ACTA ARITHMETICA
130.1 (2007)

Low-discrepancy sequences using duality and global function fields

by

Harald Niederreiter (Singapore) and
Ferruh Özbudak (Singapore and Ankara)

1. Introduction. Let $s \geq 1$ be an integer and I^s be the s-dimensional unit cube $[0,1]^s$. We consider (finite) point sets and (infinite) sequences of points in I^s, where the term "point set" is used in the sense of the combinatorial notion of "multiset", that is, a set in which multiplicity of elements is allowed and taken into account.

Constructing sequences with good equidistribution properties is an important problem in number theory and has applications to quasi-Monte Carlo methods in numerical analysis (see [6], [7], [8], [15]). The precise formulation of the problem leads to the concept of star discrepancy and the requirement of constructing low-discrepancy sequences. A very powerful method for constructing low-discrepancy sequences is the construction of (t,s)-sequences using global function fields in [12] and [19] (see also [15, Chapter 8]). A relevant method for constructing low-discrepancy point sets is the construction of (t,m,s)-nets and digital nets. The concept of duality was introduced in [11] and used in [10] for the construction of digital nets from global function fields. We refer the reader to [8] and [9] for recent surveys on constructions of (t,m,s)-nets and (t,s)-sequences. Recently Kritzer [2] improved the star discrepancy bounds for (t,m,s)-nets and (t,s)-sequences.

In this paper we construct low-discrepancy sequences using the concept of duality and global function fields. For certain parameters these sequences give asymptotically better star discrepancy bounds than (t,s)-sequences. An important role in our construction is played by differentials of global function fields. We note that a completely different construction of low-discrepancy sequences using differentials of global function fields was recently given in [4].

2000 *Mathematics Subject Classification*: 11K38, 11K45, 11R58.

Key words and phrases: low-discrepancy sequences, (t,s)-sequences, global function fields, differentials.

The paper is organized as follows. We give some basic definitions in the remainder of this section. Section 2 contains some preliminaries and auxiliary results. In Section 3 we present our construction of low-discrepancy sequences. In Section 4 we obtain a star discrepancy bound for a class of sequences including those constructed in Section 3. We give concrete examples and illustrate our improvements by numerical results in Section 5.

Now we present some basic definitions. For a subinterval J of I^s and for a point set $\mathcal{P}$ of $N \geq 1$ points $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1} \in I^s$, we write $A(J; \mathcal{P})$ for the number of integers n with $0 \leq n \leq N-1$ for which $\boldsymbol{x}_n \in J$. We put

$$R(J; \mathcal{P}) = \frac{A(J; \mathcal{P})}{N} - \lambda_s(J), \tag{1.1}$$

where λ_s is the s-dimensional Lebesgue measure.

Definition 1.1. The *star discrepancy* $D_N^*(\mathcal{P})$ of the point set $\mathcal{P}$ of $N \geq 1$ elements of I^s is defined by

$$D_N^*(\mathcal{P}) = \sup_J |R(J; \mathcal{P})|,$$

where the supremum is extended over all subintervals J of I^s with one vertex at the origin. For a sequence $\mathcal{S}$ of points in I^s and $N \geq 1$, the *star discrepancy* $D_N^*(\mathcal{S})$ is meant to be the star discrepancy of the first N terms of $\mathcal{S}$.

Given an integer $b \geq 2$, an interval of the form

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

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ is called an *elementary interval in base b*.

Definition 1.2. For integers $b \geq 2$, $s \geq 1$, and $0 \leq t \leq m$, a (t, m, s)-*net in base b* is a point set $\mathcal{P}$ consisting of b^m points in I^s such that $R(J; \mathcal{P}) = 0$ for every elementary interval $J \subseteq I^s$ in base b with $\lambda_s(J) = b^{t-m}$.

2. Preliminaries. We introduce some notation which will be used in what follows. Let $b \geq 2$ be an integer and $\mathbb{Z}_b = \{0, 1, \ldots, b-1\}$ be the least residue system modulo b. For a real number $x \in [0, 1]$, let

$$x = \sum_{j=1}^{\infty} y_j b^{-j} \quad \text{with all } y_j \in \mathbb{Z}_b \tag{2.1}$$

be a b-adic expansion of x, where the case in which $y_j = b - 1$ for all but finitely many j is allowed. Using the expansion of x in (2.1), for an integer

$m \geq 1$ we define the truncation

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

Note that the truncation operates on the expansion of x and it may yield different results depending on which b-adic expansion of x is used. If $\boldsymbol{x} = (x^{(1)}, \ldots, x^{(s)}) \in I^s$ and the $x^{(i)}$, $1 \leq i \leq s$, are given by prescribed b-adic expansions, then we define

$$[\boldsymbol{x}]_{b,m} = ([x^{(1)}]_{b,m}, \ldots, [x^{(s)}]_{b,m}). \tag{2.2}$$

The concept of a $(\mathbf{T}, s)$-sequence in base b was introduced by Larcher and Niederreiter [3]. We use a slight variant of this concept which, at the same time, generalizes the version of the definition of a (t, s)-sequence in base b used in [12] and [15, Chapter 8]. We write $\mathbb{N}$ for the set of positive integers and $\mathbb{N}_0$ for the set of nonnegative integers.

Definition 2.1. Let $b \geq 2$ and $s \geq 1$ be integers and let $\mathbf{T} : \mathbb{N} \to \mathbb{N}_0$ be a function with $\mathbf{T}(m) \leq m$ for all $m \in \mathbb{N}$. Then a sequence $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots$ of points in I^s is a $(\mathbf{T}, s)$-*sequence in base* b if for all $k \in \mathbb{N}_0$ and $m \in \mathbb{N}$, the points $[\boldsymbol{x}_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a $(\mathbf{T}(m), m, s)$-net in base b.

Remark 2.2. The original definition of a $(\mathbf{T}, s)$-sequence in base b in [3] required that for all $k \in \mathbb{N}_0$ and $m \in \mathbb{N}$, the points $\boldsymbol{x}_n$ with $kb^m \leq n < (k+1)b^m$ form a $(\mathbf{T}(m), m, s)$-net in base b. For this earlier definition, all points $\boldsymbol{x}_n$ need to be in the half-open unit cube $[0, 1)^s$, whereas Definition 2.1 allows points from the closed unit cube I^s. The device of truncation in (2.2) and in Definition 2.1 guarantees that even though all the points $\boldsymbol{x}_n$ are in I^s, all the points $[\boldsymbol{x}_n]_{b,m}$ are in $[0, 1)^s$. Note that it is a necessary condition for a (t, m, s)-net $\mathcal{P}$ in base b that all points of $\mathcal{P}$ be in $[0, 1)^s$.

Remark 2.3. If $\mathbf{T}$ is such that $\mathbf{T}(m) \leq t$ for some integer $t \geq 0$ and all integers $m > t$, then Definition 2.1 yields the concept of a (t, s)-sequence in base b. The smaller the value of t, the better the equidistribution properties of a (t, s)-sequence in base b.

Next we recall the digital method for the construction of sequences of points in I^s. This method goes back to [5]. For our purposes, it is convenient to follow the presentation in [15, Section 8.2]. We fix a base $b \geq 2$ and a dimension $s \geq 1$. Let R be a finite commutative ring with identity and of order b. We set up a map $\phi_\infty : R^\infty \to [0, 1]$ by selecting a bijection $\eta : R \to \mathbb{Z}_b$ and putting

$$\phi_\infty(r_1, r_2, \ldots) = \sum_{j=1}^{\infty} \eta(r_j) b^{-j} \quad \text{for } (r_1, r_2, \ldots) \in R^\infty.$$

Furthermore, we choose $\infty \times \infty$ matrices $C^{(1)}, \ldots, C^{(s)}$ over R which are called *generating matrices*. For $n = 0, 1, \ldots$, let

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

be the digit expansion of n in base b, where $a_j(n) \in \mathbb{Z}_b$ for $j \geq 0$ and $a_j(n) = 0$ for all sufficiently large j. Choose a bijection $\psi : \mathbb{Z}_b \to R$ with $\psi(0) = 0$ and associate with n the sequence

$$\mathbf{n} = (\psi(a_0(n)), \psi(a_1(n)), \ldots) \in R^{\infty}.$$

Now we define the sequence $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots$ of points in I^s by

$$\boldsymbol{x}_n = (\phi_\infty(\mathbf{n}C^{(1)}), \ldots, \phi_\infty(\mathbf{n}C^{(s)})) \quad \text{for } n = 0, 1, \ldots. \tag{2.3}$$

Note that the products $\mathbf{n}C^{(i)}$ are well defined since $\mathbf{n}$ contains only finitely many nonzero terms.

