ACTA ARITHMETICA
LXXIII.1 (1995)

A construction of low-discrepancy sequences using global function fields

by

Chaoping Xing (Hefei) and Harald Niederreiter (Wien)

1. Introduction. The idea of using global function fields for the construction of s-dimensional low-discrepancy sequences was first sketched by Niederreiter [9, Section 5], [10, Section 5], and the details were worked out in an improved form by Niederreiter and Xing [11]. In the method of [11] one chooses a suitable global function field which contains s elements satisfying special properties. This global function field can, for instance, be a rational function field, in which case one obtains an earlier construction of low-discrepancy sequences due to Niederreiter [7]. If one chooses certain elliptic function fields, then it was shown in [11] that one gets improvements on the construction in [7].

Important progress in the construction of low-discrepancy sequences was achieved in the paper [12] of the authors. The key idea of the construction in [12] is to work with global function fields containing many rational places, i.e., places of degree 1. This method yields significantly better results than all previous methods. The only essential condition in this construction is that the global function field contains at least $s + 1$ rational places.

In the present paper we describe a different construction which is also based on global function fields, but which is somewhat more explicit than the construction in [12]. This new construction is also more flexible than that in [12], since we can now use not only rational places, but also places of larger degree. Just like the method in [12], the present construction produces low-discrepancy sequences that are in a sense asymptotically optimal. The new construction produces the best results if places of small degree are used. In the case where we work only with rational places, we get the same results as in [12], but by a different method. Some examples in Section 4 demonstrate that in certain cases the new construction yields improvements on the results in [12] if we use also places of degree greater than 1.

The research of the first author was supported by the Chinese Natural Science Foundation.

Like all the constructions mentioned above, our method is based on the general theory of (t,s)-sequences. The standard procedure is to use the so-called digital method to obtain (t,s)-sequences, usually in a prime-power base q. In Section 2 we review the digital method for constructing (t,s)-sequences by means of the finite field $\mathbb{F}_q$ of order q. Our new construction of digital (t,s)-sequences using global function fields over $\mathbb{F}_q$ is described in detail in Section 3. Some consequences of the construction are drawn in Section 4. In particular, it is shown that we can obtain digital (t,s)-sequences for which the values of t are asymptotically optimal.

2. The digital method for the construction of sequences. With regard to low-discrepancy point sets and sequences we follow the notation and terminology in the book of Niederreiter [8]. For $s \ge 1$ let $I^s = [0,1)^s$ be the half-open s-dimensional unit cube. The following standard concept is fundamental.

Definition 1. For integers $b \ge 2$ and $0 \le t \le m$, a (t,m,s)*-net in base* b is a point set consisting of b^m points in I^s such that every subinterval J of I^s of the form

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

with integers $d_i \ge 0$ and $0 \le a_i < b^{d_i}$ for $1 \le i \le s$ and of volume b^{t-m} contains exactly b^t points of the point set.

Given a base $b \ge 2$, we write $Z_b = \{0,1,\ldots,b-1\}$ for the least residue system mod b. For a real number $x \in [0,1]$ let

$$x = \sum_{j=1}^{\infty} y_j b^{-j} \quad \text{with all } y_j \in Z_b$$

be a b-adic expansion of x, where the case $y_j = b-1$ for almost all j is allowed. For an integer $m \ge 1$ we define the truncation

$$[x]_{b,m} = \sum_{j=1}^{m} y_j b^{-j}.$$

It should be emphasized that this truncation operates on the *expansion* of x and not on x itself, since it may yield different results depending on which b-adic expansion of x is used. If $\bar{I}^s = [0,1]^s$ is the closed s-dimensional unit cube and $\mathbf{x} = (x^{(1)},\ldots,x^{(s)}) \in \bar{I}^s$, where the $x^{(i)}$, $1 \le i \le s$, are given by prescribed b-adic expansions, then we define

$$[\mathbf{x}]_{b,m} = ([x^{(1)}]_{b,m},\ldots,[x^{(s)}]_{b,m}).$$

Note that we always have $[\mathbf{x}]_{b,m} \in I^s$. For the following slight generalization of a definition in [6, Section 2] see Niederreiter and Xing [12] and Tezuka [16].

Definition 2. For integers $b \geq 2$ and $t \geq 0$, a sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $\bar{I}^s$ with prescribed b-adic expansions of all coordinates is called a *(t,s)-sequence in base b* if for all integers $k \geq 0$ and $m > t$ the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a (t,m,s)-net in base b.

It is clear from Definition 2 that smaller values of t mean stronger uniformity properties of the sequence. The number t is sometimes called the "quality parameter".

Now we describe the *digital method* for the construction of sequences, where we follow the presentation in [12]. This method can be applied with any base b, but for the purposes of the present paper it suffices to consider a prime-power base q. Let $\mathbb{F}_q$ again be the finite field of order q and let $s \geq 1$ be a given dimension. Then we choose the following:

(S1) bijections $\psi_r : Z_q \to \mathbb{F}_q$ for $r \geq 0$, with $\psi_r(0) = 0$ for all sufficiently large r;

(S2) bijections $\eta_j^{(i)} : \mathbb{F}_q \to Z_q$ for $1 \leq i \leq s$ and $j \geq 1$;

(S3) elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ for $1 \leq i \leq s, j \geq 1$, and $r \geq 0$.

