ACTA ARITHMETICA
128.2 (2007)

A new construction of (t, s)-sequences and some improved bounds on their quality parameter

by

David J. S. Mayor and Harald Niederreiter (Singapore)

1. Introduction. For a given dimension $s \geq 1$, let J be a subinterval of $[0,1]^s$ and let $\mathtt{x}_1, \ldots, \mathtt{x}_N$ be a multiset of points in $[0,1]^s$. We write $A(J; \mathtt{x}_1, \ldots, \mathtt{x}_N)$ for the number of integers n with $1 \leq n \leq N$ for which $\mathtt{x}_n \in J$ and put

$$D_N^*(\mathtt{x}_1, \ldots, \mathtt{x}_N) = \sup_J \left| \frac{A(J; \mathtt{x}_1, \ldots, \mathtt{x}_N)}{N} - \mathrm{Vol}(J) \right|,$$

where the supremum is extended over all subintervals J of $[0,1]^s$ with one vertex at the origin. For a sequence S of points $\mathtt{x}_1, \mathtt{x}_2, \ldots$ in $[0,1]^s$, the *star discrepancy* of the first N terms of S is defined as $D_N^*(S) = D_N^*(\mathtt{x}_1, \ldots, \mathtt{x}_N)$. We say that S is a *low-discrepancy sequence* if

$$D_N^*(S) = O(N^{-1}(\log N)^s) \quad \text{for all } N \geq 2.$$

This is conjectured to be the least possible order of magnitude of the star discrepancy that can be obtained, and the conjecture has been proved for $s = 1$ by Schmidt [21] (see also [8, Section 2.2]).

Currently, the most powerful methods of constructing low-discrepancy sequences are built on the theory of (t, s)-sequences which was developed by Niederreiter [11] on the basis of earlier work by Sobol' [24] and Faure [3]. We refer to the monographs [13, Chapter 4] and [20, Chapter 8] as well as to the recent survey article [14] for general background on this theory. The fact that, for any integers $s \geq 1$ and $b \geq 2$, there exists a (t, s)-sequence in base b for some integer $t \geq 0$ was first shown by Niederreiter [12].

The star discrepancy of a (t, s)-sequence S in base b satisfies the following bound (see [11] and [13, Chapter 4]):

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

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

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

where

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

The nonnegative integer t is called the *quality parameter* of the sequence. It is clear from (1) that smaller values of t lead to smaller bounds on the star discrepancy of a (t,s)-sequence in a fixed base b and for a fixed dimension s. Therefore it is of great interest to consider the number $t_b(s)$ which is defined to be the least value of t such that there exists a (t,s)-sequence in base b.

Niederreiter and Xing collaborated on a series of papers [15], [16], [17], [26] which used global function fields to produce (t,s)-sequences. The last three of these constructions showed that $t_b(s) = O(s)$, which is the best possible asymptotic bound for $s \to \infty$ and fixed b in view of [17, Theorem 8]. Putting $C_b(s) := C_b(s, t_b(s))$, we deduce from (1) and Stirling's formula that

$$\limsup_{s\to\infty} \frac{\log C_b(s) + s(\log s - 1)}{s} = C(b) := \log b \cdot \limsup_{s\to\infty} \frac{t_b(s)}{s} + \log \frac{\lfloor b/2 \rfloor}{\log b}.$$

Therefore, using $t_b(s) = O(s)$ we see that, for fixed b, the coefficient of the leading term of the bound on the star discrepancy of a $(t_b(s), s)$-sequence in base b converges to 0 at a superexponential rate as $s \to \infty$.

In this paper we fulfill several objectives. Firstly, we introduce a new construction of (t,s)-sequences using global function fields (see Section 3). It will be analogous to the construction of Xing and Niederreiter [26] which uses places of arbitrary degree to produce the strongest construction. However, in contrast to the previous constructions which used functions in a Riemann–Roch space, our construction will employ differentials. In the decade since the last construction of (t,s)-sequences using global function fields, there has been progress in the area of global function fields with many rational places. In Sections 4 and 5 of this paper we show that these new developments have implications for the quality parameter of (t,s)-sequences. Finally, we demonstrate in Section 6 that these results lead to improved bounds on the quantity $C(b)$ introduced above.

2. Global function fields and (t,s)-sequences. In this section we recall some basic facts on global function fields and (t,s)-sequences. Concerning algebraic function fields, we mostly follow the terminology and notation in the book [25].

