

A Parallel Search for Good Lattice Points using LLL-Spectral Tests

Bernhard Hechenleitner and Karl Entacher¹

*Salzburg University of Applied Sciences and Technologies,
Schillerstr. 30, 5020 Salzburg, Austria*

Abstract

We present results from an extensive parallel search for rank-1 lattice rules using the LLL-spectral test with a new normalization strategy which is proposed in [1]. We introduce the main concepts concerning lattice rules and the spectral test and motivate the new normalization strategy for this test. The concepts for parallelization are explained and some results conclude the article.

Key words: lattice rules, good lattice points, spectral test

1 Introduction

The present article shows results of a large scale parallel parameter search for Korobov lattice rules. As a quality criteria for the lattices we used the spectral test with a new normalization strategy. The spectral test allows to perform efficient quality assessments for lattice rules in high dimensions and the parallel setup enables a search over a huge set of parameters. The paper is organized in the following way: In the next sections we introduce the main concepts concerning lattice rules and the spectral test and motivate the new normalization strategy for this test. The concepts for parallelization and some results represent the central part of the article.

1.1 Good Lattice Points

The method of *good lattice points* (GLP) also called *Korobov lattice rules* is a central technique from the fields of *Monte Carlo* (MC) and *quasi-Monte Carlo* (QMC) methods. Good lattice points are classical node sets for QMC integration, defined by the Russian mathematician Korobov [2–4]. For $y \in \mathbb{R}$

Email address: [bernhard.hechenleitner, karl.entacher]@fh-sbg.ac.at
(Bernhard Hechenleitner and Karl Entacher).

¹ Research supported by the Austrian Science Fund (FWF) Grant S8311-MAT.

let $\{y\} = y - \lfloor y \rfloor$ be the *fractional part* of y . Consider a vector $\vec{a} \in \mathbb{Z}^s$, $s \geq 2$. A Korobov lattice rule is defined by the set

$$P_m := \{ \vec{x}_n : 0 \leq n < m \}, \text{ with } \vec{x}_n := \left\{ \frac{n \cdot \vec{a}}{m} \right\}, \text{ and modulus } m \in \mathbb{N}. \quad (1)$$

In the following we will use the term Korobov lattice rule P_m only for special vectors \vec{a} defined by a parameter a with $1 < a < m$ and $\vec{a} := (1, a, a^2, \dots, a^{s-1})$, $s \geq 2$, see [3]. The set P_m can be seen as the intersection of the s -dimensional *unit cube* $I^s := [0, 1]^s$ with the lattice

$$L_s(a, m) = \left\{ \sum_{i=1}^s k_i \vec{b}_i : \vec{k} \in \mathbb{Z}^s \right\}, \quad (2)$$

with basis $\vec{b}_1 = (1, a, \dots, a^{s-1})/m$, $\vec{b}_2 = (0, 1, 0, \dots, 0)$, \dots , $\vec{b}_s = (0, 0, \dots, 0, 1)$.

For lattice assessment purposes often the dual lattice $L_s^*(a, m)$ of $L_s(a, m)$ is applied (see Sect. 1.2). Note that the *dual* of a lattice L_s is defined as $L_s^* := \{ \vec{v} \in \mathbb{R}^s : \vec{v} \cdot \vec{w} \in \mathbb{Z} \text{ for all } \vec{w} \in L_s \}$. The dual basis of a given lattice basis $B = \{ \vec{b}_1, \dots, \vec{b}_s \}$ is provided by the set of vectors $B^* = \{ \vec{b}_1^*, \dots, \vec{b}_s^* \}$ such that $\vec{b}_i \cdot \vec{b}_j^* = \delta_{i,j}$, with $\delta_{i,j} = 1$, if $i = j$ and $\delta_{i,j} = 0$ otherwise. For Korobov lattice rules $L_s^*(a, m)$ is given by the basis

$$\vec{b}_1^* = (m, 0, \dots, 0), \vec{b}_2^* = (-a, 1, 0, \dots, 0), \dots, \vec{b}_s^* = (-a^{s-1}, 0, \dots, 0, 1). \quad (3)$$

The classical application of Korobov lattice rules is the approximate calculation of integrals over I^s , by the (quasi-) Monte Carlo quadrature rule

$$\int_{I^s} f(\vec{x}) d\vec{x} \approx \frac{1}{m} \sum_{n=0}^{m-1} f(\vec{x}_n), \quad \vec{x}_n \in P_m. \quad (4)$$

Furthermore, Korobov lattice rules with huge moduli and good lattice quality up to high dimensions provide parameters a and m for linear congruential random number generators (LCGs) with good correlation behavior as a source for MC applications [5,6]. Note that a LCG is defined by the linear recurrence $y_{n+1} \equiv ay_n + b \pmod{m}$, $n \geq 0$, and by an initial seed y_0 , where the parameters $a, b, y_0 \in \mathbb{Z}_m := \{0, \dots, m-1\}$ (the least residue system modulo m). For standard parametrization schemes which guarantee maximal period of the recurrence see [6,7]. LCGs are currently the best analyzed and most widely used random number generators. They have recently attained special interest due to the fact that some state of the art generation methods are equivalent or approximately equivalent to big size LCGs [7].

More recent lattice rules, so-called rank- r lattice rules have been constructed by modular summation over multiples of different vectors \vec{a}_i , $1 \leq i \leq r$. Korobov lattice rules are a special case of rank-1 rules. For more details on the theory of integration lattices and their applications in MC and QMC see [6,8,9].

1.2 Spectral Test

The choice of the parameter a heavily determines the distribution quality of the lattice. Figure 1 shows examples of simple lattices P_m with $m = 2^7 - 1$, $a = 3$ (left) and $a = 53$ (right).

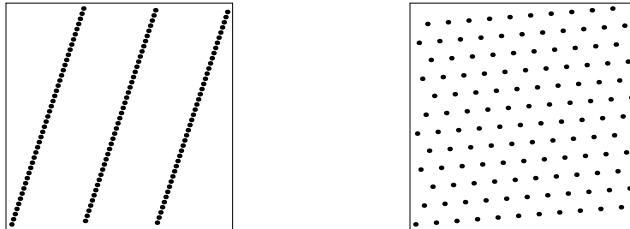


Fig. 1. Lattice rules P_m with $m = 2^7 - 1$ and $a = 3$ (left) and $a = 53$ (right).

