The Number of Lattice Rules of Specified Upper Class and Rank

J. N. Lyness[†] and S. Joe[‡]

Abstract

The upper class of a lattice rule is a convenient entity for classification and other purposes. The rank of a lattice rule is a basic characteristic, also used for classification. By introducing a rank proportionality factor and obtaining certain recurrence relations, we show how many lattice rules of each rank exist in any prime upper class. The Sylow p-decomposition may be used to obtain corresponding results for any upper class.

1 Introduction

Much of the background theory of lattice rules is covered in [SJ94]. Related results in connection with quasi-Monte Carlo methods are described in [N92]. Classification of lattice rules has been an ongoing problem and several approaches to this problem exist. Several of the earlier approaches [SL89] involve the rank of a lattice rule. In practice, howevet, it is difficult to work with this somewhat elusive quantity. The research in this paper is directed to obtaining further information about the rank.

As is conventional, we treat cubature over the region $[0,1)^s$. An s-dimensional *lattice rule* is one that can be expressed in the form

$$Qf = Q[t,D,Z,s]f = \frac{1}{d_1 d_2 \cdots d_t} \sum_{j_1=1}^{d_1} \sum_{j_2=1}^{d_2} \cdots \sum_{j_t=1}^{d_t} f\left(\left\{\sum_{i=1}^{t} j_i \frac{\mathbf{z}_i}{d_i}\right\}\right); \tag{1.1}$$

here d_i is a positive integer, an element of a $t \times t$ diagonal matrix D; $\mathbf{z}_i$ is a row of a $t \times s$ integer matrix Z; and $\{\mathbf{x}\} \in [0,1)^s$ denotes the vector whose components are the fractional parts of the components of $\mathbf{x}$.

[†] Mathematics and Computer Science Division, Argonne National Laboratory, Argonne IL 60439, USA, and School of Mathematics, University of New South Wales, Sydney NSW 2052, Australia. email: lyness@mcs.anl.gov. This author was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, U.S. Dept. of Energy, under Contract W-31-109-ENG-38.
[‡] Department of Mathematics, University of Waikato, Private Bag 3105, Hamilton, New Zealand. email: stephenj@math.waikato.ac.nz
3:26 p.m., August 6, 2002

This form is far from unique. The lattice *rank* of Q may be defined as the smallest value of t for which Q can be expressed in this $D-Z$ form. In some cases the rank of a rule is obvious. The only rank-zero rule is $Qf = f(\mathbf{0})$. The number-theoretic rule

$$Qf = Q[1, d, \mathbf{z}, s]f = \frac{1}{d}\sum_{j=1}^{d} f\left(\left\{\frac{j\mathbf{z}}{d}\right\}\right) \tag{1.2}$$

is of rank 1 unless $\left\{\frac{\mathbf{z}}{d}\right\} = \mathbf{0}$. While the rank is a natural group-theoretic concept, applying the definition given above to determine the rank of any rule of the form (1.1) more sophisticated than (1.2) may be a significant problem.

We denote by Λ_0 the s-dimensional *unit lattice*, comprising all points all of whose components are integer. The lattice Λ is an *integration lattice* if and only if $\Lambda \supseteq \Lambda_0$. It is not difficult to establish that the abscissas in (1.1) lie on an integration lattice Λ that includes points $j\mathbf{z}_i/d_i$ for $i = 1, 2, \ldots, t$ for all integer j and (in view of the symbol $\{\ \}$) all points of Λ_0. This lattice rule, denoted by $Q(\Lambda)$, has an abscissa set comprising all points of $\Lambda \cap [0, 1)^s$.

A $1-1$ correspondence exists between a lattice rule $Q(\Lambda)$ and a nonsingular integer $s \times s$ matrix in utlf (upper triangular lattice form). This is an upper triangular matrix B satisfying

$$\begin{aligned} b_{rc} &= 0 \text{ when } r > c, \\ b_{rc} &\in [0, b_{cc}) \text{ when } r < c, \\ b_{cc} &\geq 1 \text{ for } c = 1, 2, \ldots, s, \end{aligned} \tag{1.3}$$

and is one of many possible generator matrices of the lattice $\Lambda^\perp$ *dual* to Λ. (Recall that $\mathbf{x} \in \Lambda^\perp \Leftrightarrow \mathbf{x} \cdot \mathbf{p}$ is an integer for all $\mathbf{p} \in \Lambda$ and that, when B is a generator matrix of $\Lambda^\perp$, a necessary and sufficient condition that $\mathbf{x} \in \Lambda^\perp$ is simply $\mathbf{x} = \boldsymbol{\lambda} B$, for some $\boldsymbol{\lambda} \in \Lambda_0$.) For a given Λ, the generator matrix of $\Lambda^\perp$ in utlf is unique.

The abscissa count of Q is $N(Q) = b_{11}b_{22}\cdots b_{ss}$. We may refer to $N(Q)$ as the order of Q or as the order of $\Lambda^\perp$ or as the *inverse* order of Λ. Moreover, we may refer to the rank of Q as the *lattice rank* of the matrix B, and denote this by either $r(Q)$ or $r(B)$. This must not be confused with the *conventional* matrix rank of the matrix B that is, the number of linearly independent rows, which we shall denote by $\rho(B)$.

Many lattice rules having optimum properties have been discovered by computer search. The earlier searches such as those in [M72] involved populations of rules of the form (1.2) and so ignored all lattice rules of rank higher than 1. To our knowledge, the extension of searches of this particular nature to include, for example, rank-2 lattice rules has not been satisfactorily accomplished.

Many subsequent searches, for example, [CL01], used populations specified by dual lattices in the form (1.3). In some cases, this turned out to be a much better strategy. For example, the trigonometric degree of a lattice rule $Q(\Lambda)$ is more readily determined from $\Lambda^\perp$ than from Λ. In a search based on Λ, the first task for each lattice considered might be essentially the determination of elements of $\Lambda^\perp$.