We write $F/\mathbb{F}_q$ for a global function field F with full constant field $\mathbb{F}_q$ and we denote by $\mathbf{P}_F$ the set of places of F. For a global function field $F/\mathbb{F}_q$, we define its set of *differentials* as

$$\Omega_F = \{xdz : x \in F,\ z \text{ is a separating element for } F/\mathbb{F}_q\},$$

and for any differential $\omega \in \Omega_F$ and separating element z we can write

$\omega = x\,dz$ with a unique $x \in F$. If ω is a nonzero differential, then for every $P \in \mathbf{P}_F$ let $\omega = x_P\,dt_P$ where t_P is a local parameter at P (and hence a separating element). Then we can associate ω with the divisor

$$(\omega) := \sum_{P \in \mathbf{P}_F} \nu_P((\omega))P := \sum_{P \in \mathbf{P}_F} \nu_P(x_P)P,$$

which is meaningful since it is independent of the choices of t_P. Here ν_P denotes the normalized valuation of F corresponding to the place P.

For any divisor D of F, we define the following sets of functions and differentials:

$$\mathcal{L}(D) = \{f \in F^* : \operatorname{div}(f) \geq -D\} \cup \{0\},$$
$$\Omega(D) = \{\omega \in \Omega_F \setminus \{0\} : (\omega) \geq D\} \cup \{0\}.$$

Both $\mathcal{L}(D)$ and $\Omega(D)$ are finite-dimensional vector spaces over $\mathbb{F}_q$ and their dimensions are related by the identity

$$\dim \Omega(D) = \dim \mathcal{L}(D) - \deg(D) + g - 1,$$

where g is the genus of F.

For $r \geq 1$, we let $B_r(F/\mathbb{F}_q)$ be the number of places of $F/\mathbb{F}_q$ of degree r. Let $N(F/\mathbb{F}_q) := B_1(F/\mathbb{F}_q)$ be the number of rational places of $F/\mathbb{F}_q$. For a given prime power q and an integer $g \geq 0$, we let $N_q(g)$ be the maximum number of rational places that a global function field $F/\mathbb{F}_q$ of genus g can have. Finally, we let $g(F/\mathbb{F}_q)$ be the genus of a global function field $F/\mathbb{F}_q$.

Most of the known constructions of (t, s)-sequences are based on the so-called digital method, which was developed by Niederreiter [11]. We refer to (t, s)-sequences which are constructed via the digital method as *digital (t, s)-sequences*, and we define $d_q(s)$ to be the least value of t such that there exists a digital (t, s)-sequence constructed over $\mathbb{F}_q$. We trivially have $t_q(s) \leq d_q(s)$, but it is not known whether there exist q and s such that $t_q(s) < d_q(s)$. We do not replicate the digital method here, since for our construction we only need Proposition 2.1 below.

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

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

which are collected in the two-parameter system

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

For $m \geq 1$ 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 put

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

Then we have the following result which is a consequence of [20, Theorem 8.2.10].

PROPOSITION 2.1. *The system $C^{(\infty)}$ can be used to construct a digital (t,s)-sequence over $\mathbb{F}_q$ if, for any $m > t$ and any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = m - t$, the vectors $\pi_m(\mathbf{c}_j^{(i)}) \in C^{(m)}$, $1 \le j \le d_i$, $1 \le i \le s$, are linearly independent over $\mathbb{F}_q$.*

3. The new construction of sequences. In this section we introduce the first new construction of (t,s)-sequences using global function fields since the construction of Niederreiter and Xing [17]. It is the first to make use of differentials, and it is based on the most general construction of (t,s)-sequences using global function fields due to Xing and Niederreiter [26].

Let $F/\mathbb{F}_q$ be a global function field of genus g and with at least one rational place P_∞. Let D be a divisor of F with $\deg(D) = -2$ and $P_\infty \notin \operatorname{supp}(D)$. Furthermore, let $P_1, \ldots, P_s$ be distinct places of F with $P_i \neq P_\infty$ for $1 \le i \le s$, and put $e_i = \deg(P_i)$ for $1 \le i \le s$.

Note that the Riemann–Roch theorem can be used to show that we have $\dim \Omega(D) = g + 1$, $\dim \Omega(D + P_\infty) = g$, and $\dim \Omega(D + (2g+1)P_\infty) = 0$. Hence there exist integers $0 = n_0 < n_1 < \cdots < n_g \le 2g$ such that

$$\dim \Omega(D + n_u P_\infty) = \dim \Omega(D + (n_u + 1)P_\infty) + 1 \quad \text{for } 0 \le u \le g.$$

Now we choose

$$w_u \in \Omega(D + n_u P_\infty) \setminus \Omega(D + (n_u + 1)P_\infty) \quad \text{for } 0 \le u \le g.$$

It is easily seen that $\{w_0, w_1, \ldots, w_g\}$ is a basis of $\Omega(D)$. For $i = 1, \ldots, s$, consider the chain

$$\Omega(D) \subset \Omega(D - P_i) \subset \Omega(D - 2P_i) \subset \cdots$$

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

$$\{w_0, w_1, \ldots, w_g, \omega_1^{(i)}, \omega_2^{(i)}, \ldots, \omega_{ne_i}^{(i)}\}$$

of $\Omega(D - nP_i)$.

