MATHEMATICS OF COMPUTATION
Volume 85, Number 300, July 2016, Pages 1821–1835
http://dx.doi.org/10.1090/mcom3047
Article electronically published on January 7, 2016

GOOD LOW DEGREE RANK-1 LATTICE RULES OF HIGH DIMENSION

TOR SØREVIK

In memory of James N. Lyness

Abstract. In this paper we introduce a novel approach to searching for rank-1 lattice rules. The idea is to separate the search into two steps, first finding good generating vectors and then finding the corresponding optimal N value. For the trigonometric degree $\delta = 5$ we establish a simple criterion on the generating vectors. By using the theory for Golomb rulers and $\mathcal{B}_2$-series we construct efficient algorithms for finding good generating vectors. Combined with our own home-brewed algorithm for finding the corresponding optimal N, we produce new good rank-1 lattice rules of high dimension.

1. Introduction

Lattice rules are equal-weighted cubature rules for the approximation of s-dimensional integrals over the unit cube. Lattice rules were introduced by I. Sloan et al. [21–23] as a generalization of the *number theoretic rules* by Hlawka [9] and Korobov [11]. While lattice rules are easy to describe, it has proven difficult to find the optimal ones. Huge computer resources has been devoted to searching for optimal lattice rules [2,4,10,13,14,16], and for higher dimensions or high trigonometric degrees, a search strategy narrowing the number of lattices is necessary [3,15,18,24].

In this paper we present a new search strategy and use it to compute new lattice rules of low degree in several dimensions. We will restrict our search to rank-1 lattice rules, which may be expressed as

$$Qf = \frac{1}{N} \sum_{j=0}^{N-1} f\left(\left\{j \frac{\mathbf{x}}{N}\right\}\right). \tag{1.1}$$

The vector $\mathbf{x}$ is called the *generating vector*, and $\{\mathbf{x}\}$ means its fractional part. We may limit ourselves to generating vectors where all components are positive integers less than N. Moreover it is standard to request that at least one of the components be mutually prime to N, and consequently it can be replaced by unit. Permuting the components of the vector $\mathbf{x}$ creates a symmetric copy of the lattice with the same fundamental properties, including trigonometric degree. The restriction to $1 \le x_1 \le x_2 \le \cdots \le x_{s-1} < N$ is hence no limitation. We may thus without loss of generality let $\mathbf{x} = (1, x_2, \cdots, x_s) \in \mathbb{N}^s$.

Received by the editor February 27, 2014 and, in revised form, October 29, 2014 and January 7, 2015.

2010 *Mathematics Subject Classification.* Primary 65D32; Secondary 42A10.

Key words and phrases. Optimal lattice rules, trigonometric degree, Golomb rulers.

Definition 1.1. A cubature rule Q is of enhanced trigonometric degree $\delta(Q)$ if it integrates exactly all trigonometric polynomials of degree δ and there is at least one trigonometric polynomial of degree $\delta+1$ which is not integrated exactly.

The trigonometric degree of a lattice rule may be computed as

$$\delta(Q) = \min_{\mathbf{p}\in\Lambda^\perp\setminus\{0\}} ||\mathbf{p}||_1 \tag{1.2}$$

where $\Lambda^\perp$ is the dual lattice

$$\Lambda^\perp = \{\mathbf{p} \mid \mathbf{p}^T\mathbf{z} \in \mathbb{Z} \text{ for } \mathbf{z}\in\Lambda\}. \tag{1.3}$$

For lattice rules to be good for 1-periodic integrands the lattice itself needs to be 1-periodic. Lattices with this property are called *integration lattices*. For integration lattices we have $\mathbb{Z}^s \subset \Lambda$ and $\Lambda^\perp \subset \mathbb{Z}^s$. For rank-1 lattices we then have

$$\mathbf{p}^T\mathbf{z} = \mathbf{p}^T\left\{j\frac{\mathbf{x}}{N}\right\} \in \mathbb{Z}, \tag{1.4}$$

which is equivalent to

$$\mathbf{p}^T\mathbf{x} = kN, \qquad k\in\mathbb{Z}. \tag{1.5}$$

Letting $\mathbf{p} = (\lambda_1,\cdots,\lambda_s)^T$ and remembering $x_1 = 1$, admissible $\mathbf{p}$ may be written as

$$\mathbf{p}^T = \left(kN - \sum_{j=2}^{s}\lambda_j x_j, \lambda_2, \cdots, \lambda_s\right); \tag{1.6}$$

relabeling k as $-\lambda_1$ and inserting into (1.2) we obtain

$$\delta(Q) = \min_{\lambda\in\mathbb{Z}^s\setminus\{0\}} \left|\sum_{j=2}^{s}\lambda_j x_j + \lambda_1 N\right| + \sum_{j=2}^{s}|\lambda_j|. \tag{1.7}$$

This is the operational definition we will use for the trigonometric degree. As the quantity to minimize must hold for all $\lambda\in\mathbb{Z}^s\setminus\{0\}$ it must in particular hold for λ with $\lambda_1 = 0$. Thus a necessary condition $\mathbf{x}$ must satisfy is

$$\delta(Q) \le \min_{\lambda\in\mathbb{Z}^{s-1}\setminus\{0\}} \left|\sum_{j=2}^{s}\lambda_j x_j\right| + \sum_{j=2}^{s}|\lambda_j|. \tag{1.8}$$

This expression has no reference to N, and for that reason it suggests a two-step procedure when searching for good rank-1 lattice rules. We may first find a set of vectors satisfying (1.8), and then find the minimal N for this set.

For a search of good lattice rules in high dimension and/or of high degree, a full enumeration will quickly exhaust all computational resources. Thus it is necessary to restrict our search space further before proceeding. In Section 2 we develop some simple lemmas which provide bounds useful for restricting the search space. In Section 3 we introduce the concept of δ-sequences and describe the general algorithm which we use to compute a few new optimal lattice rules. However, the search space increases exponentially, and consequently we are prohibited from taking this approach to really high dimensions. We therefore seek new ways of restricting the search. In Section 4 we prove a key property of δ-sequences of

degree 5, and in Sections 5 and 6 we point out an interesting connection to Golomb rulers. We believe this to be the most interesting part of this paper. This connection gives us access to the full arsenal of Golomb ruler tools in our quest for good δ-sequences. In Section 7 we discuss efficient ways to find the optimal N for a fixed δ-sequence. In particular we show how to use the relationship between the family of δ-sequences produced by the same circulant Golomb ruler to speed up the computation of N. The numerical results are reported in Section 8.

