ACTA ARITHMETICA
LXXII.3 (1995)

Low-discrepancy sequences obtained from algebraic function fields over finite fields

by

Harald Niederreiter (Wien) and Chaoping Xing (Hefei)

1. Introduction. We present a new general construction of s-dimensional low-discrepancy sequences which is based on the theory of algebraic function fields with finite constant fields. In this framework, the best general construction that was known so far, namely that in Niederreiter [8], can then be viewed as the special case in which one operates in a rational function field over a finite field. We show that the new construction yields better low-discrepancy sequences than the earlier construction for a wide range of dimensions s if one chooses for the underlying algebraic function fields for example certain elliptic function fields over small finite fields. We remark that the new construction improves on an earlier construction using algebraic function fields over finite fields which was sketched in Niederreiter [11, Section 5], [12, Section 5].

The most powerful known methods for the construction of low-discrepancy sequences are based on the theory of (t,s)-sequences. The standard procedure is to use the so-called digital method (see Section 3 for details) to obtain (t,s)-sequences, usually in a prime-power base q. In addition to the constructions mentioned above, important previous constructions using the digital method are those of Sobol' [13], Faure [2], and Niederreiter [7]. Our new construction also employs the digital method as the fundamental construction principle, and we concentrate on the case of a prime-power base q. The main challenge in the digital method for this case is to choose certain elements $c_{j,r}^{(i)}$ from the finite field $\mathbb{F}_q$ of order q judiciously (compare with Section 3), and this is where our use of algebraic function fields over $\mathbb{F}_q$ comes in.

In Section 2 we provide the necessary background on (t,m,s)-nets and (t,s)-sequences. In Section 3 we review the digital method (over finite fields)

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

for constructing point sets and sequences and we prove some necessary conditions for the parameters of digital (t, m, s)-nets and digital (t, s)-sequences. Section 4 serves to establish some basic notation and terminology for algebraic function fields. Our new construction of (t, s)-sequences by the digital method is described in detail in Section 5, and the main results pertaining to this construction are proved in Section 6. The arguments make heavy use of the theory of algebraic function fields. In Section 7 we present an example of an elliptic function field over $\mathbb{F}_2$ which demonstrates that with its use we can, for a wide range of dimensions s, obtain better (t, s)-sequences in base 2 than with the construction in [8] operating in the rational function field over $\mathbb{F}_2$. An analogous example of an elliptic function field over $\mathbb{F}_3$, yielding better (t, s)-sequences in base 3 for many dimensions s, is given in Section 8.

2. (t, m, s)-nets and (t, s)-sequences. With regard to low-discrepancy point sets and sequences we follow the terminology in the book of Niederreiter [10], to which we refer also for a general background on these topics. For $s \geq 1$ let $I^s = [0, 1)^s$ be the s-dimensional half-open unit cube. For a subinterval J of I^s and for a point set P consisting of the N points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1} \in I^s$ we write $A(J; P)$ for the number of integers n with $0 \leq n \leq N-1$ and $\mathbf{x}_n \in J$. The *star discrepancy* $D_N^*(P)$ of P is defined by

$$D_N^*(P) = \sup_J \left| \frac{A(J; P)}{N} - \lambda_s(J) \right|,$$

where the supremum is extended over all subintervals J of I^s with one vertex at the origin and where λ_s is the s-dimensional Lebesgue measure. For a sequence S of points in I^s, the star discrepancy $D_N^*(S)$ is meant to be the star discrepancy of the first N terms of S.

Let $b \geq 2$ and $0 \leq t \leq m$ be integers. Then a *(t, m, s)-net in base b* is a point set P consisting of b^m points in I^s such that $A(J; P) = b^t$ for 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 $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ and with $\lambda_s(J) = b^{t-m}$. For integers $b \geq 2$ and $t \geq 0$, a sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in I^s is a *(t, s)-sequence in base b* if, for all integers $k \geq 0$ and $m > t$, the point set consisting of the $\mathbf{x}_n$ with $kb^m \leq n < (k+1)b^m$ is a (t, m, s)-net in base b.

Any (t, s)-sequence S in base b is a low-discrepancy sequence, in the sense that $D_N^*(S) = O(N^{-1}(\log N)^s)$. More precisely, it was shown in [7, Section 4] (see also [10, Theorem 4.17]) that

$$D_N^*(S) \leq B(b, s) b^t N^{-1} (\log N)^s + O(b^t N^{-1} (\log N)^{s-1}) \quad \text{for all } N \geq 2,$$

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

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

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

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

It is clear from this discrepancy bound, and also from the definition of a (t,s)-sequence in base b, that small values of t are preferable if one wants sequences with strong uniformity properties. Therefore, the aim in the construction of (t,s)-sequences in base b is to make the value of t as small as possible for given b and s. The number t in a (t,m,s)-net or a (t,s)-sequence is sometimes referred to as the "quality parameter".

3. The digital method for constructing point sets and sequences. A general principle for the construction of (t,m,s)-nets and (t,s)-sequences in base b was introduced in [7, Section 6] and it is referred to as the *digital method*. This method can be applied with any base b, but for the purposes of the present paper it suffices to consider prime-power bases. To conform with standard notation, we write q for a prime-power base.