For each $i = 1, \ldots, s$ and $m \in \mathbb{N}$, let $C_m^{(i)}$ be the $m \times m$ submatrix of $C^{(i)}$ obtained from the first m rows and columns of $C^{(i)}$. For $j = 1, \ldots, m$, let $\mathbf{c}_{m,j}^{(i)}$ be the jth column vector of $C_m^{(i)}$. For any $\mathbf{d} = (d_1, \ldots, d_s) \in \mathbb{N}_0^s$ with $d_i \leq m$ for $1 \leq i \leq s$ and $d := \sum_{i=1}^s d_i > 0$, we define the $m \times d$ matrix

$$C_{m,\mathbf{d}} = [\mathbf{c}_{m,1}^{(1)} \ldots \mathbf{c}_{m,d_1}^{(1)} \ldots \mathbf{c}_{m,1}^{(s)} \ldots \mathbf{c}_{m,d_s}^{(s)}] \tag{2.4}$$

whose columns are obtained from the indicated columns of $C_m^{(1)}, \ldots, C_m^{(s)}$.

PROPOSITION 2.4. *The sequence* (2.3) *is a* $(\mathbf{T}, s)$*-sequence in base* b *if and only if for any* $m \in \mathbb{N}$ *with* $\mathbf{T}(m) < m$ *and any* $\mathbf{d} = (d_1, \ldots, d_s) \in \mathbb{N}_0^s$ *with* $\sum_{i=1}^s d_i = m - \mathbf{T}(m)$ *the system of homogeneous linear equations*

$$\mathbf{k}C_{m,\mathbf{d}} = \mathbf{0} \in R^{m-\mathbf{T}(m)}$$

has exactly $b^{\mathbf{T}(m)}$ *solutions* $\mathbf{k} \in R^m$*, where* $C_{m,\mathbf{d}}$ *is the matrix in* (2.4).

Proof. This is shown by the same argument as in the proof of [15, Theorem 8.2.9]. Note that we need not check the condition in Definition 2.1 when $\mathbf{T}(m) = m$ since any point set consisting of b^m points in $[0,1)^s$ is an (m, m, s)-net in base b. ∎

We now consider the special case where the ring R is the finite field $\mathbb{F}_q$ of order q, with q being an arbitrary prime power. As above, let $\mathbf{c}_{m,1}^{(i)}, \ldots, \mathbf{c}_{m,m}^{(i)}$ denote the column vectors of the matrix $C_m^{(i)}$. For integers $0 < d \leq m$, we call $\{\mathbf{c}_{m,j}^{(i)} \in \mathbb{F}_q^m : 1 \leq j \leq m,\ 1 \leq i \leq s\}$ a (d, m, s)*-system over* $\mathbb{F}_q$ if for any $(d_1, \ldots, d_s) \in \mathbb{N}_0^s$ with $\sum_{i=1}^s d_i = d$ the vectors $\mathbf{c}_{m,j}^{(i)}$, $1 \leq j \leq d_i$, $1 \leq i \leq s$, are linearly independent over $\mathbb{F}_q$ (see [11, Definition 3]).

COROLLARY 2.5. *Suppose that for any* $m \in \mathbb{N}$ *with* $\mathbf{T}(m) < m$, $\{\mathbf{c}_{m,j}^{(i)} \in \mathbb{F}_q^m : 1 \le j \le m, 1 \le i \le s\}$ *is an* $(m - \mathbf{T}(m), m, s)$*-system over* $\mathbb{F}_q$. *Then* (2.3) *is a* $(\mathbf{T}, s)$*-sequence in base* q.

Proof. The given hypothesis guarantees that any matrix $C_{m,\mathbf{d}}$ in Proposition 2.4 has rank $m - \mathbf{T}(m)$, and so the result follows immediately from Proposition 2.4. ∎

We need some notation and concepts from the duality theory developed by Niederreiter and Pirsic [11]. For $m \in \mathbb{N}$ and $\mathbf{a} = (a_1, \dots, a_m) \in \mathbb{F}_q^m$, we put $v(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0}$, and otherwise

$$v(\mathbf{a}) = \max\{j : a_j \neq 0\}.$$

For integers $s \ge 2$, we extend this definition to $\mathbb{F}_q^{ms}$ by writing a vector $\mathbf{A} \in \mathbb{F}_q^{ms}$ as the concatenation of s vectors of length m, i.e.,

$$\mathbf{A} = (\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(s)}) \in \mathbb{F}_q^{ms} \quad \text{with } \mathbf{a}^{(i)} \in \mathbb{F}_q^m \text{ for } 1 \le i \le s,$$

and putting

$$V_m(\mathbf{A}) = \sum_{i=1}^{s} v(\mathbf{a}^{(i)}).$$

DEFINITION 2.6. For any nonzero $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$, we define the *minimum distance*

$$\delta_m(\mathcal{N}) = \min_{\mathbf{A} \in \mathcal{N} \setminus \{\mathbf{0}\}} V_m(\mathbf{A}).$$

For any $\mathbb{F}_q$-linear subspace $\mathcal{M}$ of $\mathbb{F}_q^{ms}$, we define its *dual space* $\mathcal{M}^\perp$ by

$$\mathcal{M}^\perp = \{\mathbf{A} \in \mathbb{F}_q^{ms} : \mathbf{A} \cdot \mathbf{M} = 0 \text{ for all } \mathbf{M} \in \mathcal{M}\},$$

where "$\cdot$" denotes the standard inner product on $\mathbb{F}_q^{ms}$. Note that

$$\dim(\mathcal{M}^\perp) = ms - \dim(\mathcal{M}), \tag{2.5}$$

where here and subsequently we write $\dim(\mathcal{W})$ for the $\mathbb{F}_q$-dimension of a finite-dimensional vector space $\mathcal{W}$ over $\mathbb{F}_q$.

Let $C^{(1)}, \dots, C^{(s)}$ again be the generating matrices over $\mathbb{F}_q$ in (2.3). For each $i = 1, \dots, s$ and $m \in \mathbb{N}$, let $C_m^{(i)}$ be the $m \times m$ submatrix of $C^{(i)}$ defined above. Then we set up the $m \times ms$ matrix

$$C_m = [C_m^{(1)} \mid C_m^{(2)} \mid \dots \mid C_m^{(s)}] \tag{2.6}$$

over $\mathbb{F}_q$ and let $\mathcal{C}_m$ be the row space of C_m. It is trivial that $\dim(\mathcal{C}_m) \le m$, and so (2.5) shows that $\mathcal{C}_m^\perp$ has positive dimension whenever $s \ge 2$. Therefore the minimum distance $\delta_m(\mathcal{C}_m^\perp)$ is defined in this case.

PROPOSITION 2.7. *Let* $s \ge 2$ *and suppose that for any* $m \in \mathbb{N}$ *with* $\mathbf{T}(m) < m$, *the dual space* $\mathcal{C}_m^\perp$ *of* $\mathcal{C}_m$ *satisfies*

$$\delta_m(\mathcal{C}_m^\perp) \ge m - \mathbf{T}(m) + 1.$$

Then the sequence (2.3) *with generating matrices* $C^{(1)}, \ldots, C^{(s)}$ *over* $\mathbb{F}_q$ *is a* $(\mathbf{T}, s)$*-sequence in base* q*.*

Proof. For any $m \in \mathbb{N}$ with $\mathbf{T}(m) < m$, consider the system $\{\mathbf{c}_{m,j}^{(i)} \in \mathbb{F}_q^m : 1 \le j \le m,\ 1 \le i \le s\}$ of column vectors of the matrix C_m in (2.6). In view of [11, Theorem 1 and Definition 3], the given hypothesis implies that $\{\mathbf{c}_{m,j}^{(i)} \in \mathbb{F}_q^m : 1 \le j \le m,\ 1 \le i \le s\}$ is an $(m - \mathbf{T}(m), m, s)$-system over $\mathbb{F}_q$. The desired result now follows from Corollary 2.5. ∎

3. A construction from global function fields. Throughout this section we assume the existence of a global function field F satisfying the following assumption.

