# Low-Discrepancy and Low-Dispersion Sequences

HARALD NIEDERREITER

*Mathematical Institute, Austrian Academy of Sciences,*
*Dr. Ignaz-Seipel-Platz 2, A-1010 Vienna, Austria*

*Communicated by W. Schmidt*

Received October 2, 1987

We generalize and improve earlier constructions of low-discrepancy sequences by Sobol', Faure, and the author, thus obtaining sequences in the $s$-dimensional unit cube with the smallest discrepancy that is currently known. The construction is based on the theory of $(t, s)$-sequences. It is also shown that the dispersion of the sequences constructed here has the smallest possible order of magnitude among any sequences in the $s$-dimensional unit cube. © 1988 Academic Press, Inc.

## 1. Introduction

The discrepancy and the dispersion are well-known measures for the irregularity of distribution of a sequence. They are not only of number-theoretic interest, but they are also important for applications to numerical analysis. Sequences with small discrepancy (or *low-discrepancy sequences*) play a central role in quasi-Monte Carlo methods for numerical integration (see [4, 5, 9]), and sequences with small dispersion (or *low-dispersion sequences*) play a similar role in quasi-Monte Carlo methods for global optimization (see [10, 12, 15]).

In this paper we present new constructions of low-discrepancy sequences which generalize and improve earlier constructions and yield sequences with the smallest discrepancy that is currently known. As a by-product of these constructions we also obtain new low-dispersion sequences. The basis for these new constructions is the systematic theory of $(t, m, s)$-nets and $(t, s)$-sequences developed in Niederreiter [14]. We also employ a methodological innovation which allows us to replace earlier arguments based on the evaluation of complicated determinants by more transparent arguments based on formal Laurent series (see Section 3).

We recall the definition of discrepancy. For $N$ points $\mathbf{x}_1, ..., \mathbf{x}_N$ in the $s$-dimensional half-open unit cube $I^s = [0, 1)^s$, $s \geqslant 1$, and a subinterval $J$ of $I^s$ we put

$$D(J; N) = A(J; N) - V(J)\, N,$$

0022-314X/88 $3.00

where $A(J; N)$ is the number of $n$, $1 \leqslant n \leqslant N$, with $\mathbf{x}_n \in J$ and $V(J)$ is the volume of $J$. Then the *discrepancy* $\Delta(N)$ of the points $\mathbf{x}_1, ..., \mathbf{x}_N$ is defined by

$$\Delta(N) = \sup_J |D(J; N)|,$$

where the supremum is extended over all half-open subintervals $J = \prod_{i=1}^s [0, u_i)$ of $I^s$. Thus we have $\Delta(N) = ND_N^*$, where $D_N^*$ is the usual star discrepancy of the points $\mathbf{x}_1, ..., \mathbf{x}_N$ (see [5, 9]). For a sequence $\mathbf{x}_1, \mathbf{x}_2, ...$ of points in $I^s$ we define $\Delta(N)$ to be the discrepancy of the first $N$ terms of the sequence.

The principal aim in the construction of low-discrepancy point sets and sequences is to find, for any $N \geqslant 2$, $N$ points in $I^s$ with

$$\Delta(N) \leqslant B_s(\log N)^{s-1} + O((\log N)^{s-2}) \tag{1}$$

and sequences of points in $I^s$ with

$$\Delta(N) \leqslant C_s(\log N)^s + O((\log N)^{s-1}) \qquad \text{for all } N \geqslant 2, \tag{2}$$

where the constants $B_s$ and $C_s$ are as small as possible. Constructions with successively smaller values of these constants were obtained (in chronological order) by Halton [3], Sobol' [19], Faure [2], and Niederreiter [14]. By a well-known principle (compare with Section 5), low-discrepancy point sets in $I^s$, $s \geqslant 2$, can be obtained from low-discrepancy sequences in $I^{s-1}$. Therefore we shall concentrate on the problem of constructing low-discrepancy sequences.

The following three definitions from [14] are basic. In these definitions the dimension $s \geqslant 1$ and the integer $b \geqslant 2$ are fixed.

Definition 1. An *elementary interval in base b* is an interval of the form

$$E = \prod_{i=1}^s [a_i b^{-d_i}, (a_i + 1) b^{-d_i})$$

with integers $d_i \geqslant 0$ and integers $0 \leqslant a_i < b^{d_i}$ for $1 \leqslant i \leqslant s$.

Definition 2. Let $0 \leqslant t \leqslant m$ be integers. A *$(t, m, s)$-net in base b* is a point set of $b^m$ points in $I^s$ such that $A(E; b^m) = b^t$ for every elementary interval $E$ in base $b$ with $V(E) = b^{t-m}$.

Definition 3. Let $t \geqslant 0$ be an integer. A sequence $\mathbf{x}_1, \mathbf{x}_2, ...$ of points in $I^s$ is called a *$(t, s)$-sequence in base b* if for all integers $k \geqslant 0$ and $m > t$ the point set consisting of the $\mathbf{x}_n$ with $kb^m < n \leqslant (k+1)\,b^m$ is a $(t, m, s)$-net in base $b$.

The construction by Sobol' [19] yields $(t, s)$-sequences in base 2 with values of $t$ that depend on $s$. The construction by Faure [2] yields $(0, s)$-sequences in prime bases $\geqslant s$ and the construction by Niederreiter [14] yields $(0, s)$-sequences in prime power bases $\geqslant s$. According to [14, Sect. 4] the discrepancy of a $(t, s)$-sequence in base $b$ satisfies an effective bound

$$\Delta(N) \leqslant C(t, s, b)(\log N)^s + O((\log N)^{s-1}) \qquad \text{for all } N \geqslant 2, \tag{3}$$

where $C(t, s, b)$ is given as

$$C(t, s, b) = \frac{1}{8}\, b^t \left(\frac{b-1}{\log b}\right)^2 \qquad \text{for} \quad s = 2,$$

$$C(t, s, b) = \frac{2^t}{24(\log 2)^3} \qquad \text{for} \quad s = 3 \quad \text{and} \quad b = 2,$$

$$C(t, s, b) = \frac{2^t}{64(\log 2)^4} \qquad \text{for} \quad s = 4 \quad \text{and} \quad b = 2,$$

$$C(t, s, b) = \frac{1}{s!}\, b^t \frac{b-1}{2\lfloor b/2 \rfloor} \left(\frac{\lfloor b/2 \rfloor}{\log b}\right)^s \qquad \text{in all other cases,}$$

where $\lfloor u \rfloor$ denotes the greatest integer $\leqslant u$. In particular, we obtain a bound of the form (2) for the discrepancy. For fixed $s$ and $b$ the parameter $t$ should be as small as possible to get a small value of the constant $C(t, s, b)$. The constructions in the present paper yield $(t, s)$-sequences in base $b$ with relatively small values of $t$.

