Nets, (t, s)-Sequences, and Algebraic Curves over Finite Fields with Many Rational Points

Harald Niederreiter

Abstract. The current status of the theory of (t, m, s)-nets and (t, s)-sequences is presented in a brief form, with some emphasis on the connections with algebraic geometry. Closely related work on constructions of algebraic curves over finite fields with many rational points and on improving the Gilbert-Varshamov bound in algebraic coding theory is discussed as well.

1991 Mathematics Subject Classification: 05B15, 11G20, 11K38, 11R58, 11T71, 14G15, 14H05, 94B27, 94B65.
Keywords and Phrases: quasirandom points, orthogonal arrays, algebraic curves over finite fields, rational points, algebraic-geometry codes, Gilbert-Varshamov bound.

1. Introduction and basic concepts

Nets and (t, s)-sequences are finite point sets, respectively infinite sequences, satisfying strong uniformity properties with regard to their distribution in the s-dimensional unit cube $I^s = [0, 1]^s$. The general theory of these combinatorial objects was first developed in [12]. They have attracted a lot of interest in scientific computing in recent years because of their role as quasirandom points in quasi-Monte Carlo methods, e.g. for numerical integration over I^s (see [14] for the details). They also offer a great appeal for theoretical studies in view of the many links with other areas such as classical combinatorial designs, coding theory, algebra, number theory, and algebraic geometry. To set the stage, we first review some basic definitions.

Definition 1. For a given dimension $s \geq 1$ and integers $b \geq 2$ and $0 \leq t \leq m$, a (t, m, s)-*net in base* b is a point set P consisting of b^m points in I^s such that every subinterval 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 $\mathrm{Vol}(J) = b^{t-m}$ contains exactly b^t points of P.

For integers $b \geq 2$ and $m \geq 1$ and a point $\mathbf{x} \in I^s$, we obtain $[\mathbf{x}]_{b,m} \in I^s$ by truncating a b-adic expansion of each coordinate of $\mathbf{x}$ after m terms. Here expansions with almost all digits equal to $b-1$ are allowed – thus, the truncation operates on the expansions of the coordinates of $\mathbf{x}$ and not on $\mathbf{x}$ itself. The following definition of a (t, s)-sequence is the slightly generalized version described in [20], [21] (see [14, Chapter 4] for the original narrower definition). We assume prescribed b-adic expansions on which the truncations operate.

DEFINITION 2. For a given dimension $s \geq 1$ and integers $b \geq 2$ and $t \geq 0$, 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.

The following useful principle shows that if we can construct a (t, s)-sequence, then we can construct infinitely many nets in dimension $s+1$ (see [12, Section 5], [20, Section 6]).

LEMMA 1. *If there exists a (t, s)-sequence in base b, then for every integer $m \geq t$ there exists a $(t, m, s+1)$-net in base b.*

The aim in the construction of (t, m, s)-nets and (t, s)-sequences in base b is to make the quality parameter t as small as possible if the other parameters are fixed. Most of the known constructions of nets and (t, s)-sequences are based on the digital method which was introduced in [12, Section 6]. For the sake of brevity, we just sketch the digital method for constructing (t, m, s)-nets in base b. Select a commutative ring R with identity and of finite order $b \geq 2$. For given $m \geq 1$ and $s \geq 1$ choose a system

$$C = \left\{ \mathbf{c}_j^{(i)} \in R^m : 1 \leq i \leq s, 1 \leq j \leq m \right\}.$$

Now we get the jth b-adic digits of the ith coordinates of the points of the (t, m, s)-net by forming the inner product of $\mathbf{c}_j^{(i)}$ with all elements of R^m and then identifying elements of R with b-adic digits. The value of the quality parameter t depends on the choice of C. The resulting net is called a *digital* (t, m, s)*-net in base* b (or *constructed over* R if we want to emphasize R). Similarly, we speak of a *digital* (t, s)*-sequence in base* b (or *constructed over* R if we want to emphasize R). There is a "digital" analog of Lemma 1, i.e., a digital (t, s)-sequence yields infinitely many digital nets in dimension $s+1$ (see [20, Section 2]). For practical purposes it suffices to consider the digital method in the special case where the ring R is a finite field $\mathbf{F}_q$ of prime-power order q. Digital nets and (t, s)-sequences in an arbitrary base b can be obtained by using rings R that are direct products of finite fields (see [14, Chapter 4], [20, Section 5]).

