The Canonical Forms of a Lattice Rule

J. N. Lyness

Abstract. Much of the elementary theory of lattice rules may be presented as an elegant application of classical results. These include Kronecker group representation theorem and the Hermite and Smith normal forms of integer matrices. The theory of the canonical form is a case in point. In this paper, some of this theory is treated in a constructive rather than abstract manner. A step-by-step approach that parallels the group theory is described, leading to an algorithm to obtain a canonical form of a rule of prime power order. The number of possible distinct canonical forms is derived, and this is used to determine the number of integration lattices having specified invariants.

1. Notation Used to Describe and Classify Lattice Rules

An s-dimensional *lattice*, Λ, is a set of points having the property that, when $\mathbf{p}$ and $\mathbf{q}$ are members of Λ, so are $\mathbf{p}+\mathbf{q}$ and $\mathbf{p}-\mathbf{q}$. It may be defined by this property, together with a restriction that there are no points of accumulation. A very familiar lattice is the *unit* lattice Λ_0, which comprises all points $\mathbf{p} = (p_1, p_2, \ldots, p_s)$, all of whose components p_i are integers. An *integration* lattice is a lattice that contains the unit lattice Λ_0 as a sublattice. A *lattice rule* $Q(\Lambda)$ is a quadrature rule for $[0,1)^s$ that employs the points of $\Lambda \cap [0,1)^s$ as an abscissa set $A(Q)$ and assigns an equal weight to each. Some lattice rules are useful for integrating naturally periodic functions. Other lattice rules may be very inefficient. A representative selection of the literature on lattice rules may be found in Sloan (1992) and Niederreiter (1992).

The investigation of lattice rules is hampered by two features: first, the large numbers of different rules that are available, and second, a bewildering lack of uniqueness in the various convenient representations for investigating rules and for classifying them.

A classical approach to lattices is based on the generator matrix. It is readily shown that, given any s-dimensional lattice Λ, there exists a set of s generators $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_s$ such that all points

$$\mathbf{p} = \sum_{i=1}^{s} \lambda_i \mathbf{a}_i \qquad \lambda_i \text{ integer}$$

lie in the lattice, and all lattice points are of this form. The $s \times s$ matrix A whose j-th row is $\mathbf{a}_j$ $(j = 1, 2, \ldots, s)$ is referred to as a generator matrix of the lattice. When

Λ is an integration lattice, it is readily shown that all elements of A are rational and that $N = |\det A|^{-1}$ is the order of $A(Q)$, the abscissa set of $Q(\Lambda)$. An approach based particularly on the generator matrix $(A^{-1})^T$ of the reciprocal lattice $\Lambda^{\perp}$ has proved fruitful. However, inconvenient aspects of this approach include the absence of uniqueness of A and the difficulty of proceeding from the matrix A to a sum of function values.

The standard number theoretic rules of Korobov (1959) are also lattice rules. These are conventionally expressed in the form

$$Qf = \frac{1}{n}\sum_{j=1}^{n} \overline{f}\left(\frac{\mathbf{z}}{n}j\right). \tag{1.1}$$

Here $\mathbf{z} \in \Lambda_0$, and $\overline{f}(\mathbf{x})$ is a periodic continuation of $f(\mathbf{x})$ that coincides with $f(\mathbf{x})$ in $[0,1)^s$. As is conventional, we denote $\mathbf{x}$ modulo Λ_0 by $\{\mathbf{x}\}$. The components of $\{\mathbf{x}\}$ are the respective nonnegative fractional parts of the components of $\mathbf{x}$.

Only some lattice rules (those of rank 1) can be expressed in this form. On the other hand, all lattice rules may be expressed in a natural generalization of form (1.1) that we refer to as a t-cycle $D - Z$ rule form. This is

$$Qf = \frac{1}{d_1 d_2 \ldots d_t}\sum_{j_1=1}^{d_1}\sum_{j_2=1}^{d_2}\cdots\sum_{j_t=1}^{d_t} \overline{f}\left(\sum_{i=1}^{t}\frac{\mathbf{z}_i}{d_i}j_i\right), \tag{1.2}$$

where d_i are integers and $\mathbf{z}_i \in \Lambda_0$. Associated with this form are two integer matrices. $D = \mathrm{diag}\{d_1, d_2, \ldots, d_t\}$ is a $t \times t$ diagonal matrix, and Z is the $t \times s$ matrix whose j-th row is $\mathbf{z}_j$.

It is not difficult to show that this form represents a lattice rule. In fact, it is the rule of lowest order N that includes

$$\mathbf{c}_i = \{\mathbf{z}_i/d_i\} \qquad i = 1, 2, \ldots, t.$$

The lattice Λ is generated by these $\mathbf{c}_i$ together with the unit vectors $\mathbf{e}_k$, $k = 1, 2, \ldots, s$. Note that the m-panel product trapezoidal rule is a lattice rule. One of its s-cycle $D - Z$ forms has $D = mI$ and $Z = I$.

Form (1.2) is not unique. Moreover, it may be *repetitive*. That is, for some integer k, it may include only $d_1 d_2 \ldots d_t/k$ distinct abscissas, each repeated k times.