The central goal for QMC integration is to find lattice parameters a with optimal distribution behavior in different dimensions. For this task, several equidistribution measures for an assessment of the lattice quality have been constructed, see [6,8,10,11]. For our purposes we use the *spectral test*, which can be computed very efficiently and provides a reliable measure for lattice assessment [10]. This test has extensively been applied to find good lattices for several MC and QMC applications, e.g. see [5,12,13].

The spectral test uses the dual lattice $L_s^*(a, m)$. From its dual basis (3) the shortest vector \vec{v} of the dual lattice can be computed by means of the Fincke-Pohst algorithm [14]. One over the Euclidean length of this shortest vector yields the spectral test d_s , which determines the maximum distance between adjacent hyper-planes, taken over all families of parallel hyper-planes which contain all points of the lattice [15–17].

To enable comparisons of spectral test results obtained in different dimensions, a normalized spectral test $S_s := d_s^*/d_s$ for which $0 \leq S_s \leq 1$ was introduced [18]. The constants d_s^* are absolute lower bounds on d_s , see [16, p. 105] for $d_s^*, s \leq 8$. Lower bounds for dimension $s > 8$ have been proposed as well in order to compute S_s for arbitrary dimensions [5]. For our examples in Figure 1 we have $S_2 = 0.26$ for the left graphics and $S_2 = 0.99$ for the right one.

A typical function measuring the “quality” of a lattice parameter a in terms of the spectral test across dimensions is:

$$M_k := \min_{2 \leq s \leq k} S_s. \quad (5)$$

Fishman [18] was one of the first who applied this measure to find optimal parameters a for $m = 2^{31} - 1$ in order to get high quality linear congruential random number generators satisfying a fixed threshold $M_6 \geq 0.8$. Recently the measure M_k has been maximized for dimensions up to $k = 32$ in the context of large scale parameter searches [5,13,19].

In order to considerably speed up the computations, the LLL basis reduction algorithm [20] may be applied instead of the Fincke-Pohst algorithm as an efficient and reliable approximation to the spectral test. Our experiments use an approximation of this type. The high quality of the LLL-approximation and the speedup with respect to the “original” spectral test have been shown [12].

1.3 A new Normalization Approach to the Spectral Test

One problem with the measure M_k (5) is that the magnitudes of the single normalized spectral tests S_s vary significantly for $1 \leq s \leq k$ as can be seen from Figure 2. The figure shows the distribution behavior of normalized spectral tests S_s for $2 \leq s \leq 13$ from top left ($s = 2$) to down right ($s = 13$). The linearly scaled x-axis of each single graph within the figure represents S_s values from 0 (left) to 1 (right). To generate the histograms a modulus $m = 2^{64} - 59$ and a random sample of 1300000 parameters a for each dimension s was used. As the figure shows a fixed threshold to find the best parameter may not be optimal since it is very unlikely to find a parameter a with $S_8 > 0.8$ for example. The distribution behavior shown in Figure 2 is almost independent of the size of the modulus m for Korobov lattices, see [1] for further details and examples. Two facts can be seen from the histograms very clearly: For dimension $s = 2$ we face a triangle-type distribution and for increasing dimensions, the histograms get more and more symmetric and slightly shifted to the right half of the unit interval. The regularity of the histograms suggest the existence of an underlying classical density function. Although several attempts have

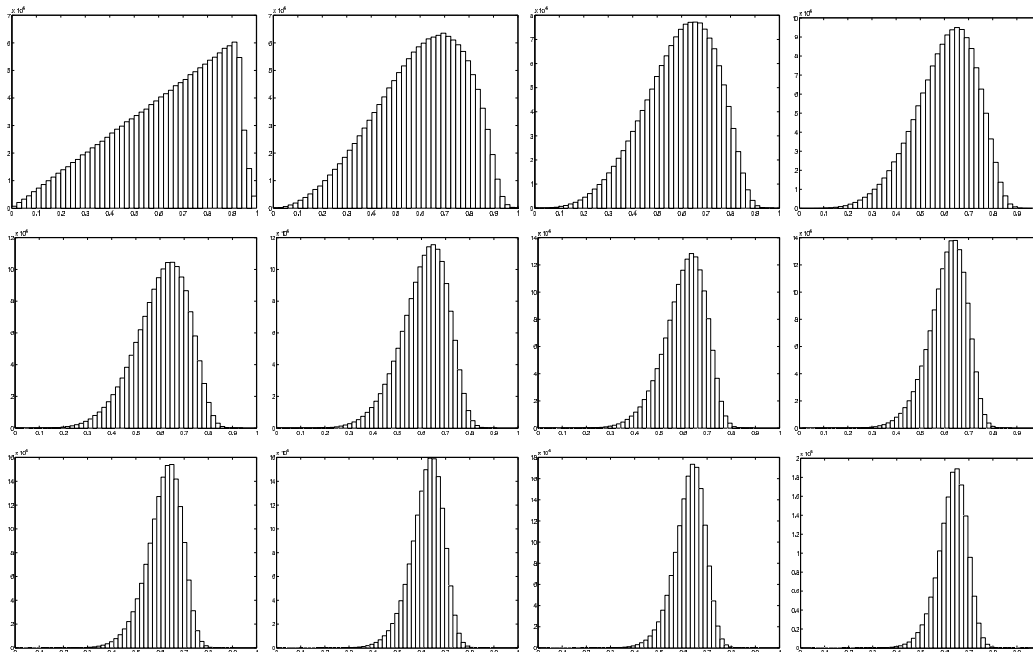


Fig. 2. Distribution behavior of normalized spectral tests S_s for $2 \leq s \leq 13$ (from top left ($s = 2$) to down right ($s = 13$)).