For $n = 0, 1, \ldots$ let

$$n = \sum_{r=0}^{\infty} a_r(n) q^r$$

be the digit expansion of n in base q, where $a_r(n) \in Z_q$ for $r \geq 0$ and $a_r(n) = 0$ for all sufficiently large r. We put

$$x_n^{(i)} = \sum_{j=1}^{\infty} y_{n,j}^{(i)} q^{-j} \quad \text{for } n \geq 0 \text{ and } 1 \leq i \leq s, \tag{1}$$

with

$$y_{n,j}^{(i)} = \eta_j^{(i)} \Big(\sum_{r=0}^{\infty} c_{j,r}^{(i)} \psi_r(a_r(n)) \Big) \in Z_q \quad \text{for } n \geq 0,\ 1 \leq i \leq s,\ \text{and } j \geq 1.$$

Note that the sum over r is always a finite sum. Now we define the sequence

$$\mathbf{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in \bar{I}^s \quad \text{for } n = 0, 1, \ldots \tag{2}$$

Definition 3. If the sequence in (2) is a (t,s)-sequence in base q for some integer $t \geq 0$, then this sequence is called a *digital (t,s)-sequence constructed over* $\mathbb{F}_q$. Here the truncations are required to operate on the expansions in (1).

The quality parameter t can be determined from the elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ in (S3) in the following way. If $\mathbb{F}_q^{\infty}$ is the sequence space over $\mathbb{F}_q$, then we use the $c_{j,r}^{(i)}$ to set up the sequences

$$\mathbf{c}_j^{(i)} = (c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots) \in \mathbb{F}_q^\infty \quad \text{for } 1 \le i \le s \text{ and } j \ge 1,$$

and we consider the two-parameter system

$$C^{(\infty)} = \{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^\infty : 1 \le i \le s \text{ and } j \ge 1\}.$$

For $m \ge 1$ we define the projection

$$\pi_m : (c_0, c_1, \ldots) \in \mathbb{F}_q^\infty \mapsto (c_0, \ldots, c_{m-1}) \in \mathbb{F}_q^m,$$

and we put

$$C^{(m)} = \{\pi_m(\mathbf{c}_j^{(i)}) \in \mathbb{F}_q^m : 1 \le i \le s, 1 \le j \le m\}.$$

As in [8, Definition 4.27], for fixed m we let $\varrho(C^{(m)})$ be the largest integer d such that any system $\{\pi_m(\mathbf{c}_j^{(i)}) : 1 \le j \le d_i, 1 \le i \le s\}$ with $0 \le d_i \le m$ for $1 \le i \le s$ and $\sum_{i=1}^s d_i = d$ is linearly independent over $\mathbb{F}_q$ (here the empty system is viewed as linearly independent). Finally, we set

$$\tau(C^{(\infty)}) = \sup_{m \ge 1} (m - \varrho(C^{(m)})).$$

We are interested only in the case where $\tau(C^{(\infty)}) < \infty$. The proofs of Theorems 4.35 and 4.36 in [8] yield the following result.

Lemma 1. *If the elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ in* (S3) *are such that $\tau(C^{(\infty)}) < \infty$, then the sequence in* (2) *is a digital (t,s)-sequence constructed over $\mathbb{F}_q$ with $t = \tau(C^{(\infty)})$.*

Most known constructions of (t,s)-sequences employ the digital method over a finite field. Important previous constructions using the digital method are those of Sobol' [14], Faure [1], Niederreiter [6], [7], and Niederreiter and Xing [11], [12]. A recent survey of (t,m,s)-net and (t,s)-sequence constructions is given in [5]. A generalization of the concept of a (t,s)-sequence was recently introduced by Larcher and Niederreiter [3].

Any (t,s)-sequence S in an arbitrary base $b \ge 2$ is a low-discrepancy sequence, in the sense that the star discrepancy $D_N^*(S)$ of the first N terms of S satisfies $D_N^*(S) = O(N^{-1}(\log N)^s)$. More precisely, by [8, Theorem 4.17] (see also [12] for the slightly more general case in Definition 2) we have

$$D_N^*(S) \le C_b(s,t) N^{-1} (\log N)^s + O(N^{-1}(\log N)^{s-1}) \quad \text{for all } N \ge 2, \tag{3}$$

where the implied constant in the Landau symbol depends only on b, s, and t. Here

$$C_b(s,t) = \frac{b^t}{s}\left(\frac{b-1}{2\log b}\right)^s$$

if either $s = 2$ or $b = 2$, $s = 3, 4$; otherwise

$$C_b(s,t) = \frac{b^t}{s!} \cdot \frac{b-1}{2\lfloor b/2 \rfloor} \left(\frac{\lfloor b/2 \rfloor}{\log b} \right)^s .$$

It is again clear from the discrepancy bound (3) that small values of t are preferable if one wants to obtain good low-discrepancy sequences. Thus, the aim in the construction of (t,s)-sequences in base b is to make the value of the quality parameter t as small as possible for given b and s.

3. The new construction of sequences. We now describe our new method of obtaining digital (t,s)-sequences constructed over the finite field $\mathbb{F}_q$ by means of global function fields over $\mathbb{F}_q$. The notation $K/\mathbb{F}_q$ for a global function field signifies that $\mathbb{F}_q$ is the full constant field of the algebraic function field K. The genus of $K/\mathbb{F}_q$ is denoted by $g(K/\mathbb{F}_q)$. We write ν_P for the normalized discrete valuation corresponding to the place P of $K/\mathbb{F}_q$. For an arbitrary divisor D of $K/\mathbb{F}_q$, the $\mathbb{F}_q$-vector space

$$\mathcal{L}(D) = \{k \in K \backslash \{0\} : (k) + D \geq 0\} \cup \{0\}$$

has a finite dimension which we denote by $l(D)$. Here (k) is the principal divisor of k.