Definition 1.3 *The component* $\mathbf{z}/n$, *where* $\mathbf{z} = (\zeta_1, \zeta_2, \ldots, \zeta_s) \in \Lambda_0$ *is termed* proper *when* $gcd(\zeta_1, \zeta_2, \ldots, \zeta_s, n) = 1$ *and* $\mathbf{c} = \mathbf{z}/n \in [0,1)^s$. *(Colloquially,* $\mathbf{z}/n$ *is in its lowest terms and the point is in the integration region.)*

If $\mathbf{z}/n$ in (1.1) is not proper, then the form is repetitive. This sort of trivial repetition is easy to recognize. However, possible repetition in the general t-cycle $D - Z$ form need not be at all obvious.

It is straightforward to show (see Sloan and Lyness 1989) that a necessary and sufficient condition for the rule form Qf in (1.2) to be repetitive is that there exist integers $j_1, j_2, \ldots, j_t$ with $j_i \in [0, d_i)$, not all zero, such that

$$\sum_{i=1}^{t} \frac{j_i \mathbf{z}_i}{d_i} \in \Lambda_0. \tag{1.4}$$

One classification of lattice rules based on the t-cycle form relies on the circumstance that the elements of the abscissa set $A(Q)$ form a group G under addition modulo Λ_0.

In Sloan and Lyness (1989), the Kronecker group representation theorem was applied to this group to show that a t-cycle nonrepetitive $D - Z$ form exists in which all elements d_i exceed 1, and $d_{i+1} \mid d_i$, and the $\mathbf{z}_i$ are linearly independent. Such a rule form was termed a *canonical form*. From the nomenclature of group theory, these particular values of d_i are termed *invariants*, and this particular value of t is termed the *rank* of the rule Q. The rank and invariants are unique to the lattice, but the choice of $\mathbf{z}_i$ in the canonical form is far from unique. However, no constructive approach for proceeding from a general t-cycle form to a canonical form was made available at that time.

This paper is concerned with finding a canonical form of a rule defined by a general t-cycle $D - Z$ form. We shall, in fact, show only how to find *nonrepetitive* forms in which $d_{i+1} \mid d_i$. We may then rely on Corollary 4.6 of Sloan and Lyness (1989) which assures us that a form that appears to be canonical is indeed canonical if it is nonrepetitive. (See Theorem 3.1 below.)

2. Decomposition and Reassembly

The accompanying table illustrates the underlying group theory.

G	F_1	F_2		F_s
S_1	E_{11}	E_{12}	$\ldots$	E_{1s}
S_2	E_{21}	E_{22}	$\ldots$	E_{2s}
$\vdots$				
S_q	E_{q1}	E_{q2}	$\ldots$	E_{qs}

Each entry is an Abelian group. Any group in the initial row (column) is the direct sum of the other groups in that row (column), and the groups in all but the initial column are cyclic groups. The table illustrates the decomposition of an *Abelian* group G of order $N = p_1^{\beta_1} p_2^{\beta_2} \ldots p_q^{\beta_q}$ into the direct sum of *cyclic* groups F_k. Here

$p_1, p_2, \ldots, p_q$ are distinct primes, and β_i are positive integers. The first stage is the decomposition of G into the direct sum

$$G = S_1 \oplus S_2 \oplus \ldots \oplus S_q \tag{2.1}$$

of its Sylow p groups. S_j, which is of order $p_j^{\beta_j}$, contains all elements of G whose order is any integer power of p_j. Any *noncyclic* Abelian group of prime power order may be decomposed into a direct sum of *cyclic* groups. Thus,

$$S_j = E_{j,1} \oplus E_{j,2} \oplus \ldots \oplus E_{j,s}, \tag{2.2}$$

where $E_{j,k}$ is a *cyclic* group of order $p_j^{\beta_{j,k}}$. These have been arranged in order so that $\beta_{j,k} \geq \beta_{j,k+1}$. Clearly, $\sum_{k=1}^{s} \beta_{j,k} = \beta_j$. There may be fewer nontrivial groups than indicated here. The theory is not compromised if some trivial groups $E_{j,k}$, which contain only the identity element, are included but ignored. For these, $\beta_{j,k} = 0$.

Finally, we apply the result that the direct sum of *cyclic* groups whose orders are mutually prime is also a cyclic group. Thus,

$$F_k = E_{1,k} \oplus E_{2,k} \oplus \ldots \oplus E_{q,k} \tag{2.3}$$

is a *cyclic* group of order $n_k = \prod_{j=1}^{q} p_j^{\beta_{jk}}$. Note that, since $\beta_{j,k} \geq \beta_{j,k+1}$, it follows that $n_{k+1} \mid n_k$.

What is illustrated here is the Kronecker decomposition of an Abelian group G into the direct sum of s cyclic groups F_k; $k = 1, 2, \ldots, s$. The nontrivial values of n_k are termed the invariants of G, and the number of these is termed the rank of G.

The above remarks comprise at most a schematic for a possible derivation of a famous theorem in group theory. For our purposes, as we shall see, we do not *need* group theory. We may use the schematic to derive a canonical form.

It appears that in our application, the decomposition (2.1) into Sylow p groups is very simple, as is the recomposition (2.3) of the cyclic groups $E_{j,k}$ into F_k. However, the middle stage (2.2) is nontrivial. The following examples illustrate the first and third operations. These are justified in the following theorem.

