ACTA ARITHMETICA
LXXVIII.4 (1997)

Bounds for digital nets and sequences

by

Wolfgang Ch. Schmid and Reinhard Wolf (Salzburg)

1. Introduction. Currently, the most effective constructions of low-discrepancy point sets and sequences, which are of great importance for quasi-Monte Carlo methods in multidimensional numerical integration, are based on the concept of (t, m, s)-nets and (t, s)-sequences. A detailed theory was developed in Niederreiter [9] (see also [10, Chapter 4] for surveys of this theory).

So-called digital nets and sequences are of special interest due to the following two reasons. First, until now all construction methods for (t, m, s)-nets and (t, s)-sequences which are relevant for applications in quasi-Monte Carlo methods are digital methods over certain rings. Second, digital (t, m, s)-nets behave extremely well for the numerical integration of functions which are representable by an in some sense rapidly converging multivariate Walsh series. In a series of papers, Larcher and several co-authors established lattice rules for the numerical integration of multivariate Walsh series by digital nets. We refer to [5] for a concise introduction in the field of Larcher's lattice rules.

1.1. *Definitions and notations.* The concepts of (t, m, s)-nets and of (t, s)-sequences in a base b provide point sets of b^m points, respectively infinite sequences, in the half-open s-dimensional unit cube $I^s := [0, 1)^s$, $s \geq 1$, which are extremely well distributed if the quality parameters $t \in \mathbb{N}_0$ are "small". We follow [10] in our basic notation and terminology.

Definition 1. Let $b \geq 2$, $s \geq 1$, and $0 \leq t \leq m$ be integers. Then a point set consisting of b^m points of I^s forms a (t, m, s)-*net in base* b if every subinterval $J = \prod_{i=1}^{s} [a_i b^{-d_i}, (a_i + 1)b^{-d_i})$ of I^s 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.

1991 *Mathematics Subject Classification*: 11K38, 11K45, 11T99, 94B65.

The first author was supported by the Austrian Science Foundation (FWF) project P11009 MAT.

DEFINITION 2. Let $b \geq 2$, $s \geq 1$, and $t \geq 0$ be integers. Then a sequence $\mathbf{y}_0, \mathbf{y}_1, \ldots$ of points in I^s is a (t,s)-*sequence in base* b if for all $k \geq 0$ and $m \geq t$ the point set consisting of the $\mathbf{y}_n$ with $kb^m \leq n < (k+1)b^m$ forms a (t,m,s)-net in base b.

DEFINITION 3. Let $b \geq 2$, $s \geq 1$, and $m \geq 1$ be integers. We consider the following construction principle for point sets P consisting of b^m points in I^s. We choose:

(i) a commutative ring R with identity and $\mathrm{card}(R) = b$;

(ii) bijections $\psi_r : Z_b = \{0, 1, \ldots, b-1\} \to R$ for $0 \leq r \leq m-1$;

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

(iv) elements $c_{jr}^{(i)} \in R$ 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

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

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

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

with

$$y_{nj}^{(i)} = \eta_j^{(i)}\Big(\sum_{r=0}^{m-1} c_{jr}^{(i)} \psi_r(a_r(n)) \Big) \in Z_b \qquad \text{for } 0 \leq n < b^m,\ 1 \leq i \leq s, 1 \leq j \leq m.$$

If for some integer t with $0 \leq t \leq m$ the point set

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

is a (t,m,s)-net in base b, then it is called a *digital* (t,m,s)-*net* constructed over R.

In a quite similar way we define digital (t,s)-sequences constructed over a finite ring R.

DEFINITION 4. Let $b \geq 2$ and $s \geq 1$ be integers. We choose R, ψ_r for $r \geq 0$ with $\psi_r(0) = 0$ for all sufficiently large r, $\eta_j^{(i)}$ for $1 \leq i \leq s$ and $j \geq 1$, and $c_{jr}^{(i)}$ for $1 \leq i \leq s$, $j \geq 1$, and $r \geq 0$ as in Definition 3. 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 $a_r(n) \in Z_b$ for $r \geq 0$ and $a_r(n) = 0$ for all sufficiently large r. We put

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

with

$$y_{nj}^{(i)} = \eta_j^{(i)}\Big(\sum_{r=0}^{\infty} c_{jr}^{(i)} \psi_r(a_r(n))\Big) \in Z_b \quad \text{for } n \geq 0,\ 1 \leq i \leq s, \text{ and } j \geq 1,$$

and we assume that for each $n \geq 0$ and $1 \leq i \leq s$ we have $y_{nj}^{(i)} < b - 1$ for infinitely many j. If for some integer $t \geq 0$ the sequence

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

is a (t, s)-sequence in base b, then it is called a *digital* (t, s)*-sequence* constructed over R.

R e m a r k. The condition on the $y_{nj}^{(i)}$ in Definition 4 is satisfied, for instance, if $\eta_j^{(i)}(0) = 0$ and, for $r \geq 0$, $c_{jr}^{(i)} = 0$ for $1 \leq i \leq s$ and all sufficiently large j (compare with [10, p. 72]). In most practical implementations we actually have one fixed identification of the elements of R and Z_b independent of i, j, and r. Then the above construction method for nets can be symbolically illustrated by the following scheme. (Here we do not explicitly use the identification of the elements of R and Z_b.) For $1 \leq i \leq s$ let $C^{(i)}$ be the $m \times m$ matrix over R with rows

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

Every n with $0 \leq n < b^m$ and digit expansion $n = \sum_{r=0}^{m-1} a_r(n) b^r$ in base b is identified with

$$\mathbf{n} = \begin{pmatrix} a_0(n) \\ \vdots \\ a_{m-1}(n) \end{pmatrix}$$

over R, and each $x \in [0, 1)$ with finite digit expansion $x = \sum_{j=1}^{m} y_j(x) b^{-j}$ is identified with

$$\mathbf{x} = \begin{pmatrix} y_1(x) \\ \vdots \\ y_m(x) \end{pmatrix}$$

over R. Then we have

$$\mathbf{x}_n^{(i)} = C^{(i)} \cdot \mathbf{n} \quad \text{for } 0 \leq n < b^m \text{ and } 1 \leq i \leq s,$$
$$\mathbf{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \quad \text{for } n = 0, \ldots, b^m - 1.$$

1.2. *Some properties of digital nets.* For $m \geq 2$ let $C = \{\mathbf{c}_j^{(i)} \in R^m : 1 \leq i \leq s, 1 \leq j \leq m\}$ be a two-parameter system of elements of R^m. Again (compare with the remark following Definition 4) we may also think of C as an s-tuple $(C^{(1)}, \ldots, C^{(s)})$ of $m \times m$ matrices over R, where $\mathbf{c}_j^{(i)}$ is the jth row of $C^{(i)}$.

DEFINITION 5. For a system $C = \{\mathbf{c}_j^{(i)} \in R^m : 1 \leq i \leq s, 1 \leq j \leq m\}$ we define $S(C, t, m)$ to be the set of all subsystems $\{\mathbf{c}_j^{(i)} \in C : 1 \leq j \leq d_i, 1 \leq i \leq s\}$ of C for any integers $d_1, \ldots, d_s \geq 0$ with $\sum_{i=1}^{s} d_i = m - t$.

For a subsystem $\mathcal{C} \in S(C, t, m)$ with $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_{m-t}\}$ we may also think of $\mathcal{C}$ as an $(m-t) \times m$ matrix over R, where $\mathbf{c}_j$ is the jth row of $\mathcal{C}$. We now rephrase [10, Theorem 4.26], using this terminology:

LEMMA 1 ([10, Theorem 4.26]). *Suppose that for every subsystem $\mathcal{C} \in S(C, t, m)$ and for every $\mathbf{f} \in R^{m-t}$ the equation $\mathcal{C} \cdot \mathbf{z} = \mathbf{f}$ has exactly b^t solutions $\mathbf{z} \in R^m$. Then and only then the system C, used for the elements in part* (iv) *of Definition* 3, *provides a digital (t, m, s)-net constructed over R.*

LEMMA 2. *Suppose a system C provides a digital $(t, t+k, s)$-net constructed over R. Then any subsystem $\mathcal{C} \in S(C, t, t+k)$ (k elements of R^{t+k}) is linearly independent over R.*

Proof. Let $\mathcal{C} = \{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ be an arbitrary subsystem of $S(C, t, t+k)$. Let $\lambda_1, \ldots, \lambda_k$ be arbitrary elements of R with $\lambda_1\mathbf{a}_1 + \ldots + \lambda_k\mathbf{a}_k = \mathbf{0}$, and let $\mathbf{z}_j$ be a solution of $\mathcal{C} \cdot \mathbf{z}_j = \mathbf{e}_j$ ($\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)^T$ denotes the jth unit element of R^k for $j = 1, \ldots, k$). Since for every $j = 1, \ldots, k$ we have $0 = \mathbf{0} \cdot \mathbf{z}_j = (\lambda_1\mathbf{a}_1 + \ldots + \lambda_k\mathbf{a}_k) \cdot \mathbf{z}_j = \lambda_1(\mathbf{a}_1 \cdot \mathbf{z}_j) + \ldots + \lambda_k(\mathbf{a}_k \cdot \mathbf{z}_j) = \lambda_j$, we get $\lambda_1 = \ldots = \lambda_k = 0$. ∎

1.3. *Propagation rules for digital nets.* In [9, Lemmas 2.6–2.8] Niederreiter has established some fundamental properties of (t, m, s)-nets in an arbitrary base $b \geq 2$, which were later called the "three propagation rules" which allow one to obtain a new net from a given net. We show that these propagation rules also hold for digital nets.