Let $\mathbb{F}_q$ be the finite field of order q and let $m \ge 1$ and $s \ge 1$ be integers. We write $Z_q = \{0, 1, \dots, q-1\}$ for the least residue system mod q. Now we choose the following:

(N1) bijections $\psi_r : Z_q \to \mathbb{F}_q$ for $0 \le r \le m-1$;
(N2) bijections $\eta_{i,j} : \mathbb{F}_q \to Z_q$ for $1 \le i \le s$ and $1 \le j \le m$;
(N3) elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ for $1 \le i \le s, 1 \le j \le m$, and $0 \le r \le m-1$.

For $n = 0, 1, \dots, q^m - 1$ let

$$n = \sum_{r=0}^{m-1} a_r(n) q^r \quad \text{with all } a_r(n) \in Z_q$$

be the digit expansion of n in base q. We put

$$x_n^{(i)} = \sum_{j=1}^{m} y_{n,j}^{(i)} q^{-j} \quad \text{for } 0 \le n < q^m \text{ and } 1 \le i \le s,$$

with

$$y_{n,j}^{(i)} = \eta_{i,j}\Big(\sum_{r=0}^{m-1} c_{j,r}^{(i)} \psi_r(a_r(n))\Big) \in Z_q \quad \text{for } 0 \le n < q^m, 1 \le i \le s, 1 \le j \le m,$$

and define the point set

$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}) \in I^s \quad \text{for } n = 0, 1, \dots, q^m - 1. \tag{1}$$

If this point set is a (t,m,s)-net in base q, then it is called a *digital* (t,m,s)-*net in base* q.

For the construction of sequences one proceeds in an analogous fashion. Let the prime power q and the dimension $s \ge 1$ be given. Then we choose the following:

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

(S2) bijections $\eta_{i,j} : \mathbb{F}_q \to Z_q$ for $1 \le i \le s$ and $j \ge 1$, with $\eta_{i,j}(0) = 0$ for $1 \le i \le s$ and all sufficiently large j;

(S3) elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ for $1 \le i \le s, j \ge 1$, and $r \ge 0$, where for fixed i and r we have $c_{j,r}^{(i)} = 0$ for all sufficiently large j.

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 $r \ge 0$ and $a_r(n) = 0$ for all sufficiently large r. We put

$$x_n^{(i)} = \sum_{j=1}^{\infty} y_{n,j}^{(i)} q^{-j} \qquad \text{for } n \ge 0 \text{ and } 1 \le i \le s,$$

with

$$y_{n,j}^{(i)} = \eta_{i,j}\Big(\sum_{r=0}^{\infty} c_{j,r}^{(i)} \psi_r(a_r(n))\Big) \in Z_q \qquad \text{for } n \ge 0,\ 1 \le i \le s,\ \text{and } j \ge 1.$$

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 (S2) and (S3) it follows that each $x_n^{(i)}$ is given by an expansion with finitely many terms. We now define the sequence

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

If this sequence is a (t,s)-sequence in base q, then it is called a *digital* (t,s)-*sequence in base* q. A recent survey of (t,m,s)-net and (t,s)-sequence constructions, most of which use the digital method, is given in [6].

Remark 1. In the terminology of Larcher, Niederreiter, and Schmid [3] we would have to speak of digital (t,m,s)-nets and digital (t,s)-sequences "constructed over the finite field $\mathbb{F}_q$", but since for each prime power q there is exactly one finite field of order q (up to field isomorphisms), our shorter terminology will cause no confusion.

The quality parameter t arising from the construction of nets by the digital method is determined by Lemma 1 below. The following definition is a special case of [10, Definition 4.27].

Definition 1. For a two-parameter system $C = \{\mathbf{c}_j^{(i)} \in F^m : 1 \le i \le s,\ 1 \le j \le m\}$ of vectors in F^m, where F is an arbitrary field, let $\varrho(C)$ be the largest integer d such that any subsystem $\{\mathbf{c}_j^{(i)} : 1 \le j \le d_i,\ 1 \le i \le s\}$ 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 F (here the empty system is viewed as linearly independent).

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

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

where the elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ are as in (N3). *Then the point set in* (1) *is a digital (t, m, s)-net in base q if and only if $\varrho(C) \ge m - t$.*

Proof. This follows by combining Theorems 6.10 and 6.14 in [7]. Observe that the quantity $\varrho(C)$ used in [7, Section 6] exceeds the quantity $\varrho(C)$ given by Definition 1 above by 1. ■

To get an analogous result for sequences, we let $\mathbb{F}_q^\infty$ be the sequence space over $\mathbb{F}_q$ and we consider the two-parameter system

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

where

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

and where the elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ are as in (S3). 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

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

Lemma 2. *With the notation above, the sequence in* (2) *is a digital (t, s)-sequence in base q if and only if*

$$\varrho(C^{(m)}) \ge m - t \quad \textit{for all integers } m > t.$$

Proof. This follows by combining Theorems 6.23 and 6.25 in [7] and using the observation in the proof of Lemma 1. ■

Remark 2. It follows from Lemmas 1 and 2 that the quality parameter t in digital (t, m, s)-nets and digital (t, s)-sequences in base q depends only on the elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ in (N3) and (S3), respectively, and not on the bijections chosen in the digital method.

