Bull. Austral. Math. Soc. 65D30, 65D32, 20K05
Vol. 46 (1992) [479–495]

THE NUMBER OF LATTICE RULES HAVING GIVEN INVARIANTS

Stephen Joe and David C. Hunt

A lattice rule is a quadrature rule used for the approximation of integrals over the s-dimensional unit cube. Every lattice rule may be characterised by an integer r called the rank of the rule and a set of r positive integers called the invariants. By exploiting the group-theoretic structure of lattice rules we determine the number of distinct lattice rules having given invariants. Some numerical results supporting the theoretical results are included. These numerical results are obtained by calculating the Smith normal form of certain integer matrices.

1. Introduction

Lattice rules are used to approximate the s-dimensional integral

$$If = \int_{U^s} f(\mathbf{x})\,d\mathbf{x},$$

where $U^s = [0,1)^s$ is the half-open cube in s dimensions, and f is assumed to be 1-periodic in each of its s variables. They are quadrature rules of the form

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

in which the quadrature points $\mathbf{x}_0, \ldots, \mathbf{x}_{N-1}$ consist of all the points in U^s that also belong to some 'integration lattice'. A lattice is a discrete set of points in $\mathbb{R}^s$ such that the sum and difference of every point in the set also belongs to the set; it is an integration lattice if it contains $\mathbb{Z}^s$ as a subset. A lattice rule with N distinct quadrature points is said to be of order N.

Simple examples of lattice rules are given by the number-theoretic rules which were developed by Korobov [5] and Hlawka [3]. Number-theoretic rules of order N may be expressed in the form

$$Qf = \frac{1}{N}\sum_{j=0}^{N-1} f\left(\left\{j\frac{\mathbf{z}}{N}\right\}\right), \tag{1.2}$$

Received 2nd December 1991

The authors would like to thank T.N. Langtry for comments on an earlier version of the paper, as well as Professor I.H. Sloan for some useful suggestions. The continuing financial support of the Australian Research Council is gratefully acknowledged.

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

where $\mathbf{z}$ is an integer vector having no nontrivial factor in common with N, that is, $j\mathbf{z}/N \notin \mathbb{Z}^s$, $1 \leqslant j \leqslant N-1$. Here the braces around a vector indicate that we take the fractional part of each component, that is, $\{(x_1, \dots, x_s)\} = (x_1 \bmod 1, \dots, x_s \bmod 1)$.

The work of Sloan and Lyness [11] shows that every lattice rule may be written in canonical form as the expression

$$Qf = \frac{1}{N} \sum_{j_r=0}^{n_r-1} \cdots \sum_{j_1=0}^{n_1-1} f\left(\left\{j_1 \frac{\mathbf{z}_1}{n_1} + \cdots + j_r \frac{\mathbf{z}_r}{n_r}\right\}\right), \tag{1.3}$$

where N, the order of the rule, is given by

$$N = n_1 n_2 \cdots n_r, \tag{1.4}$$

$\mathbf{z}_1, \dots, \mathbf{z}_r$ are linearly independent integer vectors,

$$n_r > 1, \text{ and } n_{k+1} \text{ divides } n_k \text{ for } 1 \leqslant k \leqslant r-1. \tag{1.5}$$

The number r, which satisfies $1 \leqslant r \leqslant s$, is the rank of the rule and $n_1, \dots, n_r$ are the invariants. Both the rank and invariants are uniquely determined for a given lattice rule. It is clear that the number-theoretic rule given in (1.2) is a rank-1 rule with single invariant $n_1 = N$. We see in (1.3) that for $1 \leqslant k \leqslant r$ we may replace $\mathbf{z}_k$ by $\mathbf{z}_k + n_k \mathbf{h}_k$, where $\mathbf{h}_k \in \mathbb{Z}^s$, without changing Qf. Thus without loss of generality, we shall always assume that the vectors $\mathbf{z}_k$ have components z_{ki} satisfying

$$0 \leqslant z_{ki} \leqslant n_k - 1, \quad 1 \leqslant i \leqslant s, \quad 1 \leqslant k \leqslant r. \tag{1.6}$$

One problem of interest is the total number of distinct lattice rules having order N. Here we say that two lattice rules (having the same order) are distinct when the sets of quadrature points for the two rules are different. If we denote this quantity by $T_s(N)$, then the following result of Lyness and Sørevik [9] allows $T_s(N)$ to be calculated for any N.

Theorem 1.

(a) *If M and N are relatively prime numbers, then*

$$T_s(MN) = T_s(M)T_s(N),$$

that is, $T_s(N)$ is a multiplicative function.

(b) *For p prime and $\gamma > 0$, we have*

$$T_s(p^\gamma) = \prod_{i=1}^{s-1} \left[\frac{p^{\gamma+i}-1}{p^i-1}\right] \tag{1.7}$$

$$= \prod_{i=1}^{\gamma} \left[\frac{p^{s+i-1}-1}{p^i-1}\right]. \tag{1.8}$$

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

The expression given in (1.8) is actually not found in [9]. However it is easily obtained by expanding out the product in (1.7) and then cancelling common terms in the numerator and denominator.

In general for given N, one can obtain different sets of invariants $n_1, \dots, n_r$ that satisfy (1.4) and (1.5). For example with $s \geqslant 2$ and $N = 36 = 2^2 3^2$, one can obtain rank-1 rules with $n_1 = 36$ or rank-2 rules with invariants $n_1 = 18$, $n_2 = 2$ or $n_1 = 12$, $n_2 = 3$ or $n_1 = n_2 = 6$. So though Theorem 1 gives the total number of distinct lattice rules of order N, it does not give the number of distinct lattice rules having a given set of invariants $n_1, \dots, n_r$. This is the problem addressed in this paper. We shall denote this quantity by $\nu_s(n_1, \dots, n_r)$. For later use we shall also need the quantity $\widetilde{\nu}_s(n_1, \dots, n_r)$, the total number of possible collections of vectors $\mathbf{z}_1, \dots, \mathbf{z}_r$ (having components satisfying (1.6)) which give rise to a lattice rule having invariants $n_1, \dots, n_r$. We shall refer to $\widetilde{\nu}_s(n_1, \dots, n_r)$ as the total number of lattice rules having invariants $n_1, \dots, n_r$. Not all these lattice rules will be distinct and it turns out that $\nu_s(n_1, \dots, n_r)$ is a divisor of $\widetilde{\nu}_s(n_1, \dots, n_r)$.

The next section gives some relevant background material as well as the statement (in Theorem 5) of the main result of this paper. The proof of Theorem 5, given in Section 3, is obtained by exploiting the group-theoretic structure of lattice rules.