2. Limiting the search

Not only permuting the components of the generating vector creates symmetric copies of the lattice. Symmetric copies are also made by changing sign of one or more of the components. Lattices which are symmetric copies of each other share all basic properties, such as the trigonometric degree. Thus the search space will be reduced if we can avoid checking lattices which are symmetric copies of one another.

Theorem 2.1. *Every N-point rank one lattice rule has a symmetric copy with generating vector $\mathbf{x}$ satisfying*

$$1 \le x_2 \le \cdots \le x_s \le N/2. \tag{2.1}$$

Proof. Replacing a component x_k by $-x_k$ corresponds to replacing it with $N - x_k$ due to the modulo operation. Thus any $x_k > N/2$ can be replaced by $N - x_k$ to obtain a symmetric equivalent lattice satisfying $x_k \le N/2$. By picking the particular symmetric copy which keeps the components in increasing order we obtain the specific generating vector of the theorem. □

Step one of this proof can obviously be modified to restrict the elements of $\mathbf{x}$ such that $N/2 \le x_j < N$ for $j = 1, \cdots, s$.

Corollary 2.2. *Any rank-1 lattice generated by $(\mathbf{x}, N)$ has another symmetric copy satisfying*

$$N/2 \le x_1 \le \cdots \le x_s < N. \tag{2.2}$$

We refer to sequences satisfying (2.1) as *low sequences* and those satisfying (2.2) as *high sequences*. From (1.2) it follows that the 1-norm of any point on the dual lattice provides an upper bound on the degree of the lattice rule. This observation helps us establish the following lemma.

Lemma 2.3. *For a rank-1 lattice rule with generating vector satisfying* (2.1) *necessary conditions for $\delta(Q) \ge \delta$ are*

$$\begin{aligned} x_2 &\ge \delta - 1 \\ x_j - x_{j-1} &\ge \delta - 2, \qquad 2 < j < s \\ x_s &\le (N - \delta)/2 + 1. \end{aligned}$$

Proof. For any $\lambda \in \mathbb{Z}^s$ we must have

$$|\sum_{j=2}^{s} \lambda_j x_j + \lambda_1 N| + \sum_{j=2}^{s} |\lambda_j| \ge \delta(Q) \tag{2.3}$$

for (1.7) to hold. For the following λ's:

$$\begin{aligned}\lambda^{(1)} &= (0,1,0,\cdots,0)\\ \lambda^{(2)} &= (0,\cdots,0,-1,1,0,\cdots,0)\\ \lambda^{(3)} &= (1,0,\cdots,0,-2)\end{aligned}$$

the inequalities of the lemma need to be satisfied for (2.3) to hold. In the last inequality the assumption $x_s \le N/2$ is used. □

In view of this lemma we see that any lattice rule with $\delta > 2$ requires $1 < x_2 < \cdots < x_s$, and for the rest of this paper we will assume this is the case.

3. Delta-sequences and the basic algorithm

Definition 3.1. δ-sequence A vector $\mathbf{y} = (y_1, \cdots, y_n)$ is said to be a δ-sequence if and only if:

(*i*): $0 < y_1 < \cdots < y_n$,
(*ii*): $|\sum_{j=1}^{n} \lambda_j y_j| + \sum_{j=1}^{n} |\lambda_j| \ge \delta$ for any $\lambda \in \mathbb{Z}^n$.

If there exists a $\lambda \in \mathbb{Z}^n$ giving equality in *(ii)* we say $\mathbf{x}$ is a *strict δ-sequence*.

Evidently a δ-sequence bears close resemblance with the right-hand side of (1.8), and having found a δ-sequence of length n we can readily produce a rank-1 lattice rule of dimension $s = n+1$ of degree at most δ for some N and generating vector $\mathbf{x} = (1, y_1, \cdots, y_n)$. As our generating vector satisfies (2.1), Lemma 2.3 requires that we must have $N \ge 2(y_n - 1) + \delta$. An upper bound on N is $N \le (\delta - 1)y_n$, as any N larger than this upper bound cannot minimize (1.7) for $|\lambda_1| > 0$. As these bounds for N depend on y_n we naturally seek δ-sequences with low value on y_n.

If item (*ii*) of the definition is satisfied, it is in particular satisfied for λ with $\lambda_n = 0$. It follows that we can produce δ-sequences by extension. Given an $n-1$-dimensional δ-sequence we can search for $y_n \ge y_{n-1} + \delta - 2$ to obtain n-dimensional sequences. This is the simple logic behind our search algorithm.

The computation consists of two functions. A logical function (*check_good*) takes as input a δ-sequence of length k and checks if a candidate y_{k+1} may be used to extend the sequence to δ-sequence of size $k+1$. The other function (*find_best_n*) finds the optimal N value for the sequence. To limit the possible candidates y_{k+1} we use Lemma 2.3. The lower bound is straightforward and by a "backward" calculation we obtain a value *upper* such that $y_{k+1} > upper$ implies that this δ-sequence must produce a rank-1 lattice rule of degree δ with $N(\Lambda) > N_{upper}$. This bounds the search provided an upper bound on N, N_{upper} is available.

Below is a formal description of the algorithm. It becomes simple and elegantly written as a recursive algorithm. We return to the question of how to implement *find_best_n* in Section 7.

