We construct digital \((t, s)\)-sequences in a prime-power base \(q\) for which the quality parameter \(t\) has the least possible order of magnitude. The construction uses algebraic function fields over the finite field of order \(q\) which contain many places of degree 1 relative to the genus.

fields. Then a new method using global function fields was sketched by Niederreiter [16, 17] and worked out in detail and in an improved form by Niederreiter and Xing [18]. This method yields some improvements on the earlier construction in [13].

In the present paper we introduce a new way of using global function fields for the construction of \((t, s)\)-sequences. The key idea is to work with global function fields containing many places of degree 1. This method yields significantly better results than all previous methods. In fact, we will show that the \((t, s)\)-sequences obtained by this method are, in a sense, asymptotically optimal (see Section 5).

With regard to low-discrepancy point sets and sequences we follow the notation and terminology in the book of Niederreiter [15]. For \(s \geq 1\) let \(I^s = [0, 1)^s\) be the half-open \(s\)-dimensional unit cube. The following concept is fundamental. For integers \(b \geq 2\) and \(0 \leq t \leq m\), a \((t, m, s)\)-net in base \(b\) is a point set consisting of \(b^m\) points in \(I^t\) such that every subinterval \(J\) of \(I^t\) 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 of volume \(b^{t-m}\) contains exactly \(b^t\) points of the point set. The number \(t\) is sometimes called the “quality parameter” or “uniformity parameter.” Clearly, smaller values of \(t\) mean stronger uniformity properties of the net.

The sequence analogs of \((t, m, s)\)-nets are the \((t, s)\)-sequences to be defined in Section 2. We concentrate mainly on the most important family of \((t, s)\)-sequences, namely digital \((t, s)\)-sequences constructed over finite rings. Within this family, the crucial case is the one where the finite ring is a finite field \(F_q\) of order \(q\). In Section 3 we describe our new class of digital \((t, s)\)-sequences constructed over \(F_q\) which is obtained from global function fields over \(F_q\). By optimizing this construction, we get digital \((V_q(s), s)\)-sequences constructed over \(F_q\) for every dimension \(s\) and every prime power \(q\), where the quality parameter \(V_q(s)\) depends only on \(q\) and \(s\). The construction yields, in particular, \((t, m, s)\)-nets in base \(q\) with \(t\) independent of \(m\). A detailed study of the quantity \(V_q(s)\) is carried out in Section 4. Using results on class field towers of global function fields, we show that for fixed \(q\) we have \(V_q(s) = O(s)\) as \(s \to \infty\). According to a lower bound in Section 5, this is the best possible order of magnitude for the quality parameter in the family of digital \((t, s)\)-sequences. In all previous constructions the quality parameter grows at least like \(s \log s\) as \(s \to \infty\). In Section 5 we also derive consequences for digital \((t, s)\)-sequences constructed over finite rings. In Section 6 we introduce an elementary principle which leads to further improvements on some bounds.
2. Digital Constructions Over Finite Rings

The digital method for the construction of \((t, m, s)\)-nets and \((t, s)\)-sequences was introduced in [12, Section 6]; compare also with [15, Section 4.3]. We fix a commutative ring \(R\) with identity and of finite order \(b \geq 2\). We write \(Z_b = \{0, 1, \ldots, b - 1\}\) for the least residue system mod \(b\). If the integers \(m \geq 1\) and \(s \geq 1\) are given, then the construction of \((t, m, s)\)-nets in base \(b\) by the digital method proceeds by choosing the following:

(N1) bijections \(\psi_r: Z_b \rightarrow R\) for \(0 \leq r \leq m - 1\);
(N2) bijections \(\eta_i^{(1)}: R \rightarrow Z_b\) for \(1 \leq i \leq s\) and \(1 \leq j \leq m\);
(N3) elements \(c_{i,j}^{(1)} \in R\) for \(1 \leq i \leq s\), \(1 \leq j \leq m\), and \(0 \leq r \leq m - 1\).

For \(n = 0, 1, \ldots, b^m - 1\) let

\[
n = \sum_{r=0}^{m-1} a_r(n)b^r \quad \text{with all } a_r(n) \in Z_b
\]

be the digit expansion of \(n\) in base \(b\). We put

\[
x_n^{(i)} = \sum_{j=1}^{m} y_{n,j}^{(i)} b^{-j} \quad \text{for } 0 \leq n < b^m \text{ and } 1 \leq i \leq s,
\]

with

\[
y_{n,j}^{(i)} = \eta_i^{(1)} \left( \sum_{r=0}^{m-1} c_{i,j}^{(1)} \psi_r(a_r(n)) \right) \in Z_b \quad \text{for } 0 \leq n < b^m, 1 \leq i \leq s, 1 \leq j \leq m,
\]

and define the point set

\[
x_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in I^s \quad \text{for } n = 0, 1, \ldots, b^m - 1.
\]

If this point set is a \((t, m, s)\)-net in base \(b\), then it is called a digital \((t, m, s)\)-net constructed over \(R\).

Before we describe the digital method for the construction of sequences, we introduce further notation. Let \(I^s\) denote the closed \(s\)-dimensional unit cube. Given a base \(b \geq 2\) and a real number \(x \in [0, 1]\), let

\[
x = \sum_{j=1}^{\infty} y_j b^{-j} \quad \text{with all } y_j \in Z_b
\]
be a $b$-adic expansion of $x$, where the case $y_j = b - 1$ for almost all $j$ is allowed. For an integer $m \geq 1$ we define the truncation

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

It should be emphasized that this truncation operates on the expansion of $x$ and not on $x$ itself, since it may yield different results depending on which $b$-adic expansion of $x$ is used. If $\mathbf{x} = (x^{(1)}, \ldots, x^{(s)}) \in \mathcal{T}'$ and the $x^{(i)}$, $1 \leq i \leq s$, are given by prescribed $b$-adic expansions, then we define

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

Note that we always have $[\mathbf{x}]_{b,m} \in \mathcal{T}'$.

Now we fix again a ring $R$ as above with $|R| = b$. For a given dimension $s \geq 1$ we choose the following:

1. bijections $\psi_r: Z \to R$ for $r \geq 0$, with $\psi_r(0) = 0$ for all sufficiently large $r$;
2. bijections $\eta^{(i)}_j: R \to Z_b$ for $1 \leq i \leq s$ and $j \geq 1$;
3. elements $c^{(i)}_{j,r} \in R$ for $1 \leq i \leq s$, $j \geq 1$, and $r \geq 0$.

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

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

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

$$x^{(i)}_n = \sum_{j=1}^{\infty} y^{(i)}_{n,j} b^{-j} \quad \text{for } n \geq 0 \text{ and } 1 \leq i \leq s,$$

with

$$y^{(i)}_{n,j} = \eta^{(i)}_j \left( \sum_{r=0}^{\infty} c^{(i)}_{j,r} \psi_r(a_r(n)) \right) \in Z_b \quad \text{for } n \geq 0, 1 \leq i \leq s, \text{ and } j \geq 1.$$
Note that the sum over \( r \) is always a finite sum. Now we define the sequence

\[
x_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in \mathbb{T}^s \quad \text{for } n = 0, 1, \ldots
\]  

**Definition 1.** Let \( t \geq 0 \) be an integer. If the sequence in (2) has the property that for all integers \( k \geq 0 \) and \( m > t \) the points \([x_n]_{b,m}\) with \( kb^m \leq n < (k + 1)b^m \) form a \((t, m, s)\)-net in base \( b \), then the sequence in (2) is called a digital \((t, s)\)-sequence constructed over \( R \). Here the truncations are required to operate on the expansions in (1). A sequence which is a digital \((t, s)\)-sequence constructed over \( R \) for some \( R \) of order \( b \) is called a digital \((t, s)\)-sequence in base \( b \).

**Remark 1.** This definition differs slightly from that of a \((t, s)\)-sequence in base \( b \) given in [15, Definition 4.2]. The latter definition postulates that the original points \( x_n \) with \( kb^m \leq n < (k + 1)b^m \) rather than the truncated points \([x_n]_{b,m}\) form a \((t, m, s)\)-net in base \( b \). The reason for the changed definition is that now we do not require any supplementary conditions in the digital method. In the earlier approach in [15, Section 4.3], the following additional condition had to be imposed in the digital method: for each \( n \geq 0 \) and \( 1 \leq i \leq s \) we have \( y_{n,i}^{(i)} \leq b - 1 \) for infinitely many \( j \). It is clear that if a sequence satisfying this condition is a \((t, s)\)-sequence in base \( b \) in the sense of [15, Definition 4.2], then it is also a digital \((t, s)\)-sequence constructed over \( R \) in the sense of Definition 1 above. In [12, Section 6], the following even more restrictive condition was imposed on the elements \( c_{ij}^{(i)} \) in (S3): for any fixed \( i \) and \( r \) we must have \( c_{ij}^{(i)} = 0 \) for all sufficiently large \( j \). This condition is satisfied, for instance, in the construction of \((t, s)\)-sequences introduced in [13], but it leads to the unpleasant “leading-zeros phenomenon” pointed out by Bratley *et al.* [1]. Thus, there are some practical advantages in our present setup. For similar reasons, namely in order to avoid any conditions on the \( y_{n,i}^{(i)} \) or \( c_{ij}^{(i)} \), the operation of truncation was already used by Tezuka [27] in the theory of \((t, s)\)-sequences.

The following lemma, which is a variant of [12, Lemma 5.15], shows a simple but important connection between digital nets and digital sequences constructed over the same ring.

**Lemma 1.** If there exists a digital \((t, s)\)-sequence constructed over \( R \), then for every integer \( m \geq t \) there exists a digital \((t, m, s + 1)\)-net constructed over \( R \).

