MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 225–234

GOOD PARAMETERS FOR A CLASS OF NODE SETS IN QUASI-MONTE CARLO INTEGRATION

TOM HANSEN, GARY L. MULLEN, AND HARALD NIEDERREITER

Dedicated to the memory of D. H. Lehmer

ABSTRACT. For $2 \leq s \leq 12$ we determine good parameters in a general construction of node sets for s-dimensional quasi-Monte Carlo integration recently introduced by the third author. Some of the parameters represent optimal choices in this construction and lead to improvements on node sets obtained by earlier techniques.

1. INTRODUCTION

We consider the problem of multidimensional numerical integration, with the closed s-dimensional unit cube $\mathbf{I}^s = [0, 1]^s$, $s \geq 2$, as a normalized integration domain. In the standard *Monte Carlo method* the integration rule

$$\int_{\mathbf{I}^s} f(\mathbf{t})d\mathbf{t} \approx \frac{1}{N}\sum_{n=0}^{N-1} f(\mathbf{x}_n) \tag{1}$$

is used, where the nodes $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1} \in \mathbf{I}^s$ are N independent random samples from the uniform distribution on $\mathbf{I}^s$. In practical implementations of this method, one actually works with nodes derived from uniform pseudorandom numbers, such as Lehmer's linear congruential pseudorandom numbers [5]. Concretely, if $x_0, x_1, \dots$ is a sequence of uniform pseudorandom numbers in $[0, 1]$, then one employs the nodes

$$\mathbf{x}_n = (x_n, x_{n+1}, \dots, x_{n+s-1}) \in \mathbf{I}^s \quad \text{for } 0 \leq n \leq N-1.$$

The integration error incurred in (1) with these nodes was analyzed by Niederreiter [9] for the cases of Lehmer pseudorandom numbers and shift-register pseudorandom numbers.

It is well known that under mild regularity conditions on the integrand f we may improve on Monte Carlo integration by using the approximation (1) with suitably chosen deterministic nodes. This yields the *quasi-Monte Carlo method* for numerical integration, which is surveyed, e.g., in Hua and Wang [3] and Niederreiter [8], [14]. To guarantee small integration errors, the nodes

Received by the editor July 27, 1992.

1991 *Mathematics Subject Classification*. Primary 11K45, 65D32; Secondary 11K38, 11Y99.

The first two authors would like to thank the NSA for partial support under the second author's grant agreement # MDA904-87-H-2023.

$\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1} \in I^s = [0, 1)^s$ have to be selected in such a way that their *star discrepancy* D_N^* is small. Here

$$D_N^* = \sup_J |E_N(J) - \mathrm{Vol}\,(J)|\,,$$

where, for an arbitrary subinterval J of I^s, $E_N(J)$ is N^{-1} times the number of $0 \le n \le N-1$ with $\mathbf{x}_n \in J$ and $\mathrm{Vol}\,(J)$ denotes the s-dimensional volume of J, and where the supremum is extended over all J of the form $J = \prod_{i=1}^s [0, t_i)$ with $0 < t_i \le 1$ for $1 \le i \le s$.

Currently, the most effective constructions of node sets for quasi-Monte Carlo integration are based on the theory of nets. We fix the dimension $s \ge 2$ and an integer $b \ge 2$. By an *elementary interval in base* b we mean a 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 $d_i \ge 0$ and $0 \le a_i < b^{d_i}$ for $1 \le i \le s$.

Definition 1. Let $0 \le t \le m$ be integers and put $N = b^m$. Then the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1} \in I^s$ form a (t, m, s)-*net in base* b if every elementary interval J in base b with $\mathrm{Vol}\,(J) = b^{t-m}$ contains exactly b^t points $\mathbf{x}_n$, i.e., $E_N(J) = \mathrm{Vol}\,(J)$.

The general theory of nets was developed in Niederreiter [11]; see also [14, Chapter 4] for an expository account. For the special case $b = 2$ on which we will concentrate, some results were obtained earlier by Sobol′ [17]. The case $b = 2$ offers the advantage of easier implementation of the known constructions of nets, and recent tests suggest that nets in base 2 tend to perform better in numerical integration than nets in larger bases [2]. The following discrepancy bound for nets in base 2 is a special case of results in [11, §3].

