Searching for extensible Korobov rules

Hardeep S. Gill [a] and Christiane Lemieux [b,*,1]

[a] *Department of Mathematics, University of British Columbia*

[b] *Department of Statistics and Actuarial Science, University of Waterloo*

Dedicated to Prof. Henryk Woźniakowski on the occasion of his 60th birthday

Abstract

Extensible lattice sequences have been proposed and studied in [5–7]. For the special case of extensible Korobov sequences, parameters can be found in [6]. The searches made to obtain these parameters were based on quality measures that look at several projections of the lattice. Because it is often the case in practice that low-dimensional projections are very important, it is of interest to find parameters for these sequences based on measures that look more closely at these projections.

In this paper, we prove the existence of "good" extensible Korobov rules with respect to a quality measure that considers two-dimensional projections. We also report results of experiments made on different problems where the newly obtained parameters compare favorably with those given in [6].

Key words: lattice sequences, Korobov rules, highly-uniform point sets
2000 MSC: 11D45, 11K36, 65C05, 65D30

1 Introduction

Point sets and sequences that are more uniform than random ones are often used within various numerical methods, namely for multidimensional integra-

---

* Corresponding author.
Email addresses: `hsgill@math.ubc.ca` (Hardeep S. Gill), `clemieux@math.uwaterloo.ca` (Christiane Lemieux).

1 We thank the co-editor of this special issue and the anonymous referees for their helpful comments and suggestions. This work was funded by NSERC–Canada.

tion. More precisely, for an integral of the form

$$\int_{[0,1)^s} f(\mathbf{u}) d\mathbf{u}, \tag{1}$$

where f is a real-valued function, an approximation for (1) can be formed by using

$$\hat{\mu} = \frac{1}{n} \sum_{i=0}^{n-1} f(\mathbf{u}_i),$$

where $P_n = \{\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}\}$ is some point set in $[0,1)^s$. The *Monte Carlo method* amounts to choosing P_n randomly and uniformly, while using a *highly-uniform point set* (HUPS) is often referred to as the *quasi-Monte Carlo* method. Several practical problems can be formulated as (1), with a dimension s that can be quite large or even infinite. Other problems can benefit from the availability of HUPS or sequences, for instance optimization problems [11,17].

There are two main families of constructions used to generate HUPS: digital nets and lattice rules. A class of lattice rules that is often used in practice are *Korobov rules*. While digital nets often come from digital sequences containing an infinite number of points, lattice rules are generally built for a fixed number of points n. Point sets that come from a sequence are preferred for applications where the user may want to increase the number of points without discarding previous function evaluations. In an effort to make lattice rules useful in that context, Hickernell and Hong [5] proposed a method to construct *extensible lattice rules*, that is, infinite sequences of points that can be used to provide lattice rules. The construction is investigated further in [6,7], and more recently in [1,3]. In particular, parameters for extensible Korobov rules are given in [6]. These parameters were found by performing computer searches based on quality measures that assess the quality of different *projections* of the point set, but that do not put a special emphasis on low-dimensional projections. Because it is quite important that these low-dimensional projections be of good quality in practice, using quality measures that put more emphasis on those projections seems like a promising approach to perform parameter searches for extensible lattices.

This paper investigates this idea, both from a theoretical and practical point of view. More precisely, we look at a quality measure that can be used to put more emphasis on low-dimensional projections [4,15], and prove that for a special case of this measure where only two-dimensional projections are considered, there exist extensible Korobov rules that are "good" with respect to that measure. We then investigate empirically the quality of sequences of Korobov rules found using this measure.

The rest of this paper is organized as follows. In Section 2, we recall how extensible lattice rules are constructed. In Section 3, we describe the general quality measure considered in this paper, and prove the existence result mentioned above. In Section 4, we give numerical results where we compare the quality of rules obtained by a computer search based on the two-dimensional criterion studied in the previous section against other ones obtained in [6]. The comparison is done by looking at the empirical variance of the resulting estimators on two practical problems. A conclusion with ideas for future research is given in Section 5.