Algorithm: Lattice rules by δ-sequence extension
extend_sequence $(n, \delta, k, y(1:k), N_{upper})$
$upper = (N_{upper} - \delta)/2 + 1 - (n - k - 1) * (\delta - 2)$
for $y_{k+1} = y_k + \delta - 2,\ upper$
  ok = *check_good* $(\delta, k+1, y(1:k+1))$
  if ok **then**
    if $(k+1 = n)$ then
      $N =$ *find_best_n*$(n, \mathbf{x})$ /* $\mathbf{x} = (1, y_1, \cdots, y_n)$ */

```
        if N < N_bsf then
          N_bsf = N
          N_upper = min(N_upper, N_bsf)
        endif
      else
        extend_sequence (n, δ, k + 1, y(1 : k + 1), N_upper)
      endif
    endif
  end for
```

Using this function with sharper bounds for N_{upper} gives a lower *upper*, tightens the loops and speeds up the computation. An obvious improvement in a search is to keep an N_{bsf} (N "best-so-far") and update N_{upper} whenever $N_{bsf} < N_{upper}$.

4. The case $\delta = 5$

We have implemented the algorithm of Section 3 and found some new best rank-1 lattice rule of moderate degree, listed in Section 8. However, the search space fans out quickly with increasing dimension; hence we have to seek ways to limit it. Our main result in this respect is a way of characterizing δ-sequences of $\delta = 5$, which allows us to quickly generate high-dimensional δ-sequences with low value on y_n. We limit ourselves to a restricted kind of δ-sequence.

Definition 4.1. A δ-sequence is a *sky sequence* if and only if $y_n < 2y_1 - \delta$.

When used together with an admissible N for constructing lattice rules it can easily be transformed into a symmetric copy satisfying (2.1) or (2.2). We now formulate our main theorem:

Theorem 4.2. *A sky sequence is a δ-sequence with $\delta \geq 5$ if and only if:*

(*i*)**:** *All the elements of the set $E = \{\varepsilon_{ij} = y_i - y_j\}$; $1 \leq j < i \leq n$ are distinct.*

(*ii*)**:** $\min \varepsilon_{ij} \geq 3$.

The proof of this theorem is done by inspecting all possible integer values for $(\lambda_1, \cdots, \lambda_n)$ of (*ii*) in Definition 3.1. A first inspection shows that a necessary condition is $\sum_{i=1}^{n} |\lambda_i| < 5$. To assist in the proof we first establish a couple of lemmas.

Lemma 4.3. *Let $\lambda_1, \lambda_2, \lambda_3$ and λ_4 be four integers satisfying*

$$0 < \sum_{i=1}^{4} |\lambda_i| \leq 4 \qquad \text{and} \qquad \sum_{i=1}^{4} \lambda_i > 0. \tag{4.1}$$

Then either all $\lambda_i \geq 0$ or just one, say $\lambda_k = -1$, and all the others satisfy $\lambda_i \geq 0$, $i \neq k$.

Proof. Assuming (4.1) is satisfied, we have

$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 \leq |\lambda_1| + |\lambda_2| + |\lambda_3| + \lambda_4 \leq 4 - |\lambda_4| + \lambda_4.$$

If $\lambda_4 < -1$ the first sum is not positive, leading to a contradiction. Thus we must have $\lambda_4 \geq -1$. The same argument applies to λ_1, λ_2 and λ_3. Assume two of them,

say λ_1 and λ_2, equal -1. Then by (4.1) $|\lambda_3| + |\lambda_4| \leq 2$, and we have

$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = \lambda_3 + \lambda_4 - 2 \leq |\lambda_3| + |\lambda_4| - 2 \leq 0,$$

which again contradicts the hypothesis. This establishes the lemma. □

Lemma 4.4. *Let* $0 < y_1 < y_2 < \cdots < y_n$ *and* $y_n \leq 2y_1$, $\sum_{i=1}^n |\lambda_i| < 5$ *and* $\sum_{i=1}^n \lambda_i \neq 0$. *Then*

$$|\sum_{i=1}^n \lambda_i y_i| \geq 2y_1 - y_n. \tag{4.2}$$

Proof. At most four of the λ_i's are non-zero. By the previous lemma it is sufficient to consider all four non-negative or at most one component equal to -1. All $\lambda_i \geq 0$ and $\sum_{i=1}^n \lambda_i > 0$ give

$$\sum_{i=1}^n |\lambda_i y_i| \geq y_1 > 2y_1 - y_n,$$

while one component, say $\lambda_k = -1$ and $\sum_{i \neq k} \lambda_i = 2$,

$$\sum_{i=1}^n |\lambda_i y_i| \geq 2y_1 - y_k \geq 2y_1 - y_n$$

and $\lambda_k = -1$ and $\sum_{i \neq k} \lambda_i = 3$ give

$$\sum_{i=1}^n |\lambda_i y_i| \geq 3y_1 - y_k > 2y_1 - y_n.$$

□

We are now ready to prove the main theorem.

Proof of Theorem 4.2. We first prove by contradiction that all $\varepsilon_{i,j}$ different is a necessary condition for the δ-sequence in question to have $\delta \geq 5$. Assume $\varepsilon_{i,j} = \varepsilon_{k,l}$; then $y_i - y_j - y_k + y_l = 0$. Thus for $\lambda_i = -\lambda_j = -\lambda_k = \lambda_l = 1$ and all other components zero, we have $\sum_{i=1}^n |\lambda_i| + |\sum_{i=1}^n \lambda_i y_i| = 4$, which proves that the elements of E need to be distinct for the sequence to have $\delta \geq 5$.

Obviously λ-vectors where $\sum_{i=1}^n |\lambda_i| \geq 5$ cannot violate the condition $\delta \leq 5$. Thus it is sufficient to check the possible combinations of $\sum_{i=1}^n |\lambda_i| < 5$.

