ELSEVIER

Journal of Computational and Applied Mathematics 59 (1995) 129–143

JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS

The determination of canonical forms for lattice quadrature rules

T.N. Langtry

School of Mathematical Sciences, University of Technology, Sydney, P.O. Box 123, Broadway, NSW 2007, Australia

Received 15 September 1991; revised 12 January 1994

Abstract

Lattice rules are equal weight numerical quadrature rules for the integration of periodic functions over the s-dimensional unit hypercube $U^s = [0,1)^s$. For a given lattice rule, say Q_L, a set of points L (the integration lattice), regularly spaced in all of $\mathbb{R}^s$, is generated by a finite number of rational vectors. The abscissa set for Q_L is then $P(Q_L) = L \cap U^s$. It is known that $P(Q_L)$ is a finite Abelian group under addition modulo the integer lattice $\mathbb{Z}^s$, and that $Q_L(f)$ may be written in the form of a nonrepetitive multiple sum,

$$Q_L(f) = \frac{1}{n_1 \cdots n_m} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f\left(\frac{j_1}{n_1} z_1 + \cdots + \frac{j_m}{n_m} z_m\right),$$

known as a canonical form, in which $+$ denotes addition modulo $\mathbb{Z}^s$. In this form, $z_i \in \mathbb{Z}^s$, m is called the *rank* and $n_1, n_2, \ldots, n_m$ are called the *invariants* of Q_L, and $n_{i+1} | n_i$ for $i = 1, 2, \ldots, m-1$. The rank and invariants are uniquely determined for a given lattice rule. In this paper we provide a construction of a canonical form for a lattice rule Q_L, given a generator set for the lattice L. We then show how the rank and invariants of Q_L may be determined directly from the generators of the dual lattice $L^\perp$.

Keywords: Numerical quadrature; Numerical cubature; Multiple integration; Lattice rules; Abelian groups

1. Introduction

Lattice rules are numerical quadrature rules for the integration of periodic functions over the unit hypercube $U^s = [0,1)^s$. They are generalisations, introduced in [10, 11], of the trapezoidal rule in one dimension, and of number theoretic rules in higher dimensions.

Definition 1.1. Let $s \geqslant 1$.

(a) An *integration lattice in s dimensions* is a subset L of $\mathbb{R}^s$ such that:

(i) $L \supseteq \mathbb{Z}^s$,

(ii) $\boldsymbol{x}_1, \boldsymbol{x}_2 \in L \Rightarrow \boldsymbol{x}_1 \pm \boldsymbol{x}_2 \in L$, and

(iii) $\inf\{\|\boldsymbol{x}_1 - \boldsymbol{x}_2\| : \boldsymbol{x}_1, \boldsymbol{x}_2 \in L, \boldsymbol{x}_1 \neq \boldsymbol{x}_2\} > 0$.

0377-0427/95/$09.50
SSDI 0377-0427(94)00025-V

(b) The *lattice rule* Q_L corresponding to the integration lattice L is the rule defined by

$$Q_L(f) = \frac{1}{N(Q_L)} \sum_{x \in L \cap U^s} f(x),$$

where $N(Q_L)$ is the cardinality of the set $L \cap U^s$.

(c) The *abscissa set* of the lattice rule Q_L is the set $P(Q_L) = L \cap U^s$.

Sloan and Lyness [12, Theorem 2.3] have shown that $P(Q_L)$ is an Abelian group under addition modulo $\mathbb{Z}^s$ and, in particular, that $P(Q_L) \cong L/\mathbb{Z}^s$. Further, $P(Q_L)$ is finite and so the basis theorem [12, Theorem 3.1] for finite Abelian groups holds. For ease of reference, we restate this theorem here.

Theorem 1.2 (Basis theorem for finite Abelian groups). *A nontrivial finite Abelian group P may be expressed as a direct sum*

$$P \cong D_1 \oplus D_2 \oplus \cdots \oplus D_m,$$

where D_i is a cyclic subgroup of P of order $n_i > 1$, and

$$n_{i+1} | n_i \quad \text{for } i = 1, \ldots, m-1.$$

The numbers m and $n_1, n_2, \ldots, n_m$ are uniquely determined.