2 Background on lattice rules

Because of its widespread use in practice, the lattice construction we chose to study in this paper is a *Korobov rule* [9], which for a dimension s and a number of points n is defined by a *generator* a as follows:

$$P_n = \left\{ \frac{i}{n}(1, a \bmod n, a^2 \bmod n, \ldots, a^{s-1} \bmod n) \bmod 1 : i = 0, \ldots, n-1 \right\}. \tag{2}$$

This construction is a special case of a rank-1 lattice rule, which is determined by a generating vector $\mathbf{z} = (z_1, \ldots, z_s)$ as follows:

$$P_n = \left\{ \frac{i}{n}(z_1, \ldots, z_s) \bmod 1 : i = 0, \ldots, n-1 \right\}. \tag{3}$$

Here, it is assumed that each component z_j is between 1 and $n-1$, and usually we also have $\gcd(z_j, n) = 1$ so that the n coordinates $\{iz_j/n, i = 0, \ldots, n-1\}$ are distinct.

To explain how extensible lattice rules are constructed, we follow [6]. First, we recall the definition of the *radical-inverse function* φ_b: for $b \geq 2$, let n be a non-negative integer and consider its unique digit expansion in base b given by

$$n = \sum_{i=0}^{\infty} a_i b^i, \tag{4}$$

where $0 \leq a_i < b$, and $a_i = 0$ for all sufficiently large i, i.e., the sum in (4) is actually finite. Then we have

$$\varphi_b(n) = \sum_{i=0}^{k} a_i b^{-i-1}.$$

Now, to define extensible rank-1 lattice rules, we need to remove the dependence on n in the definition (3) of a rank-1 lattice. First, as pointed out in [6], if the number of points n in (3) is a power of some integer $b \geq 2$, then we can replace i/n in that definition by $\varphi_b(i)$, and get the same point set, but with the points generated in a different order. Second, the generating vectors used for extensible rules should not depend on n. Therefore, we can assume that each component z_j has a base b expansion of the form $z_j = \ldots z_{j2}z_{j1}$. That is, we write $z_j = \sum_{l=1}^{\infty} z_{jl}b^{l-1}$.

We can now define an infinite rank-1 lattice sequence based on the generating vector $\mathbf{z}$ as

$$\{\varphi_b(i)\mathbf{z} \bmod 1 : i = 0, 1, 2, \ldots\}.$$

Hence, such sequences are entirely determined by the integer vector $\mathbf{z}$, which in case of a Korobov sequence amounts to choosing an integer a, as $\mathbf{z} = (1, a, a^2, \ldots, a^{s-1})$. It is easy to see that for any $m \geq 1$, the first b^m points produced by this sequence correspond to a rank-1 lattice with generating vector $\mathbf{z}_m = (z_1 \bmod b^m, \ldots, z_s \bmod b^m) = (z_{1m} \ldots z_{12}z_{11}, \ldots, z_{sm} \ldots z_{s2}z_{s1})$. Hence the first b^m points do not depend on the digits z_{jk} of the generating vector for $k > m$.

3 An Existence Result for Extensible Korobov Rules

As seen in the previous section, to construct extensible Korobov rules, we simply need to select a generator a. In order to do this, we need to choose a search criterion that can be used to assess the quality of the Korobov point sets of different sizes defined by a given generator. In this section, we introduce the general quality measure that will be used for this purpose, and then show that for a special case of that measure, there exist "good" extensible Korobov rules, i.e., for which that quality measure behaves asymptotically better than for a random point set.

Before we proceed to the definition of this quality measure, we need to introduce some notation and recall some definitions. First, in what follows we will be working with the $b-$adic integers as in [7]. Let $\mathbb{Z}_b$ be the set of all $b-$adic integers $i = \sum_{l=1}^{\infty} i_l b^{l-1}$, where $i_l \in \{0, 1, \ldots, b-1\}$ for all $l \geq 1$. Then define $A_b = \{i \in \mathbb{Z}_b : \gcd(i_1, b) = 1\}$. We will be looking at generating vectors of the form $\mathbf{z} = (1, a, a^2, \ldots) \in A_b^{\infty} = A_b \times A_b \times \cdots$ for extensible Korobov rules, i.e., vectors that can be used for an arbitrary large dimension s. Also, for a given n, we denote by $A_{b,n} = \{a \in A_b : 1 \leq a < n\}$ the set of admissible generators a.

