Nets, (t, s)-Sequences, and Codes

Harald Niederreiter

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

Summary. Nets and (t, s)-sequences are standard sources of quasirandom points for quasi-Monte Carlo methods. Connections between nets and error-correcting codes have been noticed for a long time, and these links have become even more pronounced with the development of the duality theory for digital nets. In this paper, we further explore these fascinating connections. We present also a recent construction of digital (t, s)-sequences using global function fields and new general constructions of nets and (t, s)-sequences.

1 Introduction and Basic Definitions

Low-discrepancy point sets and sequences are the workhorses of quasi-Monte Carlo methods. Currently, the most powerful methods for the construction of low-discrepancy point sets and sequences are based on the theory of (t, m, s)-nets and (t, s)-sequences. This paper describes further contributions to this theory.

The concept of a (t, m, s)-net is a special case of the notion of a uniform point set introduced in [Nie03]. As usual in the area, we follow the convention that a *point set* is a "multiset" in the sense of combinatorics, i.e., a set in which multiplicities of elements are allowed and taken into account. We write $I^s = [0, 1]^s$ for the s-dimensional unit cube.

Definition 1. Let $(X, \mathcal{B}, \mu)$ be an arbitrary probability space and let $\mathcal{E}$ be a nonempty subset of $\mathcal{B}$. A point set $P = \{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$ of $N \geq 1$ elements of X is called $(\mathcal{E}, \mu)$-*uniform* if

$$\frac{1}{N} \sum_{n=1}^{N} \chi_E(\mathbf{x}_n) = \mu(E) \qquad \text{for all } E \in \mathcal{E},$$

where χ_E denotes the characteristic function of E.

Definition 2. Let $s \geq 1$, $b \geq 2$, and $0 \leq t \leq m$ be integers and let λ_s be the probability measure on I^s induced by the s-dimensional Lebesgue measure. Let $\mathcal{J}_{b,m,t}^{(s)}$ be the collection of all subintervals J of I^s of the form

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

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ and with $\lambda_s(J) = b^{t-m}$. Then a $(\mathcal{J}_{b,m,t}^{(s)}, \lambda_s)$-uniform point set consisting of b^m points in I^s is called a (t, m, s)-*net in base* b.

It is important to note that the smaller the value of t for given b, m, and s, the larger the family $\mathcal{J}_{b,m,t}^{(s)}$ of intervals in Definition 2, and so the stronger the uniform point set property in Definition 1. The number t is often called the *quality parameter* of a (t, m, s)-net in base b.

For the definition of a (t, s)-sequence, we need a few preliminaries. Given a real number $x \in [0, 1]$, let

$$x = \sum_{j=1}^{\infty} y_j \, b^{-j} \qquad \text{with all } y_j \in Z_b := \{0, 1, \ldots, b-1\}$$

be a b-adic expansion of x, where the case $y_j = b - 1$ for all but finitely many j is allowed. For any 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 $\mathbf{x} = (x^{(1)}, \ldots, x^{(s)}) \in I^s$ and the $x^{(i)}$, $1 \leq i \leq s$, are given by prescribed b-adic expansions, then we define

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

Definition 3. Let $s \geq 1$, $b \geq 2$, and $t \geq 0$ be integers. A sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in I^s is a (t, s)-*sequence in base* b if for all integers $k \geq 0$ and $m > t$ the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a (t, m, s)-net in base b. Here the coordinates of all points $\mathbf{x}_n$, $n = 0, 1, \ldots$, are given by prescribed b-adic expansions.

As before, we are interested in small values of t in the construction of (t, s)-sequences. We call t the *quality parameter* of a (t, s)-sequence in base b. For general background on (t, m, s)-nets and (t, s)-sequences, we refer to the monograph [Nie92] and the recent survey article [Nie05].

The rest of the paper is organized as follows. In Section 2, we recall the digital method for the construction of (t, m, s)-nets and (t, s)-sequences. Section 3

presents a review of the duality theory for digital nets and its connections with the theory of error-correcting codes. Recent constructions of digital nets using duality theory and other links with coding theory are described in Section 4. The recent construction in [MN] of digital (t, s)-sequences using differentials in global function fields is presented in Section 5, together with upper bounds on the well-known quantity $d_q(s)$. Sections 6 and 7 contain new ideas on how to generalize the digital method for the construction of (t, m, s)-nets and (t, s)-sequences, respectively.

2 Digital Nets and Digital (t, s)-Sequences

Most of the known constructions of (t, m, s)-nets and (t, s)-sequences are based on the so-called digital method introduced in [Nie87, Section 6]. In order to describe the digital method for the construction of (t, m, s)-nets in base b, we need the following ingredients. First of all, let integers $m \geq 1$, $s \geq 1$, and $b \geq 2$ be given. Then we choose the following:

(i) a commutative ring R with identity and $\mathrm{card}(R) = b$;
(ii) bijections $\eta_j^{(i)} : R \to Z_b$ for $1 \leq i \leq s$ and $1 \leq j \leq m$;
(iii) $m \times m$ matrices $C^{(1)}, \ldots, C^{(s)}$ over R.

Now let $\mathbf{r} \in R^m$ be an m-tuple of elements of R and define

$$p_j^{(i)}(\mathbf{r}) = \eta_j^{(i)}(\mathbf{c}_j^{(i)} \cdot \mathbf{r}) \in Z_b \qquad \text{for } 1 \leq i \leq s,\ 1 \leq j \leq m,$$

where $\mathbf{c}_j^{(i)}$ is the jth row of the matrix $C^{(i)}$ and $\cdot$ denotes the inner product. Next we put

$$p^{(i)}(\mathbf{r}) = \sum_{j=1}^{m} p_j^{(i)}(\mathbf{r})\, b^{-j} \in [0, 1] \qquad \text{for } 1 \leq i \leq s$$

and

$$P(\mathbf{r}) = (p^{(1)}(\mathbf{r}), \ldots, p^{(s)}(\mathbf{r})) \in I^s.$$

By letting $\mathbf{r}$ range over all b^m possibilities in R^m, we arrive at a point set P consisting of b^m points in I^s.