Since $P(Q_L)$ is a finite Abelian group, it follows [12, Theorem 4.1] that a lattice rule Q_L is expressible in a form

$$Q_L(f) = \frac{1}{N(Q_L)} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f(j_1 \boldsymbol{g}_1 + \cdots + j_m \boldsymbol{g}_m), \tag{1.1}$$

where $+$ denotes addition modulo $\mathbb{Z}^s$, $\boldsymbol{g}_i \in P(Q_L)$ for each $i = 1, \ldots, m$, and $\boldsymbol{g}_i = (1/n_i)\boldsymbol{z}_i$, with $n_i \in \mathbb{Z}$ and $\boldsymbol{z}_i \in \mathbb{Z}^s$. The implication of Theorem 1.2 is that there exists an expression for $Q_L(f)$ in the form of (1.1) in which each element of $P(Q_L)$ is generated only once during the summation. Such a form is said to be *nonrepetitive*. Using this terminology, the application of Theorem 1.2 to $P(Q_L)$, together with the observation that an integration lattice L in s dimensions is generated by s linearly independent vectors, yields the following result [12, Theorem 4.5].

Theorem 1.3 (Sloan–Lyness). *An s-dimensional lattice rule Q_L can be expressed as a nonrepetitive form*

$$Q_L(f) = \frac{1}{n_1 \cdots n_m} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f\left(\frac{j_1}{n_1}\boldsymbol{z}_1 + \cdots + \frac{j_m}{n_m}\boldsymbol{z}_m\right), \tag{1.2}$$

where m and $n_1, \ldots, n_m$ are uniquely determined natural numbers satisfying $1 \leqslant m \leqslant s$ and

$$n_{i+1} | n_i, \quad i = 1, \ldots, m-1; \qquad n_m > 1.$$

The vectors $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m$ are linearly independent and have integer components.

Definition 1.4 (Sloan–Lyness). Using the terminology of Theorem 1.3,
(a) the number m is called the *rank* of Q_L,
(b) the numbers $n_1, \ldots, n_m$ are called the *invariants* of Q_L, and
(c) the expression for Q_L given in (1.2) is called a *canonical form* for the lattice rule.

In investigating the properties of lattice rules it is of interest to be able to compute a canonical form for a given lattice rule. Usually a rule Q_L is defined by a set of generating vectors for $P(Q_L)$, with no guarantee that the form (1.1) corresponding to this set is either canonical or nonrepetitive. Also, the proof in [12] that a canonical form of the rule exists is nonconstructive, leaving open the question of how to compute such a form for Q_L. This is the primary question that we shall address in this paper.

The approach which we shall follow is based on a constructive proof of Theorem 1.2. In Section 2 we show how the construction may be adapted to provide an algorithm for computing a canonical form for a lattice rule, given a generator set for the rule. This section contains the principal results of the paper. In Section 3 we present a simple example to illustrate the use of the algorithm, and in Section 4 we consider the significance of our results in the context of the *dual* of the integration lattice, a definition of which will be given in that section. Some concluding remarks are presented in Section 5.

2. Construction of a canonical form

We consider now the problem of constructing a canonical form for a lattice quadrature rule Q_L. Before proceeding with the development of the construction, we recall that the algebraic structure of the abscissa set $P(Q_L)$ is that of an Abelian group. The algebraic structure of the corresponding integration lattice L is that of a particular type of Abelian group, namely a *free* Abelian group, which term we define below. Loosely speaking, the axioms obeyed by a free Abelian group are those obeyed by a vector space in which the underlying field has been replaced by the ring of integers. Consequently, many of the techniques of linear algebra may be drawn upon, with some modification, in the study of free Abelian groups and related structures. In particular, we shall require the following definitions and results from Abelian group theory for the construction of a canonical form for a lattice rule. A more complete discussion of them may be found in standard texts such as [3, 6]. Note that we shall use additive notation for the group operation, but we shall denote quotient groups using the notation F/K.

Definition 2.1. Let F be an Abelian group and $G = \{g_1, g_2, \ldots, g_v\} \subseteq F$.
(a) An element $f \in F$ is a *linear combination (over* $\mathbb{Z}$*)* of the elements $g_1, \ldots, g_v$ of G if there exist integers $\lambda_1, \ldots, \lambda_v$ such that $\sum_{i=1}^{v} \lambda_i g_i = f$. The set of all such linear combinations is denoted by span(G).
(b) A *relation* on G is a linear combination over $\mathbb{Z}$ of the elements of G satisfying $\sum_{i=1}^{v} \lambda_i g_i = 0$. The tuple $(\lambda_1, \lambda_2, \ldots, \lambda_v) \in \mathbb{Z}^v$ is called a *relator* on G.
(c) G is called a *generator set* for F if every $f \in F$ can be written as a linear combination over $\mathbb{Z}$ of elements of G.