**Proof.** Let \( x_0, x_1, \ldots \) be a digital \((t, s)\)-sequence constructed over the ring \( R \) with \( |R| = b \). For fixed \( m \geq t \) consider the points
\[ y_n = \left( \left[ x_n \right]_{b,m}, \frac{n}{b^m} \right) \in P^{s+1} \quad \text{for } n = 0, 1, \ldots, b^m - 1. \]

We first prove that these points form a \((t, m, s + 1)\)-net in base \(b\). Let

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

be a subinterval of \(P^{s+1}\) with integers \(d_i \geq 0\) and \(0 \leq a_i < b^{d_i}\) for \(1 \leq i \leq s\) and of volume \(b^{t-m}\); hence \(\Sigma_{i=1}^{s+1} d_i \geq m - t\). Then \(y_n \in J\) if and only if \(a_{s+1}b^{m-d_{s+1}} \leq n < (a_{s+1} + 1)b^{m-d_{s+1}}\) and

\[ \left[ x_n \right]_{b,m} \in J' := \prod_{i=1}^{s} [a_i b^{-d_i}, (a_i + 1)b^{-d_i}). \]

Since we have \(m - d_{s+1} = t\) and \(x_0, x_1, \ldots\) is a digital \((t, s)\)-sequence constructed over \(R\), the points \([x_n]_{b,m-d_{s+1}}\) with \(a_{s+1}b^{m-d_{s+1}} \leq n < (a_{s+1} + 1)b^{m-d_{s+1}}\) form a \((t, m - d_{s+1}, s)\)-net in base \(b\). Consequently, the point set \(P\) consisting of the \([x_n]_{b,m}\) with \(a_{s+1}b^{m-d_{s+1}} \leq n < (a_{s+1} + 1)b^{m-d_{s+1}}\) is a \((t, m - d_{s+1}, s)\)-net in base \(b\). Thus, \(J'\) contains exactly \(b^t\) points of \(P\), and so \(J\) contains exactly \(b^t\) points \(y_n\) with \(0 \leq n \leq b^m - 1\).

It remains to show that the \(y_n\) are obtained by the digital method for the construction of nets, and it suffices to prove this for the last coordinates of these points (note that we can assume \(\psi_i(0) = 0\) for all \(r \geq 0\) since the property of being a digital \((t, s)\)-sequence constructed over \(R\) depends only on the \(c^{(s+1)}_{i,r}\) and not on the chosen bijections, e.g., by Lemma 7 in Section 5). In (N2) we choose \(\eta^{(s+1)}_{y} \) to be the inverse map of \(\psi_{b-m}\) for \(1 \leq j \leq m\), and in (N3) we choose

\[ c^{(s+1)}_{j,r} = \delta_{r,m-j} \quad \text{for } 1 \leq j \leq m \text{ and } 0 \leq r \leq m - 1, \]

where on the right-hand side we have the Kronecker symbol viewed as an element of \(R\). Then the digital method yields \(x_n^{(s+1)} = n/b^m\) for \(0 \leq n \leq b^m - 1\). \(\blacksquare\)

In the case \(R = \mathbb{F}_q\), which is of greatest interest, the quality parameter \(t\) can be determined from the elements \(c^{(i)}_{j,r} \in \mathbb{F}_q\) in (S3) in the following way. If \(\mathbb{F}_q^s\) is the sequence space over \(\mathbb{F}_q\), then we use the \(c^{(i)}_{j,r}\) to set up the sequences

\[ c^{(i)}_j = (c^{(i)}_{j,0}, c^{(i)}_{j,1}, \ldots) \in \mathbb{F}_q^s \quad \text{for } 1 \leq i \leq s \text{ and } j \geq 1, \]
and we consider the two-parameter system
\[ C^{(s)} = \{ c_{ij}^{(s)} \in \mathbb{F}_q^s : 1 \leq i \leq s \text{ and } j \geq 1 \} . \]

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 we put
\[ C^{(m)} = \{ \pi_m(c_{ij}^{(s)}) \in \mathbb{F}_q^m : 1 \leq i \leq s, 1 \leq j \leq m \}. \]

As in [15, Definition 4.27], for fixed \( m \) we let \( \rho(C^{(m)}) \) be the largest integer \( d \) such that any system \( \{ \pi_m(c_{ij}^{(s)}) : 1 \leq j \leq d_i, 1 \leq i \leq s \} \) with \( 0 \leq d_i \leq m \) for \( 1 \leq i \leq s \) and \( \sum_{i=1}^s d_i = d \) is linearly independent over \( \mathbb{F}_q \) (here the empty system is viewed as linearly independent). Finally, we set
\[ \tau(C^{(s)}) = \sup_{m \geq 1} (m - \rho(C^{(m)})) . \]

We are interested only in the case where \( \tau(C^{(s)}) < \infty \). The proofs of Theorems 4.35 and 4.36 in [15] yield the following result.

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

Most known constructions of \((t, s)\)-sequences employ the digital method over a finite field. Important previous constructions using the digital method are those of Sobol’ [24], Faure [2], Niederreiter [12, 13], and Niederreiter and Xing [18]. A recent survey of \((t, m, s)\)-net and \((t, s)\)-sequence constructions is given in [10]. A generalization of the concept of a \((t, s)\)-sequence was recently introduced by Larcher and Niederreiter [7].

Any digital \((t, s)\)-sequence \( S \) in an arbitrary base \( b \geq 2 \) is a low-discrepancy sequence, in the sense that the star discrepancy \( D_\infty^*(S) \) of the first \( N \) terms of \( S \) satisfies \( D_\infty^*(S) = O(N^{-1}(\log N)^t) \). More precisely, it was shown in [12, Section 4] and also in [15, Theorem 4.17] that
\[ D_\infty^*(S) \leq C_b(s, t)N^{-1}(\log N)^t + O(N^{-1}(\log N)^{t-1}) \quad \text{for all } N \geq 2, \]
where the implied constant in the Landau symbol depends only on \( b, s, \) and \( t \). Here

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

if either \( s = 2 \) or \( b = 2, s = 3, 4 \); otherwise

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

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

**Remark 2.** Strictly speaking, the discrepancy bound (3) is not immediately implied by the indicated sources since our definition of a digital \((t, s)\)-sequence in base \( b \) is slightly more general than that in [12] and [15] (compare with Remark 1). But note that the only difference is that for \( kb^m \leq n < (k + 1)b^m \) we replaced the points \( x_n \) by the truncated points \( \lfloor x_n \rfloor_{b,m} \). This replacement can change the star discrepancy of the involved sets of \( b^m \) points by at most \( s b^{-m} \). Thus, in [12, Lemma 4.1], which is the basis for (3), the quantity \( D_b(t, m, s) \) has to be replaced by \( D_b(t, m, s) + s \). But this change affects only the \( O(N^{-1} \log N) \) term in the bound for \( D_b^* \) (5), and so (3) holds for \( s \geq 2 \). This fact was noted also by Tezuka [27]. For \( s = 1 \) we can work with the same value \( \Delta_b(t, m, 1) = b^t \) as for the truncated points, and so (3) holds for \( s = 1 \).

3. THE NEW CONSTRUCTION OF SEQUENCES

Let \( \mathbf{F}_q \) again be the finite field of order \( q \). The notation \( K/\mathbf{F}_q \) for a global function field signifies that \( \mathbf{F}_q \) is the full constant field of the algebraic function field \( K \). We write \( g(K/\mathbf{F}_q) \) for the genus of \( K/\mathbf{F}_q \). By a *rational place* of \( K/\mathbf{F}_q \) we mean a place of \( K/\mathbf{F}_q \) of degree 1. Let \( N(K/\mathbf{F}_q) \) denote the number of rational places of \( K/\mathbf{F}_q \).

We write \( \nu_P \) for the normalized discrete valuation corresponding to the place \( P \) of \( K/\mathbf{F}_q \). Using standard notation (see, e.g., [26]), we define the following divisors of \( K/\mathbf{F}_q \) for any nonzero \( k \in K \):
\[(k)_0 = \sum_{P \mid k \delta P} v_P(k)P, \]

\[(k)_n = \sum_{P \mid k \delta P} (-v_P(k))P, \]

\[(k) = (k)_0 - (k)_n. \]

For an arbitrary divisor \(D\) of \(K/F_q\), the \(F_q\)-vector space

\[\mathcal{L}(D) = \{k \in K\setminus\{0\} : (k) + D \geq 0\} \cup \{0\}\]

has a finite dimension which we denote by \(l(D)\).

If \(D\) is a divisor of \(K/F_q\) with \(\deg(D) = g(K/F_q)\) and \(l(D) = 1\) and if \(P\) is any rational place of \(K/F_q\), then \(l(D + nP) \geq n + 1\) for \(n \geq 0\) by the Riemann–Roch theorem. On the other hand, \(l(D + nP) \leq l(D) + n = n + 1\), and so \(l(D + nP) = n + 1\). If \(k \in \mathcal{L}(D + nP)\), then it is easy to see that \(v_P(k) = -v_P(D) - n\).