Theorem A. *The star discrepancy* D_N^* *of a* (t, m, s)*-net in base* 2 *satisfies*

$$D_N^* \le B_s 2^t N^{-1} (\log N)^{s-1} + O(2^t N^{-1} (\log N)^{s-2}),$$

where the implied constant in the Landau symbol depends only on s, *and where* $B_s = 1/(\log 4)^{s-1}$ *for* $2 \le s \le 4$ *and*

$$B_s = \frac{1}{(s-1)!(\log 2)^{s-1}} \quad \textit{for } s \ge 5.$$

It is clear from this discrepancy bound, and also from Definition 1, that the value of t should be as small as possible. Prior to the present work, the least value of t for each dimension $s \ge 2$ was obtained by combining the construction of a special class of sequences in Niederreiter [12] with [11, Lemma 5.15]. If $T_2(s)$ is defined by [12, equation (10)], and if we put $V_s = T_2(s-1)$ for $s \ge 2$, then this yields, for every $s \ge 2$ and $m \ge V_s$, a (V_s, m, s)-net in base 2. For the range of dimensions discussed in this paper, we obtain the values of V_s in Table 1 from [12, Table II].

TABLE 1. Values of V_s for $2 \le s \le 12$

s	2	3	4	5	6	7	8	9	10	11	12
V_s	0	0	1	3	5	8	11	14	18	22	26

Furthermore, there are known lower bounds on t that are obtained from combinatorial constraints on the existence of nets; see Mullen and Whittle [7] and Niederreiter [15]. For the case $b = 2$, a result in [7] yields the following: for $m \geq t+2$ a (t, m, s)-net in base 2 can only exist if $s \leq 2^{t+2} - 1$. This implies the lower bound

$$t \geq \lceil \log_2(s+1) \rceil - 2 \tag{2}$$

provided that $m \geq t+2$, where $\log_2$ is the logarithm to the base 2 and $\lceil x \rceil$ denotes the smallest integer $\geq x$. Except for some small dimensions s, there is a considerable gap between the lower bound in (2) and the values of V_s in Table 1.

It is one of the aims of the present paper to reduce this gap. This is achieved by considering a construction of nets recently introduced in Niederreiter [13] and by searching for optimal, or nearly optimal, parameters in this construction. A detailed description of these nets and their properties is provided in §2. The search procedure for good parameters is described in §3 and the computational results are reported in §4.

2. Description of the node sets

We describe node sets for the quasi-Monte Carlo integration (1) which form (t, m, s)-nets in base 2 and were introduced by Niederreiter [13]. Further results on these nets can be found in [14, Chapter 4]. It is convenient to use an equivalent, but simpler, description of these nets given in [16].

Let $F_2 = \{0, 1\}$ be the field with two elements and let $F_2((x^{-1}))$ be the field of formal Laurent series over F_2 in the variable x^{-1}. Thus, the elements of $F_2((x^{-1}))$ have the form $\sum_{k=w}^{\infty} u_k x^{-k}$, where w is an arbitrary integer and all $u_k \in F_2$. Note that $F_2((x^{-1}))$ contains the rational function field $F_2(x)$ as a subfield. For an integer $m \geqslant 1$ let ϕ_m be the map from $F_2((x^{-1}))$ to the interval $[0, 1)$ defined by

$$\phi_m\left(\sum_{k=w}^{\infty} u_k x^{-k}\right) = \sum_{k=\max(1, w)}^{m} u_k 2^{-k}. \tag{3}$$

For a given dimension $s \geq 2$ we choose $f \in F_2[x]$ with $\deg(f) = m$ and $g_1, \dots, g_s \in F_2[x]$. For $n = 0, 1, \dots, 2^m - 1$ let

$$n = \sum_{r=0}^{m-1} a_r(n) 2^r,$$

with all $a_r(n) \in F_2$, be the binary expansion of n. With each such n we can then associate the polynomial

$$n(x) = \sum_{r=0}^{m-1} a_r(n) x^r \in F_2[x].$$

Then we define the node set consisting of the 2^m points

$$\mathbf{x}_n = \left(\phi_m\left(\frac{n(x)g_1(x)}{f(x)}\right), \dots, \phi_m\left(\frac{n(x)g_s(x)}{f(x)}\right)\right) \in I^s \tag{4}$$

$$\text{for } n = 0, 1, \dots, 2^m - 1.$$

We write $\mathbf{g} = (g_1, \dots, g_s) \in F_2[x]^s$ for the s-tuple of polynomials $g_1, \dots, g_s$ and we use the convention $\deg(0) = -1$. The following quantity plays a crucial role.