(d) The set G is *linearly independent over* $\mathbb{Z}$ if the equation $\sum_{i=1}^{v} \lambda_i g_i = 0$ has the unique solution $\lambda_1 = \cdots = \lambda_v = 0$, where $\lambda_i \in \mathbb{Z}$.

(e) A *presentation* of F is a pair $\langle G : R \rangle$ such that G is a generator set for F and R is a defining set of relators on G, that is, a set $\{r_1, r_2, \ldots, r_t\}$ of relators on G such that

$$\sum_{i=1}^{v} \lambda_i g_i = 0 \text{ if and only if } (\lambda_1, \lambda_2, \ldots, \lambda_v) \in \operatorname{span}(R).$$

(f) The set G is said to *generate F freely* if
  (i) G generates F, and
  (ii) G is linearly independent over $\mathbb{Z}$.

In this case G is called a *basis* of F, and F is said to be *free*.

Theorem 2.2. *Let F be an Abelian group and $G = \{g_1, g_2, \ldots, g_v\} \subseteq F$. Then the following are equivalent:*

(a) *G generates F freely,*
(b) *every map $G \to P$, where P is an Abelian group, extends to a homomorphism $F \to P$,*
(c) *every $f \in F$ is uniquely expressible in the form $f = \sum_{i=1}^{v} \lambda_i g_i$, where $\lambda_i \in \mathbb{Z}$, and*
(d) *every $g_i \in G$ is aperiodic, and $F \cong \mathbb{Z}g_1 \oplus \mathbb{Z}g_2 \oplus \cdots \oplus \mathbb{Z}g_v$.*

Corollary 2.3. *An Abelian group F is freely generated by v elements if and only if $F \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, with the direct sum containing v terms.*

Theorem 2.4. *Let F be a free Abelian group. Then every basis of F has the same number of elements.*

Definition 2.5. Let F be an Abelian group freely generated by v elements. Then v is called the *rank* of F.

The terminology introduced in these definitions may be applied to both the integration lattice L and the abscissa set $P(Q_L)$ of a given rule Q_L, since both are finitely generated Abelian groups. The following result establishes that L is free.

Theorem 2.6. *Let L be an s-dimensional integration lattice. Then L is a finitely generated free Abelian group of rank s.*

Proof. Since L is closed under addition in $\mathbb{R}^s$ it follows that L is an Abelian group. We show firstly that it is finitely generated. From part (a) (iii) of Definition 1.1 it follows that $P(Q_L)$ is finite. Further, $G = \{e_1, \ldots, e_s\} \cup P(Q_L)$, where $\{e_1, \ldots, e_s\}$ is the standard Cartesian basis for $\mathbb{Z}^s$, is a (finite) generator set for L. To establish this we may use the following argument by contradiction. Assume that there is some $x \in L$ such that x is not expressible as a linear combination over $\mathbb{Z}$ of the elements of G, and let $\lfloor x \rfloor = \sum_{i=1}^{s} \lfloor x_i \rfloor e_i$ denote the integer part of x. Then $\lfloor x \rfloor \in L$ and $x' = x - \lfloor x \rfloor \in L$ by the closure of L under addition, and clearly $x' \in U^s$. Hence $x' \in P(Q_L) \subseteq G$. But $x = x' + \lfloor x \rfloor = \sum_{i=1}^{s} \lfloor x_i \rfloor e_i + x'$, which contradicts our assumption.