In Section 5 we provide some numerical results which support the theoretical results found in Section 2. These numerical results are obtained by calculating the Smith normal form of certain integer matrices. Background material on the Smith normal form and its relevance to the general theory of lattice rules as well as to the work here may be found in Section 4.

2. Background material and results

Firstly, it is useful to find the number of possible sets of invariants obtainable from a given N. Suppose N has the prime factorisation $p_1^{\beta_1} p_2^{\beta_2} \cdots p_q^{\beta_q}$. For convenience let us assume that $\beta_1 = \max\limits_{1 \leqslant i \leqslant q} \beta_i$. Then one can always obtain a set of r invariants that satisfy (1.4) and (1.5), where $1 \leqslant r \leqslant \min(s, \beta_1)$, by setting $n_1 = p_1^{\beta_1 - r + 1} p_2^{\beta_2} \cdots p_q^{\beta_q}$, $n_2 = \cdots = n_r = p_1$. In general, any set of invariants $n_1, \dots, n_r$ that satisfy (1.4) and (1.5) must be of the form

$$n_k = p_1^{\beta_{1k}} p_2^{\beta_{2k}} \cdots p_q^{\beta_{qk}}, \quad 1 \leqslant k \leqslant r, \tag{2.1}$$

where

$$0 \leqslant \beta_{ir} \leqslant \beta_{i,r-1} \leqslant \cdots \leqslant \beta_{i1} \text{ and } \sum_{k=1}^{r} \beta_{ik} = \beta_i, \ 1 \leqslant i \leqslant q. \tag{2.2}$$

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

Then it is not hard to see that the number of ways of forming the invariants is given by

$$\prod_{i=1}^{q} \chi(\beta_i), \tag{2.3}$$

where $\chi(\beta_i)$ is the number of partitions of β_i into positive summands. We remark that the number given in (2.3) is well-known as the number of different (pairwise non-isomorphic) abelian groups having order $N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_q^{\beta_q}$.

We now give a result from [**11**] concerning the group-theoretic structure of lattice rules. The proof is trivial and so not given here.

Theorem 2. *Let $\mathcal{A}(Q)$ denote the set of N quadrature points for the lattice rule* (1.1).

(a) *$\mathcal{A}(Q)$, together with the group operation*

$$\mathbf{x}_i \circ \mathbf{x}_j = \{\mathbf{x}_i + \mathbf{x}_j\}, \tag{2.4}$$

forms an abelian group of order N with the identity element being $\mathbf{0}$.

(b) *If the lattice rule in* (1.1) *is a rank-*1 *rule of order N* (*as given by* (1.2)), *then $\mathcal{A}(Q)$, together with the group operation given by* (2.4), *forms a cyclic group of order N.*

This theorem will be used throughout the rest of this paper without further comment. The canonical form for lattice rules that was obtained by Sloan and Lyness [**11**] (and given in equations (1.3) to (1.5)) is then a consequence of a well-known structure theorem for abelian groups. Theorem 2 shows that $\mathcal{A}(Q)$ is an abelian group under addition modulo $\mathbb{Z}^s$ so that it is natural to make the assumption given in (1.6). In the rest of the paper we shall not distinguish between the set $\mathcal{A}(Q)$ and the group $\mathcal{A}(Q)$.

We now show that $\nu_s(n_1, \ldots, n_r)$ is in a certain sense a multiplicative function in each of its arguments.

Theorem 3. *Suppose $n_1, \ldots, n_r$ are given invariants expressed in the form given in* (2.1) *and* (2.2) *so that $n_1 n_2 \cdots n_r = p_1^{\beta_1} p_2^{\beta_2} \cdots p_q^{\beta_q}$. Then*

$$\nu_s(n_1, \ldots, n_r) = \prod_{i=1}^{q} \nu_s\left(p_i^{\beta_{i1}}, \ldots, p_i^{\beta_{it_i}}\right),$$

where for $1 \leqslant i \leqslant q$, t_i is the largest integer t^* for which $\beta_{it^*} > 0$ with $1 \leqslant t_i \leqslant r$.

Proof: Let $\mathcal{A}(Q)$ be the set of quadrature points for any lattice rule Q having invariants $n_1, \ldots, n_r$. It follows from [7, p.154] that $\mathcal{A}(Q)$ may be expressed as the direct sum of q subgroups,

$$\mathcal{A}(Q) = \mathcal{S}_1(Q) \oplus \cdots \oplus \mathcal{S}_q(Q),$$

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

where $\mathcal{S}_i(Q)$ is of order $p_i^{\beta_i}$, $1 \leqslant i \leqslant q$. The group $\mathcal{S}_i(Q)$, $1 \leqslant i \leqslant q$, is the Sylow p_i-subgroup of $\mathcal{A}(Q)$.

We want the number of distinct lattice rules having invariants $n_1, \ldots, n_r$ where the n_k, $1 \leqslant k \leqslant r$, satisfy (2.1) and (2.2). Clearly the $p_i^{\beta_i}$ elements of $\mathcal{S}_i(Q)$ are the points of a lattice rule having invariants $p_i^{\beta_{i1}}, \ldots, p_i^{\beta_{it_i}}$. Hence for $1 \leqslant i \leqslant q$, there are $\nu_s\left(p_i^{\beta_{i1}}, \ldots, p_i^{\beta_{it_i}}\right)$ distinct Sylow p_i-subgroups possible. Since the elements of $\mathcal{S}_i(Q)$ consists of those elements of $\mathcal{A}(Q)$ which have order a power of p_i, it follows that the q Sylow p_i-subgroups for a given lattice rule having invariants $n_1, \ldots, n_r$ must be unique. Hence we conclude that the number of distinct lattice rules having invariants $n_1, \ldots, n_r$ is

$$\nu_s(n_1, \ldots, n_r) = \prod_{i=1}^{q} \nu_s\left(p_i^{\beta_{i1}}, \ldots, p_i^{\beta_{it_i}}\right),$$

as claimed. □

Theorem 3 shows that we need consider only $\nu_s(p^{\alpha_1}, \ldots, p^{\alpha_r})$, where p is prime, and $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_r > 0$. The first and simplest such case to look at is the number of rank-1 lattice rules having order p^{α_1}.

Theorem 4.

(a) $\tilde{\nu}_s(p^{\alpha_1}) = p^{\alpha_1 s} - p^{\alpha_1 s - s}$.

(b) $\nu_s(p^{\alpha_1}) = \dfrac{p^{\alpha_1 s} - p^{\alpha_1 s - s}}{p^{\alpha_1} - p^{\alpha_1 - 1}}$.