In this paper we give a brief review of the state-of-the-art in the area of (t, m, s)-nets and (t, s)-sequences, with some emphasis on the connections with algebraic geometry. Section 2 discusses links with classical combinatorial objects such as MOLS and orthogonal arrays. Constructions of nets and (t, s)-sequences, e.g. by methods using algebraic curves over finite fields, are presented in Section 3. This leads to the discussion of algebraic curves over finite fields with many rational points in Section 4. As a by-product we obtain the applications to algebraic coding theory in Section 5, such as improvements on the Gilbert-Varshamov bound. For various aspects, more detailed expository accounts can be found in [14, Chapter 4], [21], [25], [32].

2. Connections with combinatorial designs

The fact that there are close links between nets and combinatorial designs was noticed already in [12, Section 5]. For instance, it was shown there that for $s \geq 2$ the existence of a $(0, 2, s)$-net in base b is equivalent to the existence of $s-2$ MOLS of order b. Later it was proved by Mullen and Whittle [11] that for $s \geq 2$ and any $t \geq 0$, the existence of a $(t, t+2, s)$-net in base b is equivalent to the existence of a certain set of mutually orthogonal hypercubes of order b. In the language of orthogonal arrays, there is the result in [15] that there exists a $(t, t+2, s)$-net in base b if and only if there exists an orthogonal array $\mathrm{OA}(b^{t+2}, s, b, 2)$ of index b^t.

Lawrence [6] and Mullen and Schmid [10] independently established a combinatorial equivalence between arbitrary (t, m, s)-nets in base b and suitable combinatorial designs. Depending on the language that is used, these designs can be generalized orthogonal arrays, ordered orthogonal arrays, or strongly orthogonal hypercubes. The proofs of all these combinatorial results are constructive.

These connections with combinatorial designs imply obstructions to the existence of (t, m, s)-nets for $m \geq t+2$ (nets exist trivially for $m - t = 0, 1$). Consider e.g. the following simple argument: if there exists a $(0, m, s)$-net in base b for some $m \geq 2$, then there exists a $(0, 2, s)$-net in base b, hence there are $s - 2$ MOLS of order b, and so we must have $s \leq b + 1$. A more general argument of this type, combined with bounds for the appropriate combinatorial designs, leads to upper bounds on s in terms of b, m, and t, under the assumption that there exists a (t, m, s)-net in base b with $m \geq t + 2$. A description of this method, together with tables of bounds, can be found in [2]. More recently, this approach was further refined by Martin and Stinson [7], [8] and improved bounds were obtained. In view of Lemma 1, combinatorial obstructions to the existence of (t, m, s)-nets yield combinatorial obstructions to the existence of (t, s)-sequences, such as the following bound from [21].

Theorem 1. *Given $b \geq 2$ and $s \geq 1$, a (t, s)-sequence in base b can exist only if*

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

3. Constructions of nets and (t, s)-sequences

The number of known construction methods for nets and (t, s)-sequences is already quite large and ideas from various areas are employed. The combinatorial approach to the construction of nets uses the equivalences between (t, m, s)-nets and suitable combinatorial designs mentioned in Section 2 and techniques of constructing such combinatorial designs. Surveys of combinatorial methods for the construction of nets are given in [2], [9]. Other important methods for the construction of nets are based on coding theory. This approach goes back to an observation in [12, Section 7] that there is a connection between the digital method over a finite field $\mathbf{F}_q$ and the construction of parity-check matrices for good linear codes over $\mathbf{F}_q$. This connection is conveniently formalized through the notion of a (d, m, s)-*system over* $\mathbf{F}_q$ introduced in [32], which is a system $\left\{\mathbf{a}_j^{(i)} \in \mathbf{F}_q^m : 1 \leq i \leq s, 1 \leq j \leq m\right\}$ of vectors such that for any integers $d_1, \ldots, d_s \geq 0$ with $\sum_{i=1}^s d_i = d$ the $\mathbf{a}_j^{(i)}, 1 \leq j \leq d_i, 1 \leq i \leq s$, are linearly independent over $\mathbf{F}_q$. Finding a digital (t, m, s)-

