i^{f_i}}, \frac{v_i+1}{b_i^{f_i}}\biggr) \times [0, w)$$

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

$$n \equiv d \pmod{B} \quad \text{and} \quad \{n\alpha\} \in [0, w)$$

for some integer d with $0 \le d < B$ which depends only on J. Thus, $n = kB + d$ for some integer k, and the condition $0 \le n \le N-1$ is equivalent to $0 \le k \le \lfloor (N-d-1)/B \rfloor$. Recall that $N \ge B \ge d+1$. It follows that

$$A(J;N) = \#\left\{0 \le k \le \left\lfloor \frac{N-d-1}{B} \right\rfloor : \{kB\alpha + d\alpha\} \in [0, w)\right\},$$

and so

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

where $D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor}$ is the discrepancy of the first $\lfloor (N-d-1+B)/B \rfloor$ terms of the sequence $(\{kB\alpha\})$, $k = 0, 1, \ldots$. Therefore

$$A(J;N) = N\lambda_{s+1}(J) + O\left(\left\lfloor \frac{N-d-1+B}{B} \right\rfloor D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor}\right). \tag{9}$$

Since α is of constant type c, it follows immediately from Definition 2 that $B\alpha$ is of constant type Bc. By combining (9) with Lemmas 4 and 5, we obtain

$$A(J;N) = N\lambda_{s+1}(J) + O\left(\frac{Bc}{\log(Bc+1)} \log\left(\frac{N}{B} + 2\right)\right).$$

The definition of the f_i yields $b_i^{f_i} \ge (N/c)^{1/(2s+1)}$ for $1 \le i \le s$, and so $B \ge (N/c)^{s/(2s+1)}$. Therefore

$$\frac{\log(N/B+2)}{\log(Bc+1)} \le \frac{\log(c^{s/(2s+1)} N^{(s+1)/(2s+1)} + 2)}{\log(c^{(s+1)/(2s+1)} N^{s/(2s+1)} + 1)} \le 2,$$

which implies in turn that

$$A(J;N) = N\lambda_{s+1}(J) + O(Bc). \tag{10}$$

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

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

with $v_1, \ldots, v_s \in \mathbb{Z}$, $1 \le v_i \le b_i^{f_i}$ for $1 \le i \le s$, and $0 < w \le 1$. By adding at most B identities of the form (10), we obtain

$$A(J;N) = N\lambda_{s+1}(J) + O(B^2 c). \tag{11}$$

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

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

with $0 < u_i \le 1$ for $1 \le i \le s$ and $0 < w \le 1$. 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 (11) that

$$D_N^* \le \sum_{i=1}^{s} b_i^{-f_i} + O(B^2 c N^{-1}), \tag{12}$$

where D_N^* is the star discrepancy of the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$. Using again $b_i^{f_i} \ge (N/c)^{1/(2s+1)}$ for $1 \le i \le s$, we get

$$D_N^* = O_s(c^{1/(2s+1)} N^{-1/(2s+1)} + B^2 c N^{-1}).$$

As noted earlier in this proof, we have $b_i^{f_i} \le b_i (N/c)^{1/(2s+1)}$ for $1 \le i \le s$, hence by squaring and multiplying together these inequalities we obtain

$$B^2 \le (b_1 \cdots b_s)^2 \left(\frac{N}{c}\right)^{2s/(2s+1)}.$$

This yields

$$D_N^* = O_{b_1,\dots,b_s}(c^{1/(2s+1)} N^{-1/(2s+1)}),$$

and an application of (3) completes the proof. ■

3.3. *The general case.* We now consider the sequence (4). In order to get a reasonable discrepancy bound, we assume that $\boldsymbol{\alpha} \in \mathbb{R}^t$ is of finite type according to the following standard definition (see e.g. [15, Definition 6.1]), where we use the notation of Definition 1.

Definition 3. Let η be a real number. Then $\boldsymbol{\alpha} \in \mathbb{R}^t$ 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

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

As noted in [15, p. 164], it is an easy consequence of Minkowski's linear forms theorem that we always have $\eta \ge 1$.

Lemma 6. *If $\boldsymbol{\alpha} \in \mathbb{R}^t$ is of finite type η, then for any integer $L \ge 1$ the discrepancy D_L of the first L terms of the sequence $(\{n\boldsymbol{\alpha}\})$, $n = 0, 1, \dots,$ satisfies*

$$D_L = O_{\boldsymbol{\alpha},\varepsilon}(L^{-1/((\eta-1)t+1)+\varepsilon}) \quad \textit{for all } \varepsilon > 0.$$

Proof. By Lemma 2 we have

$$D_L = O_t\biggl(\frac{1}{K} + \frac{1}{L} \sum_{\substack{\mathbf{h}\in\mathbb{Z}^t\\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1}\Bigl|\sum_{n=0}^{L-1} \mathrm{e}(n(\mathbf{h}\cdot\boldsymbol{\alpha}))\Bigr|\biggr)$$

for any integer $K \ge 1$. Then we apply Lemma 3 to obtain

$$D_L = O_{\boldsymbol{\alpha},\varepsilon}\biggl(\frac{1}{K} + \frac{1}{L}\, K^{(\eta-1)t+\varepsilon}\biggr) \quad \text{for all } \varepsilon > 0.$$

Choosing $K = \lfloor L^{1/((\eta-1)t+1)}\rfloor$ yields the assertion of the lemma. We note that this result is also an immediate consequence of Exercise 3.17 on p. 132 of [11], but for the sake of completeness we have included a proof here. ∎

THEOREM 2. *If $b_1,\dots,b_s$ are pairwise coprime integers ≥ 2 and $\boldsymbol{\alpha}\in\mathbb{R}^t$ is of finite type η, then for any integer $N \ge 1$ the discrepancy D_N of the first N terms of the sequence* (4) *satisfies*

$$D_N = O_{b_1,\dots,b_s,\boldsymbol{\alpha},\varepsilon}\bigl(N^{-\frac{1}{(\eta-1)(st^2+t)+s(t+1)+1}+\varepsilon}\bigr) \quad \textit{for all } \varepsilon > 0$$

with an implied constant depending only on $b_1,\dots,b_s$, $\boldsymbol{\alpha}$, and ε.