By Lemma 4.4 it follows that when $\sum_{i=1}^n \lambda_i \neq 0$ and $2y_1 - y_n > 3$ we have $\sum_{i=1}^n |\lambda_i| + |\sum_{i=1}^n \lambda_i y_i| \geq 5$. For $\sum_{i=1}^n \lambda_i = 0$ and $\sum_{i=1}^n |\lambda_i| \leq 4$ we have these non-trivial combinations of at most four non-zeros:

$$\begin{aligned}
i) &\quad (\lambda_i, \lambda_j, \lambda_k, \lambda_l) = (1, -1, 0, 0) \\
ii) &\quad (\lambda_i, \lambda_j, \lambda_k, \lambda_l) = (2, -2, 0, 0) \\
iii) &\quad (\lambda_i, \lambda_j, \lambda_k, \lambda_l) = (1, -1, 1, -1) \\
iv) &\quad (\lambda_i, \lambda_j, \lambda_k, \lambda_l) = (2, -1, -1, 0).
\end{aligned}$$

Under the assumption that all $\varepsilon_{i,j} \geq 3$ and $\varepsilon_{i,j} \neq \varepsilon_{k,l}$ the four cases above give:

$$\begin{aligned}
i) &\quad \textstyle\sum_{i=1}^n |\lambda_i| + |\sum_{i=1}^n \lambda_i y_i| = \quad 2 + |\varepsilon_{i,j}| \geq 5 \\
ii) &\quad \textstyle\sum_{i=1}^n |\lambda_i| + |\sum_{i=1}^n \lambda_i y_i| = \quad 4 + 2|\varepsilon_{i,j}| > 5 \\
iii) &\quad \textstyle\sum_{i=1}^n |\lambda_i| + |\sum_{i=1}^n \lambda_i y_i| = \quad 4 + |\varepsilon_{i,j} \pm \varepsilon_{k,l}| \geq 5 \\
iv) &\quad \textstyle\sum_{i=1}^n |\lambda_i| + |\sum_{i=1}^n \lambda_i y_i| = \quad 4 + |\varepsilon_{i,j} \pm \varepsilon_{i,k}| \geq 5.
\end{aligned}$$

Permutation and sign changes of the components in *i*)–*iv*) do not alter any of the computations. This exhausts the possibilities of $\sum_{i=1}^{n} \lambda_i = 0$ and $\sum_{i=1}^{n} |\lambda_i| \leq 4$ and thus concludes the proof. □

5. Golomb rulers and $\mathcal{B}_2$-sequences

Sequences satisfying (*i*) of Theorem 4.2 are known as *Golomb rulers* or $\mathcal{B}_2$-sequences. There is a rich literature on these sequences. A comprehensive overview with emphasis on the computation of near optimal Golomb rulers is given in [7]. In this section we briefly review definitions and some useful results.

Definition 5.1. A set of integers

$$A = \{y_1, y_2, \cdots, y_n\} \qquad y_1 < y_2 < \cdots < y_n \tag{5.1}$$

is called a *Golomb ruler* if

$$y_k - y_l = y_j - y_i \qquad \text{iff} \qquad \{k, l\} = \{j, i\}. \tag{5.2}$$

If, in addition, there exists a p such that the above holds for all differences modulo p, the Golomb ruler is said to be *cyclic modulo p*.

The following three properties of Golomb rulers follow easily from the definition:

Property 5.1. If the set $A = \{y_1, y_2, \cdots, y_n\}$ is a Golomb ruler, then so are the sets

$$\begin{array}{lrcl} \text{Translation:} & A_1 & = & \{y_1 + z, y_2 + z, \cdots, y_n + z\} \\ \text{Multiplication:} & A_2 & = & \{cy_1, cy_2, \cdots, cy_n\} \\ \text{Mirroring:} & A_3 & = & \{y_n - y_n, y_n - y_{n-1}, \cdots, y_n - y_1\} \end{array}$$

for any non-zero integers z and c.

$G(n) = y_n - y_1$ is called the *length of the ruler*, while n is its number of *markers*. We are particularly interested in the *optimal ruler*, the ruler of minimum length, $G(n)$, among the rulers with n markers. The translation property implies that every Golomb ruler may be translated into one where $y_1 = 0$ in which case $G(n) = y_n$. For cyclic rulers we may choose where to start and end, and its length does of course depend on this choice.

A different approach to this problem is taken by stating the problem in terms of a $\mathcal{B}_2$-set defined as:

Definition 5.2. A set of integers

$$A = \{y_1, y_2, \cdots, y_n\}, \quad y_1 < y_2 < \cdots < y_n \tag{5.3}$$

is called a Sidon set or a $\mathcal{B}_2$ sequence if, for any sum of pairs,

$$y_k + y_l = y_j + y_i \qquad \text{iff} \qquad \{k, l\} = \{j, i\}. \tag{5.4}$$

Since

$$y_k + y_l = y_j + y_i \Leftrightarrow y_k - y_i = y_j - y_l \tag{5.5}$$

it follows that Golomb rulers and $\mathcal{B}_2$ sequences are equivalent. The theory of Golomb rulers and that of $\mathcal{B}_2$ sets have been developed in parallel. Researchers formulating the problem in terms of $\mathcal{B}_2$-sequences have focused on establishing bounds for the length of optimal sequences, while the researchers working with Golomb rulers have taken an algorithmic approach and focused on the construction of good rulers. General formulae for optimal rulers are not available, but for a

limited number of markers finite searches have established the optimal length of rulers with $n \leq 27$.

A huge amount of computer time has been devoted to a distributed search for optimal Golomb rulers over the last decade, and by February 19, 2014, the search for the optimal ruler with 27 markers was found to be $G(27) = 553$ [6]. The search took 1,822 days, and 19,919 participants across the Web contributed cycles. The search for the optimal ruler with 28 markers is now under way.

We first summarize some of the results obtained for $\mathcal{B}_2$-sequences. In particular we are interested in the results which explicitly explain how to construct good rulers. Where necessary, we have changed the notation to that introduced above.

Theorem 5.3 (Lower bound)**.** *For all rulers with n markers the optimal length is bounded by*

$$G(n) > n^2 - 2n\sqrt{n} + \sqrt{n} - 2. \tag{5.6}$$

This is the best lower bound on the length of a Golomb ruler. The theorem is due to Dimitromanolakis [7] and is based on a result on $\mathcal{B}_2$ sequences due to Lindström [12].

A simple and efficient algorithm for computing Golomb rulers can be built on the following theorem due to Rusza [19].