To establish that L is free and of rank s we note that G consists of $v = s + N$ elements, where N is the order of $P(Q_L)$. It is known [11, Lemma 1] that the quadrature points of Q_L are rational vectors, from which it now follows that the elements of L are rational vectors. Thus we may denote the elements of G by $\boldsymbol{p}_1/q_1, \ldots, \boldsymbol{p}_v/q_v$, where these are rational vectors in their lowest terms, that is, where $q_i > 0, \boldsymbol{p}_i = (p_i^{(1)}, \ldots, p_i^{(s)}) \in \mathbb{Z}^s$ and $\gcd(p_i^{(1)}, \ldots, p_i^{(s)}, q_i) = 1$. Let $M = \mathrm{LCM}(q_1, \ldots, q_v)$, where LCM denotes the least common multiple of its arguments, and define by ML the set $\{M\boldsymbol{x}: \boldsymbol{x} \in L\}$. Then clearly ML is an Abelian group under the operation of addition in $\mathbb{R}^s$ and, furthermore, it is isomorphic to L. But the elements of ML are integer vectors, so ML is also a subgroup of $\mathbb{Z}^s$ and thus is free and of rank at most s (see, for example, [3, Theorem 7.8]). Consequently, L is also free and of rank at most s. Finally we observe that $\mathbb{Z}^s \subseteq L$ and hence that L must be of rank at least s. The result now follows. □

Both L and $P(Q_L)$ may be specified by presentations. Since L is free it has no nontrivial relators and so is completely specified by a generator set $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_v\}$, say. On the other hand, $P(Q_L)$ is isomorphic to the quotient group $L/\mathbb{Z}^s$, with the group operation being addition modulo $\mathbb{Z}^s$ in L. Thus a presentation of $P(Q_L)$ is $\langle G:R\rangle$, where R spans the set of tuples $(\lambda_1, \ldots, \lambda_v)$ such that $\sum_{i=1}^{v} \lambda_i \boldsymbol{g}_i \in \mathbb{Z}^s$.

Before stating our main results we note that a set of v generators for an s-dimensional integration lattice L (with, necessarily, $v \geqslant s$), represented by an $s \times v$ matrix of column vectors, can always be reduced to a basis of L by a finite sequence of elementary integer column operations. The execution of such a sequence of operations reduces the complexity of subsequent calculations. In particular, if $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_v\}$ is a generator set for L then it is straightforward to show that the following algorithm provides one method for computing a basis $A = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s\}$ of L. Note that a multiplicative factor μ is used to transform the problem into one whose solution requires only integer arithmetic.

Algorithm 2.7.

Notation: *The jth column of a matrix* $\boldsymbol{X}$ *is denoted by* $\boldsymbol{x}_j$. *The symbol* $\lfloor q \rfloor$ *denotes the greatest integer* z *less than or equal to* q.

Input: *An* $s \times v$ *matrix* $\boldsymbol{G}$ *with nonzero columns which generate the* s*-dimensional integration lattice* L.

Output: *An* $s \times v$ *matrix* $\boldsymbol{G} = (\boldsymbol{A}|\boldsymbol{0})$ *such that* $\boldsymbol{A}$ *is lower triangular and has linearly independent columns which form a basis for* L.

Begin
  For $j = 1, 2, \ldots, v$ *do*
    $m_j \leftarrow$ *least* $m \in \mathbb{N}$ *such that* $m\boldsymbol{g}_j \in \mathbb{Z}^s$
  Endfor
  $\mu \leftarrow \mathrm{LCM}(m_1, m_2, \ldots, m_v)$
  $\boldsymbol{H} \leftarrow \mu \boldsymbol{G}$
  For $k = 1, 2, \ldots, s$ *do*
    For $j = k, k+1, \ldots, v$ *do*
      If $h_{kj} < 0$ *then* $\boldsymbol{h}_j \leftarrow -1\boldsymbol{h}_j$
    Endfor
    While $\exists j \in \{k+1, \ldots, v\}$ *such that* $h_{kj} \neq 0$ *do*

$p \leftarrow m \in \{k, \ldots, v\}$ *such that* $\forall j \in \{k, \ldots, v\}$, $(h_{kj} = 0$ *or* $0 < h_{km} \leqslant h_{kj})$
$m^* \leftarrow h_{kp}$
$\boldsymbol{h}_p \leftrightarrow \boldsymbol{h}_k$
For $j = k + 1, k + 2, \ldots, v$ *do*
$\boldsymbol{h}_j \leftarrow \boldsymbol{h}_j - \lfloor (h_{kj}/m^*) \rfloor \boldsymbol{h}_k$
Endfor
Endwhile
Endfor
$\boldsymbol{G} \leftarrow (1/\mu)\boldsymbol{H}$
Stop

Remark. Algorithm 2.7 is included for completeness, and has not been designed with efficiency in mind. The basic idea of the algorithm is to compute a lower triangular matrix $\boldsymbol{H}$ whose columns span the integer lattice generated by the columns of $\mu\boldsymbol{G}$. Further reduction of the nonzero elements of $\boldsymbol{H}$ leads to a *Hermite normal form of* $\mu\boldsymbol{G}$, as described in [1], which has the same property. More sophisticated algorithms which produce the Hermite normal form of a matrix are described in [5, 7].