As to lower bounds for $\Delta(N)$, we recall the classical result of Roth [17] which says that $\Delta(N) = \Omega((\log N)^{s/2})$ for any sequence of points in $I^s$. This has only been improved in the case $s = 1$, where Schmidt [18] has shown that $\Delta(N) = \Omega(\log N)$ for any sequence of points in $I^1$.

In Section 2 we describe the general principles on which our constructions are based. The details of the constructions are carried out in Section 3 for prime power bases, and they are extended to general bases in Section 4. Consequences of these constructions for the values of the constants $B_s$ and $C_s$ in (1) resp. (2) that can now be obtained are pointed out in Section 5. The implementation of the low-discrepancy sequences constructed here is briefly discussed in Section 6. The dispersion of $(t, m, s)$-nets and $(t, s)$-sequences is studied in Section 7. The Appendix contains some numerical tables.

## 2. Principles of the Construction

The following construction principle was used in [14] to obtain $(t, s)$-sequences in base $b$. Let $s \geqslant 1$ and $b \geqslant 2$ be given integers and write $B = \{0, 1, ..., b-1\}$ for the set of digits in base $b$. Then choose the following:

(i) a commutative ring $R$ with identity and $\operatorname{card}(R) = b$;

(ii) bijections $\psi_r : B \to R$ for $r = 0, 1, ...,$ with $\psi_r(0) = 0$ for all sufficiently large $r$;

(iii) bijections $\lambda_{ij} : R \to B$ for $i = 1, 2, ..., s$ and $j = 1, 2, ...,$ with $\lambda_{ij}(0) = 0$ for $1 \leqslant i \leqslant s$ and all sufficiently large $j$;

(iv) elements $c_{jr}^{(i)} \in R$ for $1 \leqslant i \leqslant s$, $j \geqslant 1$, $r \geqslant 0$, where for fixed $i$ and $r$ we have $c_{jr}^{(i)} = 0$ for all sufficiently large $j$.

For $n = 1, 2, ...$ let

$$n - 1 = \sum_{r=0}^{\infty} a_r(n)\, b^r, \qquad a_r(n) \in B,$$

be the representation of $n-1$ in base $b$. Put

$$x_n^{(i)} = \sum_{j=1}^{\infty} x_{nj}^{(i)} b^{-j} \qquad \text{for} \quad 1 \leqslant i \leqslant s \quad \text{and} \quad n \geqslant 1$$

with

$$x_{nj}^{(i)} = \lambda_{ij}\left(\sum_{r=0}^{\infty} c_{jr}^{(i)} \psi_r(a_r(n))\right) \in B \qquad \text{for} \quad 1 \leqslant i \leqslant s, \quad j \geqslant 1, \quad n \geqslant 1.$$

Note that the sum over $r$ is a finite sum since $\psi_r(0) = 0$ and $a_r(n) = 0$ for all sufficiently large $r$. From the conditions (iii) and (iv) it follows that each $x_n^{(i)}$ is given by an expansion with finitely many terms. Now define the sequence

$$\mathbf{x}_n = (x_n^{(1)}, ..., x_n^{(s)}) \in I^s \qquad \text{for} \quad n = 1, 2, .... \tag{4}$$

The bijections in (ii) and (iii) can be chosen arbitrarily, but the ring $R$ in (i) and the elements $c_{jr}^{(i)}$ in (iv) have to be chosen judiciously for (4) to become a $(t, s)$-sequence in base $b$ with a small value of $t$. We quote the following result from [14, Remark 6.24].

Lemma 1. *Let $b \geqslant 2$ and $t \geqslant 0$ be integers and let $R$ be a commutative ring with identity and* $\operatorname{card}(R) = b$. *Suppose that for any integers $m > t$ and*

*$d_1, ..., d_s \geqslant 0$ with $\sum_{i=1}^{s} d_i = m - t$ and any elements $\alpha_j^{(i)} \in R$, $1 \leqslant j \leqslant d_i$, $1 \leqslant i \leqslant s$, the system*

$$\sum_{r=0}^{m-1} c_{jr}^{(i)} y_r = \alpha_j^{(i)} \qquad \textit{for} \quad 1 \leqslant j \leqslant d_i, \quad 1 \leqslant i \leqslant s,$$

*in the unknowns $y_0, ..., y_{m-1}$ over $R$ has exactly $b^t$ solutions. Then the sequence* (4) *is a $(t, s)$-sequence in base $b$.*

Now we consider the case where $b$ is a prime power and $R = F_b$, the finite field with $b$ elements. The quantity $\sigma(C)$ introduced in the following definition is related to the quantity $\rho(C)$ in [14, Definition 6.8] by $\rho(C) = \sigma(C) + 1$. The subsequent lemma follows from [14, Theorem 6.23].

DEFINITION 4. Let $b$ be a prime power, let $m$ and $s$ be positive integers, and let $C = \{\mathbf{c}_j^{(i)}: 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant s\}$ be a system of vectors in the $m$-dimensional vector space $F_b^m$. Then $\sigma(C)$ is defined as the largest integer $d$ such that any system $\{\mathbf{c}_j^{(i)}: 1 \leqslant j \leqslant d_i, 1 \leqslant i \leqslant s\}$ with $0 \leqslant d_i \leqslant m$ for $1 \leqslant i \leqslant s$ and $\sum_{i=1}^{s} d_i = d$ is linearly independent over $F_b$.

LEMMA 2. *Let $b$ be a prime power, let $R = F_b$, and let $t \geqslant 0$ be an integer. Suppose that for each integer $m > t$ the system $C(m)$ consisting of the vectors*

$$\mathbf{c}_j^{(i)}(m) = (c_{j0}^{(i)}, ..., c_{j,m-1}^{(i)}) \in F_b^m \qquad \textit{for} \quad 1 \leqslant j \leqslant m, \quad 1 \leqslant i \leqslant s,$$

*satisfies $\sigma(C(m)) \geqslant m - t$. Then the sequence* (4) *is a $(t, s)$-sequence in base $b$.*

Therefore the problem of constructing $(t, s)$-sequences in base $b$ reduces to the problem of finding elements $c_{jr}^{(i)} \in R$ for which the condition in Lemma 1 or 2 is satisfied.

## 3. PRIME POWER BASES

For an arbitrary field $F$ let $G = F((x^{-1}))$ be the field of formal Laurent series

$$L = \sum_{r=w}^{\infty} b_r x^{-r}$$

in $x^{-1}$, where all $b_r \in F$ and $w$ is an arbitrary integer. Define the discrete exponential valuation $v$ on $G$ as follows: for $L \neq 0$ put $v(L) = -w$ if $w$ is the least index with $b_w \neq 0$, and for $L = 0$ put $v(L) = -\infty$. The field $G$ contains the field of rational functions over $F$ as a subfield. For $f, g \in F[x]$ with $g \neq 0$ we have $v(f/g) = \deg(f) - \deg(g)$, where $\deg(0) = -\infty$.