For lattice point sets, a quality measure that is widely used is the *weighted* $\mathcal{P}_\alpha$ [4], which for a point set of size n in dimension s generated by a, is defined as

$$\mathcal{P}_{\alpha,n,s}(a) = \sum_{\mathbf{0} \neq \mathbf{h} : \mathbf{h} \cdot \mathbf{a} \equiv 0 \bmod n} \gamma_{I_{\mathbf{h}}} \|\mathbf{h}\|^{-\alpha}, \tag{5}$$

where $\mathbf{h} \cdot \mathbf{a} = h_1 + h_2 a + + \ldots + h_s a^{s-1}$, $I_{\mathbf{h}} = \{j : h_j \neq 0, 1 \leq j \leq s\}$, $\{\gamma_I, \emptyset \neq I \subseteq \{1, \ldots, s\}\}$ is a set of weights, $\|\mathbf{h}\| = \prod_{i=1}^{s} \bar{h}_i$, and $\bar{h} = \max(1, |h|)$. In what follows, we will make use of the fact that

$$\mathcal{P}_{\alpha,n,s}(a) = \sum_{I} \gamma_I \mathcal{P}_{\alpha,n,s,I}(a),$$

where $\mathcal{P}_{\alpha,n,s,I}(a)$ is the value of the measure $\mathcal{P}_{\alpha,n,|I|}(a)$ for the projection of the Korobov point set (2) over I when all weights are set to 1 (i.e., this is the unweighted $\mathcal{P}_\alpha$ as studied, for example, in [14]). That is, for $I = \{i_1, \ldots, i_t\} \subseteq \{1, \ldots, s\}$,

$$\mathcal{P}_{\alpha,n,s,I}(a) = \sum_{\substack{\mathbf{0} \neq \mathbf{h} \in \mathbb{Z}^t, \\ \mathbf{h} \cdot \mathbf{a}_I \equiv 0 \bmod n}} \|\mathbf{h}\|^{-\alpha},$$

where $\mathbf{h} \cdot \mathbf{a}_I = h_1 a^{i_1 - 1} + \ldots + h_t a^{i_t - 1}$.

Of special interest in this paper are versions of the weighted $\mathcal{P}_\alpha$ with *finite-order weights*, which are studied in [15] in the context of tractability of multivariate integration over Korobov spaces. That is, we consider versions of $\mathcal{P}_{\alpha,n,s}(a)$ where all weights γ_I are zero when $|I| > q$ for some order $q \in \{1, \ldots, s\}$. In particular, we consider here the finite-order weighted $\mathcal{P}_\alpha$ measure with order $q = 2$. Also, since Korobov point sets are dimension-stationary [10], in our case the order-2 weighted $\mathcal{P}_\alpha$ can be written as

$$\mathcal{M}_{\alpha,n,s}(a) := \sum_{k=2}^{s} \gamma_{\{1,k\}} \mathcal{P}_{\alpha,n,s,\{1,k\}}(a). \tag{6}$$

Note that by setting $\gamma_{\{1,k\}}$ in (6) to

$$\sum_{l=1}^{s-k+1} \gamma_{\{l,l+k-1\}} \tag{7}$$

the criterion (6) becomes equivalent to the order-2 version of (5), where all two-dimensional projections are included in the sum. Using this equivalence, one can more easily put our results into the framework of [15].

We can now present our first result, which states that for any $n = b^m$, where b is some prime, any dimension s, and any $\alpha > 1$, we can find a generator a for which the criterion $\mathcal{M}_{\alpha,n,s}(a)$ is bounded by a constant over n. At first sight, this may seem like a weak result, but as in [16], Jensen's inequality can be used to improve the behavior of this bound with respect to n. This approach is used in our second result, where we prove the existence of a generator a that can define a "good" sequence of Korobov rules, i.e., an a for which the criterion $\mathcal{M}_{\alpha,n,s}(a)$ is $O(n^{-v} \log^c n)$ for some $v > 1$. This is done using an approach very similar to the one presented in [7, Theorem 2], in combination with Jensen's inequality. Note however that by contrast with [7], the existence result proved here is for the particular case of Korobov rules rather than the more general rank-1 rules (proofs based on averaging arguments as those used here are typically easier in the latter case), and is also based on a different quality measure.

Proposition 1. *Given $n = b^m$, b prime, $\alpha > 1$, and $s \geq 1$, there exists a Korobov lattice rule generator a^* such that*

$$\mathcal{M}_{\alpha,n,s}(a^*) \leq c(\alpha, s)n^{-1},$$

where $c(\alpha, s)$ is a constant with respect to n.

Proof. The proof proceeds by finding a bound on the average value of $\mathcal{M}_{\alpha,n,s}(a)$ over all generators a. Note that similar bounds for Korobov rules can be found elsewhere (e.g., [11,16]), but the approach used here is somewhat different as n is a power of a prime.