Definition 2. The *figure of merit* $\rho(\mathbf{g}, f)$ is given by

$$\rho(\mathbf{g}, f) = s - 1 + \min \sum_{i=1}^{s} \deg(h_i),$$

where the minimum is extended over all nonzero s-tuples $(h_1, \dots, h_s) \in F_2[x]^s$ for which $\deg(h_i) < m$ for $1 \le i \le s$ and f divides $\sum_{i=1}^{s} g_i h_i$.

We always have $0 \le \rho(\mathbf{g}, f) \le m$. Note that the figure of merit in Definition 2 differs by 1 from the figure of merit introduced in [13, Definition 3]. Observing this fact, we can now rephrase [13, Theorem 4] as follows.

Theorem B. *The points in* (4) *form a* (t, m, s)*-net in base* 2 *with* $t = m - \rho(\mathbf{g}, f)$.

Therefore, to obtain (t, m, s)-nets in base 2 with a small value of t, and hence good node sets for quasi-Monte Carlo integration, we should choose the parameters f and $\mathbf{g}$ in such a way that $\rho(\mathbf{g}, f)$ is large. If $s \ge 2$ and $f \in F_2[x]$ with $\deg(f) = m \ge 1$ are fixed, and if $\mathbf{g}$ runs through the set

$$G_s(f) = \{\mathbf{g} = (g_1, \dots, g_s) \in F_2[x]^s : \gcd(g_i, f) = 1 \text{ and } \deg(g_i) < m \text{ for } 1 \le i \le s\},$$

then it follows from results in [13], [14, Chapter 4] that, on the average, the node set (4) has star discrepancy $D_N^* = O(N^{-1}(\log N)^s)$. Thus, for any s and f, a good choice of $\mathbf{g}$ can always be made, but the proof of this result is nonconstructive.

It should be noted that we need the Laurent series expansion of the rational functions $n(x)g_i(x)/f(x)$ in (4) in order to calculate their images under ϕ_m according to (3). A very convenient choice for this purpose is $f(x) = x^m$, since for any $c(x) = \sum_{j=0}^{q} c_j x^j \in F_2[x]$ the Laurent series expansion of $c(x)/x^m$ is immediately obtained as

$$\frac{c(x)}{x^m} = \sum_{j=0}^{q} c_j x^{j-m}.$$

In the remainder of this paper, we assume that the choice $f(x) = x^m$ has been made. For this case, there is even a more precise existence theorem due to Larcher [4], namely, that for every $s \ge 2$ there exists a $\mathbf{g}$ such that the node set (4) has star discrepancy $D_N^* = O(N^{-1}(\log N)^{s-1} \log\log(N+1))$. Again, the proof of this result is nonconstructive.

3. The search procedure

Given the dimension $s \ge 2$ and the polynomial $f(x) = x^m \in F_2[x]$ with $m \ge 2$, we want to find an s-tuple $\mathbf{g} = (g_1, \dots, g_s)$ of polynomials over F_2 such that the figure of merit $\rho(\mathbf{g}, f)$ is large. As explained in §2, this yields then a (t, m, s)-net in base 2 with a small value of t. We impose the restriction $s \le 12$ since it is in this range where quasi-Monte Carlo integration is most useful (compare with [2]).

In the case $s = 2$ there is a general construction of a $\mathbf{g} = (g_1, g_2)$ which yields the optimal value of $\rho(\mathbf{g}, f)$. Put $g_1(x) = 1$ and

$$g_2(x) = \sum_{j=0}^{r} x^{m - \lfloor m/2^j \rfloor} \tag{5}$$

with $r = \lfloor \log_2 m \rfloor$, where $\lfloor\ \rfloor$ denotes the greatest integer function. Then [10, Theorem 2] shows that all partial quotients in the continued fraction expansion of $g_2(x)/x^m$ have degree 1. Hence it follows from a formula mentioned in [13] (see also [14, Theorem 4.46] for a detailed proof) that with this choice of $\mathbf{g} = (g_1, g_2)$ we obtain $\rho(\mathbf{g}, f) = m$. Since we always have $\rho(\mathbf{g}, f) \leq m$, as noted after Definition 2, we thus get the maximal value of $\rho(\mathbf{g}, f)$. By Theorem B the corresponding points in (4) form a $(0, m, 2)$-net in base 2.