Lemma 3. *Let $p_1, \dots, p_s \in F[x]$ be pairwise coprime and $\deg(p_i) = e_i \geqslant 1$ for $1 \leqslant i \leqslant s$. Let $h_1, \dots, h_s$ be positive integers and for $1 \leqslant j \leqslant h_i$, $1 \leqslant i \leqslant s$, let $f_{ij}, g_{ij} \in F[x]$ with $\deg(f_{ij}) < e_i$ and $\gcd(g_{ij}, p_i) = 1$. Suppose that*

$$\sum_{i=1}^{s} \sum_{j=1}^{h_i} \frac{f_{ij} g_{ij}}{p_i^j} = f + L \tag{5}$$

*with $f \in F[x]$, $L \in G$, and $v(L) < -\sum_{i=1}^{s} h_i e_i$. Then $f_{ij} = 0$ for all $1 \leqslant j \leqslant h_i$, $1 \leqslant i \leqslant s$.*

*Proof.* Multiplying (5) by $p_1^{h_1} \cdots p_s^{h_s}$, we get on the left a polynomial and on the right $g + L_1$ with $g \in F[x]$, $L_1 \in G$, and $v(L_1) < 0$. But then $L_1 \in F[x]$, hence $L_1 = 0$ and

$$p_1^{h_1} \cdots p_s^{h_s} \sum_{i=1}^{s} \sum_{j=1}^{h_i} \frac{f_{ij} g_{ij}}{p_i^j} = p_1^{h_1} \cdots p_s^{h_s} f.$$

Considering this polynomial identity $\bmod\, p_i$, $1 \leqslant i \leqslant s$, we get

$$f_{ih_i} g_{ih_i} \prod_{\substack{k=1 \\ k \neq i}}^{s} p_k^{h_k} \equiv 0 \bmod p_i.$$

Since the polynomial by which $f_{ih_i}$ is multiplied on the left is coprime to $p_i$, we obtain $f_{ih_i} \equiv 0 \bmod p_i$, and since $\deg(f_{ih_i}) < e_i$, this implies $f_{ih_i} = 0$. Continuing in this manner we get the desired conclusion. ▮

Let again $p_1, \dots, p_s \in F[x]$ be pairwise coprime and $\deg(p_i) = e_i \geqslant 1$ for $1 \leqslant i \leqslant s$. For $1 \leqslant i \leqslant s$ and $j \geqslant 1$ let $g_{ij} \in F[x]$ with $\gcd(g_{ij}, p_i) = 1$. For $0 \leqslant k < e_i$, $1 \leqslant i \leqslant s$, and $j \geqslant 1$ consider the expansion

$$\frac{x^k g_{ij}(x)}{p_i(x)^j} = \sum_{r=w}^{\infty} a^{(i)}(j, k, r)\, x^{-r-1}, \tag{6}$$

by which the elements $a^{(i)}(j, k, r) \in F$ are determined. Here $w \leqslant 0$ may depend on $i, j, k$. Then define

$$c_{jr}^{(i)} = a^{(i)}(q+1, u, r) \qquad \text{for} \quad 1 \leqslant i \leqslant s, \quad j \geqslant 1, \quad r \geqslant 0, \tag{7}$$

where $j - 1 = q e_i + u$ with integers $q = q^{(i)}(j)$ and $u = u^{(i)}(j)$ satisfying $0 \leqslant u < e_i$.

Lemma 4. *Let the elements $c_{jr}^{(i)} \in F$ be given by (7). Then for each integer $m > \sum_{i=1}^{s} (e_i - 1)$ and any integers $d_1, \dots, d_s \geqslant 0$ with*

$$1 \leqslant \sum_{i=1}^{s} d_i \leqslant m - \sum_{i=1}^{s} (e_i - 1)$$

*the vectors*

$$\mathbf{c}_j^{(i)}(m) = (c_{j0}^{(i)}, \ldots, c_{j,m-1}^{(i)}) \in F^m \qquad \textit{for} \quad 1 \leqslant j \leqslant d_i, \quad 1 \leqslant i \leqslant s, \tag{8}$$

*are linearly independent over F.*

*Proof.* Let $d_1, \ldots, d_s$ be as in the lemma and suppose that the vectors in (8) satisfy a linear dependence relation

$$\sum_{i=1}^{s} \sum_{j=1}^{d_i} f_j^{(i)} \mathbf{c}_j^{(i)}(m) = \mathbf{0} \in F^m$$

with all $f_j^{(i)} \in F$. Without loss of generality we can assume that all $d_i \geqslant 1$. Write $d_i - 1 = q_i e_i + u_i$ with integers $q_i$ and $u_i$ satisfying $0 \leqslant u_i < e_i$. In view of (7) the linear dependence relation can be put in the form

$$\sum_{i=1}^{s} \sum_{q=1}^{q_i+1} \sum_{u=0}^{e(i,q)} f^{(i)}(q, u)\, a^{(i)}(q, u, r) = 0 \qquad \text{for} \quad 0 \leqslant r \leqslant m-1,$$

where $e(i, q) = e_i - 1$ for $1 \leqslant q \leqslant q_i$, $e(i, q_i + 1) = u_i$, and $f^{(i)}(q, u) = f_{(q-1)e_i+u+1}^{(i)}$. Now consider

$$\sum_{i=1}^{s} \sum_{q=1}^{q_i+1} \sum_{u=0}^{e(i,q)} f^{(i)}(q, u) \frac{x^u g_{iq}(x)}{p_i(x)^q}$$
$$= \sum_{r=w}^{\infty} \left( \sum_{i=1}^{s} \sum_{q=1}^{q_i+1} \sum_{u=0}^{e(i,q)} f^{(i)}(q, u)\, a^{(i)}(q, u, r) \right) x^{-r-1}, \tag{9}$$

where $w \leqslant 0$ is suitable. With

$$f_{iq}(x) = \sum_{u=0}^{e(i,q)} f^{(i)}(q, u)\, x^u \qquad \text{for} \quad 1 \leqslant q \leqslant q_i + 1, \quad 1 \leqslant i \leqslant s,$$

we have $\deg(f_{iq}) < e_i$. Furthermore, for the formal Laurent series on the right-hand side of (9) the coefficient of $x^{-r-1}$ is 0 for $0 \leqslant r \leqslant m-1$. Thus (9) can be written in the form

$$\sum_{i=1}^{s} \sum_{q=1}^{q_i+1} \frac{f_{iq}\, g_{iq}}{p_i^q} = f + L$$

with $f \in F[x]$, $L \in G$, and

$$v(L) < -m \leqslant -\sum_{i=1}^{s} d_i - \sum_{i=1}^{s} (e_i - 1)$$
$$\leqslant -\sum_{i=1}^{s} (d_i - u_i - 1 + e_i) = -\sum_{i=1}^{s} (q_i + 1)\, e_i.$$

Therefore Lemma 3 yields $f_{iq}=0$ for all $1 \leqslant q \leqslant q_i+1$, $1 \leqslant i \leqslant s$. It follows that all $f^{(i)}(q, u)$ appearing in (9) are 0, and so all $f_j^{(i)}=0$. ▌

In the application of Lemma 4 to the construction of low-discrepancy sequences we let $F$ be a finite field $F_b$ of prime power order $b$. For the ring $R$ in Section 2 we also take $R=F_b$.