Theorem 2.4 *Let $n = pq$, $(p, q) = 1$, and $\mathbf{z}, \mathbf{z}_1, \mathbf{z}_2 \in \Lambda_0$. Then*

$$\sum_{j=1}^{n} \overline{f}\left(\frac{j\mathbf{z}}{n} + \epsilon\right) = \sum_{j_1=1}^{p} \sum_{j_2=1}^{q} \overline{f}\left(\frac{j_1\mathbf{z}}{p} + \frac{j_2\mathbf{z}}{q} + \epsilon\right)$$

and

$$\sum_{j_1=1}^{p} \sum_{j_2=1}^{q} \overline{f}\left(\frac{j_1\mathbf{z}_1}{p} + \frac{j_2\mathbf{z}_2}{q} + \epsilon\right) = \sum_{j=1}^{n} \overline{f}\left(\frac{j\mathbf{z}_3}{pq} + \epsilon\right),$$

where $\mathbf{z}_3 = q\mathbf{z}_1 + p\mathbf{z}_2$. Moreover, if $\mathbf{z}_1/p$ and $\mathbf{z}_2/q$ are proper *(see Definition (1.3) above), so is $\{\mathbf{z}_3/pq\}$.*

The proof of either part is trivial. Note that there are no minor restrictions. For example, $\mathbf{z}_2/q$ need not be in its lowest terms. The ϵ is notationally helpful in establishing extensions of these results.

As an example, we put the following rule into canonical form.

Example 2.5

$$Qf = \frac{1}{12.15} \sum_{j_1=1}^{12} \sum_{j_2=1}^{15} \overline{f}\left(\frac{(5,8,3)}{12} j_1 + \frac{(8,1,0)}{15} j_2 \right). \tag{2.5}$$

This may be reexpressed as

$$\frac{1}{4.3.3.5} \sum_{j_1=1}^{4} \sum_{j_2=1}^{3} \sum_{j_3=1}^{3} \sum_{j_4=1}^{5} \overline{f}(\mathbf{x}),$$

where

$$\mathbf{x} = \frac{(5,8,3)}{4} j_1 + \frac{(5,8,3)}{3} j_2 + \frac{(8,1,0)}{3} j_3 + \frac{(8,1,0)}{5} j_4.$$

This may be replaced by

$$\mathbf{x}' = \frac{(1,0,3)}{4} j_1 + \frac{(2,2,0)}{3} j_2 + \frac{(2,1,0)}{3} j_3 + \frac{(3,1,0)}{5} j_4.$$

The sum in (2.5), which contains 180 elements of G, has now been reexpressed as the direct sum of three Sylow p groups, with $p = 2$, 3, and 5, respectively. Those with $p = 2$ and 5 are already cyclic groups. The Sylow 3 group is the direct sum of two cyclic groups.

The intermediate stage comprises, in general, removing repetition from each of the Sylow p groups. In this case, it is clear by inspection that the groups of order 3 are distinct. That is, the sums over j_2 and j_3 include nine distinct terms and not three. Applying the second part of Theorem 2.4 twice, we find successively

$$\begin{aligned} Qf &= \frac{1}{180} \sum_{j_{12}=1}^{12} \sum_{j_3=1}^{3} \sum_{j_4=1}^{5} \overline{f}(\mathbf{x}'') \\ &= \frac{1}{180} \sum_{j_{124}=1}^{60} \sum_{j_3=1}^{3} \overline{f}(\mathbf{x}''') \\ &= \frac{1}{180} \sum_{k_1=1}^{60} \sum_{k_2=1}^{3} \overline{f}\left(\frac{(31,52,45)}{60} k_1 + \frac{(2,1,0)}{3} k_2 \right). \end{aligned} \tag{2.6}$$

Here

$$\mathbf{x}'' = \frac{(11,8,9)}{12} j_{12} + \frac{(2,1,0)}{3} j_3 + \frac{(3,1,0)}{5} j_4,$$

and

$$\mathbf{x}''' = \frac{(91,52,45)}{60} j_{124} + \frac{(2,1,0)}{3} j_3.$$

This rule form (2.6) is in canonical form.

The reader may have noticed that the overall result can be significantly altered by what appears at first sight to be a minor change in the problem. For example, if in Example 2.5 we replace the second vector (8,1,0) by (7,1,0), we find that the vector (2,1,0) in $\mathbf{x}'$ must be replaced by (1,1,0). The middle stage becomes

$$\sum_{j_2=1}^{3}\sum_{j_3=1}^{3}\overline{f}\left(\frac{(2,2,0)}{3}j_2+\frac{(1,1,0)}{3}j_3+\epsilon\right)=3\sum_{j_{23}=1}^{3}\overline{f}\left(\frac{(1,1,0)}{3}j_{23}+\epsilon\right).$$

The new form Qf is repetitive, and Q has one invariant instead of two.

A satisfactory procedure to obtain the canonical form cannot rely on the chance recognition of this sort of circumstance. Subsequent sections are devoted to providing an algorithm for handling this problem.

3. Rules of Prime Power Order

As a preliminary, we remove some trivial complications. We are interested only in sequential proper forms. Qf is *sequential* if $d_1 \geq d_2 \geq \ldots \geq d_t > 1$. The i-th component is *proper* if $\mathbf{z}_i/d_i$ is in its lowest terms and $\mathbf{c}_i = \mathbf{z}_i/d_i \in [0,1)^s$. The form is sequential proper when it is sequential and each element is proper. It is a trivial task to reexpress Qf in a t' cycle $D-Z$, sequential proper form.

