

---

---

# 1 (t,m,s)-Nets

---

---

WILLIAM J. MARTIN

## 1.1 Definitions and Motivation

- 1.1** Let  $[0, 1)^s$  be the half-open unit cube of dimension  $s$  and suppose numerical computation is to be done in base  $b \geq 2$ . An *elementary interval in base  $b$*  in  $[0, 1)^s$  is a Euclidean set of the form
- $$E = \prod_{i=1}^s \left[ \frac{a_i}{b^{d_i}}, \frac{a_i+1}{b^{d_i}} \right)$$
- where each integer  $d_i \geq 0$  and for each  $i$ , the integer  $a_i$  satisfies  $0 \leq a_i < b^{d_i}$ . Clearly  $\text{Vol}(E) = b^{-\sum d_i}$ .
- 1.2 Example** The set  $E = [0, 1/2) \times [9/16, 10/16) \times [0, 1)$ , contained in the unit 3-cube, is an elementary interval in base two having volume  $2^{-5}$ .
- 1.3** Let  $s \geq 1$ ,  $b \geq 2$  and  $m \geq t \geq 0$  be integers. A *(t, m, s)-net in base b* is a multiset  $\mathcal{N}$  of  $b^m$  points in  $[0, 1)^s$  with the property that every elementary interval in base  $b$  of volume  $b^{t-m}$  contains precisely  $b^t$  points from  $\mathcal{N}$ .
- 1.4 Remark** For a collection  $\mathcal{N}$  of  $N$  points in the unit  $s$ -cube, the expected number of points in an interval  $E = \prod_i [a_i, b_i)$  of volume  $\epsilon$  is  $\epsilon N$ .
- 1.5** The *local discrepancy* of a particular interval  $E$  is the absolute value of  $|\mathcal{N} \cap E|/N - \text{Vol}(E)$ . The *star-discrepancy* of a set  $\mathcal{N}$  is then  $D_N^*(\mathcal{N}) = \sup_E \left| \frac{|\mathcal{N} \cap E|}{N} - \text{Vol}(E) \right|$  where the supremum is over all intervals  $E = \prod_i [0, a_i)$  contained in  $[0, 1)^s$ .
- 1.6 Theorem** Koksma-Hlawka Inequality: If  $f$  is a function of  $s$  variables with bounded variation  $V(f) < +\infty$ , then  $\left| \int_{[0,1]^s} f(u) du - \frac{1}{N} \sum_{x \in \mathcal{N}} f(x) \right| \leq V(f) D_N^*(\mathcal{N})$ .
- 1.7 Theorem** ([6, 7]) A  $(t, m, s)$ -net in base  $b = 2$  satisfies  $D_N^*(\mathcal{N}) \leq \frac{2^t}{N} \sum_{i=0}^{s-1} \binom{m-t}{i}$  and a  $(t, m, s)$ -net in base  $b \geq 3$  satisfies  $D_N^*(\mathcal{N}) \leq \frac{b^t}{N} \sum_{i=0}^{s-1} \binom{s-1}{i} \binom{m-t}{i} \lfloor \frac{b}{2} \rfloor^i$ .
- 1.8 Remark** From Theorems 1.6 and 1.7, it is evident that  $(t, m, s)$ -nets yield Quasi-Monte Carlo methods for numerical integration (deterministic surrogates for Monte-Carlo methods). These are important in contexts where random number generation becomes computationally expensive, but also note that, as the net gets larger, the error bound scales as  $O(N^{-1})$  in comparison to  $O(N^{-\frac{1}{2}})$  for Monte Carlo methods.
- 1.9 Remark** While we have focused on the application to numerical integration,  $(t, m, s)$ -nets are also useful for simulations and pseudorandom number generation.
- 1.10 Remark** For applications, it is important to have a nested sequence of  $(t_i, m_i, s)$ -nets (with  $m_i$  going to infinity) in the same dimension  $s$  and with all  $t_i$  bounded above by a constant  $t$ . This allows the practitioner to improve estimates on an integral without losing the benefit of preliminary computations. Such a sequence of nets can be constructed via  $(t, s)$ -sequences.