Theorem 1. *Let $b$ be an arbitrary prime power and let $p_1, ..., p_s \in F_b[x]$ be pairwise coprime, where $s \geqslant 1$ is arbitrary and $\deg(p_i)=e_i \geqslant 1$ for $1 \leqslant i \leqslant s$. For $1 \leqslant i \leqslant s$ and $j \geqslant 1$ let $g_{ij} \in F_b[x]$ with $\gcd(g_{ij}, p_i)=1$ and*

$$\lim_{j \to \infty} (je_i - \deg(g_{ij})) = \infty \qquad \textit{for} \quad 1 \leqslant i \leqslant s.$$

*If the elements $c_{jr}^{(i)} \in F_b$ are defined by (7), then the sequence (4) is a $(t, s)$-sequence in base $b$ with*

$$t = \sum_{i=1}^{s} (e_i - 1).$$

*Proof.* In (6) we have

$$v\left(\frac{x^k g_{ij}(x)}{p_i(x)^j}\right) = k + \deg(g_{ij}) - je_i,$$

thus $a^{(i)}(j, k, r)=0$ for $r < je_i - \deg(g_{ij}) - k - 1$. Hence for fixed $i$ and $r$ we have $a^{(i)}(j, k, r)=0$ for all sufficiently large $j$ and all $0 \leqslant k < e_i$. Therefore the elements $c_{jr}^{(i)}$ defined by (7) satisfy the condition (iv) in Section 2. Furthermore, for each integer $m > t = \sum_{i=1}^{s} (e_i - 1)$ the system $C(m)$ consisting of the vectors

$$\mathbf{c}_j^{(i)}(m) = (c_{j0}^{(i)}, ..., c_{j,m-1}^{(i)}) \in F_b^m \qquad \text{for} \quad 1 \leqslant j \leqslant m, \quad 1 \leqslant i \leqslant s,$$

satisfies $\sigma(C(m)) \geqslant m - t$ by Lemma 4. The desired result follows then from Lemma 2. ▌

To get the optimal consequence out of Theorem 1, the value of $t$ in Theorem 1 has to be minimized for fixed $s$ and $b$. In other words, the degrees of the polynomials $p_1, ..., p_s$ have to be chosen as small as possible. This is achieved as follows. We list all monic irreducible polynomials over $F_b$ in a sequence $p_1, p_2, ...$ in such a way that $\deg(p_i) \leqslant \deg(p_h)$ whenever $i \leqslant h$. Then we let $p_1, ..., p_s$ be the first $s$ terms in this sequence of polynomials. If we set $e_i = \deg(p_i)$, $1 \leqslant i \leqslant s$, for this choice of polynomials, then the number

$$T_b(s) = \sum_{i=1}^{s} (e_i - 1) \tag{10}$$

is well defined and represents the minimal value of $t$ in Theorem 1 for fixed $s$ and $b$. We summarize this as follows.

COROLLARY 1. *For every prime power $b$ and every integer $s \geqslant 1$ there exists a $(T_b(s), s)$-sequence in base $b$.*

For a prime power $b \geqslant s$ we can take $p_1, ..., p_s$ to be linear polynomials, hence $T_b(s) = 0$. Therefore Corollary 1 includes a result of the author [14, Corollary 6.20] as a special case. In the even more special case where $b$ is a prime $\geqslant s$, Corollary 1 yields a result of Faure [2].

The number $T_b(s)$ can be expressed easily in terms of the number $N_b(n)$ of monic irreducible polynomials over $F_b$ of degree $n$. Note that by [8, Theorem 3.25] we have

$$N_b(n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) b^d \qquad \text{for all } n \geqslant 1, \tag{11}$$

where $\mu$ is the Möbius function. Let $M_b(n) = \sum_{h=1}^{n} N_b(h)$ be the number of monic irreducible polynomials over $F_b$ of degree $\leqslant n$, with $M_b(0) = 0$. For given $s \geqslant 1$ let $n = n(b, s)$ be the largest integer with $M_b(n) \leqslant s$. Then we clearly have

$$T_b(s) = \sum_{h=1}^{n} (h-1) N_b(h) + n(s - M_b(n)). \tag{12}$$

Values of $T_b(s)$ for $b = 2, 3, 4, 5$ and $1 \leqslant s \leqslant 30$ are tabulated in the Appendix. A general upper bound for $T_b(s)$ is obtained in Theorem 2 below.

LEMMA 5. *For any prime power $b$ we have*

$$M_b(n) \geqslant \frac{b^n}{n} \qquad \textit{for all } n \geqslant 1.$$

*Proof.* This is trivial for $n = 1, 2, 3$. For $n \geqslant 3$ we use induction and (11):

$$M_b(n+1) = M_b(n) + N_b(n+1) \geqslant \frac{b^n}{n} + \frac{1}{n+1}\left(b^{n+1} - \sum_{d=1}^{\lfloor (n+1)/2 \rfloor} b^d\right)$$

$$> \frac{b^{n+1}}{n+1} + \frac{1}{n}\left(b^n - b^{(n+3)/2}\right) \geqslant \frac{b^{n+1}}{n+1}. \quad \blacksquare$$

THEOREM 2. *Let $b$ be any prime power and $s \geqslant 1$. For $s \leqslant b$ we have $T_b(s) = 0$ and for $s > b$ we have*

$$T_b(s) < s(\log_b s + \log_b \log_b s + 1),$$

*where $\log_b$ denotes the logarithm to the base $b$.*

*Proof.* The trivial first part was already noted earlier. For $s > b$ we have

$$T_b(s) < n(b, s)\, s \tag{13}$$

by (12). Put

$$k = \lfloor \log_b s + \log_b \log_b s \rfloor + 2.$$

If either $b = 2$, $y \geqslant 4$, or $b \geqslant 3$, $y > 1$, then

$$(b-1)\, y \geqslant \log_b y + 2.$$

With $y = \log_b s$ we obtain

$$b \log_b s \geqslant \log_b s + \log_b \log_b s + 2 \geqslant k$$

if either $b = 2$, $s \geqslant 16$, or $b \geqslant 3$, $s > b$. In these cases it follows that

$$k > \log_b s + \log_b \log_b s + 1 \geqslant \log_b s + \log_b k,$$

hence by Lemma 5,

$$M_b(k) \geqslant \frac{b^k}{k} > s.$$

By the definition of $n(b, s)$ we get

$$n(b, s) \leqslant k - 1 \leqslant \log_b s + \log_b \log_b s + 1,$$

and the bound for $T_b(s)$ follows from (13). In the remaining case $b = 2$, $3 \leqslant s \leqslant 15$, the bound for $T_b(s)$ is checked directly by using Table II in the Appendix. ∎