A geometric view is that the rule may be defined by t points $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_t$ of orders $d_1, d_2, \ldots, d_t$, respectively. A sequential proper form may be immediately constructed by reordering the points so that $d_1 \geq d_2 \ldots \geq d_t > 1$, and setting $\mathbf{z}_i = d_i\{\mathbf{c}_i\}$.

It still may be repetitive (trivially if $\mathbf{c}_i = \mathbf{c}_{i+1}$ and $d_i = d_{i+1}$).

Theorem 4.5 and its corollary 4.6 in Sloan and Lyness 1989 assure us that a non repetitive sequential proper rule form in which $d_{i+1} \mid d_i$ is a canonical form. This is difficult to exploit as it is difficult in general to recognize a non repetitive form. However, the theory becomes much easier as soon as we restrict ourselves to prime power forms. In this section we deal with lattices and rule forms of prime power order; these are t cycle $D-Z$ rule forms in which

$$d_j = p^{\alpha_j} \qquad j = 1, 2, \ldots, t, \tag{3.1}$$

where p is a prime. For these, the divisibility condition is naturally satisfied and it follows:

Theorem 3.1 *A prime power sequential proper form is canonical if and only if it is non repetitive.*

In other words, a prevalent situation in which a rule form is both non repetitive and not canonical does not arise in the prime power order context.

In this section and in sections 4 and 5, we deal with lattices and rule forms of prime power order only. The problem of finding a canonical form reduces to that of recognizing and removing repetition.

Theorem 3.2 *Let Qf and $Q'f$ be prime power t-cycle $D - Z$ forms having the same prime p, and the same Z matrix. Let $D = diag(d_1, d_2, \ldots, d_t)$ and $D' = diag(p, p, \ldots, p) = pI$. Then Qf and $Q'f$ are either both repetitive or both nonrepetitive.*

Proof. The condition for Qf to be repetitive is that there exist integers $j_i \in [0, d_i)$ $i = 1, 2, \ldots, t$ not all zero such that

$$\sum_{i=1}^{t} j_i \mathbf{z}_i / d_i \in \Lambda_0. \tag{3.3}$$

Let us suppose that Qf is repetitive and the above j_i exist. Let I' be $\{i \mid j_i \neq 0\}$. Let $j_i/d_i = \gamma_i/m_i$ in their lowest terms. Then $\gamma_i \neq 0$, $i \in I'$, and

$$\sum_{i \in I'} \gamma_i \mathbf{z}_i / m_i \in \Lambda_0. \tag{3.4}$$

Let $p^\lambda = \max_{i \in I'} m_i$. Let I'' be $\{i \mid m_i = p^\lambda\}$. Then multiplying (3.4) by $p^{\lambda-1}$ and subsuming all integers to the right, we obtain

$$\sum_{i \in I''} \gamma_i \mathbf{z}_i / p \in \Lambda_0. \tag{3.5}$$

This statement implies that $Q'f$ is repetitive.

The converse is marginally simpler to prove. If we set

$$\begin{array}{ll} j_i = \gamma_i d_i / p & i \in I'' \\ j_i = 0 & i \notin I'', \end{array}$$

we recover (3.3) from (3.5). □

Recasting this theorem geometrically is revealing.

Corollary 3.6 *Any nonrepetitive prime power t-cycle rule form includes precisely $p^t - 1$ distinct points of order p.*

Theorem 3.2 shows that the critical quantities in determining whether a prime power form is repetitive is the Z matrix. The integers d_i play a secondary role. This is confirmed in the following theorem.

Theorem 3.7 *A t-cycle $D - Z$ form of a prime power rule is repetitive if and only if the rank of Z modulo p is less than t.*

Proof: In view of Theorem 3.2, we need only establish this for a t-cycle $D' - Z$ form where

$$D' = \text{diag}\{p, p, \ldots, p\}.$$

If this is repetitive, there exist $j_1, j_2, \ldots, j_t$, not all zero such that

$$\left\{ \sum_{i=1}^{t} j_i \mathbf{z}_i / p \right\} = \mathbf{0}.$$

This implies that $\sum_{i=1}^{t} j_i \mathbf{z}_i = p\mathbf{u}$ for some $\mathbf{u} \in \Lambda_0$; this is the condition that the rank of Z modulo p is less than t. $\square$

The simple results of this section may be readily incorporated into an algorithm that transforms a general p-power t-cycle $D - Z$ rule form into a sequential, proper, and non-repetitive form. In the final form, Z either is unimodular or contains a $t \times t$ unimodular submatrix.

This algorithm is a variant of a standard triangularization technique.

At the start of the j-th stage, we have

$$d_1 \geq d_2 \geq \ldots \geq d_j \geq \ldots \geq d_t > 1$$

all being powers of p, and $\mathbf{z}_i/d_i$ $i = 1 \ldots j-1$ are all proper. Associated with $\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_{j-1}$ we have distinct integers $i_1, i_2, \ldots, i_{j-1}$, which we term *column indices*. Moreover,

$$\left.\begin{array}{ll} Z_{r,i_c} = 1 & \text{when} \quad r = c \\ Z_{r,i_c} = 0 & \text{when} \quad r > c \end{array}\right\} \begin{array}{l} c = 1, 2, \ldots, j-1 \\ r = 1, 2, \ldots, t \end{array}.$$

The j-th stage comprises the following:

1. Let $\mathbf{z}_j = (\zeta_1, \zeta_2, \ldots, \zeta_s)$. Identify a component, say ζ_ℓ, for which $(\zeta_\ell, p) = 1$. Set $i_j = \ell$. Replace $\mathbf{z}_j$ by $k\mathbf{z}_j$, where $k = \zeta_\ell^{-1} (\text{mod } d_j)$ and then replace $\mathbf{z}_j$ by $\mathbf{z}'_j = (\zeta'_1, \zeta'_2, \ldots, \zeta'_s)$ with $\zeta'_i \in [0, d_j)$. (This leaves $\zeta'_\ell = 1$.)