For $s \geq 3$ no general construction of s-tuples $\mathbf{g}$ with a large value of $\rho(\mathbf{g}, x^m)$ is known, and as a result we have to resort to a computer search. In order to arrive at a manageable problem, we must restrict the values of m. We take $m \leq 20$ for $s = 3$ and $s = 4$, and $m \leq 10$ for $5 \leq s \leq 12$. The larger range of values of m is used for $s = 3$ and $s = 4$ since these dimensions occur frequently in applications. Because of computer limitations, only for low dimensions are larger values of m feasible in our search. In order to implement the search, Fortran code was written and run on a SUN SPARCstation 1^+. We note that in the context of shift-register pseudorandom numbers, Mullen and Niederreiter [6] and André, Mullen, and Niederreiter [1] have implemented search procedures for other types of figures of merit.

As indicated above, for a given $s \geq 3$ and $m \geq 2$ we let $f(x) = x^m$ and wish to locate an s-tuple $\mathbf{g} = (g_1, \dots, g_s) \in F_2[x]^s$ so that the figure of merit $\rho(\mathbf{g}, x^m)$ defined in Definition 2 is large, i.e., as near as possible to m. Without a serious loss of generality we may assume that $g_1 = 1$.

When s and m are both small, an exhaustive search was conducted over all s-tuples $\mathbf{g}$ so that the resulting figure of merit was optimal. When either s or m is large, it was not possible to do an exhaustive search, and so in these cases the resulting figure of merit is large but not necessarily optimal. In these nonexhaustive cases the resulting values of $t = m - \rho(\mathbf{g}, x^m)$ in Table 2 of §4 will be marked with an asterisk (*).

In the actual search process, given an s-tuple $\mathbf{g} = (g_1, \dots, g_s) \in F_2[x]^s$ with $g_1 = 1$, we search for a nonzero s-tuple $\mathbf{h} = (h_1, \dots, h_s) \in F_2[x]^s$ with the property that $\sum_{i=1}^{s} \deg(h_i) = d$ is small and $\sum_{i=1}^{s} g_i h_i \equiv 0 \pmod{x^m}$. Those $\mathbf{h}$ for which $\sum_{i=1}^{s} \deg(h_i) > d$ need not be considered in Definition 2. Our search then proceeds over all nonzero $\mathbf{h}$ with $\sum_{i=1}^{s} \deg(h_i) < d$ to see if $\sum_{i=1}^{s} g_i h_i \equiv 0 \pmod{x^m}$. If such an $\mathbf{h}$ is found, then the process is repeated with this smaller value of d. We continue until no smaller value of d is found, so that the resulting figure of merit is thus obtained as $\rho(\mathbf{g}, x^m) = s - 1 + \min \sum_{i=1}^{s} \deg(h_i)$. After completing the calculation of the figure of merit $\rho(\mathbf{g}, x^m)$ for a given $\mathbf{g}$, we consider other s-tuples $\mathbf{g}'$ in order to try and locate a figure of merit $\rho(\mathbf{g}', x^m) > \rho(\mathbf{g}, x^m)$. This process was then continued until either all $\mathbf{g}$ were tested, or in the nonexhaustive cases, until a point was reached at which after testing many s-tuples $\mathbf{g}$, the resulting largest figure of merit obtained for the given values of s and m failed to increase in value.

In spite of using nonexhaustive searches for numerous values of s and m, it will be seen in the next section that when $s \geq 5$ our results yield (t, m, s)-nets in base 2 with smaller values of t than those obtained from the best previously known constructions.