Since both kinds of searches are in vogue, a natural task is collating the results. A key problem is recognizing the rank of $Q(\Lambda)$ from the parameters of B. Methods for determining the rank of a lattice rule can be time consuming. We shall deal with this problem in a companion paper. Here we approach the problem of determining in some measure the distribution of lattice rules over various ranks.

In this paper we take only a short (and relatively difficult) step in this direction. Following [LSK91] we define the upper class of a lattice rule $Q(\Lambda)$ as the s-tuple $[b_{11}, b_{22}, \ldots, b_{ss}]$ of the diagonal elements of B, the generator matrix in utlf (form (1.3)) of the dual lattice $\Lambda^\perp$. The number of distinct lattice rules in this upper class is

$$\nu_s([\mathbf{b}]) = \nu_s([b_{11}, b_{22}, \ldots, b_{ss}]) = b_{22}b_{33}^2 \cdots b_{ss}^{s-1}.$$

We derive straightforward formulas for $\nu_{s,r}([\mathbf{b}])$, the number of these lattice rules of rank r, and for $\bar{\nu}_{s,r}([\mathbf{b}])$, the number of these lattice rules having rank not exceeding r.

In Section 2 we reintroduce class factorization and apply it to show that

$$\bar{\nu}_{s,r}([\mathbf{b}]) = \prod_{j=1}^{q} \bar{\nu}_{s,r}([\boldsymbol{\sigma}^{(p_j)}]), \tag{1.4}$$

where $\prod_{j=1}^{q}[\boldsymbol{\sigma}^{(p_j)}]$ is the unique prime factorization of $[\mathbf{b}]$. Further sections are restricted to prime power rules. In Section 3 we derive a key theorem, the rank proportionality theorem, that allows us to express $\nu_{s,r}([\boldsymbol{\sigma}^{(p)}])$ as a power of p multiplied by a factor $\nu_{\ell,r}([p,p,\ldots,p])$ for a specified $\ell \leq s$. Section 4 is devoted to the evaluation of this factor, which is a polynomial of modest degree in p. We provide a general recurrence relation for this factor and tabulate it for $r \leq \ell \leq 5$. These results are applied in a numerical example in Section 5.

2 Background Theory

In this section, we reintroduce the upper classes $[\mathbf{b}]$, define a class prime factorization, and re-express $\bar{\nu}_{s,r}([\mathbf{b}])$ in terms of $\bar{\nu}_{s,r}([\boldsymbol{\sigma}^{(p_j)}])$, where $[\boldsymbol{\sigma}^{(p_j)}]$ is a prime upper class. The principal result is (1.4) above.

While the lattice rank occurs in the theoretical development in a natural way, the problem of determining the rank of a given lattice rule remains nontrivial. One standard method introduced in [LK95] is by means of the classical Smith normal form (snf).

Theorem 2.1 *A nonsingular integer matrix B may be uniquely diagonalized as*

$$S = UBV,$$

where U and V are unimodular integer matrices ($|\det U| = |\det V| = 1$) and $S = diag\{n_1, n_2, \ldots, n_r, 1, 1, \ldots, 1\}$ with $n_{i+1} \mid n_i$ and $n_r > 1$.

The integers n_i are the (nontrivial) *invariants* of the corresponding lattice rule Q (see [LK95], [SL89], and [SJ94]), and the number of (nontrivial) invariants is the rank of Q.

In the case of a prime power rule, that is, one for which $N = |\det B| = p^\alpha = n_1 n_2 \cdots n_r$ for some prime p, all the (nontrivial) invariants are positive powers of p. The (modulo p) matrix rank of a matrix B, denoted by $\rho_p(B)$, is the rank obtained when all matrix elements b_{ij} are replaced by b_{ij} modulo p, and all elementary arithmetic operations involving matrix elements are carried out using modulo p arithmetic. It is trivial to show that elementary row and column operations do not alter the (modulo p) matrix rank of a matrix. Since the unimodular matrices U and V in the statement of Theorem 2.1 have the effect of elementary row and column operations on B, it follows from the theorem that

$$\rho_p(B) = \rho_p(S). \tag{2.2}$$

Since S (modulo p) = diag$(0, 0, \ldots, 0, 1, 1, \ldots, 1)$, there being r zero elements and $s - r$ unit elements, it is clear that $\rho_p(S) = s - r$. In view of (2.2) we then have the following theorem.

Theorem 2.3 *Let $Q(\Lambda)$ be an s-dimensional prime power rule, and let B be any generator matrix of the dual lattice $\Lambda^\perp$. Then the rank of Q is given by*

$$r(B) = s - \rho_p(B) := \bar{\rho}_p(B),$$

where $\rho_p(B)$ is the modulo p matrix rank of the matrix B and $\bar{\rho}_p(B)$ the corresponding rank deficiency.

As mentioned in the introduction, the diagonal elements of any integer matrix B in utlf may be used to classify lattice rules into *upper classes*. In [LSK91] the theory of upper classes was developed with a view to the recognition and classification of sublattices and superlattices of a given integration lattice.

Definition 2.4 *The upper class of an s-dimensional integer matrix $\bar{B}$ is an integer s-vector denoted by $[\mathbf{b}] = [b_{11}, b_{22}, \ldots, b_{ss}]$, where $B = V\bar{B}$ is the utlf of $\bar{B}$.*

Definition 2.5 *The upper class of $Q(\Lambda)$ is the upper class of any generator matrix of $\Lambda^\perp$.*

By extension, we occasionally refer to this as the upper class of $\Lambda^\perp$; and we write $\Lambda^\perp \in [\mathbf{b}]$. We define the order of an upper class as $b_{11}b_{22}\cdots b_{ss}$.

A simple counting exercise indicates that the number of distinct rules $Q(\Lambda)$ belonging to the specified upper class $[\mathbf{b}] = [b_{11}, b_{22}, \ldots, b_{ss}]$ is

$$\nu_s([\mathbf{b}]) = \nu_s([b_{11}, b_{22}, \ldots, b_{ss}]) = b_{22}b_{33}^2 \cdots b_{ss}^{s-1}. \tag{2.6}$$

This is the number of distinct matrices B in utlf having diagonal elements $b_{11}, b_{22}, \ldots, b_{ss}$.