2. For $i > j$, replace $\mathbf{z}_i$ by $\mathbf{z}_i - Z_{i,\ell}\mathbf{z}_j$. (This leaves $Z_{i,\ell} = 0$; $i > j$.)

3. Carry out trivial adjustments on Z and D necessary to leave a t'-cycle $D - Z$ sequential proper form.

Comments:

1. We have by hypothesis that $\mathbf{z}_j/d_j$ is proper. Thus, there is some component of $\mathbf{z}_j$, say the ℓ-th, that is not a multiple of p, and ℓ may be chosen for i_j in 1.

3. These adjustments include the following:

   a. Put any improper $\mathbf{z}_i/d_i$ into proper form $\mathbf{z}'_i/d'_i$.

b. Remove any rows $\mathbf{z}_i$ for which either $\mathbf{z}_i = \mathbf{0}$ or $d_i = 1$; naturally this step reduces the value of t.

c. If necessary, reorder the rows of Z so that the ordering of d_i is sequential.

The final Z matrix is an integer matrix. If its columns were permuted in accordance with the column indices, it would be upper triangular with unit diagonal. Thus, it contains a $t \times t$ unimodular submatrix (corresponding to retaining only the columns numbered $i_1, i_2, \ldots, i_t$).

Because of this unimodularity, it follows that when $t = s$, the matrix $A = D^{-1}Z$ is a generator matrix of Λ. In general, $t < s$, and $\tilde{A} = D^{-1}Z$ comprises the first t rows of a generator matrix. The remaining $s - t$ rows of the generator matrix may be chosen as unit vectors $\mathbf{e}_\lambda$, the λ being the elements of $[1, s]$ not assigned to be column indices.

Finally, note that Z is *not* unique. In general, the column indices can be chosen in many ways, and rows having the same d element may be interchanged.

4. Canonical Form Redundancy of Prime Power Forms

In the preceding section, we remarked that the Z matrix is not unique. In this section, we quantify this lack of uniqueness. We take an r-cycle prime power rule form Qf which is in canonical form; we see how many distinct reassignments of Z exist. Initially, we shall have to assume that the result depends on p, D, and Z. However, it will appear that it simply depends on p and D. Let

$$Qf = \frac{1}{n_1 n_2 \ldots n_r} \sum_{j_1=1}^{n_1} \sum_{j_2=1}^{n_2} \cdots \sum_{j_r=1}^{n_r} \overline{f}\left(\sum_{k=1}^{r} \frac{j_k \mathbf{z}_k}{n_k}\right) \tag{4.1}$$

be a canonical form of Q. Here as before,

$$n_1 \geq n_2 \geq \ldots \geq n_r > 1,$$

and each n_i is a power of p. Also, $\mathbf{z}_k \in [0, n_k)^s$, $k = 1, 2, \ldots, r$. Note that, since this is a canonical form, we know that $\mathbf{z}_k / n_k$ is in its lowest terms. Each member of the set of generators

$$\mathbf{c}_k = \mathbf{z}_k / n_k \tag{4.2}$$

is itself an element of $[0, 1)^s$.

Definition 4.3 $\bar{\bar{\mu}}_s(n_1, n_2, \ldots, n_s; N; Z)$ *is the number of distinct ways of assigning the Z-matrix so that the rule is the same. (Here $\mathbf{z}_k \in [0, n_k)^s$.)*

Geometrically, this is the number of different point sets $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_r$ that can be put into (4.1) leaving the same rule. These points are $\in [0, 1)^s$.

It will appear that $\bar{\bar{\mu}}_s$ is independent of Z, and we shall later drop the Z in the definition.

The construction of a formula for $\bar{\bar{\mu}}_s$ uses relatively straightforward concepts that nevertheless must be applied with care. We shall suppose that we assign the vectors $\mathbf{z}_j$ (or $\mathbf{c}_j = \mathbf{z}_j/n_j$) in turn, starting with $j = 1$ and ending with $j = r$. Clearly, every $\mathbf{c}_j$ has to be a member of the abscissa set. Thus, when we start the j-th stage, we may limit the choice for $\mathbf{c}'_j$ as follows:

$$\mathbf{c}'_j = \sum_{i=1}^{r} \lambda_i^j \mathbf{c}_i \qquad \lambda_i^j \in [0, n_i) \tag{4.4}$$

or

$$\mathbf{z}'_j = \sum_{i=1}^{r} \lambda_i^j \frac{n_j}{n_i} \mathbf{z}_i. \tag{4.5}$$

It is convenient to drop the { } symbol here. The restriction $\lambda_i^j \in [0, n_i)$ in (4.4) simply prevents duplication, since $\lambda_i^j \mathbf{c}_i \equiv (\lambda_i^j + n_i)\mathbf{c}_i$. When assigning $\mathbf{c}'_j$, it is clear that for those values of i for which $n_i < n_j$, we may choose any available λ_i^j, and hence there are n_i distinct choices for each such λ_i^j. However, for those values of i for which $n_i > n_j$, the choice has to be restricted so that $\mathbf{z}'_j$ in (4.5) turns out to be in Λ_0. That is, $\lambda_i^j(n_j/n_i)$ must be an integer. Thus, for these values of i, there are only n_j distinct choices for each λ_i^j. (Geometrically, this recognizes that $\mathbf{c}_j$ is of order n_j and therefore only multiples of $\mathbf{c}_i$ of this order or less may be included.) There remain values of i for which $n_i = n_j$.