LEMMA 3. *Let $t \geq 0$, $m \geq t$, $s \geq 1$, and $b \geq 2$ be integers and let R be a commutative ring with identity and of order b.*

(a) *Every digital (t, m, s)-net over R is a digital (u, m, s)-net over R for $t \leq u \leq m$.*

(b) *If there exists a digital (t, m, s)-net over R, then for each s' with $1 \leq s' \leq s$ there exists a digital (t, m, s')-net over R.*

(c) *If there exists a digital (t, m, s)-net over R, then for each u with $t \leq u \leq m$ there exists a digital (t, u, s)-net over R.*

The proof of (a) is the same as for (t, m, s)-nets in [9, Lemma 2.6]. For (b) we just have to use any s' of the s matrices defining the digital (t, m, s)-net. This fact was already mentioned in [4].

(c) The proof for $t = 0$ was done in Schmid [15]. One problem for a generalization to $t > 0$ was: is it possible to complete an arbitrary number ($\leq m$) of linearly independent elements of R^m to m linearly independent elements of R^m?

In [8] Nashier and Nichols defined a ring $\widetilde{R}$ with identity to be *weakly left semi-Steinitz* if any finite linearly independent subset of a finitely generated free left R-module F can be extended to a basis of F. In Corollary 2.5 they show that a commutative noetherian ring $\widetilde{R}$ is weakly semi-Steinitz if and only if every non-zero-divisor of $\widetilde{R}$ is a unit. Clearly this meets the conditions of our finite commutative rings R with identity and therefore we have: An $(m-t)\times m$ row-regular matrix in R can be completed (by adding additional rows) to an $m \times m$ row-regular square matrix in R which therefore is regular and invertible.

Proof of Lemma 3(c). Let $C = (C^{(1)}, \ldots, C^{(s)})$ be the system providing the digital (t, m, s)-net over R. From Lemma 2 it follows that the first $m - t$ rows of each of the s matrices are linearly independent over R. Since only these rows are of significance for the net (Lemma 1), we can omit the other rows and complete C to a system of regular matrices $(X^{(1)}, \ldots, X^{(s)})$. In particular, there exists a regular $m \times m$ matrix Z such that $X^{(s)}Z = I'_m := (\mathbf{e}_m, \mathbf{e}_{m-1}, \ldots, \mathbf{e}_1)$. Furthermore, the s regular matrices $X^{(1)}Z, \ldots, X^{(s)}Z$ provide the same net as $C^{(1)}, \ldots, C^{(s)}$. (Multiplication with a regular matrix Z only causes a permutation of the net points.)

In the following we suppose that each of the $m\times m$ matrices $C^{(1)}, \ldots, C^{(s)}$ is regular, and $C^{(s)} = I'_m$. Let $\mathbf{c}_j^{(i)}$ be the jth row of $C^{(i)}$ and let $\gamma_v : R^m \to R^{m-v}$ be such that

$$\gamma_v(r_1, \ldots, r_{m-v}, r_{m-v+1}, \ldots, r_m) = (r_1, \ldots, r_{m-v}).$$

We construct a new system $X = (X^{(1)}, \ldots, X^{(s)})$ of $u \times u$ matrices over R, where $\mathbf{x}_j^{(i)}$ is the jth row of $X^{(i)}$, $1 \leq j \leq u$, in the following way:

$$\mathbf{x}_j^{(i)} := \gamma_{m-u}(\mathbf{c}_j^{(i)}) \quad \text{for } 1 \leq i \leq s-1,$$
$$\mathbf{x}_j^{(s)} := \gamma_{m-u}(\mathbf{c}_{m-u+j}^{(s)}) = \mathbf{e}_{u+1-j} \in R^u,$$

and we show that X provides a digital (t, u, s)-net over R.

Let $\mathcal{X}$ be an arbitrary subsystem of $S(X, t, u)$ with $\sum_{i=1}^{s} d_i = u - t$. Now we consider the subsystem $\mathcal{C}$ of $S(C, t, m)$ with $\sum_{i=1}^{s} d'_i = m - t$ where $d'_i = d_i$, for $1 \leq i < s$, and $d'_s = d_s + m - u$. Without loss of generality we consider the last d'_s elements of $\mathcal{C}$, originating from $C^{(s)} = I'_m$, in reverse order.

The equation $\mathcal{C} \cdot \mathbf{z} = (f_1, \ldots, f_u, 0, \ldots, 0)^T$ with arbitrary $f_1, \ldots, f_u \in R$ has b^t solutions $\mathbf{z}_1, \ldots, \mathbf{z}_{b^t} \in R^m$. By the definition of $C^{(s)}$ we find that, for $1 \le j \le b^t$, the last $m - u$ coordinates of each solution $\mathbf{z}_j$ all are 0 (moreover, if $d_s > 0$, we have $z_{j,u-(d_s-v)} = f_{j,u-(d_s-v)}$ for $1 \le v \le d_s$ where $\mathbf{z} = (z_{j,1}, \ldots, z_{j,m})^T$).

Therefore it follows that the equation $\mathcal{X} \cdot \mathbf{z}' = (f_1, \ldots, f_u)^T$ also has exactly b^t solutions $\mathbf{z}'_1, \ldots, \mathbf{z}'_{b^t}$ with $\mathbf{z}'_j = \gamma_{m-u}(\mathbf{z}_j) \in R^u$.

Since $\mathcal{X}$ and $f_1, \ldots, f_u$ are arbitrary the proof is finished by Lemma 1. ∎

2. Best bounds for the dimension of digital nets and sequences over $\mathbb{F}_2$ with small quality parameter. In [12] Niederreiter and Xing introduced a new way for the construction of digital (t, s)-sequences. The key idea is to work with global function fields containing many places of degree 1 instead of working with rational function fields as was done in earlier construction methods (see for example [10]). The new method yields significantly better results than all previous methods. Table 1 gives a comparison, in the case of $\mathbb{F}_2$, of their t-values ($NX_2(s)$) with the best values of the quality parameter ($M_2(s)$) obtained from all previous constructions.

Table 1. Quality parameters of binary (t, s)-sequences

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$M_2(s)$	0	0	1	3	5	8	11	14	18	22	26	30	34	38
$NX_2(s)$	0	0	1	1	2	3	4	5	6	8	9	10	11	13

Niederreiter and Xing show that for any integers $s \ge 1$ and $b \ge 2$ there exists a digital (t, s)-sequence in base b with quality parameter $t = O(s)$ (see for example [12, Corollary 2]). This result is asymptotically best possible, in the sense that t must grow at least linearly with s. In [13] they improve the lower bound for the quality parameter to:

[13, Theorem 8] *If for some integers $s \ge 1$, $t \ge 0$, and $b \ge 2$ there exists a general (t, s)-sequence in base b, then we must have*

$$t \ge \frac{s}{b} - \log_b \frac{(b-1)s + b + 1}{2}.$$

This improvement was based on a result of Lawrence [6], who used a new lower bound, established by Bierbrauer [1, Theorem 1], for the number of rows in an orthogonal array. We will give the key ideas of the proof ($OA(b^{t+k}, s+1, b, k)$ denotes an orthogonal array of size b^{t+k}, $s+1$ constraints, b levels, and strength k):

(1) Suppose $\exists$ (t, s)-sequence in base b.

(2) $\Rightarrow \exists$ $(t, t+k, s+1)$-net in base b for all $k \ge 0$ [9, Lemma 5.15].

(3) $\Rightarrow \exists\ OA(b^{t+k}, s+1, b, k)$ for $s+1 \geq k \geq 2$ [15, Corollary 15].

(4) $\Rightarrow b^{t+k} \geq b^{s+1}\left(1 - \dfrac{(b-1)(s+1)}{b(k+1)}\right)$ [1, Theorem 1].

(5) $\Rightarrow t \geq \max\limits_{s+1 \geq k \geq \lfloor (b-1)(s+1)/b \rfloor} s - k + \log_b \left(b - \dfrac{(b-1)(s+1)}{k+1}\right)$.

(6) Following the proof of [13, Theorem 8], inserting the value $k = \lfloor s - s/b \rfloor + 1$ yields the desired result.

R e m a r k. This bound clearly holds for digital sequences. For an independent proof in the digital case over $\mathbb{F}_q$, the following arguments are sufficient:

(2) Use [12, Lemma 1].

(3) The existence of a digital $(t, t+k, s+1)$-net over $\mathbb{F}_q$ implies, for $s+1 \geq t+k$, the existence of a linear $[s+1, s+1-(t+k), k+1]$-code over $\mathbb{F}_q$ (see for example the next section).

(4) Using the Plotkin bound [16, Theorem 5.2.4] we obtain

$$q^{s+1-(t+k)} \leq \frac{k+1}{k+1-(s+1)\frac{q-1}{q}}$$

and therefore the same result as before.

In the binary case we have computed lower bounds on the quality parameters provided by [13, Theorem 8]. Using these results we have tabulated (Table 2) upper bounds s_t on the dimension of binary (t, s)-sequences.