In the theory of upper classes, a concept of *class factorization* was introduced. Thus,

$$[b_{11}, b_{22}, \ldots, b_{ss}] = [\ell_{11}, \ell_{22}, \ldots, \ell_{ss}][r_{11}, r_{22}, \ldots, r_{ss}] \tag{2.7}$$

implies that

$$b_{ii} = \ell_{ii} r_{ii}, \quad 1 \le i \le s.$$

Moreover, in view of (2.6) and (2.7), we have immediately

$$\nu_s([b_{11}, b_{22}, \ldots, b_{ss}]) = \nu_s([\ell_{11}, \ell_{22}, \ldots, \ell_{ss}])\nu_s([r_{11}, r_{22}, \ldots, r_{ss}]). \tag{2.8}$$

Definition 2.9 *A* prime *upper class is one of the form $[p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}]$, where p is a prime and $\gamma_i \ge 0$.*

Each member Q of this upper class is a prime power rule of order $N(Q) = p^{\gamma_1+\gamma_2+\cdots+\gamma_s}$. The *prime factorization* of an upper class is one in which each factor is a prime upper class, corresponding to a different prime. An example of a prime factorization is

$$[42, 36, 14] = [2, 4, 2][3, 9, 1][7, 1, 7]. \tag{2.10}$$

Thus $[3, 9, 1]$ is one of the prime factors of $[42, 36, 14]$.

In view of (2.6) we have

$$\nu_s([p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}]) = p^{\gamma_2+2\gamma_3+\cdots+(s-1)\gamma_s}. \tag{2.11}$$

One context in which this concept of factorization is helpful is in applications of the following theorem.

Theorem 2.12 (*LSK91; Theorem 2.1*) *Let $s \times s$ nonsingular integer matrices B and R be the generator matrices of Λ_B and Λ_R, respectively. Then $\Lambda_R \supseteq \Lambda_B$ if and only if $L = BR^{-1}$ is an integer matrix.*

The proof is straightforward and is given in [LSK91]. If we treat B in utlf and seek R in upper triangular form, then L is also in upper triangular form. Moreover, in this situation we require $b_{ii} = \ell_{ii} r_{ii}$ for $1 \le i \le s$. In [LSK91] it is shown in detail how R may be obtained in utlf.

An almost trivial consequence of this theorem is the following result.

Theorem 2.13 *Let Λ_R and Λ_B be of upper classes $[r_{11}, r_{22}, \ldots, r_{ss}]$ and $[b_{11}, b_{22}, \ldots, b_{ss}]$, respectively. For Λ_R to be a superlattice of Λ_B, that is, $\Lambda_R \supseteq \Lambda_B$, it is necessary that $[r_{11}, r_{22}, \ldots, r_{ss}]$ be a factor of $[b_{11}, b_{22}, \ldots, b_{ss}]$.*

Since the earliest papers on lattice rules, for example, [SL89], the structure of lattice rules in terms of finite group theory has influenced the development of the general theory. In [LJ99], the classical theory regarding the decomposition of an Abelian group as the direct sum of Sylow p-components was applied in a *constructive* manner to lattice rules. We now review briefly some of this theory and extend it in a minor way.

The *order* of a point $\mathbf{x}$ is the smallest integer λ for which $\lambda\mathbf{x} \in \Lambda_0$. For every prime number p, the subset of points in Λ having orders 1, p, and all higher integer powers of p form a sublattice which is termed the *Sylow* p-component of Λ and is denoted here by $\Lambda^{(p)}$.

A sum operator for integration lattices was defined; the lattice sum $\Lambda = \Lambda_1 + \Lambda_2$ comprises all points $\mathbf{x}$ that may be expressed in the form $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$, where $\mathbf{x}_1 \in \Lambda_1$ and $\mathbf{x}_2 \in \Lambda_2$. It was shown that any *integration* lattice Λ for which $N(Q)$, the order of $Q(\Lambda)$, has the prime factor decomposition

$$N(Q) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_q^{\alpha_q} \tag{2.14}$$

may be uniquely expressed as the lattice sum of its Sylow components:

$$\Lambda = \Lambda^{(p_1)} + \Lambda^{(p_2)} + \cdots + \Lambda^{(p_q)}. \tag{2.15}$$

Each Sylow component $\Lambda^{(p_i)}$ is of inverse order $p_i^{\alpha_i}$ and is the unique sublattice of Λ having this inverse order. A simple way of obtaining the $D-Z$ form for each $Q(\Lambda^{(p_i)})$ from the $D-Z$ form (1.1) of $Q(\Lambda)$ is given in [LJ99].

In the present context, we are interested in the upper class to which the dual lattice of $\Lambda^{(p_i)}$, the Sylow p_i-component, belongs. This is given by the following not unexpected theorem.

Theorem 2.16 *Let $\Lambda^{\perp} \in [\mathbf{b}]$ have order* (2.14)*, and let the unique prime factorization of* $[\mathbf{b}]$ *be*

$$[\mathbf{b}] = [\boldsymbol{\sigma}^{(p_1)}]\,[\boldsymbol{\sigma}^{(p_2)}] \cdots [\boldsymbol{\sigma}^{(p_q)}],$$

$[\boldsymbol{\sigma}^{(p_j)}]$ *being the unique prime factor of* $[\mathbf{b}]$ *having order $p_j^{\alpha_j}$. Then the dual lattice $(\Lambda^{(p_j)})^{\perp}$ of the Sylow component in* (2.15) *belongs to the upper class $[\boldsymbol{\sigma}^{(p_j)}]$.*

