ACTA ARITHMETICA
102.2 (2002)

Constructions of digital nets

by

HARALD NIEDERREITER (Singapore)
and CHAOPING XING (Singapore and Anhui)

1. Introduction. The theory of digital (t, m, s)-nets provides powerful tools for the construction of low-discrepancy point sets in the s-dimensional unit cube. Various types of constructions of digital nets are already known; see [9] for the most recent survey. In this paper we first apply the duality theory for digital nets developed recently by Niederreiter and Pirsic [10] to establish a new propagation rule for digital nets (see Section 2). In Section 3 we construct families of digital (t, m, s)-nets with the property that if $m - t$ is fixed and the dimension s tends to ∞, then the quality parameter t grows at the minimal rate.

We follow the standard terminology in the area which goes back to the paper [7] and the monograph [8]. We refer also to the recent book of the authors [12, Chapter 8] for an expository account of the theory of (t, m, s)-nets.

2. A propagation rule from duality theory. We recall the basic definitions and facts of the duality theory for digital nets from [10]. In the context of digital nets, we may always assume $s \geq 2$ to avoid the trivial one-dimensional case. Let q be an arbitrary prime power and let $\mathbb{F}_q$ denote the finite field of order q. For a positive integer m and any vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ we introduce the weight $v(\mathbf{a})$ by $v(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0}$ and $v(\mathbf{a}) = \max\{j : a_j \neq 0\}$ if $\mathbf{a} \neq \mathbf{0}$. We extend this definition to $\mathbb{F}_q^{sm}$ by writing a vector $\mathbf{A} \in \mathbb{F}_q^{sm}$ as the concatenation of s vectors of length m, i.e.,

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

2000 *Mathematics Subject Classification*: 11K38, 11K45, 94B05.

Both authors are partially supported by the MOE-ARF grant R-146-000-029-112, the second author is also partially supported by the 100-person program of the Chinese Academy of Science. This paper was written while both authors were associated with the Institute for Mathematical Sciences at the National University of Singapore.

and putting

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

The following concept is crucial.

Definition 1. For any nonzero $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{sm}$ we define the *minimum distance*

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

Let the $m \times m$ matrices $C_1, \ldots, C_s$ over $\mathbb{F}_q$ be the generating matrices of a digital (t, m, s)-net $\mathcal{P}$ constructed over $\mathbb{F}_q$. As in [10] we set up the overall generating matrix

$$(C_1 | C_2 | \ldots | C_s) \in \mathbb{F}_q^{m \times sm}$$

and call its row space $\mathcal{C}$ the *row space* of the digital (t, m, s)-net $\mathcal{P}$. For an arbitrary $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{sm}$ we define its *dual space* $\mathcal{N}^{\perp}$ as in coding theory, i.e., as the dual space of $\mathcal{N}$ with respect to the standard inner product on $\mathbb{F}_q^{sm}$. Note that

$$\dim(\mathcal{N}^{\perp}) = sm - \dim(\mathcal{N}) \quad \text{and} \quad (\mathcal{N}^{\perp})^{\perp} = \mathcal{N}.$$

In particular, for the row space $\mathcal{C}$ of the digital (t, m, s)-net $\mathcal{P}$ we have $\dim(\mathcal{C}^{\perp}) \geq sm - m$. We note the following easy consequence of a result in [10].

Lemma 1. *Let q be a prime power and let $s \geq 2$ and $m \geq 1$ be integers. Then from any $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{sm}$ with $\dim(\mathcal{N}) \geq sm - m$ we obtain a digital (t, m, s)-net constructed over $\mathbb{F}_q$ with $t = m - \delta_m(\mathcal{N}) + 1$.*