Proof. We apply a method similar to that in the proof of Theorem 1. We put

$$f_i := \biggl\lceil \frac{1}{(\eta-1)(st^2+t)+s(t+1)+1}\cdot\frac{\log N}{\log b_i}\biggr\rceil \quad \text{for } 1\le i\le s$$

and

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

We fix $\varepsilon > 0$. We first consider the case where $N \ge B$. Let the interval $J \subseteq [0,1)^{s+t}$ be of the form

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

with $v_1,\dots,v_s\in\mathbb{Z}$, $0\le v_i < b_i^{f_i}$ for $1\le i\le s$, and $0 < w_j \le 1$ for $1\le j\le t$. As in (9) we get

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

where $D_L^{(B)}$ denotes the discrepancy of the first L terms of the sequence $(\{kB\boldsymbol{\alpha}+d\boldsymbol{\alpha}\})$, $k=0,1,\dots$. By Lemmas 1 and 6 we obtain

$$D_L^{(B)} = O_{\boldsymbol{\alpha},\varepsilon}(B^t L^{-1/((\eta-1)t+1)+\varepsilon})$$

for all integers $L \ge 1$. Therefore

$$A(J;N) = N\lambda_{s+t}(J) + O_{\boldsymbol{\alpha},\varepsilon}\left(B^t\left(\frac{N}{B}\right)^{1-\frac{1}{(\eta-1)t+1}+\varepsilon}\right).$$

For $J \subseteq [0,1)^{s+t}$ 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 $v_1, \dots, v_s \in \mathbb{Z}$, $1 \le v_i \le b_i^{f_i}$ for $1 \le i \le s$, and $0 < w_j \le 1$ for $1 \le j \le t$, the analog of (11) is

$$\begin{aligned} A(J;N) &= N\lambda_{s+t}(J) + O_{\boldsymbol{\alpha},\varepsilon}\left(B^{t+1}\left(\frac{N}{B}\right)^{1-\frac{1}{(\eta-1)t+1}+\varepsilon}\right) \\ &= N\lambda_{s+t}(J) + O_{\boldsymbol{\alpha},\varepsilon}(B^{t+\frac{1}{(\eta-1)t+1}}N^{1-\frac{1}{(\eta-1)t+1}+\varepsilon}). \end{aligned}$$

In analogy with (12) we obtain

$$D_N^* \le \sum_{i=1}^{s} b_i^{-f_i} + O_{\boldsymbol{\alpha},\varepsilon}(B^{t+\frac{1}{(\eta-1)t+1}}N^{-\frac{1}{(\eta-1)t+1}+\varepsilon}).$$

This bound is trivial for $1 \le N < B$, and so it holds for all integers $N \ge 1$. By the definition of the f_i, we have

$$b_i^{f_i} \ge N^{\frac{1}{(\eta-1)(st^2+t)+s(t+1)+1}} \qquad \text{for } 1 \le i \le s,$$

and so

$$D_N^* = O_{s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{(\eta-1)(st^2+t)+s(t+1)+1}} + B^{t+\frac{1}{(\eta-1)t+1}}N^{-\frac{1}{(\eta-1)t+1}+\varepsilon}). \tag{13}$$

Again by the definition of the f_i, we have

$$b_i^{f_i} \le b_i N^{\frac{1}{(\eta-1)(st^2+t)+s(t+1)+1}} \qquad \text{for } 1 \le i \le s,$$

and so

$$B \le b_1 \cdots b_s N^{\frac{s}{(\eta-1)(st^2+t)+s(t+1)+1}}.$$

Using this bound in (13) and a straightforward computation, we arrive at

$$D_N^* = O_{b_1,\dots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{(\eta-1)(st^2+t)+s(t+1)+1}+\varepsilon}).$$

An application of (3) completes the proof. ∎

COROLLARY 1. *If $b_1, \dots, b_s$ are pairwise coprime integers ≥ 2 and $\boldsymbol{\alpha} \in \mathbb{R}^t$ is of finite type $\eta = 1$, then for any integer $N \ge 1$ the discrepancy of the first N terms of the sequence* (4) *satisfies*

$$D_N = O_{b_1,\dots,b_s,\boldsymbol{\alpha},\varepsilon}(N^{-\frac{1}{s(t+1)+1}+\varepsilon}) \qquad \textit{for all } \varepsilon > 0$$

with an implied constant depending only on $b_1, \dots, b_s, \boldsymbol{\alpha}$, and ε.

Remark 2. Well-known examples of points $\boldsymbol{\alpha} \in \mathbb{R}^t$ of finite type $\eta = 1$ are the following: (i) $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ with real algebraic numbers $\alpha_1, \ldots, \alpha_t$ such that $1, \alpha_1, \ldots, \alpha_t$ are linearly independent over $\mathbb{Q}$ (see [31]); (ii) $\boldsymbol{\alpha} = (\mathrm{e}^{r_1}, \ldots, \mathrm{e}^{r_t})$ with distinct nonzero rational numbers $r_1, \ldots, r_t$ (see [1]).