Definition 4. If the point set P constructed above forms a (t, m, s)-net in base b, then it is called a *digital (t, m, s)-net in base b*. If we want to emphasize that the construction uses the ring R, then we speak also of a *digital (t, m, s)-net over R*.

The quality parameter of a digital (t, m, s)-net over R depends only on the so-called *generating matrices* $C^{(1)}, \ldots, C^{(s)}$ over R. A convenient algebraic condition on the generating matrices to guarantee a certain value of t is known (see [Nie92, Theorem 4.26]), and a generalization of this condition will be given in Theorem 7 below.

For (t, s)-sequences the order of the terms is important, and so in the constructions care has to be taken that the points are obtained in a suitable order. We present the digital method for the construction of (t, s)-sequences in base b in the form given in [NX96b, Section 2] which is somewhat more general than the original version in [Nie87, Section 6]. Let integers $s \geq 1$ and $b \geq 2$ be given. Then we choose the following:

(i) a commutative ring R with identity and $\mathrm{card}(R) = b$;
(ii) bijections $\psi_r : Z_b \to R$ for $r = 0, 1, \ldots$, with $\psi_r(0) = 0$ for all sufficiently large r;
(iii) bijections $\eta_j^{(i)} : R \to Z_b$ for $1 \leq i \leq s$ and $j \geq 1$;
(iv) $\infty \times \infty$ matrices $C^{(1)}, \ldots, C^{(s)}$ over R.

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

$$n = \sum_{r=0}^{\infty} a_r(n)\, b^r \tag{1}$$

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

$$\mathbf{n} = (\psi_r(a_r(n)))_{r=0}^{\infty} \in R^{\infty}. \tag{2}$$

Next we define

$$y_{n,j}^{(i)} = \eta_j^{(i)}(\mathbf{c}_j^{(i)} \cdot \mathbf{n}) \in Z_b \qquad \text{for } n \geq 0,\ 1 \leq i \leq s, \text{ and } j \geq 1,$$

where $\mathbf{c}_j^{(i)}$ is the jth row of the matrix $C^{(i)}$. Note that the inner product $\mathbf{c}_j^{(i)} \cdot \mathbf{n}$ makes sense since $\mathbf{n}$ has only finitely many nonzero coordinates. Then we put

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

Finally, we define the sequence S consisting of the points

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

Definition 5. If the sequence S constructed above forms a (t, s)-sequence in base b, then it is called a *digital (t, s)-sequence in base b*. If we want to emphasize that the construction uses the ring R, then we speak also of a *digital (t, s)-sequence over R*.

As in the case of digital (t, m, s)-nets, the quality parameter of a digital (t, s)-sequence over R depends only on the *generating matrices* $C^{(1)}, \ldots, C^{(s)}$ over R. A convenient algebraic condition on the generating matrices to guarantee a certain value of t is known (see [NX96b, Lemma 7 and Remark 4]), and a generalization of this condition will be given in Theorem 8 below.

The standard low-discrepancy sequences used nowadays in quasi-Monte Carlo methods, such as the sequences of Sobol' [Sob67], Faure [Fau82], and

Niederreiter [Nie88] as well as the sequences obtained by Niederreiter and Xing using algebraic-geometry methods (see [NX01, Chapter 8] for an exposition of the latter constructions), are all digital (t, s)-sequences. There are interesting generalizations and variants of (digital) (t, s)-sequences which we will not discuss here; see for instance Dick [Dic06b], [Dic06a] and Larcher and Niederreiter [LN95].

3 Codes and Duality Theory

It is known since the first paper [Nie87] on the general theory of (t, m, s)-nets and (t, s)-sequences that there are interesting links between digital nets and error-correcting codes. Recently, these links have become more pronounced with the development of a duality theory for digital nets which puts digital nets squarely into a framework of a distinctly coding-theoretic nature.

We recall the rudiments of coding theory. We refer to MacWilliams and Sloane [MWS77] for a full treatment of coding theory and to Ling and Xing [LX04] for an introduction to the area. Let $\mathbb{F}_q$ be the finite field with q elements, where q is an arbitrary prime power. For an integer $n \geq 1$, we consider the n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. The number of nonzero coordinates of $\mathbf{a} \in \mathbb{F}_q^n$ is the Hamming weight $w(\mathbf{a})$. Then $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b})$ for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ defines the Hamming metric. The vector space $\mathbb{F}_q^n$, endowed with the Hamming metric, is the Hamming space $\mathbb{F}_q^n$. A linear code over $\mathbb{F}_q$ is a nonzero $\mathbb{F}_q$-linear subspace C of the Hamming space $\mathbb{F}_q^n$. The minimum distance $\delta(C)$ of C is defined by

$$\delta(C) = \min \{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in C,\ \mathbf{a} \neq \mathbf{b}\}.$$

It is easy to see that we also have

$$\delta(C) = \min_{\mathbf{a} \in C \setminus \{\mathbf{0}\}} w(\mathbf{a}).$$

One of the principal aims of coding theory is to construct linear codes C over $\mathbb{F}_q$ with a large minimum distance $\delta(C)$ for given n and $k = \dim(C)$, or with a large relative minimum distance $\frac{\delta(C)}{n}$ for a given information rate $\frac{k}{n}$.

We now describe the duality theory for digital nets developed by Niederreiter and Pirsic [NP01]. We mention in passing that a completely different application of coding theory to multidimensional numerical integration occurs in the recent paper of Kuperberg [Kup06].

We first have to generalize the definition of the Hamming space. Let $m \geq 1$ and $s \geq 1$ be integers; they will have the same meaning as m and s in a digital (t, m, s)-net over $\mathbb{F}_q$. The following weight function V_m on $\mathbb{F}_q^{ms}$ was introduced by Niederreiter [Nie86] and later used in an equivalent form in coding theory by Rosenbloom and Tsfasman [RT97]. We start by defining a weight function

v on $\mathbb{F}_q^m$. We put $v(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0} \in \mathbb{F}_q^m$, and for $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ with $\mathbf{a} \neq \mathbf{0}$ we set

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

Then we extend this definition to $\mathbb{F}_q^{ms}$ by writing a vector $\mathbf{A} \in \mathbb{F}_q^{ms}$ as the concatenation of s vectors of length m, that is,

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

and putting

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

Note that $d_m(\mathbf{A}, \mathbf{B}) = V_m(\mathbf{A} - \mathbf{B})$ for $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{ms}$ defines a metric on $\mathbb{F}_q^{ms}$ which for $m = 1$ reduces to the Hamming metric on $\mathbb{F}_q^s$.