The best general construction of digital (t, s)-sequences in a prime-power base q that was available so far is the construction in Niederreiter [8, Section 3]. This construction yields, for every prime power q and every dimension $s \ge 1$, a digital $(T_q(s), s)$-sequence in base q, where the number $T_q(s)$

is defined as follows. We list all monic irreducible polynomials over $\mathbb{F}_q$ by nondecreasing degrees in a sequence $k_1, k_2, \ldots$, and then with $e_i = \deg(k_i)$ we put

$$T_q(s) = \sum_{i=1}^{s} (e_i - 1). \tag{3}$$

It follows from [8, Theorem 2] that

$$T_q(s) = O(s \log s). \tag{4}$$

A software implementation of these sequences was carried out by Bratley, Fox, and Niederreiter [1]. The numerical experiments in [1] indicate that among these sequences, those in base $q = 2$ perform best in the important task of multidimensional numerical integration. The case $q = 2$ is also the most convenient one for computer implementation. For these reasons, and also for the sake of comparison with our new construction, we tabulate some values of $T_q(s)$ for $q = 2$. Table 1 is extracted from [8, Table II]. Further values of $T_2(s)$ can be found in Table 2.

Table 1. Values of $T_2(s)$ for $1 \le s \le 15$

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

The following lemma is a variant of [7, Lemma 5.15].

Lemma 3. *If there exists a digital (t, s)-sequence in base q, then for every $m \ge t$ there exists a digital $(t, m, s+1)$-net in base q.*

Proof. Let

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

be a digital (t, s)-sequence in base q. In view of Remark 2 we can assume that the bijections ψ_r in (S1) are chosen in such a way that $\psi_r(0) = 0$ for all $r \ge 0$. For fixed $m \ge t$ the points

$$\mathbf{y}_n = (x_n^{(1)}, \ldots, x_n^{(s)}, n/q^m) \in I^{s+1} \quad \text{for } n = 0, 1, \ldots, q^m - 1$$

form a $(t, m, s+1)$-net in base q by [7, Lemma 5.15]. It remains to prove that the $\mathbf{y}_n$ (with appropriate truncations of the q-adic expansions of the coordinates $x_n^{(i)}$) are obtained by the digital method for the construction of nets, and it clearly suffices to show this for the last coordinates of these points. In (N2) we choose $\eta_{s+1,j}$ to be the inverse map of ψ_{m-j} for $1 \le j \le m$, and in (N3) we choose

$$c_{j,r}^{(s+1)} = \delta_{r,m-j} \quad \text{for } 1 \le j \le m \text{ and } 0 \le r \le m-1,$$

where on the right-hand side we have the Kronecker symbol viewed as an element of $\mathbb{F}_q$. Then the digital method yields $x_n^{(s+1)} = n/q^m$ for $0 \le n < q^m$. ■

The following result is based on an idea of Larcher and Schmid [4]. We present a slightly different proof that allows us to use a well-known bound from coding theory (the connection between digital nets and coding theory was already pointed out in [7, Remark 7.13]).

PROPOSITION 1. *Suppose that for some integers $s \ge 1, t \ge 0$, and $u \ge 0$ there exists a digital $(t, t+u, s)$-net in base q. Then*

$$\sum_{h=0}^{\min(\lfloor u/2\rfloor, s)} \binom{s}{h} (q-1)^h \le q^{t+u}.$$

Proof. We can assume $u \ge 2$ and $m := t + u < s$, for otherwise the bound is trivial. Let $C = \{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^m : 1 \le i \le s, 1 \le j \le m\}$ be the system derived from the given digital $(t, t+u, s)$-net in base q as in Lemma 1. By this lemma we have $\varrho(C) \ge m - t = u$, hence any u of the vectors $\mathbf{c}_1^{(i)}, 1 \le i \le s$, are linearly independent over $\mathbb{F}_q$. Now we use the $\mathbf{c}_1^{(i)}, 1 \le i \le s$, as the columns of an $m \times s$ parity-check matrix of a linear code L over $\mathbb{F}_q$ with length s and dimension $k \ge s - m$. In view of [5, Lemma 8.14], L has minimum distance $\ge u + 1$, and so L can correct up to $\lfloor u/2 \rfloor$ errors by [5, Theorem 8.12]. Now the Hamming bound [5, Theorem 8.25] yields

$$q^k \sum_{h=0}^{\lfloor u/2\rfloor} \binom{s}{h} (q-1)^h \le q^s,$$

and this implies the desired result. ■

COROLLARY 1. *Suppose that for some integers $s \ge 1$ and $t \ge 0$ there exists a digital (t, s)-sequence in base q. Then*

$$\sum_{h=0}^{\min(u, s+1)} \binom{s+1}{h} (q-1)^h \le q^{t+2u} \quad \textit{for all integers } u \ge 0.$$

Proof. This follows from Lemma 3 and Proposition 1. ■

COROLLARY 2. *Suppose that for some integers $s \ge 1$ and $t \ge 0$ there exists a digital (t, s)-sequence in base q. Then*

$$s + 1 < \frac{q^2 e}{q-1} (\lfloor t \log q \rfloor + 1).$$

Proof. Put $u = \lfloor t \log q \rfloor + 1$. If $u > s + 1$, then the bound is trivial. If $u \le s + 1$, then an application of Corollary 1 yields

$$\left(\frac{s+1}{u}\right)^u (q-1)^u \le \binom{s+1}{u}(q-1)^u < q^{t+2u},$$

and so

$$s+1 < \frac{q^2}{q-1} u q^{t/u} < \frac{q^2 e}{q-1} u. \ \blacksquare$$

Remark 3. Corollary 2 shows that, for fixed q, the least value $d_q(s)$ of t such that there exists a digital (t,s)-sequence in base q grows at least linearly with s. On the other hand, we have $d_q(s) = O(s \log s)$ by (4). In particular, the construction of digital (t,s)-sequences in base q due to Niederreiter [8, Section 3] yields quality parameters t which, in terms of asymptotic orders of magnitude as $s \to \infty$, are off by at most a factor $\log s$ from $d_q(s)$.