Proof. This is almost self-evident and depends critically on the uniqueness of a Sylow p-component. Let $(\Lambda^{(p_j)})^{\perp}$ belong to some upper class $[\mathbf{r}]$. Since $\Lambda^{(p_j)}$ is a sublattice of Λ of inverse order $p_j^{\alpha_j}$, it follows that $(\Lambda^{(p_j)})^{\perp}$ is a superlattice of $\Lambda^{\perp}$ of order $p_j^{\alpha_j}$. Thus $[\mathbf{r}]$ is of order $p_j^{\alpha_j}$. Also, since $(\Lambda^{(p_j)})^{\perp}$ is a superlattice of $\Lambda^{\perp}$, Theorem 2.13 reveals that $[\mathbf{r}]$ is a factor of $[\mathbf{b}]$. The unique upper class $[\mathbf{r}]$ satisfying both these conditions is $[\boldsymbol{\sigma}^{(p_j)}]$. $\square$

Let $[\mathbf{b}] = [\boldsymbol{\sigma}^{(p_1)}][\boldsymbol{\sigma}^{(p_2)}]\cdots[\boldsymbol{\sigma}^{(p_q)}]$ be the prime factorization of $[\mathbf{b}]$, and let the order of each element $\Lambda^\perp$ belonging to $[\mathbf{b}]$ be $N = b_{11}b_{22}\cdots b_{ss} = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_q^{\alpha_q}$. It follows from (2.8) that

$$\nu_s([\mathbf{b}]) = \prod_{j=1}^{q} \nu_s([\boldsymbol{\sigma}^{(p_j)}]). \tag{2.17}$$

In this paper we are interested in calculating $\nu_{s,r}([\mathbf{b}])$, the number of rules of rank r belonging to $[\mathbf{b}]$, and incidentally

$$\bar{\nu}_{s,r}([\mathbf{b}]) = \sum_{m=1}^{r} \nu_{s,m}([\mathbf{b}]),$$

the number of rules belonging to $[\mathbf{b}]$ whose rank does not exceed r. It was established in [LJ99] that

$$r(Q(\Lambda)) = \max_{1\le j\le q} r(Q(\Lambda^{(p_j)})).$$

Thus the lattices in the upper class $[\mathbf{b}]$ that are of rank r or less stem from lattices in $[\boldsymbol{\sigma}^{(p_j)}]$ that are of rank r or less. Limiting the contributions in (2.17) in this way gives

$$\bar{\nu}_{s,r}([\mathbf{b}]) = \prod_{j=1}^{q} \bar{\nu}_{s,r}([\boldsymbol{\sigma}^{(p_j)}]).$$

This allows us to restrict our attention to $\bar{\nu}_{s,r}([\boldsymbol{\sigma}])$, where $[\boldsymbol{\sigma}]$ is a prime upper class.

3 Number of *Prime Power* Lattice Rules Having Specified Upper Class and Rank

In this section we treat prime power rules only. The main result is Theorem 3.1 below, which shows that $\nu_{s,r}([p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}])$ may be expressed simply in terms of $\nu_{\ell,r}([p,p,\ldots,p])$. Here the prime p occurs ℓ times, where ℓ is the number of nonzero components of $\boldsymbol{\gamma}$.

While dealing exclusively with prime upper classes, it is convenient to modify the notation. Since $[\mathbf{b}] = [b_{11}, b_{22}, \ldots, b_{ss}]$ is now of the form $[p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}]$, we shall replace $[\mathbf{b}]$ by $(\boldsymbol{\gamma})$, the value of p being understood. We set

$$\begin{aligned}\nu_{s,r}([\mathbf{b}]) &= \nu_{s,r}([b_{11}, b_{22}, \ldots, b_{ss}]) = \nu_{s,r}([p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}]) \\ &= \nu_{s,r}(\gamma_1, \gamma_2, \ldots, \gamma_s) = \nu_{s,r}(\boldsymbol{\gamma}).\end{aligned}$$

We shall also abbreviate by $\nu_{s,r}(1^s)$ the quantity

$$\nu_{s,r}([p,p,\ldots,p]) = \nu_{s,r}(1,1,\ldots,1).$$

The same notation, but without the r subscript, refers to the total number of rules in the upper class.

Theorem 3.1 *Let $\ell(\boldsymbol{\gamma})$ be the number of nonzero components in $\boldsymbol{\gamma}$, and let $\nu_s(\boldsymbol{\gamma})$ be the total number of members having upper class $[p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}]$. Then*

$$\frac{\nu_{s,r}(\boldsymbol{\gamma})}{\nu_s(\boldsymbol{\gamma})} = \frac{\nu_{\ell,r}(1^\ell)}{\nu_\ell(1^\ell)}, \tag{3.2}$$

where $\nu_\ell(1^\ell)$ and $\nu_{\ell,r}(1^\ell)$ are the number of lattice rules in upper class $[p, p, \ldots, p]$ (the p being repeated ℓ times) and the number of these of rank r, respectively.

Let us define the ratio

$$\mu_{s,r}(\boldsymbol{\gamma}) = \frac{\nu_{s,r}(\boldsymbol{\gamma})}{\nu_s(\boldsymbol{\gamma})} \tag{3.3}$$

as a *rank proportionality factor.* Then Theorem 3.1 equates two distinct rank proportionality factors, that is, $\mu_{s,r}(\boldsymbol{\gamma}) = \mu_{\ell,r}(1^\ell)$. We refer to this theorem as the rank proportionality theorem.

The formula (3.2) holds when ν is replaced by $\bar{\nu}$ in the numerators. Here,

$$\bar{\nu}_{s,r}(\boldsymbol{\gamma}) = \sum_{m=1}^{r} \nu_{s,m}(\boldsymbol{\gamma})$$

is the number of lattice rules of this upper class having rank not exceeding r.