Proof: We see from either (1.2) or (1.3) that a rank-1 lattice rule of order p^{α_1} in canonical form may be written as

$$Qf = \frac{1}{p^{\alpha_1}} \sum_{j=0}^{p^{\alpha_1}-1} f\left(\left\{j \frac{\mathbf{z}}{p^{\alpha_1}}\right\}\right).$$

The cyclic group formed by the set of p^{α_1} points for this lattice rule is generated by the element $\mathbf{c} = \mathbf{z}/p^{\alpha_1}$. Since this generator must have order p^{α_1}, that is, p^{α_1} is the least positive integer u for which $\{u\mathbf{c}\} = \mathbf{0}$ (recall that the group operation is given by (2.4)), it follows that at least one of the components of $\mathbf{z}$ is not divisible by p. (Otherwise, if $\mathbf{z} = p\mathbf{z}'$, then $\mathbf{c} = \mathbf{z}/p^{\alpha_1} = \mathbf{z}'/p^{\alpha_1 - 1}$ has order at most $p^{\alpha_1 - 1}$.)

For any positive integer M, let $\phi(M)$ be Euler's totient function. We recall that $\tilde{\nu}_s(p^{\alpha_1})$ is the number of $\mathbf{z}$ with components satisfying $0 \leqslant z_i \leqslant p^{\alpha_1} - 1$, $1 \leqslant i \leqslant s$, that produce a rank-1 rule of order p^{α_1}. Because $p^{\alpha_1} - \phi(p^{\alpha_1}) = p^{\alpha_1 - 1}$ [7, p.17], we see that though there are $p^{\alpha_1 s}$ possible choices of $\mathbf{z}$, $\left(p^{\alpha_1 - 1}\right)^s$ of them do not produce a rank-1 rule of order p^{α_1} since all their components are divisible by p. Thus $\tilde{\nu}_s(p^{\alpha_1})$ is given by

$$\tilde{\nu}_s(p^{\alpha_1}) = p^{\alpha_1 s} - p^{\alpha_1 s - s}.$$

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

However different $\mathbf{z}$ may produce the same rank-1 lattice rule of order p^{α_1}. The theory of cyclic groups (for example, see [7, p.159]) shows that the generating element may be chosen in $\phi(p^{\alpha_1})$ ways. Thus we obtain

$$\nu_s(p^{\alpha_1}) = \frac{\widetilde{\nu}_s(p^{\alpha_1})}{\phi(p^{\alpha_1})} = \frac{p^{\alpha_1 s} - p^{\alpha_1 s - s}}{p^{\alpha_1} - p^{\alpha_1 - 1}},$$

which completes the proof. □

We now give expressions for $\widetilde{\nu}_s(p^{\alpha_1}, \dots, p^{\alpha_r})$ and $\nu_s(p^{\alpha_1}, \dots, p^{\alpha_r})$.

Theorem 5. *Suppose $p^{\alpha_1}, \dots, p^{\alpha_r}$ are given invariants.*

(a) *The total number of s-dimensional lattice rules having the given invariants is*

$$\widetilde{\nu}_s(p^{\alpha_1}, \dots, p^{\alpha_r}) = \prod_{k=1}^{r} \left(p^{\alpha_k s} - p^{\alpha_k s - s + k - 1}\right). \tag{2.5}$$

(b) *Suppose d of the given invariants are distinct. Let $p^{\alpha_1^*}, \dots, p^{\alpha_d^*}$ be these distinct invariants with $\alpha_1^* > \cdots > \alpha_d^* > 0$, and let ω_k be the number of invariants equal to $p^{\alpha_k^*}$, $1 \leqslant k \leqslant d$. If*

$$\delta_k = \alpha_k^* \sum_{j=1}^{k} \omega_j + \sum_{j=k+1}^{d} \omega_j \alpha_j^*, \quad 1 \leqslant k \leqslant d,$$

then the number of distinct s-dimensional lattice rules having the given invariants is

$$\nu_s(p^{\alpha_1}, \dots, p^{\alpha_r}) = \frac{\prod_{k=1}^{r} \left(p^{\alpha_k s} - p^{\alpha_k s - s + k - 1}\right)}{\prod_{k=1}^{d} \left[\prod_{j=1}^{\omega_k} \left(p^{\delta_k} - p^{\delta_k - \omega_k + j - 1}\right)\right]}. \tag{2.6}$$

Note. In early November 1991, it was learnt that Dr. J.N. Lyness of Argonne National Laboratory had independently obtained a result equivalent to Theorem 5(b). However, his approach to the problem was different from the group-theoretic approach that is used here.

As the proof of Theorem 5 is quite lengthy, we shall defer it until the next section. We remark that (2.6) yields $\nu_s(p^{\alpha_1}, \dots, p^{\alpha_r}) = 0$ when $r > s$ which is a sensible conclusion since we already know that the rank of a lattice rule cannot exceed s.

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

As a simple example, consider the case when all the α_k, $1 \leqslant k \leqslant r$, are equal to 1 so that $d = 1$, $\omega_1 = r$, and $\delta_1 = r$. Then by using (2.6) and a few lines of algebra, it is easy to show that

$$\nu_s[p;r] = \prod_{k=1}^{r} \frac{p^{s-r+k} - 1}{p^k - 1}, \tag{2.7}$$

where, for simplicity, we have used $\nu_s[p;r]$ to denote $\nu_s\Bigl(\underbrace{p,\dots,p}_{r \text{ times}}\Bigr)$. Using (2.7), it is easily verified that we have the relationship

$$\nu_s[p;r] = \nu_{s-1}[p;r] + p^{s-r}\nu_{s-1}[p;r-1], \quad 2 \leqslant r \leqslant s-1. \tag{2.8}$$

A derivation of (2.8) using the Smith normal form for integer matrices may be found in Section 4.

From Theorems 1(b) and 4(b) we see that algebraically $T_s(p)$ and $\nu_s(p)$ are the same, while these same theorems along with (2.7) can be used to verify that the identity $T_s(p^2) = \nu_s(p^2) + \nu_s(p,p)$ holds algebraically too. By using (2.6) to obtain

$$\nu_s(p^2,p) = \frac{(p^{2s-2} - p^{s-2})(p^{s-1} - 1)}{(p-1)^2},$$

one can verify (after some tedious algebra) that algebraically we also have $T_s(p^3) = \nu_s(p^3) + \nu_s(p^2,p) + \nu_s(p,p,p)$.