- 1.11** Let  $s \geq 1$ ,  $b \geq 2$  and  $t \geq 0$  be integers. A  $(t, s)$ -sequence in base  $b$  is an infinite sequence  $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \dots$  of points in  $[0, 1]^s$  with the property that, for every  $m > t$  and every  $k \geq 0$ , the set

$$\mathcal{N} = \{[\mathbf{x}_i] : kb^m \leq i < (k+1)b^m\}$$

is a  $(t, m, s)$ -net in base  $b$ . Here,  $[\mathbf{x}]$  represents the point obtained by truncating each coordinate of  $\mathbf{x}$  to  $m$  digits of accuracy in a fixed prescribed  $b$ -adic expansion of it.

- 1.12 Example** van der Corput sequence: Fix a base  $b \geq 2$  and, for an integer  $n \geq 0$ , write  $n = \sum_{j=0}^{\infty} a_j b^j$  with  $0 \leq a_j < b$  and take the rational number  $x_n = \sum_{j=0}^{\infty} a_j b^{-j-1}$ . Then  $x_0, x_1, x_2, \dots$  is a  $(0, 1)$ -sequence in base  $b$ .

- 1.13 Remarks** ([7, Ch. 3]) In the previous example, write  $\phi_b(n) = \sum_{j=0}^{\infty} a_j b^{-j-1}$ . The *Halton sequence* is then  $\mathbf{x}_n = (\phi_{b_1}(n), \dots, \phi_{b_s}(n))$ ,  $n \geq 0$  where  $b_1, b_2, \dots, b_s$  are integers greater than one and the *Hammersley point set* is the set  $\mathbf{x}_0, \dots, \mathbf{x}_{N-1}$  given by  $\mathbf{x}_n = (\frac{n}{N}, \phi_{b_1}(n), \dots, \phi_{b_{s-1}}(n))$  where the bases  $b_1, \dots, b_{s-1} \geq 2$  are arbitrary and discrepancy bounds are strongest when the  $b_i$  are relatively prime. Note that these popular low-discrepancy point sets are not  $(t, s)$ -sequences.

If we order the primitive polynomials over  $GF(2)$  by degree  $p_1(x), p_2(x), \dots$ , then the *Sobol' sequence* yields a  $(t_s, s)$ -sequence in base  $b = 2$  for each  $s$  where  $t_s = \sum_{i=1}^{s-1} (\deg p_i - 1)$ . Unrelated to this, the *Niederreiter sequence* in any prime power base  $q$  yields a  $(T_q(s), s)$ -sequence where  $T_q(s) = \sum_{i=1}^s (\deg p_i - 1)$  for any collection of pairwise relatively prime polynomials  $p_1(x), p_2(x), \dots$  of positive degree over  $GF(q)$  [7, Sec. 4.5] so that, in particular,  $T_2(s) < t_s$  for  $s \geq 8$  if polynomials of lowest possible degree are chosen for the construction of the Niederreiter sequence.

- 1.14 Theorem** ([6, Lem. 5.15]) If a  $(t, s)$ -sequence in base  $b$  exists, then there exist  $(t, m, s+1)$ -nets in base  $b$  for all  $m \geq t$ .
- 1.15 Remark** The finite problem of deciding whether a  $(t, m, s)$ -net exists can yield not only non-existence results for  $(t, s)$ -sequences but can also tell us what to aim for and how we might find it.
- 1.16 Remark** For nets, the goal is to construct  $(t, m, s)$ -nets for any dimension  $s$  and with any size  $b^m$  having *quality parameter*  $t$  as close to zero as possible. Among two nets with the same number of points, one prefers the one which evenly samples more elementary intervals. At the trivial end, when  $t = m$ , no structure is imposed and any multiset of  $b^m$  points in  $[0, 1]^s$  is an  $(m, m, s)$ -net. When  $t = m - 1$ , the requirement is simply that the projections of the points  $x \in \mathcal{N}$  onto any coordinate are uniformly distributed among the intervals  $[a/b, (a+1)/b)$  ( $0 \leq a < b$ ). Hence the cases of interest are when  $m \geq t + 2$ . At the other end of the spectrum, it is known that, for  $m > 1$  a  $(0, m, s)$ -net in base  $b$  can exist only in dimensions  $s \leq b + 1$  since a  $(0, 2, s)$ -net in base  $b$  is equivalent to  $s - 2$  MOLS of order  $b$  (see Theorem 1.18 below).