Proof. For $\mathcal{C} := \mathcal{N}^{\perp}$ we have $\dim(\mathcal{C}) \leq m$, and so $\mathcal{C}$ is the row space of a suitable digital net constructed over $\mathbb{F}_q$. This net has the parameter triple (t, m, s) with

$$t = m - \delta_m(\mathcal{C}^{\perp}) + 1 = m - \delta_m(\mathcal{N}) + 1$$

according to [10, Corollary 1]. ■

Theorem 1. *Let q be a prime power and let s, m, k, and h be positive integers with $k \geq h$. Then, given a nonzero $\mathbb{F}_{q^h}$-linear subspace $\mathcal{M}$ of $\mathbb{F}_{q^h}^{sm}$, we can construct an $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{skm}$ with*

$$\dim_{\mathbb{F}_q}(\mathcal{N}) = h \dim_{\mathbb{F}_{q^h}}(\mathcal{M}), \qquad \delta_{km}(\mathcal{N}) \geq k\delta_m(\mathcal{M}) - (h-1)s.$$

Proof. Let $\mathcal{W}$ be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^k$ given by

$$\mathcal{W} = \{(b_1, \ldots, b_k) \in \mathbb{F}_q^k : b_j = 0 \text{ for } 1 \leq j \leq k - h\}.$$

Since $\dim_{\mathbb{F}_q}(\mathcal{W}) = h$, there exists an $\mathbb{F}_q$-linear isomorphism $\phi : \mathbb{F}_{q^h} \to \mathcal{W}$. This induces the map

$$\phi^{(m)} : \mathbb{F}_{q^h}^m \to \mathbb{F}_q^{km}, \qquad (\alpha_1, \ldots, \alpha_m) \mapsto (\phi(\alpha_1), \ldots, \phi(\alpha_m)).$$

Note that $\phi^{(m)}$ is an $\mathbb{F}_q$-linear monomorphism. Now define $\psi : \mathcal{M} \to \mathbb{F}_q^{skm}$ by taking

$$\mathbf{M} = (\mathbf{m}^{(1)}, \ldots, \mathbf{m}^{(s)}) \in \mathcal{M}, \qquad \mathbf{m}^{(i)} \in \mathbb{F}_{q^h}^m \text{ for } 1 \le i \le s,$$

and setting

$$\psi(\mathbf{M}) = (\phi^{(m)}(\mathbf{m}^{(1)}), \ldots, \phi^{(m)}(\mathbf{m}^{(s)})).$$

Then ψ is again an $\mathbb{F}_q$-linear monomorphism. Put $\mathcal{N} = \psi(\mathcal{M})$. Then $\mathcal{N}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{skm}$ with

$$\dim_{\mathbb{F}_q}(\mathcal{N}) = \dim_{\mathbb{F}_q}(\mathcal{M}) = h \dim_{\mathbb{F}_{q^h}}(\mathcal{M}).$$

Now we consider $\delta_{km}(\mathcal{N})$. A typical element of $\mathcal{N}$ is

$$\psi(\mathbf{M}) = (\phi^{(m)}(\mathbf{m}^{(1)}), \ldots, \phi^{(m)}(\mathbf{m}^{(s)})).$$

Then

$$V_{km}(\psi(\mathbf{M})) = \sum_{i=1}^{s} v(\phi^{(m)}(\mathbf{m}^{(i)})).$$

Let $\psi(\mathbf{M}) \neq \mathbf{0}$, then $\mathbf{M} \neq \mathbf{0}$. Put

$$u_i = v(\mathbf{m}^{(i)}) \qquad \text{for } 1 \le i \le s.$$

If $u_i = 0$, that is, $\mathbf{m}^{(i)} = \mathbf{0}$, then $\phi^{(m)}(\mathbf{m}^{(i)}) = \mathbf{0}$, and so $v(\phi^{(m)}(\mathbf{m}^{(i)})) = 0$. If $u_i \ge 1$, then $1 \le u_i \le m$ and

$$\mathbf{m}^{(i)} = (\beta_1, \ldots, \beta_{u_i}, 0, \ldots, 0)$$

with $\beta_l \in \mathbb{F}_{q^h}$ for $1 \le l \le u_i$ and $\beta_{u_i} \neq 0$. It follows that