Table 2. Upper bounds for the dimension of binary (t, s)-sequences

$t =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$s_t \leq$	3	6	9	11	14	16	18	21	23	25	27	30	32	34

From (4) in the above sketch of a proof of [13, Theorem 8] (see also Lawrence [6, Theorem 4.4.14]) we clearly have a lower bound for the quality parameters of general nets (and therefore also for digital nets): A $(t, t+k, s)$-net in base b can exist only if

$$(*) \qquad t \geq s - 1 - k + \log_b \left(b - \frac{(b-1)s}{k+1}\right).$$

But as seen above, this bound only works for $s \geq k \geq \lfloor (b-1)s/b \rfloor$.

In the following we will provide an upper bound for the dimension (and therefore a lower bound for the quality parameter) of arbitrary digital nets over $\mathbb{F}_q$ without the above restriction on k.

2.1. *Improved upper bound for the dimension of digital nets over* $\mathbb{F}_q$

PROPOSITION 1. *Suppose that for some integers* $s \geq 1$, $t \geq 0$, *and* $k \geq 2$ *there exists a digital* $(t, t+k, s)$*-net over* $\mathbb{F}_q$. *Then we must have*

$$\sum_{u=1}^{\lfloor k/2 \rfloor} \sum_{l=1}^{u} \binom{s}{l} \binom{u-1}{l-1} (q-1)^l q^{u-l} + A_k < q^{t+k},$$

where

$$A_k = \begin{cases} 0 & \text{for } k \text{ even}, \\ \displaystyle\sum_{l=1}^{(k+1)/2} \binom{s-1}{l-1} \binom{(k+1)/2-1}{l-1} (q-1)^l q^{(k+1)/2-l} & \text{for } k \text{ odd}. \end{cases}$$

Proof. Let C be the system providing the digital $(t, t+k, s)$-net over $\mathbb{F}_q$. By Lemma 2 any subsystem $\mathcal{C} \in S(C, t, t+k)$ is linearly independent over $\mathbb{F}_q$.

For $u \in \{1, \ldots, \lfloor k/2 \rfloor\}$ we consider linear combinations of u vectors from C. Let $l \in \{1, \ldots, \min(u, s)\}$ be the number of matrices from which we take these vectors. Let $1 \leq s_1 < s_2 < \ldots < s_l \leq s$ be the numbering of these matrices. Then we choose integers $0 \leq d_1, \ldots, d_l \leq u$ with $\sum_{i=1}^{l} d_i = u$ and consider any linear combinations of the vectors

$$\mathbf{c}_j^{(s_i)}, \quad j = 1, \ldots, d_i, \ i = 1, \ldots, l,$$

with coefficients from $\mathbb{F}_q$ for $j \neq d_i$ and with coefficients from $\mathbb{F}_q \setminus \{0\}$ for $j = d_i$. Any two such combinations with different parameters have to be different, and for k even the result follows. (Since $\binom{s}{l} = 0$ for $l > s$, we sum up l to u instead of to $\min(u, s)$.)

If k is odd we additionally consider all linear combinations of $(k+1)/2$ vectors such that at least one vector is taken from one fixed matrix. Therefore we only have $\binom{s-1}{l-1}$ instead of $\binom{s}{l}$ possibilities to choose the matrices. The further arguments are the same as above. ∎

Remarks. • We have checked by computer that A_k, for k odd, seems to be too small to improve the numerical results. Until now in all of our calculations we obtained the same results when we evaluated Proposition 1 for $k-1$ even and applied Lemma 3(c).

• The result of Proposition 1 is the best possible result that can be obtained by the method of linear combinations.

• Niederreiter and Xing [11, Proposition 1] obtained a similar, but a little weaker estimate by using a bound from coding theory. However, they used only the first row vectors $\mathbf{c}_1^{(i)}$ of each of the matrices. Our improvement was possible by considering the first $\lfloor k/2 \rfloor$ row vectors of each matrix.

Table 3. Upper bounds for $\widetilde{s}(t, t+k, 2)$ from Proposition 1

$k=$	2	4	6	8	10	12	14	16	18	20	22	24
	3	5	7	9	11	13	15	17	19	21	23	25
$t=0$	2^2-1	3	4	4	5	5	6	6	6	7	7	8
$t=1$	2^3-1	5	5	6	6	6	7	7	8	8	9	9
$t=2$	2^4-1	9	8	7	8	8	8	8	9	9	10	10
$t=3$	2^5-1	13	10	10	9	9	10	10	10	11	11	11
$t=4$	2^6-1	20	14	12	12	11	11	12	12	12	12	13
$t=5$	2^7-1	29	19	16	14	14	13	13	13	14	14	14
$t=6$	2^8-1	42	25	20	17	16	16	15	15	15	15	16
$t=7$	2^9-1	61	32	24	21	19	18	17	17	17	17	17
$t=8$	$2^{10}-1$	88	42	30	25	22	21	20	19	19	19	19
$t=9$	$2^{11}-1$	125	54	36	29	26	24	22	22	21	21	21
$t=10$	$2^{12}-1$	178	69	44	35	30	27	25	24	23	23	23
$t=11$	$2^{13}-1$	253	88	54	41	34	31	28	27	26	25	25

In Table 3 we provide upper bounds for the dimension s of binary digital $(t, t+k, s)$-nets deduced from Proposition 1. Here and in the following sections, $\widetilde{s}(t, t+k, q)$ denotes the maximal dimension s for which there exists a digital $(t, t+k, s)$-net over $\mathbb{F}_q$.

As mentioned above, the bound for odd k is provided either by Proposition 1, or by taking the bound for $k-1$ even and applying Lemma 3(c).

To date, Proposition 1 provides the best upper bounds for $\widetilde{s}(t, t+k, q)$ which are deduced from a closed formula. Clearly for special values of t, k, and q, this bound can be improved (see for example the following sections).

2.2. *Best bounds for small quality parameters*. It is the aim of this section to close the gap between the results given in Tables 1 and 2 for the values $t = 0, 1, 2$ and therefore to show that in these cases the method of Niederreiter and Xing is best possible.

By Proposition 1, a digital $(2, 8, 9)$-net (and therefore a digital $(2, 8)$-sequence) over $\mathbb{F}_2$ cannot exist. We have the following improvement for the upper bound of s:

LEMMA 4. *For $s \geq 7$, a digital $(2, 8, s)$-net over $\mathbb{F}_2$ cannot exist.*

For the proof we make use of Lemma 5. First it is convenient (also for the next sections) to give the following definition:

DEFINITION 6. Let $t \geq 0$, $k \geq 2$, $s \geq 1$, and $t + k \geq d \geq 1$ be integers. A system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^{t+k} : 1 \leq j \leq t+k,\ 1 \leq i \leq s\}$ is called a $(k, t+k, d, s)$-*system* over $\mathbb{F}_q$ if any subsystem $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^{t+k} : 1 \leq j \leq d_i,\ 1 \leq i \leq s\}$ with $\sum_{i=1}^{s} d_i = k$ and $0 \leq d_1, \ldots, d_s \leq d$ is linearly independent over $\mathbb{F}_q$.

Remark. C provides a digital $(t, t+k, s)$-net over $\mathbb{F}_q$ if and only if C is a $(k, t+k, k, s)$-system over $\mathbb{F}_q$.

For the proofs of Lemmas 4, 5 and of Proposition 2 we use the following notation: Let $m \in \mathbb{N}$. We identify the linear space $\mathbb{F}_2^m$ with $\mathcal{P}(1,\dots,m)$, the class of all subsets of $\{1,\dots,m\}$ (indicating the coordinates which are 1), equipped with the symmetric difference $\triangle$. For convenience we write $+$ instead of $\triangle$. $[\dots]$ denotes the linear hull in $\mathcal{P}(1,\dots,m)$.

LEMMA 5. *Let $1 \le k \le 6$. A system*

$$A_k = \begin{pmatrix} & x \\ s_1 & x_1 \\ \vdots & \vdots \\ s_k & x_k \end{pmatrix}$$

of subsets $x, x_1, \dots, x_k$ of $\{1,\dots,6\}$ and elements $s_1,\dots,s_k$ of $\{1,\dots,6\}$ is said to have property $(*)$ if

- *$|x| \le 2$, $|x_i| \le 3$, and $s_i \ne s_j$ for $1 \le i \ne j \le k$,*
- *$s_i \notin x_i$, $x + x_i \notin [s_i, r, s]$, $x_i + x_j \notin [s_i, s_j, r, s]$ for all $1 \le r, s \le 6$ and $1 \le i \ne j \le k$.*

Now we have:

(1) *For $k = 3$ there are* $\bmod S_6$ *(up to permutations) exactly three systems A_3^1, A_3^2, A_3^3 with property $(*)$*:

$$A_3^1 = \begin{pmatrix} & \emptyset \\ 1 & 356 \\ 2 & 145 \\ 3 & 246 \end{pmatrix}, \quad A_3^2 = \begin{pmatrix} & 46 \\ 1 & 345 \\ 2 & 1 \\ 3 & 256 \end{pmatrix}, \quad A_3^3 = \begin{pmatrix} & 34 \\ 1 & 236 \\ 2 & 456 \\ 3 & 15 \end{pmatrix}.$$

(2) *If $k \ge 4$ there exists no system A_k with property $(*)$.*

(3) *For $1 \le k, l \le 3$ a system $B_{k,l} = (A_k, A'_l)$ with*

$$A_k = \begin{pmatrix} & x \\ s_1 & x_1 \\ \vdots & \vdots \\ s_k & x_k \end{pmatrix}, \quad A'_l = \begin{pmatrix} & x \\ t_1 & y_1 \\ \vdots & \vdots \\ t_l & y_l \end{pmatrix}$$

is said to have property $(**)$ if both A_k and A'_l have property $(*)$ and if $s_i \ne t_j$, $x_i + y_j \notin [s_i, t_j, r]$ for all $1 \le r \le 6$, $1 \le i \le k$, and $1 \le j \le l$. Then we have:

(i) *For $k = l = 3$ there is exactly one system $B_{3,3} = (A_3^1, A'_3)$ with property $(**)$* $\bmod S_6$, *with A_3^1 being the system of part* (1) *and*

$$A'_3 = \begin{pmatrix} & \emptyset \\ 4 & 235 \\ 5 & 126 \\ 6 & 134 \end{pmatrix}.$$

(ii) *For* $k = 3$, $l = 2$ *there are exactly three systems* $B^1_{3,2} = (A^1_3, A^1_2)$, $B^2_{3,2} = (A^2_3, A^2_2)$, *and* $B^3_{3,2} = (A^3_3, A^3_2)$ *with property* $(**)$ $\bmod S_6$ *with* A^1_3, A^2_3, A^3_3 *being the systems of part* (1) *and*

$$A^1_2 = \begin{pmatrix} & \emptyset \\ 4 & 235 \\ 5 & 126 \end{pmatrix}, \quad A^2_2 = \begin{pmatrix} & 46 \\ 4 & 32 \\ 5 & 136 \end{pmatrix}, \quad A^3_2 = \begin{pmatrix} & 34 \\ 4 & 61 \\ 5 & 2 \end{pmatrix}.$$

Proof. ad (1). Since $x_i + x_j \notin [s_i, s_j, r, s]$ we get $|x_i + x_j| \geq 3$ for all $1 \leq i \neq j \leq 3$.

(a) $x = \emptyset$. Since $x_i \notin [s_i, r, s]$ and $|x_i| \leq 3$ we have $|x_i| = 3$ for all $1 \leq i \leq 3$. Then we get $\bmod S_6$: $x_1 = 356$, $x_2 = 145$, and $x_3 = 246$.

(i) $s_1 = 4$. Since $1346 = x_1 + x_2 \notin [4, s_2, r, s]$ and $s_2 \notin x_2$ we get $s_2 = 2$. From $1256 = x_2 + x_3 \notin [2, s_3, r, s]$ and $s_3 \notin x_3$ it follows that $s_3 = 3$, which contradicts $2345 = x_1 + x_3 \notin [4, 3, r, s]$.

(ii) $s_1 = 1$. As in case (i) we get $s_2 = 2$ and $s_3 = 3$.

(iii) $s_1 = 2$. We get $s_3 = 1$ and $s_2 = 3$. Notice that $\tau \in S_6$, $\tau = (54)(32)$ transforms the system (iii) into the system of (ii).

Therefore we have

$$A^1_3 = \begin{pmatrix} & \emptyset \\ 1 & 356 \\ 2 & 145 \\ 3 & 246 \end{pmatrix}.$$

(b) $|x| = 1$. Since $x + x_i \notin [s_i, r, s]$ we get $|x_i| \geq 2$ for all $1 \leq i \leq 3$. Looking at x_1, x_2, x_3 there are eight cases $\bmod S_6$:

x_1 :	12	12	12	123	123	123	123	123
x_2 :	34	34	34	145	145	145	145	456
x_3 :	56	135	156	16	24	26	246	14

Considering the first case $x_1 = 12$, $x_2 = 34$, and $x_3 = 56$ it follows from $|x| = 1$ and $|x + x_i| \geq 3$ (since $x + x_i \notin [s_i, r, s]$) that there is no subset x of $\{1, \ldots, 6\}$ with $|x| = 1$ to generate a system with the desired property. In an analogous way it is easy to see that none of the remaining seven cases leads to a system with property $(*)$.

(c) $|x| = 2$. As in case (a) and (b) we obtain the systems A^2_3 and A^3_3.

ad (2). Since $1 \leq |x_i| \leq 3$ for all $1 \leq i \leq 4$ we see from part (1) that $|x_i| = 3$ for all $1 \leq i \leq 4$, contrary to $|x_i + x_j| \geq 3$ for all $1 \leq i \neq j \leq 4$.

ad (3). Starting with the three systems of part (1) it is easy to see that they lead to the desired systems with property $(**)$. ∎

Proof of Lemma 4. By Lemma 3(b) it suffices to show that there is no digital $(2, 8, 7)$-net over $\mathbb{F}_2$.

Assume that there is a system providing a digital $(2, 8, 7)$-net over $\mathbb{F}_2$. Then there exists a subsystem S which is a $(6, 8, 3, 7)$-system over $\mathbb{F}_2$. We

identify a row vector in $\mathbb{F}_2^8$ with a subset of $\{0,1,\dots,7\}$ indicating the coordinates which are 1, and write $S = ((x_0/y_0/z_0),(x_1/y_1/z_1),\dots,(x_6/y_6/z_6))$, where x_i, y_i, z_i are subsets of $\{0,1,\dots,7\}$ for $0 \le i \le 6$. It follows that $\dim[x_0,\dots,x_6] \ge 6$.

(1) $\dim[x_0,\dots,x_6] = 6$. Without loss of generality, we get $x_0 = 0,\dots$ $\dots, x_5 = 5$ and $x_6 = 012345$. Assume that there is some y_j $(0 \le j \le 5)$ such that y_j is a subset of $\{0,1,\dots,5\}$. We can let $j = 0$. Since $y_0 \notin [0,r,s,t,u]$ for all $1 \le r,s,t,u \le 5$ we get $y_0 = 012345$ or $y_0 = 12345$, contrary to S being a $(6,8,3,7)$-system. So for each y_i, $0 \le i \le 5$, there are three possible cases:

I. $6,7 \in y_i$,
II. $6 \in y_i,\ 7 \notin y_i$,
III. $6 \notin y_i,\ 7 \in y_i$.

We can assume that y_0 and y_1 are of the same type (I or II or III). Then $y_0 + y_1$ is a subset of $\{0,1,\dots,5\}$. Since $y_0 + y_1 \notin [0,1,r,s]$ for all $2 \le r,s \le 5$ we have $|y_0 + y_1| \ge 3$. If $|y_0 + y_1| = 3$ we have $0,1 \notin y_0 + y_1$ and so without loss of generality, $y_0 + y_1 = 234$. So for the subset $((0/y_0),(1/y_1),(2),(3),(4),(5),(012345))$ of S we have $x_0 + x_1 + y_0 + y_1 + x_5 + x_6 = \emptyset$, which is a contradiction.

The cases $|y_0 + y_1| = 4,5,6$ are treated in the same manner.

(2) $\dim[x_0,\dots,x_6] = 7$. Without loss of generality, let $x_0 = 0,\dots,x_6 = 6$. Assume that there are $j_1, j_2 \in \{0,1,\dots,6\}$, $j_1 \ne j_2$, such that y_{j_1}, y_{j_2} are subsets of $\{0,1,\dots,6\}$. We can assume $j_1 = 0$ and $j_2 = 1$. Then we get $y_0 \notin [0,r,s,t,u]$, $y_1 \notin [1,r,s,t,u]$, and $y_0 + y_1 \notin [0,1,r,s]$ for all $0 \le r,s,t,u \le 6$. Since $y_i \notin [i,r,s,t,u]$ if and only if $y_i + i \notin [i,r,s,t,u]$, $0 \le i \le 1$, we can assume that $0 \in y_0$ and $1 \in y_1$. Hence, with $\alpha = 0123456$, we get $y_0 = \alpha$ or $y_0 = \alpha + i$ and $y_1 = \alpha$ or $y_1 = \alpha + j$ for some $i \in \{1,2,\dots,6\}$ and $j \in \{0,2,\dots,6\}$. All these cases lead to a contradiction. Therefore we get two cases:

(a) $7 \in y_i$ for all $0 \le i \le 6$.

(b) Without loss of generality, $7 \notin y_6$ and $7 \in y_i$ for all $0 \le i \le 5$.

Assume that $7 \notin z_0$. By looking at the cases $7 \in z_i$ or $7 \notin z_i$ for $1 \le i \le 5$ it is easy to see that in both cases (a) and (b) the system S is a $(6,8,3,7)$-system if and only if $S' = ((0/y_0/z_0 + y_0),(1/y_1/z_1),\dots,(6/y_6/z_6))$ is a $(6,8,3,7)$-system. So we can assume $7 \in z_0$. If we continue in the same way we get $7 \in z_0, z_1, \dots, z_5$ and hence we can assume

$$S = ((0/y_0/v_0 + 7),(1/y_1/v_1 + 7),\dots,(5/y_5/v_5 + 7),(6/y_6/z_6))$$

with $v_0,\dots,v_5$ subsets of $\{0,\dots,6\}$.

Now we consider the system

$$S' = ((0/y_0 + v_0/7), (1/y_1 + v_0/v_1 + v_0 + 7), \ldots, (5/y_5 + v_0/v_5 + v_0 + 7), (6/y_6'/z_6'))$$

with $y_6' = y_6 + v_0$ in case (a), $y_6' = y_6$ in case (b), and with

$$z_6' = \begin{cases} z_6 + v_0 & \text{if } 7 \in z_6, \\ z_6 & \text{otherwise.} \end{cases}$$

S' is a $(6, 8, 3, 7)$-system if and only if S is a $(6, 8, 3, 7)$-system. Hence we get, without loss of generality,

$$S = ((0/u_0 + 7/7), (1/u_1 + 7/v_1 + 7), \ldots, (5/u_5 + 7/v_5 + 7), (6/y_6/z_6))$$

with $u_0, \ldots, u_5, v_1, \ldots, v_5$ subsets of $\{0, \ldots, 6\}$.