4. Notation and terminology for algebraic function fields. For the theory of algebraic function fields we mostly follow the notation and terminology in the book of Stichtenoth [14]. For an arbitrary field F, let K be an algebraic function field with F as its full constant field. We express this fact by simply saying that K/F is an algebraic function field. The genus of K/F is denoted by g.

We write ν_P for the normalized discrete valuation corresponding to the place P of K/F. Let $x \in K\backslash\{0\}$ and denote by $Z(x)$, respectively $N(x)$, the set of zeros, respectively poles, of x. Then we define the *zero divisor* of x by

$$(x)_0 = \sum_{P \in Z(x)} \nu_P(x) P$$

and the *pole divisor* of x by

$$(x)_\infty = \sum_{P \in N(x)} (-\nu_P(x)) P.$$

Furthermore, the *principal divisor* of x is given by

$$(x) = (x)_0 - (x)_\infty.$$

For an arbitrary divisor D of K/F we put

$$\mathcal{L}(D) = \{x \in K\backslash\{0\} : (x) + D \ge 0\} \cup \{0\}.$$

Then $\mathcal{L}(D)$ is a finite-dimensional vector space over F, and we denote its dimension by $l(D)$.

If P_∞ is a place of K/F of degree 1 and z is a local uniformizing parameter at P_∞, then every $x \in K$ has an expansion

$$x = \sum_{r=v}^{\infty} a_r z^r,$$

where $\nu_{P_\infty}(x) \ge v$ and all $a_r \in F$. The following definition is crucial.

Definition 2. A positive integer n is called a *pole number* of P_∞ if there exists an element $x \in K$ with $(x)_\infty = nP_\infty$. Otherwise, n is called a *gap number* of P_∞.

By the Weierstrass gap theorem [14, Theorem I.6.7], there are exactly g gap numbers of P_∞, and 1 is a gap number of P_∞ whenever $g > 0$. In particular, if $n_1 < n_2 < \ldots$ are the pole numbers of P_∞ arranged in increasing order, then

$$n_r \le g + r \quad \text{for } r = 1, 2, \ldots \tag{5}$$

Remark 4. If K/F is a rational function field, then $g = 0$ and we have $n_r = r$ for all $r \ge 1$.

Remark 5. If K/F is an elliptic function field, then $g = 1$ and we have $n_r = r + 1$ for all $r \ge 1$.

5. The new construction of sequences. The notation in Section 4 will remain operative. For the purpose of constructing digital (t, s)-sequences in base q, it suffices to consider algebraic function fields $K/\mathbb{F}_q$, but the arguments leading to Theorem 1 in Section 6 are valid for general algebraic function fields K/F.

We fix a place P_∞ of K/F of degree 1 and let R be the ring

$$R = \{x \in K : \nu_P(x) \ge 0 \text{ for all places } P \ne P_\infty \text{ of } K/F\}.$$

Given an integer $s \ge 1$, we choose $k_1, \ldots, k_s \in R$ satisfying the following two conditions:

(i) the zero sets $Z(k_1), \ldots, Z(k_s)$ are pairwise disjoint;
(ii) $n_{e_i} - e_i < n_1$ for $1 \le i \le s$, where $e_i := -\nu_{P_\infty}(k_i) \ge 1$ for $1 \le i \le s$.

Since n_r is a pole number of P_∞, we can find $w_r \in R$ such that $(w_r)_\infty = n_r P_\infty$ for $r \ge 1$. Note that each $e_i, 1 \le i \le s$, is a pole number of P_∞ since $(k_i)_\infty = e_i P_\infty$. Thus, for each $1 \le i \le s$ there exists a uniquely determined positive integer f_i with $n_{f_i} = e_i$, and it is trivial that $f_i \le e_i$. For each $1 \le i \le s$ we define the set

$$\{w_{i,0}, w_{i,1}, \ldots, w_{i,e_i-1}\} = \{1, w_1, \ldots, w_{e_i}\} \backslash \{w_{f_i}\}.$$

Lemma 4. *For each $1 \le i \le s$, the element k_i is not an F-linear combination of $w_{i,0}, w_{i,1}, \ldots, w_{i,e_i-1}$.*

Proof. For $n \ge 1$ we have $l(nP_\infty) - l((n-1)P_\infty) = 0$ or 1, and the latter case happens if and only if n is a pole number of P_∞. Also $w_r \in \mathcal{L}(n_r P_\infty) \backslash \mathcal{L}((n_r - 1)P_\infty)$ for $r \ge 1$, and so $\{1, w_1, \ldots, w_{f_i}\}$ is a basis of