Assumption 3.1. Let $s \ge 2$ and $g \ge 0$ be integers and let q be a prime power. Assume that there exists a global function field F with full constant field $\mathbb{F}_q$ and with the following properties: (i) the genus of F is g; (ii) there exist s distinct places $P_1, \ldots, P_s$ of F of degree 1; (iii) there exists a place Q of F of degree 2.

Using places of F of sufficiently large degree, we can find a divisor G of F of degree $g-1$ such that the support of G is disjoint from $\{Q, P_1, \ldots, P_s\}$. For even integers $2\overline{m} \ge g$, let $A_{2\overline{m}}$, $G_{2\overline{m}}$, and $G_{2\overline{m}+1}$ be the divisors of F given by

$$\begin{aligned} A_{2\overline{m}} &:= G - \overline{m}Q, \\ G_{2\overline{m}} &:= G - \overline{m}Q + 2\overline{m}(P_1 + \cdots + P_s), \\ G_{2\overline{m}+1} &:= G - \overline{m}Q + (2\overline{m}+1)(P_1 + \cdots + P_s). \end{aligned}$$

For a divisor A of F, let $\Omega(A)$ denote the $\mathbb{F}_q$-linear subspace of the space Ω of differentials of F given by

$$\Omega(A) = \{\omega \in \Omega^* : (\omega) \ge A\} \cup \{0\}.$$

We refer to the book of Stichtenoth [18] for the theory of differentials of global function fields and for other background on global function fields.

Lemma 3.2. *For all even integers* $2\overline{m} \ge g$*, we have* $\Omega(A_{2\overline{m}}) \subseteq \Omega(A_{2\overline{m}+2})$ *and*

$$\dim(\Omega(A_{2\overline{m}})) = 2\overline{m}.$$

Proof. As $A_{2\overline{m}+2} \le A_{2\overline{m}}$, it is clear that $\Omega(A_{2\overline{m}}) \subseteq \Omega(A_{2\overline{m}+2})$. Note that $\deg(A_{2\overline{m}}) = g - 1 - 2\overline{m} < 0$ since $2\overline{m} \ge g$. Then we have

$$\dim(\Omega(A_{2\overline{m}})) = -\deg(A_{2\overline{m}}) + g - 1 = 2\overline{m},$$

and the proof is complete. ∎

Using Lemma 3.2, let $\omega_1, \omega_2, \ldots$ be a sequence of differentials of F such that for all integers $2\overline{m} \geq g$ we have

$$\langle \omega_1, \ldots, \omega_{2\overline{m}} \rangle = \Omega(A_{2\overline{m}}).$$

For a divisor A of F, let $\mathcal{L}(A)$ denote the Riemann–Roch space

$$\mathcal{L}(A) = \{x \in F^* : (x) \geq -A\} \cup \{0\}.$$

LEMMA 3.3. *For all even integers $2\overline{m} \geq g$ we have the following*:

(i) *If $\omega \in \Omega(A_{2\overline{m}})$ and $x \in \mathcal{L}(G_{2\overline{m}})$ are nonzero, then*

$$(x\omega) \geq -2\overline{m}(P_1 + \cdots + P_s).$$

(ii) *If $\omega \in \Omega(A_{2\overline{m}})$ and $x \in \mathcal{L}(G_{2\overline{m}+1})$ are nonzero, then*

$$(x\omega) \geq -(2\overline{m}+1)(P_1 + \cdots + P_s).$$

Proof. Note that

$$A_{2\overline{m}} - G_{2\overline{m}} = -2\overline{m}(P_1 + \cdots + P_s).$$

For nonzero $\omega \in \Omega(A_{2\overline{m}})$ and $x \in \mathcal{L}(G_{2\overline{m}})$, we have $(\omega) \geq A_{2\overline{m}}$ and $(x) \geq -G_{2\overline{m}}$. Using also the fact that $(x\omega) = (x) + (\omega)$, we complete the proof of (i). The proof of (ii) is similar. ∎

For a differential $\delta \in \Omega$ and a place P of F of degree 1, let $\mathrm{res}_P(\delta) \in \mathbb{F}_q$ denote the residue of the differential δ at P. For $i = 1, \ldots, s$, let t_i be a local parameter of F at P_i.

We will construct our low-discrepancy sequences in Theorem 3.7 below by using the images of $\mathbb{F}_q$-linear spaces $\langle \omega_1, \ldots, \omega_m \rangle$ of differentials under suitable $\mathbb{F}_q$-linear maps formed from residues of some differentials at the places $P_1, \ldots, P_s$ for $m \geq g+1$. If $m = 2\overline{m} \geq g+1$, then $\langle \omega_1, \ldots, \omega_m \rangle = \Omega(A_{2\overline{m}})$ and the image will be the image of $\Omega(A_{2\overline{m}})$ under a suitable $\mathbb{F}_q$-linear map depending on m. If $m = 2\overline{m}+1 \geq g+1$, then $\langle \omega_1, \ldots, \omega_m \rangle \subsetneq \Omega(A_{2\overline{m}+2})$ and the image will be the image of the proper subspace $\langle \omega_1, \ldots, \omega_{2\overline{m}+1} \rangle$ of $\Omega(A_{2\overline{m}+2})$ under a suitable $\mathbb{F}_q$-linear map depending on m.

Now we define these $\mathbb{F}_q$-linear maps for $m \geq g+1$. The definitions depend heavily on the parity of m. For even integers $2\overline{m} \geq g+1$ and for $i = 1, \ldots, s$, let $\varphi_{2\overline{m},i}$ and $\varphi_{2\overline{m}+1,i}$ be the $\mathbb{F}_q$-linear maps defined by

$$\varphi_{2\overline{m},i} : \Omega(A_{2\overline{m}}) \to \mathbb{F}_q^{2\overline{m}},$$
$$\omega \mapsto (\mathrm{res}_{P_i}(t_i^{-1}\omega), \mathrm{res}_{P_i}(t_i^{-2}\omega), \ldots, \mathrm{res}_{P_i}(t_i^{-2\overline{m}}\omega)),$$

and

$$\varphi_{2\overline{m}+1,i} : \Omega(A_{2\overline{m}+2}) \to \mathbb{F}_q^{2\overline{m}+1},$$
$$\omega \mapsto (\mathrm{res}_{P_i}(t_i^{-1}\omega), \mathrm{res}_{P_i}(t_i^{-2}\omega), \ldots, \mathrm{res}_{P_i}(t_i^{-2\overline{m}-1}\omega)).$$

Moreover, let $\mathbf{\Phi}_{2\overline{m}}$ and $\mathbf{\Phi}_{2\overline{m}+1}$ be the $\mathbb{F}_q$-linear maps

$$\mathbf{\Phi}_{2\overline{m}} : \Omega(A_{2\overline{m}}) \to \mathbb{F}_q^{2\overline{m}s}, \quad \omega \mapsto (\varphi_{2\overline{m},1}(\omega), \varphi_{2\overline{m},2}(\omega), \ldots, \varphi_{2\overline{m},s}(\omega)), \tag{3.1}$$

and

$$\mathbf{\Phi}_{2\overline{m}+1} : \Omega(A_{2\overline{m}+2}) \to \mathbb{F}_q^{(2\overline{m}+1)s}, \quad \omega \mapsto (\varphi_{2\overline{m}+1,1}(\omega), \varphi_{2\overline{m}+1,2}(\omega), \ldots, \varphi_{2\overline{m}+1,s}(\omega)). \tag{3.2}$$

Furthermore, we put

$$\mathcal{M}_{2\overline{m}} := \mathbf{\Phi}_{2\overline{m}}(\Omega(A_{2\overline{m}})), \quad \mathcal{M}_{2\overline{m}+1} := \mathbf{\Phi}_{2\overline{m}+1}(\langle \omega_1, \ldots, \omega_{2\overline{m}+1} \rangle).$$