4. Computational results

In this section we present the results of our searches. In Table 2 for $s = 3$ or $s = 4$ and $m \leq 20$, and for $5 \leq s \leq 12$ and $m \leq 10$, we list the value of $t = m - \rho(\mathbf{g}, x^m)$ for which we located an s-tuple $\mathbf{g}$ with $\rho(\mathbf{g}, x^m)$ as large as possible. As a result, for a given s and m, the listed value of t is the smallest t (in the set that we searched) for which the corresponding points in (4) form a (t, m, s)-net in base 2. We recall from §3 that if our search was nonexhaustive, the corresponding t is marked with an asterisk. We also indicate with a prime (′) those values of t for which we have equality in (2) and hence are best possible values of t for a (t, m, s)-net in base 2. Thus, a ′ indicates that for the given values of s and m it is not possible by any method to construct a (t_1, m, s)-net in base 2 with $t_1 < t$.

TABLE 2. Values of t in a (t, m, s)-net in base 2

m\s	3	4	5	6	7	8	9	10	11	12
2	1	1	1	1	1	1	1	1	1	1
3	1	1′	1′	1′	2	2	2	2	2	2
4	1	1′	1′	1′	2	2′	2′	2′	2′	2′
5	1	1′	2	2	2	2′	2′	2′	3*	3*
6	1	1′	2	2	3*	3*	3*	3*	4*	4*
7	1	1′	2	2*	3*	3*	4*	4*	4*	4*
8	1	2	2*	3*	4*	4*	4*	4*	4*	5*
9	2	2	3*	4*	4*	5*	5*	5*	5*	6*
10	1	2*	3*	4*	4*	5*	6*	6*	6*	6*
11	2*	3*								
12	2*	3*								
13	2*	3*								
14	2*	4*								
15	3*	4*								
16	2*	4*								
17	3*	4*								
18	3*	5*								
19	4*	5*								
20	4*	6*								

We now compare the results of our efforts against previously known methods, in particular to the values of t given in Table 1 as well as considering them in relation to the lower bound from (2). For $s = 3$ the construction of Niederreiter [12] yields $t = 0$, which when compared to (2), yields a best possible $(0, m, 3)$-net in base 2 for any $m \geq 0$. Similarly, for $s = 4$ he obtains a value of $t = 1$ as well as a $(1, m, 4)$-net in base 2 for any $m \geq 1$, which is best possible for $m \geq 3$. For $s = 3$ and $s = 4$ our construction gives a net with a very small but not best possible value of t, unless $s = 4$ and $3 \leq m \leq 7$. However, it should be noted that the nets in (4) with $f(x) = x^m$ are, in general, easier to implement than the nets obtained from [12].

From a comparison of Table 2 with Table 1 we see that for each $5 \leq s \leq 12$, our construction yields a smaller value of t. In fact, in numerous cases denoted with a ′, our search procedure gives a best possible value of t. As s increases, the level of improvement of our construction over that from [12] also increases, even in the cases where nonexhaustive searches were conducted. For fixed s, as m increases, our values of t will be less than those of [12] (which do not increase with m) at least as long as $m \leq V_s$, where V_s is given in Table 1. For fixed s our values of t increase slowly with m.

We note from [7] that for $b = 2$ and $t \geq 0$ one can construct a $(t, t+2, 2^{t+2}-1)$-net in base 2, which according to (2) is best possible. Thus, for example, for the cases of a $(0, 2, 3)$ or $(1, 3, 7)$-net in base 2, the methods of [7] give a slight improvement. The methods of [7], however, apply only to the construction of $(t, t+2, 2^{t+2}-1)$-nets, while the methods presented here can be applied to the construction of (t, m, s)-nets in base 2 for any $s \geq 2$ and $m \geq 2$. For ease of implementation, we note that if C is the complete residue system of polynomials of degree less than m modulo x^m with $m = t+2$ and $\mathbf{g} = C \backslash \{0, x^{m-1}\}$, then $\rho(\mathbf{g}, x^m) = 2$. Hence, we obtain a $(t, t+2, 2^{t+2}-2)$-net in base 2 for any $t \geq 0$. See Table $s = 6$ with $m = 3$ for an illustration.

We close by providing tables of the s-tuples $\mathbf{g}$ of polynomials that give the values of t in Table 2. As indicated in §3, for $s = 2$ and $m \geq 2$, using (5), one can construct a $(0, m, 2)$-net in base 2. For $s \geq 3$ in Table s we provide the following data.