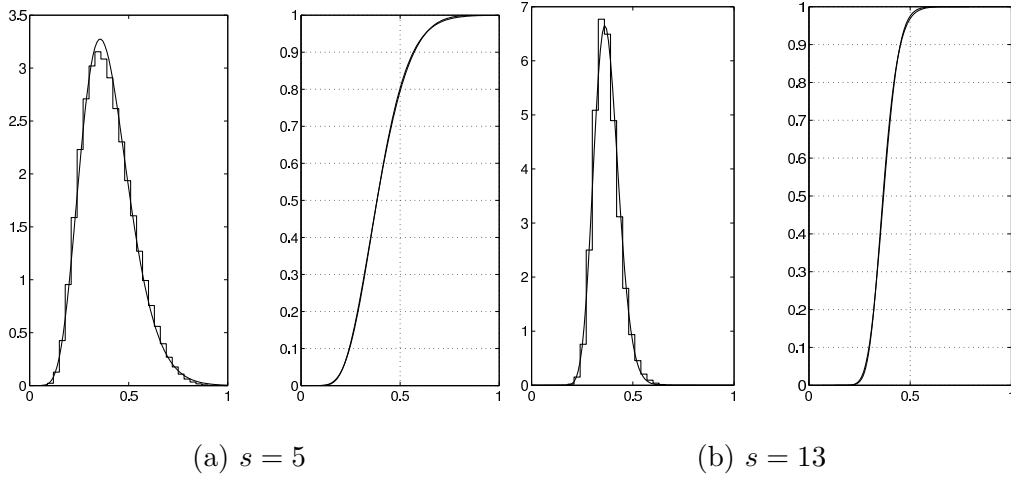


Fig. 3. MLE Gamma distribution fit for $1 - S_s$, $s = 5, 13$ where $m = 2^{64} - 59$.

been made to verify this (e.g. [21]), the distributions of the spectral test values remain an open question. Nevertheless, in [1] it was shown that among several empirical distribution fits based on maximum likelihood estimation, the Gamma distributions turned out to show the best approximations to the distributions of $1 - S_s$ with surprising good quality, for dimensions $s \geq 3$ and different moduli. With increasing dimensions the quality of approximation increased as well. Figure 3 exhibits the good quality of approximation. The left graphics show the histograms and the corresponding density, and the right graphics the empirical distribution function versus the Gamma distribution function where almost no deviation is observable. In [1], these empirical findings are the basis to suggest a new normalization strategy based on distribution dilation in order to make the measure M_k more balanced among the dimensions. To cope with empirical outliers certain estimates for 0.1% and 99.9% quantiles have been determined based on regression. To get a new spectral test normalization S'_s all values S_s between the inter-quantile ranges are linearly transformed to $[0,1]$, and values of S_s outside of the quantiles are mapped to zero and one respectively. For more details and examples see [1]. Figure 4 illustrates the normalization adjustment.

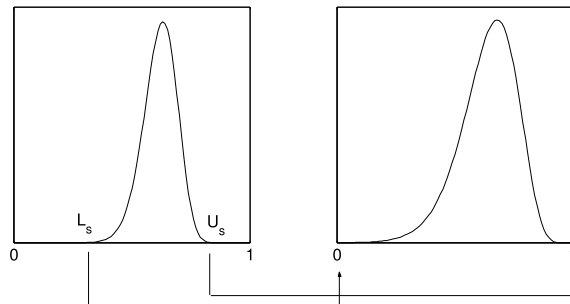


Fig. 4. Normalization adjustment $S'_s = (S_s - L_s) / (U_s - L_s)$ from distribution dilation.

The regression models for the lower quantile L_s and the upper quantile U_s for $s = 2, 3, \dots$ are:

$$L_s := 0.000042s^3 - 0.0027s^2 + 0.067s - 0.097 \quad (6)$$

$$U_s := -0.000058s^3 + 0.0036s^2 - 0.059s + 1.09 \quad (7)$$

Using these functions we linearly transformed the spectral tests S_s in dimension $2 \leq s \leq 24$ and used the transformed measure $S'_s = (S_s - L_s)/(U_s - L_s)$ as a new normalized spectral test for the computer experiments in Sect. 2.

2 Parallel Search for GLP

Although the spectral test was chosen as the method for assessing the quality of a lattice, the search for GLPs can become computationally intensive. Therefore, the approach of a parallel application using a cluster was chosen. We restrict our parameter searches to prime moduli m in the range $2^6 < m < 2^{256}$. Parameters for "small" moduli, e.g. $m \leq 2^{31} - 1$ may be applied as lattice rules for QMC-integration, and the parameters for larger m as multipliers for multiplicative LCGs with prime moduli. Therefore our main task is to find the best GLP or multiplier $a \in A$ where A is the set of all primitive roots modulo m since this restriction provides parameters for multiplicative LCGs with full period [6]. For moduli $m \leq 2^{31} - 1$ we performed exhaustive searches, i.e. the search space contained all multipliers in A . For larger moduli only a subset of A was considered as the search space.

As a search criterion we use the measure M_k (5). Concerning the normalization method for the spectral test, the "old" normalization method with S_s and the "new" strategy using S'_s in (5) instead of S_s are distinguished.

The basic sketch of the search method is

- Find a primitive root e modulo m . Because m is restricted to be a prime number e is a generator of the cyclic group $\mathbb{Z}_m \setminus \{0\}$ (i.e. the multiplicative order of e modulo m is $\phi(m) = m - 1$ where ϕ is Euler's totient function).
- Take relevant powers $a = e^\varepsilon \pmod{m}$ as multipliers for which $\gcd(\varepsilon, \phi(m)) = 1$. The latter constraint ensures that a is also a primitive root modulo m .
- For each a in the search space and all dimensions up to dimension k , calculate the LLL reduction, find the spectral test value d_s , calculate the defined normalization ("old" or "new"), and find the minimum M_k of the corresponding normalized spectral test values.
- Find the largest M_k value across all chosen multipliers in A .

For this purpose, a prototype of a distributed application for the parallel search of GLPs has been developed.

2.1 Components and Activities

For increasing efficiency, the PC-cluster *Gaisberg* of the High Performance Computing Group² of the department of Scientific Computing at the University of Salzburg has been used to conduct parallel searches. The cluster consists of 25 identically equipped nodes as described in Table 1.

Table 1

Cluster nodes.