Definition 2.8. A nonsingular matrix $\boldsymbol{A}$ is a *generator matrix* for an integration lattice L if the columns of $\boldsymbol{A}$ form a basis for L.

Algorithm 2.7 and Definition 2.8 allow us to restate our problem as follows: given a generator matrix $\boldsymbol{A}$ for the s-dimensional integration lattice L, find a canonical form for Q_L.

Theorem 2.9. *Let L be an s-dimensional integration lattice with generator matrix $\boldsymbol{A}$ and let $\boldsymbol{R} = \boldsymbol{A}^{-1}$. Then there exist $s \times s$ integer matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$, invertible over $\mathbb{Z}$, such that*

$$\boldsymbol{D} = \boldsymbol{XRY} = \operatorname{diag}(d_1, d_2, \ldots, d_s)$$

and $d_1 \mid d_2 \mid \cdots \mid d_s$, that is, $\boldsymbol{D}$ is the Smith normal form of $\boldsymbol{A}^{-1}$. Also, let $m = s - u$, where u denotes the number of unit entries in $\boldsymbol{D}$, and, for $i = 1, 2, \ldots, s$, let $n_i = d_{s+1-i}$ and $z_i = y_{s+1-i}$. Then, for $f: \mathbb{R}^s \to \mathbb{R}$,

$$Q_L(f) = \frac{1}{n_1 \cdots n_m} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f\left(\frac{j_1}{n_1} z_1 + \cdots + \frac{j_m}{n_m} z_m\right) \tag{2.1}$$

is a canonical form of the lattice rule Q_L.

Remark. The proof of Theorem 2.9 relies on the fact that $P(Q_L)$ is a finite Abelian group [12, Theorem 2.3] and that therefore Theorem 1.2 applies. A constructive proof of Theorem 1.2 has long been known. The earliest version of which we are aware is due to van der Waerden [15] in the more general context of finitely generated modules over principal ideal domains. More recent treatments appear in [3, 6]. We shall restrict our consideration to the class of finite Abelian groups.

Constructive proofs of Theorem 1.2 rely on the existence of a homomorphism from a finitely generated free Abelian group onto the group P. That homomorphism is determined by an explicit presentation of P and gives rise to an integer matrix $\boldsymbol{R}$ from which may be deduced, using a result of Smith [14, Article 14], a direct sum decomposition of P into cyclic subgroups. The essential step is

the reduction of $\boldsymbol{R}$ to Smith normal form, that is, the construction of integer matrices $\boldsymbol{D},\boldsymbol{X}$ and $\boldsymbol{Y}$ such that $\boldsymbol{D} = \boldsymbol{XRY}$ is diagonal and each diagonal entry divides the succeeding ones. The matrix $\boldsymbol{D}$ may be constructed by integer elementary row and column operations with greatest common divisor calculations replacing the division operations used in linear spaces over a field. The matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ are products of the elementary matrices which correspond respectively to the row and column operations and are therefore invertible over $\mathbb{Z}$. From here it may be shown (see, for example, [3, Ch. 10]) that, if $\boldsymbol{r}_i$ is the ith column of $\boldsymbol{R}$ and $\langle g_1, g_2, \ldots, g_v : \boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_v \rangle$ is a presentation of P, then the group elements g_i' defined by

$$g_i' = \sum_{j=1}^{s} \bar{x}_{ji} g_j,$$

where $\bar{\boldsymbol{x}}_{ji}$ denotes the entry in row j and column i of $\boldsymbol{X}^{-1}$, are generators of P with orders $d_1 \mid d_2 \mid \cdots \mid d_v$ satisfying the requirements of Theorem 1.2. Note that, in general, some of these generators may be the identity element, with order 1.