## 1.2 Constructions and Propagation Rules

- 1.17 Remark** Theorem 1.18 gives a connection between orthogonal arrays and certain  $(t, m, s)$ -nets. See also Theorems 1.32 and 1.21 as well as Remark 1.28.
- 1.18 Theorem** [6] A  $(0, 2, s)$ -net in base  $b$  exists if and only if there exist  $s - 2$  MOLS of order  $b$ . (More generally, a  $(t, t + 2, s)$ -net in base  $b$  is equivalent to an  $OA_{b^t}(2, s, b)$ .)
- 1.19 Construction** Suppose we have  $s - 2$  mutually orthogonal latin squares  $L_h = [\ell_{ij}^{(h)}]$  ( $1 \leq h \leq s - 2$ ) defined over the digits  $0, 1, \dots, b - 1$  and with rows and columns indexed by  $0, 1, \dots, b - 1$ . Let  $\sigma$  be any function from  $\{1, \dots, s - 2\}$  to itself satisfying

$\sigma i \neq i$  for all  $i$ . The  $b^2$  points  $\mathbf{x}_n$  ( $0 \leq n < b^2$ ) in  $[0, 1]^s$  are defined by  $\mathbf{x}_{ib+j} = \frac{1}{b^2} (b\ell_{ij}^{(1)} + \ell_{ij}^{(\sigma 1)}, \dots, b\ell_{ij}^{(s-2)} + \ell_{ij}^{(\sigma(s-2))}, bi + \ell_{ij}^{(1)}, bj + \ell_{ij}^{(1)})$ .

**1.20 Example** To see how 2 MOLS(3) are used to construct the (0, 2, 4)-net in base 3

$$\mathcal{N} = \{(0, 0, 0, 0), (\frac{4}{9}, \frac{4}{9}, \frac{1}{9}, \frac{4}{9}), (\frac{8}{9}, \frac{8}{9}, \frac{2}{9}, \frac{8}{9}), (\frac{5}{9}, \frac{7}{9}, \frac{4}{9}, \frac{1}{9}), (\frac{2}{3}, \frac{2}{9}, \frac{5}{9}, \frac{5}{9}), (\frac{1}{9}, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}), (\frac{7}{9}, \frac{5}{9}, \frac{8}{9}, \frac{2}{9}), (\frac{2}{9}, \frac{2}{3}, \frac{2}{3}, \frac{1}{3}), (\frac{1}{3}, \frac{1}{9}, \frac{7}{9}, \frac{7}{9})\}$$

apply the construction to the 2 MOLS(3) on the left below, with rows and columns numbered 0,1,2 and with  $\sigma$  swapping 1 and 2.

0	1	2
1	2	0
2	0	1

0	1	2
2	0	1
1	2	0

.00	.00	.00	.00
.11	.11	.01	.11
.22	.22	.02	.22
.12	.21	.11	.01
.20	.02	.12	.12
.01	.10	.10	.20
.21	.12	.22	.02
.02	.20	.20	.10
.10	.01	.21	.21

**1.21 Theorem** ([1]) If there is a linear  $q$ -ary  $[s, s-m, k+1]$  code and  $\text{GR}(2k-2\ell, s-1, \ell, b) < b^{m-\ell+1}$  for all  $2 \leq \ell < k$ , then there exists a  $(t, m, s)$ -net in base  $b$  where  $t = m - k$ .