Now let \(s \geq 1\) and the prime power \(q\) be given, and suppose that the global function field \(K/F_q\) satisfies \(N(K/F_q) \geq s + 1\). Let \(P_*, P_1, P_2, \ldots, P_s\) be \(s + 1\) distinct rational places of \(K/F_q\) and choose a positive divisor \(D\) of \(K/F_q\) with \(\deg(D) = g(K/F_q)\) and \(l(D) = 1\) (compare with Lemma 6). By the argument above, for \(1 \leq i \leq s\) and \(j \geq 1\) we can determine elements \(k_j^{(i)} \in \mathcal{L}(D + jP_i)\) such that

\[v_{P_i}(k_j^{(i)}) = -v_{P_i}(D) - j.\]

Let \(z\) be a local uniformizing parameter at \(P_*\), then since \(v_{P_*}(k_j^{(i)}) \geq -v_{P_*}(D)\), we have the expansions

\[k_j^{(i)} = z^{-v} \sum_{r=0}^{v} b_j^{(i)} r^r \quad \text{for} \ 1 \leq i \leq s \text{ and } j \geq 1,\]

with \(v = v_{P_*}(D)\) and all coefficients \(b_j^{(i)} \in F_q\). We note that \(0 \leq v \leq g(K/F_q)\). For \(1 \leq i \leq s\) and \(j \geq 1\) we now define

\[c_j^{(i)} = \begin{cases} 
  b_j^{(i)} & \text{for } 0 \leq r \leq v - 1, \\
  b_j^{(i)} r & \text{for } r \geq v.
\end{cases} \quad \text{(4)}\]

The elements \(c_j^{(i)}\) in (4) are used in our new construction of digital \((t, s)\)-sequences. In the digital method for the construction of sequences described
in Section 2, we choose $R = \mathbf{F}_q$ and we select bijections $\psi_r$ and $\eta_{i}^{(r)}$ as in (S1) and (S2), respectively. The $c_{i,j}^{(r)} \in \mathbf{F}_q$ from (4) serve as the elements in (S3). Then the digital method yields the sequence $x_0, x_1, \ldots$ of points in $T'$ as in (2).

To obtain the quality parameter for this sequence, we proceed as in Section 2. We use the $c_{i,j}^{(r)}$ from (4) to set up

$$c_{i,j}^{(r)} = (c_{i,j,0}^{(r)}, c_{i,j,1}^{(r)}, \ldots) \in \mathbf{F}_q^s$$

for $1 \leq i \leq s$ and $j \geq 1$,

and we consider the system

$$C^{(s)} = \{c_{i,j}^{(r)} \in \mathbf{F}_q^s : 1 \leq i \leq s, j \geq 1 \}.$$

**Theorem 1.** Given a prime power $q$ and a dimension $s \geq 1$, let $K/\mathbf{F}_q$ be a global function field with $N(K/\mathbf{F}_q) \geq s + 1$ and let $D$ be a positive divisor of $K/\mathbf{F}_q$ with $\deg(D) = g(K/\mathbf{F}_q)$ and $l(D) = 1$. Then the system $C^{(s)}$ defined above satisfies

$$\tau(C^{(s)}) \leq g(K/\mathbf{F}_q).$$

**Proof.** With $g = g(K/\mathbf{F}_q)$ it suffices to verify the following property: for any integer $m > g$ and any integers $d_1, \ldots, d_s \geq 0$ with $1 \leq \sum_{i=1}^{s} d_i \leq m - g$, the vectors

$$\pi_m(c_{i,j}^{(r)}) = (c_{i,j,0}^{(r)}, c_{i,j,1}^{(r)}, \ldots, c_{i,j,m-1}^{(r)}) \in \mathbf{F}_q^m$$

for $1 \leq j \leq d_i, 1 \leq i \leq s$,

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

$$\sum_{i \in H} \sum_{j=1}^{d_i} a_{i,j}^{(r)} \pi_m(c_{i,j}^{(r)}) = 0 \in \mathbf{F}_q^m$$

for some $a_{i,j}^{(r)} \in \mathbf{F}_q$, that is,

$$\sum_{i \in H} \sum_{j=1}^{d_i} a_{i,j}^{(r)} b_{i,j}^{(r)} = 0 \quad \text{for } 0 \leq r \leq m \text{ with } r \neq v. \quad (5)$$

Now we consider the element $k \in K$ given by

$$k = \sum_{i \in H} \sum_{j=1}^{d_i} a_{i,j}^{(r)} k_{i,j}^{(r)} = z^{-v} \sum_{r=0}^{m} \left( \sum_{i \in H} \sum_{j=1}^{d_i} a_{i,j}^{(r)} b_{i,j}^{(r)} \right) z^r.$$
From (5) we get

\[ k = z^{-v} \sum_{r=m+1}^{n} \left( \sum_{i \in H} \sum_{j=1}^{d_i} a_i^{(i)} b_j^{(i)} \right) z^r + c \]

with

\[ c = \sum_{i \in H} \sum_{j=1}^{d_i} a_i^{(i)} b_j^{(i)} \in F_q. \]

We put \( f = k - c \). If we had \( f \neq 0 \), then \( \deg((f)_0) \geq m + 1 - v \). On the other hand, the definitions of \( f \) and \( k \) imply that

\[ (f)_a = (k)_a \leq D - vP_a + \sum_{i=1}^{s} d_i P_i, \]

and hence \( \deg((f)_0) \leq g - v + \sum_{i=1}^{s} d_i \leq m - v \), a contradiction. Therefore \( f = 0 \), and hence

\[ \sum_{i \in H} \sum_{j=1}^{d_i} a_i^{(i)} k_j^{(i)} = c. \]

For fixed \( h \in H \) we have

\[ \sum_{j=1}^{d_h} a_j^{(h)} k_j^{(h)} = c - \sum_{i \in H \setminus \{h\}} \sum_{j=1}^{d_i} a_j^{(i)} k_j^{(i)}. \]

If not all \( a_j^{(h)} = 0 \), then the choice of the \( k_j^{(i)} \) would imply

\[ \nu_{P_a} \left( \sum_{j=1}^{d_h} a_j^{(h)} k_j^{(h)} \right) \leq -\nu_{P_a}(D) - 1 \]

and

\[ \nu_{P_a} \left( c - \sum_{i \in H \setminus \{h\}} \sum_{j=1}^{d_i} a_j^{(i)} k_j^{(i)} \right) \geq -\nu_{P_a}(D), \]

a contradiction. Thus \( a_j^{(h)} = 0 \) for \( 1 \leq j \leq d_h \).

In the following we will prove that a divisor \( D \) as in Theorem 1, namely
a positive divisor $D$ of $K/F_q$ with $\deg(D) = g(K/F_q)$ and $l(D) = 1$, always exists as soon as $N(K/F_q) \geq 4$ (see Lemma 6 below).

For the following four lemmas, $K/F_q$ is an arbitrary global function field of genus $g = g(K/F_q)$. For any integer $n \geq 0$, we denote by $A_n$ the number of positive divisors of $K/F_q$ of degree $n$. Note that $A_0 = 1$ and $A_1 = N(K/F_q)$. The zeta function of $K/F_q$ is

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n = \frac{L(t)}{(1-t)(1-qt)}$$

with a polynomial $L(t)$ of the form

$$L(t) = \prod_{j=1}^{g} (1 - \alpha_j t)(1 - \overline{\alpha}_j t),$$

where the $\alpha_j$, $1 \leq j \leq g$, are complex numbers. By the class number of $K/F_q$ we mean the order of the group of divisor classes of $K/F_q$ of degree 0. The results of the following lemma can also be found in [6].

**Lemma 3.** Let $g$ be the genus of $K/F_q$ and $h$ the class number.

(i) If $g \geq 1$, then for $0 \leq n \leq 2g - 2$ we have

$$A_n = q^{n+1-g} A_{2g-2-n} + h q^{n+1-g} - 1.$$

(ii) If $g \geq 2$, then

$$\sum_{n=0}^{g-2} A_n t^n + \sum_{n=0}^{g-1} q^{2g-1-n} A_n t^{2g-2-n} = \frac{L(t) - h t^g}{(1-t)(1-qt)}.$$

**Proof.** Part (i) follows from the functional equation of the zeta function and from Lemma V.1.4(c) and Corollary V.1.11 in [26]. Part (ii) follows from (i) and the same results in [26]. □

**Lemma 4.** If $N(K/F_q) \geq m$ for some integer $m \geq 1$, then

$$A_n \geq mA_{n-1} - \frac{m(m-1)}{2} A_{n-2} \quad \text{for all } n \geq 2.$$

**Proof.** For a divisor $D$ and a set $\mathcal{A}$ of divisors of $K/F_q$ we put $D + \mathcal{A} = \{D + A : A \in \mathcal{A}\}$. Now let $P_1, \ldots, P_m$ be $m$ distinct rational places of $K/F_q$ and let $\mathcal{A}_n$ be the set of positive divisors of $K/F_q$ of degree $n$. Then for $n \geq 2$,
LOW-DISCREPANCY SEQUENCES

\[ \bigcup_{i=1}^{m} (P_i + \mathcal{A}_{n-1}) \subseteq \mathcal{A}_n. \]

We have \( |P_i + \mathcal{A}_{n-1}| = |\mathcal{A}_{n-1}| = A_{n-1} \), and it is clear that \( (P_i + \mathcal{A}_{n-1}) \cap (P_j + \mathcal{A}_{n-1}) = P_i + P_j + \mathcal{A}_{n-2} \) for \( i \neq j \). Thus,

\[ A_n \geq m \left( \sum_{i=1}^{m} |P_i + \mathcal{A}_{n-1}| - \sum_{1 \leq i < j \leq m} |(P_i + \mathcal{A}_{n-1}) \cap (P_j + \mathcal{A}_{n-1})| \right) = mA_{n-1} - \frac{m(m-1)}{2} A_{n-2}. \]

**Lemma 5.** If \( N(K/F_q) \geq 1 \) and \( l(D) \geq 2 \) for any positive divisor \( D \) of \( K/F_q \) of degree \( g = g(K/F_q) \), then

\[ A_g \geq (q + 1)h, \]

where \( h \) is the class number of \( K/F_q \).