$$\phi^{(m)}(\mathbf{m}^{(i)}) = (\phi(\beta_1), \ldots, \phi(\beta_{u_i}), \mathbf{0}, \ldots, \mathbf{0}) = (\mathbf{c}_1, \ldots, \mathbf{c}_{u_i}, \mathbf{0}, \ldots, \mathbf{0})$$

with $\mathbf{c}_l \in \mathcal{W} \subseteq \mathbb{F}_q^k$ for $1 \le l \le u_i$ and $\mathbf{c}_{u_i} \neq \mathbf{0}$. Thus,

$$v(\phi^{(m)}(\mathbf{m}^{(i)})) = k(u_i - 1) + v(\mathbf{c}_{u_i}) \ge k(u_i - 1) + k - h + 1 = ku_i - h + 1,$$

where we used the obvious fact that $\delta_k(\mathcal{W}) = k - h + 1$. The above inequality holds trivially if $u_i = 0$, and so in all cases. Therefore we obtain

$$\begin{aligned} V_{km}(\psi(\mathbf{M})) &\ge \sum_{i=1}^{s} (ku_i - h + 1) = k \sum_{i=1}^{s} v(\mathbf{m}^{(i)}) - (h-1)s \\ &= kV_m(\mathbf{M}) - (h-1)s \ge k\delta_m(\mathcal{M}) - (h-1)s, \end{aligned}$$

which implies the desired lower bound on $\delta_{km}(\mathcal{N})$. ■

COROLLARY 1. *Let q be a prime power and let s, m, and h be positive integers with $s \ge 2$. Then, given a digital (t, m, s)-net constructed over $\mathbb{F}_{q^h}$,* *we can obtain a digital* (u, hm, s)*-net constructed over* $\mathbb{F}_q$ *with* $u \le ht + (h-1)(s-1)$.

Proof. Let $\mathcal{C}$ be the row space of the given digital (t, m, s)-net. Then its dual space $\mathcal{M} := \mathcal{C}^{\perp}$ satisfies

$$\dim_{\mathbb{F}_{q^h}}(\mathcal{M}) \ge sm - m, \quad \delta_m(\mathcal{M}) \ge m - t + 1,$$

where the second inequality follows from [10, Theorem 2]. Now we apply Theorem 1 with $k = h$. This yields an $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{shm}$ with

$$\dim_{\mathbb{F}_q}(\mathcal{N}) \ge shm - hm$$

and

$$\delta_{hm}(\mathcal{N}) \ge h(m - t + 1) - (h-1)s = hm + 1 - (ht + (h-1)(s-1)).$$

The rest follows from Lemma 1. ∎

Corollary 1 yields a new propagation rule for digital nets which can be viewed as an analog of Propagation Rule 6 in [9] for general nets (see also [11], [14] for the latter propagation rule).

In the following result we use the standard notation $F/\mathbb{F}_{q^h}$ for a global function field F with full constant field $\mathbb{F}_{q^h}$.

Corollary 2. *Let* q *be a prime power and let* $s, m, h,$ *and* g *be integers with* $s \ge 2$, $h \ge 1$, $g \ge 0$, *and* $m \ge \max(1, g)$. *Then we get a digital* $(hg + (h-1)(s-1), hm, s)$*-net constructed over* $\mathbb{F}_q$ *whenever there is a global function field* $F/\mathbb{F}_{q^h}$ *of genus* g *with at least* s *places of degree* 1.

Proof. It was shown in [11], [13] that, under the given conditions, there exists a digital (g, m, s)-net constructed over $\mathbb{F}_{q^h}$. The rest follows from Corollary 1. ∎

Example 1. We apply Corollary 2 with F being the rational function field over $\mathbb{F}_{q^h}$. Then $g = 0$ and we can take $s = q^h + 1$. Thus, for any prime power q and any positive integers h and m we obtain a digital $((h-1)q^h, hm, q^h + 1)$-net constructed over $\mathbb{F}_q$.