For the more general case, suppose $N = p^\alpha$, $\alpha > 0$, is given. Then (2.3) shows that there are $\chi(\alpha)$ ways of forming invariants $p^{\alpha_1},\dots,p^{\alpha_r}$ such that $\alpha = \alpha_1 + \dots + \alpha_r$, and $\alpha_1 \geqslant \dots \geqslant \alpha_r > 0$. For given s, we must then have the (formal) identity

$$T_s(p^\alpha) = \sum_{\substack{\alpha_1+\dots+\alpha_r=\alpha \\ \alpha_1\geqslant\dots\geqslant\alpha_r>0}} \nu_s(p^{\alpha_1},\dots,p^{\alpha_r}),$$

where we assume that $\nu_s(p^{\alpha_1},\dots,p^{\alpha_r}) = 0$ in the cases when $r > s$. Clearly this identity must not only hold formally but algebraically as well.

3. Proof of Theorem 5

The proof of Theorem 5 depends on the following three lemmas. We shall say that a lattice rule Q' is 'embedded' in the lattice rule Q if the quadrature points of Q' are also quadrature points of Q.

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

Lemma 1. *Suppose Q_{r-1} is a lattice rule which has rank $r-1$ and invariants $p^{\alpha_1}, \dots, p^{\alpha_{r-1}}$.*

(a) *Let $\mathcal{A}(Q_{r-1})$ be the set of quadrature points for Q_{r-1}, and let $\mathcal{C}_r$ be the set of points for a rank-1 lattice rule of order p^{α_r}. Also let*

$$\mathcal{A}(Q_{r-1}) \circ \mathcal{C}_r = \{\mathbf{a} \circ \mathbf{c} \mid \mathbf{a} \in \mathcal{A}(Q_{r-1}) \text{ and } \mathbf{c} \in \mathcal{C}_r\},$$

where $\circ$ is the group operation given by (2.4). Then a necessary and sufficient condition for the elements of $\mathcal{A}(Q_{r-1}) \circ \mathcal{C}_r$ to be the quadrature points of a lattice rule having rank r and invariants $p^{\alpha_1}, \dots, p^{\alpha_r}$ is that $\mathcal{A}(Q_{r-1})$ and $\mathcal{C}_r$ do not have a subgroup of order p in common.

(b) *There are $(p^{r-1}-1)/(p-1)$ distinct rank-1 lattice rules of order p embedded in Q_{r-1}.*

Proof: In [11] we see that $\mathcal{A}(Q_{r-1})$ may be written as

$$\mathcal{A}(Q_{r-1}) = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1},$$

where $\mathcal{C}_k$ is a cyclic group of order p^{α_k}, $1 \leqslant k \leqslant r-1$. In the terminology of the theory of abelian groups of prime-power order, $\mathcal{A}(Q_{r-1})$ is said to be of 'type' $(\alpha_1, \dots, \alpha_{r-1})$. Thus we see that the elements of $\mathcal{A}(Q_{r-1}) \circ \mathcal{C}_r$ are the points of a rank-r lattice rule having invariants $p^{\alpha_1}, \dots, p^{\alpha_{r-1}}, p^{\alpha_r}$ if $\mathcal{A}(Q_{r-1}) \circ \mathcal{C}_r$ is of type $(\alpha_1, \dots, \alpha_r)$. Hence we require $\mathcal{A}(Q_{r-1}) \circ \mathcal{C}_r = \mathcal{A}(Q_{r-1}) \oplus \mathcal{C}_r$. It follows from the discussion in [7, pp.139–140] that this is the case if and only if $\mathcal{A}(Q_{r-1})$ and $\mathcal{C}_r$ do not have an element (except the identity $\mathbf{0}$) in common.

Clearly if they do not have a nontrivial common element, then they cannot have a common subgroup of order p. Also if $\mathcal{A}(Q_{r-1})$ and $\mathcal{C}_r$ do not have a subgroup of order p in common, then they cannot have any nontrivial element in common. (Otherwise, if $\mathbf{c}$ was such a common element, then there would exist a γ satisfying $0 \leqslant \gamma \leqslant \alpha_r - 1$ for which $\{p^\gamma \mathbf{c}\}$ would be an element of order p, and hence be a generator for a common subgroup of order p.) Hence part (a) is proved.

To prove part (b), we firstly note that $\mathcal{A}(Q_{r-1})$ has exactly $p^{r-1}-1$ elements of order p [7, p.159]. Given any such element $\mathbf{a}$, it follows that the elements $\mathbf{a}, \{2\mathbf{a}\}, \dots, \{(p-1)\mathbf{a}\}$ must each be of order p and in $\mathcal{A}(Q_{r-1})$. Thus these $p-1$ elements together with the identity element form a subgroup of order p. It then follows that the $p^{r-1}-1$ elements of order p in $\mathcal{A}(Q_{r-1})$ must form $(p^{r-1}-1)/(p-1)$ subgroups of order p. Since p is prime, these subgroups must be cyclic. Hence they are distinct rank-1 lattice rules of order p which are embedded in Q_{r-1}. $\square$

Lemma 2. *Each one of the $\nu_s(p)$ distinct rank-1 lattice rules of order p is embedded in exactly $(p-1)p^{\gamma s - s}$ of the $\widetilde{\nu}_s(p^\gamma)$ rank-1 rules of order p^γ, $\gamma > 0$.*

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

PROOF: Let

$$\frac{1}{p}\sum_{j=0}^{p-1} f\left(\left\{j\frac{\mathbf{z}'}{p}\right\}\right)$$

be any one of the $\nu_s(p)$ distinct rank-1 rules of order p. Also let

$$\mathbf{z} = \mathbf{z}' + p\mathbf{h},$$

where $\mathbf{h}$ is an integer vector whose components satisfy

$$(3.1) \qquad 0 \leqslant h_i \leqslant p^{\gamma-1} - 1, \quad 1 \leqslant i \leqslant s.$$

Since at least one of the components of $\mathbf{z}'$ is not 0, it means that at least one of the components of $\mathbf{z}$ is not divisible by p. Hence

$$\frac{1}{p^\gamma}\sum_{j=0}^{p^\gamma-1} f\left(\left\{j\frac{\mathbf{z}}{p^\gamma}\right\}\right)$$

is a rank-1 rule of order p^γ. By letting j take on the values $j = kp^{\gamma-1}$ for $0 \leqslant k \leqslant p-1$, it is not hard to see that the original rank-1 rule of order p is embedded in this rank-1 rule of order p^γ. Note also that it follows from (3.1) that the components of $\mathbf{z}$ satisfy $0 \leqslant z_i \leqslant p^\gamma - 1$, since the components of $\mathbf{z}'$ satisfy $0 \leqslant z_i' \leqslant p-1$, $1 \leqslant i \leqslant s$.