Architecture	PC
CPU	2 AMD Athlon MP 2800+ (2.1 GHz)
Memory	2 GByte
Operating System	Red Hat Linux 7.3
Linux Kernel	2.4.20
Cluster Interconnect	<i>Scalable Coherent Interface</i> (SCI) from Scali ^a
Programming Interface	<i>Message Passing Interface</i> (MPI) from Scali

^a Home page: <http://www.scali.com> (28.09.2004)

The dependencies of the software components are shown in the UML component and deployment diagram in Figure 5. The **Master Node** controls the system setup. The distributed **Spectral test application** is started via the **MPI Monitor** application called `mpimon` at the **Master Node**, together with corresponding arguments in the form of command line options. A typical setup is to start two instances of the search application per **Working Node** for maximum efficiency, as each node provides two CPUs.

The **Spectral test application** at the **Master Node** determines important parameters for the search and distributes their values to the search processes at the **Working Nodes** utilizing MPI. When a search process finishes its partial search, it passes back its best result – consisting of the best M_k value, its corresponding multiplier a , and the number of executed search loops – to the master process, again by utilizing MPI. The master process sorts the received results, calculates the spectral test values for the best global multiplier and the corresponding values for $M_k, k \in \{8, 16, 24\}$ with regard to both normalization methods, and prints out the detailed values. Finally, the best result may be stored in a **Database**.

2.2 Search Algorithm

The search algorithm for each search process is as follows. Assume, the modulus m , the search dimension k , and the normalization method for the nor-

² Home page: <http://hpc.sbg.ac.at> (28.09.2004)

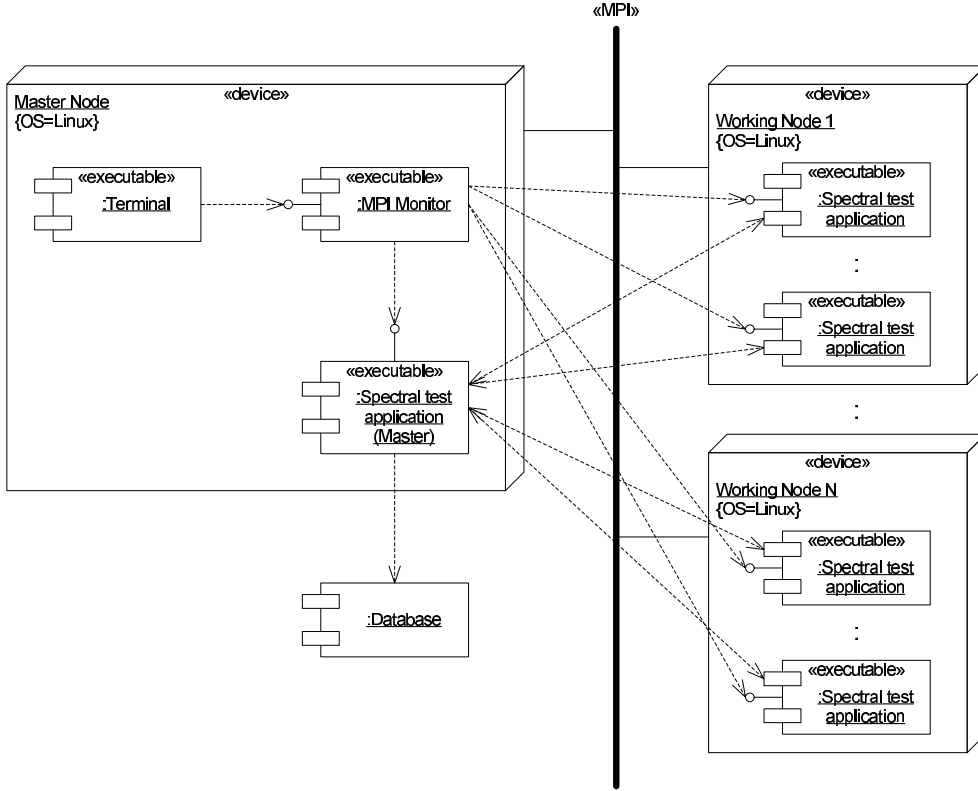


Fig. 5. Software components and their deployment within the MPI cluster setup.

malized spectral test value *method* have been defined. In the current version of our `Spectral test application` we applied prime numbers $m < 2^{256}$ and dimensions $k \in \{8, 16, 24\}$ and $method \in \{old, new\}$.

In a first step, the values for the best global minimum M_k , denoted as M_k^* , and the best global multiplier a^* are initialized to 0. Then the primitive root e and a starting exponent α , which have been determined and distributed by the master process, are set. Note that for an exhaustive search α is 1. If only a subset of A is considered we pick α randomly from all possible exponents. Next, the ending exponent β for e , which also represents the loop boundary, is determined and set by each search process. Only those exponents ε are relevant for consideration which fulfill the condition $gcd(\varepsilon, m - 1) = 1$. Since m is a prime number, all even values of ε are irrelevant and therefore may additionally be skipped. For this purpose the exponent increment distance δ is set to 2 by default. Applying a leapfrog method across the search processes, the exponent increment value γ for each search process is

$$\gamma = \delta \cdot n_p \tag{8}$$

where n_p is the total number of search processes. The starting exponent ε for

Algorithm 1. Search Loop.

```

WHILE  $\varepsilon < \beta$  DO
  IF  $\gcd(\varepsilon, m - 1) = 1$  THEN
    set multiplier  $a \leftarrow e^\varepsilon \pmod{m}$ ;
    set minimum of normalized spectral test value  $M_k \leftarrow 1$ ;
    FOR  $s \leftarrow 2$  to  $k$  DO
      do LLL reduction;
      find spectral test value  $d_s$ ;
      set  $S_s \leftarrow d_s^*/d_s$ ;
      IF method is new THEN
        set  $S_s \leftarrow (S_s - L_s)/(U_s - L_s)$ ;
      ENDIF
      IF  $S_s < M_k$  THEN
         $M_k \leftarrow S_s$ ;
      ENDIF
    ENDFOR
    IF  $M_k > M_k^*$  THEN
       $M_k^* \leftarrow M_k$ ;
       $a^* \leftarrow a$ ;
    ENDIF
  ENDIF
   $\varepsilon \leftarrow \varepsilon + \gamma$ ;
ENDWHILE

```

each search process is defined by its rank³ r_p :

$$\varepsilon = \alpha + \delta \cdot (r_p - 1) \tag{9}$$

After initialization of important search parameters, the search process enters the central search loop, which is described in Algorithm 1. As long as the exponent ε is smaller than the ending exponent β , in a first step it has to be checked if the new exponent yields another primitive root a when applied as $a = e^\varepsilon \pmod{m}$. If not, ε is incremented by γ and the next loop cycle is executed. However, if ε yields another primitive root, a is set as the new multiplier for the modulus m , and the minimum of the normalized spectral test values M_k is initialized to the value 1.