Now take

$$u_i' = \begin{cases} u_i + i & \text{if } i \notin u_i, \\ u_i & \text{otherwise,} \end{cases} \quad \text{for } 0 \le i \le 5,$$

$$v_i' = \begin{cases} v_i + i & \text{if } i \notin v_i, \\ v_i & \text{otherwise,} \end{cases} \quad \text{for } 1 \le i \le 5,$$

and

$$y_6' = \begin{cases} y_6 + 6 & \text{if } 6 \notin y_6, \\ y_6 & \text{otherwise.} \end{cases}$$

It is easy to check that

$$S' = ((0/u_0' + 7/7), (1/u_1' + 7/v_1' + 7), \ldots, (5/u_5' + 7/v_5' + 7), (6/y_6'/z_6))$$

is a $(6, 8, 3, 7)$-system if and only if S is a $(6, 8, 3, 7)$-system. Summing up we get

$$S = ((0/u_0 + 7/7), (1/u_1 + 7/v_1 + 7), \ldots, (5/u_5 + 7/v_5 + 7), (6/y_6/z_6))$$

with $6 \in y_6$, $0 \in u_0$, $i \in u_i, v_i$, and u_0, u_i, v_i subsets of $\{0, \ldots, 6\}$ for $1 \le i \le 5$.

Now we take a detailed look at cases (a) and (b):

(a) $7 \in y_6$. Write $y_6 = u_6 + 7$ with u_6 a subset of $\{0, \ldots, 6\}$. We can assume $0 \in u_1, \ldots, u_k$ and $0 \notin u_{k+1}, \ldots, u_6$ for some $0 \le k \le 6$. Now it is easy to see that

$$B_{k,6-k} = \begin{pmatrix} \alpha + u_0 & & \alpha + u_0 \\ 1 \quad \alpha + u_1 & k+1 & \alpha + u_{k+1} + 0 \\ \vdots \quad \vdots & \vdots & \vdots \\ k \quad \alpha + u_k & 6 & \alpha + u_6 + 0 \end{pmatrix}$$

meets the conditions of Lemma 5 ($\alpha = 0123456$). Hence we can assume

$$S = ((0/0123456 + 7/7), (1/0124 + 7/v_1 + 7), (2/0236 + 7/v_2 + 7), (3/0135 + 7/v_3 + 7), (4/146 + 7/v_4 + 7), (5/345 + 7/v_5 + 7), (6/256 + 7/z_6)).$$

It is easy to check that there is no subset v_5 of $\{0, \ldots, 6\}$ such that

$$((0/0123456 + 7/7), (1/0124 + 7), (2/0236 + 7), (3/0135 + 7), (4/146 + 7), (5/345 + 7/v_5 + 7), (6/256 + 7))$$

is a subsystem of S.

(b) $7 \notin y_6$. We can assume $0 \in u_1, \ldots, u_k$ and $0 \notin u_{k+1}, \ldots, u_5$ for some $0 \le k \le 5$. As in case (a), it is easy to see that

$$B_{k,5-k} = \begin{pmatrix} \alpha + u_0 & & \alpha + u_0 \\ 1 & \alpha + u_1 & k+1 & \alpha + u_{k+1} + 0 \\ \vdots & \vdots & \vdots & \vdots \\ k & \alpha + u_k & 5 & \alpha + u_5 + 0 \end{pmatrix}$$

meets the conditions of Lemma 5 ($\alpha = 0123456$). Therefore we get:

(i) $S = ((0/0123456 + 7/7), (1/0124 + 7/v_1 + 7), (2/0236 + 7/v_2 + 7), (3/0135 + 7/v_3 + 7), (4/146 + 7/v_4 + 7), (5/345 + 7/v_5 + 7), (6/y_6/z_6))$, or

(ii) $S = ((0/01235 + 7/7), (1/0126 + 7/v_1 + 7), (2/023456 + 7/v_2 + 7), (3/0134 + 7/v_3 + 7), (4/1456 + 7/v_4 + 7), (5/245 + 7/v_5 + 7), (6/y_6/z_6))$, or

(iii) $S = ((0/01256 + 7/7), (1/0145 + 7/v_1 + 7), (2/0123 + 7/v_2 + 7), (3/02346 + 7/v_3 + 7), (4/2345 + 7/v_4 + 7), (5/13456 + 7/v_5 + 7), (6/y_6/z_6))$.

The following is easy to check:

(i) There is no subset y_6 (containing 6) of $\{0, \ldots, 6\}$ such that

$$((0/0123456 + 7/7), (1/0124 + 7), (2/0236 + 7), (3/0135 + 7), (4/146 + 7), (5/345 + 7), (6/y_6))$$

is a subsystem of S.

(ii) There is no subset y_6 (containing 6) of $\{0, \ldots, 6\}$ such that

$$((0/01235 + 7/7), (1/0126 + 7), (2/023456 + 7), (3/0134 + 7), (4/1456 + 7), (5/245 + 7), (6/y_6))$$

is a subsystem of S.

(iii) The subsystem

$$((0/01256+7/7),(1/0145+7),(2/0123+7),$$
$$(3/02346+7),(4/2345+7),(5/13456+7/v_5+7),(6/y_6))$$

implies $y_6 = 0123456$. But no subset v_5 (containing 5) of $\{0,\dots,6\}$ exists with the desired property. ∎

THEOREM 1. (a) *There exists a digital* $(0,s)$*-sequence over* $\mathbb{F}_2$ *if and only if* $s \le 2$.

(b) *There exists a digital* $(1,s)$*-sequence over* $\mathbb{F}_2$ *if and only if* $s \le 4$.

(c) *There exists a digital* $(2,s)$*-sequence over* $\mathbb{F}_2$ *if and only if* $s \le 5$.

P r o o f. (a) was already shown in [4, Theorem 2b)]. The existence of digital $(1,4)$- and $(2,5)$-sequences follows from the construction using global function fields which was introduced by Niederreiter and Xing [12] (see Table 1). From Proposition 1 we deduce that for the existence of a digital $(1,5,s)$-net over $\mathbb{F}_2$ we must have $s \le 5$. Combining this result resp. Lemma 4 with [12, Lemma 1] completes the proof. ∎

3. Improved construction of digital $(t,t+4,s)$-nets over $\mathbb{F}_q$ from linear codes. In [7] a new method for the construction of digital nets in prime power bases was discussed which makes use of sets of independent vectors over finite fields.

An (n,k)*-set* in $\mathbb{F}_q^{t+k}$ is a set of n vectors in $\mathbb{F}_q^{t+k}$ with the property that any k of them are linearly independent over $\mathbb{F}_q$. Further, let $\max_k(t+k,q)$ be the maximal number of vectors of length $t+k$ over $\mathbb{F}_q$ with the property that any k of the vectors are linearly independent over $\mathbb{F}_q$. ($\max_k(t+k,q) := \max\{n \in \mathbb{N} : \exists (n,k)\text{-set in } \mathbb{F}_q^{t+k}\}$.)

[7, Theorem 1] *Let* q *be a prime power, and let* $n,t \ge 0$, *and* $k \ge 2$ *be integers. Given an* (n,k)*-set in* $\mathbb{F}_q^{t+k}$, *a digital* $(t,t+k,s)$*-net can be constructed over* $\mathbb{F}_q$ *with*

$$s = \begin{cases} \left\lfloor \dfrac{n-1}{h} \right\rfloor & \text{if } k = 2h+1, \\ \left\lfloor \dfrac{n}{h} \right\rfloor & \text{if } \ k = 2h. \end{cases}$$

A well known upper bound for the dimension of digital (t,m,s)-nets over $\mathbb{F}_q$ is $s \le (q^{t+2}-1)/(q-1)$. By using $\max_2(t+2,q) = (q^{t+2}-1)/(q-1)$ (see [3, Theorem 14.4]) and $\max_3(t+3,2) = 2^{t+2}$ (see [3, Corollary 14.12]), this upper bound can be achieved by [7, Theorem 1]. As pointed out in [7], there is a small gap between the lower and upper bound for the maximal dimension s already for digital $(t,t+3,s)$-nets over $\mathbb{F}_q$ with $q > 2$. The following improvement has closed this gap (for a detailed proof see [15]).

[7, Theorem 4] *Let q be a prime power and $t \geq 0$ be an integer. Then a digital $(t, t+3, s)$-net can be constructed over $\mathbb{F}_q$ if and only if*

$$s \leq \begin{cases} \max_3(t+3,q) - 1 = \dfrac{q^{t+2}-1}{q-1} & \text{if } q = 2, \text{ or if } q \text{ is even and } t = 0, \\ \max_3(t+3,q) & \text{else.} \end{cases}$$

Remark. In the theory of error-correcting codes it is well known that the existence of an (n,k)-set in $\mathbb{F}_q^{t+k}$ is equivalent to the existence of a linear $[n, n-(t+k), k+1]$-code over $\mathbb{F}_q$. (We refer to [3] for an introduction to linear coding theory.) Therefore [7, Theorem 4] provides a complete solution, in terms of linear codes, for the existence of digital $(t, t+3, s)$-nets over $\mathbb{F}_q$.