The vector $\mathbf{z}'$ for the chosen rank-1 rule of order p may be chosen in $\phi(p) = p-1$ ways. Also (3.1) shows that there are $p^{\gamma s - s}$ possibilities for $\mathbf{h}$. Thus the rank-1 rule of order p is embedded in *at least* $(p-1)p^{\gamma s - s}$ of the $\tilde{\nu}_s(p^\gamma)$ rank-1 rules of order p^γ.

To show that the number is exactly $(p-1)p^{\gamma s - s}$, we firstly note that one may deduce from Lemma 1(b) that any rank-1 rule of order p^γ has only one rank-1 rule of order p embedded in it. Also Theorem 4(b) yields

$$\nu_s(p) \times (p-1)p^{\gamma s - s} = (p^s - 1)p^{\gamma s - s} = p^{\gamma s} - p^{\gamma s - s}.$$

However this last quantity is just $\tilde{\nu}_s(p^\gamma)$. Hence we see that the exact number is as given. □

The last lemma we need concerns the number of ways in which an ordered basis for an abelian group may be chosen. The result given below is presumably well-known though a reference does not appear to be readily available.

LEMMA 3. *Let $\mathcal{G}$ be an abelian p-group of type $(\alpha_1, \dots, \alpha_r)$ with identity element 0. Suppose d of the $\alpha_1, \dots, \alpha_r$ are distinct so that we have the distinct values*

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

$\alpha_1^*, \dots, \alpha_d^*$, where $\alpha_1^* > \dots > \alpha_d^* > 0$. If ω_k is the number of the $\alpha_1, \dots, \alpha_r$ equal to α_k^*, $1 \leqslant k \leqslant d$, and

$$\delta_k = \alpha_k^* \sum_{j=1}^{k} \omega_j + \sum_{j=k+1}^{d} \omega_j \alpha_j^*, \quad 1 \leqslant k \leqslant d,$$

then an ordered basis for $\mathcal{G}$ may be chosen in $\kappa(\alpha_1, \dots, \alpha_r)$ ways, where

$$\kappa(\alpha_1, \dots, \alpha_r) = \prod_{k=1}^{d} \left[\prod_{j=1}^{\omega_k} \left(p^{\delta_k} - p^{\delta_k - \omega_k + j - 1} \right) \right]. \tag{3.2}$$

Proof: In this proof we shall adopt the standard additive notation for abelian groups. For any positive integer m, let $\mathcal{G}_m$ be the subgroup of $\mathcal{G}$ given by

$$\mathcal{G}_m = \{ w \in \mathcal{G} : p^m w = 0 \}. \tag{3.3}$$

Also, for $1 \leqslant k \leqslant d$, let τ_k and ε_k be the unique integers satisfying

$$\alpha_{\tau_k} \geqslant \alpha_k^* > \alpha_{\tau_k+1} \text{ and } \alpha_{\varepsilon_k} \geqslant \alpha_k^* - 1 > \alpha_{\varepsilon_k+1}$$

(with the convention that $\alpha_{r+1} = 0$). Then it is known (see [1, p.320] or [2, p.104]) that the orders of $\mathcal{G}_{\alpha_k^*}$ and $\mathcal{G}_{\alpha_k^*-1}$ are given by p^{u_k} and p^{v_k} respectively, where

$$u_k = \alpha_k^* \tau_k + \alpha_{\tau_k+1} + \dots + \alpha_r + \alpha_{r+1}, \text{ and } v_k = (\alpha_k^* - 1)\varepsilon_k + \alpha_{\varepsilon_k+1} + \dots + \alpha_r + \alpha_{r+1}.$$

Now any element of order $p^{\alpha_k^*}$ in $\mathcal{G}$ belongs to $\mathcal{G}_{\alpha_k^*}$, but not to $\mathcal{G}_{\alpha_k^*-1}$. Hence the number of elements of order $p^{\alpha_k^*}$ in $\mathcal{G}$ is given by $p^{u_k} - p^{v_k}$. We remark that because any group has only one element of order 1 (namely, the identity) and $\alpha_r \geqslant 1 > \alpha_{r+1}$, then it is not hard to deduce from above that an abelian group of type $(\alpha_1, \dots, \alpha_r)$ has $p^r - 1$ elements of order p.

Let $\sigma(k) = \sum_{m=1}^{k} \omega_m$ so that $\sigma(d) = r$. It is easily seen that $\tau_k = \sigma(k)$. Some simple algebra then yields $u_k = \delta_k$. Also when $\alpha_{k+1}^* = \alpha_k^* - 1$ we obtain $\varepsilon_k = \sigma(k+1)$, while in the case $\alpha_{k+1}^* < \alpha_k^* - 1$ we obtain $\varepsilon_k = \sigma(k)$. Then it turns out in both cases that $v_k = \delta_k - \sigma(k)$. Thus the number of elements of order $p^{\alpha_k^*}$ in $\mathcal{G}$ is given by $p^{\delta_k} - p^{\delta_k - \sigma(k)}$.

The r generators required for the basis set may be chosen in d major stages. At the kth major stage, $1 \leqslant k \leqslant d$, we need to choose ω_k elements of order $p^{\alpha_k^*}$. Thus each kth major stage may be split up into ω_k minor stages in which we choose one element of order $p^{\alpha_k^*}$ for the basis set. Suppose for some j satisfying $1 \leqslant j \leqslant \omega_k$ we

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

are currently at the start of the jth minor stage in the kth major stage. Hence we have chosen all the generators of order $p^{\alpha_1^*},\dots,p^{\alpha_{k-1}^*}$ as well as $j-1$ generators of order $p^{\alpha_k^*}$.

We now have to choose a generator of order $p^{\alpha_k^*}$ which we shall denote by g_{kj}. The cyclic group of order $p^{\alpha_k^*}$ generated by such an g_{kj} contains one subgroup of order p. Since g_{kj} is of order $p^{\alpha_k^*}$, then clearly the element $p^{\alpha_k^*-1}g_{kj}$ (of order p) will be a generator for this subgroup. Arguments analogous to those used in the proof of Lemma 1(a) show that this subgroup of order p must not be in $\mathcal{B}_{k,j-1}$, where $\mathcal{B}_{k,j-1}$ is the group generated by $g_{\ell m}$, $1 \leqslant m \leqslant \omega_\ell$, $1 \leqslant \ell \leqslant k-1$, and $g_{k1},\dots,g_{k,j-1}$, the $\sigma(k-1)+j-1$ generators already chosen. Hence g_{kj} has to satisfy the requirement that $p^{\alpha_k^*-1}g_{kj} \notin \mathcal{B}_{k,j-1}$.