Now let z be a local parameter at P_∞. For $r = 0, 1, \ldots$ we put

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

Note that $\nu_{P_\infty}((z_r)) = r$ for all $r \ge 0$. For $1 \le i \le s$ and $j \ge 1$, we have $\omega_j^{(i)} \in \Omega(D - kP_i)$ for some $k \ge 1$ and also $P_\infty \notin \operatorname{supp}(D - kP_i)$, hence

$\nu_{P_\infty}((\omega_j^{(i)})) \geq 0$. Thus, we have expansions at P_∞ of the form

$$\omega_j^{(i)} = \sum_{r=0}^{\infty} a_{r,j}^{(i)} z_r \quad \text{for } 1 \leq i \leq s \text{ and } j \geq 1,$$

where all coefficients $a_{r,j}^{(i)} \in \mathbb{F}_q$. For $1 \leq i \leq s$ and $j \geq 1$, we define the sequence of elements $c_{r,j}^{(i)} \in \mathbb{F}_q$, $r = 0, 1, \ldots$, by considering the sequence of elements $a_{r,j}^{(i)}$, $r = 0, 1, \ldots$, and then deleting the terms with $r = n_u$ for some $u \in \{0, 1, \ldots, g\}$. Finally, we set up the system

$$C^{(\infty)} = \{\mathbf{c}_j^{(i)} = (c_{0,j}^{(i)}, c_{1,j}^{(i)}, \ldots) \in \mathbb{F}_q^{\infty} : 1 \leq i \leq s \text{ and } j \geq 1\}.$$

We write $S_\Omega(P_\infty, P_1, \ldots, P_s; D)$ for a sequence obtained from this system by the digital method.

THEOREM 3.1. *Let $F/\mathbb{F}_q$ be a global function field of genus g and with at least one rational place P_∞, let D be a divisor of F with* $\deg(D) = -2$ *and $P_\infty \notin \operatorname{supp}(D)$, and let $P_1, \ldots, P_s$ be distinct places of F with $P_i \neq P_\infty$ for $1 \leq i \leq s$. Then $S_\Omega(P_\infty, P_1, \ldots, P_s; D)$ is 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 $1 \leq i \leq s$.

Proof. By Proposition 2.1, it suffices to show that for any $m > t$ and any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = m - t$, the vectors

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

are linearly independent over $\mathbb{F}_q$. Fix integers $m, d_1, \ldots, d_s$ satisfying the above conditions. Let H be the set of i with $1 \leq i \leq s$ for which $d_i \geq 1$, and suppose that we have

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

for some $b_j^{(i)} \in \mathbb{F}_q$. With $R = \{n_0, n_1, \ldots, n_g\}$ this means that

$$\sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} a_{r,j}^{(i)} = 0 \tag{2}$$

for the first m nonnegative integers r that are not in R. Now consider the

differential ω of F given by

$$\omega = \sum_{i\in H}\sum_{j=1}^{d_i} b_j^{(i)}\Big(\omega_j^{(i)} - \sum_{u=0}^{g} a_{n_u,j}^{(i)} w_u\Big) = \sum_{\substack{r=0\\ r\notin R}}^{\infty}\Big(\sum_{i\in H}\sum_{j=1}^{d_i} b_j^{(i)} a_{r,j}^{(i)}\Big) z_r.$$

Since $n_g \le 2g$ and $g \le m-1$, we have $\nu_{P_\infty}((\omega)) \ge m+g+1$ by (2), and together with the choice of the $\omega_j^{(i)}$ this shows that

$$\omega \in \Omega\bigg(D - \sum_{i=1}^{s}\bigg(\bigg\lfloor \frac{d_i-1}{e_i}\bigg\rfloor + 1\bigg)P_i + (m+g+1)P_\infty\bigg).$$

Note that

$$\begin{aligned}\deg\bigg(D - \sum_{i=1}^{s}\bigg(\bigg\lfloor \frac{d_i-1}{e_i}\bigg\rfloor + 1\bigg)P_i + (m+g+1)P_\infty\bigg)&\\ = -2 - \sum_{i=1}^{s}\bigg(\bigg\lfloor \frac{d_i-1}{e_i}\bigg\rfloor + 1\bigg)e_i + (m+g+1)&\\ \ge m - t - \sum_{i=1}^{s} d_i + 2g - 1 = 2g-1.&\end{aligned}$$

Therefore $\omega = 0$, and so we have

$$\sum_{i\in H}\sum_{j=1}^{d_i} b_j^{(i)}\omega_j^{(i)} =: w \in \Omega(D).$$

Fix an $h \in H$. We claim that $b_j^{(h)} = 0$ for $1 \le j \le d_h$. Suppose, on the contrary, that some $b_j^{(h)} \ne 0$. Then by choice of the $\omega_j^{(h)}$ we have

$$\sum_{j=1}^{d_h} b_j^{(h)}\omega_j^{(h)} \in \Omega(D - kP_h) \setminus \Omega(D) \quad \text{for some } k \ge 1,$$

and so

$$\nu_{P_h}\Big(\Big(\sum_{j=1}^{d_h} b_j^{(h)}\omega_j^{(h)}\Big)\Big) \le \nu_{P_h}(D) - 1.$$