Theorem 5.4. *Let p be a prime number and g a primitive element of the multiplicative group Z_p^*. The following sequence is a Golomb ruler:*

$$R_k(p,g) = pk + (p-1)g^k \bmod p(p-1);\ \textit{for}\ 1 \leq k \leq p-1. \tag{5.7}$$

As the $p-1$ integers of the set $R_k(p,g)$ are reduced modulo $p(p-1)$ we will have:

Corollary 5.5. *$G(n) < n^2 + n$ whenever $n+1$ is prime.*

An existence theorem due to Singer [20] provides an even tighter upper bound.

Theorem 5.6. *Let $q = p^m$ be a prime power. Then there exists $q+1$ integers $d_0, d_1, \cdots, d_q$ such that the q^2+q differences $d_i - d_j \bmod (q^2+q+1)$ are all different non-zero integers less than q^2+q+1.*

Thus in this case, for $n+1$ being a prime power, we have $G(n) < n^2$, and Erdös [8] has conjectured that this bound holds for all natural numbers. The conjecture has indeed been computationally verified for $n < 65000$ [7].

Another algorithm for computing good Golomb rulers is due to Bose and Chowla [1], based on the following theorem.

Theorem 5.7. *Let $q = p^m$ be a prime power and θ a primitive element in the Galois field $GF(q^2)$. Then the q integers*

$$d_1, \cdots, d_q = \{a | 1 \leq a < q^2 \textit{ and } \theta^a - \theta \in GF(q)\} \tag{5.8}$$

have distinct pairwise modulo differences modulo q^2-1.

In addition the $q(q-1)$ differences $d_i - d_j$, $i \neq j$, when reduced modulo q^2-1 are all the different non-zero integers less than q^2-1 which are not divisible by $q+1$.

The last part of the theorem states that these rulers are cyclic difference sequences. This is also the case for rulers obtained by Rusza's construction. For a cyclic difference sequence the analogue of the translation property becomes a *cyclic*

shift property, and addition modulo q^2-1 for the difference set. This shift property gives us a family of Golomb rulers all with q markers, but of different length, and we can pick the shortest one.

For example when $q = 11$, $\theta = 2x + 3$ is a primitive element of $GF(11^2)$. The following Golomb ruler is produced by equation (5.8):

$$1, 6, 20, 27, 38, 40, 55, 65, 71, 117, 118. \tag{5.9}$$

As all these differences modulo 120 are different, the sequence $\hat{d}_i = (d_i+3) \bmod 120$ also has 120 different differences, and thus another Golomb ruler of this family would be

$$0, 1, 4, 9, 23, 30, 41, 43, 58, 68, 74, \tag{5.10}$$

reducing the length from 117 to 74. As seen from this example the shortest member of this family is found by breaking the cyclic sequence at its longest gap.

The multiplication property can also be applied to a cyclic difference sequence. For any cyclic difference sequence modulo z it is easy to prove the following lemma.

Lemma 5.8. *If* $\{d_1, \cdots, d_n\}$ *is a cyclic difference sequence modulo* z*, then so is* $\{cd_1 \bmod z, \cdots, cd_n \bmod z\}$ *if* $\gcd(z, c) = 1$.

By working with cyclic difference sequences and combining the multiplication and cyclic shift property it has been possible to construct Golomb rulers of n marks of length less than n^2 for $n < 65000$.

As seen from the above, computing optimal rulers is extremely expensive, while fast algorithms for finding near optimal rulers with thousands of markers are readily available. A lesson learned from the limited computation done with the algorithm of Section 3 is that in none of the cases the optimal δ-sequences/Golomb ruler gave the optimal lattice rule. Thus we intend to settle for the use of good Golomb rulers produced by one of the algorithms introduced in this section as the δ-sequences in our rank-1 lattice rule.

6. Golomb rulers, sky sequences and lattice rules

Golomb rulers satisfy (*i*) of Theorem 4.2. Property (*ii*) is easily satisfied by removing one marker from each pair producing the differences 1 and 2. In the case of cyclic difference sets, one may remove the elements before starting the search for the longest gap to obtain the shortest possible ruler.

Next one can use the translation property to make y_1 and y_n as small as possible for the ruler to satisfy $y_n < 2y_1 - 5$. An implication of the translation property is that not only may this particular Golomb ruler be used for a rank-1 lattice rule of enhanced degree 5, but so may all other rulers obtained by a positive integer shift. Numerical experiments show that we may easily end up with a lower optimal N for a shifted sequence. Thus in the search for the lattice rule with smallest possible N we allow shifted rulers as candidates.

To turn an $(s-1)$-dim δ-sequence $\mathbf{y}$ into an s-dim simple rank-1 lattice with generating vector $\mathbf{x} = (1, x_2, \cdots, x_s) = (1, y_1, \cdots, y_{s-1})$ and enhanced degree δ, we need a value of N satisfying

$$\left| \sum_{j=2}^{s} \lambda_j x_j + \lambda_1 N \right| + \sum_{j=2}^{s} |\lambda_j| \geq \delta \qquad \forall \lambda \in \mathbb{Z}^s \backslash \{0\}. \tag{6.1}$$

Equation (6.1) is always satisfied for $N \geq (\delta-1)x_s + 1$. When the δ-sequence is an $(s-1)$-dimensional Golumb ruler translated such that $y_1 = G(s-1)+\delta$, a sky sequence will satisfy $y_{s-1} \leq 2G(s-1)+\delta$. In view of the Erdös conjecture and the computational verification of this for $n \leq 65000$, we have the following proposition:

Proposition 6.1. *For $s \leq 65000$ there do exist rank-1 lattice rules with $\delta = 5$ and $N \leq 8(s-1)^2 + 4$.*

The upper bound on the number of lattice points in this proposition is crude and could probably be sharpened. The interesting thing is that it does prove that there exist lattice rules having $\delta = 5$ with abscissa count of order $O(s^2)$. This should be compared with Möller's [17] lower bound for the abscissa count of any integration rule of dimension s and enhanced degree δ. See also [5]. For $\delta = 5$ this lower bound becomes

$$N_{ME}[s,5] = 2\left(s+\frac{1}{2}\right)^2 + \frac{1}{2}. \tag{6.2}$$

7. Finding the optimal N

Any of the above algorithms for finding good Golomb rulers can be used for fast computation of near optimal δ-sequences. To compute good lattice rules based on these δ-sequences we need to be able to find the minimal N for fixed $\mathbf{x}$ and s quickly.