LEMMA 3.4. *For even integers $2\overline{m} \geq g+1$, the $\mathbb{F}_q$-linear maps $\mathbf{\Phi}_{2\overline{m}}$ and $\mathbf{\Phi}_{2\overline{m}+1}$ are injective and*

$$\dim(\mathcal{M}_{2\overline{m}}) = 2\overline{m}, \quad \dim(\mathcal{M}_{2\overline{m}+1}) = 2\overline{m}+1.$$

Proof. It is well known that for a divisor A of F with $\deg(A) \geq 2g-1$ we have $\dim(\Omega(A)) = 0$. Moreover, for $i = 1, \ldots, s$ and $l \in \mathbb{N}$, if $\nu_{P_i}((\omega)) \geq 0$ and

$$\operatorname{res}_{P_i}(t_i^{-1}\omega) = \operatorname{res}_{P_i}(t_i^{-2}\omega) = \cdots = \operatorname{res}_{P_i}(t_i^{-l}\omega) = 0,$$

then $\nu_{P_i}((\omega)) \geq l$. Assume that $\omega \in \Omega(A_{2\overline{m}})$ is nonzero and $\mathbf{\Phi}_{2\overline{m}}(\omega) = \mathbf{0} \in \mathbb{F}_q^{2\overline{m}s}$. Then

$$(\omega) \geq A_{2\overline{m}} + 2\overline{m}(P_1 + \cdots + P_s) = G - \overline{m}Q + 2\overline{m}(P_1 + \cdots + P_s).$$

Thus, $\omega \in \Omega(A_{2\overline{m}} + 2\overline{m}(P_1 + \cdots + P_s))$ and $\deg(A_{2\overline{m}} + 2\overline{m}(P_1 + \cdots + P_s)) = g - 1 + 2\overline{m}(s-1) \geq g - 1 + 2\overline{m} \geq 2g$, where we have used the facts that $s \geq 2$ and $2\overline{m} \geq g+1$. Hence $\dim(\Omega(A_{2\overline{m}} + 2\overline{m}(P_1 + \cdots + P_s))) = 0$, a contradiction. This shows that $\mathbf{\Phi}_{2\overline{m}}$ is injective, and so $\dim(\mathcal{M}_{2\overline{m}}) = 2\overline{m}$ by Lemma 3.2. Similarly, the injectivity of $\mathbf{\Phi}_{2\overline{m}+1}$ follows from the observation that

$$\deg(A_{2\overline{m}+2} + (2\overline{m}+1)(P_1 + \cdots + P_s)) = g - 1 + (s-2) + 2\overline{m}(s-1) \geq 2g.$$

It is then obvious that $\dim(\mathcal{M}_{2\overline{m}+1}) = 2\overline{m}+1$. ∎

For even integers $2\overline{m} \geq g+1$, we define further $\mathbb{F}_q$-linear maps. For $i = 1, \ldots, s$ and $x \in \mathcal{L}(G_{2\overline{m}})$, let $x_i^{(-1)}, x_i^{(-2)}, \ldots, x_i^{(-2\overline{m})}$ be the elements of $\mathbb{F}_q$ which are the coefficients in the local expansion

$$x = x_i^{(-2\overline{m})} t_i^{-2\overline{m}} + x_i^{(-2\overline{m}+1)} t_i^{-2\overline{m}+1} + \cdots$$

of x at P_i. Similarly, for $i = 1, \ldots, s$ and $x \in \mathcal{L}(G_{2\overline{m}+1})$, we define $x_i^{(-1)}, x_i^{(-2)}, \ldots, x_i^{(-2\overline{m}-1)} \in \mathbb{F}_q$. Let

$$\psi_{2\overline{m},i} : \mathcal{L}(G_{2\overline{m}}) \to \mathbb{F}_q^{2\overline{m}}, \quad x \mapsto (x_i^{(-1)}, x_i^{(-2)}, \ldots, x_i^{(-2\overline{m})}),$$

$$\psi_{2\overline{m}+1,i} : \mathcal{L}(G_{2\overline{m}+1}) \to \mathbb{F}_q^{2\overline{m}+1}, \quad x \mapsto (x_i^{(-1)}, x_i^{(-2)}, \ldots, x_i^{(-2\overline{m}-1)}).$$

Moreover, let $\mathbf{\Psi}_{2\overline{m}}$ and $\mathbf{\Psi}_{2\overline{m}+1}$ be the $\mathbb{F}_q$-linear maps

$$\begin{aligned}\mathbf{\Psi}_{2\overline{m}} : \mathcal{L}(G_{2\overline{m}}) &\to \mathbb{F}_q^{2\overline{m}s},\\ x &\mapsto (\psi_{2\overline{m},1}(x), \psi_{2\overline{m},2}(x), \dots, \psi_{2\overline{m},s}(x)),\end{aligned}$$

and

$$\begin{aligned}\mathbf{\Psi}_{2\overline{m}+1} : \mathcal{L}(G_{2\overline{m}+1}) &\to \mathbb{F}_q^{(2\overline{m}+1)s},\\ x &\mapsto (\psi_{2\overline{m}+1,1}(x), \psi_{2\overline{m}+1,2}(x), \dots, \psi_{2\overline{m}+1,s}(x)).\end{aligned}$$

Furthermore, we put

$$\mathcal{N}_{2\overline{m}} := \mathbf{\Psi}_{2\overline{m}}(\mathcal{L}(G_{2\overline{m}})), \quad \mathcal{N}_{2\overline{m}+1} := \mathbf{\Psi}_{2\overline{m}+1}(\mathcal{L}(G_{2\overline{m}+1})).$$

LEMMA 3.5. *For even integers $2\overline{m} \ge g+1$, the $\mathbb{F}_q$-linear maps $\mathbf{\Psi}_{2\overline{m}}$ and $\mathbf{\Psi}_{2\overline{m}+1}$ are injective and*

$$\dim(\mathcal{N}_{2\overline{m}}) = 2\overline{m}s - 2\overline{m}, \quad \dim(\mathcal{N}_{2\overline{m}+1}) = (2\overline{m}+1)s - 2\overline{m}.$$

Proof. Assume that $x \in \mathcal{L}(G_{2\overline{m}})$ and $\mathbf{\Psi}_{2\overline{m}}(x) = \mathbf{0} \in \mathbb{F}_q^{2\overline{m}s}$. Then $\nu_{P_i}(x) \ge 0$ for $1 \le i \le s$ and hence $x \in \mathcal{L}(G_{2\overline{m}} - 2\overline{m}(P_1 + \cdots + P_s))$. Note that $\deg(G_{2\overline{m}} - 2\overline{m}(P_1 + \cdots + P_s)) = g - 1 - 2\overline{m} < 0$ as $2\overline{m} \ge g+1$. Hence $x = 0$ and $\mathbf{\Psi}_{2\overline{m}}$ is injective. We also have $\deg(G_{2\overline{m}}) = g - 1 - 2\overline{m} + 2\overline{m}s > 2g - 1$ as $2\overline{m} \ge g+1$ and $s \ge 2$. Therefore by the Riemann–Roch theorem, $\dim(\mathcal{N}_{2\overline{m}}) = \dim(\mathcal{L}(G_{2\overline{m}})) = \deg(G_{2\overline{m}}) + 1 - g = 2\overline{m}s - 2\overline{m}$.

Next assume that $x \in \mathcal{L}(G_{2\overline{m}+1})$ and $\mathbf{\Psi}_{2\overline{m}+1}(x) = \mathbf{0} \in \mathbb{F}_q^{(2\overline{m}+1)s}$. Similarly, we have $x \in \mathcal{L}(G_{2\overline{m}+1} - (2\overline{m}+1)(P_1 + \cdots + P_s))$ and hence $x = 0$ and $\mathbf{\Psi}_{2\overline{m}+1}$ is injective. Also $\deg(G_{2\overline{m}+1}) = g - 1 - 2\overline{m} + (2\overline{m}+1)s \ge s + 2g - 1 > 2g - 1$ and then $\dim(\mathcal{N}_{2\overline{m}+1}) = \dim(\mathcal{L}(G_{2\overline{m}+1})) = \deg(G_{2\overline{m}+1}) + 1 - g = (2\overline{m}+1)s - 2\overline{m}$. ∎

PROPOSITION 3.6. *For even integers $2\overline{m} \ge g+1$ we have*:

(i) $\mathcal{M}_{2\overline{m}}^{\perp} = \mathcal{N}_{2\overline{m}}$.
(ii) $\mathcal{M}_{2\overline{m}+1}^{\perp} \subseteq \mathcal{N}_{2\overline{m}+1}$.