However, we also know that

$$\nu_{P_h}\Big(\Big(\sum_{j=1}^{d_h} b_j^{(h)}\omega_j^{(h)}\Big)\Big) = \nu_{P_h}\Big(\Big(w - \sum_{i\in H\setminus\{h\}}\sum_{j=1}^{d_i} b_j^{(i)}\omega_j^{(i)}\Big)\Big) \ge \nu_{P_h}(D),$$

a contradiction. Thus, for any $i \in H$, we get $b_j^{(i)} = 0$ for $1 \le j \le d_i$. ∎

Remark 3.2. Note that the only condition in our construction different from that of Xing and Niederreiter [26] is that we use a divisor D with

$\deg(D) = -2$, whereas they use a divisor D' with $\deg(D') = 2g$. Such divisors can always be found and hence any global function field $F/\mathbb{F}_q$ with places $P_\infty, P_1, \ldots, P_s$ can be used to construct two different digital (t,s)-sequences over $\mathbb{F}_q$, where $t = g + \sum_{i=1}^{s}(\deg(P_i) - 1)$.

A project of cataloging upper bounds on $d_q(s)$ for $q = 2, 3, 5$ and $1 \le s \le 50$ was begun by Niederreiter and Xing (see, for example, [17, Table 4], [19, Table 5]) and has been continued by Niederreiter (see, for example, [14, Table 1]). We now provide an example which demonstrates that it is possible to use nonrational places to gain improved bounds on $d_q(s)$.

EXAMPLE 3.3. Let $F/\mathbb{F}_5$ be the global function field given in [18, Example 4], i.e., $F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x(x^2 - 2), \qquad y_2^5 - y_2 = \frac{x^4 - 1}{y_1 - 1}.$$

We have $g(F/\mathbb{F}_5) = 11$ and $N(F/\mathbb{F}_5) = 32$. Consider the place Q of $\mathbb{F}_5(x)$ corresponding to the irreducible polynomial $x^2 + 2x - 2$ over $\mathbb{F}_5$. If $\alpha \in \mathbb{F}_{25}$ is a root of $x^2 + 2x - 2$, then in $\mathbb{F}_{25}[y]$ we have the factorization

$$y^2 - \alpha(\alpha^2 - 2) = (y - \alpha + 2)(y + \alpha - 2).$$

Hence by Kummer's theorem [25, Theorem III.3.7], there is a place Q_1 of $K := \mathbb{F}_5(x, y_1)$ of degree 2 lying over Q, with $y_1 \equiv \alpha - 2 \bmod Q_1$. Next we consider the factorization of

$$f(y) := y^5 - y - \frac{\alpha^4 - 1}{(\alpha - 2) - 1} = y^5 - y - (-\alpha - 1)$$

in $\mathbb{F}_{25}[y]$. A trace calculation shows that

$$\mathrm{Tr}_{\mathbb{F}_{25}/\mathbb{F}_5}(-\alpha - 1) = -\mathrm{Tr}_{\mathbb{F}_{25}/\mathbb{F}_5}(\alpha) - 2 = 0$$

since $\mathrm{Tr}_{\mathbb{F}_{25}/\mathbb{F}_5}(\alpha) = -2$. Thus, $f(y)$ splits into five distinct monic linear factors over $\mathbb{F}_{25}$ by [10, Theorem 2.25], and so by Kummer's theorem Q_1 splits completely in the extension F/K. Therefore F contains at least five places of degree 2. Combining this with Theorem 3.1, we obtain

$$d_5(32) \le 12,$$

which is an improvement on the bound $d_5(32) \le 13$ given in [14, Table 1].

4. Explicit bounds on the quality parameter. In the next two sections, for certain values of b, we will improve the upper bound on the quantity

$$\limsup_{s \to \infty} \frac{t_b(s)}{s}$$

whose existence is implied by the result $t_b(s) = O(s)$ mentioned in Section 1. We start by introducing some explicit bounds.

We can bound $d_q(s)$ for arbitrary s by finding towers of global function fields with many places of small degree. For example, Niederreiter and Xing [16], [26] made use of the tower of global function fields due to Garcia and Stichtenoth [4], which was the first explicit tower of function fields that was asymptotically good, i.e., it is a tower $\mathcal{F} = (F_1, F_2, \ldots)$ of function fields over $\mathbb{F}_q$ satisfying the condition

$$\lim_{i\to\infty} \frac{N(F_i/\mathbb{F}_q)}{g(F_i/\mathbb{F}_q)} > 0.$$

In the decade since the last construction of (t, s)-sequences in [17], Garcia, Stichtenoth, and Thomas [6], Li, Maharaj, Stichtenoth, and Elkies [9], Garcia and Stichtenoth [5], and Bezerra, Garcia, and Stichtenoth [1] were among the mathematicians who have constructed new explicit towers which are asymptotically good. We will now utilise these new results to produce improved bounds on $d_q(s)$ for arbitrary s.