## 4. GENERAL BASES

Let the base $b = q_1 \cdots q_h$ be a product of arbitrary prime powers $q_1, ..., q_h$. For $1 \leqslant v \leqslant h$ let $F_{q_v}$ be the finite field of order $q_v$, and let the ring $R = \prod_{v=1}^{h} F_{q_v}$ be the direct product of these finite fields. Then $R$ is a commutative ring with identity and $\mathrm{card}(R) = b$. Note that all operations in $R$ are performed coordinatewise.

Following the construction principle in Section 2, we choose elements $c_{jr}^{(i)} \in R$ for $1 \leqslant i \leqslant s$, $j \geqslant 1$, $r \geqslant 0$, which satisfy condition (iv) in Section 2. These elements are of the form

$$c_{jr}^{(i)} = (c_{jr1}^{(i)}, ..., c_{jrh}^{(i)}), \tag{14}$$

where $c_{jrv}^{(i)} \in F_{q_v}$ for $1 \leqslant i \leqslant s$, $j \geqslant 1$, $r \geqslant 0$, $1 \leqslant v \leqslant h$. For fixed $i$, $r$, and $v$ we must have $c_{jrv}^{(i)} = 0$ for all sufficiently large $j$. The following is a generalization of Lemma 2.

THEOREM 3. *Let $b = q_1 \cdots q_h$ be a product of arbitrary prime powers $q_1, ..., q_h$, let $R = \prod_{v=1}^{h} F_{q_v}$, and let $t \geqslant 0$ be an integer. Suppose that for each integer $m > t$ and each $v$ with $1 \leqslant v \leqslant h$ the system $C_v(m)$ consisting of the vectors*

$$\mathbf{c}_{jv}^{(i)}(m) = (c_{j0v}^{(i)}, ..., c_{j,m-1,v}^{(i)}) \in F_{q_v}^m \qquad \textit{for} \quad 1 \leqslant j \leqslant m, \quad 1 \leqslant i \leqslant s,$$

*satisfies $\sigma(C_v(m)) \geqslant m - t$. Then the sequence (4) is a $(t, s)$-sequence in base $b$.*

*Proof.* We proceed by Lemma 1. For integers $m > t$ and $d_1, ..., d_s \geqslant 0$ with $\sum_{i=1}^{s} d_i = m - t$ and elements

$$\alpha_j^{(i)} = (\alpha_{j1}^{(i)}, ..., \alpha_{jh}^{(i)}) \in R \qquad \text{for} \quad 1 \leqslant j \leqslant d_i, \quad 1 \leqslant i \leqslant s,$$

consider the system

$$\sum_{r=0}^{m-1} c_{jr}^{(i)} y_r = \alpha_j^{(i)} \qquad \text{for} \quad 1 \leqslant j \leqslant d_i, \quad 1 \leqslant i \leqslant s, \tag{15}$$

in the unknowns $y_0, ..., y_{m-1}$ over $R$. Because of the direct product structure of $R$, this is equivalent to considering for $1 \leqslant v \leqslant h$ the system of $m - t$ equations

$$\sum_{r=0}^{m-1} c_{jrv}^{(i)} y_{rv} = \alpha_{jv}^{(i)} \in F_{q_v} \qquad \text{for} \quad 1 \leqslant j \leqslant d_i, \quad 1 \leqslant i \leqslant s, \tag{16}$$

in the $m$ unknowns $y_{0v}, ..., y_{m-1,v}$ over $F_{q_v}$. From $\sigma(C_v(m)) \geqslant m - t$ we get that the system matrix of (16) has rank $m - t$ for each $v$. Thus the system (16) has exactly $q_v^t$ solutions for each $v$. Consequently, the system (15) has exactly $q_1^t \cdots q_h^t = b^t$ solutions. ▌

THEOREM 4. *Let $b = q_1 \cdots q_h$ be a product of arbitrary prime powers*

*$q_1, ..., q_h$. Then for every integer $s \geqslant 1$ there exists a $(t, s)$-sequence in base $b$ with*

$$t = \max_{1 \leqslant v \leqslant h} T_{q_v}(s),$$

*where $T_{q_v}(s)$ is defined by* (10).

*Proof.* For each $v$ with $1 \leqslant v \leqslant h$ we choose elements $c_{jrv}^{(i)} \in F_{q_v}$ for $1 \leqslant i \leqslant s$, $j \geqslant 1$, and $r \geqslant 0$ as in Theorem 1, with the polynomials $p_{1v}, ..., p_{sv} \in F_{q_v}[x]$ being chosen in such a way that

$$\sum_{i=1}^{s} (\deg(p_{iv}) - 1) = T_{q_v}(s).$$

Then we define the elements $c_{jr}^{(i)} \in R = \prod_{v=1}^{h} F_{q_v}$ for $1 \leqslant i \leqslant s, j \geqslant 1$, and $r \geqslant 0$ by (14). Now we proceed by similar arguments as in the proof of Theorem 1 and use Theorem 3. ▌

## 5. Consequences for Low-Discrepancy Sequences

We now return to a question raised in Section 1, namely to find a sequence of points in $I^s$ whose discrepancy satisfies

$$\Delta(N) \leqslant C_s(\log N)^s + O((\log N)^{s-1}) \qquad \text{for all } N \geqslant 2,$$

where the constant $C_s$ is as small as possible. For $s = 1$ we can take

$$C_1 = \frac{1919}{3454 \log 12} + \varepsilon \qquad \text{for any } \varepsilon > 0$$

by a result of Faure [1]. For $s \geqslant 2$ and any prime power $b$ the sequences constructed in Theorem 1 are $(t, s)$-sequences in base $b$ and so they satisfy the discrepancy bound (3) with the constant $C(t, s, b)$ given there. By Corollary 1 we can always achieve $t = T_b(s)$ with $T_b(s)$ given in (10). Therefore we can take

$$C_s = \min_b C(T_b(s), s, b),$$

where the minimum is extended over all prime powers $b$. For $s = 2$ this yields

$$C_2 = C(0, 2, 2) = \frac{1}{8(\log 2)^2}.$$

For $s \geqslant 3$ let $b_1(s)$ be the least even prime power $\geqslant s$, let $b_2(s)$ be the least odd prime power $\geqslant s$, and put

$$C'_s = \min_{b<s} C(T_b(s), s, b),$$

where the minimum is extended over all prime powers $b<s$. Then

$$C_s = \min(C'_s, \min_{b \geqslant s} C(0, s, b))$$

since $T_b(s)=0$ for $b \geqslant s$. Therefore we can take

$$C_s = \min\left(C'_s, \frac{1}{s!}\left(1-\frac{1}{b_1(s)}\right)\left(\frac{b_1(s)}{2\log b_1(s)}\right)^s, \frac{1}{s!}\left(\frac{b_2(s)-1}{2\log b_2(s)}\right)^s\right)$$
$$\text{for} \quad s \geqslant 3. \tag{17}$$

This expresses $C_s$ as a minimum of finitely many numbers. These values of $C_s$ improve those obtained previously by the author [14].