Proof. First we prove (i). We will show that for $\omega \in \Omega(A_{2\overline{m}})$ and $x \in \mathcal{L}(G_{2\overline{m}})$, we have $\mathbf{\Phi}_{2\overline{m}}(\omega) \cdot \mathbf{\Psi}_{2\overline{m}}(x) = 0$, where the inner product is the standard inner product on $\mathbb{F}_q^{2\overline{m}s}$. This implies that $\mathcal{M}_{2\overline{m}} \perp \mathcal{N}_{2\overline{m}}$ in $\mathbb{F}_q^{2\overline{m}s}$. Moreover, by Lemmas 3.4 and 3.5, $\dim(\mathcal{M}_{2\overline{m}}) + \dim(\mathcal{N}_{2\overline{m}}) = 2\overline{m}s$ and hence we get $\mathcal{M}_{2\overline{m}}^{\perp} = \mathcal{N}_{2\overline{m}}$ by (2.5).

Now we prove that for $\omega \in \Omega(A_{2\overline{m}})$ and $x \in \mathcal{L}(G_{2\overline{m}})$, we have $\mathbf{\Phi}_{2\overline{m}}(\omega) \cdot \mathbf{\Psi}_{2\overline{m}}(x) = 0$. For $i = 1, \dots, s$, the local expansion of $x \in \mathcal{L}(G_{2\overline{m}})$ at P_i is

$$x = x_i^{(-2\overline{m})} t_i^{-2\overline{m}} + x_i^{(-2\overline{m}+1)} t_i^{-2\overline{m}+1} + \cdots + x_i^{(-1)} t_i^{-1} + y_i, \tag{3.3}$$

where $\nu_{P_i}(y_i) \ge 0$. For $\omega \in \Omega(A_{2\overline{m}})$, using the $\mathbb{F}_q$-linearity of the residue map res_{P_i} we get

$$\operatorname{res}_{P_i}(x\omega) = x_i^{(-2\overline{m})} \operatorname{res}_{P_i}(t_i^{-2\overline{m}}\omega) + \cdots + x_i^{(-1)} \operatorname{res}_{P_i}(t_i^{(-1)}\omega) + \operatorname{res}_{P_i}(y_i\omega).$$

As $\nu_{P_i}(y_i) \geq 0$ and $\nu_{P_i}(\omega) \geq \nu_{P_i}(A_{2\overline{m}}) = 0$, we have $\mathrm{res}_{P_i}(y_i\omega) = 0$ and hence

$$\mathrm{res}_{P_i}(x\omega) = \varphi_{2\overline{m},i}(\omega) \cdot \psi_{2\overline{m},i}(x), \tag{3.4}$$

where the inner product is the standard inner product on $\mathbb{F}_q^{2\overline{m}}$. Using the Residue Theorem (cf. [1, Section III.5, Theorems 2 and 3]), Lemma 3.3(i), and (3.4), we obtain

$$0 = \sum_P \mathrm{res}_P(x\omega) = \sum_{i=1}^{s} \varphi_{2\overline{m},i}(\omega) \cdot \psi_{2\overline{m},i}(x) = \mathbf{\Phi}_{2\overline{m}}(\omega) \cdot \mathbf{\Psi}_{2\overline{m}}(x),$$

where the first sum is over all places P of F. This finishes the proof of (i).

Now we consider (ii). Let $\mathcal{W}$ be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{(2\overline{m}+1)s}$ given by

$$\mathcal{W} = \mathbf{\Phi}_{2\overline{m}+1}(\Omega(A_{2\overline{m}})).$$

By Lemmas 3.2 and 3.4, we have $\dim(\mathcal{W}) = 2\overline{m}$ and $\mathcal{M}_{2\overline{m}+1} \supseteq \mathcal{W}$. It suffices to prove that $\mathcal{W}^{\perp} = \mathcal{N}_{2\overline{m}+1}$. Indeed, this implies that $\mathcal{M}_{2\overline{m}+1}^{\perp} \subseteq \mathcal{W}^{\perp} = \mathcal{N}_{2\overline{m}+1}$. Using Lemma 3.5, we deduce that $\dim(\mathcal{W}) + \dim(\mathcal{N}_{2\overline{m}+1}) = 2\overline{m} + (2\overline{m}+1)s - 2\overline{m} = (2\overline{m}+1)s$. Therefore it remains to show that if $\omega \in \Omega(A_{2\overline{m}})$ and $x \in \mathcal{L}(G_{2\overline{m}+1})$, then $\mathbf{\Phi}_{2\overline{m}+1}(\omega) \cdot \mathbf{\Psi}_{2\overline{m}+1}(x) = 0$, where the inner product is the standard inner product on $\mathbb{F}_q^{(2\overline{m}+1)s}$. We follow similar arguments to those in the proof of (i). For $i = 1, \ldots, s$, for $x \in \mathcal{L}(G_{2\overline{m}+1})$ and $\omega \in \Omega(A_{2\overline{m}})$, using the local expansion of x at P_i, we obtain

$$\mathrm{res}_{P_i}(x\omega) = \varphi_{2\overline{m}+1,i}(\omega) \cdot \psi_{2\overline{m}+1,i}(x), \tag{3.5}$$

where the inner product is the standard inner product on $\mathbb{F}_q^{2\overline{m}+1}$. Note that in the local expansion of $x \in \mathcal{L}(G_{2\overline{m}+1})$ at P_i, we have the extra term $x_i^{(-2\overline{m}-1)} t_i^{-2\overline{m}-1}$, in addition to the terms in (3.3). Then, similarly to the case (i), using the Residue Theorem, Lemma 3.3(ii), and (3.5), we complete the proof of (ii). ∎

For an integer $m \geq g+1$, let C_m be the $m \times ms$ matrix over $\mathbb{F}_q$ given by

$$C_m = \begin{bmatrix} \mathbf{\Phi}_m(\omega_1) \\ \mathbf{\Phi}_m(\omega_2) \\ \vdots \\ \mathbf{\Phi}_m(\omega_m) \end{bmatrix}. \tag{3.6}$$

Note that for an integer $m \geq g+1$, if m is even (resp. odd), then $\mathbf{\Phi}_m$ is defined by (3.1) (resp. (3.2)). Let $C_m^{(1)}, C_m^{(2)}, \ldots, C_m^{(s)}$ be the $m \times m$ matrices over $\mathbb{F}_q$ defined by

$$C_m = [C_m^{(1)} \,|\, C_m^{(2)} \,|\, \ldots \,|\, C_m^{(s)}]. \tag{3.7}$$

We observe that for each $i = 1, \dots, s$, $C_m^{(i)}$ is the $m \times m$ submatrix of the $(m+1) \times (m+1)$ matrix $C_{m+1}^{(i)}$ formed from the first m rows and columns of $C_{m+1}^{(i)}$. Hence, for each $i = 1, \dots, s$, we can build an $\infty \times \infty$ matrix $C^{(i)}$ over $\mathbb{F}_q$ such that for any integer $m \geq g+1$ the $m \times m$ submatrix of $C^{(i)}$ formed from the first m rows and columns of $C^{(i)}$ is equal to $C_m^{(i)}$.

Our construction of low-discrepancy sequences now proceeds by the digital method described in Section 2. We use the matrices $C^{(1)}, \dots, C^{(s)}$ over $\mathbb{F}_q$ defined in the previous paragraph as the generating matrices in (2.3). The resulting sequence is a $(\mathbf{T}, s)$-sequence in base q in the sense of Definition 2.1, with the function $\mathbf{T} : \mathbb{N} \to \mathbb{N}_0$ given in the following theorem.