Define

$$\bar{M}_{\alpha,n,s} = \frac{1}{|A|} \sum_{a \in A} \mathcal{M}_{\alpha,n,s}(a),$$

where we dropped the subscripts in $A_{b,n}$ to ease the notation. Because $n = b^m$, it holds that $\gcd(a, b) = 1$ for all $a \in A$, and thus $|A| = \phi(n) = n(1 - 1/b)$. Next, we use the notation $\delta_n(l) = 1$ if $n|l$, and 0 otherwise. We then expand the sums in the definition of $\mathcal{M}_{\alpha,n,s}(a)$ and use the fact that for $\alpha > 1$, $\sum_{\mathbf{0} \neq \mathbf{h} \in \mathbb{Z}^2} \|\mathbf{h}\|^{-\alpha} \delta_n(\mathbf{h} \cdot (1, a^{k-1}))$ converges absolutely for all $a \in A_{b,n}$, to get:

$$\bar{M}_{\alpha,n,s} = \frac{1}{|A|} \sum_{k=2}^{s} \gamma_{\{1,k\}} \sum_{\mathbf{0} \neq \mathbf{h} \in \mathbb{Z}^2} \sum_{a \in A} \frac{\delta_n(\mathbf{h} \cdot (1, a^{k-1}))}{\|\mathbf{h}\|^{\alpha}}.$$

Hence, we must obtain a bound on the number of $a \in A$ satisfying $\delta_n(\mathbf{h} \cdot (1, a^{k-1})) = 1$ for a given $\mathbf{h} \in \mathbb{Z}^2$ and k. Equivalently, we need to find the number of $a \in A$ satisfying $h_1 + h_2 a^{k-1} \equiv 0 \bmod n$.

This problem can be solved in two steps. First, we find the number of solutions of $h_1 + h_2 x \equiv 0 \bmod n$ that lie in $\{0, \ldots, n-1\}$. Next we use Propositions 4.2.2 and 4.2.3 in [8] to bound the number of solutions to the equivalence $a^{k-1} \equiv x_0 \bmod n$ for each solution x_0 of the equivalence in the first step.

Now, a solution x_0 for the first equivalence exists only if $d|(-h_1)$, where $d = \gcd(h_2, n)$, and in that case, there is a total of d solutions. Note that d has to be of the form b^i for some $0 \leq i \leq m$ because $n = b^m$. In addition, using the fact that x_0 must be such that a solution exists to the second equivalence, it can be proved that $\mathbf{h}$ must satisfy $\gcd(h_1, n) = \gcd(h_2, n)$. Hence

$$\bar{M}_{\alpha,n,s} = \frac{1}{|A|} \sum_{k=2}^{s} \gamma_{\{1,k\}} \sum_{\mathbf{h} \in L'} \sum_{a \in A} \frac{\delta_n(h_1 + h_2 a^{k-1})}{\|\mathbf{h}\|^{\alpha}},$$

where $L' = \{\mathbf{h} \in \mathbb{Z}^2 \backslash \mathbf{0} : \gcd(h_1, n) = \gcd(h_2, n)\}$. Next, we decompose the set

L' as $L' = \cup_{0 \le q \le m} L_q$, where for $0 \le q \le m$,

$$L_q = \{\mathbf{h} \in \mathbb{Z}^2 \backslash \mathbf{0} : b^q = \gcd(h_1, n) = \gcd(h_2, n)\}.$$

We also define

$$\Gamma_k = \sum_{\mathbf{h} \in L'} \sum_{a \in A} \frac{\delta_n(h_1 + h_2 a^{k-1})}{\|\mathbf{h}\|^\alpha} = \sum_{0 \le q \le m} \sum_{\mathbf{h} \in L_q} \sum_{a \in A} \frac{\delta_n(h_1 + h_2 a^{k-1})}{\|\mathbf{h}\|^\alpha}.$$

So for each $\mathbf{h} \in L_q$, there are b^q solutions to $h_1 + h_2 x \equiv 0 \bmod n$. Next, for each solution x_0 we can find an upper bound—denoted $d_b(k)$—on the number of solutions $a \in A$ to the equivalence $a^{k-1} \equiv x_0 \bmod n$, where $1 \le k \le s$.

First, if $b = 2$, then $d_2(k) = 2\gcd(k-1, 2^{m-2})$ by Proposition 4.2.2 in [8]. If $b > 2$, then $d_b(k) = \gcd(k-1, n(1-1/b))$, by Proposition 4.2.3 in [8]. Note that the value $d_b(k)$ is at most $2(k-1)$, and occurs when $b = 2$ and $k = 2^e + 1$ for some $e < m - 1$.