Computer programs which implement the construction of a Smith normal form have been published by a number of authors, the first to our knowledge being Smith [13]. More recently, a variation of the algorithm due to Havas and Sterling [4] has been included in the standard function library of the group theoretic programming language *Cayley* [2]. Other relevant variations are described in [1, 5, 7].

In order to prove Theorem 2.9, then, we must derive an explicit presentation of $P(Q_L)$ by establishing that the columns of $\boldsymbol{R} = \boldsymbol{A}^{-1}$ constitute a defining set of relators on the generators $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s$ given by the columns of $\boldsymbol{A}$. Van der Waerden's construction then yields a set of nontrivial generators $\{(1/n_1)z_1, (1/n_2)z_2, \ldots, (1/n_m)z_m\}$ which satisfies the requirements of a canonical form of Q_L.

Proof of Theorem 2.9. Since $\boldsymbol{A}$ is a generator matrix for L it is nonsingular, that is, $\boldsymbol{R} = \boldsymbol{A}^{-1}$ exists. Let $\boldsymbol{a}_i$ denote the ith column of $\boldsymbol{A}$. We must show that $R = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_s\}$, the set of columns of $\boldsymbol{R}$, is a defining set of relators on the set $A = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s\}$ for the group $P(Q_L)$. Now $P(Q_L) \cong L/\mathbb{Z}^s$, so a defining set of relators must span the solutions of the system of congruences

$$\sum_{j=1}^{s} c_j \boldsymbol{a}_j \equiv \boldsymbol{0} \quad \text{modulo } \mathbb{Z}^s,$$

that is, the set $S \subseteq \mathbb{Z}^s$ defined by

$$S = \{\boldsymbol{c} \in \mathbb{Z}^s : \boldsymbol{Ac} \equiv \boldsymbol{0} \text{ modulo } \mathbb{Z}^s\}.$$

Let $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_s\}$ be the standard Cartesian basis for $\mathbb{Z}^s$. Now A is a basis for L and $L \supseteq \mathbb{Z}^s$, so for each $i = 1, 2, \ldots, s$ there exists a unique linear combination of the elements of A such that

$$\sum_{j=1}^{s} r_j \boldsymbol{a}_j = \boldsymbol{e}_i.$$

That is, there is a unique $\boldsymbol{r} \in \mathbb{Z}^s$ such that $\boldsymbol{Ar} = \boldsymbol{e}_i$. Clearly, these solution vectors are the elements of R and, therefore, $R \subseteq S \subseteq \mathbb{Z}^s$. Next we show that $\text{span}(R) = S$. We have: $\boldsymbol{Ar} \equiv \boldsymbol{0}$ modulo $\mathbb{Z}^s$ if and only if $\boldsymbol{Ar} = \boldsymbol{c} = \sum_{i=1}^{s} c_i \boldsymbol{e}_i$ for some $\boldsymbol{c} \in \mathbb{Z}^s$. This is the case if and only if

$\boldsymbol{r} = \sum_{i=1}^{s} c_i \boldsymbol{A}^{-1} \boldsymbol{e}_i = \sum_{i=1}^{s} c_i \boldsymbol{r}_i$. Thus $S = \text{span}(R)$ and R is a defining set of relators on A. We may now construct a decomposition of $P(Q_L)$ into direct sum of cyclic subgroups via the reduction of $\boldsymbol{R}$ to Smith normal form as described in the preceding remark. For further details, the interested reader is referred to [3, 6]. In particular we obtain by this construction the required matrices $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\boldsymbol{D}$. Now $\boldsymbol{D} = \boldsymbol{X}\boldsymbol{A}^{-1}\boldsymbol{Y}$ and hence $\boldsymbol{A}\boldsymbol{X}^{-1}\boldsymbol{D} = \boldsymbol{Y}$. For $i = 1, \ldots, s$ let

$$z_i = y_{s+1-i} = n_i \sum_{j=1}^{s} \bar{x}_{j,s+1-i} \boldsymbol{a}_j,$$

where $\boldsymbol{X}^{-1} = (\bar{x}_{jk})$, then by construction $n_{i+1} | n_i$ for $i = 1, 2, \ldots, m-1$, with $P(Q_L) \cong \langle (1/n_1) z_1 \rangle \oplus \cdots \oplus \langle (1/n_m) z_m \rangle$. Thus (2.1) is a canonical form of Q_L. □

In practice, the method implied by Theorem 2.9 for computing a canonical form of a given lattice rule consists of finding a generator matrix $\boldsymbol{A}$ for the integration lattice, inverting this matrix and then reducing the inverse to Smith normal form. We may improve upon this method by avoiding the computation of $\boldsymbol{A}^{-1}$ and instead reducing an appropriately scaled multiple of $\boldsymbol{A}$ directly to Smith normal form.