$\mathcal{L}(e_iP_\infty)$. Since $k_i \in \mathcal{L}(e_iP_\infty)$, we have

$$k_i = a_0 + \sum_{h=1}^{f_i} a_h w_h$$

with $a_0, a_1, \ldots, a_{f_i} \in F$, and it is easy to see that $a_{f_i} \neq 0$ since $\nu_{P_\infty}(k_i) = -e_i = \nu_{P_\infty}(w_{f_i})$. On the other hand, the elements $1, w_1, \ldots, w_{e_i}$ are linearly independent over F, and so k_i is not an F-linear combination of the elements of $\{1, w_1, \ldots, w_{e_i}\} \backslash \{w_{f_i}\}$. ■

We can now define the elements $c_{j,r}^{(i)} \in F$ which in the case $F = \mathbb{F}_q$ serve as the elements in (S3) in the construction of sequences described in Section 3. For $1 \leq i \leq s$ and $j \geq 1$ we write

$$j - 1 = Q(i,j)e_i + u(i,j)$$

with integers $Q(i,j)$ and $u(i,j)$, where $0 \leq u(i,j) \leq e_i - 1$. Then

$$\begin{aligned}\nu_{P_\infty}(w_{i,u(i,j)}k_i^{-Q(i,j)-1}) &\geq \nu_{P_\infty}(w_{e_i}) - (Q(i,j)+1)\nu_{P_\infty}(k_i)\\ &= -n_{e_i} + (Q(i,j)+1)e_i \geq e_i - n_{e_i} \geq -g,\end{aligned}$$

where we used (5) in the last step. Hence we have the following expansion at P_∞:

$$w_{i,u(i,j)}k_i^{-Q(i,j)-1} = z^{-g} \sum_{r=0}^{\infty} c_{j,r}^{(i)} z^r \qquad \text{with } c_{j,r}^{(i)} \in F. \tag{6}$$

For fixed i it is clear that $Q(i,j) \to \infty$ as $j \to \infty$, and so for fixed i and r we have $c_{j,r}^{(i)} = 0$ for all sufficiently large j. Thus, in the case $F = \mathbb{F}_q$ the condition in (S3) in Section 3 is satisfied.

Remark 6. The condition (ii) above is clearly satisfied if the set of gap numbers of P_∞ is $\{1, \ldots, g\}$. Properties equivalent to the latter property are: (a) $n_1 = g + 1$; (b) $n_r = g + r$ for all $r \geq 1$; (c) $l(nP_\infty) = n + 1 - g$ for all $n \geq g$. In particular, the condition (ii) is satisfied if K/F is a rational function field or an elliptic function field (compare with Remarks 4 and 5).

6. The main results.

Let the elements $c_{j,r}^{(i)} \in F$ be defined by (6). In analogy with the definition of the two-parameter system $C^{(\infty)}$ in Section 3 we put

$$\mathbf{c}_j^{(i)} = (c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots) \in F^\infty \qquad \text{for } 1 \leq i \leq s \text{ and } j \geq 1,$$

and

$$C^{(\infty)} = \{\mathbf{c}_j^{(i)} : 1 \leq i \leq s \text{ and } j \geq 1\}.$$

Furthermore, with the projection

$$\pi_m : (c_0, c_1, \ldots) \in F^\infty \mapsto (c_0, \ldots, c_{m-1}) \in F^m \qquad \text{for } m \geq 1$$

we define

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

Then for the numbers $\varrho(C^{(m)})$ given by Definition 1 we have the following result.

THEOREM 1. *With the notation above, and under the conditions in Section* 5, *we have*

$$\varrho(C^{(m)}) \ge m - g - 1 - \sum_{i=1}^{s}(e_i - 1) \quad \text{for all } m \ge 1,$$

where g is the genus of K/F and $e_i = -\nu_{P_\infty}(k_i)$ for $1 \le i \le s$.

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

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

are linearly independent over F. Suppose that we have

$$\sum_{i=1}^{s}\sum_{j=1}^{d_i} a_j^{(i)} \pi_m(\mathbf{c}_j^{(i)}) = \mathbf{0} \in F^m \tag{7}$$

for some $a_j^{(i)} \in F$, where we can assume without loss of generality that all $d_i \ge 1$. Then we consider the element $k \in K$ given by

$$\begin{aligned} k &= \sum_{i=1}^{s}\sum_{j=1}^{d_i} a_j^{(i)} w_{i,u(i,j)} k_i^{-Q(i,j)-1} \\ &= \sum_{i=1}^{s}\sum_{j=1}^{d_i} a_j^{(i)} z^{-g} \sum_{r=0}^{\infty} c_{j,r}^{(i)} z^r = z^{-g} \sum_{r=0}^{\infty} \Big(\sum_{i=1}^{s}\sum_{j=1}^{d_i} a_j^{(i)} c_{j,r}^{(i)} \Big) z^r. \end{aligned}$$

From (7) we get $\nu_{P_\infty}(k) \ge m - g$.