Definition 6. The *minimum distance* $\delta_m(\mathcal{N})$ of a nonzero $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ is given by

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

Now let the $m \times m$ matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{F}_q$ be the generating matrices of a digital net P. Set up an $m \times ms$ matrix M as follows: for $1 \le j \le m$, the jth row of M is obtained by concatenating the jth columns of $C^{(1)}, \ldots, C^{(s)}$. Let $\mathcal{M} \subseteq \mathbb{F}_q^{ms}$ be the row space of M and let $\mathcal{M}^\perp$ be its dual space as in coding theory, that is,

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

Then we have the following results from [NP01].

Theorem 1. *Let $m \ge 1$ and $s \ge 2$ be integers. Then, with the notation above, the point set P is a digital (t, m, s)-net over $\mathbb{F}_q$ if and only if*

$$\delta_m(\mathcal{M}^\perp) \ge m - t + 1.$$

Corollary 1. *Let $m \ge 1$ and $s \ge 2$ be integers. Then from any $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ with $\dim(\mathcal{N}) \ge ms - m$ we can construct a digital (t, m, s)-net over $\mathbb{F}_q$ with*

$$t = m + 1 - \delta_m(\mathcal{N}).$$

Note that $\mathcal{N}$ in Corollary 1 plays the role of $\mathcal{M}^\perp$ in Theorem 1. Since $\mathcal{M}$ as the row space of an $m \times ms$ matrix has dimension at most m, we must have

$$\dim(\mathcal{N}) = \dim(\mathcal{M}^\perp) = ms - \dim(\mathcal{M}) \ge ms - m,$$

which explains the condition on $\dim(\mathcal{N})$ in Corollary 1.

It is of interest to note that the line of research started by Rosenbloom and Tsfasman [RT97] in coding theory was continued in that area. Some of the theorems obtained in this direction can be translated into results on digital nets. Typical coding-theoretic papers on this topic are Dougherty and Skriganov [DS02] and Siap and Ozen [SO04].

4 Digital Nets Inspired by Codes

Corollary 1 is a powerful tool for the construction of digital nets. It was already used in the paper [NP01] that introduced duality theory, where it was applied to obtain an analog of the classical $(u, u + v)$ construction of codes. An improved version of the $(u, u + v)$ construction for digital nets was given by Bierbrauer, Edel, and Schmid [BES02]. A considerable generalization of this construction was obtained by Niederreiter and Özbudak [NO04] who designed an analog of the matrix-product construction of codes. This yields the following result.

Theorem 2. *Let h be an integer with $2 \le h \le q$. If for $k = 1, \ldots, h$ there exists a digital (t_k, m_k, s_k)-net over $\mathbb{F}_q$ and if $s_1 \le \cdots \le s_h$, then there exists a digital $(t, \sum_{k=1}^{h} m_k, \sum_{k=1}^{h} s_k)$-net over $\mathbb{F}_q$ with*

$$t = 1 + \sum_{k=1}^{h} m_k - \min_{1 \le k \le h} (h - k + 1)(m_k - t_k + 1).$$

The $(u, u + v)$ construction of digital nets is the special case $h = 2$ of Theorem 2. The matrix-product construction of codes and digital nets affords a way of combining given linear codes, respectively digital nets, to produce a new linear code, respectively digital net. Another principle of this type is obtained by the Kronecker-product construction which is well known in coding theory. Kronecker-product constructions of digital nets were proposed by Bierbrauer, Edel, and Schmid [BES02] and Niederreiter and Pirsic [NP02].

Further links between coding theory and digital nets can be established by considering special families of linear codes and searching for their analogs in the realm of digital nets. For instance, an important special type of linear code is a cyclic code, i.e., a linear code that is invariant under cyclic shifts. An analog for digital nets was introduced by Niederreiter [Nie04] who adopted the viewpoint that cyclic codes can be defined by prescribing roots of polynomials (compare with [LN94, Section 8.2]). For integers $m \ge 1$ and $s \ge 2$, consider the vector space

$$\mathcal{P} = \{f \in \mathbb{F}_{q^m}[x] : \deg(f) < s\}$$

of polynomials over the extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. Note that $\dim(\mathcal{P}) = ms$ as a vector space over $\mathbb{F}_q$. We fix an element $\alpha \in \mathbb{F}_{q^m}$ and define

$$\mathcal{P}_\alpha = \{f \in \mathcal{P} : f(\alpha) = 0\}.$$

It is clear that $\mathcal{P}_\alpha$ is an $\mathbb{F}_q$-linear subspace of $\mathcal{P}$ with $\dim(\mathcal{P}_\alpha) = ms - m$ as a vector space over $\mathbb{F}_q$. For each $i = 1, \ldots, s$, we choose an ordered basis B_i of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Next we set up a map $\tau : \mathcal{P} \to \mathbb{F}_q^{ms}$ in the following way. Take $f \in \mathcal{P}$ and write this polynomial explicitly as

$$f(x) = \sum_{i=1}^{s} \gamma_i \, x^{i-1}$$

with $\gamma_i \in \mathbb{F}_{q^m}$ for $1 \le i \le s$. For each $i = 1, \ldots, s$, let $\mathbf{c}_i(f) \in \mathbb{F}_q^m$ be the coordinate vector of γ_i with respect to the ordered basis B_i. Then we define

$$\tau : f \in \mathcal{P} \mapsto (\mathbf{c}_1(f), \ldots, \mathbf{c}_s(f)) \in \mathbb{F}_q^{ms}.$$

It is obvious that τ is an $\mathbb{F}_q$-linear isomorphism from $\mathcal{P}$ onto $\mathbb{F}_q^{ms}$. Finally, let $\mathcal{N}_\alpha$ be the image of the subspace $\mathcal{P}_\alpha$ under τ. Since τ is an isomorphism, we have

$$\dim(\mathcal{N}_\alpha) = \dim(\mathcal{P}_\alpha) = ms - m$$

as a vector space over $\mathbb{F}_q$. Thus, we can apply Corollary 1 to the $\mathbb{F}_q$-linear subspace $\mathcal{N}_\alpha$ of $\mathbb{F}_q^{ms}$. The resulting digital net is called a *cyclic digital net* over $\mathbb{F}_q$ relative to the bases $B_1, \ldots, B_s$. A theorem guaranteeing the existence of good cyclic digital nets was recently shown by Pirsic, Dick, and Pillichshammer [PDP06].