Now let $s \geq 1$ be a given dimension. Let $K/\mathbb{F}_q$ be a global function field containing at least one rational place P_∞, and let D be a positive divisor of $K/\mathbb{F}_q$ with $\deg(D) = 2g(K/\mathbb{F}_q)$ and $P_\infty \notin \operatorname{supp}(D)$. We choose s distinct places $P_1, \ldots, P_s$ of $K/\mathbb{F}_q$ with $P_i \neq P_\infty$ for $1 \leq i \leq s$, and we put $e_i = \deg(P_i)$ for $1 \leq i \leq s$. With the abbreviation $g = g(K/\mathbb{F}_q)$ we have $l(D) = g + 1$ by the Riemann–Roch theorem. We choose a basis of $\mathcal{L}(D)$ in the following way. Note that $l(D - P_\infty) = g$ by the Riemann–Roch theorem and $l(D - (2g+1)P_\infty) = 0$, hence there exist integers $0 = n_0 < n_1 < \ldots < n_g \leq 2g$ such that

$$l(D - n_f P_\infty) = l(D - (n_f + 1)P_\infty) + 1 \quad \text{for } 0 \leq f \leq g.$$

Choose $w_f \in \mathcal{L}(D - n_f P_\infty) \backslash \mathcal{L}(D - (n_f + 1)P_\infty)$, then

$$\nu_{P_\infty}(w_f) = n_f \quad \text{for } 0 \leq f \leq g, \tag{4}$$

and it is easily seen that $\{w_0, w_1, \ldots, w_g\}$ is a basis of $\mathcal{L}(D)$.

For each $1 \leq i \leq s$ we consider the chain

$$\mathcal{L}(D) \subset \mathcal{L}(D + P_i) \subset \mathcal{L}(D + 2P_i) \subset \ldots$$

of $\mathbb{F}_q$-vector spaces. By starting from the basis $\{w_0, w_1, \ldots, w_g\}$ of $\mathcal{L}(D)$ and successively adding basis vectors at each step of the chain, we obtain for each $n \geq 1$ a basis

$$\{w_0, w_1, \ldots, w_g, k_1^{(i)}, k_2^{(i)}, \ldots, k_{ne_i}^{(i)}\}$$

of $\mathcal{L}(D+nP_i)$. We note that we then have

$$k_j^{(i)} \in \mathcal{L}\Big(D + \Big(\Big\lfloor \frac{j-1}{e_i} \Big\rfloor + 1\Big)P_i\Big) \quad \text{for } 1 \le i \le s \text{ and } j \ge 1. \tag{5}$$

Lemma 2. *The system* $\{w_0, w_1, \ldots, w_g\} \cup \{k_j^{(i)}\}_{1\le i\le s, j\ge 1}$ *of elements of* K *is linearly independent over* $\mathbb{F}_q$.

Proof. Suppose that

$$\sum_{f=0}^{g} a_f w_f + \sum_{i=1}^{s}\sum_{j=1}^{N} b_j^{(i)} k_j^{(i)} = 0$$

for some $N \ge 1$ and $a_f, b_j^{(i)} \in \mathbb{F}_q$. For a fixed $1 \le h \le s$ we write

$$\sum_{j=1}^{N} b_j^{(h)} k_j^{(h)} = -\sum_{f=0}^{g} a_f w_f - \sum_{\substack{i=1\\ i\ne h}}^{s} b_j^{(i)} k_j^{(i)}. \tag{6}$$

Abbreviate the left-hand side of (6) by k. If $k \ne 0$, then by the construction of the $k_j^{(h)}$ we have $k \notin \mathcal{L}(D)$, and so

$$\nu_{P_h}(k) \le -\nu_{P_h}(D) - 1$$

in view of (5). On the other hand, by using the expression for k on the right-hand side of (6) we get

$$\nu_{P_h}(k) \ge -\nu_{P_h}(D),$$

thus we must have $k = 0$. It follows that all $b_j^{(h)} = 0$, and since h was arbitrary, we get $b_j^{(i)} = 0$ for $1 \le i \le s$ and $1 \le j \le N$, and so also $a_f = 0$ for $0 \le f \le g$. ∎

Let z be a local uniformizing parameter at P_∞ and let the integers $0 = n_0 < n_1 < \ldots < n_g \le 2g$ be as in (4). For $r = 0, 1, \ldots$ we put

$$z_r = \begin{cases} z^r & \text{if } r \notin \{n_0, n_1, \ldots, n_g\}, \\ w_f & \text{if } r = n_f \text{ for some } f \in \{0, 1, \ldots, g\}. \end{cases}$$

Note that then $\nu_{P_\infty}(z_r) = r$ for all $r \ge 0$. For $1 \le i \le s$ and $j \ge 1$ we have $k_j^{(i)} \in \mathcal{L}(D + nP_i)$ for some $n \ge 1$ and also $P_\infty \notin \operatorname{supp}(D + nP_i)$, hence $\nu_{P_\infty}(k_j^{(i)}) \ge 0$. Thus we have the expansions

$$k_j^{(i)} = \sum_{r=0}^{\infty} a_{j,r}^{(i)} z_r \quad \text{for } 1 \le i \le s \text{ and } j \ge 1, \tag{7}$$

where all coefficients $a_{j,r}^{(i)} \in \mathbb{F}_q$. For $1 \le i \le s$ and $j \ge 1$ we now define the sequences

$$\mathbf{c}_j^{(i)} = (\widehat{a_{j,n_0}^{(i)}}, a_{j,1}^{(i)}, \ldots, \widehat{a_{j,n_1}^{(i)}}, a_{j,n_1+1}^{(i)}, \ldots, \widehat{a_{j,n_g}^{(i)}}, a_{j,n_g+1}^{(i)}, \ldots) \in \mathbb{F}_q^\infty, \tag{8}$$

where the hat indicates that the corresponding term is deleted. If we then write

$$\mathbf{c}_j^{(i)} = (c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots),$$

then the terms $c_{j,r}^{(i)} \in \mathbb{F}_q$ serve as the elements in (S3) in the digital method for the construction of (t,s)-sequences described in Section 2. The bijections ψ_r and $\eta_j^{(i)}$ are chosen as in (S1) and (S2), respectively. Then the digital method yields the sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $\bar{I}^s$ as in (2), and this completes the description of our new construction of sequences.