Theorem 2.10. *Let L be an s-dimensional integration lattice with generator matrix $\boldsymbol{A}$. Then there exist $s \times s$ integer matrices $\boldsymbol{U}$ and $\boldsymbol{V}$, invertible over $\mathbb{Z}$, and an $s \times s$ integer matrix $\boldsymbol{D}^* = \text{diag}(n_1, n_2, \ldots, n_s)$ such that $n_s | n_{s-1} | \cdots | n_1$ and*

$$\boldsymbol{U}^{-1} \boldsymbol{D}^{*-1} = \boldsymbol{A}\boldsymbol{V}.$$

Also, let $m = s - u$, where u is the number of unit entries in $\boldsymbol{D}^*$, let $\boldsymbol{Z} = \boldsymbol{U}^{-1}$ and let the ith column of $\boldsymbol{Z}$ be denoted by z_i. Then, for $f: \mathbb{R}^s \to \mathbb{R}$, (2.1) is a canonical form of the lattice rule Q_L.

Proof. Let $\boldsymbol{a}_i$ denote the ith column of $\boldsymbol{A}$. As we have noted previously, the elements of $\boldsymbol{a}_i$ are rational since $\boldsymbol{A}$ is a generator matrix for L. Hence, for each $i = 1, 2, \ldots, s$ there exists a positive integer m_i such that $m_i \boldsymbol{a}_i \in \mathbb{Z}^s$ and $k\boldsymbol{a}_i \notin \mathbb{Z}^s$ for $0 < k < m_i$. Let $\mu = \text{LCM}(m_1, m_2, \ldots, m_s)$. Then $\mu \boldsymbol{A}$ is an integer matrix and so there exist $s \times s$ matrices $\boldsymbol{U}$ and $\boldsymbol{V}$, invertible over $\mathbb{Z}$, and a diagonal matrix $\boldsymbol{T} = \text{diag}(t_1, t_2, \ldots, t_s)$, the Smith normal form of $\mu \boldsymbol{A}$, such that $t_i | t_{i+1}$ for $i = 1, 2, \ldots, s-1$ and

$$\boldsymbol{U}(\mu \boldsymbol{A})\boldsymbol{V} = \mu \boldsymbol{U}\boldsymbol{A}\boldsymbol{V} = \boldsymbol{T}.$$

Inverting both sides of this equation and multiplying by μ, we obtain

$$\boldsymbol{V}^{-1} \boldsymbol{A}^{-1} \boldsymbol{U}^{-1} = \mu \boldsymbol{T}^{-1} = \text{diag}\left(\frac{\mu}{t_1}, \frac{\mu}{t_2}, \ldots, \frac{\mu}{t_s} \right).$$

But, by the argument of Theorem 2.9, the columns of $\boldsymbol{A}^{-1}$ are relators on the generator set $A = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s\}$ of the Abelian group $P(Q_L)$ formed by the abscissae of Q_L, and so $\boldsymbol{A}^{-1}$ is an integer matrix. From this it follows that $\mu \boldsymbol{T}^{-1}$ is an integer matrix and, in particular, that $\mu/t_1, \mu/t_2, \ldots, \mu/t_s \in \mathbb{Z}$. Let $n_i = \mu/t_i$ and let $\boldsymbol{D}^* = \text{diag}(n_1, n_2, \ldots, n_s)$. Then, for $i = 1, 2, \ldots, s-1$, we