To establish the rank proportionality theorem, we first define two subsets of $\{1, 2 \ldots, s\}$: these are

$$T(\boldsymbol{\gamma}) = \{j : \gamma_j \geq 1\}, \quad U(\boldsymbol{\gamma}) = \{j : \gamma_j = 0\}.$$

And we define

$$\tilde{\gamma}_j = \min(1, \gamma_j) = \begin{cases} 1 \text{ when } j \in T, \text{ i.e. when } \gamma_j \geq 1, \\ 0 \text{ when } j \in U, \text{ i.e. when } \gamma_j = 0. \end{cases}$$

Lemma 3.4 *The rank proportionality factor* (3.3) *satisfies*

$$\mu_{s,r}(\boldsymbol{\gamma}) = \mu_{s,r}(\tilde{\boldsymbol{\gamma}}).$$

Proof. Let $L_s(\boldsymbol{\gamma})$ be the set of $s \times s$ matrices in utlf of upper class $(\boldsymbol{\gamma})$ and let $M \in L_s(\boldsymbol{\gamma})$ be specified. Then there is a unique member B of $L_s(\tilde{\boldsymbol{\gamma}})$ whose non-diagonal elements are $b_{ij} = m_{ij} \bmod p$ and whose diagonal elements are $p^{\tilde{\gamma}_i}$, that is, p or 1 according to whether γ_i is positive or zero. On the other hand, for specified $B \in L_s(\tilde{\boldsymbol{\gamma}})$, there are precisely $\prod_{j \in T} p^{(j-1)(\gamma_j - 1)}$ matrices $M \in L_s(\boldsymbol{\gamma})$. These are obtained from B by replacing the diagonal elements by p^{γ_j} and, for $j \in T$ and

$i < j$, by setting m_{ij} to be one of the $p^{\gamma_j - 1}$ values for which $m_{ij} \equiv b_{ij} \pmod p$ with $b_{ij} \in [0, p)$. (When $j \in U$, both m_{ij} and b_{ij} are zero.)

Since $M \bmod p = B \bmod p$, it follows from Theorem 2.3 that M and B have the same lattice rank. Thus, corresponding to each $B \in L_s(\tilde{\gamma})$, there are $N_T = \prod_{j \in T} p^{(j-1)(\gamma_j - 1)}$ matrices $M \in L_s(\gamma)$ having the same lattice rank. Since this is an N_T to 1 correspondence between elements of $L_s(\gamma)$ and $L_s(\tilde{\gamma})$ and this correspondence preserves the lattice rank r, it follows that the proportion in each set is the same. This establishes the lemma. $\square$

We now use a similar argument to establish the following result.

Lemma 3.5 *Let $\tilde{\gamma}_j$ be 1 or 0 according to whether $\gamma_j \geq 1$ or $\gamma_j = 0$, and let ℓ be the number of unit components in $\tilde{\gamma}$. Then for $1 \leq r \leq \ell$,*

$$\mu_{s,r}(\tilde{\gamma}) = \mu_{\ell,r}(1^\ell).$$

Proof. Suppose $B \in L_s(\tilde{\gamma})$. Since $\tilde{\gamma}$ has precisely $s - \ell$ zero components, $s - \ell$ diagonal elements of B are units and their corresponding column vector includes only one nonzero element, which appears in the diagonal position. Using elementary row and column interchanges one may transform B into B' having the form

$$B' = \left[\begin{array}{cc} I_{s-\ell} & C \\ 0 & B'' \end{array} \right],$$

where $I_{s-\ell}$ is a unit matrix and B'' is a member of $L_\ell(1^\ell)$. Theorem 2.3 shows that $r(B) = r(B') = s - \rho_p(B')$. Since $\rho_p(B') = s - \ell + \rho_p(B'') = s - \bar{\rho}_p(B'')$, we see that the lattice rank of B coincides with the lattice rank of B'' and is independent of the elements in C. Because C is obtained from B by deleting every column with a unit diagonal element and every row without a unit diagonal element, we see that the elements of C are b_{ij} for $i \in U$ and $j \in T$. When $j < i$, then $b_{ij} = 0$; when $j > i$, b_{ij} may take any value in $[0, p)$. Suppose there are n elements b_{ij} such that $i \in U$, $j \in T$, and $j > i$. These are the only elements in C that can be nonzero.

Suppose B'' is of lattice rank r. Then corresponding to this B'' are p^n distinct matrices B of this lattice rank, these being obtained by allowing the n elements in C that can be nonzero to take values in $[0, p)$ independently of each other.

Since every distinct matrix $B \in L_s(\tilde{\gamma})$ corresponds to one unique matrix $B'' \in L_\ell(1^\ell)$, it follows that the proportion of matrices having a particular rank is the same for each set. That is,

$$\mu_{s,r}(\tilde{\gamma}) = \frac{\nu_{s,r}(\tilde{\gamma})}{\nu_s(\tilde{\gamma})} = \frac{\nu_{\ell,r}(1^\ell)}{\nu_\ell(1^\ell)} = \mu_{\ell,r}(1^\ell).$$

This establishes the lemma and hence Theorem 3.1. $\square$

A direct corollary of Theorem 3.1 is obtained by a double substitution of (2.11) in (3.2).

Corollary 3.6 *Let $\ell(\boldsymbol{\gamma})$ be the number of nonzero components in $\boldsymbol{\gamma}$, and let $\nu_s(\boldsymbol{\gamma})$ be the total number of members having upper class $[p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}]$. Then*

$$\nu_{s,r}(\boldsymbol{\gamma}) = \nu_{\ell,r}(1^\ell) p^{\gamma_2 + 2\gamma_3 + \cdots + (s-1)\gamma_s} / p^{\ell(\ell-1)/2},$$

where $\nu_{\ell,r}(1^\ell)$ is the number of lattice rules of rank r in upper class $[p, p, \ldots, p]$.

This reduces significantly the scope of the problem. Essentially the dependency on $\boldsymbol{\gamma}$ has been factored out of $\nu_{s,r}(\boldsymbol{\gamma})$. We now need only expressions for $\nu_{\ell,r}(1^\ell)$, a two-parameter set.

4 Recurrence Relations for $\nu_{\ell,r}(1^\ell)$

In simple cases, we may obtain expressions for $\nu_{\ell,r}(1^\ell)$, $1 \le r \le \ell$, directly. For example, we have $\nu_{\ell,\ell}(1^\ell) = 1$. This is a consequence of Theorem 2.3; the number of matrices B'' for which $\tilde{B} = B'' \bmod p$ has matrix rank zero is just 1. We shall now derive a recurrence formula that yields expressions for other choices of the parameters r and ℓ relatively painlessly as polynomials in p.