To obtain the quality parameter for this sequence, we proceed as in Section 2, i.e., we use the $\mathbf{c}_j^{(i)}$ from (8) to set up the two-parameter system

$$C^{(\infty)} = \{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^\infty : 1 \le i \le s \text{ and } j \ge 1\}. \tag{9}$$

THEOREM 1. *Given a prime power q and a dimension $s \ge 1$, let $K/\mathbb{F}_q$ be a global function field of genus $g = g(K/\mathbb{F}_q)$ which contains at least one rational place P_∞, and let D be a positive divisor of $K/\mathbb{F}_q$ with* $\deg(D) = 2g$ *and $P_\infty \notin$* supp(D). *Let $P_1, \ldots, P_s$ be s distinct places of $K/\mathbb{F}_q$ with $P_i \ne P_\infty$ for $1 \le i \le s$. Then the system $C^{(\infty)}$ in* (9) *satisfies*

$$\tau(C^{(\infty)}) \le g + \sum_{i=1}^{s} (e_i - 1),$$

where $e_i = \deg(P_i)$ for $1 \le i \le s$.

Proof. It suffices to verify the following property: for any integer $m > g + \sum_{i=1}^s (e_i - 1)$ and any integers $d_1, \ldots, d_s \ge 0$ with $1 \le \sum_{i=1}^s d_i \le m - g - \sum_{i=1}^s (e_i - 1)$, the vectors

$$\pi_m(\mathbf{c}_j^{(i)}) = (c_{j,0}^{(i)}, \ldots, c_{j,m-1}^{(i)}) \in \mathbb{F}_q^m \quad \text{for } 1 \le j \le d_i,\ 1 \le i \le s,$$

are linearly independent over $\mathbb{F}_q$. Let H be the set of i with $1 \le i \le s$ for which $d_i \ge 1$, and suppose that we have

$$\sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} \pi_m(\mathbf{c}_j^{(i)}) = \mathbf{0} \in \mathbb{F}_q^m \tag{10}$$

for some $b_j^{(i)} \in \mathbb{F}_q$. Now we consider the element $k \in K$ given by

$$k = \sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} k_j^{(i)} - \sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} \sum_{f=0}^{g} a_{j,n_f}^{(i)} w_f. \tag{11}$$

We put $R = \{n_0, n_1, \ldots, n_g\}$ and use (7) to obtain

$$k = \sum_{i\in H}\sum_{j=1}^{d_i} b_j^{(i)}\Big(\sum_{r=0}^{\infty} a_{j,r}^{(i)} z_r - \sum_{f=0}^{g} a_{j,n_f}^{(i)} z_{n_f}\Big) = \sum_{\substack{r=0\\ r\notin R}}^{\infty}\Big(\sum_{i\in H}\sum_{j=1}^{d_i} b_j^{(i)} a_{j,r}^{(i)}\Big) z_r.$$

From (8) and (10) we get

$$\sum_{i\in H}\sum_{j=1}^{d_i} b_j^{(i)} a_{j,r}^{(i)} = 0$$

for the first m nonnegative integers r that are not in R. If we use also $m > g$ and $n_g \le 2g$, then we arrive at

$$\nu_{P_\infty}(k) \ge m + g + 1.$$

Furthermore, (5) and (11) yield

$$k \in \mathcal{L}\Big(D + \sum_{i\in H}\Big(\Big\lfloor\frac{d_i - 1}{e_i}\Big\rfloor + 1\Big)P_i\Big).$$

If we had $k \neq 0$, then by looking at the poles of k we would obtain

$$\deg\Big(D + \sum_{i\in H}\Big(\Big\lfloor\frac{d_i - 1}{e_i}\Big\rfloor + 1\Big)P_i\Big) \ge m + g + 1,$$

and so

$$\sum_{i=1}^{s} d_i \ge m - g - \sum_{i\in H}(e_i - 1) + 1 \ge m - g - \sum_{i=1}^{s}(e_i - 1) + 1,$$

a contradiction. Thus $k = 0$, and by appealing to (11) and Lemma 2 we conclude that all $b_j^{(i)} = 0$. ■

THEOREM 2. *Given a prime power q and a dimension $s \ge 1$, let $K/\mathbb{F}_q$ be a global function field of genus g and $P_1, \ldots, P_s$ be places of $K/\mathbb{F}_q$ satisfying the conditions in Theorem 1. Then there exists a digital (t, s)-sequence constructed over $\mathbb{F}_q$ with*

$$t = g + \sum_{i=1}^{s}(e_i - 1),$$

where $e_i = \deg(P_i)$ for $1 \le i \le s$.

Proof. This follows from Lemma 1 and Theorem 1. Note also that any (t, s)-sequence in an arbitrary base b is a (u, s)-sequence in base b for every integer $u \ge t$ (compare with [8, Remark 4.3]). ■

4. Some consequences of the construction. In the following let $N(K/\mathbb{F}_q)$ denote the number of rational places of a global function field

$K/\mathbb{F}_q$. As in [12], for any prime power q and any dimension $s \geq 1$ we define

$$V_q(s) = \min g(K/\mathbb{F}_q),$$

where the minimum is extended over all global function fields $K/\mathbb{F}_q$ with $N(K/\mathbb{F}_q) \geq s+1$ (by [13, Théorème 4] such global function fields always exist). Now choose $K/\mathbb{F}_q$ such that $g(K/\mathbb{F}_q) = V_q(s)$ and $N(K/\mathbb{F}_q) \geq s+1$, and let $P_\infty, P_1, \ldots, P_s$ be $s+1$ distinct rational places of $K/\mathbb{F}_q$. Then we can apply the construction in Section 3 with $D = 2g(K/\mathbb{F}_q)P_1$, for instance, and this yields a digital $(V_q(s), s)$-sequence constructed over $\mathbb{F}_q$ according to Theorem 2. Let us point out that the somewhat less explicit method in [12] yields also a digital $(V_q(s), s)$-sequence constructed over $\mathbb{F}_q$ for every prime power q and every $s \geq 1$. By means of deep results from the class field theory of global function fields it was shown in [12] that $V_q(s) = O(s)$ with an absolute implied constant.