4. Mixing Halton sequences and linear congruential sequences. Let $p \geq 3$ be a prime, let $g \in \mathbb{Z}$ with $2 \leq g < p$, and let $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. For an integer $b \geq 2$, let ϕ_b denote the radical-inverse function in base b (see Section 2). Let $b_1, \ldots, b_s$ be pairwise coprime integers ≥ 2 and consider the sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), \{g^n a/p\}) \in [0,1)^{s+1}, \qquad n = 0, 1, \ldots. \tag{14}$$

Theorem 3. *Let p, g, a be as above and put $\tau = \mathrm{ord}_p(g)$. Let $b_1, \ldots, b_s$ be pairwise coprime integers ≥ 2 with $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$. Then for $1 \leq N \leq \tau$ the discrepancy D_N of the first N terms of the sequence* (14) *satisfies*

$$D_N = O_{b_1,\ldots,b_s}((N^{-1}p^{1/2}(\log p)\log \tau)^{1/(s+1)})$$

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

Proof. The discrepancy bound is trivial if $N \leq p^{1/2}(\log p)\log \tau$, and so we can assume that $p^{1/2}(\log p)\log \tau < N \leq \tau$. We introduce the positive integers

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

and

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

We assume next that $N \geq B$. We proceed as in the proof of Theorem 1. We first consider an interval $J \subseteq [0,1)^{s+1}$ of the form

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

with $v_1, \ldots, v_s \in \mathbb{Z}$, $0 \leq v_i < b_i^{f_i}$ for $1 \leq i \leq s$, and $0 < w \leq 1$. As in (9) we get

$$A(J; N) = N\lambda_{s+1}(J) + O\biggl(\biggl\lfloor \frac{N - d - 1 + B}{B} \biggr\rfloor D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor} \biggr), \tag{15}$$

where $D_L^{(B)}$ denotes the discrepancy of the first L terms of the sequence $(\{g^{kB+d}a/p\})$, $k = 0, 1, \ldots$. Recall that $N \geq B \geq d + 1$. The last sequence can be written as $(\{(g^B)^k g^d a/p\})$, $k = 0, 1, \ldots$. The hypothesis $\gcd(b_i, \tau) = 1$ for $1 \leq i \leq s$ implies that $\gcd(B, \tau) = 1$, and so the multiplicative order of g^B modulo p is equal to τ. Then [16, Theorem 2] shows that

$$LD_L^{(B)} = O(p^{1/2}(\log p)\log\tau) \quad \text{for } 1 \le L \le \tau$$

with an absolute implied constant. It thus follows from (15) that

$$A(J;N) = N\lambda_{s+1}(J) + O(p^{1/2}(\log p)\log\tau)$$

with an absolute implied constant.

For $J \subseteq [0,1)^{s+1}$ of the form

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

with $v_1,\dots,v_s \in \mathbb{Z}$, $1 \le v_i \le b_i^{f_i}$ for $1 \le i \le s$, and $0 < w \le 1$, the analog of (11) is

$$A(J;N) = N\lambda_{s+1}(J) + O(Bp^{1/2}(\log p)\log\tau)$$

with an absolute implied constant.

In analogy with (12) we obtain

$$D_N^* \le \sum_{i=1}^{s} b_i^{-f_i} + O(N^{-1}Bp^{1/2}(\log p)\log\tau).$$

This bound is trivial for $N < B$, and so it holds for all integers N with $p^{1/2}(\log p)\log\tau < N \le \tau$. By the definition of the f_i we have

$$\left(\frac{N}{p^{1/2}(\log p)\log\tau}\right)^{1/(s+1)} \le b_i^{f_i} \le b_i\left(\frac{N}{p^{1/2}(\log p)\log\tau}\right)^{1/(s+1)}$$

for $1 \le i \le s$, and so

$$B \le b_1\cdots b_s\left(\frac{N}{p^{1/2}(\log p)\log\tau}\right)^{s/(s+1)}.$$

This yields

$$D_N^* = O_{b_1,\dots,b_s}((N^{-1}p^{1/2}(\log p)\log\tau)^{1/(s+1)}).$$

An application of (3) completes the proof. ∎

Remark 3. We can extend the analysis to the case where a Halton sequence is "mixed" with several linear congruential sequences. The crucial ingredient of this generalization is the following result of Bourgain [2, Theorem 2]. Let p be a prime and fix ε with $0 < \varepsilon < 1$. For an arbitrary integer $m \ge 1$, let $g_1,\dots,g_m \in \mathbb{Z}$ with $\gcd(g_j,p) = 1$ for $1 \le j \le m$. Assume that $\mathrm{ord}_p(g_j) > p^\varepsilon$ for $1 \le j \le m$ and $\mathrm{ord}_p(g_j\overline{g_l}) > p^\varepsilon$ for $1 \le j < l \le m$, where $\overline{g_l} \in \mathbb{Z}$ is such that $g_l\overline{g_l} \equiv 1 \pmod{p}$. Then there exists a $\delta > 0$ depending only on m and ε such that for any $h_1,\dots,h_m \in \mathbb{Z}$ that are not all divisible by p, and any integer $N > p^{\varepsilon}$, we have

$$\left|\sum_{n=0}^{N-1} \mathrm{e}\biggl(\frac{1}{p}\sum_{j=1}^{m} h_j\, g_j^n\biggr)\right| < p^{-\delta} N. \tag{16}$$

Now we choose $a_1, \dots, a_m \in \mathbb{Z}$ with $\gcd(a_j, p) = 1$ for $1 \le j \le m$ and we consider, for a given $N > p^{\varepsilon}$, the discrepancy D_N of the points

$$(\{g_1^n\, a_1/p\}, \dots, \{g_m^n\, a_m/p\}) \in [0,1)^m, \qquad n = 0, 1, \dots, N-1.$$

Then as an immediate consequence of (16) and [18, Corollary 3.11] we obtain

$$D_N = O_m(p^{-\delta}(\log p)^m). \tag{17}$$

For pairwise coprime integers $b_1, \dots, b_s \ge 2$, we now consider the sequence

$$\mathbf{x}_n = (\phi_{b_1}(n), \dots, \phi_{b_s}(n), \{g_1^n\, a_1/p\}, \dots, \{g_m^n\, a_m/p\}) \in [0,1)^{s+m}, \qquad n = 0, 1, \dots, \tag{18}$$

under the same conditions on $g_1, \dots, g_m$ and $a_1, \dots, a_m$ as above and with the additional hypothesis $\gcd(b_i, \mathrm{ord}_p(g_j)) = 1$ for all $1 \le i \le s$ and $1 \le j \le m$. Then on the basis of (17) and adapting the method in the proof of Theorem 3, we obtain a bound on the discrepancy of sufficiently long initial segments of the sequence (18). This yields a weak, but nevertheless nontrivial discrepancy bound. The bound is of the form

$$O_{b_1,\dots,b_s,m}(\max(N^{-1/s}, p^{-\delta}(\log p)^m))$$

for the discrepancy of the first $N > p^{\varepsilon}$ terms of (18).