Theorem 4.1 *For $1 \le r \le \ell$,*

$$\nu_{\ell+1,r}(1^{\ell+1}) = (p^\ell - p^{\ell-r})\nu_{\ell,r}(1^\ell) + p^{\ell+1-r}\nu_{\ell,r-1}(1^\ell).$$

Proof. Suppose $E \in L_{\ell+1}(1^{\ell+1})$ has lattice rank r, and let $\tilde{E} = E \bmod p$. Then the $(\ell+1) \times (\ell+1)$ matrix $\tilde{E}$ may be written as

$$\tilde{E} = \begin{bmatrix} \tilde{B} & \mathbf{b} \\ \mathbf{0} & 0 \end{bmatrix},$$

where $\tilde{B} = B \bmod p$ for some $B \in L_\ell(1^\ell)$ and $\mathbf{b}$ is a $\ell \times 1$ column vector having components in $[0, p)$. Note that there are p^ℓ possible choices of the vector $\mathbf{b}$ and that each $\tilde{B}$ corresponds to a unique B. The matrix E has lattice rank r if and only if $\tilde{E}$ has matrix rank $\ell + 1 - r$. In this situation, $\tilde{B}$ must have a matrix rank of either $\ell + 1 - r$ or $\ell - r$.

If $\tilde{B}$ has matrix rank $\ell+1-r$, then it has $\ell+1-r$ linearly independent column vectors, say, $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_{\ell+1-r}$. When $\tilde{E}$ has matrix rank $\ell + 1 - r$, $\mathbf{b}$ is linearly dependent on these vectors, and hence we may write

$$\mathbf{b} = \sum_{i=1}^{\ell+1-r} \lambda_i \tilde{\mathbf{b}}_i \bmod p,$$

where $\lambda_i \in [0, p)$. We see that each choice of the λ_i produces a different $\mathbf{b}$. Thus the number of possible $\mathbf{b}$ for which both $\tilde{B}$ and $\tilde{E}$ have matrix rank $\ell+1-r$ is given by $p^{\ell+1-r}$. Moreover, there are $\nu_{\ell,r-1}(1^\ell)$ matrices $\tilde{B}$ that have matrix rank $\ell+1-r$, and so we conclude that the number of matrices $\tilde{E}$ for which both $\tilde{E}$ and $\tilde{B}$ have matrix rank $\ell+1-r$ is given by $p^{\ell+1-r}\nu_{\ell,r-1}(1^\ell)$.

In the second case, when $\tilde{B}$ has matrix rank $\ell-r$, the argument in the preceding paragraph shows that there are $p^{\ell-r}$ vectors $\mathbf{b}$ that result in $\tilde{E}$ having matrix rank $\ell-r$. It then follows that there are $p^\ell - p^{\ell-r}$ vectors $\mathbf{b}$ for which $\tilde{E}$ has the desired matrix rank $\ell+1-r$. Thus the number of matrices $\tilde{E}$ for which $\tilde{E}$ has matrix rank $\ell+1-r$ and $\tilde{B}$ has matrix rank $\ell-r$ (and hence rank deficiency r) is given by $(p^\ell - p^{\ell-r})\nu_{\ell,r}(1^\ell)$.

The arguments in the two preceding paragraphs then establish that for $1 \le r \le \ell$,

$$\nu_{\ell+1,r}(1^{\ell+1}) = (p^\ell - p^{\ell-r})\nu_{\ell,r}(1^\ell) + p^{\ell+1-r}\nu_{\ell,r-1}(1^\ell). \tag{4.2}$$

□

This may be used as a recurrence relation to evaluate $\nu_{\ell,r}(1^\ell)$ as long as it is correctly anchored. For this, one needs $\nu_{\ell,\ell}(1^\ell) = 1$ and $\nu_{\ell,0}(1^\ell) = 0$ for $\ell \ge 1$.

In Theorem 4.1, we obtained the recurrence relation (4.2) for $\nu_{\ell,r}(1^\ell)$, this being the number of ℓ-dimensional lattice rules of rank r belonging to the upper class $[p, p, \dots, p]$. We now note some minor algebraic corollaries that could be useful in practice.

In some contexts, one requires the number of rules $\bar{\nu}_{\ell,r}(\boldsymbol{\gamma})$ of the upper class $(\boldsymbol{\gamma})$ whose rank does not exceed r. As mentioned after the statement of Theorem 3.1, this is

$$\bar{\nu}_{s,r}(\boldsymbol{\gamma}) = \frac{\nu_s(\boldsymbol{\gamma})}{\nu_\ell(1^\ell)} \sum_{m=1}^{r} \nu_{\ell,m}(1^\ell) = \frac{\nu_s(\boldsymbol{\gamma})}{\nu_\ell(1^\ell)} \bar{\nu}_{\ell,r}(1^\ell). \tag{4.3}$$

An independent recurrence relation for $\bar{\nu}_{\ell,r}(1^\ell)$ can be obtained by elementary manipulation of (4.2). This yields

$$\bar{\nu}_{\ell+1,r}(1^{\ell+1}) = (p^\ell - p^{\ell-r})\bar{\nu}_{\ell,r}(1^\ell) + p^{\ell-r}\bar{\nu}_{\ell,r-1}(1^\ell) \quad \text{for } 1 \le r \le \ell, \tag{4.4}$$

anchored by $\bar{\nu}_{\ell,\ell}(1^\ell) = \nu_\ell(1^\ell) = p^{\ell(\ell-1)/2}$ and $\bar{\nu}_{\ell,0}(1^\ell) = 0$ for $\ell \ge 1$. Note that (4.2) and (4.4) are almost identical; the difference being the replacement of a single coefficient $p^{\ell+1-r}$ by $p^{\ell-r}$ in the second term. The same remark applies to (4.6) and (4.8) below.