For any prime power q and any dimension $s \geq 1$, let $d_q(s)$ be the least value of t such that there exists a digital (t, s)-sequence constructed over $\mathbb{F}_q$. It is clear from the above that $d_q(s) \leq V_q(s)$, so that in particular $d_q(s) = O(s)$ with an absolute implied constant. It should be pointed out, though, that in most cases class field theory does not describe the required global function fields explicitly. The following result shows $d_q(s) = O(s)$ via explicitly given global function fields. The construction in the proof of Theorem 3 does not work with the method in [12] since the former makes use of places of degree 2, whereas the construction in [12] allows only rational places.

THEOREM 3. *For every prime power q and every dimension $s \geq 1$ we have*

$$d_q(s) \leq \frac{3q-1}{q-1}(s-1) - \frac{(2q+4)(s-1)^{1/2}}{(q^2-1)^{1/2}} + 2.$$

Proof. Consider the tower $K_1 \subseteq K_2 \subseteq \ldots$ of global function fields over $\mathbb{F}_q$, where $K_1 = \mathbb{F}_q(x_1)$ is a rational function field and $K_{n+1} = K_n(z_{n+1})$ for $n = 1, 2, \ldots$ with

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \quad \text{and} \quad x_{n+1} = \frac{z_{n+1}}{x_n}.$$

If for each $n \geq 1$ we let $E_n = K_n\mathbb{F}_{q^2}$ be a constant field extension of K_n, then we obtain the tower $E_1 \subseteq E_2 \subseteq \ldots$ of global function fields over $\mathbb{F}_{q^2}$ constructed by Garcia and Stichtenoth [2]. It follows from the invariance of the genus under constant field extensions [15, Theorem III.6.3] and from the genus bound in [2] that

$$g(K_n/\mathbb{F}_q) = g(E_n/\mathbb{F}_{q^2}) \leq q^n + q^{n-1} - q^{(n+1)/2} - 2q^{(n-1)/2} + 1 \quad \text{for all } n \geq 1.$$

By another result from [2] we have

$$N(E_n/\mathbb{F}_{q^2}) \ge (q^2-1)q^{n-1}+1 \quad \text{for all } n \ge 1.$$

Let Q_1 be the pole of x_1 in $K_1/\mathbb{F}_q$. We will prove by induction on n that Q_1 is totally ramified in K_n/K_1 and that its unique extension Q_n to $K_n/\mathbb{F}_q$ satisfies $\nu_{Q_n}(x_n) = -1$. This being trivial for $n=1$, we assume that it has been shown for some $n \ge 1$. If Q_{n+1} is a place of $K_{n+1}/\mathbb{F}_q$ lying over Q_n, then with $e(Q_{n+1}|Q_n)$ denoting the ramification index we get

$$\nu_{Q_{n+1}}(x_n^{q+1}) = e(Q_{n+1}|Q_n)\nu_{Q_n}(x_n^{q+1}) = -(q+1)e(Q_{n+1}|Q_n),$$

but also

$$\nu_{Q_{n+1}}(x_n^{q+1}) = \nu_{Q_{n+1}}(z_{n+1}^q + z_{n+1}) = q\nu_{Q_{n+1}}(z_{n+1}).$$

Thus, q divides $e(Q_{n+1}|Q_n)$. On the other hand, $e(Q_{n+1}|Q_n) \le [K_{n+1} : K_n] \le q$, hence $e(Q_{n+1}|Q_n) = [K_{n+1} : K_n] = q$, and so Q_1 is totally ramified in K_{n+1}/K_1. Moreover, $\nu_{Q_{n+1}}(z_{n+1}) = -q-1$, thus

$$\nu_{Q_{n+1}}(x_{n+1}) = \nu_{Q_{n+1}}\left(\frac{z_{n+1}}{x_n}\right) = -q-1-q\nu_{Q_n}(x_n) = -1,$$

and the induction is complete. Note that we have shown in particular that $N(K_n/\mathbb{F}_q) \ge 1$ for all $n \ge 1$.

Since E_n/K_n is an unramified extension of degree 2, we have

$$N(K_n/\mathbb{F}_q) + 2N_2(K_n/\mathbb{F}_q) = N(E_n/\mathbb{F}_{q^2}) \ge (q^2-1)q^{n-1}+1 \quad \text{for all } n \ge 1,$$

where $N_2(K_n/\mathbb{F}_q)$ denotes the number of places of $K_n/\mathbb{F}_q$ of degree 2. Together with $N(K_n/\mathbb{F}_q) \ge 1$ this yields

$$N(K_n/\mathbb{F}_q) + N_2(K_n/\mathbb{F}_q) \ge \tfrac{1}{2}(q^2-1)q^{n-1}+1 \quad \text{for all } n \ge 1. \tag{12}$$

Now we are ready to prove the bound for $d_q(s)$ in the theorem. For all s we will get this bound by applying the construction in Section 3 with a suitable global function field $K_n/\mathbb{F}_q$ from the tower described above. First let $1 \le s \le q$. Then an obvious application of Theorem 2 to $K_1/\mathbb{F}_q$ yields $d_q(s) = 0$, and the bound holds. Next let $q+1 \le s \le \frac{1}{2}(q^2-1)$. Since $N(K_1/\mathbb{F}_q) = q+1$ and $N_2(K_1/\mathbb{F}_q) = \frac{1}{2}(q^2-q)$, it follows from Theorem 2, applied to $K_1/\mathbb{F}_q$ with q places of degree 1 (the remaining rational place serving as P_∞) and $s-q$ places of degree 2, that

$$d_q(s) \le s-q \le \frac{3q-1}{q-1}(s-1) - \frac{(2q+4)(s-1)^{1/2}}{(q^2-1)^{1/2}} + 2.$$