We now have that

$$\Gamma_k \le d_{b,s} \sum_{0 \le q \le m} b^q \sum_{\mathbf{h} \in L_q} \frac{1}{\|\mathbf{h}\|^\alpha},$$

where $d_{b,s} = \max_{2 \le k \le s} d_b(k)$. Next, we get the following bound for $0 \le q < m$:

$$\sum_{\mathbf{h} \in L_q} \frac{1}{\|\mathbf{h}\|^\alpha} \le \left(\sum_{l \ne 0} \frac{1}{(l b^q)^\alpha} \right)^2 = \frac{1}{b^{2q\alpha}} 4\zeta^2(\alpha).$$

Similarly, we can find a bound of $4b^{-2m\alpha}(\zeta(\alpha)+1)^2$ for the case $q = m$. Hence we get that

$$\Gamma_k \le 4 d_{b,s} (\zeta(\alpha)+1)^2 \sum_{0 \le q \le m} \frac{1}{b^{q(2\alpha-1)}} = 4 d_{b,s} (\zeta(\alpha)+1)^2 \frac{1 - (nb)^{1-2\alpha}}{1 - b^{1-2\alpha}} \le \beta(\alpha, s),$$

where $\beta(\alpha, s) = 4 d_{b,s} (\zeta(\alpha)+1)^2 (1 - b^{1-2\alpha})^{-1}$. Therefore

$$\bar{M}_{\alpha,n,s} = \frac{1}{|A|} \sum_{k=2}^{s} \gamma_{\{1,k\}} \Gamma_k \le \frac{1}{n(1-1/b)} \sum_{k=2}^{s} \gamma_{\{1,k\}} \beta(\alpha, s),$$

and by letting $c(\alpha, s) = \beta(\alpha, s) W_s (1 - 1/b)^{-1}$, where $W_s = \sum_{k=2}^{s} \gamma_{\{1,k\}}$, we get the desired result. $\square$

Note that the behavior of $c(\alpha, s)$ with respect to s depends on the size of the bound W_s on the sum of the weights $\gamma_{\{1,k\}}$. For instance, if we make the assumption that each $\gamma_{\{1,k\}}$ is bounded by 1, then W_s is $O(s)$ and $c(\alpha, s)$ is $O(s^2)$, since $d_{b,s}$ is bounded by $2(s-1)$. If the weights $\gamma_{\{1,k\}}$ arise as sums of weights as in (7) (which are derived from the order-2 version of the criterion

(5) that considers all two-dimensional projections), then W_s is $O(s^2)$, which still yields a function $c(\alpha, s)$ that is polynomial in s.

We can now present our main result:
Proposition 2. *For any prime b, $\alpha > 1$, $v \in [1, \alpha)$, and $\epsilon > 0$, there exists a generator a such that*

$$\mathcal{M}_{\alpha,n,s}(a) \leq k^*(s, \epsilon)[\log(\log(n) + 1)]^{v(1+\epsilon)}(\log(n)n^{-1})^v$$

for $n = b, b^2, \ldots$, and $s = 1, 2, \ldots$, where $k^*(s, \epsilon)$ is a constant with respect to n.

Proof. The proof follows closely that of Theorem 2 in [7]. As in [7], let μ be a probability measure on the set $\mathbb{Z}_b$ for which the set of all $i \in \mathbb{Z}_b$ with specified first l digits has measure b^{-l}. This probability measure, conditional on the set A_b, is denoted μ_b.

From Proposition 1, we have that for any fixed $m \geq 0, s > 0$,

$$\bar{M}_{\alpha,b^m,s} = \int_{A_b} \mathcal{M}_{\alpha,b^m,s}(a) d\mu_b(a) \leq c(\alpha, s)n^{-1} =: \tilde{M}(\alpha, m, s).$$

We then use this result to define sets of "bad" generating vectors. More precisely, let

$$G_{b,m,s} = \{a \in A_b : \mathcal{M}_{\alpha,b^m,s}(a) \geq c_m c_s \tilde{M}(\alpha, m, s)\},$$

where $c_j = c_j(\epsilon) = c_0(\epsilon)j[\log(j + 1)]^{1+\epsilon}$, $j \geq 1$, and

$$c_0(\epsilon) > \sum_{k=1}^{\infty} k^{-1}[\log(k + 1)]^{-1-\epsilon}.$$

Then $\mu_b(G_{b,m,s}) < 1/(c_m c_s)$ because

$$\begin{aligned}\mu_b(G_{b,m,s})c_m c_s \tilde{M}(\alpha, m, s) &\leq \int_{G_{b,m,s}} \mathcal{M}_{\alpha,b^m,s}(a) d\mu_b(a) \\ &\leq \int_{A_b} \mathcal{M}_{\alpha,b^m,s}(a) d\mu_b(a) = \tilde{M}(\alpha, m, s).\end{aligned}$$