**Proof.** Let \( P \) be a rational place of \( K/F_q \) and let \( \mathcal{C}_K^0 \) be the group of divisor classes of \( K/F_q \) of degree 0. With \( \mathcal{A}_g \) as in the proof of Lemma 4, we consider the map

\[ \Phi: D \in \mathcal{A}_g \mapsto [D - gP] \in \mathcal{C}_K^0. \]

If \( E \) is any divisor of \( K/F_q \) of degree 0, then \( l(E + gP) \geq 1 \) by the Riemann–Roch theorem. Choose \( f \in \mathcal{C}(E + gP) \setminus \{0\} \) and let \( D \) be the divisor \( (f + E + gP) \), then \( D \in \mathcal{A}_g \) and \( [D - gP] = [E] \). This means that \( \Phi \) is surjective.

Let \( D_1, D_2, \ldots, D_h \in \mathcal{A}_g \) be such that \( [D_1 - gP], [D_2 - gP], \ldots, [D_h - gP] \) are all distinct elements of \( \mathcal{C}_K^0 \). If

\[ \mathcal{D}_i = \{ D \in \mathcal{A}_g : [D] = [D_i] \} \text{ for } 1 \leq i \leq h, \]

then \( |\mathcal{D}_i| = (q^{[D_i]} - 1)/(q - 1) \). Now \( l(D_i) \geq 2 \) by hypothesis, and hence \( |\mathcal{D}_i| \geq q + 1 \). It is obvious that \( \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_h \) are pairwise disjoint, since \( [D_i - gP] \neq [D_j - gP] \) for \( i \neq j \). Therefore, \( A_g = |\mathcal{A}_g| \geq (q + 1)h. \]

**Lemma 6.** There exists a positive divisor \( D \) of \( K/F_q \) with \( \deg(D) = g(K/F_q) \) and \( l(D) = 1 \) if either \( N(K/F_q) \geq 2 \) and \( q \geq 3 \), or \( N(K/F_q) \geq 4 \) and \( q = 2 \).
Proof. Put $g = g(K/F_q)$. The lemma is trivial for $g = 0$. If $g = 1$, let $D$ be a rational place of $K/F_q$, then $l(D) = 1$. Now let $g \geq 2$. Suppose, by way of contradiction, that $l(D) \geq 2$ for any positive divisor $D$ of $K/F_q$ with $\deg(D) = g$. If $g = 2$, then by Lemma 3(i) we have $A_2 = q + h$ and by Lemma 5 we have $A_2 \geq (q + 1)h$. Thus $h \leq 1$, which contradicts $h \geq A_1 \geq 2$ (note that if $g \geq 1$, then any two different rational places of $K/F_q$ are inequivalent).

So we may assume $g \geq 3$. Substituting $t = q^{-1/2}$ in the identity in Lemma 3(ii), we obtain

$$2 \sum_{n=0}^{g-2} q^{-n/2} A_n + q^{-(g-1)/2} A_{g-1} = \frac{h - q^{g/2} L(q^{-1/2})}{(q^{1/2} - 1)^2 q^{g-3/2}}.$$ 

Since

$$L(q^{-1/2}) = \prod_{j=1}^{g} |1 - \alpha_j q^{-1/2}| \geq 0,$$

we infer that

$$2 \sum_{n=0}^{g-2} q^{(g-1-n)/2} A_n + A_{g-1} \leq \frac{h}{(q^{1/2} - 1)^2}.$$ (6)

Lemma 3(i) yields $A_g = h + qA_{g-2}$ and Lemma 5 yields $A_g \geq (q + 1)h$, and thus $A_{g-2} \geq h$. From (6) we then get

$$2q^{1/2} \leq \frac{1}{(q^{1/2} - 1)^2}.$$ 

This inequality is impossible if $q \geq 3$, and hence it remains to prove the lemma for $q = 2$.

If $q = 2$ and $N(K/F_q) \geq 4$, then from (6) we obtain

$$4A_{g-3} + 2\sqrt{2} A_{g-2} + A_{g-1} \leq \frac{h}{(\sqrt{2} - 1)^2}.$$ (7)

Together with Lemma 4 with $m = 3$ and $n = g - 1$ this yields

$$A_{g-3} + (3 + 2\sqrt{2}) A_{g-2} \leq \frac{h}{(\sqrt{2} - 1)^2}.$$ (8)
If we use Lemma 4 with $m = 4$ and $n = g - 1$ in (7), then we get

$$-2A_{k-3} + (4 + 2\sqrt{2})A_{k-2} \leq \frac{h}{(\sqrt{2} - 1)^2}. \quad (9)$$

By eliminating $A_{k-3}$ from (8) and (9), we arrive at

$$(10 + 6\sqrt{2})A_{k-2} \leq \frac{3h}{(\sqrt{2} - 1)^2},$$

and therefore

$$10 + 6\sqrt{2} \leq \frac{3}{(\sqrt{2} - 1)^2},$$

which is absurd. \[\square\]

For any given prime power $q$ and any given dimension $s \geq 1$ we define

$$V_q(s) = \min g(K/F_q), \quad (10)$$

where the minimum is extended over all global function fields $K/F_q$ with $N(K/F_q) \equiv s + 1$. The reader who may wonder whether $N(K/F_q) \equiv s + 1$ can always be achieved by a suitable choice of $K/F_q$ (for fixed $q$ and $s$) is referred to Section 4 for an affirmative answer.

**Theorem 2.** For every prime power $q$ and every dimension $s \geq 1$ there exists a digital $(V_q(s), s)$-sequence constructed over $F_q$.

**Proof.** If $s \leq q$, then in Theorem 1 we can choose $K/F_q$ to be the rational function field over $F_q$ and $D$ the zero divisor. Then $\tau(C^{(s)}) = 0$ by Theorem 1, and so by Lemma 2 we get a digital $(t, s)$-sequence constructed over $F_q$ with $t = 0 = V_q(s)$. If $s \geq q + 1$, then let $K/F_q$ be a global function field with $N(K/F_q) \equiv s + 1$ and $g(K/F_q) = V_q(s)$. Then $N(K/F_q) \geq 4$, and so by Lemma 6 there exists a positive divisor $D$ of $K/F_q$ with $\deg(D) = g(K/F_q)$ and $l(D) = 1$. Now Theorem 1 yields $\tau(C^{(s)}) \equiv V_q(s)$, and hence the desired result follows from Lemma 2. Here we use also the fact that any digital $(t, s)$-sequence in an arbitrary base $b$ is a digital $(u, s)$-sequence in base $b$ for every integer $u \geq t$ (compare with [15, Remark 4.3]). \[\square\]

**Corollary 1.** For every prime power $q$, every integer $s \geq 1$, and every integer $m \geq V_q(s)$ there exists a digital $(V_q(s), m, s + 1)$-net constructed over $F_q$.

**Proof.** This follows from Lemma 1 and Theorem 2. \[\square\]
4. Results on $V_q(s)$

The values of $V_q(s)$ defined by (10) are closely connected with those of a function that is studied in the theory of algebraic curves over finite fields. In the language of global function fields, this function is defined, for any prime power $q$ and any integer $g \geq 0$, by

$$N_q(g) = \max N(K/F_q),$$

where the maximum is extended over all global function fields $K/F_q$ of genus $g$. By the Serre bound [20] (see also [26, Theorem V.3.1]) we have

$$N_q(g) \leq q + 1 + g[2q^{1/2}].$$

It is clear that

$$V_q(s) = \min \{g : N_q(g) \geq s + 1\}. \quad (11)$$

Remark 3. It is trivial that $N_q(0) = q + 1$. A formula for $N_q(1)$ can be found, e.g., in Waterhouse [30]. We have $N_q(1) = q + 1 + \lceil 2q^{1/2} \rceil$, except in the case where $q = p^e$ with a prime $p$ dividing $\lceil 2q^{1/2} \rceil$ and an odd integer $e \geq 3$, in which case $N_q(1) = q + \lceil 2q^{1/2} \rceil$. Serre [20–22] determined the values of $N_q(2)$. Write again $q = p^e$ with a prime $p$ and an integer $e \geq 1$. If $e$ is even and $q \neq 4, 9$, then $N_q(2) = q + 1 + 4q^{1/2}$, whereas $N_q(2) = 10, N_q(2) = 20$. We call $q$ special if either $p$ divides $\lceil 2q^{1/2} \rceil$ or $q$ is of the form $m^2 + 1$, $m^2 + m + 1$, or $m^2 + m + 2$ for some integer $m$. If $e$ is odd and $q$ is not special, then $N_q(2) = q + 1 + 2\lceil 2q^{1/2} \rceil$. If $e$ is odd and $q$ is special, then $N_q(2) = q + 2\lceil 2q^{1/2} \rceil$ or $q + 2\lceil 2q^{1/2} \rceil - 1$, depending on whether the fractional part of $2q^{1/2}$ is greater than $(\sqrt{5} - 1)/2$ or not.