Finally, let $s \ge \frac{1}{2}(q^2-1)+1$. Then there exists some $n \ge 1$ such that

$$\tfrac{1}{2}(q^2-1)q^{n-1}+1 \le s \le \tfrac{1}{2}(q^2-1)q^n.$$

Recall that we have $N(K_{n+1}/\mathbb{F}_q) \ge 1$ and (12), so that $K_{n+1}/\mathbb{F}_q$ has at least one rational place which can serve as P_∞ and s additional places of degree ≤ 2. Thus, Theorem 2 yields

$$\begin{aligned} d_q(s) &\leq g(K_{n+1}/\mathbb{F}_q) + s \leq q^{n+1} + q^n - q^{(n+2)/2} - 2q^{n/2} + 1 + s \\ &\leq \frac{2q}{q-1}(s-1) - (q+2)\left(\frac{2q(s-1)}{q^2-1}\right)^{1/2} + 1 + s \\ &\leq \frac{3q-1}{q-1}(s-1) - \frac{(2q+4)(s-1)^{1/2}}{(q^2-1)^{1/2}} + 2. \ \blacksquare \end{aligned}$$

Remark 1. From Theorem 3 we get for all $s \geq 1$ the bounds

$$\begin{aligned} d_2(s) &\leq 5s - \frac{8}{\sqrt{3}}(s-1)^{1/2} - 3, \\ d_3(s) &\leq 4s - \frac{5}{\sqrt{2}}(s-1)^{1/2} - 2, \\ d_5(s) &\leq \frac{7}{2}s - \frac{7}{\sqrt{6}}(s-1)^{1/2} - \frac{3}{2}, \end{aligned}$$

which are better than the bounds $d_2(s) \leq 9s+1, d_3(s) \leq 6s+1$, and $d_5(s) \leq 4s+1$ obtained from the results in [12].

Corollary 1. *For every prime power q we have*

$$L_q := \liminf_{s\to\infty} \frac{d_q(s)}{s} \leq \frac{q+1}{q-1}.$$

Proof. We proceed as in the proof of Theorem 3, and with the notation there we put

$$s_n = N(K_n/\mathbb{F}_q) + N_2(K_n/\mathbb{F}_q) - 1 \quad \text{for all } n \geq 1.$$

Then by Theorem 2 and results from the proof of Theorem 3 we obtain

$$\frac{d_q(s_n)}{s_n} \leq \frac{g(K_n/\mathbb{F}_q) + s_n}{s_n} \leq 1 + \frac{q^n + q^{n-1} - q^{(n+1)/2} - 2q^{(n-1)/2} + 1}{\frac{1}{2}(q^2-1)q^{n-1}}$$

for all $n \geq 1$, and so the desired bound for L_q follows. $\blacksquare$

Remark 2. Corollary 1 yields the bounds $L_2 \leq 3$, $L_3 \leq 2$, and $L_5 \leq 3/2$, which improves on the bounds $L_2 \leq 9/2$, $L_3 \leq 3$, and $L_5 \leq 2$ obtained from the results in [12].

Example 1. Let $K = \mathbb{F}_3(x,y)$ be the Artin–Schreier extension of the rational function field $\mathbb{F}_3(x)$ with

$$y^3 - y = \frac{x^3 - x}{(x^2+x-1)^2}.$$

Then we have $g(K/\mathbb{F}_3) = 4$ and $N(K/\mathbb{F}_3) = 12$; the rational places of $K/\mathbb{F}_3$ are obtained from the four rational places of $\mathbb{F}_3(x)$ which split completely in the extension $K/\mathbb{F}_3(x)$. Furthermore, the zero of x^2+x-1 is totally ramified in the extension $K/\mathbb{F}_3(x)$ by [15, Proposition III.7.8], hence $K/\mathbb{F}_3$ has at least one place of degree 2. Let $P_\infty, P_1, \ldots, P_{11}$ be the 12 rational places of $K/\mathbb{F}_3$ and let P_{12} be a place of $K/\mathbb{F}_3$ of degree 2. Then by Theorem 2 we get $d_3(12) \le g(K/\mathbb{F}_3) + 1 = 5$. This improves on the corresponding bound in [12].

Example 2. Let $K = \mathbb{F}_3(x, y_1, y_2)$ be the extension of the rational function field $\mathbb{F}_3(x)$ with

$$y_1^3 - y_1 = x(x-1), \qquad y_2^3 - y_2 = \frac{x(x-1)}{x+1}.$$

Note that K can be obtained from $\mathbb{F}_3(x)$ by two successive Artin–Schreier extensions. We have $g(K/\mathbb{F}_3) = 9$ and $N(K/\mathbb{F}_3) = 19$; the rational places of $K/\mathbb{F}_3$ are obtained from the pole of x which is totally ramified in the extension $K/\mathbb{F}_3(x)$ and from the zeros of x and $x-1$ which split completely in the extension $K/\mathbb{F}_3(x)$. Furthermore, there is a unique place Q of $\mathbb{F}_3(x, y_1)/\mathbb{F}_3$ of degree 3 lying over the zero of $x+1$, and Q is totally ramified in the extension $K/\mathbb{F}_3(x, y_1)$. Thus, $K/\mathbb{F}_3$ has at least one place of degree 3. Let $P_\infty, P_1, \ldots, P_{18}$ be the 19 rational places of $K/\mathbb{F}_3$ and let P_{19} be a place of $K/\mathbb{F}_3$ of degree 3. Then by Theorem 2 we get $d_3(19) \le g(K/\mathbb{F}_3) + 2 = 11$. This improves on the corresponding bound in [12].