THEOREM 3.7. *Under Assumption* 3.1, *let* $\mathcal{S}$ *be the sequence of points in* I^s *which is constructed in* (2.3) *using the generating matrices* $C^{(1)}, \dots, C^{(s)}$ *over* $\mathbb{F}_q$ *defined after* (3.7). *Then* $\mathcal{S}$ *is a* $(\mathbf{T}, s)$*-sequence in base* q *with* $\mathbf{T}(m) = m$ *for* $1 \leq m \leq g$, $\mathbf{T}(m) = g$ *for even* $m \geq g+1$, *and* $\mathbf{T}(m) = g+1$ *for odd* $m \geq g+1$.

Proof. We proceed by Proposition 2.7. First let $m = 2\overline{m}$ be even. We can assume that $m = 2\overline{m} \geq g+1$. Then by construction, the row space $\mathcal{C}_m$ of the matrix C_m in (3.6) is given by $\mathcal{C}_m = \mathcal{M}_{2\overline{m}}$. Hence it follows from Proposition 3.6 that $\mathcal{C}_m^\perp = \mathcal{N}_{2\overline{m}}$. Now we apply [10, Theorem 3.1] with $\mathcal{N} = C_m(P_1, \dots, P_s; G_{2\overline{m}})$ in the notation of that theorem and we observe that $\mathcal{N} = \mathcal{N}_{2\overline{m}}$. This yields, again in the notation of [10, Theorem 3.1],

$$\delta_m(\mathcal{C}_m^\perp) = \delta_m(\mathcal{N}_{2\overline{m}}) \geq \delta_m^*(1, \dots, 1; ms - m + g - 1).$$

Next we use [10, Lemma 2.1] to obtain

$$\delta_m^*(1, \dots, 1; ms - m + g - 1) \geq m - g + 1,$$

and so

$$\delta_m(\mathcal{C}_m^\perp) \geq m - g + 1.$$

Now let $m = 2\overline{m} + 1$ be odd. We can assume that $m = 2\overline{m} + 1 \geq g + 2$. So we have $\mathcal{C}_m = \mathcal{M}_{2\overline{m}+1}$, and hence Proposition 3.6 yields $\mathcal{C}_m^\perp \subseteq \mathcal{N}_{2\overline{m}+1}$. We apply [10, Theorem 3.1] with $\mathcal{N} = C_m(P_1, \dots, P_s; G_{2\overline{m}+1}) = \mathcal{N}_{2\overline{m}+1}$ and obtain

$$\delta_m(\mathcal{C}_m^\perp) \geq \delta_m(\mathcal{N}_{2\overline{m}+1}) \geq \delta_m^*(1, \dots, 1; ms - m + g).$$

By [10, Lemma 2.1] we get

$$\delta_m^*(1, \dots, 1; ms - m + g) \geq m - g,$$

and so

$$\delta_m(\mathcal{C}_m^\perp) \geq m - (g+1) + 1.$$

Thus, the theorem is proved in all cases. ∎

REMARK 3.8. Previous constructions of low-discrepancy sequences using global function fields over $\mathbb{F}_q$ led to (t, s)-sequences in base q (see Remark 2.3). For fixed q and $s \geq 2$, the best previous constructions of this type using a global function field F satisfying Assumption 3.1 yield (t, s)-sequences in base q with $t = g + 1$ (see [4], [15, Theorem 8.4.1], [19]). Theorem 3.7 improves on these constructions under Assumption 3.1. This improvement is also reflected in better bounds on the star discrepancy of the new sequences, as will be shown in Section 4. There are combinations of values of q and s for which the global function fields satisfying Assumption 3.1 have given the best previous constructions of (t, s)-sequences in base q, for instance when $s = q + 1$. Examples of this type will be presented in Section 5.

REMARK 3.9. Our construction of low-discrepancy sequences starts from sequences of certain $\mathbb{F}_q$-linear spaces of differentials of F. In order to construct such low-discrepancy sequences, it is possible to use a dual approach starting from sequences of certain Riemann–Roch spaces of F. Since we start from differentials of F, in the proof of Theorem 3.7 we can estimate the **T**-parameters of the low-discrepancy sequences by using results of [10], which would not have been possible in a dual approach. Thus, the essential points of our approach are using the Residue Theorem and reducing the estimation of **T**-parameters to the results of [10].

4. Bounds on the star discrepancy. In this section we obtain bounds on the star discrepancy of a class of sequences of points in I^s, including those constructed in Theorem 3.7. This will imply that the sequences in Theorem 3.7 have asymptotically better bounds on the star discrepancy than (t, s)-sequences for certain parameters. We will also illustrate our improvements by some concrete examples in Section 5.

For integers $b \geq 2$, $m \geq 1$, $0 \leq t \leq m$, and $s \geq 2$, let $\Delta_b(t, m, s)$ be a number for which

$$b^m D^*_{b^m}(\mathcal{P}) \leq \Delta_b(t, m, s)$$

holds for any (t, m, s)-net $\mathcal{P}$ in base b. We quote the following result in [2, Corollary 4] in a simplified form.

PROPOSITION 4.1. *If b is even, then we can take*

$$\Delta_b(t, m, s) = \frac{b^{t+s}}{(b+1)2^s(s-1)!}\, m^{s-1} + \mathcal{O}(b^t m^{s-2}),$$

and if b is odd, then we can take

$$\Delta_b(t, m, s) = \frac{b^t(b-1)^{s-1}}{2^s(s-1)!}\, m^{s-1} + \mathcal{O}(b^t m^{s-2}).$$

In both cases, the implied constants in the Landau symbols depend only on b and s.

The following lemma allows us to use a star discrepancy bound for the original concept of $(\mathbf{T}, s)$-sequences in base b (see Remark 2.2) just as well for the concept of $(\mathbf{T}, s)$-sequences in base b introduced in this paper (see Definition 2.1).

LEMMA 4.2. *Let $\mathcal{P}$ be the point set consisting of the points $\boldsymbol{y}_n$, $n = 0, 1, \ldots, b^m - 1$, in I^s. Suppose that the points $[\boldsymbol{y}_n]_{b,m}$, $n = 0, 1, \ldots, b^m - 1$, form a (t, m, s)-net in base b. Then*

$$b^m D^*_{b^m}(\mathcal{P}) \le \Delta_b(t, m, s).$$

Proof. For $n = 0, 1, \ldots, b^m - 1$, we can write

$$\boldsymbol{y}_n = [\boldsymbol{y}_n]_{b,m} + \boldsymbol{z}_n \quad \text{with } \boldsymbol{z}_n \in [0, b^{-m}]^s.$$

Let $0 < \varepsilon \le 1$ be given and let $\mathcal{P}(\varepsilon)$ be the point set consisting of

$$\boldsymbol{y}_n(\varepsilon) = [\boldsymbol{y}_n]_{b,m} + (1 - \varepsilon)\boldsymbol{z}_n, \quad n = 0, 1, \ldots, b^m - 1.$$

By Definition 1.2 and the assumption that the points $[\boldsymbol{y}_n]_{b,m}$, $n = 0, 1, \ldots, b^m - 1$, form a (t, m, s)-net in base b, it is clear that $\mathcal{P}(\varepsilon)$ is a (t, m, s)-net in base b. Therefore

$$b^m D^*_{b^m}(\mathcal{P}(\varepsilon)) \le \Delta_b(t, m, s).$$

Furthermore, for each $n = 0, 1, \ldots, b^m - 1$, corresponding coordinates of $\boldsymbol{y}_n$ and $\boldsymbol{y}_n(\varepsilon)$ differ by at most $b^{-m}\varepsilon$. Therefore, by a well-known principle (see e.g. [6, Lemma 2.5] for the one-dimensional case, which can be immediately extended to the multidimensional case),

$$|b^m D^*_{b^m}(\mathcal{P}) - b^m D^*_{b^m}(\mathcal{P}(\varepsilon))| \le s\varepsilon,$$

and so

$$b^m D^*_{b^m}(\mathcal{P}) \le \Delta_b(t, m, s) + s\varepsilon.$$

Letting $\varepsilon \to 0+$, we get the desired result. ∎

THEOREM 4.3. *Let $s \ge 2$, $b \ge 2$, and $t \ge 0$ be integers. Assume that $\mathcal{S}$ is a $(\mathbf{T}, s)$-sequence in base b with $\mathbf{T}(m) = m$ for $1 \le m \le t$, $\mathbf{T}(m) = t$ for even $m \ge t + 1$, and $\mathbf{T}(m) = t + 1$ for odd $m \ge t + 1$. Then for $N \ge 2$, the star discrepancy $D^*_N(\mathcal{S})$ of the first N terms of $\mathcal{S}$ satisfies*

$$D^*_N(\mathcal{S}) \le B_s(b, t)\,\frac{(\log N)^s}{N} + \mathcal{O}\left(\frac{(\log N)^{s-1}}{N}\right),$$

where the implied constant in the Landau symbol does not depend on N.