Now let $G_b = \bigcup_{m=1}^{\infty} \bigcup_{s=1}^{\infty} G_{b,m,s}$. Then

$$\begin{aligned}\mu_b(G_b) =&\mu_b\left(\bigcup_{m=1}^{\infty} \bigcup_{s=1}^{\infty} G_{b,m,s}\right) \leq \sum_{m=1}^{\infty} \sum_{s=1}^{\infty} \mu_b(G_{b,m,s}) \\ =&c_0^{-2}(\epsilon) \sum_{m=1}^{\infty} \sum_{s=1}^{\infty} \frac{1}{ms(\log(m + 1)\log(s + 1))^{1+\epsilon}} < 1\end{aligned}$$

by the definition of $c_0(\epsilon)$. Thus $\mu_b(A_b \backslash G_b) > 0$, and so there exists at least one

$a^* \in A_b$ such that for all s, m, we have

$$\begin{aligned}\mathcal{M}_{\alpha,b^m,s}(a^*) < & \, c_m c_s \tilde{M}(\alpha, m, s) \\ =& c(\alpha, s) c_0^2(\epsilon) s \log(n) [\log(s+1) \log(\log(n)+1)]^{1+\epsilon} n^{-1} \\ =& k(\alpha, s, \epsilon) \log(n) [\log(\log(n)+1)]^{1+\epsilon} n^{-1},\end{aligned}$$

where $k(\alpha, s, \epsilon) = c(\alpha, s) c_0^2(\epsilon) s$. As in [16], we can now apply Jensen's inequality to show that

$$\mathcal{M}_{\alpha,n,s}(a) \leq (\mathcal{M}_{\alpha\nu,n,s}(a))^{1/\nu}$$

for some $\nu \in (1/\alpha, 1]$, where the weights in $\mathcal{M}_{\alpha\nu,n,s}(a)$ are obtained by raising to the power ν the weights in $\mathcal{M}_{\alpha,n,s}(a)$. Hence for some a^* and for all s, m, we have that

$$\begin{aligned}\mathcal{M}_{\alpha,b^m,s}(a^*) \leq & (k(\alpha\nu, s, \epsilon)(\log(n)[\log(\log(n)+1)]^{1+\epsilon} n^{-1})^{1/\nu} \\ =& k^*(s, \epsilon)[\log(\log(n)+1)]^{(1+\epsilon)/\nu} (\log(n) n^{-1})^{1/\nu},\end{aligned}$$

where $k^*(s, \epsilon) = (k(\alpha\nu, s, \epsilon))^{1/\nu}$. Setting $v = 1/\nu$ gives the desired result. □

4 Numerical Results

Using the quality measure $\mathcal{M}_{\alpha,n,s}(a)$, we can now define a criterion to be used for computer searches of "good" generators a. To do so, we must choose a dimension s and an integer m_1 that will define the range of point set sizes considered. That is, the criterion will measure the quality of each potential generator a by computing $\mathcal{M}_{\alpha,n,s}(a)$ for $n = b, b^2, \ldots, b^{m_1}$, and divide it by a scaling factor as in [6]. Definition 1 describes the criterion $\hat{G}_{m_1,s}(a)$ used in our searches.

Definition 1. *Let* $\hat{G}_{m_1,s}(a) = \max_{1 \leq m \leq m_1} G_{m,s}(a)$*, where*

$$G_{m,s}(a) = \frac{\mathcal{M}_{\alpha,b^m,s}(a)}{b^{-m}(1 + m \log b)^{1/2}}.$$

In the following experiments, we restrict our attention to the case $b = 2$. Also, we choose $\alpha = 2$ and use weights of the form $\gamma_{\{1,k\}} = \gamma^{k-2}$ for some $\gamma \in (0, 1)$. In Figure 1, we show in the left table the generators a obtained with $s = 32$ and different values of m_1 and γ, while in the right table, we fix $m_1 = 15$ and $\gamma = 0.8$, and list the generators obtained for varying dimensions s.