By collecting equal powers of k_i, we can write k in the form

$$k = \sum_{i=1}^{s} \sum_{h=1}^{Q_i+1} p_{i,h} k_i^{-h},$$

where $Q_i = \lfloor (d_i - 1)/e_i \rfloor$ and $p_{i,h} \in R$ is an F-linear combination of $w_{i,0}, w_{i,1}, \ldots, w_{i,e_i-1}$. Let

$$b = \prod_{i=1}^{s} k_i^{Q_i+1} \in R.$$

Then $kb \in R$ and

$$\nu_{P_\infty}(kb) \geq m - g - \sum_{i=1}^{s}(Q_i + 1)e_i \geq m - g - \sum_{i=1}^{s}(d_i - 1 + e_i) \geq 1.$$

It follows that $k = 0$, hence

$$\sum_{i=1}^{s}\sum_{h=1}^{Q_i+1} p_{i,h}k_i^{-h} = 0. \tag{8}$$

Now we fix an i with $1 \leq i \leq s$. From (8) and condition (i) in Section 5 we obtain

$$p_{i,Q_i+1} = k_i x \quad \text{with some } x \in R.$$

Suppose we had $p_{i,Q_i+1} \neq 0$. Then, since p_{i,Q_i+1} is an F-linear combination of $1, w_1, \ldots, w_{e_i}$, we get

$$n_{e_i}P_\infty \geq (p_{i,Q_i+1})_\infty = (k_i x)_\infty = e_i P_\infty + (x)_\infty,$$

and so

$$(x)_\infty \leq (n_{e_i} - e_i)P_\infty < n_1 P_\infty$$

by condition (ii) in Section 5. But n_1 is the least pole number of P_∞, hence we must have $x \in F$. It follows that $k_i = x^{-1}p_{i,Q_i+1}$ is an F-linear combination of $w_{i,0}, w_{i,1}, \ldots, w_{i,e_i-1}$, which is a contradiction to Lemma 4. Thus we have proved that $p_{i,Q_i+1} = 0$.

Now we return to (8) and, using the same arguments, we can show that $p_{i,h} = 0$ for all i and h, that is, $a_j^{(i)} = 0$ for $1 \leq j \leq d_i, 1 \leq i \leq s$. ∎

Remark 7. If K/F is a rational function field, then $g = 0$ and $f_i = e_i$ for $1 \leq i \leq s$ by Remark 4. Thus, in Section 5 we have

$$\nu_{P_\infty}(w_{i,u(i,j)}k_i^{-Q(i,j)-1}) \geq 1 = -g + 1,$$

and so obvious modifications in the proof of Theorem 1 yield the result

$$\varrho(C^{(m)}) \geq m - g - \sum_{i=1}^{s}(e_i - 1) = m - \sum_{i=1}^{s}(e_i - 1) \quad \text{for all } m \geq 1.$$

Now we specialize F to be the finite field $\mathbb{F}_q$. We choose bijections ψ_r and $\eta_{i,j}$ as in (S1) and (S2), respectively, in Section 3. Furthermore, we determine the elements $c_{j,r}^{(i)} \in \mathbb{F}_q$ by (6), where we work with an algebraic function field $K/\mathbb{F}_q$ in Section 5. These $c_{j,r}^{(i)}$ serve as the elements in (S3) in Section 3. If we now follow the digital method for the construction of sequences described in Section 3, then we obtain the sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in I^s.

THEOREM 2. *Let q be a prime power and $s \geq 1$. Then, under the conditions in Section 5 relating to the algebraic function field $K/\mathbb{F}_q$, the sequence*

$\mathbf{x}_0, \mathbf{x}_1, \ldots$ *defined above is a digital* (t, s)*-sequence in base* q *with*

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

where g *is the genus of* $K/\mathbb{F}_q$ *and* $e_i = -\nu_{P_\infty}(k_i)$ *for* $1 \leq i \leq s$.

Proof. This follows from Lemma 2 and the case $F = \mathbb{F}_q$ of Theorem 1. ∎

Corollary 3. *Let* q *be a prime power and* $s \geq 1$. *Suppose that the conditions in Section* 5 *relating to the algebraic function field* $K/\mathbb{F}_q$ *are satisfied*, *and let* t *be as in Theorem* 2. *Then for every* $m \geq t$ *there exists a digital* $(t, m, s+1)$*-net in base* q.

Proof. This follows from Lemma 3 and Theorem 2. ∎

Remark 8. Let $\mathbb{F}_q(z)$ be the rational function field over $\mathbb{F}_q$. In the construction described in Section 5, we choose P_∞ to be the pole of z and we let $k_1, \ldots, k_s$ be s distinct monic irreducible polynomials over $\mathbb{F}_q$ of least degrees. Then condition (i) in Section 5 holds trivially and condition (ii) in Section 5 holds in view of Remark 6, and we note that $e_i = \deg(k_i)$ for $1 \leq i \leq s$. If we also take into account Remark 7, then the construction in Section 5 yields a digital $(T_q(s), s)$-sequence in base q, where $T_q(s)$ is as in (3). Therefore the present construction, when applied to $\mathbb{F}_q(z)$, yields the same quality parameters as the construction in [8, Section 3].

Remark 9. The result of Theorem 1 with $F = \mathbb{F}_q$ is also of relevance in the combinatorial problem for vector spaces over finite fields discussed by Niederreiter [9], [12, Section 5].

7. An example for $q = 2$.

We show by way of an example that our new construction yields (t, s)-sequences in base 2 which, for a wide range of dimensions s of practical interest (e.g. for $16 \leq s \leq 126$), have the currently smallest quality parameters t. In particular, this example demonstrates that certain algebraic function fields $K/\mathbb{F}_2$ of positive genus produce better sequences than the rational function field over $\mathbb{F}_2$ (see Remark 8 for the latter). We recall from Section 3 that (t, s)-sequences in base 2 tend to be the most useful ones from the practical point of view. For this and the following section, we refer to [14, Chapters V and VI] for the necessary background.