For all dimensions $s, 2 \leq s \leq k$, first of all the LLL reduction is calculated and the spectral test value d_s is determined. Next, the normalized spectral test value with regard to the old normalization S_s is calculated. If the new normalization is desired, S_s is transformed to S'_s according to the methods of the new normalization (see Sect. 1.3). If this normalized or transformed value results in a new minimum, M_k is reassigned accordingly. Finally, if the specific

³ The rank of the first search process is 1.

multiplier a yields a new highest global value for M_k , then this pair of values (a, M_k) is taken as the new best global pair of values (a^*, M_k^*) . Before entering the loop again, the value for ε is increased by γ .

Note that this algorithm can be trivially modified to provide M_k values for both normalization methods and an arbitrary set of k values for any $k \leq 24$.

3 Results

First results of parallel searches for GLPs using the parallel setup described in Sect. 2 are depicted in the following tables. The set of considered moduli consisted of selected primes m near powers of 2 for which $m < 2^{256}$.

For the results in Table 2, exhaustive searches for moduli up to $m < 2^{31}$ have been considered. The search dimension was $k = 8$ with regard to the old normalization. The main intention was to find improved multipliers compared to the tables of L'Ecuyer [5] where exhaustive searches have been performed only for $m < 2^{26}$.

Table 2

Best multipliers a with regard to M_8 old (exhaustive search).

m	a	M_8 old	M_{16} old	M_{24} old
		M_8 new	M_{16} new	M_{24} new
$2^{28} - 57$	83353756	0.760345	0.551917	0.551917
		0.776517	0.432971	0.432971
	246049789	0.742150	0.528200	
		0.786990	0.344963	
$2^{29} - 3$	130051211	0.758436	0.532918	0.532918
		0.808612	0.333811	0.333811
	520332806	0.752380	0.595380	
		0.814203	0.472398	
$2^{30} - 35$	149186228	0.759227	0.549709	0.549709
		0.843378	0.454777	0.454777
	771645345	0.748810	0.605400	
		0.782242	0.508062	
$2^{31} - 1$	1977654935	0.766574	0.546750	0.546750
		0.781826	0.448292	0.379117
	1583458089	0.727710	0.619960	
		0.799961	0.545305	

The found improvements are shown as boldface values in the table, together with their corresponding values for M_k , $k \in \{8, 16, 24\}$ for both normalization methods in the first two lines of each entry. For comparison, the previous best multipliers taken from [5] together with their values for M_8 old and M_{16} old (L'Ecuyer used $k \in \{8, 16, 32\}$) are shown as well in line three of each entry. For completeness, their accordant values regarding the new normalization are also depicted in the last line of each entry.

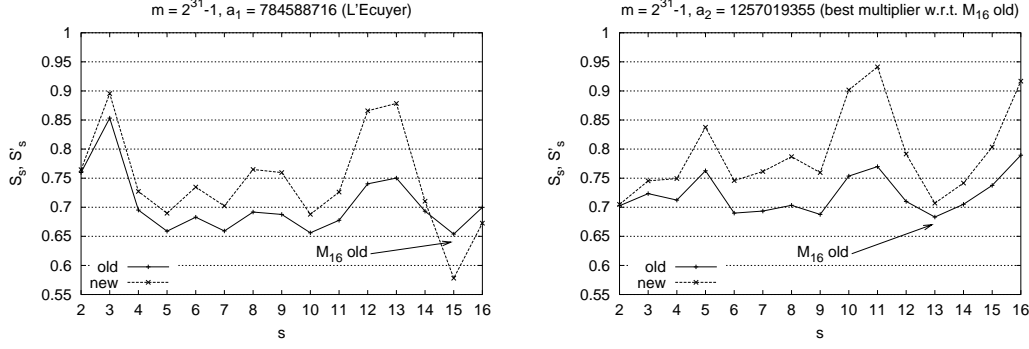


Fig. 6. Spectral test behaviors of two different multipliers $a_1 = 784588716$ ([5]), $a_2 = 1257019355$ (Table 3) with modulus $m = 2^{31} - 1$.

The same search method has been applied for dimension $k = 16$ with regard to the old normalization. Again, the improvements and the previous best values are shown in Table 3. Interestingly, in these cases also the values for M_{16} new have been improved whereas this is not the case for all M_8 new values in Table 2. The latter effect may happen since the normalization adjustment is more sensitive for increasing dimension.

Figure 6 demonstrates such a normalization effect. We compare spectral test values $S_s, S'_s, 2 \leq s \leq 16$ for two multipliers $a_1 = 784588716, a_2 = 1257019355$ with $m = 2^{31} - 1$. Multiplier a_1 is given in [5]. It was selected by a random search according to M_{16} with the old normalization method. Multiplier a_2 corresponds to our exhaustive search results according to M_{16} with the same normalization, see Table 3.