To fix ideas, suppose $n_{j+1} > n_j > n_{j-1}$. Then there is only one value λ_j^j remaining to assign. Since $\mathbf{z}_j$ itself must be attainable, we can allow λ_j^j to take one of $n_j(1 - p^{-1})$ distinct values only.

In this case, then, the number of ways of assigning $\mathbf{z}'_j$ is the product over i of the number of ways of assigning λ_j^i. This gives

$$\prod_{i=1}^{j-1} n_j \times n_j \left(1 - \frac{1}{p}\right) \times \prod_{i=j+1}^{r} n_i.$$

Thus, when $n_{j-1} > n_j > n_{j+1}$, whatever the individual values of $\mathbf{z}_i$, $i = 1, 2, \ldots, r$, the number of ways of reassigning $\mathbf{z}_j$, without changing any other $\mathbf{z}_i$ is

$$n_j^j \prod_{i=j+1}^{r} n_i \left(1 - \frac{1}{p^{\lambda(j)}}\right) \text{ with } \lambda(j) = 1.$$

In general, we cannot expect all n_j to be distinct. Let us suppose

$$n_j > n_{j+1} = n_{j+2} = \ldots = n_{j+w} > n_{j+w+1} \tag{4.6}$$

and isolate the part of the calculation involving the assignment of $\mathbf{c}'_{j+1} \ldots \mathbf{c}'_{j+w}$ to the extent that this is affected by $\mathbf{c}_{j+1} \ldots \mathbf{c}_{j+w}$. For convenience, we suppress the

subscript j and denote by n the common value n_{j+1}. We need to consider the number of possibilities for

$$\begin{aligned} \mathbf{c}'_1 &= \sum_{i=1}^{w} \lambda_i^1 \mathbf{c}_i \\ \mathbf{c}'_2 &= \sum_{i=1}^{w} \lambda_i^2 \mathbf{c}_i \\ &\cdots \\ \mathbf{c}'_w &= \sum_{i=1}^{w} \lambda_i^w \mathbf{c}_i. \end{aligned} \tag{4.7}$$

These are assigned in the following order. First, λ_i^1, $i = 1, 2, \ldots, w$ are assigned. We need $\mathbf{c}'_1$ to be of order n. To ensure this, λ_i^1 may be chosen in any way so long as at least one term $\lambda_i^1 \mathbf{c}_i$ is of order n. This is equivalent to choosing a point of order n in a w-dimensional space. The number of points is $n^w(1 - p^{-w})$. Later in the calculation, we have to assign $\mathbf{c}'_2$. However, $\mathbf{c}_1$ has already been assigned and is of order n. To ensure that $n\mathbf{c}_2$ is independent of $n\mathbf{c}_1$, one must ensure that at least one of $\lambda_i^2 \mathbf{c}_i$, $i = 2, 3, \ldots, w$ is of order n. λ_1^2 is not restricted. The number of points available is $n^w(1 - p^{-w+1})$.

Continuing in this way, we find the number of ways of assigning $\mathbf{c}'_k$, $k = 1, 2, \ldots, w$ to be

$$n^w(1 - p^{-w-1+k}).$$

We note again that the result does not depend in detail on the rule form. It depends only on p and on $n_1, n_2, \ldots, n_r$. When several n_j are equal, it depends particularly on the pattern. It is notationally convenient to define an integer index.

Definition 4.8 *With respect to*

$$\begin{aligned} &n_1 \geq n_2 \geq n_3 \geq \ldots \geq n_r, \text{ the index} \\ &\lambda(j) = k - j, \end{aligned} \tag{4.8}$$

where k is the smallest integer for which $n_k < n_j$.

Theorem 4.9 *Given a rule form Qf, the number of nontrivial ways of reassigning $\mathbf{c}_j$ so that the rule remains unaltered is*

$$\prod_{i=1}^{r} n_{\max(i,j)} \left(1 - \frac{1}{p^{\lambda(j)}}\right). \tag{4.9}$$

This number, large as it is, refers only to the number of ways of reassigning $\mathbf{c}_j$. Since it is independent of the individual choice for the other generators $\mathbf{c}_i$ $(i \neq j)$, we obtain the total number of nontrivial assignments as the product of r corresponding terms. Thus, we have the following corollary.

Corollary 4.10

$$\begin{aligned}\bar{\bar{\mu}}_s(n_1, n_2, \ldots, n_s; N) &= \prod_{j=1}^{r} n_j^j \prod_{i=j+1}^{r} n_i(1 - p^{-\lambda(j)}) \\ &= N \prod_{t=1}^{r} n_t^{2t-2}(1 - p^{-\lambda(t)}).\end{aligned} \tag{4.10}$$

5. The Number of Distinct Prime Power Rules Having Specified Invariants

In the preceding section we derived a formula for $\bar{\bar{\mu}}_s(n_1, n_2, \ldots, n_s; N)$. This is the number of distinct assignments for $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_r$ that give rise to the same rule Q. The formula is the same for any rule having these invariants. We may exploit this fact to derive a formula for the number of distinct rules $\nu_s(n_1, n_2, \ldots, n_s; N)$ having these invariants.