A powerful family of linear codes is that of algebraic-geometry codes. A general framework for constructing digital nets by means of algebraic curves over finite fields, or equivalently by global function fields, was developed by Niederreiter and Özbudak [NO02]. The basic construction in [NO02] uses a global function field F with full constant field $\mathbb{F}_q$ (see Section 5 for the definition of these terms) and a divisor G of F. An $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ is defined as the image of the Riemann-Roch space $\mathcal{L}(G)$ under an $\mathbb{F}_q$-linear map from $\mathcal{L}(G)$ to $\mathbb{F}_q^{ms}$ derived from the local expansions of elements of $\mathcal{L}(G)$ at distinct places $Q_1, \ldots, Q_s$ of F. Under suitable conditions, we can invoke Corollary 1 to arrive at a digital (t, m, s)-net over $\mathbb{F}_q$ for some t.

We end this section by describing a recent construction of digital nets due to Pirsic, Dick, and Pillichshammer [PDP06]. For an integer $m \ge 1$ consider, as earlier in this section, the extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. Then, for an integer $s \ge 2$, we take the s-dimensional vector space $\mathcal{Q} := \mathbb{F}_{q^m}^s$ over $\mathbb{F}_{q^m}$ which has dimension ms as a vector space over $\mathbb{F}_q$. Now fix $\boldsymbol{\alpha} \in \mathcal{Q}$ with $\boldsymbol{\alpha} \ne \mathbf{0}$ and put

$$\mathcal{Q}_{\boldsymbol{\alpha}} = \{\boldsymbol{\gamma} \in \mathcal{Q} : \boldsymbol{\alpha} \cdot \boldsymbol{\gamma} = 0\}.$$

Clearly, $\mathcal{Q}_{\boldsymbol{\alpha}}$ is an $\mathbb{F}_{q^m}$-linear subspace of $\mathcal{Q}$ of dimension $s-1$, and so $\mathcal{Q}_{\boldsymbol{\alpha}}$ has dimension $ms - m$ as a vector space over $\mathbb{F}_q$. Since $\mathcal{Q}$ and $\mathbb{F}_q^{ms}$ are isomorphic as vector spaces over $\mathbb{F}_q$, we get in this way an $\mathbb{F}_q$-linear subspace $\mathcal{N}_{\boldsymbol{\alpha}}$ of $\mathbb{F}_q^{ms}$ of dimension $ms - m$ as a vector space over $\mathbb{F}_q$. Thus, we can apply Corollary 1 to obtain a digital (t, m, s)-net over $\mathbb{F}_q$ for some t. A digital net produced by this construction is called a *hyperplane net*. An analysis of how hyperplane nets, cyclic digital nets, and other types of digital nets are related among each other was carried out by Pirsic [Pir05].

5 Constructing Digital (t, s)-Sequences from Differentials

There are altogether four known constructions of digital (t, s)-sequences based on general global function fields, all of them due to Niederreiter and Xing.

A systematic account of these constructions is given in Niederreiter and Xing [NX96a]. In this section, we describe the first new construction of digital (t, s)-sequences using global function fields since 1996. It is also the first construction using differentials in global function fields. This construction is due to Mayor and Niederreiter [MN].

Let F be a global function field with constant field $\mathbb{F}_q$, that is, F is a finite extension of the rational function field $\mathbb{F}_q(x)$. We assume that $\mathbb{F}_q$ is the full constant field of F, which means that $\mathbb{F}_q$ is algebraically closed in F. We refer to the book of Stichtenoth [Sti93] for general background and terminology on global function fields.

Let $\mathbf{P}_F$ be the set of places of F and Ω_F the set of differentials of F, that is,

$$\Omega_F = \{f\,dz : f \in F,\ z \text{ is a separating element for } F\}.$$

For any $\omega \in \Omega_F$ and separating element z, we can write $\omega = f\,dz$ with a unique $f \in F$. If $\omega \in \Omega_F^*$ is a nonzero differential, then for every $Q \in \mathbf{P}_F$ let $\omega = f_Q\,dt_Q$, where $t_Q \in F$ is a local parameter at Q (and hence a separating element). Then we can associate ω with the divisor

$$(\omega) := \sum_{Q \in \mathbf{P}_F} \nu_Q(f_Q)\,Q,$$

where ν_Q is the normalized valuation of F corresponding to the place Q. For any divisor G of F, we define

$$\Omega(G) = \{\omega \in \Omega_F^* : (\omega) \geq G\} \cup \{0\}.$$

Note that $\Omega(G)$ is a finite-dimensional vector space over $\mathbb{F}_q$.

Now let the dimension $s \geq 1$ in the construction of a digital (t, s)-sequence be given. We assume that F contains at least one rational place Q_∞; recall that a rational place is a place of degree 1. Choose a divisor D of F with $\deg(D) = -2$ and Q_∞ not in the support of D (such a divisor always exists). Furthermore, let $Q_1, \ldots, Q_s$ be s distinct places of F with $Q_i \neq Q_\infty$ for $1 \leq i \leq s$, and put $e_i = \deg(Q_i)$ for $1 \leq i \leq s$.