We tabulate $N_q(g)$ for small values of $g$ in Table I. The values of $N_q(1)$ and $N_q(2)$ are obtained from Remark 3, and the values of $N_q(3)$ and $N_q(4)$ are from Serre [22] (for the case $g = 3$ see also [28, Theorem 2.3.19]).

| $q$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| $N_q(1)$ | 5 | 7 | 9 | 10 | 13 | 14 | 16 | 18 | 21 | 25 | 26 | 28 | 33 | 36 | 38 | 40 | 50 | 66 |
| $N_q(2)$ | 6 | 8 | 10 | 12 | 16 | 18 | 20 | 24 | 26 | 33 | 32 | 36 | 42 | 46 | 48 | 50 | 66 |
| $N_q(3)$ | 7 | 10 | 14 | 16 | 20 | 24 | 28 | 28 | 32 | 38 | 40 | 44 | 56 | 66 |
| $N_q(4)$ | 8 | 12 | 15 | 18 | 20 | 24 | 26 | 28 | 32 | 38 | 40 | 44 | 48 | 48 | 50 | 52 | 66 |
TABLE II

<table>
<thead>
<tr>
<th>$g$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N_1(g)$</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>12*</td>
</tr>
<tr>
<td>$N_2(g)$</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>13*</td>
<td>14*</td>
<td>15*</td>
<td>15*</td>
<td>19*</td>
<td>....</td>
</tr>
<tr>
<td>$N_3(g)$</td>
<td>5</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>14</td>
<td>15</td>
<td>16*</td>
<td>17*</td>
<td>18*</td>
<td>19*</td>
<td>21*</td>
<td>....</td>
</tr>
<tr>
<td>$N_4(g)$</td>
<td>6</td>
<td>10</td>
<td>12</td>
<td>16</td>
<td>18</td>
<td>18</td>
<td>21*</td>
<td>....</td>
<td>....</td>
<td>....</td>
<td>....</td>
<td>....</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$g$</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>39</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N_5(g)$</td>
<td>14*</td>
<td>14*</td>
<td>15*</td>
<td>17*</td>
<td>16*</td>
<td>17*</td>
<td>18*</td>
<td>20</td>
<td>19*</td>
<td>21</td>
<td>33</td>
<td>40</td>
</tr>
</tbody>
</table>

Note. Entries marked with an asterisk represent a lower bound for $N_q(g)$ and not necessarily the exact value.

Blank entries in the table indicate that the corresponding values of $N_q(g)$ are not known to us. On account of (11), the tabulated values allow the determination of various values of $V_q(s)$. For larger values of $q$ which are powers of 2, values of $N_q(g)$ can be obtained from [29].

We tabulate $N_q(g)$ for small values of $q$ in Table II. For practical work with digital $(t, s)$-sequences in base $q$, the case $q = 2$ is actually the most important one. Some values of $N_q(g)$ in Table II are reproduced from Table I for the sake of completeness. The values of $N_2(g)$ are from Serre [21]. Entries marked with an asterisk represent a lower bound for $N_q(g)$ and not necessarily the exact value. The lower bounds in the cases $q = 3, 4, 5$ were determined by us, and the function fields yielding these lower bounds are listed in the Appendix. From Table II and the formula (11) we can derive the values of $V_q(s)$ tabulated in Table III. Since some entries in Table II provide only a lower bound, certain entries in Table III (marked again with an asterisk) represent an upper bound for $V_q(s)$ and not necessarily the exact value (we were able to remove some asterisks because of additional information in [21, Table I]). It is important to note, however, that any integer $t \geq V_q(s)$ can serve as a quality parameter for a digital $(t, s)$-sequence constructed over $F_q$, in view of a remark in the proof of Theorem 2.

Further bounds obtained from Table II and the formula (11) are $V_2(s) \leq 39$ for $21 \leq s \leq 32$ and $V_2(s) \leq 50$ for $33 \leq s \leq 39$. The values or upper bounds for $V_q(s)$ in Table III are smaller than the previously best quality parameters (see Niederreiter [13] and Niederreiter and Xing [18]) for $s \geq q + 2$ if $2 \leq q \leq 5$. For those cases where $V_q(s) = 0$ or 1, these values of the quality parameter are actually best possible (compare with Remark 6 in Section 5).
### TABLE III
Values of $V_q(s)$ for $2 \leq q \leq 5$ and $1 \leq s \leq 20$

<table>
<thead>
<tr>
<th>$s$</th>
<th>$1$</th>
<th>$2$</th>
<th>$3$</th>
<th>$4$</th>
<th>$5$</th>
<th>$6$</th>
<th>$7$</th>
<th>$8$</th>
<th>$9$</th>
<th>$10$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_2(s)$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>$V_3(s)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>$V_4(s)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$V_5(s)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

$s$ | $11$ | $12$ | $13$ | $14$ | $15$ | $16$ | $17$ | $18$ | $19$ | $20$ |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_2(s)$</td>
<td>9</td>
<td>11$^*$</td>
<td>12$^*$</td>
<td>14$^*$</td>
<td>15$^*$</td>
<td>15$^*$</td>
<td>18$^*$</td>
<td>19$^*$</td>
<td>19$^*$</td>
<td>21$^*$</td>
</tr>
<tr>
<td>$V_3(s)$</td>
<td>4</td>
<td>6$^*$</td>
<td>7$^*$</td>
<td>8$^*$</td>
<td>9$^*$</td>
<td>9$^*$</td>
<td>9$^*$</td>
<td>9$^*$</td>
<td>9$^*$</td>
<td>9$^*$</td>
</tr>
<tr>
<td>$V_4(s)$</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5$^*$</td>
<td>6$^*$</td>
<td>7$^*$</td>
<td>10$^*$</td>
<td>10$^*$</td>
<td>10$^*$</td>
</tr>
<tr>
<td>$V_5(s)$</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>6$^*$</td>
<td>6$^*$</td>
<td>6$^*$</td>
</tr>
</tbody>
</table>

**Note.** Entries marked with an asterisk represent an upper bound for $V_q(s)$ and not necessarily the exact value.

If $q$ is a square (of an integer), then a good upper bound for $V_q(s)$ can be given for a relatively wide range of dimensions $s$.

**Proposition 1.** If $q$ is a square, then

$$V_q(s) \leq \frac{1}{2} (q - q^{1/2}) \quad \text{for} \quad 1 \leq s \leq q^{3/2}.$$  

**Proof.** With $r = q^{1/2}$ consider the Hermitian function field $K = F_q(x, y)$ with $y^r + y = x^{r+1}$. By [26, Lemma VI.4.4], we have $g(K/F_q) = r(r-1)/2$ and $N(K/F_q) = r^3 + 1$. In view of the definition of $V_q(s)$ this yields the desired result. 

For any prime power $q$, Ihara [5] introduced the number

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g},$$

where $g$ runs through positive values. Serre [20, 23] proved that always $A(q) > 0$, in fact, $A(q) \geq c \log q$ with an absolute constant $c > 0$. If $q$ is a square, then it is known that $A(q) = q^{1/2} - 1$ (see [28, Theorem 2.3.24]). Further results on $A(q)$ can be found in [28, Theorems 2.3.22 and 2.3.25]. More recently, it was shown by Schoof [19] that $A(2) \geq \frac{7}{5}$ and by Xing [31] that $A(3) \geq \frac{1}{2}$ and $A(5) \geq \frac{1}{2}$. Now we define

$$B(q) = \liminf_{s \to \infty} \frac{V_q(s)}{s}.$$  

Then we have the following upper bounds for $B(q)$.  

Proposition 2. (i) For all prime powers \( q \) we have
\[
B(q) \leq \frac{1}{A(q)}.
\]

(ii) There exists an absolute constant \( d > 0 \) such that for all prime powers \( q \) we have
\[
B(q) \leq \frac{d}{\log q}.
\]

(iii) If \( q \) is a square, then
\[
B(q) \leq \frac{1}{q^{1/2} - 1}.
\]

(iv) \( B(2) \leq \frac{3}{2}, B(3) \leq 3, B(5) \leq 2. \)

Proof. Let \( 0 < g_1 < g_2 \cdots \) be such that
\[
\lim_{n \to \infty} \frac{N_q(g_n)}{g_n} = A(q).
\]
With \( s_n = N_q(g_n) - 1 \) it follows from (11) that
\[
B(q) \leq \lim_{n \to \infty} \frac{g_n}{s_n} = \frac{1}{A(q)}.
\]
The remaining results follow from the facts about \( A(q) \) mentioned above. 

Now we establish general upper bounds for \( V_q(s) \) by using class field towers of global function fields. Let \( l \) be a prime number, let \( K/F_q \) be a global function field, and let \( \mathcal{P} \) be a nonempty set of rational places of \( K/F_q \). Fix a separable closure \( \overline{K} \) of \( K \). Then the \((l, \mathcal{P})\)-Hilbert class field \( H(l, \mathcal{P}) \) of \( K/F_q \) is defined to be the maximal unramified abelian \( l \)-extension of \( K \) in \( \overline{K} \) in which all places in \( \mathcal{P} \) split completely. One can repeat this construction: with \( K_1 = H(l, \mathcal{P}) \) and \( \mathcal{P}_1 \) being the set of all places of \( K_1/F_q \), and so on. In this way one gets a tower
\[
K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots,
\]
which is called the \((l, \mathcal{P})\)-class field tower of \(K/\mathbb{F}_q\). The \((l, \mathcal{P})\)-class field tower is called finite if there is an index \(i\) such that \(K_n = K_i\) for all \(n \geq i\), and infinite otherwise.