We tabulate these values of $C_s$ for $1 \leqslant s \leqslant 20$. We note again that for $s \geqslant 2$ each value of $C_s$ is obtained by considering a $(T_b(s), s)$-sequence in a suitable base $b$. The appropriate value of $b$ is listed in Table I. All the values of $C_s$ in Table I have been rounded to three significant digits.

We note that for $s \geqslant 2$ the value of $C_s$ is not always obtained by considering a base $b \geqslant s$ as in the earlier constructions by Faure [2] and Niederreiter [14]. For instance, in the case $s=4$ one uses a $(1, 4)$-sequence in base 3 and in the case $s=14$ a $(1, 14)$-sequence in base 13. For $s \geqslant 3$ the minimum in (17) is not always attained by the term corresponding to an odd prime power $b$. For instance, in the case $s=32$ the minimum is attained for $b=b_1(s)=32$.

For the base $b=2$, Sobol' [19] has constructed $(t, s)$-sequences in base 2

TABLE I

| $s$ | $C_s$ | $b$ | $s$ | $C_s$ | $b$ |
|---|---|---|---|---|---|
| 1 | $(2.24)\times 10^{-1}$ | | 11 | $(8.12)\times 10^{-5}$ | 11 |
| 2 | $(2.60)\times 10^{-1}$ | 2 | 12 | $(5.60)\times 10^{-5}$ | 13 |
| 3 | $(1.26)\times 10^{-1}$ | 3 | 13 | $(1.01)\times 10^{-5}$ | 13 |
| 4 | $(8.58)\times 10^{-2}$ | 3 | 14 | $(2.19)\times 10^{-5}$ | 13 |
| 5 | $(2.47)\times 10^{-2}$ | 5 | 15 | $(4.42)\times 10^{-6}$ | 17 |
| 6 | $(1.86)\times 10^{-2}$ | 7 | 16 | $(7.80)\times 10^{-7}$ | 17 |
| 7 | $(4.11)\times 10^{-3}$ | 7 | 17 | $(1.30)\times 10^{-7}$ | 17 |
| 8 | $(2.99)\times 10^{-3}$ | 9 | 18 | $(8.47)\times 10^{-8}$ | 19 |
| 9 | $(6.05)\times 10^{-4}$ | 9 | 19 | $(1.36)\times 10^{-8}$ | 19 |
| 10 | $(4.28)\times 10^{-4}$ | 11 | 20 | $(3.28)\times 10^{-8}$ | 23 |

for any dimension $s$. Let $U(s)$ denote the least value of $t$ that can be achieved by the construction of Sobol' for given $s$. By Corollary 1 our construction yields a $(T_2(s), s)$-sequence in base 2 for any $s$. A comparison with the formula for $U(s)$ given in [19, Theorem 3.4] shows that $T_2(s) = U(s)$ for $1 \leqslant s \leqslant 7$ and $T_2(s) < U(s)$ for all $s \geqslant 8$. Also, the general upper bound for $T_2(s)$ obtained from Theorem 2 is better than the general upper bound for $U(s)$ given in Sobol' [20, Chap. 6, Theorem 6]. Therefore, for all dimensions $s \geqslant 8$ our construction yields dyadic sequences having a smaller discrepancy than the sequences of Sobol'.

The results in Sections 3 and 4 are relevant to a problem raised by the author [14, Sect. 8]. Following [14, Definition 8.7], we define for given $b \geqslant 2$ and $s \geqslant 1$ the number $t_b(s)$ as the least value of $t$ for which there exists a $(t, s)$-sequence in base $b$. The problem is to determine $t_b(s)$. If $b$ is a prime power, then by results of [14] we have $t_b(s) = 0$ for all $s \leqslant b$ and $t_b(s) \geqslant 1$ for all $s > b$. By Corollary 1 we get $t_b(s) \leqslant T_b(s)$ for all prime powers $b$ and all $s$. Since $T_b(b+1) = 1$, this shows in particular that $t_b(b+1) = 1$ for all prime powers $b$. For arbitrary $b \geqslant 2$ it follows from Theorem 4 that in the notation of this theorem,

$$t_b(s) \leqslant \max_{1 \leqslant v \leqslant h} T_{q_v}(s) \qquad \text{for all } s \geqslant 1. \tag{18}$$

If $q$ denotes the least prime power appearing in the canonical factorization of $b$ into a product of prime powers, then $t_b(s) = 0$ for all $s \leqslant q$, as was already noted in [14]. For $s > q$ it follows from (18) and Theorem 2 that

$$t_b(s) < s(\log_q s + \log_q \log_q s + 1).$$

The following principle goes back to Roth [17] (see also [14, Lemma 8.9]). If for $s \geqslant 2$ we have a sequence

$$\mathbf{x}'_n = (x_n^{(1)}, ..., x_n^{(s-1)}) \in I^{s-1} \qquad \text{for} \quad n = 1, 2, ...$$

whose discrepancy $\Delta'(N)$ satisfies

$$\Delta'(N) \leqslant C_{s-1}(\log N)^{s-1} + O((\log N)^{s-2}) \qquad \text{for all } N \geqslant 2,$$

then for any $N \geqslant 2$ the discrepancy $\Delta(N)$ of the $N$ points

$$\mathbf{x}_n = \left(\frac{n-1}{N}, x_n^{(1)}, ..., x_n^{(s-1)}\right) \in I^s \qquad \text{for} \quad 1 \leqslant n \leqslant N$$

satisfies the same bound. Therefore, for any $N \geqslant 2$ and $s \geqslant 2$ we can find $N$ points in $I^s$ whose discrepancy satisfies (1) with $B_s = C_{s-1}$. Admissible values of $C_{s-1}$ are obtained from (17) and Table I.

## 6. Implementation of the Sequences

The construction in Theorem 1 uses the elements $c_{jr}^{(i)}$ defined by (7), which are in turn obtained from the elements $a^{(i)}(j, k, r)$ defined by (6). Therefore, for the concrete implementation of our sequences one needs methods for calculating the elements $a^{(i)}(j, k, r)$.