The Riemann-Roch theorem can be used to show that $\dim(\Omega(D)) = g + 1$, $\dim(\Omega(D + Q_\infty)) = g$, and $\dim(\Omega(D + (2g+1)Q_\infty)) = 0$, where g is the genus of F. Hence there exist integers $0 = n_0 < n_1 < \cdots < n_g \leq 2g$ such that

$$\dim(\Omega(D + n_u Q_\infty)) = \dim(\Omega(D + (n_u + 1)Q_\infty)) + 1 \qquad \text{for } 0 \leq u \leq g.$$

Now we choose

$$\omega_u \in \Omega(D + n_u Q_\infty) \setminus \Omega(D + (n_u + 1)Q_\infty) \qquad \text{for } 0 \leq u \leq g.$$

It is easily seen that $\{\omega_0, \omega_1, \ldots, \omega_g\}$ is a basis of $\Omega(D)$. For $i = 1, \ldots, s$, consider the chain

$$\Omega(D) \subset \Omega(D - Q_i) \subset \Omega(D - 2Q_i) \subset \ldots$$

of vector spaces over $\mathbb{F}_q$. By starting from the basis $\{\omega_0, \omega_1, \ldots, \omega_g\}$ of $\Omega(D)$ and successively adding basis vectors at each step of the chain, we obtain for each integer $n \geq 1$ a basis

$$\{\omega_0, \omega_1, \ldots, \omega_g, \omega_1^{(i)}, \omega_2^{(i)}, \ldots, \omega_{ne_i}^{(i)}\}$$

of $\Omega(D - nQ_i)$. Now let $z \in F$ be a local parameter at Q_∞. For $r = 0, 1, \ldots$ we put

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

Note that $\nu_{Q_\infty}((z_r)) = r$ for all $r \geq 0$. For $1 \leq i \leq s$ and $j \geq 1$, we have $\omega_j^{(i)} \in \Omega(D - kQ_i)$ for some $k \geq 1$ and also Q_∞ not in the support of $D - kQ_i$, hence $\nu_{Q_\infty}((\omega_j^{(i)})) \geq 0$. Thus, we have local expansions at Q_∞ of the form

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

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 $u \in \{0, 1, \ldots, g\}$. Then we put

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

Finally, for each $i = 1, \ldots, s$, we let $C^{(i)}$ be the $\infty \times \infty$ matrix over $\mathbb{F}_q$ whose jth row is $\mathbf{c}_j^{(i)}$ for $j = 1, 2, \ldots$. We write $S_\Omega(Q_\infty, Q_1, \ldots, Q_s; D)$ for a sequence obtained from the generating matrices $C^{(1)}, \ldots, C^{(s)}$ by the digital method (compare with Section 2). The following result was shown by Mayor and Niederreiter [MN].

Theorem 3. *Let F be a global function field with full constant field $\mathbb{F}_q$ and with at least one rational place Q_∞. Let D be a divisor of F with $\deg(D) = -2$ and Q_∞ not in the support of D. Furthermore, let $Q_1, \ldots, Q_s$ be distinct places of F with $Q_i \neq Q_\infty$ for $1 \leq i \leq s$. Then $S_\Omega(Q_\infty, Q_1, \ldots, Q_s; D)$ is a digital (t, s)-sequence over $\mathbb{F}_q$ with*

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

where g is the genus of F and $e_i = \deg(Q_i)$ for $1 \leq i \leq s$.

We report now on further results from the paper [MN]. We use the standard notation $d_q(s)$ for the least value of t such that there exists a digital (t, s)-sequence over $\mathbb{F}_q$.

Example 1. Let $q = 5$ and $s = 32$. Let F be the global function field given by $F = \mathbb{F}_5(x, y_1, y_2)$ with

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

Then F has 32 rational places $Q_\infty, Q_1, \ldots, Q_{31}$ and genus $g = 11$. Furthermore, F has at least one place Q_{32} of degree 2 lying over the place $x^2 + 2x - 2$ of $\mathbb{F}_5(x)$. We can choose $D = -2Q_1$. Now we consider the sequence $S_\Omega(Q_\infty, Q_1, \ldots, Q_{32}; D)$ and apply Theorem 3. We have $e_i = 1$ for $1 \le i \le 31$ and $e_{32} = 2$, therefore $t = 12$. Hence we obtain $d_5(32) \le 12$, which is an improvement on the previously best bound $d_5(32) \le 13$ given in [Nie05, Table 1]. This improved value has already been entered into the database at

`http://mint.sbg.ac.at`

for parameters of (t, m, s)-nets and (t, s)-sequences (see [SS06] for a description of this database).

Theorem 4. *For every odd prime p and every dimension $s \ge 1$, we have*

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

Theorem 5. *For every odd prime p and every dimension $s \ge 1$, we have*

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

Theorem 6. *For every prime power q and every dimension $s \ge 1$, we have*

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

Theorems 4, 5, and 6 are derived from Theorem 3 by using towers of global function fields that were constructed in the last few years (see [MN] for the details).

Very recently, Niederreiter and Özbudak [NO07] used differentials in global function fields and the duality theory for digital nets to give a new construction of $(\mathbf{T}, s)$-sequences in the sense of [LN95]. In various cases, this construction yields low-discrepancy sequences with better discrepancy bounds than previous constructions.

6 A General Construction of Nets

We present a method of constructing (t, m, s)-nets which generalizes the digital method in Section 2. The idea is to move away from linear algebra and to allow for nonlinearity in the construction. This is motivated by the well-known

fact in coding theory that there are good parameters of nonlinear codes that cannot be achieved by linear codes (see [LX04, Section 5.6]). One would hope for a similar phenomenon for nets, namely that there are parameters of nets attainable by "nonlinear" constructions, but not by the digital method in Section 2.

As in Section 2, let integers $m \geq 1$, $s \geq 1$, and $b \geq 2$ be given. We recall that $Z_b = \{0, 1, \ldots, b-1\}$ denotes the set of digits in base b. Then we choose the following:

(i) a set R with $\mathrm{card}(R) = b$;
(ii) bijections $\eta_j^{(i)} : R \to Z_b$ for $1 \leq i \leq s$ and $1 \leq j \leq m$;
(iii) maps $\phi_j^{(i)} : R^m \to R$ for $1 \leq i \leq s$ and $1 \leq j \leq m$.

Now let $\mathbf{r} \in R^m$ and define

$$p^{(i)}(\mathbf{r}) = \sum_{j=1}^{m} \eta_j^{(i)}(\phi_j^{(i)}(\mathbf{r}))\, b^{-j} \in [0,1] \qquad \text{for } 1 \leq i \leq s$$

and

$$P(\mathbf{r}) = (p^{(1)}(\mathbf{r}), \ldots, p^{(s)}(\mathbf{r})) \in I^s.$$

By letting $\mathbf{r}$ range over all b^m possibilities in R^m, we arrive at a point set P consisting of b^m points in I^s.