Here

$$B_s(b,t) = \begin{cases} \dfrac{(b-1)b^{t+s}}{2^{s+2}s!(\log b)^s} & \text{if } b \text{ is even}, \\ \dfrac{(b-1)^s(b+1)b^t}{2^{s+2}s!(\log b)^s} & \text{if } b \text{ is odd}. \end{cases}$$

Proof. For a given $N \geq 2$, let $k \in \mathbb{N}_0$ be such that $b^k \leq N < b^{k+1}$ and let $r \in \mathbb{N}_0$ be maximal such that b^r divides N. Note that $r \leq k$. In view of Lemma 4.2, we can apply [3, Lemma 2]. Putting $\mathbf{T}(0) = 0$ and $\Delta_b(0,0,s) = 1$, this yields

$$ND_N^*(\mathcal{S}) \leq \frac{b-1}{2} \sum_{m=r}^{k} \Delta_b(\mathbf{T}(m), m, s) + \frac{1}{2}\,\Delta_b(\mathbf{T}(r), r, s) + \frac{1}{2}\,\Delta_b(\mathbf{T}(k+1), k+1, s).$$

Now we use the values of $\Delta_b(t,m,s)$ in Proposition 4.1. The case $k = 0$ is trivial, and so we can assume $k \geq 1$. Then we obtain

$$ND_N^*(\mathcal{S}) \leq \frac{b-1}{2} \sum_{m=1}^{k} \Delta_b(\mathbf{T}(m), m, s) + \mathcal{O}(b^t k^{s-1}),$$

where the implied constant in the Landau symbol depends only on b and s. If b is even, then we get

$$\begin{aligned} ND_N^*(\mathcal{S}) &\leq \frac{(b-1)b^{t+s}}{(b+1)2^{s+1}(s-1)!} \sum_{\substack{m=1 \\ m \text{ even}}}^{k} m^{s-1} \\ &\quad + \frac{(b-1)b^{t+s+1}}{(b+1)2^{s+1}(s-1)!} \sum_{\substack{m=1 \\ m \text{ odd}}}^{k} m^{s-1} + \mathcal{O}(b^t k^{s-1}) \\ &\leq \frac{(b-1)b^{t+s}}{(b+1)2^{s+1}(s-1)!} \cdot \frac{k^s}{2s} + \frac{(b-1)b^{t+s+1}}{(b+1)2^{s+1}(s-1)!} \cdot \frac{k^s}{2s} + \mathcal{O}(b^t k^{s-1}) \\ &= \frac{(b-1)b^{t+s}}{2^{s+2}s!}\, k^s + \mathcal{O}(b^t k^{s-1}). \end{aligned}$$

If b is odd, then we similarly get

$$ND_N^*(\mathcal{S}) \leq \frac{(b-1)^s(b+1)b^t}{2^{s+2}s!}\, k^s + \mathcal{O}(b^t k^{s-1}).$$

Using $k \leq (\log N)/(\log b)$, we arrive at the desired result. ∎

Using Theorems 3.7 and 4.3, we obtain the following corollary.

COROLLARY 4.4. *Let $s \geq 2$ be an integer and q be a prime power. Suppose that there exists a global function field F of genus g satisfying Assump-*

tion 3.1. *Let* $\mathcal{S}$ *be the* $(\mathbf{T}, s)$*-sequence in base* q *constructed in Theorem* 3.7 *using the global function field* F*. Then, for* $N \geq 2$*, the star discrepancy* $D_N^*(\mathcal{S})$ *of the first* N *terms of* $\mathcal{S}$ *satisfies*

$$D_N^*(\mathcal{S}) \leq B_s(q,g)\,\frac{(\log N)^s}{N} + \mathcal{O}\bigg(\frac{(\log N)^{s-1}}{N}\bigg),$$

where the implied constant in the Landau symbol does not depend on N*. Here*

$$B_s(q,g) = \begin{cases} \dfrac{(q-1)q^{g+s}}{2^{s+2}s!(\log q)^s} & \text{if } q \text{ is even,} \\ \dfrac{(q-1)^s(q+1)q^g}{2^{s+2}s!(\log q)^s} & \text{if } q \text{ is odd.} \end{cases}$$

Remark 4.5. According to the currently best bound (see [2, Corollary 11]), the star discrepancy $D_N^*(\mathcal{S})$ of the first $N \geq 2$ terms of a (t,s)-sequence $\mathcal{S}$ in base b satisfies

$$D_N^*(\mathcal{S}) \leq C_s(b,t)\,\frac{(\log N)^s}{N} + \mathcal{O}\bigg(\frac{(\log N)^{s-1}}{N}\bigg),$$

where the implied constant in the Landau symbol does not depend on N and where

$$C_s(b,t) = \begin{cases} \dfrac{(b-1)b^{t+s}}{(b+1)2^{s+1}s!(\log b)^s} & \text{if } b \text{ is even,} \\ \dfrac{(b-1)^s b^t}{2^{s+1}s!(\log b)^s} & \text{if } b \text{ is odd.} \end{cases}$$

5. Examples. In this section we give some concrete examples and we illustrate our improvements by numerical results. First we give some examples of global function fields satisfying Assumption 3.1. For $d = 1, 2$, we write $N_d(F)$ for the number of places of F of degree d.

Example 5.1. Let q be any prime power, $g = 0$, $s = q+1$, and $F = \mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$. Then F is a function field with full constant field $\mathbb{F}_q$ and the genus of F is 0. Moreover, $N_1(F) = q+1$ and $N_2(F) = (q^2-q)/2$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_{q+1}(q,0)$ of the leading term in the star discrepancy bound. On the other hand, for $s = q+1$ the smallest possible t-value of a (t,s)-sequence in base q is $t = 1$ (see [6, Corollary 4.24] and Remark 3.8). By Remark 4.5, this yields the coefficient $C_{q+1}(q,1)$ of the leading term in the star discrepancy bound. It is now easily seen that $B_{q+1}(q,0) < C_{q+1}(q,1)$ for any prime power q. Thus, for any prime power q and $s = q+1$, we always get an asymptotic improvement on the previously best star discrepancy bound for a $(\mathbf{T}, s)$-sequence in base q by using the construction in Theorem 3.7.

EXAMPLE 5.2. Let $q = 3$, $g = 2$, $s = 8$, and $F = \mathbb{F}_3(x, y)$ with

$$y^2 = x^6 - x^2 + 1$$

(cf. [13, Example 3.2] and [15, Table 4.2.1, F.13]). Then F is a global function field with full constant field $\mathbb{F}_3$ and the genus of F is 2. Moreover, $N_1(F) = 8$ and $N_2(F) = 2$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_8(3, 2)$ of the leading term in the star discrepancy bound. On the other hand, the smallest known t-value of a $(t, 8)$-sequence in base 3 is $t = 3$ (see [8, Table 1] and [16]). By Remark 4.5, this yields the coefficient $C_8(3, 3)$ of the leading term in the star discrepancy bound. We have $B_8(3, 2) < C_8(3, 3)$.

EXAMPLE 5.3. Let $q = 3$, $g = 4$, $s = 12$, and $F = \mathbb{F}_3(x, y)$ with

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

(cf. [13, Example 3.4]). Then F is a global function field with full constant field $\mathbb{F}_3$ such that the genus of F is 4 and $N_1(F) = 12$. Moreover, $N_2(F) \geq 1$ since x^2+1 is totally ramified in the extension $F/\mathbb{F}_3(x)$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_{12}(3, 4)$ of the leading term in the star discrepancy bound. On the other hand, the smallest known t-value of a $(t, 12)$-sequence in base 3 is $t = 5$ (see [8, Table 1] and [16]). By Remark 4.5, this yields the coefficient $C_{12}(3, 5)$ of the leading term in the star discrepancy bound. We have $B_{12}(3, 4) < C_{12}(3, 5)$.