Let b be any element of order p belonging to $\mathcal{B}_{k,j-1}$. Because b is of order p and the generators $g_{\ell m}$, $1 \leqslant \ell \leqslant k$, are of order $p^{\alpha_\ell^*}$, it follows that there exist integers $\xi_{\ell m}$ such that

$$b = \sum_{\ell=1}^{k-1}\sum_{m=1}^{\omega_\ell} p^{\alpha_\ell^*-1}\xi_{\ell m}g_{\ell m} + \sum_{m=1}^{j-1} p^{\alpha_k^*-1}\xi_{km}g_{km}.$$

Then the element

$$c = \sum_{\ell=1}^{k-1}\sum_{m=1}^{\omega_\ell} p^{\alpha_\ell^*-\alpha_k^*}\xi_{\ell m}g_{\ell m} + \sum_{m=1}^{j-1} \xi_{km}g_{km} \in \mathcal{B}_{k,j-1}$$

is of order $p^{\alpha_k^*}$ and satisfies $p^{\alpha_k^*-1}c = b$. Suppose w is any element of $\mathcal{G}_{\alpha_k^*-1}$, where $\mathcal{G}_{\alpha_k^*-1}$ is the subgroup of $\mathcal{G}$ given by (3.3) (with $m = \alpha_k^*-1$). Then it is clear that $p^{\alpha_k^*-1}(c+w) = p^{\alpha_k^*-1}c = b$. Also $c' = c+w$ is an element of order $p^{\alpha_k^*}$ and the order of $\mathcal{G}_{\alpha_k^*-1}$ is $p^{\delta_k-\sigma(k)}$. Hence for any element b of order p belonging to $\mathcal{B}_{k,j-1}$, it follows that there are exactly $p^{\delta_k-\sigma(k)}$ elements c' of order $p^{\alpha_k^*}$ in $\mathcal{G}$ such that $b = p^{\alpha_k^*-1}c'$,

Since $\mathcal{B}_{k,j-1}$ is of type $(\alpha_1,\dots,\alpha_{\sigma(k-1)+j-1})$, then it has $p^{\sigma(k-1)+j-1}-1$ elements of order p. Hence there are $p^{\delta_k-\sigma(k)}\left(p^{\sigma(k-1)+j-1}-1\right)$ elements in $\mathcal{G}$ of order $p^{\alpha_k^*}$ which may *not* be used as the generating element g_{kj}. As a consequence, g_{kj} may then be chosen in

$$\left(p^{\delta_k} - p^{\delta_k-\sigma(k)}\right) - p^{\delta_k-\sigma(k)}\left(p^{\sigma(k-1)+j-1} - 1\right) = p^{\delta_k} - p^{\delta_k-\omega_k+j-1}$$

ways, where we have used the fact that $\sigma(k)-\sigma(k-1) = \omega_k$. Hence we conclude that

$$\kappa(\alpha_1,\dots,\alpha_r) = \prod_{k=1}^{d}\left[\prod_{j=1}^{\omega_k}\left(p^{\delta_k} - p^{\delta_k-\omega_k+j-1}\right)\right],$$

as required. $\square$

We see that (3.2) gives $\kappa(\alpha_1) = p^{\alpha_1} - p^{\alpha_1 - 1}$ as expected. If all the α_k, $1 \leqslant k \leqslant r$, are equal to 1 so that $d = 1$ and $\omega_1 = r$, then this same equation yields

$$\kappa\Bigl(\underbrace{1,\ldots,1}_{r \text{ times}}\Bigr) = \prod_{k=1}^{r} \left(p^r - p^{k-1}\right).$$

This result may be found in classical texts on group theory such as Burnside [**2**, p.110]. With $d = r$, $\omega_k = 1$, $\alpha_k^* = \alpha_k = r - k + 1$, $1 \leqslant k \leqslant r$, we can also obtain

$$\kappa(r, r-1, \ldots, 2, 1) = p^{r(r+1)(2r+1)/6 - r}(p-1)^r,$$

which agrees with the result found in [**2**, p.118].

We are now ready to give the proof of Theorem 5.

Proof of Theorem 5: We firstly prove part (a) by using induction. For $r = 1$ the right hand side of (2.5) yields $p^{\alpha_1 s} - p^{\alpha_1 s - s}$, which we know from Theorem 4(a) is $\widetilde{\nu}_s\left(p^{\alpha_1}\right)$. Thus (2.5) is true for $r = 1$.

Let us now assume that

$$\widetilde{\nu}_s\left(p^{\alpha_1}, \ldots, p^{\alpha_{r-1}}\right) = \prod_{k=1}^{r-1} \left(p^{\alpha_k s} - p^{\alpha_k s - s + k - 1}\right).$$

Suppose Q_{r-1} is any lattice rule having rank $r-1$ and invariants $p^{\alpha_1}, \ldots, p^{\alpha_{r-1}}$. We see from Lemma 1(a) that a rank-r rule having invariants $p^{\alpha_1}, \ldots, p^{\alpha_{r-1}}, p^{\alpha_r}$ is obtained from Q_{r-1} by 'adding in' a rank-1 lattice rule of order p^{α_r}. However Lemma 1 also shows that the rank-1 rule of order p embedded in such a rule must not be one of the $\left(p^{r-1} - 1\right)/(p-1)$ rank-1 lattice rules of order p that are embedded in Q_{r-1}.

We see from Lemma 2 that each one of these rank-1 rules of order p is embedded in $(p-1)p^{\alpha_r s - s}$ rank-1 lattice rules of order p^{α_r}. Thus of the $\widetilde{\nu}_s\left(p^{\alpha_r}\right) = p^{\alpha_r s} - p^{\alpha_r s - s}$ rank-1 rules of order p^{α_r}, there are

$$\left(\left(p^{r-1} - 1\right)/(p-1)\right) \times (p-1)p^{\alpha_r s - s} = \left(p^{r-1} - 1\right)p^{\alpha_r s - s}$$

which are *not* permissible. Hence we see that

$$\begin{aligned}\widetilde{\nu}_s\left(p^{\alpha_1}, \ldots, p^{\alpha_{r-1}}, p^{\alpha_r}\right) &= \widetilde{\nu}_s\left(p^{\alpha_1}, \ldots, p^{\alpha_{r-1}}\right) \times \left(p^{\alpha_r s} - p^{\alpha_r s - s} - \left(p^{r-1} - 1\right)p^{\alpha_r s - s}\right) \\ &= \prod_{k=1}^{r} \left(p^{\alpha_k s} - p^{\alpha_k s - s + k - 1}\right).\end{aligned}$$

Thus part (a) holds by induction.