net constructed over $\mathbf{F}_q$ is then equivalent to finding a (d, m, s)-system over $\mathbf{F}_q$ with $d = m - t$. The surveys [2], [9] report on coding-theory methods for the construction of nets and new methods of this type can be found in [32].

Standard constructions of digital (t, s)-sequences in base b are due to Sobol' [38] for $b = 2$ and any s, to Faure [3] for prime bases $b \geq s$, and to Niederreiter [13] for any b and any s. Generalizations of these sequences are described in Tezuka [39, Chapter 6]. As a by-product, these constructions yield digital $(t, m, s+1)$-nets in base b.

An important recent development is the use of algebraic curves over finite fields (or, equivalently, of global function fields) for the construction of (t, s)-sequences. The basic idea goes back to Niederreiter [16], [17]. At present, four different construction principles using algebraic curves are available and they all rely on the digital method over $\mathbf{F}_q$. We refer to [18], [20], [21], [44] for the detailed description of these constructions and to [25], [32] for further discussions. Three of the methods, and indeed the most effective ones, are based on algebraic curves over $\mathbf{F}_q$ with many $\mathbf{F}_q$-rational points (or, equivalently, on global function fields with many rational places). Given q and a dimension $s \geq 1$, the typical procedure is to choose a smooth, projective, absolutely irreducible algebraic curve $\mathcal{C}$ over $\mathbf{F}_q$ containing at least $s + 1$ $\mathbf{F}_q$-rational points, say $P_\infty, P_1, \ldots, P_s$. The point $P_i, 1 \leq i \leq s$, is used to produce the data that are needed in the digital method (i.e., certain elements of $\mathbf{F}_q$) for generating the ith coordinates of the points of the (t, s)-sequence. These elements of $\mathbf{F}_q$ are obtained by expansions on the curve $\mathcal{C}$ in local coordinates at P_∞. The methods in [20] and [44] yield digital (t, s)-sequences constructed over $\mathbf{F}_q$ with t being the genus of $\mathcal{C}$. If we optimize these constructions, we arrive in a natural way at the following important quantity from algebraic geometry over $\mathbf{F}_q$ and at the subsequent theorem in [20].

DEFINITION 3. For given $g \geq 0$ and q, let $N_q(g)$ be the maximum number of $\mathbf{F}_q$-rational points that a smooth, projective, absolutely irreducible algebraic curve over $\mathbf{F}_q$ of genus g can have.

THEOREM 2. *For every q and s there exists a digital $(V_q(s), s)$-sequence constructed over $\mathbf{F}_q$, where $V_q(s)$ is the least value of g such that $N_q(g) \geq s + 1$.*

The behavior of $V_q(s)$ as $s \to \infty$ can be obtained from class field towers and the asymptotic theory of $N_q(g)$ (see Section 5). As stated in Section 1, we can also pass from prime-power bases q to arbitrary bases b in the digital method. Finally, this leads to the following bound (see [20, Section 5]), which in view of Theorem 1 is best possible as far as the order of magnitude in s is concerned.

THEOREM 3. *For every $b \geq 2$ and $s \geq 1$ there exists a digital (t, s)-sequence in base b with*

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

where $c > 0$ is an absolute constant and q_1 is the least prime power in the factorization of b into pairwise coprime prime powers.

4. ALGEBRAIC CURVES WITH MANY RATIONAL POINTS

The constructions of (t, s)-sequences in Section 3 based on algebraic curves over $\mathbf{F}_q$ lead to the requirement of finding good lower bounds for the number $N_q(g)$ in Definition 3, or in other words to the problem of constructing algebraic curves over $\mathbf{F}_q$ of given genus g with many $\mathbf{F}_q$-rational points. This problem is also of great importance in the theory of algebraic-geometry codes (see Section 5). Recent surveys of this problem, also in the equivalent language of global function fields, are given in Garcia and Stichtenoth [4], Niederreiter and Xing [26], [30], and van der Geer and van der Vlugt [42].