Theorem 7. *The point set P constructed above forms a (t, m, s)-net in base b if and only if for any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = m - t$ and any $f_j^{(i)} \in R$, $1 \leq j \leq d_i$, $1 \leq i \leq s$, the system of $m - t$ equations*

$$\phi_j^{(i)}(z_1, \ldots, z_m) = f_j^{(i)} \qquad \text{for } 1 \leq j \leq d_i,\ 1 \leq i \leq s, \tag{3}$$

in the unknowns $z_1, \ldots, z_m$ over R has exactly b^t solutions.

Proof. Assume that (3) satisfies the given condition. According to Definition 2, we have to show that every 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 $1 \leq i \leq s$ and with $\sum_{i=1}^{s} d_i = m - t$ contains exactly b^t points of the point set P. For $1 \leq i \leq s$, let

$$a_i = \sum_{j=1}^{d_i} a_{i,j}\, b^{d_i - j}$$

be the digit expansion in base b, where all $a_{i,j} \in Z_b$. For the points $P(\mathbf{r})$ of P, we have $P(\mathbf{r}) \in J$ if and only if

$$p^{(i)}(\mathbf{r}) \in [a_i b^{-d_i}, (a_i + 1)b^{-d_i}) \qquad \text{for } 1 \le i \le s.$$

This is equivalent to

$$\eta_j^{(i)}(\phi_j^{(i)}(\mathbf{r})) = a_{i,j} \qquad \text{for } 1 \le j \le d_i,\ 1 \le i \le s,$$

which is, in turn, equivalent to

$$\phi_j^{(i)}(\mathbf{r}) = (\eta_j^{(i)})^{-1}(a_{i,j}) \qquad \text{for } 1 \le j \le d_i,\ 1 \le i \le s,$$

where $(\eta_j^{(i)})^{-1}$ denotes the inverse map of $\eta_j^{(i)}$. By hypothesis, the last system of equations has exactly b^t solutions $\mathbf{r} \in R^m$, and so P forms a (t, m, s)-net in base b. This shows the sufficiency part of the theorem. The converse is proved by similar arguments. □

Remark 1. The digital method for the construction of nets described in Section 2 is the special case of the present construction where R is a commutative ring with identity and the maps $\phi_j^{(i)}$ are linear forms in m variables over R. It can be argued that the construction principle in the present section is also a digital method since the coordinates of the points of the net are obtained digit by digit. We propose to refer to the nets produced by the method in this section also as *digital* (t, m, s)*-nets in base* b or as *digital* (t, m, s)*-nets over* R. The nets in Section 2 could then be called *linear digital* (t, m, s)*-nets in base* b or *linear digital* (t, m, s)*-nets over* R, to emphasize that they are obtained by the use of linear forms $\phi_j^{(i)}$.

The construction principle described above is too general to be useful in practice, so it is meaningful to consider situations in which we can introduce some structure. If we choose for R a finite field $\mathbb{F}_q$, then each map $\phi_j^{(i)} : \mathbb{F}_q^m \to \mathbb{F}_q$ can be represented by a polynomial over $\mathbb{F}_q$ in m variables and of degree less than q in each variable (see [LN97, Section 7.5]). We assume that the maps $\phi_j^{(i)}$, $1 \le i \le s$, $1 \le j \le m$, are so represented. Then, by using the concept of an orthogonal system of polynomials in $\mathbb{F}_q$ (see [LN97, Definition 7.35]), we obtain the following consequence of Theorem 7.

Corollary 2. *Let the point set P be obtained by the construction in this section with $R = \mathbb{F}_q$. Then P is a (t, m, s)-net in base q if and only if for any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^s d_i = m - t$ the polynomials $\phi_j^{(i)}$, $1 \le j \le d_i$, $1 \le i \le s$, form an orthogonal system in $\mathbb{F}_q$.*

There are several useful criteria for orthogonal systems of polynomials in $\mathbb{F}_q$. One such criterion, due to Niederreiter [Nie71] and given in Proposition 1 below, is in terms of permutation polynomials over $\mathbb{F}_q$. We recall that a polynomial over $\mathbb{F}_q$ (in one or several variables) is called a permutation polynomial over $\mathbb{F}_q$ if it attains each value of $\mathbb{F}_q$ equally often (see [LN97, Chapter 7] for the theory of permutation polynomials).

Proposition 1. *Let $1 \le h \le m$ be integers and let $g_1, \ldots, g_h \in \mathbb{F}_q[z_1, \ldots, z_m]$. Then $g_1, \ldots, g_h$ form an orthogonal system of polynomials in $\mathbb{F}_q$ if and only if for all $b_1, \ldots, b_h \in \mathbb{F}_q$ not all 0, the polynomial $b_1 g_1 + \cdots + b_h g_h$ is a permutation polynomial over $\mathbb{F}_q$.*

It follows, in particular, that every polynomial occurring in an orthogonal system of polynomials in $\mathbb{F}_q$ is a permutation polynomial over $\mathbb{F}_q$. In view of Corollary 2, this shows that a necessary condition for the polynomials $\phi_j^{(i)}$, $1 \le i \le s$, $1 \le j \le m$, to yield a (t, m, s)-net in base q is that each polynomial $\phi_j^{(i)}$ with $1 \le i \le s$ and $1 \le j \le m - t$ is a permutation polynomial over $\mathbb{F}_q$.