5. Mixing $n\boldsymbol{\alpha}$ sequences and linear congruential sequences.

Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ for an arbitrary dimension $t \ge 1$, let $p \ge 3$ be a prime, let $g \in \mathbb{Z}$ with $2 \le g < p$, and let $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. Consider the sequence

$$\mathbf{x}_n = (\{n\boldsymbol{\alpha}\}, \{g^n a/p\}) \in [0,1)^{t+1}, \qquad n = 0, 1, \dots. \tag{19}$$

We first establish a bound for the following exponential sum. For $\mathbf{h}_1 \in \mathbb{Z}^t$, $h \in \mathbb{Z}$, and an integer $N \ge 1$, put

$$E_N(\mathbf{h}_1, h) := \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + hg^n a/p). \tag{20}$$

We use the following result shown in [16, Lemma 3].

LEMMA 7. *Let $p \ge 3$ be a prime, let $g \in \mathbb{Z}$ with $2 \le g < p$, and let $h \in \mathbb{Z}$ with* $\gcd(h, p) = 1$. *Put $\tau = \mathrm{ord}_p(g)$. Then*

$$\left|\sum_{n=0}^{N-1} \mathrm{e}(hg^n/p)\right| = O(p^{1/2} \log \tau) \quad \textit{for } 1 \le N \le \tau.$$

Lemma 8. *Let p, g, a be as above and put $\tau = \mathrm{ord}_p(g)$. Let $\boldsymbol{\alpha} \in \mathbb{R}^t$, $\mathbf{h}_1 \in \mathbb{Z}^t$, and $h \in \mathbb{Z}$ with* $\gcd(h, p) = 1$. *Then for the exponential sum $E_N(\mathbf{h}_1, h)$ in* (20) *we have*

$$|E_N(\mathbf{h}_1, h)| = O(N^{1/2} p^{1/4} (\log \tau)^{1/2}) \quad \textit{for } 1 \le N \le \tau.$$

Proof. We have

$$\begin{aligned}|E_N(\mathbf{h}_1, h)|^2 &= \sum_{k,n=0}^{N-1} \mathrm{e}((k-n)(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + h(g^k - g^n)a/p) \\ &\le N + 2\Big| \sum_{\substack{k,n=0 \\ k>n}}^{N-1} \mathrm{e}((k-n)(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + hg^n(g^{k-n} - 1)a/p)\Big| \\ &= N + 2\Big| \sum_{d=1}^{N-1} \sum_{n=0}^{N-1-d} \mathrm{e}(d(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + hg^n(g^d - 1)a/p)\Big| \\ &\le N + 2 \sum_{d=1}^{N-1} \Big| \sum_{n=0}^{N-1-d} \mathrm{e}(hg^n(g^d - 1)a/p)\Big|.\end{aligned}$$

Since $1 \le N \le \tau$, we have $g^d \not\equiv 1 \pmod{p}$ for $1 \le d \le N-1$. It therefore follows from Lemma 7 that

$$\Big| \sum_{n=0}^{N-1-d} \mathrm{e}(hg^n(g^d - 1)a/p)\Big| = O(p^{1/2} \log \tau).$$

Hence

$$|E_N(\mathbf{h}_1, h)|^2 = O(Np^{1/2} \log \tau),$$

which yields the desired result. ■

In the following theorem, we again use the notion of finite type η introduced in Definition 3.

Theorem 4. *Let p, g, a be as above and put $\tau = \mathrm{ord}_p(g)$. Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be of finite type η. Then for $1 \le N \le \tau$ the discrepancy D_N of the first N terms of the sequence* (19) *satisfies*

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

for all $\varepsilon > 0$ with an implied constant depending only on $\boldsymbol{\alpha}$ and ε.

Proof. Since the discrepancy bound is trivial for $N = 1$, we can assume that $2 \le N \le \tau$. We apply the Erdős–Turán–Koksma inequality (see

Lemma 2) with $K = \lceil N^{1/((\eta-1)t+1)} \rceil$, so that

$$D_N = O_t\biggl(\frac{1}{K} + \frac{1}{N} \sum_{\substack{\mathbf{h}\in\mathbb{Z}^{t+1}\\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1} \biggl|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\biggr|\biggr). \tag{21}$$

Note that $2 \le K \le N < p$. For $\mathbf{h} = (h_1, \ldots, h_{t+1}) \in \mathbb{Z}^{t+1}$ with $\mathbf{h} \ne \mathbf{0}$ and $h_{t+1} = 0$, we have

$$\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n) = \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}_1\cdot\boldsymbol{\alpha})),$$

where $\mathbf{h}_1 = (h_1, \ldots, h_t) \in \mathbb{Z}^t$. Now fix an $\varepsilon > 0$. Then by Lemma 3 we get

$$\begin{aligned}\sum_{\substack{\mathbf{h}\in\mathbb{Z}^{t+1},\, h_{t+1}=0\\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1} \biggl|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\biggr| &= O_{\boldsymbol{\alpha},\varepsilon}(K^{(\eta-1)t+\varepsilon})\\ &= O_{\boldsymbol{\alpha},\varepsilon}(N^{(\eta-1)t/((\eta-1)t+1)+\varepsilon}).\end{aligned}$$

Furthermore, for $\mathbf{h} \in \mathbb{Z}^{t+1}$ with $M(\mathbf{h}) \le K$ and $h_{t+1} \ne 0$, we can apply Lemma 8 to obtain

$$\biggl|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\biggr| = |E_N(\mathbf{h}_1, h_{t+1})| = O(N^{1/2}p^{1/4}(\log\tau)^{1/2}).$$