In general, the calculation of the $a^{(i)}(j, k, r)$ is facilitated by the observation that if $i, j$, and $k$ are fixed and $a^{(i)}(j, k, r)$ is considered as a function of $r$, then these elements satisfy a linear recurrence relation with characteristic polynomial $p_i(x)^j$. The calculation of the $a^{(i)}(j, k, r)$ can be further simplified by a convenient choice of the polynomials $g_{ij}(x)$.

For instance, a suitable choice would be $g_{ij}(x) = 1$ for fixed $i$ and all $j \geqslant 1$. In this case the identity (6) attains the form

$$\frac{x^k}{p_i(x)^j} = \sum_{r=0}^{\infty} a^{(i)}(j, k, r)\, x^{-r-1}. \tag{19}$$

Now also fix $j$ and let first $k = 0$. Put $v_r = a^{(i)}(j, 0, r)$ for $r \geqslant 0$ and let

$$p_i(x)^j = x^m - b_{m-1}x^{m-1} - \cdots - b_0,$$

where we have assumed w.l.o.g. that $p_i(x)$ is monic. Then a comparison of coefficients in the identity

$$1 = (x^m - b_{m-1}x^{m-1} - \cdots - b_0)(v_0 x^{-1} + v_1 x^{-2} + \cdots)$$

shows that $v_0 = v_1 = \cdots = v_{m-2} = 0$, $v_{m-1} = 1$, and

$$v_{r+m} = b_{m-1}v_{r+m-1} + \cdots + b_0 v_r \qquad \text{for} \quad r = 0, 1, \ldots.$$

In other words, the sequence $v_0, v_1, \ldots$ is the impulse response sequence corresponding to the characteristic polynomial $p_i(x)^j$ (compare with [8, Chap. 8]). For arbitrary $k$ with $0 \leqslant k < e_i = \deg(p_i)$ it follows from (19) that

$$a^{(i)}(j, k, r) = v_{r+k} \qquad \text{for} \quad r = 0, 1, \ldots.$$

Another convenient choice for the polynomials $g_{ij}(x)$ is obtained as follows. For fixed $i$ let

$$p_i(x) = \prod_{h=1}^{e_i} (x - \beta_{ih})$$

be the factorization of $p_i(x)$ in its splitting field. For $j \geqslant 1$ choose

$$g_{ij}(x) = \sum_{h=1}^{e_i} \left( \frac{p_i(x)}{x - \beta_{ih}} \right)^j .$$

Then for $0 \leqslant k < e_i$ we have

$$\begin{aligned} \frac{x^k g_{ij}(x)}{p_i(x)^j} &= x^k \sum_{h=1}^{e_i} \frac{1}{(x-\beta_{ih})^j} = x^{k-j} \sum_{h=1}^{e_i} \frac{1}{(1-\beta_{ih} x^{-1})^j} \\ &= \sum_{h=1}^{e_i} \sum_{r=0}^{\infty} \binom{r+j-1}{j-1} \beta_{ih}^r x^{-r+k-j} \\ &= \sum_{r=j-k-1}^{\infty} \left( \sum_{h=1}^{e_i} \binom{r+k}{j-1} \beta_{ih}^{r+k-j+1} \right) x^{-r-1}. \end{aligned}$$

A comparison with (6) shows that

$$a^{(i)}(j, k, r) = \binom{r+k}{j-1} \sum_{h=1}^{e_i} \beta_{ih}^{r+k-j+1} \qquad \text{for} \quad r = 0, 1, ...,$$

where this expression is interpreted to be 0 if $r+k < j-1$. In the case of greatest interest, namely when $p_i(x)$ is irreducible over the finite field $F_b$, then the explicit formula above can be put in the form

$$a^{(i)}(j, k, r) = \binom{r+k}{j-1} \mathrm{Tr}_i(\gamma_i^{r+k-j+1}) \qquad \text{for} \quad r = 0, 1, ...,$$

where $\gamma_i$ is a fixed root of $p_i(x)$ and $\mathrm{Tr}_i$ denotes the trace over $F_b$ of the splitting field of $p_i(x)$.

For both of these choices for the polynomials $g_{ij}(x)$ it is seen immediately that the condition $\lim_{j \to \infty}(je_i - \deg(g_{ij})) = \infty$ in Theorem 1 is satisfied. Concrete irreducible polynomials $p_i(x)$ can be obtained from the extensive tables of irreducible polynomials over finite fields in [8, Chap. 10].

## 7. Low-Dispersion Sequences

The dispersion of point sets and sequences was introduced in Niederreiter [10] (see also [15]) in connection with quasi-Monte Carlo methods for global optimization. Let $d$ be the metric on $I^s$, $s \geqslant 1$, given by

$$d(\mathbf{y}, \mathbf{z}) = \max_{1 \leqslant i \leqslant s} |y_i - z_i|$$

for $\mathbf{y} = (y_1, ..., y_s) \in I^s$ and $\mathbf{z} = (z_1, ..., z_s) \in I^s$. The *dispersion* $d_N$ of the points $\mathbf{x}_1, ..., \mathbf{x}_N$ in $I^s$ is defined by

$$d_N = \sup_{\mathbf{x} \in I^s} \min_{1 \leqslant n \leqslant N} d(\mathbf{x}, \mathbf{x}_n).$$

For a sequence $\mathbf{x}_1, \mathbf{x}_2, ...$ of points in $I^s$ we define $d_N$ to be the dispersion of the first $N$ terms of the sequence. For any $N$ points in $I^s$ we have $d_N \geqslant \frac{1}{2} N^{-1/s}$ by [12, Theorem 1], and there exist sequences of points in $I^s$ with $d_N = O(N^{-1/s})$ by a construction in [11]. Further constructions of point sets and sequences of points in $I^s$ with $d_N = O(N^{-1/s})$ can be found in Niederreiter [12, 13], and for $s = 2$ in Lambert [6], Larcher [7], and Peart [16]. We show now that the dispersion of $(t, m, s)$-nets and $(t, s)$-sequences also satisfies $d_N = O(N^{-1/s})$, thus generalizing a result of Sobol' [21].