A well-known technique for establishing the existence of various algebraic curves over $\mathbf{F}_q$ with many $\mathbf{F}_q$-rational points is due to Serre [37] and uses methods of class field theory. This approach was continued by Auer [1] and Lauter [5]. Usually, the curves obtained by this technique are not in an explicit form. On the other hand, constructions in the function field setting that work with Artin-Schreier and Kummer extensions and with subfields of cyclotomic function fields yield explicit generators and defining equations. Such constructions can be found e.g. in [19], [21], [26], [46] for $q = 2$, in [22], [27] for $q = 3$, in [22], [23] for $q = 4$, in [22], [24], [35] for $q = 5$, in [29] for $q = 8, 16$, and in [32] for $q = 9, 27$. Explicit constructions inspired by techniques from coding theory were introduced by van der Geer and van der Vlugt [41] (see also the survey [42]).

In the function field setting, a powerful technique of obtaining global function fields with many rational places is based on Hilbert class fields. The aim is to construct unramified abelian extensions of a given global function field F in which certain selected rational places of F split completely. This method works particularly well if the divisor class number of F is large relative to the genus of F. Applications of this method can be found in [22], [24], [26], [27], [29], [30], [35], [46]. A more general approach, which contains both cyclotomic function fields and Hilbert class fields as special cases, uses the theory of narrow ray class extensions obtained from Drinfeld modules of rank 1 and was introduced in [45]. This method allows great flexibility and produces a large number of families of global function fields with many rational places. We refer to [23], [24], [26], [27], [29], [30], [31], [35], [46] for further results and examples with this method.

Table 1 contains all bounds for $N_q(g)$ available to the author for $q = 2, 3, 4, 5, 8, 9, 16, 27$ and $1 \leq g \leq 50$ (for $g = 0$ we trivially have $N_q(0) = q + 1$). In each entry of the table, the first number is a lower bound for $N_q(g)$ and the second an upper bound for $N_q(g)$. If only one number is given, then this is the exact value of $N_q(g)$. A program for calculating upper bounds for $N_q(g)$, which is based on Weil's explicit formula for the number of $\mathbf{F}_q$-rational points in terms of the zeta function and on the trigonometric polynomials of Oesterlé, was kindly supplied by Jean-Pierre Serre. The lower bounds in Table 1 are obtained by combining [32, Table 3] with new data in [1], [35]. We refer also to the tables of van der Geer and van der Vlugt [43] which represent the most recent result of an ongoing project to update bounds for $N_q(g)$ periodically.

5. Applications to coding theory

There is an asymptotic theory of $N_q(g)$ which has significant applications to algebraic coding theory. The basic quantity here is

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

For values of q for which $A(q)$ is larger than a known comparison function, Goppa's construction of algebraic-geometry codes leads to improvements on the classical Gilbert-Varshamov bound for the existence of good linear codes over $\mathbf{F}_q$.

Let U_q be the set of ordered pairs $(\delta, R) \in [0,1]^2$ for which there exists a sequence of linear codes over $\mathbf{F}_q$ of increasing lengths such that δ is the limit of the relative minimum distances and R the limit of the information rates. It is known that for some continuous function α_q on $[0,1]$ we have

$$U_q = \{(\delta, R) : 0 \leq R \leq \alpha_q(\delta), 0 \leq \delta \leq 1\},$$

where $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for $\delta \in [(q-1)/q, 1]$. The function α_q is unknown, and it is an important issue in algebraic coding theory to obtain good lower bounds for α_q on the interval $(0, (q-1)/q)$. The Gilbert-Varshamov bound says that

$$\alpha_q(\delta) \geq R_{GV}(q, \delta) := 1 - H_q(\delta) \quad \text{for } 0 < \delta < (q-1)/q,$$

where H_q is the q-ary entropy function. Algebraic-geometry codes lead to the bound

$$\alpha_q(\delta) \geq R_{AG}(q, \delta) := 1 - \frac{1}{A(q)} - \delta \quad \text{for } 0 \leq \delta \leq 1.$$

By showing that $A(q) \geq q^{1/2} - 1$ if q is a square, Tsfasman, Vlădut, and Zink [40] proved that $R_{AG}(q, \delta) > R_{GV}(q, \delta)$ if q is a sufficiently large square and δ belongs to a suitable subinterval of $[0,1]$.