TABLE s

$$m \quad t \quad g_1 \quad g_2 \quad \cdots \quad g_s.$$

In the first column is the value of m, while the second column contains the value of t for a (t, m, s)-net in base 2, where $t = m - \rho(\mathbf{g}, x^m)$ and where $\rho(\mathbf{g}, x^m)$ is the largest figure of merit obtained from our calculations for the given values of s and m. For $i = 1, \dots, s$ the number listed under g_i is the number whose base-2 representation corresponds to the coefficients of g_i where $g_i \in F_2[x]$. Thus a polynomial $g \in F_2[x]$ with $g(x) = \sum_{i=0}^{m-1} a_i x^i$ is represented by the corresponding number $\sum_{i=0}^{m-1} a_i 2^i$.

TABLE s=3

m	t	g_1	g_2	g_3
2	1	1	1	1
3	1	1	2	3
4	1	1	5	6
5	1	1	10	13
6	1	1	19	25
7	1	1	35	49
8	1	1	90	97
9	2	1	74	97
10	1	1	321	402
11	2	1	381	615
12	2	1	2382	2631
13	2	1	6238	5771
14	2	1	11097	11345
15	3	1	26294	26791
16	2	1	24250	25245
17	3	1	80092	82081
18	3	1	67899	238395
19	4	1	66000	80952
20	4	1	666401	696305

TABLE s=4

m	t	g_1	g_2	g_3	g_4
2	1	1	1	1	1
3	1	1	2	3	5
4	1	1	5	6	9
5	1	1	10	13	18
6	1	1	25	39	47
7	1	1	45	61	81
8	2	1	36	49	66
9	2	1	77	98	133
10	2	1	183	316	321
11	3	1	209	268	326
12	3	1	291	1286	2281
13	3	1	5964	6461	6958
14	4	1	1528	2523	3518
15	4	1	9629	11618	13608
16	4	1	4387	5382	6376
17	4	1	29394	33132	96799
18	5	1	39611	62523	182139
19	5	1	101150	228484	355818
20	6	1	301297	392945	484593

TABLE s=5

m	t	g_1	g_2	g_3	g_4	g_5
2	1	1	1	1	1	1
3	1	1	2	3	5	6
4	1	1	5	6	9	13
5	2	1	4	6	9	11
6	2	1	9	13	17	20
7	2	1	19	27	35	41
8	2	1	43	60	103	142
9	3	1	40	50	65	350
10	3	1	82	113	136	749

TABLE s=6

m	t	g_1	g_2	g_3	g_4	g_5	g_6
2	1	1	1	1	1	1	1
3	1	1	2	3	5	6	7
4	1	1	5	6	9	13	14
5	2	1	4	6	9	11	14
6	2	1	14	20	25	31	34
7	2	1	18	34	59	83	89
8	3	1	18	26	34	40	199
9	4	1	22	28	33	40	399
10	4	1	36	49	129	499	754

TABLE s=7

m	t	g_1	g_2	g_3	g_4	g_5	g_6	g_7
2	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1
4	2	1	2	3	4	5	6	7
5	2	1	5	6	9	13	14	25
6	3	1	5	6	8	11	17	39
7	3	1	8	15	18	20	33	100
8	4	1	9	13	17	37	127	195
9	4	1	23	29	33	40	234	410
10	4	1	41	73	104	206	301	400

TABLE s=8

m	t	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
2	1	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1	1
4	2	1	2	3	4	5	6	7	9
5	2	1	4	6	9	11	14	17	20
6	3	1	5	6	8	11	17	18	39
7	3	1	11	13	18	21	34	38	99
8	4	1	18	23	25	31	34	40	199
9	5	1	11	14	16	20	63	177	300
10	5	1	777	807	836	865	894	923	953

TABLE s=9

m	t	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9
2	1	1	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1	1	1
4	2	1	2	3	4	5	6	7	9	10
5	2	1	5	6	9	13	14	17	21	22
6	3	1	4	6	9	11	14	17	20	43
7	4	1	5	6	9	13	14	41	66	100
8	4	1	11	13	20	54	115	136	177	200
9	5	1	11	56	101	146	190	235	280	290
10	6	1	9	16	23	61	116	203	304	422