For $Q = \sum_{j=2}^{s} \lambda_j x_j$ and $M = \sum_{j=2}^{s} |\lambda_j|$ we rewrite (6.1) as

$$|Q + \lambda_1 N| \geq \delta - M. \tag{7.1}$$

Due to the integer constraints, the left-hand side is minimized for $\lambda_1 = -\left\lfloor \frac{Q}{N} \right\rceil$[1].

For $\delta = 5$ this inequality is always satisfied unless $M \leq 4$. Thus we only need to inspect the finite number of λ vectors corresponding to $M \leq 4$. If we arrange these vectors as rows in a matrix $\mathbf{H} \in \mathbb{Z}^{r\times(s-1)}$, computing all possible Q corresponds to computing $\mathbf{q} = \mathbf{H}\mathbf{y}$. Computing the corresponding M corresponds to computing $\mathbf{m} = \mathbf{H}\mathbf{e}$, where $\mathbf{e} = (1,\cdots,1)^T \in \mathbb{Z}^{(s-1)}$. The test for whether or not $(\mathbf{x}, N)$ construct a rank-1 lattice rule of degree δ becomes:

$$(\mathbf{x},N) \text{ of degree } \delta \Leftrightarrow |\mathbf{q} - \left\lfloor \frac{\mathbf{q}}{N} \right\rceil N| + \mathbf{m} \geq \delta, \tag{7.2}$$

where this vector inequality needs to be satisfied for all components.

The main computation here is to set up the matrix $\mathbf{H}$ and compute $\mathbf{q}$=$\mathbf{H}\mathbf{y}$. However, these operations are done only once and need not be repeated when multiple N need to be checked. A factor 2 in savings is possible by noting that negating the sign of all λ_i gives exactly the same answer to (7.2). Our implementation takes advantage of this observation.

Furthermore, when we have multiple δ-sequences, $\mathbf{y}$, of equal dimension, they all relate to the same matrix $\mathbf{H}$, and when multiple δ-sequences are constructed by the translation property ($\mathbf{y}^{(k)} = \mathbf{y} + k\mathbf{e}$) we have

$$\mathbf{q}^{(k)} = \mathbf{H}\mathbf{y}^{(k)} = \mathbf{H}\mathbf{y} + k\mathbf{H}\mathbf{e} = \mathbf{q} + k\mathbf{m}. \tag{7.3}$$

We utilize these properties in our search program. After having obtained an n-dimensional cyclic Golomb ruler we remove one or two markers to satisfy the $\varepsilon_{ij} \geq 3$

[1] $\lfloor x \rceil$ denotes rounding to nearest integer.

constraint and construct $s-1$ basic δ-sequences by cyclic shift. These are then translated to become sky-sequences. To each of these basic sequences further translations may be applied. In higher dimensions we try hundreds of translations and for each of these, hundreds of N values before the optimal is found. As a consequence the set-up of $\mathbf{H}$ and computation of $\mathbf{q} = \mathbf{Hy}$ and $\mathbf{m} = \mathbf{He}$ are only a small fraction of the computational costs. The main cost is evaluating the acceptance criteria (7.2).

The complete search may be summarized in the following algorithm.

Algorithm: Find minimal N for δ-sequences generated by a cyclic Golomb ruler

$\mathbf{y} =$ *constructGolombRuler(n)*
$[s, \tilde{\mathbf{y}}] =$ *reduceGR(n)*
$\mathbf{H} =$ *setupH(s)*
$\mathbf{m} = \mathbf{He}$
for $i = 1 : s-1$ /* `loop for cyclic shift of` $\tilde{\mathbf{y}}$ */
  $\mathbf{v} = [\tilde{\mathbf{y}}(i : s-1), \tilde{\mathbf{y}}(1 : i-1)]$
  $\mathbf{q_0} = \mathbf{Hv}$
  for $k = 0 : kmax$ /* `loop for translation of the ruler` */
    $N = N_{min}$
    while $(N \le N_{bsf}$ & $|\mathbf{q}_k - \lfloor \frac{\mathbf{q}_k}{N} \rceil N| + \mathbf{m} < \delta)$
      $N = N + 1$
    end
    if $|\mathbf{q}_k - (\lfloor \frac{\mathbf{q}_k}{N} \rceil N| + \mathbf{m} \ge \delta)$ **then** $N_{bsf} = N$
    $\mathbf{q}_{k+1} = \mathbf{q}_k + \mathbf{m}$
  end
end

The routine *reduceGR* is a simple procedure to remove one or two elements from the Golomb ruler to satisfy the additional criterion that $\varepsilon_{ij} \ge 3$. The effect is that from a Golomb ruler with n markers we will produce a generating vector for a rank-1 lattice rule of dimension s: $s = n - 1$ when two markers are removed or $s = n$ when only one marker is removed. There are always multiple possibilities when removing elements from the δ-sequence. As a rule of thumb we typically try to remove the one making the length of the δ-sequence as short as possible, but there is of course no guarantee that this makes the best lattice rule, and we have come across examples where this is not the case.

We do keep an N_{bsf} value. This not only works as a stopping criterion for the while loop, but might also be used to bound $kmax$. $N_{\min}$ is computed by the formula

$$N_{\min} = \max(N_{ME}, \tilde{\mathbf{y}}(s) + 3). \tag{7.4}$$

8. New lattice rules

In Tables 1 and 2 we present some new rank-1 lattice rules found by the algorithm given in Section 3. The *find_best_n* routine used there is based on an exhaustive search and requires the lion's share of the computing time. Computing the last entries of these two tables takes typically a day or two on a desktop, and the time explodes with higher s or δ. This search is exhaustive, and thus these rules are indeed optimal rank-1 lattice rules.