An upper bound for $\max_k(t+k,q)$ is an upper bound for the dimension s of a digital $(t, t+k, s)$-net over $\mathbb{F}_q$, which is easily seen by the following fact: if $C^{(1)}, \ldots, C^{(s)}$ are the matrices providing a digital $(t, t+k, s)$-net over $\mathbb{F}_q$ then the first row vectors of each of the matrices provide an (s,k)-set in $\mathbb{F}_q^{t+k}$.

Brouwer [2] has made available a data base of bounds for the minimum distance for binary, ternary and quaternary codes. We have used this data base and improved values of Bierbrauer and Edel (for the various manuscripts see the homepage of J. Bierbrauer under URL http://www.math.mtu.edu/home/math/jbierbra/Home.html) to compute upper and lower bounds for $\max_4(t+4,q)$ (see Table 4).

If we use these bounds, we find by the above mentioned fact and by [7, Theorem 1], that there are large differences between the lower and upper bounds for the maximal dimension $\widetilde{s}(t, t+4, q)$ of digital $(t, t+4, s)$-nets over $\mathbb{F}_q$. For example, we have $8 \leq \widetilde{s}(4,8,2) \leq 17$, $11 \leq \widetilde{s}(5,9,2) \leq 23$, or $21 \leq \widetilde{s}(3,7,4) \leq 59$ (see Table 4).

There is the following considerable improvement:

Theorem 2. *Let q be a prime power, and let s and $t \geq 0$ be integers. Given an $(s,4)$-set in $\mathbb{F}_q^{t+4}$ with*

$$\frac{q(q-1)^2}{2}s^2 - \frac{q(q-1)(q-5)}{2}s - q(2q-3) < q^{t+4},$$

a digital $(t, t+4, s)$-net can be constructed over $\mathbb{F}_q$.

Proof. Let $\{\mathbf{c}_1^{(1)}, \ldots, \mathbf{c}_1^{(s)}\}$ be an $(s,4)$-set in $\mathbb{F}_q^{t+4}$ with

$$c(s) := \frac{q(q-1)^2}{2}s^2 - \frac{q(q-1)(q-5)}{2}s - q(2q-3) < q^{t+4}.$$

Notice that $S := ((\mathbf{c}_1^{(1)}), \ldots, (\mathbf{c}_1^{(s)}))$ is, in our terminology, a $(4, t+4, 1, s)$-system over $\mathbb{F}_q$ if and only if all vectors of

$$A_1 := \{\mathbf{0},\ \lambda\mathbf{c}_1^{(i)},\ \lambda\mathbf{c}_1^{(j_1)} + \mu\mathbf{c}_1^{(j_2)} : \lambda, \mu \in \mathbb{F}_q \setminus 0,\ 1 \leq i \leq s,\ 1 \leq j_1 < j_2 \leq s\}$$

are different (then $|A_1| = 1 + (q-1)s + (q-1)^2\binom{s}{2}$).

For each $\alpha \in \mathbb{F}_q$ define $f_\alpha^1 : \mathbb{F}_q^{t+4} \to \mathbb{F}_q^{t+4}$, $f_\alpha^1(x) = x + \alpha \mathbf{c}_1^{(1)}$. Let

$$\overline{A}_1 := \{\mathbf{0},\ \lambda \mathbf{c}_1^{(i)},\ \lambda \mathbf{c}_1^{(1)} + \mu \mathbf{c}_1^{(j)} : \lambda, \mu \in \mathbb{F}_q \setminus 0,\ 1 \le i \le s,\ 2 \le j \le s\} \subseteq A_1.$$

Note that $f_\alpha^1(\overline{A}_1) = \overline{A}_1$ for all $\alpha \in \mathbb{F}_q$, $|\overline{A}_1| = 1 + (q-1)s + (q-1)^2(s-1)$, and $f_\alpha^1(\mathbb{F}_q^{t+4} \setminus \overline{A}_1) = \mathbb{F}_q^{t+4} \setminus \overline{A}_1$. Since $c(s) < q^{t+4}$ we find that $f_\alpha^1(\mathbb{F}_q^{t+4} \setminus A_1)$, $\alpha \in \mathbb{F}_q$, are q subsets of $\mathbb{F}_q^{t+4} \setminus \overline{A}_1$ such that

$$|f_\alpha^1(\mathbb{F}_q^{t+4} \setminus A_1)| = |\mathbb{F}_q^{t+4} \setminus A_1| > \frac{q-1}{q} |\mathbb{F}_q^{t+4} \setminus \overline{A}_1|.$$

Therefore we have $\bigcap_{\alpha \in \mathbb{F}_q} f_\alpha^1(\mathbb{F}_q^{t+4} \setminus A_1) \neq \emptyset$.

So we get some $\mathbf{c}_2^{(1)}$ in $\mathbb{F}_q^{t+4}$ with $\mathbf{c}_2^{(1)} \in f_\alpha^1(\mathbb{F}_q^{t+4} \setminus A_1)$ for all $\alpha \in \mathbb{F}_q$. Hence $f_\alpha^1(\mathbf{c}_2^{(1)}) = \mathbf{c}_2^{(1)} + \alpha \mathbf{c}_1^{(1)} \notin A_1$ for all $\alpha \in \mathbb{F}_q$. So we have found some $\mathbf{c}_2^{(1)}$ such that $((\mathbf{c}_1^{(1)}/\mathbf{c}_2^{(1)}), (\mathbf{c}_1^{(2)}), \ldots, (\mathbf{c}_1^{(s)}))$ is a subsystem of the desired $(4, t+4, 2, s)$-system.

Now let $1 \le k \le s$ and assume that we have found $\mathbf{c}_2^{(1)}, \ldots, \mathbf{c}_2^{(k-1)}$ such that $((\mathbf{c}_1^{(1)}/\mathbf{c}_2^{(1)}), \ldots, (\mathbf{c}_1^{(k-1)}/\mathbf{c}_2^{(k-1)}), (\mathbf{c}_1^{(k)}), \ldots, (\mathbf{c}_1^{(s)}))$ is a subsystem of the desired $(4, t+4, 2, s)$-system.

For $A_k := A_1 \cup \{\lambda \mathbf{c}_2^{(i)},\ \lambda \mathbf{c}_1^{(i)} + \mu \mathbf{c}_2^{(i)} : \lambda, \mu \in \mathbb{F}_q \setminus 0,\ 1 \le i \le k-1\}$ we have $|A_k| = |A_1| + (k-1)(q - 1 + (q-1)^2)$.

For each $\alpha \in \mathbb{F}_q$ define $f_\alpha^k : \mathbb{F}_q^{t+4} \to \mathbb{F}_q^{t+4}$, $f_\alpha^k(x) = x + \alpha \mathbf{c}_1^{(k)}$. Let

$$\overline{A}_k := \{\mathbf{0},\ \lambda \mathbf{c}_1^{(i)},\ \lambda \mathbf{c}_1^{(k)} + \mu \mathbf{c}_1^{(j)} : \lambda, \mu \in \mathbb{F}_q \setminus 0,\ 1 \le i \le s,\ 1 \le j \ne k \le s\},$$

$\overline{A}_k \subseteq A_k$. As before we get $f_\alpha^k(\overline{A}_k) = \overline{A}_k$ for all $\alpha \in \mathbb{F}_q$, $|\overline{A}_k| = 1 + (q-1)s + (q-1)^2(s-1)$, and $f_\alpha^k(\mathbb{F}_q^{t+4} \setminus \overline{A}_k) = \mathbb{F}_q^{t+4} \setminus \overline{A}_k$. Since $k \le s$ and $c(s) < q^{t+4}$ the same arguments as before lead to $\bigcap_{\alpha \in \mathbb{F}_q} f_\alpha^k(\mathbb{F}_q^{t+4} \setminus A_k) \neq \emptyset$.

Hence there is some $\mathbf{c}_2^{(k)}$ in $\mathbb{F}_q^{t+4}$ such that $\mathbf{c}_2^{(k)} + \alpha \mathbf{c}_1^{(k)} \notin A_k$ for all $\alpha \in \mathbb{F}_q$ and so $((\mathbf{c}_1^{(1)}/\mathbf{c}_2^{(1)}), \ldots, (\mathbf{c}_1^{(k)}/\mathbf{c}_2^{(k)}), (\mathbf{c}_1^{(k+1)}), \ldots, (\mathbf{c}_1^{(s)}))$ is a subsystem of a $(4, t+4, 2, s)$-system.

We now extend the above constructed $(4, t+4, 2, s)$-system to a $(4, t+4, 3, s)$-system. For fixed $1 \le i \le s$ let

$$S(i) := \{\mathbf{0}, \lambda \mathbf{c}_1^{(j)},\ \lambda \mathbf{c}_2^{(i)},\ \lambda \mathbf{c}_1^{(i)} + \mu \mathbf{c}_1^{(k)},\ \lambda \mathbf{c}_2^{(i)} + \mu \mathbf{c}_1^{(j)},\ \lambda \mathbf{c}_1^{(i)} + \mu \mathbf{c}_2^{(i)} + \nu \mathbf{c}_1^{(k)}\}$$

for $1 \le j \le s$, $1 \le k \ne i \le s$, and $\lambda, \mu, \nu \in \mathbb{F}_q \setminus 0$. All these vectors $\in \mathbb{F}_q^{t+4}$ are different. For $s \ge 3$ we have $|S(i)| = 1 + (q-1)(s+1) + (q-1)^2(2s-1) + (q-1)^3(s-1) \le c(s) < q^{t+4}$, and therefore there exists a vector $\mathbf{c}_3^{(i)} \in \mathbb{F}_q^{t+4}$ with $\mathbf{c}_3^{(i)} \notin S$. $\mathbf{c}_3^{(1)}, \ldots, \mathbf{c}_3^{(s)}$ extend our system to a $(4, t+4, 3, s)$-system.