For nonsquares q only weaker lower bounds for $A(q)$ are known. Serre [37] showed that $A(q)$ is at least of the order of magnitude $\log q$, and an alternative proof and an effective version of this result were recently given in [33]. In many cases the following result in [28] yields a considerable improvement: if $q = p^e$ with a prime p and an odd integer $e \geq 3$, then $A(q)$ is at least of the order of magnitude $q^{1/(2k)}$, where k is the least prime factor of e. Further discussions and refinements of this result can be found in [30], [33]. As a consequence we get the following theorem in [28] which improves on the Gilbert-Varshamov bound for sufficiently large composite nonsquares q.

THEOREM 4. *Let $m \geq 3$ be an odd integer and let r be a prime power with $r \geq 100m^3$ for odd r and $r \geq 576m^3$ for even r. Then there exists an open interval $(\delta_1, \delta_2) \subseteq (0,1)$ containing $(r^m - 1)/(2r^m - 1)$ such that*

$$R_{AG}(r^m, \delta) > R_{GV}(r^m, \delta) \quad \textit{for all } \delta \in (\delta_1, \delta_2).$$

In connection with lower bounds for $A(q)$ we mention that there is a method of Perret [36] for obtaining such lower bounds which depends, however, on a conjecture that would provide a sufficient condition for the infinitude of certain ramified class field towers. It was recently shown in [34] by a counterexample that this conjecture is wrong. Therefore, the lower bounds for $A(q)$ in Perret [36, Section III] remain unproved.

Table 1: Bounds for $N_q(g)$

$g\backslash q$	2	3	4	5	8	9	16	27
1	5	7	9	10	14	16	25	38
2	6	8	10	12	18	20	33	48
3	7	10	14	16	24	28	38	58
4	8	12	15	18	25-29	30	45-47	64-68
5	9	12-14	17-18	20-22	29-32	32-36	49-55	55-78
6	10	14-15	20	21-25	33-36	35-40	65	76-88
7	10	16-17	21-22	22-27	33-39	39-43	63-70	64-98
8	11	15-18	21-24	22-29	34-43	38-47	61-76	92-108
9	12	19	26	26-32	45-47	40-51	72-81	82-118
10	13	19-21	27-28	27-34	38-50	54-55	81-87	91-128
11	14	20-22	26-30	32-36	48-54	55-59	80-92	96-138
12	14-15	22-24	29-31	30-38	49-57	55-63	68-97	109-148
13	15	24-25	33	36-40	50-61	60-66	97-103	136-156
14	15-16	24-26	32-35	39-43	65	56-70	97-108	84-164
15	17	28	33-37	35-45	54-68	64-74	98-113	136-171
16	17-18	27-29	36-38	40-47	56-71	74-78	93-118	136-178
17	17-18	24-30	40	42-49	61-74	56-82	96-124	128-185
18	18-19	26-31	41-42	32-51	65-77	46-85	113-129	94-192
19	20	27-32	37-43	45-54	58-80	84-88	121-134	126-199
20	19-21	30-34	37-45	30-56	68-83	48-91	121-140	133-207
21	21	32-35	41-47	50-58	72-86	82-95	129-145	163-214
22	21-22	28-36	40-48	51-60	66-89	78-98	129-150	112-221
23	22-23	26-37	41-50	55-62	68-92	92-101	126-155	114-228
24	20-23	28-38	42-52	46-64	66-95	91-104	129-161	166-235
25	24	36-40	51-53	52-66	66-97	64-108	144-166	196-242
26	24-25	36-41	55	45-68	72-100	110-111	150-171	108-249
27	22-25	39-42	49-56	52-70	96-103	60-114	145-176	114-256
28	25-26	37-43	51-58	54-71	97-106	105-117	136-181	108-263
29	25-27	42-44	49-60	56-73	97-109	104-120	161-187	114-270
30	25-27	34-46	53-61	58-75	80-112	60-123	161-192	117-277
31	27-28	40-47	60-63	72-77	72-115	84-127	150-197	114-284
32	26-29	38-48	57-65	62-79	72-118	81-130	132-202	126-291
33	28-29	37-49	65-66	64-81	92-121	78-133	193-207	220-298
34	27-30	44-50	57-68	76-83	80-124	111-136	156-213	135-305
35	29-31	47-51	58-69	68-85	106-127	84-139	144-218	126-312
36	30-31	46-52	64-71	64-87	105-130	110-142	185-223	244-319
37	29-32	48-54	66-72	72-89	121-132	120-145	208-228	162-326
38	28-33	36-55	56-74	78-91	129-135	105-149	193-233	144-333
39	33	46-56	65-75	76-93	117-138	84-152	160-239	271-340
40	32-34	54-57	75-77	65-94	100-141	90-155	162-244	244-346