3. Digital nets with good asymptotic behavior. We study the existence of digital $(t, t+d, s)$-nets constructed over $\mathbb{F}_q$ for a fixed integer $d \ge 0$ and a fixed prime power q. Since it is trivial that for $d = 0, 1$ such digital nets always exist, we assume $d \ge 2$ in the remainder of the paper. In any sequence of such digital nets with the dimension s tending to ∞, the quality parameter t must have a certain minimal rate of growth. In detail, if $d \ge 2$ and q are fixed, then for any sequence of digital $(t_r, t_r + d, s_r)$-nets constructed over $\mathbb{F}_q$ with $s_r \to \infty$ as $r \to \infty$ we have

$$\liminf_{r \to \infty} \frac{t_r}{\log_q s_r} \ge \left\lfloor \frac{d}{2} \right\rfloor, \tag{1}$$

where $\log_q$ denotes the logarithm to the base q. This was deduced in [13] from a result of Schmid and Wolf [15].

The interesting question is then whether one can construct such sequences of digital nets with the optimal growth rate $t_r = \mathcal{O}(\log s_r)$. The following result was obtained in [13] by using global function fields: if $d \geq 2$ and q are fixed and $\varepsilon > 0$ is given, then there exists a sequence of digital $(t_r, t_r + d, s_r)$-nets constructed over $\mathbb{F}_q$ such that $s_r \to \infty$ as $r \to \infty$ and

$$\lim_{r\to\infty} \frac{t_r}{\log_q s_r} = d + 1 + \varepsilon. \tag{2}$$

This still leaves the problem of improving the constant on the right-hand side of (2), and it is this problem which we address in this section.

We use some tools from coding theory and refer to the standard monographs [6], [16] for the necessary background. For a linear code over $\mathbb{F}_q$ the parameter triple $[n, k, \geq d+1]$ indicates that the code has length n, dimension k, and minimum distance at least $d+1$. The following quantity is well known in coding theory (see e.g. [3, Chapter 14]).

Definition 2. For a given prime power q and integers $r \geq d \geq 2$, let $M_d(r, q)$ be the largest value of n for which there exists a linear $[n, n-r, \geq d+1]$ code over $\mathbb{F}_q$.

It is trivial that $M_d(r, q) \geq r + 1$. The following two remarks on the asymptotic behavior of $M_d(r, q)$ for fixed d and q and $r \to \infty$ belong to the folklore of coding theory, but we give the short proofs for the sake of completeness.

Remark 1. If there exists a linear $[n, n-r, \geq d+1]$ code over $\mathbb{F}_q$, then by the Hamming bound

$$\sum_{i=0}^{f} \binom{n}{i} (q-1)^i \leq q^r$$

with $f := \lfloor d/2 \rfloor$. Choose $r \geq d \geq 2$ and $n = M_d(r, q) \geq r + 1$. Then $n \geq 2f$, and so

$$\frac{1}{f!}\left(\frac{n}{2}\right)^f \leq \binom{n}{f} \leq q^r.$$

This implies

$$\log_q c_d + f \log_q n \leq r$$

with some constant $c_d > 0$ depending only on d, and so

$$\liminf_{r\to\infty} \frac{r}{\log_q M_d(r, q)} \geq \left\lfloor \frac{d}{2} \right\rfloor.$$

Remark 2. By the Gilbert–Varshamov bound there exists a linear $[n, n-r, \geq d+1]$ code over $\mathbb{F}_q$ whenever

$$q^r > \sum_{i=0}^{d-1} \binom{n-1}{i} (q-1)^i.$$

Choose again $r \geq d \geq 2$ and put

$$n = \lfloor q^{r/(d-1)-3} \rfloor + 1.$$

Then $n - 1 \geq 2(d-1)$ for sufficiently large r, and so

$$\begin{aligned}\sum_{i=0}^{d-1} \binom{n-1}{i} (q-1)^i &\leq d\binom{n-1}{d-1}(q-1)^{d-1} < d(n-1)^{d-1} q^d \\ &\leq dq^{r-3(d-1)} q^d = dq^{r-2d+3} \leq q^r.\end{aligned}$$

Thus, the Gilbert–Varshamov bound is satisfied for the chosen parameters, and so

$$M_d(r, q) \geq \lfloor q^{r/(d-1)-3} \rfloor + 1$$

for sufficiently large r. This implies

$$\limsup_{r\to\infty} \frac{r}{\log_q M_d(r,q)} \leq d - 1.$$

The following result shows the connection between the problem raised at the beginning of this section and the asymptotic behavior of $M_d(r, q)$.