$\mathbf{c}_4^{(1)} := \mathbf{c}_1^{(2)}$ and $\mathbf{c}_4^{(i)} := \mathbf{c}_1^{(1)}$, $2 \le i \le s$, extend, for example, this system to a $(4, t+4, 4, s)$-system over $\mathbb{F}_q$ and therefore to a digital $(t, t+4, s)$-net over $\mathbb{F}_q$. ∎

R e m a r k. If we compute $N := N(t,q)$ to be the largest integer for which we have $c(N) < q^{t+4}$, then, for $s \le \min(N(t,q), \max_4(t+4,q))$, a digital $(t, t+4, s)$-net over $\mathbb{F}_q$ exists.

In Table 4 we compare the lower bounds for $\widetilde{s}(t, t+4, q)$ deduced from Theorem 2 ($\min(N(t,q), \max_4(t+4,q))$) with the results deduced from [7, Theorem 1] ($\max_4(t+4,q)/2$). Note that "$\max_4(t+4,q)$: upp" is also an upper bound for $\widetilde{s}(t, t+4, q)$.

Table 4. Lower bounds for $\widetilde{s}(t, t+4, q)$

t	1	2	3	4	5	6	7	8	9	10
$N(t,2)$	4	6	9	14	21	30	43	62	89	126
$\max_4(t+4,2)$: low	6	8	11	17	23	33	47	65	81	128
[7, Theorem 1]	3	4	5	8	11	16	23	32	40	64
Theorem 2	4	6	9	14	21	30	43	62	81	126
$\max_4(t+4,2)$: upp	6	8	11	17	23	37	61	88	124	179
$N(t,3)$	5	10	18	32	56	98	171	297	514	892
$\max_4(t+4,3)$: low	11	14	27	41	86	122	130	–	–	–
[7, Theorem 1]	5	7	13	20	43	61	65	–	–	–
Theorem 2	5	10	18	32	56	98	130	–	–	–
$\max_4(t+4,3)$: upp	9	14	31	55	97	–	–	–	–	–
$N(t,4)$	7	14	30	60	120	241	482	965	1930	3861
$\max_4(t+4,4)$: low	11	21	43	65	82	126	128	156	–	–
[7, Theorem 1]	5	10	21	32	41	63	64	78	–	–
Theorem 2	7	14	30	60	82	126	128	156	–	–
$\max_4(t+4,4)$: upp	11	29	59	119	–	–	–	–	–	–

4. Best bounds for the dimension of digital $(t, t+k, s)$-nets over $\mathbb{F}_2$ with small k. In this section we give a survey of lower and upper bounds for the maximal dimension $\widetilde{s}(t, t+k, 2)$ of digital nets and close some gaps between these bounds.

Table 5. Best bounds for $\widetilde{s}(t, t+k, 2)$

	$t=1$		$t=2$		$t=3$	
$\widetilde{s}(t, t+4, 2)$ low	shift–net	5	"by hand"	8	"by hand"	11
$\widetilde{s}(t, t+4, 2)$ upp	Prop. 1	5	$\max_4(6,2)$	8	$\max_4(7,2)$	11
$\widetilde{s}(t, t+5, 2)$ low	Nied.–Xing	5	shift–net	7	Lemma 3(c)	9
$\widetilde{s}(t, t+5, 2)$ upp	Lemma 3(c)	5	Prop. 2	7	Lemma 3(c)	11
$\widetilde{s}(t, t+6, 2)$ low	Nied.–Xing	5	"by hand"	6	shift–net	9
$\widetilde{s}(t, t+6, 2)$ upp	Lemma 3(c)	5	Lemma 4	6	Prop. 1	10

Explanations to Table 5:

• "shift–net" means that the net is provided by the so-called shift method of Schmid [14]. This method improves many of the best known values. The article [14] is in preparation so we enclose the concrete matrices in the appendix.

• "by hand" means that the matrices providing this net were found by trying and using linear properties — see the appendix.

• "Nied.–Xing" refers to the method of Niederreiter and Xing which we have mentioned in the section on digital sequences. We also have found matrices providing such nets "by hand" but we have resigned to include them in the appendix. We remark that the lower bound for $\widetilde{s}(t, t+4, 2)$ can also be deduced by their method.

• As mentioned in the previous section, an upper bound for $\max_k(t+k, q)$ is also an upper bound for $\widetilde{s}(t, t+k, q)$.

R e m a r k. We want to point out that the lower bounds in Table 5 are not only existence results. All of the matrices providing the digital nets with the given parameters can be obtained from the authors.

PROPOSITION 2. *For $s \geq 8$, a digital $(2, 7, s)$-net over $\mathbb{F}_2$ cannot exist.*

P r o o f. By Lemma 3(b) it suffices to show that there is no digital $(2, 7, 8)$-net over $\mathbb{F}_2$. Assume that there is a system providing a digital $(2, 7, 8)$-net over $\mathbb{F}_2$. Then there exists a subsystem S which is a $(5, 7, 2, 8)$-system over $\mathbb{F}_2$. We identify a row vector in $\mathbb{F}_2^7$ with a subset of $\{0, 1, \ldots, 6\}$ indicating the coordinates which are 1, and write $S = ((x_0/y_0), (x_1/y_1), \ldots$ $\ldots, (x_7/y_7))$ where x_i, y_i are subsets of $\{0, 1, \ldots, 6\}$ for $0 \leq i \leq 7$. It follows that $\dim[x_0, \ldots, x_7] \geq 5$.

(1) $\dim[x_0, \ldots, x_7] = 5$. We can assume $x_0 = 0, \ldots, x_4 = 4$ and $x_5, x_6, x_7 \in [0, 1, \ldots, 4]$. It follows that $x_5 = x_6 = 01234$, which is a contradiction.

(2) $\dim[x_0, \ldots, x_7] = 6$. We can assume $x_0 = 0, \ldots, x_5 = 5$ and $x_6, x_7 \in [0, 1, \ldots, 5]$. It follows that $x_6, x_7 \in \{\alpha, \alpha + i : 0 \leq i \leq 5\}$ with $\alpha = 012345$, which leads to a contradiction.

(3) $\dim[x_0, \ldots, x_7] = 7$. We can assume $S = ((0/y_0), \ldots, (6/y_6), (x_7/y_7))$ where x_7, y_i are subsets of $\{0, 1, \ldots, 6\}$ for $0 \leq i \leq 7$. Now let

$$y_i' = \begin{cases} y_i & \text{if } i \notin y_i, \\ y_i + i & \text{otherwise,} \end{cases} \qquad \text{for } 0 \leq i \leq 6.$$

It is easy to check that S is a $(5, 7, 2, 8)$-system if and only if $S' = ((0/y_0'), \ldots$ $\ldots, (6/y_6'), (x_7/y_7))$ is a $(5, 7, 2, 8)$-system. So without loss of generality we get the above system S with $i \notin y_i$, $0 \leq i \leq 6$. It follows that $5 \leq |x_7| \leq 7$.

(a) $|x_7| = 7$. Hence $x_7 = 0123456$. It follows that there is no y_7 such that $((0), (1), \ldots, (6), (0123456/y_7))$ is a subsystem of S.

(b) $|x_7| = 6$. We can assume $x_7 = 012345$. For $((0), (1), \ldots, (6), (012345/y_7))$ is a subsystem of S it follows that $|y_7| = 4$; we can assume $y_7 =$

0126. But now we conclude that there is no y_6 such that $((0),(1),\dots,(5),(6/y_6),(012345/y_7))$ is a subsystem of S.

(c) $|x_7| = 5$. We can assume $x_7 = 01234$. Searching for some y_7 we get $|y_7| = 4$ or 5. It follows that $5,6 \in y_7$ and that there is no $0 \le i \le 4$ such that $|y_i| = 6$.

(i) $|y_7| = 5$. We can assume $y_7 = 01256$. Now take a look at the subsystem $((0/y_0),(1),(2),(3/y_3),(4/y_4),(5),(6),(01234/01256))$ of S. It is easy to see that $|y_3| = |y_4| = 5$ and $4,5,6 \in y_3$ and $3,5,6 \in y_4$. Furthermore, we get $y_3 \in \{01456, 02456, 12456\}$ and $y_4 \in \{01356, 02356, 12356\}$ and, without loss of generality, $y_3 = 01456$. Hence we have $y_4 = 02356$ or $y_4 = 12356$ and, without loss of generality, $y_4 = 02356$. Looking at the cases $|y_0| = 4$ or 5 it is easy to see that no y_0 exists such that $((0/y_0),(1),(2),(3/01456),(4/02356),(5),(6),(01234/01256))$ is a subsystem of S.