$g\backslash q$	2	3	4	5	8	9	16	27
41	33-35	50-58	65-78	80-96	112-144	84-158	216-249	153-353
42	33-35	39-59	66-80	60-98	129-147	90-161	209-254	280-360
43	33-36	55-60	72-81	84-100	100-150	120-164	226-259	196-367
44	33-37	42-61	68-83	60-102	129-153	90-167	162-264	153-374
45	32-37	48-62	80-84	88-104	144-156	112-170	242-268	171-381
46	34-38	55-63	81-86	75-106	129-158	138-173	243-273	162-388
47	36-38	47-65	73-87	92-108	120-161	154-177	176-277	174-395
48	34-39	55-66	77-89	82-110	126-164	163-180	184-282	325-402
49	36-40	63-67	81-90	96-111	130-167	168-183	192-286	268-409
50	40	56-68	91-92	70-113	130-170	182-186	225-291	180-416

REFERENCES

[1] R. Auer, Ray class fields of global function fields with many rational places, preprint, 1998.

[2] A.T. Clayman, K.M. Lawrence, G.L. Mullen, H. Niederreiter, and N.J.A. Sloane, Updated tables of parameters of (t, m, s)-nets, *J. Combinatorial Designs*, to appear.

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

[4] A. Garcia and H. Stichtenoth, Algebraic function fields over finite fields with many rational places, *IEEE Trans. Inform. Theory* 41, 1548–1563 (1995).

[5] K. Lauter, Ray class field constructions of curves over finite fields with many rational points, *Algorithmic Number Theory* (H. Cohen, ed.), Lecture Notes in Computer Science, Vol. 1122, pp. 187–195, Springer, Berlin, 1996.

[6] K.M. Lawrence, A combinatorial characterization of (t, m, s)-nets in base b, *J. Combinatorial Designs* 4, 275–293 (1996).

[7] W.J. Martin and D.R. Stinson, A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets, preprint, 1997.

[8] —, —, Association schemes for ordered orthogonal arrays and (t, m, s)-nets, preprint, 1997.

[9] G.L. Mullen, A. Mahalanabis, and H. Niederreiter, Tables of (t, m, s)-net and (t, s)-sequence parameters, *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing* (H. Niederreiter and P.J.-S. Shiue, eds.), Lecture Notes in Statistics, Vol. 106, pp. 58–86, Springer, New York, 1995.

[10] G.L. Mullen and W.C. Schmid, An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes, *J. Combinatorial Theory Ser. A* 76, 164–174 (1996).

[11] G.L. Mullen and G. Whittle, Point sets with uniformity properties and orthogonal hypercubes, *Monatsh. Math.* 113, 265–273 (1992).

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

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

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

[15] —, Orthogonal arrays and other combinatorial aspects in the theory of uniform point distributions in unit cubes, *Discrete Math.* 106/107, 361–367 (1992).