In the case where q is a square, Theorem 4 below yields an improvement on the bound for $d_q(s)$ in Theorem 3. First we need the following auxiliary result.

Lemma 3. *For a prime power q, let $K/\mathbb{F}_{q^2}$ be a global function field, let $w \in K$, and let P be a place of $K/\mathbb{F}_{q^2}$ satisfying $\nu_P(w) = -m < 0$ with* $\gcd(m, q) = 1$. *Let $E = K(y)$ with $y^q + y = w$, and let F be a field with $K \subseteq F \subseteq E$. Let P' and P'' be places of F, respectively E, lying over P. Then the different exponent $d(P''|P')$ is given by*

$$d(P''|P') = ([E : F] - 1)(m+1).$$

Proof. Since the polynomial $z^q + z \in \mathbb{F}_q[z]$ has all its roots in $\mathbb{F}_{q^2}$, it is clear that E/K is a Galois extension. If $e(P''|P)$ is the ramification index, then

$$\nu_{P''}(w) = e(P''|P)\nu_P(w) = -e(P''|P)m,$$

but also

$$\nu_{P''}(w) = \nu_{P''}(y^q + y) = q\nu_{P''}(y).$$

From $\gcd(m, q) = 1$ it follows that q divides $e(P''|P)$. On the other hand, $e(P''|P) \le [E : K] \le q$, hence $e(P''|P) = [E : K] = q$. Thus, P is totally ramified in the extension E/K and $\nu_{P''}(y) = -m$.

Let $x \in K$ with $\nu_P(x) = 1$ and let the integers $k \ge 1$ and h be such that $hq - km = 1$. Then $t = x^h y^k$ satisfies $\nu_{P''}(t) = 1$. For any

$\sigma \in \mathrm{Gal}(E/K)\backslash\{\mathrm{id}\}$ we have $\sigma(y) = y + c$ for some nonzero $c \in \mathbb{F}_{q^2}$, thus

$$t - \sigma(t) = t(1 - (1 + cy^{-1})^k) = -t\sum_{j=1}^{k} \binom{k}{j} c^j y^{-j}.$$

Note that $k \neq 0$ in $\mathbb{F}_{q^2}$, hence $\nu_{P''}(t - \sigma(t)) = 1 + m$. Then with $G = \mathrm{Gal}(E/F)$ we get by the arguments in the proof of [15, Proposition III.7.8(c)],

$$d(P''|P') = \sum_{\sigma\in G\backslash\{\mathrm{id}\}} \nu_{P''}(t - \sigma(t)) = ([E : F] - 1)(m + 1). \ \blacksquare$$

THEOREM 4. *If $q = p^r$ with a prime p and a positive integer r, then for every dimension $s \geq 1$ we have*

$$d_{q^2}(s) \leq \frac{ps}{q-1}.$$

Proof. Let $E_1 \subseteq E_2 \subseteq \ldots$ be the tower of global function fields over $\mathbb{F}_{q^2}$ considered in the proof of Theorem 3, i.e., $E_1 = \mathbb{F}_{q^2}(x_1)$ and $E_{n+1} = E_n(z_{n+1})$ for $n = 1, 2, \ldots$ with

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \quad \text{and} \quad x_{n+1} = \frac{z_{n+1}}{x_n}.$$

Then E_{n+1}/E_n is a Galois extension of degree q for each $n \geq 1$. Hence there exists a chain of fields

$$E_n = K_{n,0} \subset K_{n,1} \subset \ldots \subset K_{n,r} = E_{n+1}$$

such that $[K_{n,i+1} : K_{n,i}] = p$ for $0 \leq i \leq r - 1$. From results in [2] we know that for all $n \geq 1$ we have

$$g(E_n/\mathbb{F}_{q^2}) \leq q^n + q^{n-1}, \quad N(E_n/\mathbb{F}_{q^2}) \geq (q^2 - 1)q^{n-1}.$$

The last inequality implies

$$N(K_{n,i}/\mathbb{F}_{q^2}) \geq \frac{N(E_{n+1}/\mathbb{F}_{q^2})}{[E_{n+1} : K_{n,i}]} \geq p^i(q^2 - 1)q^{n-1} \quad \text{for } 0 \leq i \leq r. \tag{13}$$

Next we establish an upper bound for $g(K_{n,i}/\mathbb{F}_{q^2})$. From [2, Section 2] we know that for each place P of $E_n/\mathbb{F}_{q^2}$ that is ramified in the extension E_{n+1}/E_n we have $\nu_P(x_n) = -1$, hence $\nu_P(x_n^{q+1}) = -q - 1$. It follows then from the first part of the proof of Lemma 3 that P is totally ramified in E_{n+1}/E_n. According to [2, Section 2], the sum of the degrees of these places P is equal to $q^{\lfloor n/2\rfloor}$, and so the same holds for the sum of the degrees of the places P' of $K_{n,i}/\mathbb{F}_{q^2}$ that are ramified in $E_{n+1}/K_{n,i}$, where $0 \leq i \leq r - 1$. For any such P' and the unique place P'' of $E_{n+1}/\mathbb{F}_{q^2}$ lying over it we have $d(P''|P') = (p^{r-i} - 1)(q + 2)$ by Lemma 3. By combining these facts with the Hurwitz genus fomula, we obtain

$$2g(E_{n+1}/\mathbb{F}_{q^2}) - 2 = p^{r-i}(2g(K_{n,i}/\mathbb{F}_{q^2}) - 2) + q^{\lfloor n/2\rfloor}(q + 2)(p^{r-i} - 1)$$

for $0 \le i \le r$, and so

$$\begin{aligned} g(K_{n,i}/\mathbb{F}_{q^2}) &= \frac{p^i}{q}(g(E_{n+1}/\mathbb{F}_{q^2})-1) - \frac{1}{2}q^{\lfloor n/2\rfloor -1}(q+2)(q-p^i)+1 \\ &\le p^i(q^n+q^{n-1}). \end{aligned}$$