THEOREM 4.1. *For every odd prime p and every dimension $s \geq 1$ we have*

$$d_{p^2}(s) \leq \frac{2}{p-1}\, s + 1.$$

Proof. Let $F_1 \subseteq F_2 \subseteq \cdots$ be the tower of function fields over $\mathbb{F}_{p^2}$ constructed by Garcia and Stichtenoth [5], that is, for $n \geq 1$ we have

$$F_n = \mathbb{F}_{p^2}(x_1, \ldots, x_n), \quad \text{where} \quad x_{n+1}^2 = \frac{x_n^2 + 1}{2x_n}.$$

Then it is known from [5] that

$$N(F_n/\mathbb{F}_{p^2}) \geq (p-1)2^n, \qquad g(F_n/\mathbb{F}_{p^2}) \leq 2^n + 1.$$

Suppose that $1 \leq s \leq p^2$. Then $N(F_1/\mathbb{F}_{p^2}) \geq s + 1$ and hence

$$d_{p^2}(s) \leq g(F_1/\mathbb{F}_{p^2}) = 0$$

by Theorem 3.1. Now let $s \geq p^2 + 1$. Then $(p-1)2^{n-1} \leq s \leq (p-1)2^n - 1$ for some $n \geq 2$. Therefore Theorem 3.1 yields

$$d_{p^2}(s) \leq g(F_n/\mathbb{F}_{p^2}) \leq 2^n + 1 \leq \frac{2}{p-1}\, s + 1. \quad \blacksquare$$

REMARK 4.2. It is possible to obtain the bounds for $p = 5$ and $p = 7$ using earlier towers of function fields [9, Theorem 2], and it is possible to obtain the bound for $p = 3$ using two earlier towers of function fields [6, Example 2.4], [9, Theorem 2].

For odd $q = p^2$, these bounds represent improvements on the previously known theory, namely a special case of a result due to Xing and Niederreiter [26, Theorem 4] stating that for any prime p and integer $e \geq 1$ we have

$$d_{p^{2e}}(s) \leq \frac{p}{p^e - 1}\, s \quad \text{for all } s \geq 1. \tag{3}$$

EXAMPLE 4.3. For a future comparison, we note that we have proved

$$d_9(s) \le s + 1, \quad d_{25}(s) \le s/2 + 1, \quad d_{49}(s) \le s/3 + 1$$

for all $s \ge 1$.

THEOREM 4.4. *For every odd prime p and every dimension $s \ge 1$ we have*

$$d_p(s) \le \frac{p+3}{p-1}\, s + \frac{p-5}{p-1}.$$

Proof. Let $E_1 \subseteq E_2 \subseteq \cdots$ be the tower of function fields over $\mathbb{F}_p$ constructed by Garcia and Stichtenoth [5], that is, for $n \ge 1$ we have

$$E_n = \mathbb{F}_p(x_1, \ldots, x_n), \quad \text{where} \quad x_{n+1}^2 = \frac{x_n^2 + 1}{2x_n}.$$

Now let $F_n = E_n \cdot \mathbb{F}_{p^2}$. Then, because of results on constant field extensions [25, Lemma V.1.9], we know that

$$N(E_n/\mathbb{F}_p) + 2B_2(E_n/\mathbb{F}_p) = N(F_n/\mathbb{F}_{p^2}) \ge (p-1)2^n$$

and

$$g(E_n/\mathbb{F}_p) = g(F_n/\mathbb{F}_{p^2}) \le 2^n + 1.$$

Note that it is shown in [5, Proposition 4.1] that the place $1/x_1$ of E_1 is totally ramified in all extensions E_n/E_1. Hence $N(E_n/\mathbb{F}_p) \ge 1$ and therefore

$$N(E_n/\mathbb{F}_p) + B_2(E_n/\mathbb{F}_p) \ge (p-1)2^{n-1} + 1.$$

Suppose that $1 \le s \le p$. Then $N(E_1/\mathbb{F}_p) \ge s + 1$ and hence

$$d_p(s) \le g(E_1/\mathbb{F}_p) = 0$$

by Theorem 3.1. Now let $s \ge p+1$. Then $(p-1)2^{n-2} + 1 \le s \le (p-1)2^{n-1}$ for some $n \ge 2$. Therefore Theorem 3.1 yields

$$d_p(s) \le g(E_n/\mathbb{F}_p) + s \le 2^n + 1 + s \le \frac{p+3}{p-1}\, s + \frac{p-5}{p-1}. \quad \blacksquare$$