Lemma 2. *For every prime power q and every integer $d \geq 2$, there exists a sequence of digital $(t_r, t_r + d, s_r)$-nets constructed over $\mathbb{F}_q$ with $s_r \to \infty$ as $r \to \infty$ and*

$$\lim_{r\to\infty} \frac{t_r}{\log_q s_r} = \liminf_{r\to\infty} \frac{r}{\log_q M_d(r,q)}.$$

Proof. Fix q and d and choose an integer $r \geq d$. Then by the definition of $M_d(r, q)$ there exists a linear $[M_d(r, q), M_d(r, q) - r, \geq d + 1]$ code over $\mathbb{F}_q$. Now an application of [4, Corollary 2] yields a digital $(r - d, r, s_r)$-net constructed over $\mathbb{F}_q$ with

$$s_r = \frac{M_d(r,q)}{e_d} - \theta(d, r, q),$$

where $e_d > 0$ is a constant depending only on d and $0 \leq \theta(d, r, q) \leq 2$. Then

$$\frac{t_r}{\log_q s_r} = \frac{r-d}{\log_q(M_d(r,q)/e_d - \theta(d,r,q))},$$

and by letting r pass through a suitable sequence of values we get the desired result. ∎

If we combine Remark 2 and Lemma 2, then we obtain the following result: for every prime power q and every integer $d \geq 2$, there exists a sequence of digital $(t_r, t_r + d, s_r)$-nets constructed over $\mathbb{F}_q$ with $s_r \to \infty$ as $r \to \infty$ and

$$\lim_{r\to\infty} \frac{t_r}{\log_q s_r} \le d - 1. \tag{3}$$

This already yields an improvement on (2), though in a nonconstructive manner (since the proof of the Gilbert–Varshamov bound is nonconstructive). We now show a constructive result which is at least as good as (3) and in many cases yields an improvement on (3).

THEOREM 2. *For every prime power q and every integer $d \ge 2$, there is a sequence of digital $(t_r, t_r + d, s_r)$-nets constructed over $\mathbb{F}_q$ with $s_r \to \infty$ as $r \to \infty$ and*

$$\lim_{r\to\infty} \frac{t_r}{\log_q s_r} \le d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor.$$

Proof. We use BCH codes with the notation in [5, Section 8.2]. Let m be an integer such that $q^m \ge d + 2$ and let α be a primitive element of $\mathbb{F}_{q^m}$. For $i = 0, 1, \ldots$ let $m^{(i)}(x)$ be the minimal polynomial of α^i over $\mathbb{F}_q$. Then $m^{(0)}(x) = x - 1$ and $\deg(m^{(i)}(x)) \le m$ for all $i \ge 1$. Now consider the BCH code C over $\mathbb{F}_q$ of length $q^m - 1$ and designed distance $d + 1$ for which the generator polynomial is

$$g(x) = \operatorname{lcm}(m^{(0)}(x), m^{(1)}(x), \ldots, m^{(d-1)}(x)).$$

Then C is a linear $[q^m - 1, q^m - 1 - \deg(g), \ge d + 1]$ code over $\mathbb{F}_q$. It is obvious that

$$m^{(i)}(x) = m^{(iq)}(x) \quad \text{for all } i \ge 1.$$

Therefore, when we form the lcm of the polynomials $m^{(i)}(x)$, $1 \le i \le d-1$, we can omit the polynomials $m^{(iq)}(x)$ with $1 \le i \le \lfloor (d-1)/q \rfloor$. Thus,

$$\deg(g) \le \deg(m^{(0)}) + \sum_{\substack{i=1 \\ q\nmid i}}^{d-1} \deg(m^{(i)}) \le 1 + m\left(d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor\right).$$