Let $K/\mathbb{F}_2$ be the function field of the elliptic curve

$$y^2 + y = x^3 + x + 1 \quad \text{over } \mathbb{F}_2.$$

This curve has exactly one $\mathbb{F}_2$-rational point, namely the point $(0 : 1 : 0)$ at infinity. Therefore, the elliptic function field $K/\mathbb{F}_2$ has a unique place P_∞ of degree 1, and the class number of $K/\mathbb{F}_2$ is 1, where by the class number we mean the index of the subgroup of principal divisors in the group of divisors of degree 0.

We list all places $\neq P_\infty$ of $K/\mathbb{F}_2$ by nondecreasing degrees in a sequence $P_1, P_2, \ldots$ Since $K/\mathbb{F}_2$ has class number 1, the divisor

$$P_i - (\deg(P_i))P_\infty$$

is principal for $i = 1, 2, \ldots$ Given $s \geq 1$, we choose $k_1, \ldots, k_s \in K$ such that

$$(k_i) = P_i - (\deg(P_i))P_\infty \quad \text{for } 1 \leq i \leq s. \tag{9}$$

Each k_i is in R, and the condition (i) in Section 5 is clearly satisfied. In view of Remark 6, the condition (ii) in Section 5 is also satisfied, and by (9) we have $e_i = -\nu_{P_\infty}(k_i) = \deg(P_i)$. We put

$$E_2(s) = 2 + \sum_{i=1}^{s} (e_i - 1).$$

Then we can deduce the following results from Theorem 2 and Corollary 3.

Theorem 3. *For every $s \geq 1$ there exists a digital $(E_2(s), s)$-sequence in base* 2.

Corollary 4. *For every $s \geq 1$ and $m \geq E_2(s)$ there exists a digital $(E_2(s), m, s+1)$-net in base* 2.

For $r \geq 1$ let B_r be the number of places of $K/\mathbb{F}_2$ of degree r, and put $M_1 = 0$ and

$$M_n = \sum_{r=2}^{n} B_r \quad \text{for } n \geq 2.$$

For given $s \geq 1$ let $n(s)$ be the largest integer with $M_{n(s)} \leq s$. Then we clearly have

$$E_2(s) = 2 + \sum_{r=2}^{n(s)} (r-1)B_r + (s - M_{n(s)})n(s). \tag{10}$$

To tabulate $E_2(s)$, it remains to find a formula for B_r. Let $L \in \mathbb{Z}[u]$ be the L-polynomial of $K/\mathbb{F}_2$, i.e., the numerator of the zeta function of $K/\mathbb{F}_2$ (see [14, Definition V.1.14]). Then $L(u) = 2u^2 - 2u + 1$ by [14, Theorem V.1.15], and $\alpha_1 = 1 + i$ and $\alpha_2 = 1 - i$ are the reciprocals of the complex roots of L. We put

$$S_r = \alpha_1^r + \alpha_2^r = 2^{(r+2)/2} \cos \frac{\pi r}{4} \quad \text{for } r = 1, 2, \ldots$$

Then by [14, Proposition V.2.9] we have

$$B_r = \frac{1}{r} \sum_{d \mid r} \mu\left(\frac{r}{d}\right)(2^d - S_d) \quad \text{for } r \geq 2,$$

where the sum is over all positive integers d dividing r and μ is the Möbius function. Together with (10) this allows the straightforward calculation of $E_2(s)$.

We tabulate some values of $E_2(s)$ in Table 2. Since the tables of quality parameters in [6] extend to dimension $s = 50$, we go up to this value of s as well. When we compare the values of $E_2(s)$ with those of $T_2(s)$ from (3) in this range, we find that $E_2(s) > T_2(s)$ for $1 \le s \le 14, E_2(15) = T_2(15)$, and $E_2(s) < T_2(s)$ for $16 \le s \le 50$. For the purpose of getting (t, s)-sequences in base 2 with smaller quality parameters t, it is thus the last range which is of interest. The following values of B_r are needed for this range:

$$B_2 = 2,\ B_3 = 4,\ B_4 = 5,\ B_5 = 8,\ B_6 = 8,\ B_7 = 16,\ B_8 = 25.$$

In Table 2 we include the values of $T_2(s)$ for $16 \le s \le 50$ for the sake of comparison.

Table 2. Values of $E_2(s)$ and $T_2(s)$ for $16 \le s \le 50$

s	16	17	18	19	20	21	22	23	24	25	26	27
$E_2(s)$	47	51	55	59	64	69	74	79	84	89	94	99
$T_2(s)$	48	53	58	63	68	73	78	83	89	95	101	107

s	28	29	30	31	32	33	34	35	36	37	38
$E_2(s)$	105	111	117	123	129	135	141	147	153	159	165
$T_2(s)$	113	119	125	131	137	143	149	155	161	167	173

s	39	40	41	42	43	44	45	46	47	48	49	50
$E_2(s)$	171	177	183	189	195	202	209	216	223	230	237	244
$T_2(s)$	179	185	191	198	205	212	219	226	233	240	247	254

The calculation of the values of $E_2(s)$ can easily be carried further. A comparison with the values of $T_2(s)$ yields the following results:

$$\begin{aligned} E_2(s) &< T_2(s) \quad \text{for } 16 \le s \le 126,\\ E_2(s) &= T_2(s) \quad \text{for } 127 \le s \le 218,\\ E_2(s) &> T_2(s) \quad \text{for } 219 \le s \le 1378,\\ &E_2(1379) = T_2(1379),\\ &E_2(1380) < T_2(1380). \end{aligned}$$

We conjecture that the oscillating behavior of the differences $E_2(s) - T_2(s)$ continues indefinitely.