EXAMPLE 5.4. Let $q = 5$, $g = 1$, $s = 10$, and $F = \mathbb{F}_5(x, y)$ with

$$y^2 = 3(x^4 + 2)$$

(cf. [13, Example 5.1]). Then F is a global function field with full constant field $\mathbb{F}_5$ such that the genus of F is 1 and $N_1(F) = 10$. Moreover, $N_2(F) \geq 1$ since there is a place of F of degree 2 lying over the infinite place of the rational function field $\mathbb{F}_5(x)$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_{10}(5, 1)$ of the leading term in the star discrepancy bound. On the other hand, the smallest known t-value of a $(t, 10)$-sequence in base 5 is $t = 2$ (see [8, Table 1] and [16]). By Remark 4.5, this yields the coefficient $C_{10}(5, 2)$ of the leading term in the star discrepancy bound. We have $B_{10}(5, 1) < C_{10}(5, 2)$.

EXAMPLE 5.5. Let $q = 8$, $g = 3$, $s = 24$. Then it is shown in [14, Example 4.2] that there exists a global function field F with full constant field $\mathbb{F}_8$ such that the genus of F is 3 and $N_1(F) = 24$. Moreover, $N_2(F) \geq 1$ since it is noted in [14, Example 4.2] that x^2+x+1 is totally ramified in the extension $F/\mathbb{F}_8(x)$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_{24}(8, 3)$ of the leading term in the star discrepancy bound. On the other hand, the smallest known t-value of a $(t, 24)$-sequence in base 8

is $t = 4$ according to [16]. By Remark 4.5, this yields the coefficient $C_{24}(8, 4)$ of the leading term in the star discrepancy bound. We have $B_{24}(8, 3) < C_{24}(8, 4)$.

EXAMPLE 5.6. Let $q = 8$, $g = 7$, $s = 34$, and $F = \mathbb{F}_8(x, y_1, y_2)$ with

$$y_1^2 + y_1 = \frac{1}{x} + \frac{w(x + w^3)}{x^2 + w^5x + w}, \qquad y_2^2 + y_2 = \frac{1}{x} + \frac{w^2(x + w^6)}{x^2 + w^3x + w^2},$$

where $w \in \mathbb{F}_8$ with $w^3 + w + 1 = 0$ (cf. [17]). Then F is a global function field with full constant field $\mathbb{F}_8$ and the genus of F is 7. Moreover, $N_1(F) = 34$ and $N_2(F) = 14$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_{34}(8, 7)$ of the leading term in the star discrepancy bound. On the other hand, the smallest known t-value of a $(t, 34)$-sequence in base 8 is $t = 8$ according to [16]. By Remark 4.5, this yields the coefficient $C_{34}(8, 8)$ of the leading term in the star discrepancy bound. We have $B_{34}(8, 7) < C_{34}(8, 8)$.

EXAMPLE 5.7. Let $q = 9$, $g = 5$, $s = 32$, and $F = \mathbb{F}_9(x, y_1, y_2, y_3)$ with

$$\begin{aligned} y_1^2 &= x(x + w), \\ y_2^2 &= (x + 1)(x + w^3), \\ y_3^2 &= (x + w^6)(x + w^7), \end{aligned}$$

where $w \in \mathbb{F}_9$ with $w^2 + 2w + 2 = 0$ (cf. [17]). Then F is a global function field with full constant field $\mathbb{F}_9$ and the genus of F is 5. Moreover, $N_1(F) = 32$ and $N_2(F) = 12$. Therefore F satisfies Assumption 3.1. By Corollary 4.4, we obtain the coefficient $B_{32}(9, 5)$ of the leading term in the star discrepancy bound. On the other hand, the smallest known t-value of a $(t, 32)$-sequence in base 9 is $t = 6$ according to [16]. By Remark 4.5, this yields the coefficient $C_{32}(9, 6)$ of the leading term in the star discrepancy bound. We have $B_{32}(9, 5) < C_{32}(9, 6)$.

Table 1. Numerical comparison of our improvements for some values

s	q	$C_s(q)$	$B_s(q)$
3	2	0.166821150	0.125115863
4	3	0.0429044370	0.0286029580
5	4	0.0624989462	0.0390618414
6	5	0.0127862185	0.00767173109
8	3	0.000157782061	0.000105188041
12	3	$8.20551574 \times 10^{-8}$	$5.47034383 \times 10^{-8}$
10	5	$3.02485570 \times 10^{-5}$	$1.81491342 \times 10^{-5}$
24	8	$1.69121346 \times 10^{-14}$	$9.51307572 \times 10^{-15}$
34	8	$1.00979263 \times 10^{-22}$	$5.68008355 \times 10^{-23}$
32	9	$2.13890104 \times 10^{-22}$	$1.18827836 \times 10^{-22}$

For a prime power q and an integer $s \geq 2$, let $C_s(q) = C_s(q, t_0)$ with the smallest currently known t-value t_0 of a (t, s)-sequence in base q according to [16]. Let $B_s(q) = B_s(q, g)$ with g as in the examples above. In Table 1, we illustrate our improvements by comparing $C_s(q)$ and $B_s(q)$ numerically using Examples 5.1– 5.7.

Acknowledgments. This research was supported by the DSTA grant R-394-000-025-422 with Temasek Laboratories in Singapore. The second author would like to express his thanks to Temasek Laboratories and the Department of Mathematics at the National University of Singapore for the hospitality.

References

[1] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Amer. Math. Soc., Providence, RI, 1951.

[2] P. Kritzer, *Improved upper bounds on the star discrepancy of* (t, m, s)*-nets and* (t, s)*-sequences*, J. Complexity 22 (2006), 336–347.

[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] D. J. S. Mayor and H. Niederreiter, *A new construction of* (t, s)*-sequences and some improved bounds on their quality parameter*, Acta Arith. 128 (2007), 177–191.

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

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

[7] —, *High-dimensional numerical integration*, in: Applied Mathematics Entering the 21st Century: Invited Talks from the ICIAM 2003 Congress, J. M. Hill and R. Moore (eds.), SIAM, Philadelphia, 2004, 337–351.

[8] —, *Constructions of* (t, m, s)*-nets and* (t, s)*-sequences*, Finite Fields Appl. 11 (2005), 578–600.

[9] —, *Nets*, (t, s)*-sequences*, *and codes*, in: Monte Carlo and Quasi-Monte Carlo Methods 2006, A. Keller, S. Heinrich, and H. Niederreiter (eds.), Springer, Berlin, to appear.

[10] H. Niederreiter and F. Özbudak, *Constructions of digital nets using global function fields*, Acta Arith. 105 (2002), 279–302.

[11] H. Niederreiter and G. Pirsic, *Duality for digital nets and its applications*, ibid. 97 (2001), 173–182.

[12] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[13] —, —, *Cyclotomic function fields*, *Hilbert class fields*, *and global function fields with many rational places*, Acta Arith. 79 (1997), 59–76.

[14] —, —, *Algebraic curves with many rational points over finite fields of characteristic* 2, in: Number Theory in Progress, K. Győry, H. Iwaniec, and J. Urbanowicz (eds.), de Gruyter, Berlin, 1999, 359–380.

[15] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.
[16] R. Schürer and W. Ch. Schmid, *MinT: A database for optimal net parameters*, in: Monte Carlo and Quasi-Monte Carlo Methods 2004, H. Niederreiter and D. Talay (eds.), Springer, Berlin, 2006, 457–469; updated online at http://mint.sbg.ac.at.
[17] S. Sémirat, 2-*extensions with many points*, arXiv:math.NT/0011067v1.
[18] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[19] C. P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.

Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543, Republic of Singapore
E-mail: nied@math.nus.edu.sg

Temasek Laboratories
National University of Singapore
5 Sports Drive 2
Singapore 117508, Republic of Singapore
and
Department of Mathematics
Middle East Technical University
Ankara 06531, Turkey
E-mail: ozbudak@metu.edu.tr

Received on 20.3.2007
and in revised form on 29.6.2007 (5415)