The expressions for $\nu_{\ell,r}(1^\ell)$ obtained in this way contain significant factors of the form $(p-1)^a p^b$. These can be factored out of the recurrence relation (4.2). It can readily be established that

$$\pi_{\ell,r}(1^\ell) = \frac{\nu_{\ell,r}(1^\ell)}{(p-1)^{\ell-r} p^{(\ell-r)(\ell-r-1)/2}} \tag{4.5}$$

satisfies the recurrence relation

$$\pi_{\ell+1,r}(1^{\ell+1}) = \frac{p^r-1}{p-1}\pi_{\ell,r}(1^\ell) + p^{\ell+1-r}\pi_{\ell,r-1}(1^\ell) \quad \text{for } 1 \le r \le \ell, \tag{4.6}$$

anchored by $\pi_{\ell,\ell}(1^\ell) = 1$ and $\pi_{\ell,0}(1^\ell) = 0$ for $\ell \ge 1$.

Analogously, one may show that

$$\bar{\pi}_{\ell,r}(1^\ell) = \frac{\bar{\nu}_{\ell,r}(1^\ell)}{(p-1)^{\ell-r}p^{(\ell-r)(\ell-r-1)/2}} \tag{4.7}$$

satisfies the recurrence relation

$$\bar{\pi}_{\ell+1,r}(1^{\ell+1}) = \frac{p^r-1}{p-1}\bar{\pi}_{\ell,r}(1^\ell) + p^{\ell-r}\bar{\pi}_{\ell,r-1}(1^\ell) \quad \text{for } 1 \le r \le \ell, \tag{4.8}$$

anchored by $\bar{\pi}_{\ell,\ell}(1^\ell) = p^{\ell(\ell-1)/2}$ and $\bar{\pi}_{\ell,0}(1^\ell) = 0$ for $\ell \ge 1$.

This formula together with (4.6) was used to generate the expressions for $\pi_{\ell,r}(1^\ell)$ and $\bar{\pi}_{\ell,r}(1^\ell)$ for $1 \le r \le \ell \le 5$ given in Table 1.

Table 1: Expressions for $\pi_{\ell,r}(1^\ell)$ and $\bar{\pi}_{\ell,r}(1^\ell)$

ℓ	r	$\pi_{\ell,r}(1^\ell)$	$\bar{\pi}_{\ell,r}(1^\ell)$
1	1	1	1
2	1	1	1
	2	1	p
3	1	1	1
	2	$2p+1$	$(p^3-1)/(p-1)$
	3	1	p^3
4	1	1	1
	2	$3p^2+3p+1$	p^3+2p^2+3p+1
	3	$3p^2+2p+1$	$(p^6-1)/(p-1)$
	4	1	p^6
5	1	1	1
	2	$4p^3+6p^2+4p+1$	$p^4+3p^3+6p^2+4p+1$
	3	$6p^4+8p^3+7p^2+3p+1$	$p^7+2p^6+3p^5+4p^4+5p^3+6p^2+3p+1$
	4	$4p^3+3p^2+2p+1$	$(p^{10}-1)/(p-1)$
	5	1	p^{10}

5 Summary and Example

We summarize here the steps in the calculation of $\nu_{s,r}([\mathbf{b}])$. In practice, we evaluate $\bar{\nu}_{s,r}([\mathbf{b}])$ and finally set $\nu_{s,r}([\mathbf{b}]) = \bar{\nu}_{s,r}([\mathbf{b}]) - \bar{\nu}_{s,r-1}([\mathbf{b}])$.

As described in Section 2, we obtain the prime factorization of $[\mathbf{b}]$ and set

$$\bar{\nu}_{s,r}([\mathbf{b}]) = \prod_{j=1}^{q} \bar{\nu}_{s,r}([\boldsymbol{\sigma}^{(p_j)}]),$$

$[\boldsymbol{\sigma}^{(p_j)}]$ being a prime factor of $[\mathbf{b}]$. The class of the corresponding Sylow p-component is of the form

$$[\boldsymbol{\sigma}^{(p)}] = [p^{\gamma_1}, p^{\gamma_2}, \ldots, p^{\gamma_s}];$$

and for $1 \leq r \leq \ell$ (see (4.3)),

$$\begin{aligned} \bar{\nu}_{s,r}([\boldsymbol{\sigma}^{(p)}]) &= \bar{\nu}_{\ell,r}(1^\ell) p^{\gamma_2+2\gamma_3+\cdots+(s-1)\gamma_s-\ell(\ell-1)/2} \\ &= \bar{\pi}_{\ell,r}(1^\ell)(p-1)^{\ell-r} p^{(\ell-r)(\ell-r-1)/2} p^{\gamma_2+2\gamma_3+\cdots+(s-1)\gamma_s-\ell(\ell-1)/2}, \end{aligned}$$

where ℓ is the number of positive integers in the set $\{\gamma_i : 1 \leq i \leq s\}$. Note that the first factor in this last expression, which depends on ℓ and r, is a polynomial in p of degree not more than $\ell(\ell-1)/2$. The second and third factors depend on $(\ell - r)$ only. The final factor depends on γ_i and on ℓ. For $r > \ell$, we set $\bar{\nu}_{s,r}([\boldsymbol{\sigma}^{(p)}]) = \bar{\nu}_{s,\ell}([\boldsymbol{\sigma}^{(p)}])$.

As an example, we apply these formulas to obtain the number of three-dimensional rules of various ranks belonging to upper class $[42, 36, 14]$. Using the prime factorization given in (2.10), we find

$$\bar{\nu}_{3,r}([42, 36, 14]) = \bar{\nu}_{3,r}([2, 4, 2])\bar{\nu}_{3,r}([3, 9, 1])\bar{\nu}_{3,r}([7, 1, 7]). \tag{5.1}$$

For the first factor on the right, $p = 2$, $\boldsymbol{\gamma} = (1, 2, 1)$, and $\ell = 3$, giving

$$\bar{\nu}_{3,r}([2, 4, 2]) = \bar{\pi}_{3,r}(1^3)(2-1)^{3-r} 2^{(3-r)(3-r-1)/2} 2^{2+2\times 1-3\times 2/2} = \bar{\pi}_{3,r}(1^3) 2^{(3-r)(3-r-1)/2} \times 2.$$