**1.22 Remark** The quantity  $\text{GR}(2r, s, \ell, b)$  is defined below, but is also the size of a ball of radius  $r$  in so-called “NRT space” [1] and is given by the sum of the coefficients of  $x^0, x^1, \dots, x^r$  in the expansion of  $[1 + (b-1)x + (b^2-b)x^2 + \dots + (b^\ell - b^{\ell-1})x^\ell]^s$ .

**1.23 Remark** The most powerful known constructions of  $(t, s)$ -sequences are those of Niederreiter and Xing (see [9]), based on global function fields with many places. Rather than delve into algebraic geometry here, we exhibit the flavor of the constructions next with an elementary  $(t, m, s)$ -net analog of Reed-Solomon codes.

**1.24 Example** (Rosenbloom/Tsfasman) Let  $q$  be a prime power,  $S = \{a_1, \dots, a_s\} \subseteq GF(q)$  and  $1 \leq m \leq q$ . Fix any bijection  $\beta : GF(q) \rightarrow \{0, \dots, q-1\}$  and write  $((c)) = \beta(c)$  for  $c \in GF(q)$ . The set  $\mathcal{N}$  contains a point  $\mathbf{x}_f$  for each polynomial  $f(t) \in GF(q)[t]$  of degree less than  $m$ , where the  $i^{\text{th}}$  coordinate of  $\mathbf{x}_f$  is

$$(\mathbf{x}_f)_i = \sum_{j=0}^{m-1} ((f^{(j)}(a_i)))q^{-1-j},$$

where  $f^{(j)}(a_i)$  denotes the evaluation of the  $j^{\text{th}}$  derivative of  $f$  at the point  $a_i$ . Since a non-zero polynomial of degree  $n$  has at most  $n$  roots, counting multiplicities, this is a  $(0, m, s)$ -net in base  $q$ . One may obtain  $s = q + 1$  by extending the coordinates to the projective line  $PG(1, q)$ . As in coding theory, one then replaces  $S$  with the set of points on some algebraic curve to obtain  $(t, m, s)$ -net analogs of Goppa codes, etc.

**1.25 Theorem** A representative sample of the dozens of propagation rules known. (See [9] and references therein).

1. **projection:** Every  $(t, m, s)$ -net in base  $b$  yields a  $(t', m, s')$ -net in base  $b$  for every  $t \leq t' \leq m$  and every  $1 \leq s' \leq s$
2. **subnets:** Every  $(t, m, s)$ -net in base  $b$  yields a  $(t, m', s)$ -net in base  $b$  for each  $t \leq m' \leq m$
3. **base change:** Every  $(t, m, s)$ -net in base  $b^r$  with  $r \geq 1$  yields a  $(t', rm, s)$ -net in base  $b$  with  $t' = \min\{rt + (r-1)(s-1), rm\}$
4. **product:** If a  $(t_1, m_1, s_1)$ -net exists in base  $b$  and a  $(t_2, m_2, s_2)$ -net exists in base  $b$  with  $s_1 \leq s_2$ , then a  $(t, m_1+m_2, s_1+s_2)$ -net exists for  $t = \max(m_1+t_2, m_2+t_1)$ . (See also the  $(u, u+v)$ -construction in [1].)

### 1.3 Ordered Orthogonal Arrays

- 1.26** In an array with  $s\ell$  columns, labeled  $\{(i, j) : 1 \leq i \leq s, 1 \leq j \leq \ell\}$ , a set  $T$  of columns is *left-justified* if  $(i, j) \in T$  with  $j > 1$  implies  $(i, j - 1) \in T$ . An *ordered orthogonal array*  $\text{OOA}_\lambda(t, s, \ell, v)$  is a  $\lambda v^t \times s\ell$  array  $A = (a_{r,(i,j)})$  with columns indexed by ordered pairs  $(i, j)$  as above and with elements from an alphabet  $F$  of size  $v$ , with the property that every left-justified set  $T$  of  $t$  columns has the *OA property*: in the subarray obtained by restricting to columns lying in  $T$ , each  $t$ -tuple over  $F$  occurs exactly  $\lambda$  times as a row.