To test the adequacy of our quality measure, we pick one of the generators ($a = 14471$) from Figure 1, use it to construct estimators for different problems, and compute the standard error obtained on these estimators. More precisely, for

$m_1 \backslash \gamma$	0.8	0.9
10	141	221
15	14471	733
17	14471	733
19	550777	15651

s	a^*	$\hat{G}_{m_1,s}(a^*)$
4	14181	20.4147
8	12861	35.6468
16	14471	44.8125
32	14471	46.4659

Fig. 1. Best choices of a: (left) when $s = 32$; (right) when $m_1 = 15$

a Korobov point set P_n generated by a, we use a random shift Δ uniformly distributed in $[0, 1)^s$ as in [2], and construct the estimator

$$\hat{\mu} = \frac{1}{n} \sum_{\mathbf{u}_i \in P_n} f((\mathbf{u}_i + \Delta) \bmod 1).$$

We repeat this procedure $m = 100$ times with independent shifts, thus obtaining m independent estimators $\hat{\mu}_1, \ldots, \hat{\mu}_{100}$. We then compute the standard error

$$\left(\frac{1}{m(m-1)} \sum_{i=1}^{m} (\hat{\mu}_i - \bar{\mu})^2 \right)^{1/2},$$

where $\bar{\mu}$ is the average of the $\hat{\mu}_i$'s.

In Figure 2, we compare the standard error obtained for an Asian option pricing problem (see, e.g., [10] for the details) by the generator $a = 14471$ obtained using $\hat{G}_{17,32}$ with $\gamma = 0.8$, against the generators 17797 and 11335 listed in [6], which were based on criteria assessing the quality of a over the same range ($s \leq 32$ and $m \leq 17$). The parameters for the option are $s = 32$ prices entering the mean, an initial asset value of 100, a strike price of 100, a risk-free interest rate of 0.05, and a volatility of 0.2. Also shown on that figure is the Monte Carlo standard error obtained for some values of n.

Similar experiments were conducted using digital option pricing as in [13], this time with $s = 128$. Results are shown in Figure 3. Note that although the generators used in this experiment were found based on a criterion where $s = 32$, they provide estimators that perform much better than Monte Carlo even if $s = 128$ for this problem, and the generator $a = 14471$ still outperforms the other two for values of $n > 512$.

5 Conclusion

In this paper we proved the existence of good extensible Korobov rules with respect to an order-2 weighted $\mathcal{P}_\alpha$ criterion. We also provided numerical re-