By passing to a suitable $\mathbb{F}_q$-linear subspace of C, we get a linear code over $\mathbb{F}_q$ with parameter triple

$$\left[q^m - 1, q^m - 1 - \left(1 + m\left(d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor\right)\right), \ge d + 1\right].$$

The definition of $M_d(r, q)$ implies that

$$M_d\left(1 + m\left(d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor\right), q\right) \ge q^m - 1.$$

This holds for all sufficiently large m, and so

$$\begin{aligned}\liminf_{r\to\infty}\frac{r}{\log_q M_d(r,q)} &\le \liminf_{m\to\infty}\frac{1+m\left(d-1-\left\lfloor\frac{d-1}{q}\right\rfloor\right)}{\log_q M_d\left(1+m\left(d-1-\left\lfloor\frac{d-1}{q}\right\rfloor\right),q\right)}\\ &\le \lim_{m\to\infty}\frac{1+m\left(d-1-\left\lfloor\frac{d-1}{q}\right\rfloor\right)}{\log_q(q^m-1)} = d-1-\left\lfloor\frac{d-1}{q}\right\rfloor.\end{aligned}$$

The proof is completed by invoking Lemma 2. ∎

COROLLARY 3. *For every integer $d \ge 2$ there exists a sequence of digital $(t_r, t_r + d, s_r)$-nets constructed over $\mathbb{F}_2$ with $s_r \to \infty$ as $r \to \infty$ and*

$$\lim_{r\to\infty}\frac{t_r}{\log_2 s_r} = \left\lfloor\frac{d}{2}\right\rfloor,$$

and the constant $\lfloor d/2\rfloor$ is best possible.

Proof. We use Theorem 2 with $q = 2$ and note that

$$d-1-\left\lfloor\frac{d-1}{2}\right\rfloor = \left\lfloor\frac{d}{2}\right\rfloor \quad \text{for all } d \ge 2.$$

The rest follows from (1). ∎

REMARK 3. A comparison with (1) shows that Theorem 2 is also best possible in two other cases. An obvious case is $d = 2$. Another special case in which Theorem 2 is best possible is $(q,d) = (3,4)$. For $(q,d) = (2,4)$ and $(3,4)$, the result of Theorem 2 can also be deduced from the constructions of Edel and Bierbrauer [1], [2].

References

[1] Y. Edel and J. Bierbrauer, *Construction of digital nets from BCH-codes*, in: Monte Carlo and Quasi-Monte Carlo Methods 1996, H. Niederreiter *et al.* (eds.), Springer, New York, 1998, 221–231.

[2] —, —, *Families of ternary (t,m,s)-nets related to BCH-codes*, Monatsh. Math. 132 (2001), 99–103.

[3] R. Hill, *A First Course in Coding Theory*, Oxford Univ. Press, Oxford, 1986.

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

[5] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, rev. ed., Cambridge Univ. Press, Cambridge, 1994.

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

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

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

[9] H. Niederreiter, *Constructions of (t, m, s)-nets*, in: Monte Carlo and Quasi-Monte Carlo Methods 1998, H. Niederreiter and J. Spanier (eds.), Springer, Berlin, 2000, 70–85.

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

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

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

[13] —, —, *A construction of digital nets with good asymptotic behavior*, preprint, 2001.

[14] G. Pirsic, *Base changes for (t, m, s)-nets and related sequences*, Sitzungsber. Österr. Akad. Wiss. Math.-Naturw. Kl. Abt. II 208 (1999), 115–122.

[15] W. C. Schmid and R. Wolf, *Bounds for digital nets and sequences*, Acta Arith. 78 (1997), 377–399.

[16] J. H. van Lint, *Introduction to Coding Theory*, 3rd ed., Springer, Berlin, 2000.

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

Department of Mathematics
University of Science and Technology of China
Hefei, Anhui, 230026, P.R. China

Received on 3.08.2001 (4090)