TABLE s=10

m	t	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}
2	1	1	1	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1	1	1	1
4	2	1	2	3	4	5	6	7	9	10	11
5	2	1	5	6	9	13	14	17	21	22	25
6	3	1	5	6	8	11	17	18	21	28	40
7	4	1	5	7	8	12	17	26	41	62	74
8	4	1	11	13	19	20	54	115	136	177	200
9	5	1	11	56	101	146	190	235	245	290	479
10	6	1	8	13	78	104	205	320	431	988	1000

TABLE s=11

m	t	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}
2	1	1	1	1	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1	1	1	1	1
4	2	1	2	3	4	5	6	7	9	10	11	12
5	3	1	2	3	4	6	9	11	13	17	20	22
6	4	1	2	3	12	20	28	38	42	45	52	58
7	4	1	4	6	18	29	40	51	76	87	99	110
8	4	1	14	30	104	110	121	140	161	186	197	230
9	5	1	9	12	73	150	177	209	263	274	377	402
10	6	1	9	12	160	381	415	496	587	618	651	700

TABLE s=12

m	t	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}
2	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1	1	1	1	1	1
4	2	1	2	3	4	5	6	7	9	10	11	12	13
5	3	1	2	3	4	5	6	8	11	13	17	18	20
6	4	1	2	3	17	20	23	27	34	39	46	51	56
7	4	1	7	18	29	40	51	65	76	87	99	110	123
8	5	1	10	37	60	82	104	127	154	176	199	221	243
9	6	1	17	36	81	106	126	171	215	260	350	439	504
10	6	1	47	105	163	222	280	720	778	837	895	954	1012

BIBLIOGRAPHY

1. D. A. André, G. L. Mullen, and H. Niederreiter, *Figures of merit for digital multistep pseudorandom numbers*, Math. Comp. **54** (1990), 737-748.
2. P. Bratley, B. L. Fox, and H. Niederreiter, *Implementation and tests of low-discrepancy sequences*, ACM Trans. Modeling and Computer Simultation **2** (1992), 195–213.
3. L. K. Hua and Y. Wang, *Applications of number theory to numerical analysis*, Springer, Berlin, 1981.
4. G. Larcher, *Nets obtained from rational functions over finite fields*, Acta Arith. **63** (1993), 1–13.
5. D. H. Lehmer, *Mathematical methods in large-scale computing units*, Proc. 2nd Sympos. on Large-Scale Digital Calculating Machinery (Cambridge, MA, 1949), Harvard Univ. Press, Cambridge, MA, 1951, pp. 141–146.
6. G. L. Mullen and H. Niederreiter, *Optimal characteristic polynomials for digital multistep pseudorandom numbers*, Computing **39** (1987), 155-163.
7. G. L. Mullen and G. Whittle, *Point sets with uniformity properties and orthogonal hypercubes*, Monatsh. Math. **113** (1992), 265-273.
8. H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957-1041.
9. ——, *Multidimensional numerical integration using pseudorandom numbers*, Math. Programming Study **27** (1986), 17–38.
10. ——, *Rational functions with partial quotients of small degree in their continued fraction expansion*, Monatsh. Math. **103** (1987), 269-288.
11. ——, *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273–337.
12. ——, *Low-discrepancy and low-dispersion sequences*, J. Number Theory **30** (1988), 51–70.
13. ——, *Low-discrepancy point sets obtained by digital constructions over finite fields*, Czechoslovak Math. J. **42** (1992), 143-166.
14. ——, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992.

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

16. ——, *Finite fields, pseudorandom numbers, and quasirandom points*, Proc. Internat. Conf. on Finite Fields, Coding Theory, and Advances in Comm. and Comp. (Las Vegas, 1991), Dekker, New York, 1993, pp. 375–394.

17. I. M. Sobol′, *The distribution of points in a cube and the approximate evaluation of integrals*, Zh. Vychisl. Mat. i Mat. Fiz. 7 (1967), 784–802. (Russian)

(Hansen and Mullen) DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802
E-mail address: pho3@math.psu.edu
E-mail address: mullen@math.psu.edu

INSTITUTE FOR INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, SONNENFELSGASSE 19, A-1010 VIENNA, AUSTRIA
E-mail address: nied@qiinfo.oeaw.ac.at