This example **1.27** **Example** An  $\text{OOA}_2(3, 3, 3, 2)$  and an  $\text{OOA}_1(2, 3, 2, 4)$

takes up  
half a page.  
Kill it  
if necessary.

0	0	0	0	0	0	0	0	0
0	0	1	1	0	1	1	0	1
0	1	0	1	1	0	1	0	0
0	1	1	0	1	1	0	0	1
1	0	0	0	1	0	1	0	0
1	0	1	1	1	1	0	0	1
1	1	0	1	0	0	0	0	0
1	1	1	0	0	1	1	0	1
0	0	0	1	1	0	0	1	0
0	0	1	0	1	1	1	1	1
0	1	0	0	0	0	1	1	0
0	1	1	1	0	1	0	1	1
1	0	0	1	0	0	1	1	0
1	0	1	0	0	1	0	1	1
1	1	0	0	1	0	0	1	0
1	1	1	1	1	1	1	1	1

0	0	0	0	0	0
0	1	2	1	3	1
0	2	3	2	1	2
0	3	1	3	2	3
1	0	1	0	1	0
1	1	3	1	2	1
1	2	2	2	0	2
1	3	0	3	3	3
2	0	2	0	2	0
2	1	0	1	1	1
2	2	1	2	3	2
2	3	3	3	0	3
3	0	3	0	3	0
3	1	1	1	0	1
3	2	0	2	2	2
3	3	2	3	1	3

In the second example, with natural ordering of the columns, the left-justified sets of two columns are  $\{1, 2\}, \{3, 4\}, \{5, 6\}, \{1, 3\}, \{1, 5\}, \{3, 5\}$  which we have labeled  $\{(1, 1), (1, 2)\}, \{(2, 1), (2, 2)\}, \{(3, 1), (3, 2)\}, \{(1, 1), (2, 1)\}, \{(1, 1), (3, 1)\}, \{(2, 1), (3, 1)\}$  respectively.

- 1.28 Remark** For any  $1 \leq \ell' < \ell$ , we may delete columns  $(i, j)$  with  $j > \ell'$  from any  $\text{OOA}_\lambda(t, s, \ell, v)$  to obtain a  $\text{OOA}_\lambda(t, s, \ell', v)$ . In particular, with  $\ell' = 1$ , this yields an  $\text{OA}_\lambda(t, s, v)$ .

- 1.29** If the alphabet  $F$  is a field and the rows of the OOA form a subspace of  $F^{s\ell}$ , then this is a *linear OOA*. These correspond to *digital (t, m, s)-nets*.

- 1.30 Remark** All statements in Theorem 1.25 remain valid for digital nets.

- 1.31 Remark** The connection to combinatorial designs is based on the following important theorem.

- 1.32 Theorem** (Lawrence, Mullen/Schmid [2, 4]) There exists a  $(t, m, s)$ -net in base  $b$  if and only if there exists an  $\text{OOA}_{b^t}(m - t, s, m - t, b)$ .

- 1.33 Example** To illustrate the theorem, we exhibit an  $\text{OOA}_1(2, 2, 2, 2)$  and the corresponding  $(0, 2, 2)$ -net  $\mathcal{N} = \{(0, 0), (\frac{1}{4}, \frac{3}{4}), (\frac{1}{2}, \frac{1}{2}), (\frac{3}{4}, \frac{1}{4})\}$  in base  $b = 2$ :

[[Picture of (0,2,2)-net in base 2 goes here.]]

In the figure, the shading indicates the partition of the OOA determined by values in

columns (1, 1) and (2, 1) and the corresponding partition of the cube into intervals of size  $b^{-1} \times b^{-1}$ .

### 1.4 Bounds on OOAs and Nets

**1.34 Theorem Orthogonal Array Bound:** (Clayman, et al.) If a  $(t, m, s)$ -net exists in base  $b$ , then  $s \leq \min_{t+2 \leq h \leq m} f(b^h, b, h-t)$  where  $f(N, b, \tau)$  is the maximum value of  $k$  for which an  $OA(\tau, k, b)$  exists with  $N$  columns.