The result of the theorem is trivial for $1 \le s \le q^2$. If $s \ge q^2+1$, then there are integers $n \ge 1$ and $1 \le i \le r$ such that

$$p^{i-1}(q^2-1)q^{n-1} \le s \le p^i(q^2-1)q^{n-1}-1.$$

In view of (13) we get

$$d_{q^2}(s) \le V_{q^2}(s) \le g(K_{n,i}/\mathbb{F}_{q^2}) \le \frac{p}{q-1}p^{i-1}(q^2-1)q^{n-1} \le \frac{ps}{q-1}. \ \blacksquare$$

Remark 3. Since an exact formula for $g(E_n/\mathbb{F}_{q^2})$ is given in [2, Theorem 2.10], the proof of Theorem 4 yields an exact formula for $g(K_{n,i}/\mathbb{F}_{q^2})$.

We note that the bound $d_q(s) = O(s)$ is best possible as far as the order of magnitude is concerned. This follows from a result of Larcher and Schmid [4], which in the improved form given in [11, Corollary 2] says that for every prime power q and every dimension $s \ge 1$ we have

$$d_q(s) > \frac{(q-1)(s+1)}{eq^2\log q} - \frac{1}{\log q}.$$

It is a standard principle that if, for any prime power q, we are able to obtain digital (t,s)-sequences constructed over $\mathbb{F}_q$, then we can construct (t,s)-sequences in an arbitrary base $b \ge 2$, namely by using a digital method with a direct product of finite fields (see [7], [8, Chapter 4], [12]). In particular, if $b = q_1 \ldots q_h$ is a product of prime powers and if for each $1 \le v \le h$ there exists a digital (t_v,s)-sequence constructed over $\mathbb{F}_{q_v}$, then there exists a (t,s)-sequence in base b with

$$t = \max(t_1,\ldots,t_h)$$

which is obtained by a digital method (see e.g. [12]). From the fact that $d_q(s) = O(s)$ with an absolute implied constant, we can thus infer that for every base $b \ge 2$ and every dimension $s \ge 1$ there exists a (t,s)-sequence in base b obtained by a digital method such that the quality parameter $t = t(b,s)$ satisfies $t(b,s) = O(s)$ with an absolute implied constant. As far as (t,s)-sequences in base b obtained by a digital method are concerned, this order of magnitude is again best possible, according to a result in [12] which shows that t must grow at least linearly in s.

The fact that we can always achieve a value $t = t(b,s)$ of the quality parameter with $t(b,s) = O(s)$ has an important implication for the coefficient $C_b(s,t)$ of the leading term in the discrepancy bound (3). To wit, the formula for $C_b(s,t)$ yields

$$\log C_b(s,t(b,s)) \le -s\log s + O(s),$$

where the implied constant depends only on b. In the earlier constructions of Faure [1] and Niederreiter [7] we have to vary the base with increasing s, only to obtain a coefficient $C'(s)$ of the leading term $N^{-1}(\log N)^s$ in the discrepancy bound which satisfies

$$\log C'(s) \le -s\log\log s + O(s).$$

Finally, we recall another general principle according to which a (t,s)-sequence in base b obtained by a digital method yields $(t,m,s+1)$-nets in base b for every integer $m \ge t$, and these nets are again produced by a digital method (see [8, Chapter 4], [12]). Thus, by the discussion above, for every base $b \ge 2$ and every $s \ge 1$ we can construct a $(t(b,s),m,s+1)$-net in base b for every $m \ge t(b,s)$, where $t(b,s) = O(s)$ with an absolute implied constant and where the net is obtained by a digital method.

References

[1] H. Faure, *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. 41 (1982), 337–351.

[2] A. Garcia and H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound*, Invent. Math., to appear.

[3] G. Larcher and H. Niederreiter, *Generalized (t,s)-sequences, Kronecker-type sequences, and diophantine approximations of formal Laurent series*, Trans. Amer. Math. Soc. 347 (1995), 2051–2073.

[4] G. Larcher and W. C. Schmid, *Multivariate Walsh series, digital nets and quasi-Monte Carlo integration*, in: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, H. Niederreiter and P. J.-S. Shiue (eds.), Lecture Notes in Statist., Springer, Berlin, to appear.

[5] G. L. Mullen, A. Mahalanabis, and H. Niederreiter, *Tables of (t,m,s)-net and (t,s)-sequence parameters*, ibid., to appear.

[6] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.

[7] —, *Low-discrepancy and low-dispersion sequences*, J. Number Theory 30 (1988), 51–70.

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

[9] —, *Pseudorandom numbers and quasirandom points*, Z. Angew. Math. Mech. 73 (1993), T648–T652.

[10] —, *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. 192 (1993), 301–328.

[11] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences obtained from algebraic function fields over finite fields*, Acta Arith. 72 (1995), 281–298.

[12] —, —, *Low-discrepancy sequences and global function fields with many rational places*, preprint, 1995.

[13] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. 296 (1983), 397–402.

[14] 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 (in Russian).

[15] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[16] S. Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simulation 3 (1993), 99–107.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SCIENCE AND
TECHNOLOGY OF CHINA
HEFEI, ANHUI 230026, P.R. CHINA

INSTITUT FÜR INFORMATIONSVERARBEITUNG
ÖSTERREICHISCHE AKADEMIE
DER WISSENSCHAFTEN
SONNENFELSGASSE 19
A-1010 WIEN, AUSTRIA
E-mail: NIEDERREITER@OEAW.AC.AT

Received on 7.4.1995 (2769)