(ii) $|y_7| = 4$. We can assume $y_7 = 0156$. We find that the system S has the form $S = ((0/y_0),\dots,(6/y_6),(01234/0156))$ with $i \notin y_i$ and $|y_i| = 4$ or 5 for $0 \le i \le 6$. Looking at y_0 and y_1 we get $|y_0| = |y_1| = 5$ and $1,5,6 \in y_0$ and $0,5,6 \in y_1$. It follows that $y_0 \in \{12356, 12456, 13456\}$ and $y_1 \in \{02356, 02456, 03456\}$. We can assume $y_0 = 12356$ and therefore $y_1 \in \{02456, 03456\}$. We can assume $y_1 = 02456$. Looking at several cases we find that there is no y_2 such that $((0/12356),(1/02456),(2/y_2),3,4,5,6,(01234/0156))$ is a subsystem of S. ∎

Remark. In [15] it is conjectured that for prime powers q the existence of a digital net over $\mathbb{F}_q$ is equivalent to the existence of a general net in base q. But there are also many opinions against this (private communication). The sharp bounds (for the dimension of digital nets) of the last sections will make it easier to find counterexamples to this conjecture (if they exist).

Acknowledgements. We would like to thank Jürgen Bierbrauer and the referee, who both independently gave us the essential hint to improve Proposition 1 to its final form.

Appendix

A1. *Digital* $(2,6,8)$*-net over* $\mathbb{F}_2$

$$\begin{pmatrix}100000\\101110\\000011\\010000\end{pmatrix}\quad\begin{pmatrix}010000\\010111\\001100\\100000\end{pmatrix}\quad\begin{pmatrix}001000\\101101\\000110\\100000\end{pmatrix}\quad\begin{pmatrix}000100\\011101\\000011\\100000\end{pmatrix}$$

$$\begin{pmatrix}000010\\101011\\001100\\100000\end{pmatrix}\quad\begin{pmatrix}000001\\011011\\000110\\100000\end{pmatrix}\quad\begin{pmatrix}111100\\101010\\000011\\100000\end{pmatrix}\quad\begin{pmatrix}110011\\010101\\000011\\100000\end{pmatrix}$$

A2. *Digital* $(3,7,11)$*-net over* $\mathbb{F}_2$

$$\begin{pmatrix}1000000\\0100110\\0000011\\0100000\end{pmatrix}\quad\begin{pmatrix}0100000\\1010010\\0000011\\1000000\end{pmatrix}\quad\begin{pmatrix}0010000\\1101000\\0000011\\1000000\end{pmatrix}\quad\begin{pmatrix}0001000\\0110001\\0000101\\1000000\end{pmatrix}$$
$$\begin{pmatrix}0000100\\1011000\\0000011\\1000000\end{pmatrix}\quad\begin{pmatrix}0000010\\0101100\\0000101\\1000000\end{pmatrix}\quad\begin{pmatrix}0000001\\0010110\\0001100\\1000000\end{pmatrix}\quad\begin{pmatrix}1110100\\1010001\\0000011\\1000000\end{pmatrix}$$
$$\begin{pmatrix}0111010\\1100001\\0000011\\1000000\end{pmatrix}\quad\begin{pmatrix}0011101\\1001010\\0000011\\1000000\end{pmatrix}\quad\begin{pmatrix}1111111\\1001100\\0000011\\1000000\end{pmatrix}$$

A3. *Digital* $(2,8,6)$*-net over* $\mathbb{F}_2$

$$\begin{pmatrix}10000000\\01001110\\10000011\\00000001\\00010100\\01000000\end{pmatrix}\quad\begin{pmatrix}01000000\\10101011\\00100010\\00010001\\00000011\\10000000\end{pmatrix}\quad\begin{pmatrix}00100000\\11010010\\00010011\\00000101\\00000010\\10000000\end{pmatrix}$$
$$\begin{pmatrix}00010000\\01100111\\00000110\\00001001\\00000011\\10000000\end{pmatrix}\quad\begin{pmatrix}00001000\\10010111\\00000010\\00000001\\00100100\\10000000\end{pmatrix}\quad\begin{pmatrix}00000100\\00111010\\00001011\\10000001\\00000010\\10000000\end{pmatrix}$$

B1. *Digital* $(1,5,5)$*-net over* $\mathbb{F}_2$ (*shift method*)

$$\begin{pmatrix}00001\\01110\\10010\\00010\end{pmatrix}\quad\begin{pmatrix}00010\\11100\\00101\\00100\end{pmatrix}\quad\begin{pmatrix}00100\\11001\\01010\\01000\end{pmatrix}\quad\begin{pmatrix}01000\\10011\\10100\\10000\end{pmatrix}\quad\begin{pmatrix}10000\\00111\\01001\\00001\end{pmatrix}$$

B2. *Digital* $(2,7,7)$*-net over* $\mathbb{F}_2$ (*shift method*)

$$\begin{pmatrix}0000001\\0101110\\0011010\\0000110\\0000010\end{pmatrix}\quad\begin{pmatrix}0000010\\1011100\\0110100\\0001100\\0000100\end{pmatrix}\quad\begin{pmatrix}0000100\\0111001\\1101000\\0011000\\0001000\end{pmatrix}\quad\begin{pmatrix}0001000\\1110010\\1010001\\0110000\\0010000\end{pmatrix}$$

$$\begin{pmatrix}0010000\\1100101\\0100011\\1100000\\0100000\end{pmatrix}\quad\begin{pmatrix}0100000\\1001011\\1000110\\1000001\\1000000\end{pmatrix}\quad\begin{pmatrix}1000000\\0010111\\0001101\\0000011\\0000001\end{pmatrix}$$

B3. *Digital* $(3,9,9)$*-net over* $\mathbb{F}_2$ (*shift method*)

$$\begin{pmatrix}000000001\\001011110\\010110010\\000100110\\000001010\\000000010\end{pmatrix}\quad\begin{pmatrix}000000010\\010111100\\101100100\\001001100\\000010100\\000000100\end{pmatrix}\quad\begin{pmatrix}000000100\\101111000\\011001001\\010011000\\000101000\\000001000\end{pmatrix}$$

$$\begin{pmatrix}000001000\\011110001\\110010010\\100110000\\001010000\\000010000\end{pmatrix}\quad\begin{pmatrix}000010000\\111100010\\100100101\\001100001\\010100000\\000100000\end{pmatrix}\quad\begin{pmatrix}000100000\\111000101\\001001011\\011000010\\101000000\\001000000\end{pmatrix}$$

$$\begin{pmatrix}001000000\\110001011\\010010110\\110000100\\010000001\\010000000\end{pmatrix}\quad\begin{pmatrix}010000000\\100010111\\100101100\\100001001\\100000010\\100000000\end{pmatrix}\quad\begin{pmatrix}100000000\\000101111\\001011001\\000010011\\000000101\\000000001\end{pmatrix}$$

References

[1] J. Bierbrauer, *Bounds on orthogonal arrays and resilient functions*, J. Combin. Designs 3 (1995), 179–183.

[2] A. E. Brouwer, *Data base of bounds for the minimum distance for binary, ternary and quaternary codes*, URL http://www.win.tue.nl/win/math/dw/voorlincod.html.

[3] R. Hill, *A First Course in Coding Theory*, Oxford Appl. Math. Comput. Sci. Ser., Oxford University Press, 1986.

[4] G. Larcher, H. Niederreiter, and W. Ch. Schmid, *Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration*, Monatsh. Math. 121 (1996), 231–253.

[5] G. Larcher, W. Ch. Schmid, and R. Wolf, *Digital* (t,m,s)*-nets, digital* (T,s)*-sequences, and numerical integration of multivariate Walsh series*, in: P. Hellekalek, G. Larcher, and P. Zinterhof (eds.), Proc. 1st Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, 1994, Technical Report Ser. 95–4, Austrian Center for Parallel Computation, 1995, 75–107.

[6] M. Lawrence, *Combinatorial bounds and constructions in the theory of uniform point distributions in unit cubes, connections with orthogonal arrays and a poset generalization of a related problem in coding theory*, PhD thesis, University of Wisconsin, May 1995.

[7] M. Lawrence, A. Mahalanabis, G. L. Mullen, and W. Ch. Schmid, *Construction of digital (t, m, s)-nets from linear codes*, in: S. D. Cohen and H. Niederreiter (eds.), Finite Fields and Applications (Glasgow, 1995), London Math. Soc. Lecture Note Ser. 233, Cambridge University Press, Cambridge, 1996, 189–208.

[8] B. Nashier and W. Nichols, *On Steinitz properties*, Arch. Math. (Basel) 57 (1991), 247–253.

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

[10] —, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS–NSF Ser. in Appl. Math. 63, SIAM, Philadelphia, 1992.

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

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

[13] —, —, *Quasirandom points and global function fields*, in: S. D. Cohen and H. Niederreiter (eds.), Finite Fields and Applications (Glasgow, 1995), London Math. Soc. Lecture Note Ser. 233, Cambridge University Press, Cambridge, 1996, 269–296.

[14] W. Ch. Schmid, *Shift–nets: a new class of binary digital (t, m, s)-nets*, submitted to Proceedings of the Second International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, 1996.

[15] —, *(t, m, s)-nets: digital construction and combinatorial aspects*, PhD thesis, Institut für Mathematik, Universität Salzburg, May 1995.

[16] J. H. van Lint, *Introduction to Coding Theory*, Springer, Berlin, 1992.

Institut für Mathematik
Universität Salzburg
Hellbrunnerstraße 34
A-5020 Salzburg, Austria
E-mail: wolfgang.schmid@sbg.ac.at

Received on 6.5.1996
and in revised form on 17.9.1996 (2978)