Therefore

$$\begin{aligned}\sum_{\substack{\mathbf{h}\in\mathbb{Z}^{t+1},\, h_{t+1}\ne 0\\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1} \biggl|\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h}\cdot\mathbf{x}_n)\biggr| &\\ = O\Bigl(N^{1/2}p^{1/4}(\log\tau)^{1/2} \sum_{\substack{\mathbf{h}\in\mathbb{Z}^{t+1},\, h_{t+1}\ne 0\\ 0<M(\mathbf{h})\le K}} r(\mathbf{h})^{-1}\Bigr)&\\ = O_t(N^{1/2}p^{1/4}(\log\tau)^{1/2}(\log K)^{t+1})&\\ = O_t(N^{1/2}p^{1/4}(\log\tau)^{1/2}(\log N)^{t+1}).&\end{aligned}$$

By combining the above bounds with (21), we arrive at the desired result. ■

Corollary 2. *Let p, g, a be as above and put $\tau = \mathrm{ord}_p(g)$. Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be of finite type $\eta = 1$. Then for $2 \le N \le \tau$ the discrepancy D_N of the first N terms of the sequence* (19) *satisfies*

$$D_N = O_{\boldsymbol{\alpha}}(N^{-1/2}p^{1/4}(\log\tau)^{1/2}(\log N)^{t+1})$$

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

Remark 4. Fix $\boldsymbol{\alpha} \in \mathbb{R}^t$ of finite type. For each prime $p \geq 3$, choose a primitive root g modulo p and $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Note that then $\tau = \mathrm{ord}_p(g) = p-1$. Choose also positive integers $N_p \leq p-1$ with

$$\lim_{p\to\infty} \frac{p^{1/2}(\log p)(\log N_p)^{2t+2}}{N_p} = 0.$$

Then $D_{N_p} \to 0$ as $p \to \infty$ by Theorem 4. It follows therefore by the Koksma–Hlawka inequality that the corresponding quasi-Monte Carlo method yields a convergent numerical integration scheme for integrands of bounded variation in the sense of Hardy and Krause.

Remark 5. The estimate (16) in Remark 3 allows us to treat the more general case where we "mix" an $n\boldsymbol{\alpha}$ sequence with several linear congruential sequences. Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be of finite type η and let p be a prime. For an arbitrary integer $m \geq 1$, let $g_1, \ldots, g_m \in \mathbb{Z}$ and $a_1, \ldots, a_m \in \mathbb{Z}$ with $\gcd(g_j, p) = \gcd(a_j, p) = 1$ for $1 \leq j \leq m$. Then we consider the sequence

$$\mathbf{x}_n = (\{n\boldsymbol{\alpha}\}, \{g_1^n a_1/p\}, \ldots, \{g_m^n a_m/p\}) \in [0,1)^{t+m}, \qquad n = 0, 1, \ldots. \tag{22}$$

We fix ε with $0 < \varepsilon < 1$ and assume that $\mathrm{ord}_p(g_j) > p^{\varepsilon}$ for $1 \leq j \leq m$ and $\mathrm{ord}_p(g_j\overline{g_l}) > p^{\varepsilon}$ for $1 \leq j < l \leq m$. Now we choose an integer N with $p^{\varepsilon} < N \leq \min_{1\leq j\leq m} \mathrm{ord}_p(g_j)$. Then by using (16) and adapting the proofs of Lemma 8 and Theorem 4, we get a bound on the discrepancy D_N of the first N terms of the sequence (22). As in Remark 3, this yields a weak, but nontrivial discrepancy bound. The bound is of the form

$$D_N = O_{\boldsymbol{\alpha},m,\kappa}(\max(N^{-1/((\eta-1)t+1)+\kappa}, p^{-\delta/2}(\log N)^{t+m}, p^{\varepsilon}N^{-1}(\log N)^{t+m}))$$

for all $\kappa > 0$, where $\delta = \delta(m,\varepsilon) > 0$ is as in (16).

6. Mixing Halton sequences and inversive sequences. For a given dimension $s \geq 1$, let $b_1, \ldots, b_s$ be pairwise coprime integers ≥ 2. We consider the Halton sequence in the bases $b_1, \ldots, b_s$ (see Section 2) and "mix" it with an inversive sequence as described in Section 2. For a given prime $p \geq 3$, let $c_0, c_1, \ldots$ be a sequence of elements of $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ which is an inversive generator. Let T denote the least period of this sequence. Then we define

$$\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n), c_n/p) \in [0,1)^{s+1}, \qquad n = 0, 1, \ldots. \tag{23}$$

The following lemma is a special case of [24, Lemma 3]. Note that we have shifted the indices by 1 to conform with the notation in the present paper.

Lemma 9. *Let $p \geq 3$ be a prime and let χ be a nontrivial additive character of the finite field $\mathbb{F}_p$. Let $c_0, c_1, \ldots \in \mathbb{F}_p$ be an inversive generator and let T be the least period of this sequence. Let $m \geq 1$ and $0 \leq d_1 < \cdots < d_m < T$*

be integers. Let $B \ge 1$ and $L \ge 1$ be integers with $B(L-1)+d_m < T$. If $h_1,\dots,h_m \in \mathbb{F}_p$ are not all 0, *then*

$$\Big|\sum_{n=0}^{L-1} \chi\Big(\sum_{j=1}^{m} h_j\, c_{Bn+d_j}\Big)\Big| = O_m(L^{1/2}p^{1/4}).$$

THEOREM 5. *Let $b_1,\dots,b_s$ be pairwise coprime integers ≥ 2. Let $p \ge 3$ be a prime, let $c_0, c_1, \dots \in \mathbb{F}_p$ be an inversive generator, and let T be the least period of this sequence. Then for $1 \le N \le T$ the discrepancy D_N of the first N terms of the sequence* (23) *satisfies*

$$D_N = O_{b_1,\dots,b_s}((N^{-1}p^{1/2}(\log p)^2)^{1/(s+2)})$$

with an implied constant depending only on $b_1,\dots,b_s$.