For odd primes, these bounds represent improvements on the previous best bounds. For most odd primes p, this was a special case of a result due to Xing and Niederreiter [26, Theorem 3] which says that for any prime power q and $s \ge 1$ we have

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

In particular,

$$d_3(s) \le 4s - \frac{5}{2^{1/2}}\,(s-1)^{1/2} - 2, \quad d_7(s) \le \frac{10}{3}\, s - \frac{3^{3/2}}{2}\,(s-1)^{1/2} - \frac{4}{3}$$

for all $s \ge 1$. For $q = 5$, the previous best bound was obtained by Niederreiter and Xing [20, Remark 8.4.5] who used the rational places of a Hilbert class

field tower to prove that

$$d_5(s) \le \frac{11}{4}\, s + 1 \quad \text{for all } s \ge 1.$$

EXAMPLE 4.5. For a future comparison, we note that we have proved

$$d_3(s) \le 3s - 1, \quad d_5(s) \le 2s, \quad d_7(s) \le \frac{5}{3}\, s + \frac{1}{3}$$

for all $s \ge 1$.

THEOREM 4.6. *For every prime power q and every dimension $s \ge 1$ we have*

$$d_{q^3}(s) \le \frac{q(q+2)}{2(q^2-1)}\, s.$$

Proof. Let $F_1 \subseteq F_2 \subseteq \cdots$ be the tower of function fields over $\mathbb{F}_{q^3}$ constructed by Bezerra, Garcia, and Stichtenoth [1], that is, for $n \ge 1$ we have

$$F_n = \mathbb{F}_{q^3}(x_1, \ldots, x_n), \quad \text{where} \quad \frac{1 - x_{n+1}}{x_{n+1}^q} = \frac{x_n^q + x_n - 1}{x_n}.$$

Then it is known from [1] that

$$N(F_n/\mathbb{F}_{q^3}) \ge (q+1)q^n, \quad g(F_n/\mathbb{F}_{q^3}) \le \frac{(q+2)q^n}{2(q-1)}.$$

Suppose that $1 \le s \le q^3$. Then $N(F_1/\mathbb{F}_{q^3}) \ge s+1$ and hence

$$d_{q^3}(s) \le g(F_1/\mathbb{F}_{q^3}) = 0$$

by Theorem 3.1. Now let $s \ge q^3 + 1$. Then $(q+1)q^{n-1} \le s \le (q+1)q^n - 1$ for some $n \ge 2$. Therefore Theorem 3.1 yields

$$d_{q^3}(s) \le g(F_n/\mathbb{F}_{q^3}) \le \frac{(q+2)q^n}{2(q-1)} \le \frac{q(q+2)}{2(q^2-1)}\, s. \ \blacksquare$$

For small q, these bounds can offer improvements on the previous best bounds. For example, when $q^3 = 8$ this was the result (4) of Xing and Niederreiter which in this case yields

$$d_8(s) \le \frac{23}{7}\, s - \frac{20}{3 \cdot 7^{1/2}}\, (s-1)^{1/2} - \frac{9}{7}.$$

Note that Theorem 4.6 provides the better bound

$$d_8(s) \le \frac{4}{3}\, s \quad \text{for all } s \ge 1.$$

For $q^3 = 27$, the previous best bound was obtained by Niederreiter and Xing [19, Theorem 7] who used the rational places of a Hilbert class field tower to prove that

$$d_{27}(s) \le \frac{12}{5}\, s + 1 \quad \text{for all } s \ge 1.$$

Note that Theorem 4.6 provides the better bound

$$d_{27}(s) \le \frac{15}{16}\, s \quad \text{for all } s \ge 1.$$

REMARK 4.7. Note that Theorem 4.6 is not always the strongest bound available in the cubic case. When q^3 is a square we can use (3), and in the case where q^3 is not a square, the bound could still be improved upon in many cases by using [19, Theorem 6].

Recently, a new website was launched by Schürer and Schmid [22] with the aim of cataloging (t, s)-sequences and their point set analogues, (t, m, s)-nets. The values of q for which the website is valid are 2, 3, 4, 5, 7, 8, 9, 16, 25, 27, and 32. We note that in this section we have introduced improved bounds on $d_q(s)$ for all the odd prime powers mentioned above, namely $q = 3$, 5, 7, 9, 25, and 27. Furthermore, we improved the bound for $q = 8$. The known bounds for $q = 2$, 4, and 16 seem strong, whilst the known bound for $q = 32$ is weak due to the lack of knowledge about explicit towers of function fields over $\mathbb{F}_q$ in the case where q is quintic.