**Theorem 3.** For a given prime power \(q\), suppose that there exists a global function field \(K/\mathbb{F}_q\) with \(g(K/\mathbb{F}_q) > 1\) which has an infinite \((l, \mathcal{P})\)-class field tower for some prime \(l\) and some nonempty set \(\mathcal{P}\) of rational places of \(K/\mathbb{F}_q\). Then we have

\[
V_q(s) \leq \frac{g(K/\mathbb{F}_q) - 1}{|\mathcal{P}|} M s + 1 \quad \text{for all } s \geq 1,
\]

where

\[
M = \max \left( \frac{|\mathcal{P}|}{q + 1}, l \right).
\]

**Proof.** Let \(K/\mathbb{F}_q\) be as in the theorem and let

\[
K = K_0 \subset K_1 \subset K_2 \subset \cdots
\]

be the infinite \((l, \mathcal{P})\)-class field tower of \(K/\mathbb{F}_q\). We have \([K_n: K_{n-1}] = l^{m_n}\) with \(m_n \geq 1\) for \(n = 1, 2, \ldots\). By Galois theory, for any \(n \geq 1\) there is a chain of fields

\[
K_{n-1} = L_{n,0} \subset L_{n,1} \subset \cdots \subset L_{n,m_n} = K_n
\]

such that \([L_{n,j}: L_{n,j-1}] = l\) for \(1 \leq j \leq m_n\). If \(\mathcal{P}_{n,j}\) is the set of all places of \(L_{n,j}/\mathbb{F}_q\) that lie over the places in \(\mathcal{P}\) then

\[
|\mathcal{P}_{n,j}| = [L_{n,j}: K] |\mathcal{P}| \quad \text{for } 0 \leq j \leq m_n \text{ and } n \geq 1.
\]

Since the extension \(L_{n,j}/K\) is unramified, we have

\[
g(L_{n,j}/\mathbb{F}_q) = (g - 1)[L_{n,j}: K] + 1
\]

by the Hurwitz genus formula, with \(g = g(K/\mathbb{F}_q)\). For \(s \leq q\) the result of the theorem is trivial. Now let \(s \geq q + 1\). If \(s \leq |\mathcal{P}| - 1\), then

\[
V_q(s) \leq g \leq \frac{g - 1}{|\mathcal{P}|} \cdot \frac{|\mathcal{P}|}{q + 1} s + 1 \leq \frac{g - 1}{|\mathcal{P}|} M s + 1.
\]
If \( s \geq |\mathcal{P}| \), then one can find some \( n \geq 1 \) and \( 1 \leq j \leq m_n \) such that
\[
|\mathcal{P}_{n,j-1}| \leq s \leq |\mathcal{P}_n| - 1 \leq N_q(g(L_{n,j}/\mathbb{F}_q)) - 1.
\]

Hence by (11),
\[
V_q(s) = g(L_{n,j}/\mathbb{F}_q) = (g - 1)[L_{n,j}:K] + 1
\]
\[
= l(g - 1)[L_{n,j-1}:K] + 1 = l(g - 1)\frac{|\mathcal{P}_{n,j-1}|}{|\mathcal{P}|} + 1
\]
\[
\leq \frac{l(g - 1)}{|\mathcal{P}|} s + 1 \leq g - 1 \frac{1}{|\mathcal{P}|} Ms + 1.
\]

**Theorem 4.** There exists an absolute constant \( c > 0 \) such that:

(i) for all prime powers \( q \) we have
\[
V_q(s) \leq \frac{c}{\log q} s + 1 \quad \text{for all } s \geq 1;
\]

(ii) if \( q \) is a square, then
\[
V_q(s) \leq \frac{c}{q^{1/3}} s + 1 \quad \text{for all } s \geq 1.
\]

Furthermore:

(iii) \( V_2(s) \leq 9s + 1 \) for all \( s \geq 1 \);

(iv) \( V_3(s) \leq 6s + 1 \) for all \( s \geq 1 \);

(v) \( V_5(s) \leq 4s + 1 \) for all \( s \geq 1 \).

**Proof.** Parts (i) and (ii) are obtained from Theorem 3 and the following result of Serre [23]: there is an absolute constant \( d > 0 \) such that for any prime power \( q \) there exist a global function field \( K/\mathbb{F}_q \) with \( g(K/\mathbb{F}_q) \) and a set \( \mathcal{P} \) of rational places of \( K/\mathbb{F}_q \) with \( 1 = |\mathcal{P}| \leq 2q + 1 \) for which the \( (2, \mathcal{P}) \)-class field tower of \( K/\mathbb{F}_q \) is infinite and

\[
\frac{|\mathcal{P}|}{g(K/\mathbb{F}_q) - 1} \geq d \log q \quad \text{for all } q,
\]

\[
\frac{|\mathcal{P}|}{g(K/\mathbb{F}_q) - 1} \geq dq^{1/4} \quad \text{if } q \text{ is a square}.
\]
Part (iii) is obtained from Theorem 3 and the following result of Schoof [19]: there exist a global function field $K/F_2$ with $g(K/F_2) = 19$ and a set $\mathcal{P}$ of rational places of $K/F_2$ with $|\mathcal{P}| = 4$ such that the $(2, \mathcal{P})$-class field tower of $K/F_2$ is infinite. We get analogs of Schoof’s result for $q = 3$ and $q = 5$ by combining the constructions in Xing [31, Section 3] with [19, Theorem 2.3] for $l = 2$. Thus, we get the remaining parts of the theorem by applying Theorem 3 with $l = 2$ and the following values: for (iv) take $q = 3, g(K/F_3) = 13, |\mathcal{P}| = 4$; for (v) take $q = 5, g(K/F_5) = 17, |\mathcal{P}| = 8$. ■

If $q$ is a square, then with a different construction we can establish an upper bound for $V_q(s)$ that is weaker than Theorem 4(ii), but effective.

**Theorem 5.** If $q$ is a square, then

$$V_q(s) \leq \frac{q^{1/2}}{q^{1/2} - 1} s - \left(\frac{qs}{q - 1}\right)^{1/2} \quad \text{for all } s \geq 1.$$ 

**Proof.** Put $r = q^{1/2}$. In [3] the tower $K_1 \subseteq K_2 \subseteq \cdots$ of global function fields over $F_q$ is considered, where $K_1 = F_q(x_1)$ and $K_{n+1} = K_n(z_{n+1})$ for $n = 1, 2, \ldots$ with

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

It is shown in [3] that

$$g_n := g(K_n/F_q) \leq q^{n/2} + q^{(n-1)/2} - q^{(n+1)/4},$$

$$N(K_n/F_q) \geq (q - 1)q^{(n-1)/2} + 1$$

for all $n \geq 1$. For $s \leq q$ the result of the theorem is trivial. Now let $s \geq q + 1$. Then there exists an $n \geq 2$ such that $(q - 1)q^{(n-2)/2} + 1 \leq s \leq (q - 1)q^{(n-1)/2}$, and hence

$$g_n \leq \frac{q^{1/2}}{q^{1/2} - 1} s - \left(\frac{qs}{q - 1}\right)^{1/2} \quad \text{and} \quad N_q(g_n) \geq s + 1.$$ 

The desired result follows now from (11). ■

The bounds in Theorems 4 and 5 show that for any fixed prime power $q$ we have $V_q(s) = O(s)$ as $s \to \infty$, with an absolute implied constant. The best earlier quality parameters $t$ for digital $(t, s)$-sequences constructed over $F_q$ were of the order of magnitude $s \log s$ (see [13, 18]).

We note that the results in Sections 3 and 4 are also of relevance in the
Consequences for Digital \((t, s)\)-Sequences Constructed Over Finite Rings

In this section we study the implications of the results above for digital \((t, s)\)-sequences in an arbitrary base \(b \geq 2\). First we note the following way of determining the quality parameter \(t\) for a digital \((t, s)\)-sequence constructed over the ring \(R\). We use again the same notation and terminology as in Section 2. In particular, \(R\) is a commutative ring with identity and of finite order \(|R| \geq 2\), and the \(c^{(i)}_{j, r} \in R\) are the elements from (S3).

**Lemma 7.** The sequence in (2) is a digital \((t, s)\)-sequence constructed over \(R\) if and only if the elements \(c^{(i)}_{j, r} \in R\) satisfy the following property: for any integers \(m > t\) and \(d_1, \ldots, d_i \geq 0\) with \(\sum_{i=1}^{s} d_i = m - t\) and any \(f^{(i)}_j \in R\), \(1 \leq j \leq d_i\), \(1 \leq i \leq s\), the system of \(m - t\) linear equations

\[
\sum_{r=0}^{m-1} c^{(i)}_{j, r} z_r = f^{(i)}_j \quad \text{for } 1 \leq j \leq d_i, 1 \leq i \leq s,
\]

in the unknowns \(z_0, \ldots, z_{m-1}\) over \(R\) has exactly \(|R|^t\) solutions.

**Proof.** This is shown in the same way as in [15, Theorem 4.35].

**Remark 4.** It is easy to see that in Lemma 7 it suffices to consider the homogeneous case of the system of linear equations, i.e., the case where \(f^{(i)}_j = 0\) for \(1 \leq j \leq d_i\), \(1 \leq i \leq s\).

**Lemma 8.** Let the ring \(R = \prod_{u=1}^{h} R_u\) be the direct product of the finite commutative rings \(R_u\) with identity and \(|R_u| \geq 2\). If for each \(1 \leq v \leq h\) there exists a digital \((t_v, s)\)-sequence constructed over \(R_v\), then there exists a digital \((t, s)\)-sequence constructed over \(R\) with

\[
t = \max_{1 \leq u \leq h} t_u.
\]

**Proof.** For \(1 \leq v \leq h\), assume that the digital \((t_v, s)\)-sequence constructed over \(R_v\) is obtained by using in (S3) the elements \(c^{(i)}_{j, r, u} \in R_v\) for \(1 \leq i \leq s\), \(j \geq 1\), and \(r \geq 0\). Now consider a sequence obtained by the digital method with the ring \(R\) and with the elements \(c^{(i)}_{j, r} \in R\) in (S3) defined by

\[
c^{(i)}_{j, r} = (c^{(i)}_{j, r, 1}, \ldots, c^{(i)}_{j, r, h}) \in R \quad \text{for } 1 \leq i \leq s, j \geq 1, \text{ and } r \geq 0.
\]
We check the condition in Lemma 7 for the value of $t$ given in Lemma 8. For integers $m > t$ and $d_1, \ldots, d_s \geq 0$ with $\sum_{i=1}^s d_i = m - t$ consider the system

$$\sum_{r=0}^{m-1} c_{i,j}^{(r)} z_r = 0 \quad \text{for } 1 \leq j \leq d_i, 1 \leq i \leq s,$$

(12)

in the unknowns $z_0, \ldots, z_{m-1}$ over $R$. Because of the direct product structure of $R$, this is equivalent to considering, for $1 \leq v \leq h$, the system of $m - t \leq m - t_v$ linear equations

$$\sum_{r=0}^{m-1} c_{i,j,v}^{(r)} z_{r,v} = 0 \quad \text{for } 1 \leq j \leq d_i, 1 \leq i \leq s,$$

in the unknowns $z_{0,v}, \ldots, z_{m-1,v}$ over $R_v$. By the assumption at the beginning of the proof and by Lemma 7 it follows that the last system has exactly $u_{R} u_{R_v} u_t u_{R_v} u_t u_{R_v} u_t u_{R_v} u_t u_{R_v} u_t$ solutions for each $v$. Consequently, the system (12) has exactly $\prod_{v=1}^h |R_v|^h = |R|^h$ solutions.