Proof. The discrepancy bound is trivial if $N \le p^{1/2}(\log p)^2$, and so we can assume that $p^{1/2}(\log p)^2 < N \le T$. We introduce the positive integers

$$f_i := \left\lceil \frac{1}{(s+2)\log b_i} \log \frac{N}{p^{1/2}(\log p)^2} \right\rceil \quad \text{for } 1 \le i \le s$$

and

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

We assume next that $N \ge B$. We proceed by a method similar to that in the proof of Theorem 1. We start with an interval $J \subseteq [0,1)^{s+1}$ of the form

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

with $v_1,\dots,v_s \in \mathbb{Z}$, $0 \le v_i < b_i^{f_i}$ for $1 \le i \le s$, and $0 < w \le 1$. As in (9) we get

$$A(J;N) = N\lambda_{s+1}(J) + O\bigg(\left\lfloor \frac{N-d-1+B}{B} \right\rfloor D^{(B)}_{\lfloor (N-d-1+B)/B \rfloor}\bigg), \tag{24}$$

where $D_L^{(B)}$ is the discrepancy of the first L terms of the sequence (c_{kB+d}/p), $k = 0,1,\dots$. Recall that $N \ge B \ge d+1$. We apply Lemma 9 with $m=1$ and $d_1 = d$. Note that for $L = \lfloor (N-d-1+B)/B \rfloor$ we have

$$B(L-1)+d \le N-d-1+d = N-1 \le T-1 < T,$$

and so the condition $B(L-1)+d_m < T$ in Lemma 9 is satisfied. Thus, for any $h \in \mathbb{Z}$ with $\gcd(h,p)=1$ we get

$$\Big|\sum_{k=0}^{L-1} \mathrm{e}\Big(\frac{h}{p}\, c_{kB+d}\Big)\Big| = O(L^{1/2}p^{1/4}).$$

Then [18, Corollary 3.11] yields

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

It thus follows from (24) that

$$A(J;N) = N\lambda_{s+1}(J) + O(B^{-1/2}N^{1/2}p^{1/4}\log p)$$

with an absolute implied constant.

For $J \subseteq [0,1)^{s+1}$ of the form

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

with $v_1,\dots,v_s \in \mathbb{Z}$, $1 \le v_i \le b_i^{f_i}$ for $1 \le i \le s$, and $0 < w \le 1$, the analog of (11) is

$$A(J;N) = N\lambda_{s+1}(J) + O(B^{1/2}N^{1/2}p^{1/4}\log p)$$

with an absolute implied constant.

In analogy with (12) we obtain

$$D_N^* \le \sum_{i=1}^{s} b_i^{-f_i} + O(B^{1/2}N^{-1/2}p^{1/4}\log p).$$

This bound is trivial for $N < B$, and so it holds for all integers N with $p^{1/2}(\log p)^2 < N \le T$. By the definition of the f_i we have

$$\left(\frac{N}{p^{1/2}(\log p)^2}\right)^{1/(s+2)} \le b_i^{f_i} \le b_i\left(\frac{N}{p^{1/2}(\log p)^2}\right)^{1/(s+2)} \qquad \text{for } 1 \le i \le s,$$

and so

$$B \le b_1 \cdots b_s \left(\frac{N}{p^{1/2}(\log p)^2}\right)^{s/(s+2)}.$$

This yields

$$D_N^* = O_{b_1,\dots,b_s}((N^{-1}p^{1/2}(\log p)^2)^{1/(s+2)}).$$

An application of (3) completes the proof. ■

Remark 6. Fix the parameters $b_1,\dots,b_s$ as in Theorem 5. For each prime $p \ge 3$, choose an inversive generator with maximum period $T = p+1$. Choose also positive integers $N_p \le p+1$ with

$$\lim_{p\to\infty} \frac{p^{1/2}(\log p)^2}{N_p} = 0.$$

Then $D_{N_p} \to 0$ as $p \to \infty$ by Theorem 5. It therefore follows by the Koksma–Hlawka inequality that the corresponding quasi-Monte Carlo method yields a convergent numerical integration scheme for integrands of bounded variation in the sense of Hardy and Krause.

7. Mixing $n\boldsymbol{\alpha}$ sequences and inversive sequences. Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ for an arbitrary dimension $t \geq 1$, let $p \geq 3$ be a prime, and let $c_0, c_1, \ldots$ be a sequence of elements of $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ which is an inversive generator as described in Section 2. Let T denote the least period of this sequence. We consider the sequence

$$\mathbf{x}_n = (\{n\boldsymbol{\alpha}\}, c_n/p) \in [0,1)^{t+1}, \quad n = 0, 1, \ldots. \tag{25}$$

We first establish a bound for the following exponential sum. For $\mathbf{h}_1 \in \mathbb{Z}^t$, $h \in \mathbb{Z}$, and an integer $N \geq 1$, put

$$G_N(\mathbf{h}_1, h) := \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + hc_n/p). \tag{26}$$

LEMMA 10. *Let $\boldsymbol{\alpha} \in \mathbb{R}^t$, $\mathbf{h}_1 \in \mathbb{Z}^t$, and $h \in \mathbb{Z}$ with* $\gcd(h,p) = 1$. *Let T be the least period of the sequence $c_0, c_1, \ldots \in \mathbb{F}_p$ given above. Then for the exponential sum $G_N(\mathbf{h}_1, h)$ in* (26) *we have*

$$|G_N(\mathbf{h}_1, h)| = O(N^{3/4}p^{1/8}) \quad \textit{for } 1 \leq N \leq T.$$

Proof. We have

$$\begin{aligned}
|G_N(\mathbf{h}_1, h)|^2 &= \sum_{k,n=0}^{N-1} \mathrm{e}((k-n)(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + h(c_k - c_n)/p) \\
&\leq N + 2\Big|\sum_{\substack{k,n=0 \\ k>n}}^{N-1} \mathrm{e}((k-n)(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + h(c_k - c_n)/p)\Big| \\
&= N + 2\Big|\sum_{d=1}^{N-1} \sum_{n=0}^{N-1-d} \mathrm{e}(d(\mathbf{h}_1 \cdot \boldsymbol{\alpha}) + h(c_{n+d} - c_n)/p)\Big| \\
&\leq N + 2\sum_{d=1}^{N-1} \Big|\sum_{n=0}^{N-1-d} \mathrm{e}(h(c_{n+d} - c_n)/p)\Big|.
\end{aligned}$$