Example 2. Let q be an arbitrary prime power and let $m \ge 1$ be an integer. We start from a permutation polynomial g over $\mathbb{F}_{q^m}$ in one variable, for instance, $g(z) = \gamma z^k$ with $\gamma \in \mathbb{F}_{q^m}^*$ and an integer $k \ge 1$ satisfying $\gcd(k, q^m - 1) = 1$ (see [LN97, Section 7.2]). Let $B = \{\beta_1, \ldots, \beta_m\}$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and for each $\alpha \in \mathbb{F}_{q^m}$ let $(c_1(\alpha), \ldots, c_m(\alpha)) \in \mathbb{F}_q^m$ be the coordinate vector of α with respect to B. Then there exist polynomials $g_1, \ldots, g_m \in \mathbb{F}_q[z_1, \ldots, z_m]$ such that

$$g(\alpha) = \sum_{j=1}^{m} g_j(c_1(\alpha), \ldots, c_m(\alpha))\beta_j \qquad \text{for all } \alpha \in \mathbb{F}_{q^m}.$$

Since g is a permutation polynomial over $\mathbb{F}_{q^m}$, it follows that $g_1, \ldots, g_m$ form an orthogonal system of polynomials in $\mathbb{F}_q$. Now we put $R = \mathbb{F}_q$ and $s = 2$ in the construction in this section, and we define the polynomials

$$\phi_j^{(1)} = g_j \qquad \text{for } 1 \le j \le m,$$
$$\phi_j^{(2)} = g_{m-j+1} \quad \text{for } 1 \le j \le m.$$

Then it is clear that for any integers $d_1 \ge 0$ and $d_2 \ge 0$ with $d_1 + d_2 = m$, the polynomials $\phi_1^{(1)}, \ldots, \phi_{d_1}^{(1)}, \phi_1^{(2)}, \ldots, \phi_{d_2}^{(2)}$ form an orthogonal system in $\mathbb{F}_q$. Thus, by Corollary 2, we obtain a digital $(0, m, 2)$-net over $\mathbb{F}_q$ (in the sense of Remark 1). This net can be viewed as a scrambled version of the well-known two-dimensional Hammersley net in base q.

7 A General Construction of (t, s)-Sequences

In this section, we present an analog of the construction principle in Section 6 for (t, s)-sequences. Let integers $s \ge 1$ and $b \ge 2$ be given. Then we choose the following:

(i) a set R with $\mathrm{card}(R) = b$ and a distinguished element $o \in R$;

(ii) bijections $\psi_r : Z_b \to R$ for $r = 0, 1, \ldots$, with $\psi_r(0) = o$ for all sufficiently large r;

(iii) bijections $\eta_j^{(i)} : R \to Z_b$ for $1 \le i \le s$ and $j \ge 1$;

(iv) maps $\phi_j^{(i)} : \mathcal{F} \to R$ for $1 \le i \le s$ and $j \ge 1$, where $\mathcal{F}$ is the set of all sequences of elements of R with only finitely many terms $\neq o$.
For $n = 0, 1, \ldots$, we define $\mathbf{n}$ by (1) and (2) and observe that $\mathbf{n} \in \mathcal{F}$. Next we define

$$y_{n,j}^{(i)} = \eta_j^{(i)}(\phi_j^{(i)}(\mathbf{n})) \in Z_b \qquad \text{for } n \ge 0,\ 1 \le i \le s, \text{ and } j \ge 1.$$

Then we put

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

Finally, we define the sequence S consisting of the points

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

Theorem 8. *The sequence S constructed above is a (t, s)-sequence in base b if and only if for any integer $m > t$, any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = m - t$, and any $f_j^{(i)} \in R$, $1 \le j \le d_i$, $1 \le i \le s$, the system of $m - t$ equations*

$$\phi_j^{(i)}(z_0, z_1, \ldots) = f_j^{(i)} \qquad \text{for } 1 \le j \le d_i,\ 1 \le i \le s, \tag{4}$$

has the following property: if the values of the variables $z_m, z_{m+1}, \ldots$ are fixed in R in such a way that $z_r = o$ for all sufficiently large r, then the resulting system in the unknowns $z_0, z_1, \ldots, z_{m-1}$ over R has exactly b^t solutions.

Proof. In order to prove the sufficiency, we proceed by Definition 3. For given integers $k \ge 0$ and $m > t$, we consider the point set $P_{k,m}$consisting of the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \le n < (k+1)b^m$. We have to show that $P_{k,m}$ is a (t, m, s)-net in base b. Let J be an interval of the form

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

with integers $d_i \ge 0$ and $0 \le a_i < b^{d_i}$ for $1 \le i \le s$ and with $\sum_{i=1}^{s} d_i = m - t$. Then we have to prove that J contains exactly b^t points of $P_{k,m}$. For $1 \le i \le s$, let

$$a_i = \sum_{j=1}^{d_i} a_{i,j}\, b^{d_i - j}$$

be the digit expansion in base b, where all $a_{i,j} \in Z_b$. For the points of $P_{k,m}$ we have $[\mathbf{x}_n]_{b,m} \in J$ if and only if

$$[x_n^{(i)}]_{b,m} \in [a_i b^{-d_i}, (a_i + 1)b^{-d_i}) \qquad \text{for } 1 \le i \le s.$$

This is equivalent to

$$y_{n,j}^{(i)} = a_{i,j} \qquad \text{for } 1 \le j \le d_i,\ 1 \le i \le s,$$

which is, in turn, equivalent to

$$\phi_j^{(i)}(\mathbf{n}) = (\eta_j^{(i)})^{-1}(a_{i,j}) \qquad \text{for } 1 \le j \le d_i,\ 1 \le i \le s. \tag{5}$$

Recall that the range for n is $kb^m \le n < (k+1)b^m$. In this range, the digits $a_r(n)$ of n in (1) are prescribed for $r \ge m$, whereas the $a_r(n)$ with $0 \le r \le m-1$ can vary freely over Z_b. This means that the coordinates $\psi_r(a_r(n))$ of $\mathbf{n}$ in (2) are fixed for $r \ge m$ and they can vary freely over R for $0 \le r \le m-1$. Thus, the system (5) of $m-t$ equations is of the form (4), and so by the given property, (5) has exactly b^t solutions. This means that J contains exactly b^t points of $P_{k,m}$. Hence the proof of sufficiency is complete. The converse is shown by similar arguments. □

Remark 2. The digital method for the construction of (t, s)-sequences described in Section 2 is the special case of the present construction where R is a commutative ring with identity, the distinguished element o is the zero element of R, and the maps $\phi_j^{(i)}$ are linear forms over R. In analogy with Remark 1, we propose to refer to the (t, s)-sequences produced by the method in this section also as *digital* (t, s)*-sequences in base* b or as *digital* (t, s)*-sequences over* R. The (t, s)-sequences in Section 2 could then be called *linear digital* (t, s)*-sequences in base* b or *linear digital* (t, s)*-sequences over* R.