Table 3

Best multipliers a with regard to M_{16} old (exhaustive search).

m	a	M_8 old	M_{16} old	M_{24} old
		M_8 new	M_{16} new	M_{24} new
$2^{27} - 39$	66100098	0.674364	0.674364	0.671350
		0.728434	0.728434	0.563524
	3162696	0.702330	0.672640	
		0.751560	0.699585	
$2^{28} - 57$	230195011	0.692705	0.680449	0.680449
		0.734185	0.717931	0.529734
	140853223	0.704620	0.673530	
		0.723500	0.682391	
$2^{29} - 3$	507054386	0.706185	0.694721	0.664672
		0.757498	0.704076	0.545287
	530877178	0.673520	0.670880	
		0.719956	0.593768	
$2^{30} - 35$	790126461	0.680384	0.680384	0.680384
		0.738809	0.726937	0.586649
	295397169	0.683230	0.674200	
		0.749031	0.690916	
$2^{31} - 1$	1257019355	0.690019	0.683158	0.683158
		0.705018	0.705018	0.536430
	784588716	0.658850	0.653880	
		0.689715	0.578044	

The impact of the new normalization for larger dimensions is clearly shown for multiplier a_1 . The minimum M_{16} concerning the old normalization is at position $s = 15$. This value and also the S_s value for $s = 16$ lie in the lower area of the corresponding spectral test distribution used for the new normalization (cf. Sect. 1.3) and therefore the resulting S'_s values are decreased significantly by the new normalization adjustment. The S'_s values below this dimension are all increased. Multiplier a_2 avoids such a behavior. Applying the new normalization method for an exhaustive parameter search for the given modulus with regard to M_{16} we obtain $a_3 = 1624371841$. The spectral test values for this multiplier behave similar as for a_2 , but in comparison to a_2 some smaller S_s values occur for the old normalization at some dimensions. As this multiplier results in improved values at higher dimensions, the corresponding M_{16} new value is 0.740411.

Exhaustive searches for $m < 2^{31}$ have also been conducted with regard to the new normalization for dimension $k = 24$. The results are shown in Table 4.

Table 4

Best multipliers a with regard to M_{24} new (exhaustive search).

m	a	M_8 new M_8 old	M_{16} new M_{16} old	M_{24} new M_{24} old
$2^{10} - 3$	65	0.726822 0.690694	0.703401 0.663168	0.534339 0.663168
$2^{11} - 9$	1072	0.597302 0.599080	0.597302 0.599080	0.597302 0.599080
$2^{12} - 3$	500	0.665212 0.642591	0.665212 0.642591	0.665212 0.642591
$2^{13} - 1$	5900	0.663222 0.648430	0.663222 0.648430	0.663222 0.648430
$2^{14} - 3$	1543	0.657914 0.633986	0.657914 0.633986	0.657914 0.633986
$2^{15} - 19$	7912	0.726093 0.673006	0.726093 0.673006	0.726093 0.673006
$2^{16} - 15$	4623	0.662787 0.637396	0.662787 0.637396	0.662787 0.637396
$2^{17} - 1$	51308	0.728530 0.678984	0.690387 0.662301	0.688453 0.662301
$2^{18} - 5$	152508	0.686988 0.663751	0.686988 0.661700	0.686988 0.661700
$2^{19} - 1$	37698	0.711975 0.667797	0.711975 0.667797	0.707139 0.667797
$2^{20} - 3$	516672	0.668804 0.644146	0.668804 0.644146	0.668804 0.644146
$2^{21} - 9$	1531968	0.710673 0.678134	0.710673 0.674078	0.710673 0.674078
$2^{22} - 3$	1135380	0.686095 0.672307	0.686095 0.672307	0.686095 0.672307
$2^{23} - 15$	2115063	0.706835 0.660804	0.699275 0.660804	0.699275 0.660804

(continued on next page)

Table 4

Best multipliers a with regard to M_{24} new (continued).

m	a	M_8 new M_8 old	M_{16} new M_{16} old	M_{24} new M_{24} old
$2^{24} - 3$	926716	0.696865 0.655506	0.678597 0.655506	0.678597 0.655506
$2^{25} - 39$	6557845	0.716337 0.671214	0.702975 0.662974	0.702975 0.662974
$2^{26} - 5$	27830235	0.746356 0.704761	0.721056 0.696578	0.721056 0.696578
$2^{27} - 39$	33298047	0.741795 0.682116	0.732958 0.682116	0.719319 0.682116
$2^{28} - 57$	19257650	0.713572 0.664384	0.713572 0.664384	0.713572 0.664384
$2^{29} - 3$	218346125	0.713048 0.669119	0.713048 0.669119	0.713048 0.669119
$2^{30} - 35$	353791604	0.710906 0.664195	0.710906 0.664195	0.710906 0.664195
$2^{31} - 1$	1690867642	0.700438 0.661083	0.697860 0.660640	0.697860 0.660640

Figure 7 demonstrates the spectral test behaviors of the best found multipliers for two different moduli. The left graphics shows the behavior of the best multiplier for modulus $m = 2^{10} - 3$. Concerning the old normalization, this multiplier yields a M_{24} old value of 0.663168. Looking at the S'_s values it can be seen that the shape of the curve for higher dimensions strongly decreases because of the intense effects of the normalization adjustments, resulting in a rather low value for M_{24} new of only 0.534339. The special shape of the graph for larger dimensions results from the fact that this modulus and therefore the number of points is very small. Hence for all dimensions $10 \leq s \leq 24$, the corresponding lattices consist of four hyper-planes only resulting in equal non-normalized spectral test values d_s . The right graphics in Figure 7 shows the spectral test behaviors of the best multiplier for modulus $m = 2^{26} - 5$. The course of the graph of the S_s values increases for higher dimensions resulting in high values for S'_s as well. Roughly spoken, if an achieved S_s value lies in the lower area of the corresponding spectral test distribution used for the new normalization (cf. Sect. 1.3), then the resulting S'_s value will be adjusted to a value lower than S_s , and if the S_s value lies in the upper area the new normalization results in $S'_s > S_s$. Generally, a parameter search using the new normalization method enables equally stable spectral test behavior with respect to a given threshold across low and high dimensions.