We now have the total number of lattice rules having invariants $n_1, \dots, n_r$. However they cannot all be distinct (as Theorem 4 clearly shows for the case $r = 1$). To obtain $\nu_s(p^{\alpha_1}, \dots, p^{\alpha_r})$, we need to know the number of ways in which the generators for an abelian group of type $(\alpha_1, \dots, \alpha_r)$ may be chosen. This number will be dependent on the $\alpha_1, \dots, \alpha_r$ (and p), but independent of s. Lemma 3 shows that this number is just $\kappa(\alpha, \dots, \alpha_r)$, where $\kappa(\alpha, \dots, \alpha_r)$ is given by (3.2). Hence

$$\nu_s(p^{\alpha_1}, \dots, p^{\alpha_r}) = \frac{\widetilde{\nu}_s(p^{\alpha_1}, \dots, p^{\alpha_r})}{\kappa(\alpha, \dots, \alpha_r)} = \frac{\prod_{k=1}^{r} \left(p^{\alpha_k s} - p^{\alpha_k s - s + k - 1}\right)}{\prod_{k=1}^{d} \left[\prod_{j=1}^{\omega_k} \left(p^{\delta_k} - p^{\delta_k - \omega_k + j - 1}\right)\right]}.$$

This completes the proof of Theorem 5. □

4. The Smith Normal Form

In the next section we shall give some numerical results which support Theorem 5(b). These are obtained by calculating the Smith normal form of certain integer matrices. Thus it is useful to give some background material on the Smith normal form which in simple terms is a diagonalisation of an integer matrix using elementary row and column operations.

In more detail, let B be an $s \times s$ integer matrix. Then there exist $s \times s$ unimodular matrices X and Y such that $D = XBY$, where D, the Smith normal form, is an $s \times s$ diagonal matrix whose entries d_{ii} are such that d_{ii} divides $d_{i+1,i+1}$, $1 \leqslant i \leqslant s - 1$. An algorithm for computing the Smith normal form may be found in [4] (this paper also contains references to several other algorithms) while a clear description of the underlying basic procedure behind such an algorithm may be found in [**10**].

To see the relevance of the Smith normal form to the work here, we firstly need the definition of the dual lattice.

Definition 1. *Given an integration lattice L with lattice points $\mathbf{x}_0, \dots, \mathbf{x}_{N-1}$ in U^s, the dual lattice $L^\perp$ is defined by*

$$L^\perp := \{\mathbf{h} \in \mathbb{Z}^s : \mathbf{h} \cdot \mathbf{x}_j \in \mathbb{Z},\ 0 \leqslant j \leqslant N - 1\}.$$

For any dual lattice $L^\perp$, there exists an $s \times s$ integer matrix B with determinant N which is a generator matrix for $L^\perp$, that is, $L^\perp$ consists of all the integer linear combinations of the rows of B. We see from [9] that for every dual lattice (and hence every integration lattice) there exists a unique B which is upper triangular and has

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

entries b_{ij} that satisfy

$$(4.1)\qquad b_{jj} > 0 \text{ for } 1 \leqslant j \leqslant s, \ \prod_{j=1}^{s} b_{jj} = N, \text{ and } 0 \leqslant b_{ij} < b_{jj} \text{ for } 1 \leqslant i < j \leqslant s.$$

The result of Lyness and Sørevik [**9**] given in Theorem 1 was obtained by looking at the number of upper triangular integer matrices having entries that satisfy (4.1).

The relevance of the Smith normal form to lattice rules is the following result which may be found in [**6**] (as well as in [**8**]).

THEOREM 6. *Let Q be an N-point lattice rule whose corresponding dual lattice has generator matrix B. If the invariants of this lattice rule are $n_1, \dots, n_r$, then there exist unimodular matrices X and Y such that $XBY = D$, where the $s \times s$ diagonal matrix D has entries*

$$(4.2)\qquad d_{ii} = 1, \ 1 \leqslant i \leqslant s - r, \ \textit{and } d_{ii} = n_{s-i+1}, \ s - r + 1 \leqslant i \leqslant s.$$

The Smith normal form is used in group theory to determine the canonical representation of finite abelian groups so Theorem 6 should not be too unexpected in light of the abelian group structure of lattice rules. Then given $p^{\alpha_1}, \dots, p^{\alpha_r}$, Theorem 5(b) gives us the number of upper triangular integer matrices whose entries satisfy (4.1) and whose Smith normal form satisfies (4.2) (with $n_k = p^{\alpha_k}$, $1 \leqslant k \leqslant r$).

To end this section we show how the Smith normal form may be used to derive the relationship

$$(4.3)\qquad \nu_s[p;r] = \nu_{s-1}[p;r] + p^{s-r}\nu_{s-1}[p;r-1], \quad 2 \leqslant r \leqslant s-1,$$

that was given in (2.8). As was just indicated, $\nu_s[p;r]$ is the number of upper triangular integer matrices B satisfying (4.1) which have a Smith normal form in which

$$(4.4)\qquad d_{ii} = 1, \ 1 \leqslant i \leqslant s - r, \text{ and } d_{ii} = p, \ s - r + 1 \leqslant i \leqslant s.$$

It is known [**12**, p.25] that $\prod_{j=1}^{t} d_{jj}$ for $1 \leqslant t \leqslant s$ is the gcd of all the t-rowed minor determinants of B. Thus if the Smith normal form of B satisfies (4.4), then p must be the gcd of all $(s - r + 1)$-rowed minor determinants of B. Two simple consequences of this are given in the following theorem.

THEOREM 7. *Suppose B is an upper triangular integer matrix having entries satisfying* (4.1) *and a Smith normal form satisfying* (4.4).

(a) *B has exactly $s - r$ 1's on its diagonal* (*and hence the other r diagonal entries are p's*).

(b) *If $b_{mm} = p$ for some m, $1 \leqslant m < s$, then $b_{ms} = 0$.*

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

PROOF: To prove part (a), we note that if there were more than $s-r$ 1's on the diagonal, then one could form an $(s-r+1)$-rowed minor by taking $s-r+1$ rows and columns which had 1's in the corresponding diagonal position to obtain an $(s-r+1)\times(s-r+1)$ matrix which must be the identity matrix (since (4.1) shows that if $b_{jj}=1$, then $b_{ij}=0$ for $i\neq j$). Because this identity matrix has determinant 1, this results in a contradiction since then 1 is the gcd of all $s-r+1$-rowed minor determinants of B and not p as assumed.