TABLE 1. Optimal rank-1 lattice rules for $\delta = 5$.

s	$\mathbf{x}$	N
4	1 4 10 17	46
	1 6 16 19	46
5	1 4 13 19 29	69
	1 5 16 19 28	69
	1 7 16 19 29	69
	1 10 14 17 22	69
	1 13 22 29 32	69
6	1 7 10 25 29 41	103
	1 11 18 24 27 32	103
	1 11 28 31 35 49	103
	1 14 21 25 30 33	103
7	1 4 19 31 44 53 60	130
	1 7 18 22 27 57 60	130
	1 9 14 21 40 46 57	130
	1 10 16 29 34 37 41	130
8	1 9 13 16 40 46 51 74	168
9	1 5 19 22 31 56 64 71 99	209
	1 22 29 38 42 48 53 56 88	209
	1 27 33 36 44 49 56 74 95	209
10	1 5 13 24 51 54 71 86 93 114	268
	1 5 18 21 32 62 70 77 105 117	268
	1 5 23 34 42 49 74 87 101 104	268
	1 14 21 50 60 66 69 77 103 107	268
	1 35 51 90 93 97 107 112 118 130	268
	1 49 62 71 87 107 114 117 122 128	268

TABLE 2. Optimal rank-1 lattice rules of dimension 5.

δ	$\mathbf{x}$	N
6	1 15 21 25 33	110
7	1 6 45 61 81	301
	1 19 26 74 143	301
	1 26 34 81 145	301
	1 40 50 137 143	301
	1 40 62 95 107	301
8	1 9 61 101 157	448
	1 9 125 159 213	448
	1 31 117 157 169	448
	1 43 61 117 199	448
	1 167 173 199 213	448
9	1 52 375 389 459	962
	1 59 137 145 182	962
	1 104 183 303 323	962
	1 127 153 260 345	962

In Table 3 we present some new degree 5 lattice rules based on Golomb rulers. These are not optimal. To indicate their quality we compare them with the theoretical lower bound and the upper bound of Proposition 6.1 as well as the optimal rank 1 rules of Table 1, where these are available. This comparison is shown in Figure 1.

TABLE 3. p is the prime used as the basis for the Rusza construction. N_{GR} is the number of basic Golomb rulers for this particular prime. s is the length of the Golomb ruler obtained after reducing it to comply with (ii) of Definition 4.1. This is also the dimension of the lattice rule.

$p = 5$	1 33 44 47	$s = 4$
$N_{GR} = 2$	1 34 45 48	$N = 53$
	1 23 34 40	
$p = 7$	1 71 74 96 100 105	$s = 6$
$N_{GR} = 2$		$N = 112$
$p = 11$	1 187 193 201 205 218 250 269 274	$s = 9$
$N_{GR} = 4$		$N = 309$
$p = 13$	1 348 351 355 366 385 401 410 441 484 490	$s = 11$
$N_{GR} = 4$		$N = 511$
$p = 13$	1 431 475 478 485 493 507 513 518 534 564 568	$s = 12$
$N_{GR} = 4$		$N = 632$
$p = 17$	1 258 261 271 282 289 318 344 358 381 396 400 439 484 489	$s = 15$
$N_{GR} = 8$		$N = 1133$
$p = 19$	1 369 391 435 452 497 504 510 538 552 575 591 601 622 626 631 634	$s = 17$
$N_{GR} = 6$		$N = 1420$
$p = 23$	1 591 633 695 732 770 782 796 825 841 859 866 872 876 944 983	$s = 21$
$N_{GR} = 10$	992 1011 1041 1044 1065	$N = 2313$
$p = 23$	1 727 746 816 867 877 895 919 940 981 990 994 997 1024	$s = 22$
$N_{GR} = 10$	1062 1077 1088 1136 1196 1213 1221	$N = 2596$
$p = 29$	1 611 620 635 665 682 728 739 746 789 824 875 883 923 927	$s = 28$
$N_{GR} = 12$	965 996 1006 1032 1045 1066 1098 1121 1193 1196 1212 1218	$N = 4489$
$p = 29$	1 644 654 665 680 689 714 719 746 793 843 846 860 866 929	$s = 29$
$N_{GR} = 12$	937 977 981 1019 1080 1087 1099 1142 1175 1188 1206 1247 1284	$N = 4652$

We have restricted ourselves to Rusza's construct. Thus we have not done all dimensions, only prime numbers minus 1 or 2, depending on whether or not we need to remove one or two entries to satisfy condition (ii) of Theorem 4.2. The most time consuming part is finding the optimal N for a given generating vector $\mathbf{x}$. As explained in Section 7 this is done by examining every N in the interval $[\max(1.3 * N_{ME}[s,5], x_s + 4), N_{bsf}]$, where N_{bsf} is updated as the computation proceeds. $N \geq x_s + 4$ follows from an argument equivalent to those in the proof of Lemma 2.3. By (6.2) $N \geq N_{ME}[s,5]$. The factor 1.3 is based on the experience that the lower bound is far from sharp, in particular in higher dimensions. We have played with this factor in low dimension ($N \leq 13$) and found 1.3 to be safe, but of course this is not certain. As is seen from Table 3, the best lattice does not correspond to the lowest possible sky-sequence, but a translated sequence. To limit the search, we have set an upper limit on the number of translations to $\max(300, N_{ME}[s,5]/2)$. Again a better lattice could have been found had we allowed for a larger shift.

For the first three entries of Table 3 we can compare with the optimal rank-1 lattice rules listed in Table 1. We notice that none of the lattice rules based on Golomb rulers are optimal, but they are pretty close.

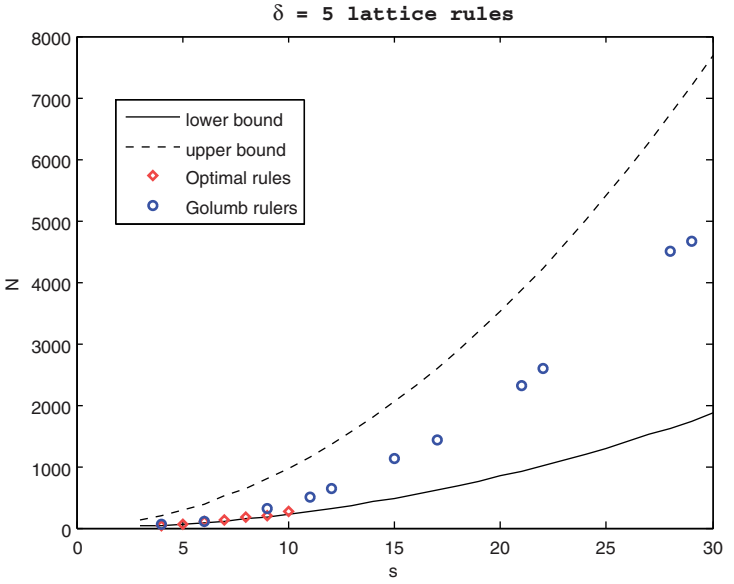

FIGURE 1. The lower bound is given by (6.2) and the upper bound by Proposition 6.1.