Figure 8 shows the time consumption for each search and a simple time complexity estimate. The shown values for the search times include both the serial and the parallel parts of the searches. Note that the serial part is only a minor fraction within a measured time. As the cluster may occasionally also be used by other research groups, the environment was not guaranteed to be unloaded

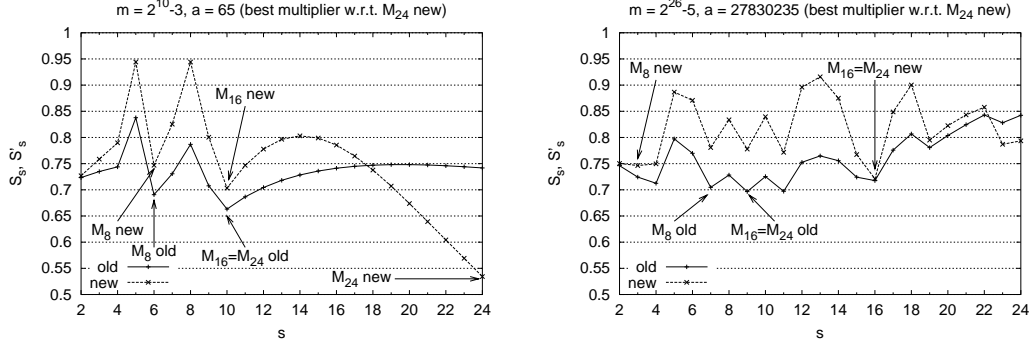


Fig. 7. Spectral test behaviors of two different multipliers and moduli.

during the searches.

Suppose we may assume a complexity of the LLL-algorithm of $O(s^4 \log(B))$, where $(\vec{b}_i^*)^2 \leq B$ for all input vectors $1 \leq i \leq s$ [20]. Since the dimension $k = 24$ for our search is fixed we may further assume that the search time for each modulus depends only on the LLL-complexity and the number of primitive roots considered for an exhaustive search. Therefore the computing time t_m may be estimated by $C \log(m) \phi(m - 1)$. Figure 8 exhibits a log-log plot of the time consumption measured and our estimated search time t_m using $C = 1/12000$.

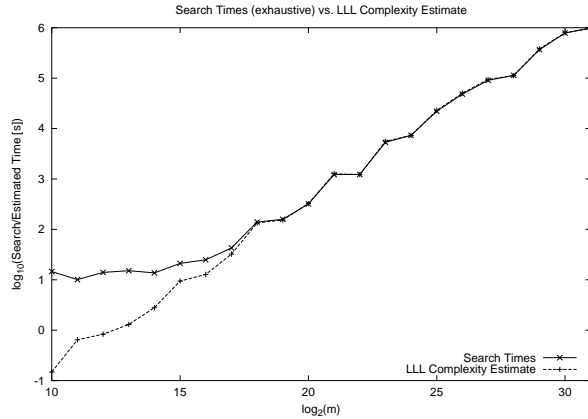


Fig. 8. Search times of exhaustive searches with regard to M_{24} new vs. LLL complexity estimate.

For selected values of $m > 2^{31}$ limited searches with 5 million search loops for each modulus have been conducted for dimension $k = 24$ with regard to the new normalization. The results are shown in Table 5.

Table 5
 Best multipliers a with regard to M_{24} new (limited search).

m	a	M_8 new M_8 old	M_{16} new M_{16} old	M_{24} new M_{24} old
$2^{32} - 5$	3045563030	0.684503 0.650929	0.684503 0.650929	0.659750 0.650929
$2^{33} - 9$	5680124861	0.671907 0.652010	0.671907 0.649141	0.671907 0.649141
$2^{34} - 41$	10262491661	0.642163 0.642150	0.640141 0.634300	0.640141 0.634300
$2^{35} - 31$	5175543096	0.664274 0.637140	0.641581 0.637140	0.636934 0.637140
$2^{36} - 5$	32976222090	0.635841 0.620643	0.635841 0.620643	0.635841 0.620643
$2^{37} - 25$	56904100967	0.694209 0.654094	0.611834 0.615198	0.611834 0.615198
$2^{38} - 45$	193003875090	0.652267 0.630387	0.648338 0.630387	0.648338 0.630387
$2^{39} - 7$	376030878980	0.612994 0.604904	0.612994 0.604904	0.612994 0.604904
$2^{40} - 87$	611344521011	0.663994 0.645850	0.645573 0.643085	0.631219 0.643085
$2^{41} - 21$	205511163269	0.628591 0.615300	0.627663 0.615300	0.627663 0.615300
$2^{42} - 11$	2772491921198	0.657837 0.634765	0.632493 0.634765	0.624052 0.634765
$2^{43} - 57$	3855359123495	0.666889 0.639705	0.606402 0.634651	0.606402 0.634651
$2^{44} - 17$	8695846065942	0.622722 0.611744	0.622722 0.611744	0.622722 0.611744
$2^{45} - 55$	10120380809261	0.672478 0.646729	0.620428 0.630280	0.620428 0.630280
$2^{46} - 21$	35838509495835	0.614844 0.606920	0.614844 0.606920	0.614330 0.606920
$2^{47} - 115$	29129223004279	0.645962 0.628084	0.601057 0.610220	0.593167 0.610220
$2^{48} - 59$	13129462975764	0.678201 0.665487	0.618082 0.624233	0.586649 0.624233
$2^{49} - 81$	453603124563892	0.596900 0.602381	0.596900 0.602381	0.596900 0.602381
$2^{50} - 27$	679446862235355	0.631693 0.618052	0.602649 0.618052	0.602649 0.618052
$2^{51} - 129$	1216895709316556	0.585842 0.585008	0.585842 0.585008	0.585842 0.585008
$2^{52} - 47$	4236078231021063	0.652165 0.636641	0.632916 0.631003	0.632916 0.631003
$2^{53} - 111$	119601990593847	0.599462 0.603742	0.599462 0.603742	0.599462 0.603742
$2^{54} - 33$	14587154633800445	0.579208 0.579964	0.579208 0.579964	0.579208 0.579964

(continued on next page)

Table 5

Best multipliers a with regard to M_{24} new (continued).