To prove part (b), suppose $b_{mm}=p$ and $b_{ms}=u>0$. Part (a) shows that there are $s-r$ 1's on the diagonal of B. Thus we can form an $s-r+1$-rowed minor by taking the $s-r$ rows and columns with 1's in the corresponding diagonal position as well as row m and column s. Let us denote this minor by S. If there are ℓ values of i such that $1\leqslant i<m$ and $b_{ii}=1$, then we see that $S_{jj}=1$, $1\leqslant j\leqslant \ell$, while $S_{j,j-1}=1$, $\ell+2\leqslant j\leqslant s-r+1$. The other entries in the first $s-r$ columns of S are all zero.

So we see that the $(\ell+1)$th row of S contains all zero entries except for the entry $S_{\ell+1,s-r+1}=u$. By doing a cofactor expansion along this row, one can show that the determinant of S is $(-1)^{\ell+s-r}u$. Since we must have $b_{ss}=p$ and (4.1) shows that $0<u<p$, this contradicts the assumption that p is the gcd of all $s-r+1$-rowed minor determinants of B. Hence the result is proved. We remark that a similar but more detailed argument may be used to show that if $b_{mm}=p$, then this entry is the only non-zero entry in the mth row of B. □

We want the number of upper triangular integer matrices B satisfying (4.1) for which the Smith normal form satisfies (4.4). Then b_{ss} is either 1 or p. Suppose firstly that $b_{ss}=1$. Then (4.1) shows that $b_{is}=0$ for $1\leqslant i<s$ and the Smith normal form of the $(s-1)\times(s-1)$ matrix obtained by discarding the last row and column of B must contain r p's. There are $\nu_{s-1}[p;r]$ of these which leads to the first term on the right hand side of (4.3).

The other case to look at is when $b_{ss}=p$. Theorem 7(b) shows that $b_{ms}=0$ for each of the $r-1$ values of m for which $b_{mm}=p$, $1\leqslant m<s$. Also we see from (4.1) that the $s-r$ rows with $b_{ii}=1$ have entries b_{is} taking on any value from 0 to $p-1$ inclusive. Thus there are p^{s-r} different possibilities for the sth column of B. Clearly the Smith normal form of the $(s-1)\times(s-1)$ matrix obtained by discarding the last row and column of B must have $r-1$ p's. Hence the actual number of matrices B that satisfy (4.1), have $b_{ss}=p$, and have a Smith normal form satisfying (4.4) is given by $p^{s-r}\nu_{s-1}[p;r-1]$. This provides the second term on the right hand side of (4.3).

5. NUMERICAL RESULTS

By using Theorem 6, we see that Theorem 5(b) may be numerically tested by

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press

	Invariants					
Diagonal Entries of B	48	24, 2	12, 4	12, 2, 2	6, 2, 2, 2	Row Total
48, 1, 1, 1, 1	5,421,361					5,421,361
24, 2, 1, 1, 1	2,655,435	2,655,435				5,310,870
16, 3, 1, 1, 1	3,037,144					3,037,144
12, 4, 1, 1, 1	1,146,200	573,100	573,100			2,292,400
8, 6, 1, 1, 1	928,797	928,797				1,857,594
12, 2, 2, 1, 1	425,410	850,820	212,705	212,705		1,701,640
8, 3, 2, 1, 1	965,731	965,731				1,931,462
6, 4, 2, 1, 1	388,920	777,840	194,460	194,460		1,555,680
4, 4, 3, 1, 1	256,674	128,337	128,337			513,348
6, 2, 2, 2, 1	28,320	99,120	35,400	60,180	3,540	226,560
4, 3, 2, 2, 1	108,416	216,832	54,208	54,208		433,664
3, 2, 2, 2, 2	1,688	5,908	2,110	3,587	211	13,504
Column Total:	15,364,096	7,201,920	1,200,320	525,140	3,751	24,295,227
Prediction:	15,364,096	7,201,920	1,200,320	525,140	3,751	

Table 1

forming, for given N, all upper triangular integer matrices with entries satisfying (4.1), reducing them all to Smith normal form, and then counting up how many there are that have a given set of invariants. This idea is implemented in a computer program in which the diagonal entries of the upper triangular matrix B are entered as input data.

The results that are given here in Table 1 are for $N = 48$ and $s = 5$. Thus, for example, we see that if the diagonal entries of B are 24, 2, 1, 1, and 1, then there are a total of $5,310,870$ upper triangular integer matrices having these diagonal entries which satisfy (4.1). On reducing all these to Smith normal form we find that $2,655,435$ of them yield an invariant of 48 while the remaining $2,655,435$ yield invariants 24 and 2.

Theorem 1 yields $T_5(48) = T_5(16)T_5(3) = 200787 \times 121 = 24,295,227$. Also Theorem 3 shows that $\nu_5(48) = \nu_5(16)\nu_5(3)$, $\nu_5(24,2) = \nu_5(8,2)\nu_5(3)$, $\nu_5(12,4) = \nu_5(4,4)\nu_5(3)$, $\nu_5(12,2,2) = \nu_5(4,2,2)\nu_5(3)$, and $\nu_5(6,2,2,2) = \nu_5(2,2,2,2)\nu_5(3)$. Theorem 5(b) then leads to the predictions given in Table 1 which, as expected, agree with the column totals.

References

[1] T.S. Blyth, *Module theory* (Clarendon Press, Oxford, 1977).

[2] W. Burnside, *Theory of groups of finite order* (Dover Publications, New York, 1955).

[3] E. Hlawka, 'Zur angenäherten Berechnung mehrfacher Integrale', *Monatsh. Math.* **66** (1962), 140–151.

[4] C.S. Iliopoulos, 'Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix', *SIAM J. Comput.* **18** (1989), 658–669.

[5] N.M. Korobov, 'The approximate computation of multiple integrals', (in Russian), *Dokl. Akad. Nauk SSSR* **124** (1959), 1207–1210.

[6] T.N. Langtry, 'The determination of canonical forms for lattice quadrature rules', (preprint).

[7] W. Ledermann, *Introduction to the theory of finite groups* (Oliver and Boyd, Edinburgh, 1964).

[8] J.N. Lyness and P. Keast, 'Application of the Smith normal form to the structure of lattice rules', (preprint).

[9] J.N. Lyness and T. Sørevik, 'The number of lattice rules', *BIT* **29** (1989), 527–534.

[10] H.M. Salkin and K. Mathur, *Foundations of integer programming* (North-Holland, New York, 1989).

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

[12] H.W. Turnbull and A.C. Aitken, *An introduction to the theory of canonical matrices* (Blackie & Son, London, 1932).

Department of Mathematics and Statistics
The University of Waikato
Hamilton
New Zealand

School of Mathematics
University of New South Wales
Sydney NSW 2033
Australia

https://doi.org/10.1017/S0004972700012144 Published online by Cambridge University Press