ACKNOWLEDGMENT

This research was initially a collaboration with James N. Lyness, who sadly passed away in December 2010. At that time the work corresponding to the content of the first four sections was more or less done, and the main ideas should be contributed to him. However, the blame for any error lies entirely with this author.

REFERENCES

[1] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962/1963), 141–147. MR0144877 (26 #2418)

[2] M. Bourdeau and A. Pitre, *Tables of good lattices in four and five dimensions*, Numer. Math. **47** (1985), no. 1, 39–43, DOI 10.1007/BF01389874. MR797876 (86h:65027)

[3] R. Cools and H. Govaert, *Five- and six-dimensional lattice rules generated by structured matrices*, J. Complexity **19** (2003), no. 6, 715–729, DOI 10.1016/j.jco.2003.08.001. Information-Based Complexity Workshop (Minneapolis, MN, 2002). MR2039626 (2005a:65021)

[4] R. Cools and J. N. Lyness, *Three- and four-dimensional K-optimal lattice rules of moderate trigonometric degree*, Math. Comp. **70** (2001), no. 236, 1549–1567, DOI 10.1090/S0025-5718-01-01326-6. MR1836918 (2002b:41026)

[5] R. Cools and I. H. Sloan, *Minimal cubature formulae of trigonometric degree*, Math. Comp. **65** (1996), no. 216, 1583–1600, DOI 10.1090/S0025-5718-96-00767-3. MR1361806 (97a:65025)

[6] http://www.distributed.net/Projects

[7] A. Dimitromanolakis, *Analysis of the Golomb ruler and the Sidon set problems, and determination of large near-optimal Golomb rulers*, Ph.D. thesis, Technical University of Crete (2002).

[8] P. Erdős, *On a problem of Sidon in additive number theory*, Acta Sci. Math. Szeged **15** (1954), 255–259. MR0064799 (16,336c)

[9] E. Hlawka, *Zur angenäherten Berechnung mehrfacher Integrale* (German), Monatsh. Math. **66** (1962), 140–151. MR0143329 (26 #888)

[10] G. Kedem and S. K. Zaremba, *A table of good lattice points in three dimensions*, Numer. Math. **23** (1974), 175–180. MR0373239 (51 #9440)

[11] N. M. Korobov, *Teoretiko-chislovye metody v priblizhennom analize* (Russian), 2nd ed., Moskovskiĭ Tsentr Nepreryvnogo Matematicheskogo Obrazovaniya, Moscow, 2004. MR2078157 (2005f:41001)

[12] B. Lindström, *An inequality for B_2-sequences*, J. Combinatorial Theory **6** (1969), 211–212. MR0236138 (38 #4436)

[13] J. N. Lyness and T. Sørevik, *A search program for finding optimal integration lattices*, Computing **47** (1991), no. 2, 103–120, DOI 10.1007/BF02253429. MR1139431 (92k:65037)

[14] J. N. Lyness and T. Sørevik, *An algorithm for finding optimal integration lattices of composite order*, BIT **32** (1992), no. 4, 665–675, DOI 10.1007/BF01994849. MR1191020 (93i:65038)

[15] J. N. Lyness and T. Sørevik, *Four-dimensional lattice rules generated by skew-circulant matrices*, Math. Comp. **73** (2004), no. 245, 279–295, DOI 10.1090/S0025-5718-03-01534-5. MR2034122 (2004k:65041)

[16] J. N. Lyness and T. Sørevik, *Five-dimensional K-optimal lattice rules*, Math. Comp. **75** (2006), no. 255, 1467–1480, DOI 10.1090/S0025-5718-06-01845-X. MR2219038 (2007d:65020)

[17] H. M. Möller, *Kubaturformeln mit minimaler Knotenzahl*, Numer. Math. **25** (1975/76), no. 2, 185–200. MR0405815 (53 #9607)

[18] D. Nuyens and R. Cools, *Fast algorithms for component-by-component construction of rank-1 lattice rules in shift-invariant reproducing kernel Hilbert spaces*, Math. Comp. **75** (2006), no. 254, 903–920, DOI 10.1090/S0025-5718-06-01785-6. MR2196999 (2007a:65032)

[19] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith. **65** (1993), no. 3, 259–282. MR1254961 (94k:11112)

[20] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385, DOI 10.2307/1990067. MR1501951

[21] I. H. Sloan, *Lattice methods for multiple integration*, Proceedings of the International Conference on Computational and Applied Mathematics (Leuven, 1984), J. Comput. Appl. Math. **12/13** (1985), 131–143, DOI 10.1016/0377-0427(85)90012-3. MR793949 (86f:65045)

[22] I. H. Sloan and S. Joe, *Lattice Methods for Multiple Integration*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1994. MR1442955 (98a:65026)

[23] I. H. Sloan and P. J. Kachoyan, *Lattice methods for multiple integration: theory, error analysis and examples*, SIAM J. Numer. Anal. **24** (1987), no. 1, 116–128, DOI 10.1137/0724010. MR874739 (88e:65023)

[24] I. H. Sloan and A. V. Reztsov, *Component-by-component construction of good lattice rules*, Math. Comp. **71** (2002), no. 237, 263–273, DOI 10.1090/S0025-5718-01-01342-4. MR1862999 (2002h:65028)

Department of Mathematics, University of Bergen, Bergen, Norway
E-mail address: tor.sorevik@math.uib.no