Definition 5.1 *$\bar{\mu}_s(n_1, n_2, \ldots, n_s; N)$ is the number of distinct ways of assigning the Z matrix so that the rule has these invariants. (Here $\mathbf{z}_k \in [0, n_k)^s$.)*

Geometrically, this is the number of different point sets $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_r$ that can be substituted into (4.1) to give a nonrepetitive rule form.

Comparing Definition 5.1 with Definition 4.3 shows that $\bar{\mu}_s$ is larger than $\bar{\bar{\mu}}_s$. Since the redundancy is the same for each distinct rule, it follows that

$$\nu_s(n_1, n_2, \ldots, n_s; N) = \frac{\bar{\mu}_s(n_1, n_2, \ldots, n_s; N)}{\bar{\bar{\mu}}_s(n_1, n_2, \ldots, n_s; N)}. \tag{5.2}$$

The determination of $\bar{\mu}_s$ is an exercise of the same type as the determination of $\bar{\bar{\mu}}_s$ but much easier in detail. (The formula does not bring in the pattern of n_i explicitly.)

The rule may be defined by an assignment of r points $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_r$. ($\mathbf{c}_i = \mathbf{z}_i/n_i$ is a point of order n_i.) $\bar{\mu}_s$ is the number of distinct point assignments. This is calculated as $\prod_{j=1}^{r} P_j$, where P_j is the number of ways of choosing $\mathbf{c}_j$ once $\mathbf{c}_1$, $\mathbf{c}_2$, and $\mathbf{c}_{j-1}$ have already been assigned.

The number of points of order n_j is $n_j^s(1 - p^{-s})$. (This is because when $n = p^\alpha$, the grid containing n^s points contains all points of orders $1, p, \ldots, p^\alpha$. The number of order precisely p^α is $(p^\alpha)^s - (p^{\alpha-1})^s$.) However, if $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{j-1}$ have already been assigned, in view of Theorem 3.2, $\mathbf{c}_j$ must be chosen so that the order p points it introduces have not been included previously. There are in total $p^s - 1$ order p points. The number of these in the span of $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{j-1}$ is $p^{j-1} - 1$. Thus, a proportion $(p^{j-1} - 1)/(p^s - 1)$ of the order p points is not available; alternatively stated, a proportion $(p^s - p^{j-1})/(p^s - 1) = (1 - p^{-s+j-1})/(1 - p^{-s})$ is available. It follows relatively painlessly that of the $n_j^s(1 - p^{-s})$ points of order n_j, only that proportion

give rise to available order p points. Thus, $\mathbf{c}_j$ may be chosen in $n_j^s(1-p^{j-1-s})$ ways. Hence,

$$\begin{aligned}\bar{\mu}_s &= \prod_{j=1}^{r} P_j = \prod_{j=1}^{r} n_j^s(1-p^{j-1-s}) \\ &= N^s \prod_{j=1}^{r}(1-p^{j-1-s}). \end{aligned} \tag{5.3}$$

The final stage gives the following theorem.

Theorem 5.4

$$\nu_s(n_1, n_2, \ldots, n_s; N) = \prod_{j=1}^{\lfloor s/2 \rfloor} \left(\frac{n_j}{n_{s+1-j}}\right)^{s-2j+1} \prod_{j=1}^{r} \frac{(1-1/p^{s+1-j})}{(1-1/p^{\lambda(j)})}. \tag{5.4}$$

Here $n_1 \geq n_2 \geq \ldots \geq n_r > 1$, and we have set $n_j = 1$ for all $j \in [r+1, s]$. The index $\lambda(j)$ is defined in (4.8).

With a single exception, $\nu_s > 1$. The exception is the s-dimensional m copy rule. Here all the invariants are equal, and the set $\lambda(j)$ comprises the first s positive integers.

The first three cases are

$$\nu_s(n_1, 1^{s-1}; N) = N^{s-1}(1-1/p^s)/(1-1/p) \tag{5.5}$$

$$\nu_s(n_1, n_2, 1^{s-2}; N) = (N^{s-1}/n_2^2)(1-1/p^s)(1-1/p^{s-1})/(1-1/p^{j_1})(1-1/p), \tag{5.6}$$

where

$$\begin{aligned} j_1 &= 1 \quad \text{when} \quad n_1 > n_2 > 1 \\ &= 2 \quad \text{when} \quad n_1 = n_2 > 1, \end{aligned}$$

$$\nu_s(n_1, n_2, n_3, 1^{s-3}; N) = \frac{N^{s-1}}{n_2^2 n_3^4} \frac{(1-1/p^s)(1-1/p^{s-1})(1-1/p^{s-2})}{(1-1/p^{k_1})(1-1/p^{k_2})(1-1/p)}, \tag{5.7}$$

where

$$\begin{array}{lll} k_1 = k_2 = 1 & \text{when} & n_1 > n_2 > n_3 > 1 \\ k_1 = 3;\ k_2 = 2 & \text{when} & n_1 = n_2 = n_3 > 1 \\ k_1 = 2;\ k_2 = 1 & \text{otherwise.} & \end{array}$$

These are valid only when $n_1 \geq n_2 \geq \ldots \geq n_r > 1$ and each n_i is a power of the same prime p.