To bound the inner sum, we apply Lemma 9 with $m = 2$, $d_1 = 0$, $d_2 = d$, $B = 1$, and $L = N - d$. Note that the condition $B(L-1) + d_2 < T$ in Lemma 9 is satisfied. Therefore we obtain

$$\Big|\sum_{n=0}^{N-1-d} \mathrm{e}(h(c_{n+d} - c_n)/p)\Big| = O(N^{1/2}p^{1/4}).$$

Hence

$$|G_N(\mathbf{h}_1, h)|^2 = O(N^{3/2}p^{1/4}),$$

which yields the desired result. ∎

In the following theorem, we again use the notion of finite type η introduced in Definition 3.

Theorem 6. *Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be of finite type η. Let T be the least period of the sequence $c_0, c_1, \ldots \in \mathbb{F}_p$ given above. Then for $1 \le N \le T$ the discrepancy D_N of the first N terms of the sequence* (25) *satisfies*

$$D_N = O_{\boldsymbol{\alpha},\varepsilon}(\max(N^{-1/((\eta-1)t+1)+\varepsilon}, N^{-1/4}p^{1/8}(\log N)^{t+1})) \quad \text{for all } \varepsilon > 0$$

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

Proof. Since the discrepancy bound is trivial for $N = 1$, we can assume that $2 \le N \le T$. We apply the Erdős–Turán–Koksma inequality (see Lemma 2) with

$$K = \min(\lceil N^{1/((\eta-1)t+1)} \rceil, p-1).$$

Then $2 \le K \le N$ and $K < p$. Furthermore,

$$D_N = O_t\biggl(\frac{1}{K} + \frac{1}{N} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^{t+1} \\ 0 < M(\mathbf{h}) \le K}} r(\mathbf{h})^{-1} \Bigl| \sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{x}_n) \Bigr| \biggr). \tag{27}$$

For $\mathbf{h} = (h_1, \ldots, h_{t+1}) \in \mathbb{Z}^{t+1}$ with $\mathbf{h} \ne \mathbf{0}$ and $h_{t+1} = 0$, we have

$$\sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{x}_n) = \sum_{n=0}^{N-1} \mathrm{e}(n(\mathbf{h}_1 \cdot \boldsymbol{\alpha})),$$

where $\mathbf{h}_1 = (h_1, \ldots, h_t) \in \mathbb{Z}^t$. Now fix an $\varepsilon > 0$. Then by Lemma 3 we get

$$\begin{aligned} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^{t+1},\, h_{t+1}=0 \\ 0 < M(\mathbf{h}) \le K}} r(\mathbf{h})^{-1} \Bigl| \sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{x}_n) \Bigr| &= O_{\boldsymbol{\alpha},\varepsilon}(K^{(\eta-1)t+\varepsilon}) \\ &= O_{\boldsymbol{\alpha},\varepsilon}(N^{(\eta-1)t/((\eta-1)t+1)+\varepsilon}). \end{aligned}$$

Moreover, for $\mathbf{h} \in \mathbb{Z}^{t+1}$ with $M(\mathbf{h}) \le K$ and $h_{t+1} \ne 0$, we can apply Lemma 10 to obtain

$$\Bigl| \sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{x}_n) \Bigr| = |G_N(\mathbf{h}_1, h_{t+1})| = O(N^{3/4}p^{1/8}).$$

Therefore

$$\begin{aligned} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^{t+1},\, h_{t+1}\ne 0 \\ 0 < M(\mathbf{h}) \le K}} r(\mathbf{h})^{-1} \Bigl| \sum_{n=0}^{N-1} \mathrm{e}(\mathbf{h} \cdot \mathbf{x}_n) \Bigr| &= O\Bigl(N^{3/4}p^{1/8} \sum_{\substack{\mathbf{h} \in \mathbb{Z}^{t+1},\, h_{t+1}\ne 0 \\ 0 < M(\mathbf{h}) \le K}} r(\mathbf{h})^{-1}\Bigr) \\ &= O_t(N^{3/4}p^{1/8}(\log K)^{t+1}) \\ &= O_t(N^{3/4}p^{1/8}(\log N)^{t+1}). \end{aligned}$$

By combining the above bounds with (27), we arrive at the desired result. ∎

Corollary 3. *Let $\boldsymbol{\alpha} \in \mathbb{R}^t$ be of finite type $\eta = 1$. Let T be the least period of the sequence $c_0, c_1, \ldots \in \mathbb{F}_p$ given above. Then for $2 \le N \le T$ the discrepancy D_N of the first N terms of the sequence* (25) *satisfies*

$$D_N = O_{\boldsymbol{\alpha}}(N^{-1/4} p^{1/8} (\log N)^{t+1})$$

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

Remark 7. Fix $\boldsymbol{\alpha} \in \mathbb{R}^t$ of finite type. For each prime $p \ge 3$, choose an inversive generator with maximum period $T = p + 1$. Choose also positive integers $N_p \le p + 1$ with

$$\lim_{p \to \infty} \frac{p^{1/2} (\log N_p)^{4t+4}}{N_p} = 0.$$

Then $D_{N_p} \to 0$ as $p \to \infty$ by Theorem 6. It therefore follows by the Koksma–Hlawka inequality that the corresponding quasi-Monte Carlo method yields a convergent numerical integration scheme for integrands of bounded variation in the sense of Hardy and Krause.

8. Concluding remarks. The discrepancy bounds in this paper are obtained by combining various number-theoretic techniques. Thus, a certain loss of precision has to be expected, and there is indeed no reason to believe that these bounds are best possible. Improvements on these results as well as lower bounds on the discrepancy of hybrid sequences going beyond known lower bounds for the constituent sequences would be desirable.