THEOREM 5. *The dispersion of a $(t, m, s)$-net in base $b$ satisfies*

$$d_N \leqslant b^{-\lfloor (m-t)/s \rfloor} \leqslant b^{(s-1+t)/s} N^{-1/s} \qquad \textit{for} \quad N = b^m.$$

*Proof.* Write $k = \lfloor (m-t)/s \rfloor$, so that $m - t = ks + r$ with $0 \leqslant r \leqslant s - 1$. Consider the partition of $I^s$ into elementary intervals in base $b$ of the form

$$\prod_{i=1}^{r} [a_i b^{-k-1}, (a_i + 1) b^{-k-1}) \times \prod_{i=r+1}^{s} [a_i b^{-k}, (a_i + 1) b^{-k})$$

with integers $0 \leqslant a_i < b^{k+1}$ for $1 \leqslant i \leqslant r$ and $0 \leqslant a_i < b^k$ for $r + 1 \leqslant i \leqslant s$. If $\mathbf{x} \in I^s$ is arbitrary, then $\mathbf{x}$ belongs to a unique interval $E$ of that partition. Since

$$V(E) = (b^{-k-1})^r (b^{-k})^{s-r} = b^{-ks-r} = b^{t-m},$$

it follows from Definition 2 that $E$ contains at least one point $\mathbf{x}_n$ of the given $(t, m, s)$-net in base $b$. Then $d(\mathbf{x}, \mathbf{x}_n) < b^{-k}$, thus

$$d_N \leqslant b^{-k} \leqslant b^{(s-1+t)/s} b^{-m/s} = b^{(s-1+t)/s} N^{-1/s}. \quad \blacksquare$$

THEOREM 6. *The dispersion of a $(t, s)$-sequence in base $b$ satisfies*

$$d_N < b^{(s+t)/s} N^{-1/s} \qquad \textit{for all } N \geqslant 1.$$

*Proof.* For $N < b^{s+t}$ we have

$$d_N \leqslant 1 < b^{(s+t)/s} N^{-1/s}.$$

For $N \geqslant b^{s+t}$ let $m$ be the largest integer with $b^m \leqslant N$, so that in particular $m > t$. By Definition 3, the first $b^m$ terms of the given $(t, s)$-sequence in base $b$ form a $(t, m, s)$-net in base $b$. Using Theorem 5 and $N < b^{m+1}$ we therefore get

$$d_N \leqslant d_{b^m} \leqslant b^{(s-1+t)/s} b^{-m/s} < b^{(s+t)/s} N^{-1/s}. \quad \blacksquare$$

The $(t, s)$-sequences in base $b$ constructed in Sections 3 and 4 are therefore also low-dispersion sequences. The dispersion of these sequences is, however, not as small as that of the best low-dispersion sequence known at present, namely the sequence constructed in Niederreiter [12, Theorem 2] which satisfies

$$\overline{\lim_{N \to \infty}} N^{1/s} d_N = \frac{1}{\log 4} = 0.721 \ldots.$$

## Appendix

TABLE II

Values of $T_2(s)$ for $1 \leqslant s \leqslant 30$

| $s$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_2(s)$ | 0 | 0 | 1 | 3 | 5 | 8 | 11 | 14 | 18 | 22 | 26 | 30 | 34 | 38 | 43 |
| $s$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| $T_2(s)$ | 48 | 53 | 58 | 63 | 68 | 73 | 78 | 83 | 89 | 95 | 101 | 107 | 113 | 119 | 125 |

TABLE III

Values of $T_3(s)$ for $1 \leqslant s \leqslant 30$

| $s$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_3(s)$ | 0 | 0 | 0 | 1 | 2 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 22 |
| $s$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| $T_3(s)$ | 25 | 28 | 31 | 34 | 37 | 40 | 43 | 46 | 49 | 52 | 55 | 58 | 61 | 64 | 67 |

TABLE IV

Values of $T_4(s)$ for $1 \leqslant s \leqslant 30$

| $s$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_4(s)$ | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 8 | 10 | 12 | 14 | 16 |
| $s$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| $T_4(s)$ | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 | 38 | 40 | 42 | 44 | 46 |

TABLE V

Values of $T_5(s)$ for $1 \leqslant s \leqslant 30$

| $s$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_5(s)$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $s$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| $T_5(s)$ | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 | 38 | 40 |

## References

1. H. Faure, Discrépances de suites associées à un système de numération (en dimension un), *Bull. Soc. Math. France* **109** (1981), 143–182.
2. H. Faure, Discrépance de suites associées à un système de numération (en dimension $s$), *Acta Arith.* **41** (1982), 337–351.
3. 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, *Numer. Math.* **2** (1960), 196.
4. L. K. Hua and Y. Wang, "Applications of Number Theory to Numerical Analysis," Springer, Berlin, 1981.
5. L. Kuipers and H. Niederreiter, "Uniform Distribution of Sequences," Wiley, New York, 1974.
6. J. P. Lambert, A sequence well dispersed in the unit square, preprint, University of Alaska, Fairbanks, 1986.
7. G. Larcher, The dispersion of a special sequence, *Arch. Math.* **47** (1986), 347–352.
8. R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, Reading, MA, 1983.
9. H. Niederreiter, Quasi-Monte Carlo methods and pseudo-random numbers, *Bull. Amer. Math. Soc.* **84** (1978), 957–1041.
10. H. Niederreiter, A quasi-Monte Carlo method for the approximate computation of the extreme values of a function, *in* "Studies in Pure Mathematics (To the Memory of Paul Turán)," pp. 523–529, Birkhäuser, Basel, 1983.

11. H. Niederreiter, On a measure of denseness for sequences, *in* "Topics in Classical Number Theory (Budapest, 1981)," Colloquia Math. Soc. János Bolyai, Vol. 34, pp. 1163–1208, North-Holland, Amsterdam, 1984.
12. H. Niederreiter, Quasi-Monte Carlo methods for global optimization, *in* "Proc. Fourth Pannonian Symp. on Math. Statistics (Bad Tatzmannsdorf, 1983)," pp. 251–267, Reidel, Dordrecht, 1986.
13. H. Niederreiter, Good lattice points for quasirandom search methods, *in* "System Modelling and Optimization" (A. Prékopa, J. Szelezsán, and B. Strazicky, Eds.), Lecture Notes in Control and Information Sciences, Vol. 84, pp. 647–654, Springer, Berlin, 1986.
14. H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* **104** (1987), 273–337.
15. H. Niederreiter and K. McCurley, Optimization of functions by quasi-random search methods, *Computing* **22** (1979), 119–123.
16. P. Peart, The dispersion of the Hammersley sequence in the unit square, *Monatsh. Math.* **94** (1982), 249–261.
17. K. F. Roth, On irregularities of distribution, *Mathematika* **1** (1954), 73–79.
18. W. M. Schmidt, Irregularities of distribution. VII, *Acta Arith.* **21** (1972), 45–50.
19. I. M. Sobol', The distribution of points in a cube and the approximate evaluation of integrals, *Zh. Vychisl. Mat. i Mat. Fiz.* **7** (1967), 784–802. [Russian]
20. I. M. Sobol', "Multidimensional Quadrature Formulas and Haar Functions," Nauka, Moscow, 1969. [Russian]
21. I. M. Sobol', On an estimate of the accuracy of a simple multidimensional search, *Dokl. Akad. Nauk SSSR* **266** (1982), 569-572. [Russian]