[16] —, Pseudorandom numbers and quasirandom points, *Z. angew. Math. Mech.* 73, T648–T652 (1993).

[17] —, Factorization of polynomials and some linear-algebra problems over finite fields, *Linear Algebra Appl.* 192, 301–328 (1993).

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

[19] —, —, Explicit global function fields over the binary field with many rational places, *Acta Arith.* 75, 383–396 (1996).

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

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

[22] —, —, Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places, *Acta Arith.* 79, 59–76 (1997).

[23] —, —, Drinfeld modules of rank 1 and algebraic curves with many rational points. II, *Acta Arith.* 81, 81–100 (1997).

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

[25] —, —, The algebraic-geometry approach to low-discrepancy sequences, *Monte Carlo and Quasi-Monte Carlo Methods 1996* (H. Niederreiter *et al.*, eds.), Lecture Notes in Statistics, Vol. 127, pp. 139–160, Springer, New York, 1998.

[26] —, —, Algebraic curves over finite fields with many rational points, *Number Theory* (K. Győry *et al.*, eds.), pp. 423–443, de Gruyter, Berlin, 1998.

[27] —, —, Global function fields with many rational places over the ternary field, *Acta Arith.* 83, 65–86 (1998).

[28] —, —, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound, *Math. Nachr.*, to appear.

[29] —, —, Algebraic curves with many rational points over finite fields of characteristic 2, *Proc. Number Theory Conf.* (Zakopane, 1997), de Gruyter, Berlin, to appear.

[30] —, —, Global function fields with many rational places and their applications, *Proc. Finite Fields Conf.* (Waterloo, 1997), Contemporary Math., American Math. Soc., Providence, to appear.

[31] —, —, A general method of constructing global function fields with many rational places, *Algorithmic Number Theory* (J.P. Buhler, ed.), Lecture Notes in Computer Science, Vol. 1423, pp. 555–566, Springer, Berlin, 1998.

[32] —, —, Nets, (t, s)-sequences, and algebraic geometry, *Pseudo- and Quasi-Random Point Sets* (P. Hellekalek and G. Larcher, eds.), Lecture Notes in Statistics, Springer, New York, to appear.

[33] —, —, Curve sequences with asymptotically many rational points, preprint, 1997.
[34] —, —, A counterexample to Perret's conjecture on infinite class field towers for global function fields, preprint, 1998.
[35] —, —, Global function fields with many rational places over the quinary field. II, *Acta Arith.*, to appear.
[36] M. Perret, Tours ramifiées infinies de corps de classes, *J. Number Theory* 38, 300–322 (1991).
[37] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris Sér. I Math.* 296, 397–402 (1983).
[38] I.M. Sobol', The distribution of points in a cube and the approximate evaluation of integrals (Russian), *Zh. Vychisl. Mat. i Mat. Fiz.* 7, 784–802 (1967).
[39] S. Tezuka, *Uniform Random Numbers: Theory and Practice*, Kluwer, Boston, 1995.
[40] M.A. Tsfasman, S.G. Vlădut, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* 109, 21–28 (1982).
[41] G. van der Geer and M. van der Vlugt, Curves over finite fields of characteristic 2 with many rational points, *C.R. Acad. Sci. Paris Sér. I Math.* 317, 593–597 (1993).
[42] —, —, How to construct curves over finite fields with many points, *Arithmetic Geometry* (F. Catanese, ed.), pp. 169–189, Cambridge Univ. Press, Cambridge, 1997.
[43] —, —, Tables of curves with many points, preprint, 1998.
[44] C.P. Xing and H. Niederreiter, A construction of low-discrepancy sequences using global function fields, *Acta Arith.* 73, 87–102 (1995).
[45] —, —, Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels, *C.R. Acad. Sci. Paris Sér. I Math.* 322, 651–654 (1996).
[46] —, —, Drinfeld modules of rank 1 and algebraic curves with many rational points, *Monatsh. Math.*, to appear.

Harald Niederreiter
Institute of Information Processing
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Vienna
Austria
E-mail: niederreiter@oeaw.ac.at