There are of course several other interesting families of basic sequences that can be used to produce hybrid sequences. For instance, an important family of low-discrepancy sequences for quasi-Monte Carlo methods is formed by digital (t, s)-sequences (see [27, Chapter 8]). A one-dimensional Halton sequence in base b, i.e., a van der Corput sequence in base b, is obviously a digital $(0, 1)$-sequence in base b, so this simple case has been covered in the paper. However, the main interest in this context is in “mixing” multidimensional digital (t, s)-sequences with other types of sequences, e.g. with sequences of pseudorandom numbers. It seems that methods different from those in the present paper have to be developed to treat such cases.

On a positive note, we observe that there are additional types of hybrid sequences for which nontrivial discrepancy bounds can be obtained by the methods in this paper. For instance, one can consider “mixing” Halton sequences or $n\boldsymbol{\alpha}$ sequences on the one hand with sequences of nonlinear congruential pseudorandom numbers (see [18, Section 8.1]) or explicit inversive congruential pseudorandom numbers (see [20, Section 3.3]) on the other hand. As in Remarks 3 and 5, one can adjoin $m \ge 1$ sequences of these pseudorandom numbers to Halton sequences or $n\boldsymbol{\alpha}$ sequences. Then one can establish nontrivial discrepancy bounds for the resulting hybrid sequences, provided that some fairly obvious conditions are met (compare e.g. with [19] for these conditions in the case of explicit inversive congruential pseudorandom numbers).

It should be quite evident from the remarks above that the question of discrepancy bounds for hybrid sequences offers a considerable range of new research activities.

Acknowledgments. This research was initiated while the author was hosted by CNRS-FR2291 (FRUMAM) and the IML at the Université de la Méditerranée in Marseille-Luminy. He thanks the IML for the kind hospitality and Christian Mauduit and Joël Rivat for stimulating discussions. This research is partially supported by the project NUGET of the Agence Nationale de la Recherche (France).

References

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

[2] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. 18 (2005), 477–499.

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

[4] J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, *A survey of quadratic and inversive congruential pseudorandom numbers*, in: Monte Carlo and Quasi-Monte Carlo Methods 1996, H. Niederreiter et al. (eds.), Lecture Notes in Statist. 127, Springer, New York, 1998, 66–97.

[5] J. E. Gentle, *Random Number Generation and Monte Carlo Methods*, 2nd ed., Springer, New York, 2003.

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

[7] E. Hlawka, *Funktionen von beschränkter Variation in der Theorie der Gleichverteilung*, Ann. Mat. Pura Appl. (4) 54 (1961), 325–333.

[8] —, *Uniform distribution modulo* 1 *and numerical analysis*, Compos. Math. 16 (1964), 92–105.

[9] L. K. Hua and Y. Wang, *Applications of Number Theory to Numerical Analysis*, Springer, Berlin, 1981.

[10] D. E. Knuth, *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, 3rd ed., Addison-Wesley, Reading, MA, 1998.

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

[12] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, MA, 1966.

[13] D. H. Lehmer, *Mathematical methods in large-scale computing units*, in: Proc. 2nd Sympos. on Large-Scale Digital Calculating Machinery (Cambridge, MA, 1949), Harvard Univ. Press, Cambridge, MA, 1951, 141–146.

[14] H. Niederreiter, *Methods for estimating discrepancy*, in: Applications of Number Theory to Numerical Analysis, S. K. Zaremba (ed.), Academic Press, New York, 1972, 203–236.

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

[16] —, *On the distribution of pseudo-random numbers generated by the linear congruential method. III*, Math. Comp. 30 (1976), 571–597.

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

[18] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[19] —, *On a new class of pseudorandom numbers for simulation methods*, J. Comput. Appl. Math. 56 (1994), 159–167.

[20] —, *New developments in uniform pseudorandom number and vector generation*, in: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, H. Niederreiter and P. J.-S. Shiue (eds.), Lecture Notes in Statist. 106, Springer, New York, 1995, 87–120.

[21] —, *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.), Proc. Appl. Math. 116, SIAM, Philadelphia, 2004, 337–351.

[22] H. Niederreiter and J. Rivat, *On the correlation of pseudorandom numbers generated by inversive methods*, Monatsh. Math. 153 (2008), 251–264.

[23] —, —, *On the Gowers norm of pseudorandom binary sequences*, Bull. Austral. Math. Soc. 79 (2009), 259–271.

[24] H. Niederreiter, J. Rivat, and A. Sárközy, *Pseudorandom sequences of binary vectors*, Acta Arith. 133 (2008), 109–125.

[25] H. Niederreiter and I. E. Shparlinski, *Recent advances in the theory of nonlinear pseudorandom number generators*, in: Monte Carlo and Quasi-Monte Carlo Methods 2000, K.-T. Fang et al. (eds.), Springer, Berlin, 2002, 86–102.

[26] H. Niederreiter and A. Winterhof, *On the structure of inversive pseudorandom number generators*, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, S. Boztaş and H. F. Lu (eds.), Lecture Notes in Comput. Sci. 4851, Springer, Berlin, 2007, 208–216.

[27] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.

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

[29] —, *Applications of a hybrid-Monte Carlo sequence to option pricing*, in: Monte Carlo and Quasi-Monte Carlo Methods 1998, H. Niederreiter and J. Spanier (eds.), Springer, Berlin, 2000, 391–406.

[30] 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.

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

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

[33] J. Spanier and L. M. Li, *Quasi-Monte Carlo methods for integral equations*, in: Monte Carlo and Quasi-Monte Carlo Methods 1996, H. Niederreiter et al. (eds.), Lecture Notes in Statist. 127, Springer, New York, 1998, 398–414.

RICAM
University of Linz
Altenbergerstr. 69
A-4040 Linz, Austria
E-mail: ghnied@gmail.com

Department of Mathematics
University of Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg, Austria

Received on 3.11.2008
and in revised form on 5.3.2009 (5843)