From Table 1 with $\ell = 3$, we find

$$\bar{\pi}_{3,1}(1^3) = 1, \quad \bar{\pi}_{3,2}(1^3) = (p^3-1)/(p-1) = 7, \quad \bar{\pi}_{3,3}(1^3) = p^3 = 8,$$

yielding

$$\bar{\nu}_{3,r}([2, 4, 2]) = 4,\ 14,\ \text{and } 16 \quad \text{for} \quad r = 1, 2, 3.$$

A similar calculation for the other two factors is marginally shorter (since $\ell = 2$, the result for $r = 3$ coincides with that for $r = 2$). We find

$$\bar{\nu}_{3,r}([3, 9, 1]) = 6,\ 9,\ \text{and } 9 \quad \text{for} \quad r = 1, 2, 3$$

and

$$\bar{\nu}_{3,r}([7,1,7]) = 42,\ 49,\ \text{and } 49 \quad \text{for} \quad r = 1,2,3.$$

Putting these values into (5.1) we obtain

$$\begin{aligned} \bar{\nu}_{3,1}([42,36,14]) &= \ \ 4 \times 6 \times 42 = 1008, \\ \bar{\nu}_{3,2}([42,36,14]) &= 14 \times 9 \times 49 = 6174, \\ \bar{\nu}_{3,3}([42,36,14]) &= 16 \times 9 \times 49 = 7056. \end{aligned}$$

These are the number of rules of that upper class having rank r or less. The number having rank r may be obtained by subtraction, giving

$$\nu_{3,r}([42,36,14]) = 1008,\ 5166,\ \text{and } 882 \quad \text{for} \quad r = 1,2,3.$$

We note that these numbers are in surprisingly simple ratio to one another. For example $\bar{\nu}_{3,3} = 7\bar{\nu}_{3,1}$. A similar observation, in a somewhat similar list appearing in [JH92], motivated the present work.

Previously published formulas for the number of lattice rules satisfying various conditions are significantly different from those presented here. The easiest formulas (see [LS89]) are for $\nu_s(N)$, the number of s-dimensional rules of order N. Formulas for $\nu_s(n_1, n_2, \dots, n_s; N)$, the number of rules having specified invariants $n_1 \geq n_2 \geq \cdots \geq n_s$, were derived independently in [L93] and in [JH92]. Both formulas use what is essentially a Sylow p-component decomposition. Formulas are given for

$$\nu_s(p_j^{\alpha_{j,1}}, p_j^{\alpha_{j,2}}, \dots, p_j^{\alpha_{j,s}}; p_j^{\alpha_j}),$$

where $N = \prod_{j=1}^{q} p_j^{\alpha_j}$ and $n_i = \prod_{j=1}^{q} p_j^{\alpha_{j,i}}$ are the prime factor decompositions with $\sum_{i=1}^{s} \alpha_{j,i} = \alpha_j$.

The relation of these results with the present results is tenuous. In our example, the rules belonging to $[42,36,14]$ form a subclass of $7,056$ rules of the total number of $651 \times 1210 \times 2850 = 2,244,973,500$ rules (see [LS89]) of order $42 \times 36 \times 14 = 21,168$. There are $4 \times 3 \times 2 = 24$ possible sets of invariants. If we are interested in the number of rules having only rank 1, one can find that there are $448 \times 1053 \times 2793 = 1,317,580,992$ rank-1 rules in this set.The problem treated here, however, is essentially different. The new result could, of course, be used, in extremis, to find the number of rank-r rules of order N; but this approach would require finding all the upper classes of order N and evaluating $\nu_{s,r}([\mathbf{b}])$ for each.

6 Concluding Remarks

The rank of a lattice rule is one of its significant theoretical properties. For a given lattice rule, however, calculating its rank is not trivial. This paper is limited to finding the number of lattice rules of rank r in a given upper class by using a nonconstructive argument based on proportions. This quantity is first calculated for prime upper classes using recurrence relations. Then the Sylow p-decomposition allows the calculation for any upper class.

At present, it appears to be easier to determine the number of lattice rules of a given rank than to determine the rank of any particular rule. In a companion paper, we shall treat the practical task of determining the individual rank of a given lattice rule when its corresponding generator matrix for the dual lattice, B, is available in utlf.

References

[CL01] R. Cools and J. N. Lyness, *Three- and four-dimensional K-optimal lattice rules of moderate trigonometric degree*, Math. Comp., **70** (2001), pp. 1549–1567.

[JH92] S. Joe and D. C. Hunt, *The number of lattice rules having given invariants*, Bull. Austral. Math. Soc., **46** (1992), pp. 479–495.

[L93] J. N. Lyness, *The canonical forms of a lattice rule*, in Numerical Integration IV, ISNM 112, H. Brass and G. Hämmerlin, eds., Birkhäuser, Basel, 1993, pp. 225–240.

[LJ99] J. N. Lyness and S. Joe, *A constructive approach to lattice rule canonical forms*, BIT, **39** (1999), pp. 701–715.

[LK95] J. N. Lyness and P. Keast, *Application of the Smith normal form to the structure of lattice rules*, SIAM J. Matrix Anal. Appl., **16** (1995), pp. 218–231.

[LS89] J. N. Lyness and T. Sørevik, T. *The number of lattice rules*, BIT, **29** (1989), pp. 527–534.

[LSK91] J. N. Lyness, T. Sørevik, and P. Keast, *Notes on integration and integer sublattices*, Math. Comp., **56** (1991), pp. 243–255.

[M72] D. Maisonneuve, *Recherche et utilisation des 'bons trellis'. Programmation et résultats numériques*, in Applications of Number Theory to Numerical Analysis, S. K. Zaremba, ed., Academic Press, New York, 1972, pp. 121–201.

[N92] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM Publications, Philadelphia, 1992.

[SJ94] I. H. Sloan and S. Joe, *Lattice Methods for Multiple Integration*, Clarendon Press, Oxford, 1994.

[SL89] I. H. Sloan and J. N. Lyness, *The representation of lattice quadrature rules as multiple sums*, Math. Comp., **52** (1989), pp. 81–94.