**Theorem 6.** Write the integer $b \geq 2$ in an arbitrary way as a product $b = \prod_{v=1}^h q_v$ of prime powers $q_v$. Then for every dimension $s \geq 1$ there exists a digital $(t, s)$-sequence in base $b$ with

$$t = \max_{1 \leq v \leq h} V_{q_v}(s).$$

**Proof.** Consider the direct product $R = \prod_{v=1}^h F_{q_v}$ of the finite fields $F_{q_v}$ and apply Theorem 2 and Lemma 8. ■

**Corollary 2.** Let $b = \prod_{v=1}^h q_v$ be the canonical factorization of the integer $b \geq 2$ into pairwise coprime prime powers $q_1 < \cdots < q_h$. Then for every dimension $s \geq 1$ there exists a digital $(t, s)$-sequence in base $b$ with

$$t \leq \frac{c}{\log q_1} s + 1,$$

where $c > 0$ is an absolute constant.

**Proof.** This follows by combining Theorems 4(i) and 6. ■

**Remark 5.** We get analogous results for digital $(t, m, s + 1)$-nets if we combine Theorem 6 and Corollary 2 with Lemma 1.

Corollary 2 has an important consequence for the coefficient $C_b(s, t)$ of the leading term in the discrepancy bound (3). If we fix the base $b \geq 2$ and...
choose for each dimension $s \geq 1$ a value $t = t(s)$ of the quality parameter satisfying the bound in Corollary 2, then the formula for $C_b(s, t)$ yields

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

where the implied constant depends only on $b$. Therefore, $C_b(s, t(s)) \to 0$ at a superexponential rate as $s \to \infty$. In all earlier constructions, this coefficient tends to $\infty$ as $s \to \infty$ for fixed $b$.

Next we show that the quality parameters $t = O(s)$ obtained from Corollary 2 are asymptotically best possible, in the sense that for fixed $R$ the values $t$ for which there exists a digital $(t, s)$-sequence constructed over $R$ must grow at least linearly with $s$.

**Proposition 3.** Let $R$ be a finite commutative ring with identity and $|R| \geq 2$, and let $q = q(R)$ be the smallest index of a maximal ideal in $R$. If for some integers $s \geq 1$ and $t \geq 0$ there exists a digital $(t, s)$-sequence constructed over $R$, then we must have

$$\min(a, a+1) \sum_{h=0}^{\min(a, a+1)} \left( \begin{array}{c} s+1 \\ h \end{array} \right) (q-1)^h \leq q^{\lfloor t \log q \rfloor}$$

for all integers $u \geq 0$.

**Proof.** If there exists a digital $(t, s)$-sequence constructed over $R$, then, by Lemma 1, for every integer $u \geq 0$ there exists a digital $(t, t+2u, s+1)$-net constructed over $R$. Now let $M$ be a maximal ideal in $R$ of index $q$. Then by [8, Lemma 5], for every $u \geq 0$ there exists a digital $(t, t+2u, s+1)$-net constructed over $R/M \cong \mathbb{F}_q$. The desired result follows now from [18, Proposition 1].

**Corollary 3.** Let $R$ and $q$ be as in Proposition 3. If for some integers $s \geq 1$ and $t \geq 0$ there exists a digital $(t, s)$-sequence constructed over $R$, then we must have

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

**Proof.** Put $u = \lfloor t \log q \rfloor + 1$. If $u > s + 1$, then the bound is trivial. If $u \equiv s + 1$, then an application of Proposition 3 yields

$$\left( \begin{array}{c} s+1 \\ u \end{array} \right) (q-1)^u \leq \left( \begin{array}{c} s+1 \\ u \end{array} \right) (q-1)^u < q^{t+2u},$$
and so

\[ s + 1 < \frac{q^2}{q - 1} uq^{t+u} < \frac{q^2 e}{q - 1} u. \]

**Remark 6.** If we put \( t = 0 \) and \( u = 1 \) in Proposition 3, then we see that a digital \((0, s)\)-sequence constructed over \( R \) can exist only if \( s \leq q(R) \). A result in [8] guarantees that for each dimension \( s \leq q(R) \) there actually exists a digital \((0, s)\)-sequence constructed over \( R \).

**Remark 7.** The argument in the proof of Proposition 3 shows that if for some integers \( s \geq 1, t \geq 0, \) and \( u \geq 0 \) there exists a digital \((t, t + u, s)\)-net constructed over \( R \), then with \( q = q(R) \) we have

\[
\sum_{h=0}^{\min\{u(2),s\}} \binom{s}{h} (q - 1)^h \leq q^{u+u}.
\]

For integers \( b \geq 2 \) and \( s \geq 1 \), let \( d_b(s) \) be the least value of \( t \) such that there exists a digital \((t, s)\)-sequence in base \( b \). Let \( b = \prod_{v=1}^{h} q_v \) be the canonical factorization of \( b \) into pairwise coprime prime powers \( q_1 < \cdots < q_h \). From the fact that any finite commutative ring \( R \) with identity and \( |R| \geq 2 \) is isomorphic to a direct product of such rings of prime-power order (see [9, p. 2]), it follows easily that \( q(R) \leq q_1 \). If we now combine Corollaries 2 and 3, then we obtain

\[
\frac{q_1 - 1}{q_1 e \log q_1} (s + 1) - \frac{1}{\log q_1} < d_b(s) \leq \frac{c}{\log q_1} s + 1.
\]

From Theorem 6 we deduce that \( d_b(s) = 0 \) for \( 1 \leq s \leq q_1 \), and Remark 6 implies that \( d_b(s) \geq 1 \) for \( s \geq q_1 + 1 \).

### 6. An Elementary Principle and Its Applications

We point out an elementary principle in the theory of \((t, s)\)-sequences (see Proposition 4 below) which has not been noticed before. In complete analogy with Definition 1, an arbitrary sequence \( x_0, x_1, \ldots \) of points in \( T^s \) is defined to be a \((t, s)\)-sequence in base \( b \) if for all integers \( k \geq 0 \) and \( m > t \) the points \( [x_n]_{b,m} \) with \( kb^m \leq n < (k + 1)b^m \) form a \((t, m, s)\)-net in base \( b \). Here we again have in mind that the coordinates of all points of the sequence are given by prescribed \( b \)-adic expansions of the form \( \sum_{j=1}^{\infty} y_j b^{-j} \) with all \( y_j \in \mathbb{Z}_b \). The discrepancy bound (3) holds as well for \((t, s)\)-
sequences in base \( b \) (compare with Remark 2), and the first part of the proof of Lemma 1 shows that this lemma is also valid in the following form: if there exists a \((t, s)\)-sequence in base \( b \), then for every integer \( m \geq t \) there exists a \((t, m, s + 1)\)-net in base \( b \). It is convenient to call an interval \( J \) 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 \( 1 \leq i \leq s \) an elementary interval in base \( b \).

**Lemma 9.** Let \( b \geq 2, h \geq 1, s \geq 1, \) and \( 0 \leq u \leq m \) be integers. Then every \((u, m, s)\)-net in base \( b^h \) is a \((t, hm, s)\)-net in base \( b \) with

\[
t = \min(hu + (h - 1)(s - 1), hm).
\]

**Proof.** The case \( t = hm \) is trivial, so we can assume that

\[
t = hu + (h - 1)(s - 1) < hm.
\]

Now let \( J \) be an elementary interval in base \( b \) as in (13) with volume \( b^{d_i} \), hence

\[
\sum_{i=1}^{s} d_i = hm - t = h(m - u) - (h - 1)(s - 1).
\]

We write

\[
d_i = he_i - r_i \quad \text{for } 1 \leq i \leq s,
\]

where \( e_i \) and \( r_i \) are integers with \( 0 \leq r_i < h \). Then

\[
J = \prod_{i=1}^{s} [a_i b^{e_i}(b^h)^{-e_i}, (a_i b^{e_i} + b^{e_i})(b^h)^{-e_i}).
\]

Furthermore, from (14) we get

\[
\sum_{i=1}^{s} r_i = 1 - s \mod h.
\]
Since $\sum_{i=1}^{s} r_i \leq (h - 1)s$, it follows that

$$\sum_{i=1}^{s} r_i \leq (h - 1)(s - 1).$$

This implies that

$$\sum_{i=1}^{s} e_i = \frac{1}{h} \sum_{i=1}^{s} d_i + \frac{1}{h} \sum_{i=1}^{s} r_i \leq m - u.$$ 

In view of (15), $J$ can thus be written as the disjoint union of $b^{r_1 + \cdots + r_s}$ elementary intervals in base $b^h$, each having volume $b^{-h(e_1 + \cdots + e_s)} \geq (b^h)^{u-m}$. Therefore, each of these elementary intervals in base $b^h$ contains exactly $b^{h(e_1 + \cdots + e_s)}$ points of a given $(u, m, s)$-net in base $b^h$ (compare with [15, Remark 4.3]), and so $J$ contains exactly $b^t$ points of the net.