These results have been obtained independently by Joe and Hunt (1992). Their general approach follows much the same lines as the one here. However, their derivation of $\bar{\bar{\mu}}_s$ is embedded in group theory.

These results resemble a similar result (Lyness and Sørevik 1989) for $\nu_s(N)$, the number of distinct lattice rules of order N. When $N = p^\beta$, this is

$$\nu_s(N) = N^{s-1} \prod_{i=1}^{s-1} \left[\left(1 - \frac{1}{p^{i+\beta}}\right) \Big/ \left(1 - \frac{1}{p^i}\right)\right]. \tag{5.8}$$

6. A General Formula for $\nu_s(\mathbf{n}; N)$

A simple application of the group decomposition described in Section 2 allows us to base a general formula for $\nu_s(\mathbf{n}; N)$ on the one valid only for prime power rules in Theorem 5.4. The decomposition (2.1) of G into the direct sum of Sylow p groups has the property that when G has invariants $\mathbf{n}(G)$, the invariants $\mathbf{n}(S_p)$ of each Sylow p group is known. The uniqueness of this decomposition leads to the result that the number of distinct abscissa sets for which G has invariants $\mathbf{n}(G)$ is the product of the several corresponding numbers for each component S_p.

Theorem 6.1 *Let the prime decomposition of N be*

$$N = p_1^{\beta_1} p_2^{\beta_2} \dots p_q^{\beta_q}.$$

Let the invariants n_k of a rule Q of order N be given by

$$n_k = p_1^{\beta_{1k}} p_2^{\beta_{2k}} \dots p_q^{\beta_{qk}} \qquad k = 1, 2, \dots, s.$$

Then the number of distinct rules Q having these invariants is

$$\nu_s(n_1, n_2, \dots, n_s, N) = \prod_{j=1}^{q} \nu_s(p_j^{\beta_{j1}}, p_j^{\beta_{j2}}, \dots, p_j^{\beta_{js}};\ p_j^{\beta_j}),$$

where an explicit expression for each of the factors on the right appears in (5.4) above.

In the statement of the above theorem, we have followed various conventions from earlier sections. In particular,

$$\beta_{j,i} \geq \beta_{j,i+1}.$$

This theorem is a natural extension of a result in Lyness and Sørevik (1989) to the effect that the number of distinct lattice rules of order N is given by

$$\nu_s(N) = \prod_{j=1}^{q} \nu_s(p_j^{\beta_j}).$$

7. Concluding Remarks

The general thrust of this article is to provide a straightforward and concrete approach to some of the basic structure of lattice rules. This approach has led through several areas which are new only in a marginal sense.

For example, spelling out the group theory and applying it as in Section 2 is new. Something like it was submitted in an earlier version of Sloan and Lyness (1989) but was excised by the referee. Again, the simple procedure in Section 3 for the reduction of a prime power rule to canonical form has not appeared before. What will soon be available is a more general process in which the Smith Normal Form of a generator

matrix is used to obtain a general canonical form; see Lyness and Keast (1991) and Langtry (1991). However, in that process the simple underlying geometry is obscured.

The results of Sections 4 to 6 about the number of lattice rules with given invariants were available to the author in 1989 and promised in 1991. These were subsequently derived independently by Joe and Hunt (1992). In broad outline, their derivation parallels the one given here. However, in their work, $\bar{\bar{\mu}}_s$ appears as the result of a nontrivial argument based on group theory, whereas here it is derived in a direct way as a straightforward redundancy factor in a matrix representation.

This author hopes that this somewhat pedestrian exposition of these ideas will help enlighten an elegant branch of numerical quadrature.

Acknowledgment

This work was supported in part by the Applied Mathematical Sciences subprogram of the Office of Energy Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

References

Joe S. and Hunt D. C. (1992), "The Number of Lattice Rules Having Given Invariants," Bull. Australian Math. Soc. 46, pp. 479–495. See also Applied Mathematics Preprint AM91/44, UNSW.

Korobov N. M. (1959), "The Approximate Computation of Multiple Integrals" (Russian), Dokl. Akad. Nauk. SSSR 124, pp. 1207–1210.

Lyness J. N. and Keast P. (1991), "Application of the Smith Normal Form to the Structure of Lattice Rules," Preprint MCS-P269-0891, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, Ill.

Lyness J. N. and Sørevik T. (1989), "The Number of Lattice Rules," BIT 29, pp. 527–534.

Langtry T. N. (1991), "The Determination of Canonical Forms for Lattice Quadrature Rules," private communication.

Niederreiter H. (1992), "Random Number Generation and Quasi-Monte Carlo Methods ,"CBMS-NSF 63, SIAM, Philadelphia.

Sloan I. H. (1992), "Numerical Integration in High Dimensions—The Lattice Rule Approach," in Numerical Integration, T. O. Espelid and A. Genz (eds.), 55–69, Kluwer Academic Publishers, The Netherlands.

Sloan I. H. and Lyness J. N. (1989), "The Representation of Lattice Quadrature Rules as Multiple Sums," Math. Comput. 52, pp. 81–94.

Dr. J. N. Lyness
Mathematics and Computer Science Division
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439
lyness@mcs.anl.gov