The construction principle described above is again too general to be useful in practice, so one will have to focus on interesting special cases such as R being a finite field (see Section 6).

In Sections 6 and 7, we have not really gone much beyond the description of new construction principles for (t, m, s)-nets and (t, s)-sequences, respectively. The challenge for future research on this topic is to find choices for the maps $\phi_j^{(i)}$ in these constructions that are not all linear forms and that yield good (and maybe even record) values of the quality parameter t. A source for optimism in this quest is the analogy with coding theory (compare with the first paragraph of Section 6).

Acknowledgment

This research was partially supported by the grant R-394-000-025-422 with Temasek Laboratories in Singapore.

References

[BES02] J. Bierbrauer, Y. Edel, and W.Ch. Schmid. Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays. *J. Combin. Designs* **10**, 403–418 (2002).

[Dic06a] J. Dick. Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order. Preprint, 2006.

[Dic06b] J. Dick. Explicit constructions of quasi-Monte Carlo rules for the numerical integration of high dimensional periodic functions. Preprint, 2006.

[DS02] S.T. Dougherty and M.M. Skriganov. Maximum distance separable codes in the ρ metric over arbitrary alphabets. *J. Algebraic Combinatorics* **16**, 71–81 (2002).

[Fau82] H. Faure. Discrépance de suites associées à un système de numération (en dimension s). *Acta Arith.* **41**, 337–351 (1982).

[Kup06] G. Kuperberg. Numerical cubature using error-correcting codes. *SIAM J. Numer. Analysis* **44**, 897–907 (2006).

[LN95] G. Larcher and H. Niederreiter. Generalized (t, s)-sequences, Kronecker-type sequences, and diophantine approximations of formal Laurent series. *Trans. Amer. Math. Soc.* **347**, 2051–2073 (1995).

[LN94] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Revised ed., Cambridge University Press, Cambridge, 1994.

[LN97] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, 1997.

[LX04] S. Ling and C.P. Xing. *Coding Theory: A First Course*. Cambridge University Press, Cambridge, 2004.

[MN] D.J.S. Mayor and H. Niederreiter. A new construction of (t, s)-sequences and some improved bounds on their quality parameter. *Acta Arith.*, to appear.

[MWS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[Nie03] H. Niederreiter. Error bounds for quasi-Monte Carlo integration with uniform point sets. *J. Comput. Appl. Math.* **150**, 283–292 (2003).

[Nie04] H. Niederreiter. Digital nets and coding theory. *Coding, Cryptography and Combinatorics* (K.Q. Feng, H. Niederreiter, and C.P. Xing, eds.), pp. 247–257, Birkhäuser, Basel, 2004.

[Nie05] H. Niederreiter. Constructions of (t, m, s)-nets and (t, s)-sequences. *Finite Fields Appl.* **11**, 578–600 (2005).

[Nie71] H. Niederreiter. Orthogonal systems of polynomials in finite fields. *Proc. Amer. Math. Soc.* **28**, 415–422 (1971).

[Nie86] H. Niederreiter. Low-discrepancy point sets. *Monatsh. Math.* **102**, 155–167 (1986).

[Nie87] H. Niederreiter. Point sets and sequences with small discrepancy. *Monatsh. Math.* **104**, 273–337 (1987).

[Nie88] H. Niederreiter. Low-discrepancy and low-dispersion sequences. *J. Number Theory* **30**, 51–70 (1988).

[Nie92] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, 1992.

[NO02] H. Niederreiter and F. Özbudak. Constructions of digital nets using global function fields. *Acta Arith.* **105**, 279–302 (2002).

[NO04] H. Niederreiter and F. Özbudak. Matrix-product constructions of digital nets. *Finite Fields Appl.* **10**, 464–479 (2004).

[NO07] H. Niederreiter and F. Özbudak. Low-discrepancy sequences using duality and global function fields. *Acta Arith.*, to appear.

[NP01] H. Niederreiter and G. Pirsic. Duality for digital nets and its applications. *Acta Arith.* **97**, 173–182 (2001).

[NP02] H. Niederreiter and G. Pirsic. A Kronecker product construction for digital nets. *Monte Carlo and Quasi-Monte Carlo Methods 2000* (K.-T. Fang, F.J. Hickernell, and H. Niederreiter, eds.), pp. 396–405, Springer, Berlin, 2002.

[NX01] H. Niederreiter and C.P. Xing. *Rational Points on Curves over Finite Fields: Theory and Applications*. Cambridge University Press, Cambridge, 2001.

[NX96a] H. Niederreiter and C.P. Xing. Quasirandom points and global function fields. *Finite Fields and Applications* (S. Cohen and H. Niederreiter, eds.), pp. 269–296, Cambridge University Press, Cambridge, 1996.

[NX96b] H. Niederreiter and C.P. Xing. Low-discrepancy sequences and global function fields with many rational places. *Finite Fields Appl.* **2**, 241–273 (1996).

[PDP06] G. Pirsic, J. Dick, and F. Pillichshammer. Cyclic digital nets, hyperplane nets, and multivariate integration in Sobolev spaces. *SIAM J. Numer. Analysis* **44**, 385–411 (2006).

[Pir05] G. Pirsic. A small taxonomy of integration node sets. *Sitzungsber. Österr. Akad. Wiss. Math.-Naturwiss. Kl. Abt. II* **214**, 133–140 (2005).

[RT97] M.Yu. Rosenbloom and M.A. Tsfasman. Codes for the m-metric. *Problems Inform. Transmission* **33**, 45–52 (1997).

[SO04] I. Siap and M. Ozen. The complete weight enumerator for codes over $\mathcal{M}_{n\times s}(R)$. *Applied Math. Letters* **17**, 65–69 (2004).

[Sob67] I.M. Sobol'. Distribution of points in a cube and approximate evaluation of integrals (Russian). *Ž. Vyčisl. Mat. i Mat. Fiz.* **7**, 784–802 (1967).

[SS06] R. Schürer and W.Ch. Schmid. MinT: A database for optimal net parameters. *Monte Carlo and Quasi-Monte Carlo Methods 2004* (H. Niederreiter and D. Talay, eds.), pp. 457–469, Springer, Berlin, 2006.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, Berlin, 1993.