**Lemma 10.** Let $b \geq 2$, $r \geq 0$, $s \geq 1$, and $0 \leq t \leq m$ be integers and let $N_1, N_2, \ldots, N_{br}$ be $(t, m, s)$-nets in base $b$. Then the multiset union $N_1 \cup N_2 \cup \cdots \cup N_{br}$ is a $(t + r, m, s)$-net in base $b$.

**Proof.** This follows by a trivial verification. ■

In the following we consider sequences in bases $b$ and $b^h$. Here it is tacitly assumed that the $b$-adic and $b^h$-adic expansions of a number are compatible, in the sense that the $b^h$-adic expansion is obtained by grouping together $h$ consecutive terms of the $b$-adic expansion at a time.

**Proposition 4.** Let $b \geq 2$, $h \geq 1$, $s \geq 1$, and $u \geq 0$ be integers. Then every $(u, s)$-sequence in base $b^h$ is a $(t, s)$-sequence in base $b$ with $t = hu + (h - 1)s$.

**Proof.** Let $x_0, x_1, \ldots$ be a given $(u, s)$-sequence in base $b^h$. With $t$ as above, we fix any integer $m > t$ and write it in the form $m = hp + r$ with integers $p$ and $r$ such that $0 \leq r < h$. Note that $p > u$. With a fixed integer $k \geq 0$, we consider the point set $N$ consisting of the points $[x_n]_{b,m}$ with $kb^m \leq n < (k + 1)b^m$. Then $N$ can be split up into $b^r$ point sets of $b^{hp}$ points, where each such point set consists of the $[x_n]_{b,m}$ with $lb^{hp} \leq n < (l + 1)b^{hp}$ for some fixed integer $l \geq 0$. Now the points $[x_n]_{b^k,p} = [x_n]_{b,lp}$ with $lb^{hp} \leq n < (l + 1)b^{hp}$ form a $(u, p, s)$-net in base $b^h$, and so it follows from Lemma 9 that the points $[x_n]_{b,m}$ with $lb^{hp} \leq n < (l + 1)b^{hp}$ form an $(hu + (h - 1)(s - 1),...
hp, s)-net in base b. An application of Lemma 10 shows that N is an 
(hu + (h - 1)(s - 1) + r, hp + r, s)-net in base b, and so a (t, m, s)-net in base b. ■

Remark 8. Let q be a prime power and s \geq 2. Determine the integer 
h \geq 1 by q^{h-1} < s \leq q^h. Then in [12, Theorem 6.18], a (0, s)-sequence in base 
q^h is constructed explicitly. By Proposition 4, this sequence is a (t, s)-
sequence in base q with 

\[ t = \left\lfloor \log_q s \right\rfloor - 1 \quad \text{for } s \geq 2, \]

where \log_q is the logarithm to the base q. The resulting bound \(t < s \log_q s\) is better than the bound obtained from [13, Corollary 1 and Theorem 2],
where a \((T_q(s), s)\)-sequence in base q is constructed. Certain actual values of \(t\) are also smaller than the corre-
sponding ones of \(T_q(s)\), for instance for \(q = 5\) and 28 \leq s \leq 32. We note also that this (t, s)-sequence in base q can be generated easily.

Proposition 5. Let b \geq 2, h \geq 1, and s \geq 1 be integers. Then 
every \((u, s)\)-sequence in base b is a \((ht, s)\)-sequence in base \(b^h\) with \(t = \left\lfloor u/h \right\rfloor\).

Proof. If \(x_0, x_1, \ldots\) is a given \((u, s)\)-sequence in base b, then it is also an \((ht, s)\)-sequence in base b. Thus, for any integers \(k \geq 0\) and \(m > t\) the points 

\[ [x_n]_{b, km} = [x_n]_{b^h, km} \quad \text{with } kb^m \leq n < (k + 1)b^m \]

form an \((ht, km, s)\)-net in base b. Now by [12, Lemma 2.9], the points 
\([x_n]_{b^h, km}\) with \(kb^m \leq n < (k + 1)b^m\) form a \((t, m, s)\)-net in base \(b^h\). ■

As in [12, Definition 8.7], for any integers \(b \geq 2\) and \(s \geq 1\) we let \(t_b(s)\) be the least value of \(t\) for which there exists a \((t, s)\)-sequence in base b. It is trivial that \(t_b(s) \leq d_b(s)\). Propositions 4 and 5 imply the following result.

Corollary 4. For all integers \(b \geq 2, h \geq 1, and s \geq 1\) we have

\[ \frac{t_b(s) - (h - 1)s}{h} \leq t_b(s) \leq \left\lceil \frac{t_b(s)}{h} \right\rceil. \]

For prime powers \(q\) we can now get an upper bound for \(t_q(s)\) with effective constants and with an explicit construction of the relevant global
function fields. In particular, we can improve the bounds for $t_q(s)$ resulting from Theorem 4(iii)–(v).

**Proposition 6.** For every prime power $q$ we have

$$t_q(s) \leq \frac{3q - 1}{q - 1} s - \frac{2qs^{1/2}}{(q^2 - 1)^{1/2}}$$

for all $s \geq 1$.

In particular, we have

$$t_2(s) \leq 5s - \frac{4}{\sqrt{3}} s^{1/2} \quad \text{for all } s \geq 1,$$

$$t_4(s) \leq 3s - \frac{3}{\sqrt{2}} s^{1/2} \quad \text{for all } s \geq 1,$$

$$t_5(s) \leq \frac{7}{2} s - \frac{5}{\sqrt{6}} s^{1/2} \quad \text{for all } s \geq 1.$$

**Proof.** We use Corollary 4 with $b = q$ and $h = 2$, together with Theorem 5, to obtain

$$t_q(s) \leq 2t_q(s) + s \leq 2V_q(s) + s \leq \frac{3q - 1}{q - 1} s - \frac{2qs^{1/2}}{(q^2 - 1)^{1/2}}. \quad \square$$

**Remark 9.** Proposition 1 and Corollary 4 imply that $t_q(s) \leq s + q^2 - q$ for any prime power $q$ and $1 \leq s \leq q^3$.

**Appendix**

Here we supply explicit global function fields which yield the lower bounds for $N_q(g)$ listed in Table II in the cases $q = 3, 4, 5$. All these examples can be verified by using [26, Proposition III.7.3, Corollary III.7.4, and Proposition III.7.8].

1. $q = 3, g = 6$. Then $N(K/F_3) = 13$ for $K = F_3(x, y_1, y_2)$ with

$$y_1^2 = x^3 - x + 1, \quad y_3^2 - y_2 = x(x - 1).$$

2. $q = 3, g = 7$. Then $N(K/F_3) = 14$ for $K = F_3(x, y_1, y_2)$ with

$$y_1^2 = -x(x^2 - x - 1), \quad y_3^2 - y_2 = \frac{x^2 - 1}{x}.$$
(3) \( q = 3, g = 8 \). Then \( N(K/F_3) = 15 \) for \( K = F_3(x, y_1, y_2) \) with
\[
y_1^2 = x^3 - x + 1, \quad y_2^2 - y_2 = \frac{x(x - 1)}{x + 1}.
\]

(4) \( q = 3, g = 9 \). Then \( N(K/F_3) = 19 \) for \( K = F_3(x, y_1, y_2) \) with
\[
y_1^3 - y_1 = x(x - 1), \quad y_2^3 - y_2 = \frac{x(x - 1)}{x + 1}.
\]

(5) \( q = 3, g = 13 \). Then \( N(K/F_3) = 21 \) for \( K = F_3(x, y_1, y_2) \) with
\[
y_1^2 = x^3 - x + 1, \quad y_2^3 - y_2 = \frac{x^3 - x}{(x^2 - x - 1)^2}.
\]

(6) \( q = 4, g = 5 \). Then \( N(K/F_4) = 16 \) for \( K = F_4(x, y_1, y_2) \) with
\[
y_1^3 + y_1 = x^3, \quad y_2^3 + y_2 = \left(\frac{y_1}{x}\right)^3.
\]

(7) \( q = 4, g = 6 \). Then \( N(K/F_4) = 17 \) for \( K = F_4(x, y_1, y_2) \) with
\[
y_1^2 + y_1 = x(x + 1)(x + a), \quad y_2^3 = x^3 + x + 1,
\]
where \( a \in F_4 \) with \( a^2 + a + 1 = 0 \).

(8) \( q = 4, g = 7 \). Then \( N(K/F_4) = 18 \) for \( K = F_4(x, y_1, y_2) \) with
\[
y_1^2 + y_1 = x(x + 1)(x + a), \quad y_2^3 + y_2 = \frac{x^2 + x + 1}{x^3 + x + 1},
\]
where \( a \in F_4 \) with \( a^2 + a + 1 = 0 \).

(9) \( q = 4, g = 10 \). Then \( N(K/F_4) = 21 \) for \( K = F_4(x, y_1, y_2) \) with
\[
y_1^3 = x^3 + x + 1, \quad y_2^3 = x^2 + x + 1.
\]

(10) \( q = 5, g = 6 \). Then \( N(K/F_5) = 21 \) for \( K = F_5(x, y) \) with
\[
y_5^5 - y = x(x - 1)(x - 2)(x - 3).
\]
REFERENCES