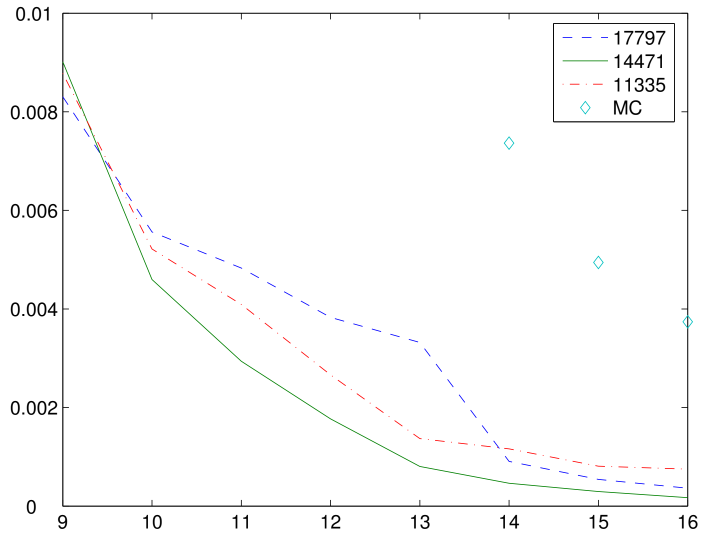

Fig. 2. Standard errors for Asian option pricing

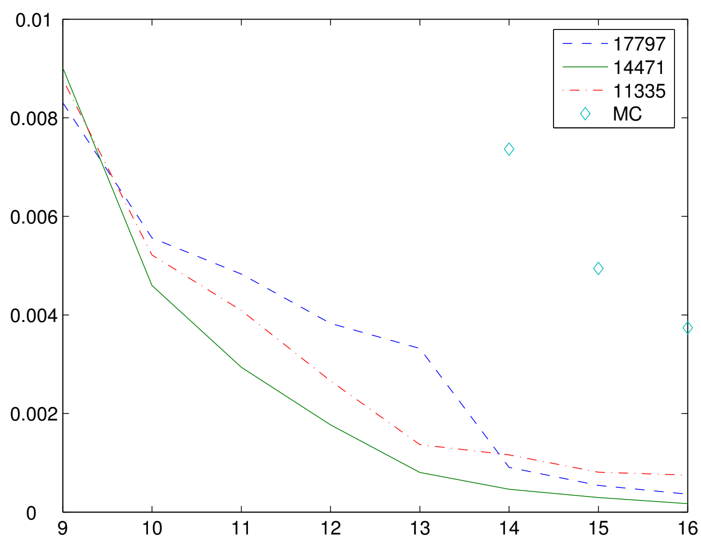

Fig. 3. Standard errors for digital option pricing

sults suggesting that rules found with this criterion can outperform previously published rules.

For future research, an obvious goal to pursue would be to prove the existence of good rules with respect to a criterion of order $q > 2$. We believe this will be mathematically challenging since bounds on the number of equations for congruences with more than one term are not readily available. In addition, it would be interesting to compare the Korobov rules obtained in this paper with extensible rank-1 rules given in [1,3], and to study how the approach used in

[3] could be applied in our setting to find generators satisfying our existence result. Finally, we would like to establish results similar to those presented in this paper, but for extensible *polynomial* Korobov rules. Existence results in that case are given in [12], but to our knowledge, no parameters have been published so far.

References

[1] R. Cools, F. Y. Kuo, and D. Nuyens. Constructing embedded lattice rules for multivariate integration. *SIAM J. Sci. Comput.*, 28(6):2162–2188, 2006.

[2] R. Cranley and T. N. L. Patterson. Randomization of number theoretic methods for multiple integration. *SIAM J. Numer. Anal.*, 13(6):904–914, 1976.

[3] J. Dick, F. Pillischammer, and B. Waterhouse. The construction of good extensible rank-1 lattices. To appear in Math. Comp.

[4] F. J. Hickernell. Lattice rules: How well do they measure up? In P. Hellekalek and G. Larcher, editors, *Random and Quasi-Random Point Sets*, volume 138 of *Lecture Notes in Statistics*, pages 109–166. Springer, New York, 1998.

[5] F. J. Hickernell and H. S. Hong. Computing multivariate normal probabilities using rank-1 lattice sequences. In G. H. Golub, S. H. Lui, F. T. Luk, and R. J. Plemmons, editors, *Proceedings of the Workshop on Scientific Computing (Hong Kong)*, pages 209–215, Singapore, 1997. Springer-Verlag.

[6] F. J. Hickernell, H. S. Hong, P. L'Ecuyer, and C. Lemieux. Extensible lattice sequences for quasi-Monte Carlo quadrature. *SIAM J. Sci. Comp.*, 22:1117–1138, 2001.

[7] F. J. Hickernell and H. Niederreiter. The existence of good extensible rank-1 lattices. *J. Complexity*, 19:286–300, 2003.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, second edition, 1998.

[9] N. M. Korobov. The approximate computation of multiple integrals. *Dokl. Akad. Nauk SSSR*, 124:1207–1210, 1959. In Russian.

[10] P. L'Ecuyer and C. Lemieux. Variance reduction via lattice rules. *Management Science*, 46(9):1214–1235, 2000.

[11] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*, volume 63 of *SIAM CBMS-NSF Regional Conference Series in Applied Mathematics.* SIAM, Philadelphia, 1992.

[12] H. Niederreiter. The existence of good extensible polynomial lattice rules. *Monatshefte für Mathematik*, 139:295–307, 2003.

[13] A. Papageorgiou. The brownian bridge does not offer a consistent advantage in quasi-Monte Carlo integration. *J. Complexity*, 18(1):171–186, 2002.

[14] I. H. Sloan and S. Joe. *Lattice Methods for Multiple Integration*. Clarendon Press, Oxford, 1994.

[15] I. H. Sloan, X. Wang, and H. Woźniakowski. Finite-order weights imply tractability of multivariate integration. *J. Complexity*, 20:46–74, 2004.

[16] X. Wang, I. H. Sloan, and J. Dick. On Korobov lattice rules in weighted Korobov spaces. *SIAM J. Numer. Anal.*, 42:1760–1779, 2004.

[17] S. Yakowitz, P. L'Ecuyer, and F. Vazquez-Abad. Global stochastic optimization with low-dispersion point sets. *Operations Research*, 48(6):939–950, 2000.