m	a	M_8 new M_8 old	M_{16} new M_{16} old	M_{24} new M_{24} old
$2^{55} - 55$	13020201480795502	0.628272 0.616252	0.577942 0.616252	0.577942 0.616252
$2^{56} - 5$	44978799721360948	0.573625 0.590012	0.573625 0.590012	0.573625 0.590012
$2^{57} - 13$	4169221353590777	0.716771 0.671491	0.602419 0.638990	0.602419 0.638990
$2^{58} - 27$	118841008606485922	0.594381 0.591655	0.593256 0.591655	0.584961 0.591655
$2^{59} - 55$	406769169513276072	0.665294 0.638728	0.593497 0.629396	0.593497 0.629396
$2^{60} - 93$	165445551279324735	0.583290 0.586433	0.583290 0.586433	0.583290 0.586433
$2^{61} - 1$	1894892306165295416	0.589985 0.598706	0.552224 0.598706	0.552224 0.598706
$2^{62} - 57$	3404837318038382571	0.586569 0.585574	0.575575 0.585574	0.564854 0.585574
$2^{63} - 25$	4647273892312704991	0.600056 0.604058	0.579089 0.599141	0.579089 0.599141
$2^{64} - 59$	16705617337514159602	0.655967 0.632745	0.575584 0.617794	0.575584 0.617794
$2^{127} - 1$	1398794276906193351\ 41502798742572336905	0.569414 0.577591	0.558320 0.577591	0.535361 0.577591
$2^{128} - 159$	1035233851360193574\ 24787461675565978903	0.615247 0.612131	0.609589 0.612131	0.535343 0.612131
$2^{256} - 189$	6267050806080154704\ 8264644292733107925\ 5412212727282634683\ 7533481987788608657	0.523400 0.541907	0.523400 0.541907	0.521277 0.541907

4 Conclusions

We used the spectral test with a new normalization strategy [1] to perform a large scale parallel parameter search for Korobov lattice rules. The new normalization method was chosen to identify parameters with equally stable behavior across low and high dimensions. The idea was to spread the relevant portion of the distributions of the classical normalized spectral test to zero and one for each dimension. The classical normalization constants have been found to give misleading results when comparing spectral test values across dimensions, for detailed examples see [1].

A selection of the parameters from this experiment is given in the article. The collection of all results of the conducted searches is also available electronically at the *Spectral Test Server* [22]. This Web-based application server

offers interactive access to a database, which contains detailed calculation results for many lattice rules, information about scientists working in the field of MC&QMC as well as many publication references. The server further provides the possibility to execute GLP search tasks according to the search algorithm described in Sect. 2.2 directly via a Web-browser in a single-threaded approach. In future work we will extend the parameter searches to rank- r rules and distribute the corresponding results at the Spectral Test Server as well.

Acknowledgments

The authors would like to kindly thank the High Performance Computing Group at the Department of Scientific Computing of the University of Salzburg, Austria, for support and access to their cluster. We further would like to thank the anonymous referees for several valuable comments and improvements.

References

- [1] K. Entacher, G. Laimer, H. Röck, A. Uhl, Normalization of the Spectral Test in High Dimensions, *Monte Carlo Methods and Applications*, **10** (3-4) (2004) 341 - 366.
- [2] N. Korobov, The approximate calculation of multiple integrals, *Dokl. Akad. Nauk SSSR* **124** (1959) 1207–1210, (in Russian).
- [3] N. Korobov, Properties and calculation of optimal coefficients, *Dokl. Akad. Nauk SSSR* **132** (1960) 1009–1012, (in Russian). English transl.: *Soviet Math. Dokl.*, **1**, 696–700.
- [4] N. Korobov, *Number-Theoretic Methods in Approximate Analysis*, Fizmatgiz, Moscow, 1963, (in Russian).
- [5] P. L’Ecuyer, Tables of linear congruential generators of different sizes and good lattice structure, *Math. Comp.* **68** (225) (1999) 249–260.
- [6] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.
- [7] P. L’Ecuyer, Random Number Generation, in: J. Banks (Ed.), *Handbook of Simulation*, Chapter 4, Wiley, 1998.
- [8] I. Sloan, S. Joe, *Lattice Methods for Multiple Integration*, Oxford Univ. Press, New York, 1994.
- [9] H. Niederreiter et al. (Eds.), *Monte Carlo and Quasi-Monte Carlo Methods 1996, 1998, 2000, 2002, 2004*, The series of proceedings for the conferences MCQMC 1996 - 2004, Springer Verlag.

- [10] K. Entacher, P. Hellekalek, P. L'Ecuyer, Quasi-Monte Carlo node sets from linear congruential generators, in: H. Niederreiter, J. Spanier (Eds.), Monte Carlo and Quasi-Monte Carlo Methods 1998, Springer, 2000, pp. 188–198.
- [11] P. Hellekalek, G. Larcher (eds.), Random and Quasi-Random Point Sets, Vol. **138** of Lecture Notes in Statistics, Springer, Berlin, 1998.
- [12] K. Entacher, T. Schell, A. Uhl, Efficient lattice assessment for LCG and GLP parameter searches, *Mathematics of Computation* **71** (239) (2001) 1231–1242.
- [13] C. Lemieux, P. L'Ecuyer, On selection criteria for lattice rules and other quasi-Monte Carlo point sets, *Mathematics and Computers in Simulation* **55** (2001) 139–148.
- [14] U. Fincke, M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Math. Comp.* **44** (1985) 463–471.
- [15] G. Fishman, Monte Carlo: Concepts, Algorithms, and Applications, Vol. 1 of Springer Series in Operations Research, Springer, New York, 1996.
- [16] D. Knuth, The Art of Computer Programming, 2nd Edition, Vol. 2: Seminumerical Algorithms, Addison-Wesley, Reading, MA, 1981.
- [17] P. L'Ecuyer, R. Couture, An implementation of the lattice and spectral tests for multiple recursive linear random number generators, *INFORMS Journal on Computing* **9** (2) (1997) 209–217.
- [18] G. Fishman, L. Moore, An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$, *SIAM J. Sci. Stat. Comput.* **7** (1986) 24–45, see erratum, *ibid.*, **7**:1058, 1986.
- [19] P. L'Ecuyer, Good Parameter Sets for Combined Multiple Recursive Random Number Generators, *Operations Research* **47** (1999) 159–164.
- [20] A. Lenstra, H. Lenstra, L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen* **261** (1982) 515–534.
- [21] L. Afflerbach, G. Gruber, Assessment of random number generators in high accuracy, in: S. Morito, H. Sakasegawa, M. Fushimi, K. Nakano (Eds.), *New Directions in Simulation for Manufacturing and Communications*, OR Society of Japan, 1994, pp. 128–133.
- [22] B. Hechenleitner, K. Entacher, Spectral Test Server, Salzburg University of Applied Sciences and Technologies, Austria, <http://spectral.fh-sbg.ac.at> (2004).