5. Asymptotic bounds on the quality parameter. In all previous attempts to use global function fields to bound $d_q(s)$ for large s, the method has involved using towers of global function fields. However, it is apparent that if we can find global function fields of every genus with many rational places, then we can also gain bounds on $d_q(s)$. When Niederreiter and Xing [17] obtained their last construction of (t, s)-sequences in 1996, this was a barren area of research. Serre [23] had previously posed the question as to whether

$$\liminf_{g\to\infty} \frac{N_q(g)}{g} > 0,$$

but it was only recently that Elkies *et al.* [2] showed that the above inequality holds for every prime power q. Furthermore, in the case where q is a square, strong explicit bounds [2, Theorem 1.2 and Corollary 6.2] were obtained, which we now reproduce.

PROPOSITION 5.1. *We have*

$$\liminf_{g\to\infty} \frac{N_q(g)}{g} \ge \begin{cases} \dfrac{q^{1/2}-1}{2+\log_q 2} & \text{if } q \text{ is an even square,} \\ \dfrac{q^{1/2}-1}{2+\log_q 4} & \text{if } q \text{ is an odd square,} \\ \dfrac{2(q^{1/2}-1)}{2+(q^{1/2}+1)\cdot\log_q 2} & \text{if } q \text{ is an odd square.} \end{cases}$$

Whilst this result does not provide bounds on $d_q(s)$ for individual s, it does produce strong asymptotic bounds on $d_q(s)$. To wit, we have the following result.

COROLLARY 5.2. *We have*

$$\limsup_{s\to\infty} \frac{d_q(s)}{s} \le \begin{cases} \dfrac{2+\log_q 2}{q^{1/2}-1} & \text{if } q \text{ is an even square,} \\ \dfrac{2+\log_q 4}{q^{1/2}-1} & \text{if } q \text{ is an odd square,} \\ \dfrac{2+(q^{1/2}+1)\cdot\log_q 2}{2(q^{1/2}-1)} & \text{if } q \text{ is an odd square.} \end{cases}$$

Proof. Note that

$$\left(\liminf_{g\to\infty} \frac{N_q(g)}{g}\right)^{-1} = \limsup_{g\to\infty} \frac{g}{N_q(g)} = \limsup_{g\to\infty} \frac{g+1}{N_q(g)}.$$

Therefore it suffices to show that

$$\limsup_{s\to\infty} \frac{d_q(s)}{s} \le \limsup_{g\to\infty} \frac{g+1}{N_q(g)}. \tag{5}$$

Choose a sequence $q+1 \le s_1 < s_2 < \cdots$ of integers with

$$\lim_{i\to\infty} \frac{d_q(s_i)}{s_i} = \limsup_{s\to\infty} \frac{d_q(s)}{s}.$$

For each $i = 1, 2, \ldots$, let g_i be the least nonnegative integer such that

$$N_q(g_i) \le s_i \quad \text{and} \quad N_q(g_i+1) \ge s_i + 1.$$

Then $d_q(s_i) \le g_i + 1$ by Theorem 3.1, and so

$$\frac{d_q(s_i)}{s_i} \le \frac{g_i+1}{N_q(g_i)}.$$

Since $g_i \to \infty$ as $i \to \infty$, we obtain (5) by letting $i \to \infty$. ∎

We know by (3) that if we have $q = p^{2e}$ where p is a prime and $e \ge 1$ is an integer, then

$$d_q(s) \le \frac{p}{q^{1/2}-1}\, s \quad \text{for all } s \ge 1.$$

Hence, we gain no improvement for even values of q. However, for odd values of q we can obtain improvements.

EXAMPLE 5.3. Corollary 5.2 provides the bounds

$$\limsup_{s\to\infty} \frac{d_9(s)}{s} \le \frac{1}{2} + \log_9 2 = 0.8154\ldots,$$

$$\limsup_{s\to\infty} \frac{d_{25}(s)}{s} \le \frac{1}{4} + \frac{3}{4}\log_{25} 2 = 0.4115\ldots,$$

$$\limsup_{s\to\infty} \frac{d_{49}(s)}{s} \le \frac{1}{6} + \frac{2}{3}\log_{49} 2 = 0.2854\ldots.$$

Note that these bounds offer asymptotic improvements on the new results presented in Example 4.3.

EXAMPLE 5.4. We note a result of Niederreiter and Xing [16, Proposition 4] which states that for all integers $b \ge 2$, $h \ge 1$, and $s \ge 1$ we have

$$t_b(s) \le h t_{b^h}(s) + (h-1)s.$$

Hence, we also gain the bounds

$$\limsup_{s\to\infty} \frac{t_3(s)}{s} \le 2(1 + \log_9 2) = 2.6309\ldots,$$
$$\limsup_{s\to\infty} \frac{t_5(s)}{s} \le \frac{3}{2}(1 + \log_{25} 2) = 1.8230\ldots,$$
$$\limsup_{s\to\infty} \frac{t_7(s)}{s} \le \frac{4}{3}(1 + \log_{49} 2) = 1.5708\ldots.$$

Note that these bounds offer asymptotic improvements on the new results presented in Example 4.5.