An asymptotic upper bound for $E_2(s)$ can be obtained in a straightforward manner. First of all, (10) implies

$$E_2(s) \le n(s)s + 2.$$

Next, for $n \geq 1$ we have

$$(M_n + 1)n = n \sum_{r=1}^{n} B_r \geq \sum_{d|n} dB_d.$$

By using the formula (2.23) on p. 178 of [14] and the Hasse–Weil bound, we get

$$(M_n + 1)n \geq 2^n + 1 - 2^{(n+2)/2}.$$

Thus, the definition of $n(s)$ yields $n(s) = O(\log s)$, and so

$$E_2(s) = O(s \log s).$$

By (4) this is the same result as for $T_2(s)$.

Remark 10. For those dimensions s for which $E_2(s) < T_2(s)$, we get improved (t, s)-sequences in base b for all $b \equiv 2 \bmod 4$. This follows by using Theorem 3 of the present paper in the proof of [10, Corollary 4.51].

8. An example for $q = 3$. We proceed in analogy with Section 7 to obtain (t, s)-sequences in base 3 with the currently smallest quality parameters t for certain dimensions s.

Let $K/\mathbb{F}_3$ be the function field of the elliptic curve

$$y^2 = x^3 + 2x + 2 \quad \text{over } \mathbb{F}_3.$$

This curve has exactly one $\mathbb{F}_3$-rational point, namely the point $(0 : 1 : 0)$ at infinity. Therefore, the elliptic function field $K/\mathbb{F}_3$ has a unique place P_∞ of degree 1, and the class number of $K/\mathbb{F}_3$ is 1. We continue in complete analogy with Section 7. In particular, for given $s \geq 1$ we choose $k_1, \ldots, k_s \in R$ such that (9) holds. Then the conditions (i) and (ii) in Section 5 are satisfied. With $e_i = \deg(P_i)$ for $1 \leq i \leq s$ we put

$$E_3(s) = 2 + \sum_{i=1}^{s} (e_i - 1).$$

Then we have the following analogs of Theorem 3 and Corollary 4, respectively.

THEOREM 4. *For every $s \geq 1$ there exists a digital $(E_3(s), s)$-sequence in base* 3.

COROLLARY 5. *For every $s \geq 1$ and $m \geq E_3(s)$ there exists a digital $(E_3(s), m, s + 1)$-net in base* 3.

Values of $E_3(s)$ are calculated by (10), with B_r and M_n now referring of course to $K/\mathbb{F}_3$. The L-polynomial of $K/\mathbb{F}_3$ is $L(u) = 3u^2 - 3u + 1$. If α_1 and α_2 are the reciprocals of the complex roots of L, then we put

$$S_r = \alpha_1^r + \alpha_2^r \quad \text{for } r = 0, 1, \ldots$$

The S_r are most conveniently computed by the recursion

$$S_{r+2} = 3S_{r+1} - 3S_r \qquad \text{for } r \geq 0,$$

with initial values $S_0 = 2$ and $S_1 = 3$. We have

$$B_r = \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right)(3^d - S_d) \qquad \text{for } r \geq 2.$$

The actual calculation of the values of $E_3(s)$ and the comparison with the values of $T_3(s)$ from (3) shows that the least dimension s for which $E_3(s) < T_3(s)$ is $s = 199$. We tabulate some selected values of $E_3(s)$ and the corresponding values of $T_3(s)$ in Table 3. The following values of B_r are needed to get the values of $E_3(s)$ in Table 3:

$$B_2 = 3,\ B_3 = 9,\ B_4 = 21,\ B_5 = 54,\ B_6 = 125.$$

Table 3. Selected values of $E_3(s)$ and $T_3(s)$

s	3	10	100	197	198	199	200	201	202	203	204
$E_3(s)$	5	19	367	852	857	862	867	872	877	882	887
$T_3(s)$	0	11	365	851	857	863	869	875	881	887	893

s	205	206	207	208	209	210	211	212
$E_3(s)$	892	897	902	907	912	917	922	927
$T_3(s)$	899	905	911	917	923	929	935	941

Further calculations of $E_3(s)$ using $B_7 = 324$ and $B_8 = 819$ show, for instance, that $E_3(s) < T_3(s)$ for $199 \leq s \leq 1355$. It seems likely, however, that $E_3(s) - T_3(s)$ is oscillating (compare with our analogous conjecture in Section 7). As before one proves that

$$E_3(s) = O(s \log s).$$

Furthermore, the analog of Remark 10 holds for bases $b \equiv 3$ or $6 \bmod 9$.

References

[1] P. Bratley, B. L. Fox and H. Niederreiter, *Implementation and tests of low-discrepancy sequences*, ACM Trans. Model. Comput. Simulation 2 (1992), 195–213.

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

[3] G. Larcher, H. Niederreiter and W. C. Schmid, *Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration*, Monatsh. Math., to appear.

[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] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, revised ed., Cambridge Univ. Press, Cambridge, 1994.

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

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

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

[9] —, *A combinatorial problem for vector spaces over finite fields*, Discrete Math. 96 (1991), 221–228.

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

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

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

[13] 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).

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

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

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

Received on 24.1.1995 (2734)