**1.35 Theorem Generalized Rao Bound:** (Martin/Stinson) If there exists a  $(t, m, s)$ -net in base  $b$ , then  $b^n \geq GR(n-t, s, n-t, b)$  for all integers  $n$  such that  $t+2 \leq n \leq m$  where

$$GR(k, s, \ell, b) = \begin{cases} 1 + \sum_{h=1}^{k/2} \sum_{w=1}^h \binom{s}{w} N_{h,w,\ell} (b-1)^w b^{h-w} & (k \text{ even}); \\ GR(k-1, s, \ell, b) + \sum_{w=1}^{(k+1)/2} \binom{s-1}{w-1} N_{\frac{k+1}{2}, w, \ell} (b-1)^w b^{\frac{k+1}{2}-w} & (k \text{ odd}) \end{cases}$$

and

$$N_{h,w,\ell} = \sum_{j=0}^{\lfloor \frac{h-w}{\ell} \rfloor} (-1)^j \binom{w}{j} \binom{h-\ell j-1}{w-1}.$$

**1.36 Theorem Dual Plotkin Bound:** (Martin/Visentin) For a  $(t, m, s)$ -net in base  $b$ , let  $\ell = 1 + \lfloor \frac{m-t}{s} \rfloor$ , then  $t \geq m + 1 - \frac{s}{1-b^{m-s\ell}} \left( \ell - \frac{1}{b} - \frac{1}{b^2} - \dots - \frac{1}{b^\ell} \right)$ .

**1.37 Remark** The above bounds are mostly special cases of the linear programming bound [3].

### 1.5 See Also

§II.??	Orthogonal arrays of higher strength.
§V.??	Linear codes.
§V. ??	Association schemes.
[10]	On-line tool at the University of Salzburg giving tables with latest constructions and bounds: <a href="http://mint.sbg.ac.at/">http://mint.sbg.ac.at/</a>
[8]	Applications of $(t, m, s)$ -nets.
[5]	TOMS647, a library of FORTRAN90 routines, using single precision arithmetic, which implements the Faure, Halton, and Sobol' quasirandom sequences.
[9, Sec. 10]	Randomized (or "scrambled") nets which allow for error analysis.

[1] J. Bierbrauer, Y. Edel and W. Ch. Schmid, Coding-theoretic constructions for  $(t, m, s)$ -nets and ordered orthogonal arrays, *J. Combin. Des.* 10 (2002), 403–418.  
 [2] K.M. Lawrence, A combinatorial characterization of  $(t, m, s)$ -nets in base  $b$ , *J. Combin. Designs* 4 (1996), 275–293.  
 [3] W.J. Martin and D.R. Stinson, Association schemes for ordered orthogonal arrays and  $(T, M, S)$ -nets, *Canad. J. Math.* 51 (1999), 326–246.  
 [4] G.L. Mullen and W.Ch. Schmid, An equivalence between  $(T, M, S)$ -nets and strongly orthogonal hypercubes, *J. Combin. Th. Ser. A* 76 (1996), 164–174.  
 [5] J. Dongarra and E. Grosse (eds.) The NetLib Repository at UTK and ORNL. <http://www.netlib.org/>  
 [6] H. Niederreiter, Point sets and sequences with small discrepancy, *Monats. Math.* 104 (1987), 273-337.

- 
- [7] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods. SIAM, Philadelphia, 1992.
  - [8] H. Niederreiter, High-dimensional numerical integration, pp. 337–351 in: Applied Mathematics Entering the 21st Century: Invited Talks from the ICIAM 2003 Congress (J.M. Hill, R. Moore, eds.), SIAM, Philadelphia, 2004.
  - [9] H. Niederreiter, Constructions of  $(t, m, s)$ -nets and  $(t, s)$ -sequences, *Finite Fields Appl.* 11 (2005), 578–600.
  - [10] R. Schürer and W.Ch. Schmid, MinT: a database for optimal net parameters, To appear, in: Monte Carlo and Quasi-Monte Carlo Methods 2004 (H. Niederreiter, D. Talay, eds.), Springer-Verlag, Berlin, 2006.