6. Implications for the star discrepancy. In this section we examine the quantity

$$C(b) = \log b \cdot \limsup_{s\to\infty} \frac{t_b(s)}{s} + \log \frac{\lfloor b/2 \rfloor}{\log b},$$

which was introduced in Section 1. We start by noting the best currently known bounds for some interesting values of b:

$$\begin{array}{lll} C(2) \le 3.8323, & C(8) \le 3.4268, & C(27) \le 4.4622, \\ C(3) \le 2.7964, & C(9) \le 2.3909, & C(32) \le 5.4426, \\ C(4) \le 3.1392, & C(11) \le 4.0283, & C(49) \le 2.9300, \\ C(5) \le 3.1513, & C(16) \le 2.9081, & C(64) \le 3.2288, \\ C(7) \le 3.4896, & C(25) \le 2.6405, & C(81) \le 3.1911. \end{array}$$

Hence, the value of b which currently provides the strongest bound on the star discrepancy of a low-discrepancy sequence for high dimensions is $b = 9$, where we have

$$C(9) \le \log 12 - \log\log 3 = 2.3908\ldots$$

by Example 5.3.

REMARK 6.1. There is currently no prior research on the quantity $C(b)$ available in the literature. However, using previously known bounds on $t_b(s)$, the best bound that could be obtained for $C(b)$ was in the case $b = 16$, where

we have

$$\limsup_{s\to\infty} \frac{d_{16}(s)}{s} \le \frac{2}{3}$$

by (3) and hence

$$C(16) \le \frac{11}{3}\log 2 - \log\log 2 = 2.9080\ldots.$$

Thus, the new bound on $C(9)$ reported above yields an improvement.

REMARK 6.2. Note that the weaker explicit bound for $d_9(s)$ presented in Example 4.3 would also have produced a stronger bound than that for $b = 16$.

REMARK 6.3. Recently, the function $C_b(s,t)$ that was provided by Niederreiter in (1) has been improved upon by Kritzer [7], who replaced $C_b(s,t)$ with a function $F_b(s,t)$ which provides a stronger bound. However, this does not affect our asymptotic analysis, as it is easily seen that

$$\limsup_{s\to\infty} \frac{\log C_b(s,t_b(s)) + s\log s}{s} = \limsup_{s\to\infty} \frac{\log F_b(s,t_b(s)) + s\log s}{s}.$$

References

[1] J. Bezerra, A. Garcia, and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. 589 (2005), 159–199.

[2] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell, and M. E. Zieve, *Curves of every genus with many points. II. Asymptotically good families*, Duke Math. J. 122 (2004), 399–422.

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

[4] A. Garcia and H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound*, Invent. Math. 121 (1995), 211–222.

[5] —, —, *On tame towers over finite fields*, J. Reine Angew. Math. 557 (2003), 53–80.

[6] A. Garcia, H. Stichtenoth, and M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. 3 (1997), 257–274.

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

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

[9] W.-C. W. Li, H. Maharaj, H. Stichtenoth, and N. D. Elkies, *New optimal tame towers of function fields over small finite fields*, in: Algorithmic Number Theory, C. Fieker and D. R. Kohel (eds.), Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 372–389.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997.

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

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

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

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

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

[16] —, —, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[17] —, —, *Quasirandom points and global function fields*, in: Finite Fields and Applications, S. Cohen and H. Niederreiter (eds.), London Math. Soc. Lecture Note Ser. 233, Cambridge Univ. Press, Cambridge, 1996, 269–296.

[18] —, —, *Global function fields with many rational places over the quinary field*, Demonstratio Math. 30 (1997), 919–930.

[19] —, —, *Nets, (t, s)-sequences, and algebraic geometry*, in: Random and Quasi-Random Point Sets, P. Hellekalek and G. Larcher (eds.), Lecture Notes in Statist. 138, Springer, New York, 1998, 267–302.

[20] —, —, *Rational Points on Curves over Finite Fields: Theory and Applications*, London Math. Soc. Lecture Note Ser. 285, Cambridge Univ. Press, Cambridge, 2001.

[21] W. M. Schmidt, *Irregularities of distribution. VII*, Acta Arith. 21 (1972), 45–50.

[22] 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`.

[23] J.-P. Serre, *Nombres de points des courbes algébriques sur $\mathbb{F}_q$*, in: Séminaire de Théorie des Nombres 1982–1983, Université de Bordeaux I, Talence, 1983, Exp. No. 22.

[24] I. M. Sobol', *Distribution of points in a cube and approximate evaluation of integrals*, Zh. Vychisl. Mat. Mat. Fiz. 7 (1967), 784–802 (in Russian); English transl.: USSR Comput. Math. Math. Phys. 7 (1967), no. 4, 86–112.

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

[26] 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: david.mayor@nus.edu.sg
nied@math.nus.edu.sg

Received on 3.11.2006 (5311)