have $n_{i+1} \mid n_i$, since $t_i \mid t_{i+1}$, and

$$\boldsymbol{D}^{*-1} = \boldsymbol{UAV}.$$

Now, the columns of $\boldsymbol{A}$ form a basis for L, and $\boldsymbol{U}$ and $\boldsymbol{V}$ are invertible over $\mathbb{Z}$, and so the columns of $\boldsymbol{ZD}^{*-1} = \boldsymbol{U}^{-1}\boldsymbol{D}^{*-1} = \boldsymbol{AV}$, that is, the vectors $(1/n_i)\boldsymbol{z}_i$, form a basis for L. Hence, again as described in the preceding remark, we have $P(Q_L) \cong \langle (1/n_1)\boldsymbol{z}_1 \rangle \oplus \cdots \oplus \langle (1/n_m)\boldsymbol{z}_m \rangle$ and thus

$$Q_L(f) = \frac{1}{n_1 \cdots n_m} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f\left(\frac{j_1}{n_1}\boldsymbol{z}_1 + \cdots + \frac{j_m}{n_m}\boldsymbol{z}_m\right)$$

is a canonical form for Q_L. □

The method of construction of a canonical form for a lattice rule Q_L described in the proof of Theorem 2.10 is summarised in Algorithm 2.11 below. This algorithm incorporates the use of Algorithm 2.7 to determine a basis of L. Also, we assume the availability of a procedure *SNF* for determining the Smith normal form $\boldsymbol{T}$ of a square matrix $\boldsymbol{C}$, along with the inverse $\boldsymbol{Z}$ of the associated pre-multiplier matrix. As we have already noted, a number of such procedures have been described by other authors [1, 3–5, 7, 13]. The matrix $\boldsymbol{Z}$ may be calculated simultaneously with $\boldsymbol{T}$ by performing the inverses of the row operations required to compute $\boldsymbol{T}$ on an $s \times s$ identity matrix. For further details, the reader is referred to [3, Ch. 10].

Algorithm 2.11.

Notation: *The jth column of a matrix* $\boldsymbol{X}$ *is denoted by* $\boldsymbol{x}_j$.

Input: *An* $s \times v$ *matrix* $\boldsymbol{G}$ *whose columns the s-dimensional integration lattice* L.

Output: *Integers* $m, n_1, \ldots, n_m$ *and integer vectors* $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m$ *such that*

$$Q_L(f) = \frac{1}{n_1 \cdots n_m} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f\left(\frac{j_1}{n_1}\boldsymbol{z}_1 + \cdots + \frac{j_m}{n_m}\boldsymbol{z}_m\right)$$

is in canonical form.

Interface with procedure SNF:

Input: s (*a positive integer*) *and* $\boldsymbol{C}$ (*an* $s \times s$ *integer matrix*).

Output: $\boldsymbol{T} = \operatorname{diag}(t_1, \ldots, t_s)$ (*the Smith normal form of* $\boldsymbol{C}$) *and* $\boldsymbol{Z}$ (*an integer matrix, invertible over* $\mathbb{Z}$, *such that* $\boldsymbol{Z}^{-1}\boldsymbol{CV} = \boldsymbol{T}$ *for some integer matrix* $\boldsymbol{V}$ *which is also invertible over* $\mathbb{Z}$).

Begin

$\mu \leftarrow \operatorname{LCM}(m_1, \ldots, m_v)$ *where* m_i *is the least positive integer* m *such that* $m\boldsymbol{g}_i \in \mathbb{Z}^s$.

$\boldsymbol{C} \leftarrow \mu \boldsymbol{A}$, *where* $\boldsymbol{A}$ *is determined by Algorithm* 2.7.

SNF $(\boldsymbol{Z}, \boldsymbol{T}, \boldsymbol{C}, s)$

$m \leftarrow s - u$, *where* u *is the number of unit entries in* $\mu \boldsymbol{T}^{-1}$.

For $i = 1, \ldots, m$ *do*

$n_i \leftarrow \mu / t_i$

Endfor

Stop

3. Example

As an illustration of Algorithm 2.11, we compute a canonical form for the lattice rule in three dimensions whose abscissa group $P(Q_L)$ has generator set $G = \{g_1, g_2, g_3\}$, where

$$g_1 = \frac{1}{6}\begin{pmatrix} 2 \\ -5 \\ 3 \end{pmatrix}, \qquad g_2 = \frac{1}{3}\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} = \frac{1}{6}\begin{pmatrix} 2 \\ 4 \\ 0 \end{pmatrix}, \qquad g_3 = \frac{1}{3}\begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} = \frac{1}{6}\begin{pmatrix} -4 \\ 4 \\ 2 \end{pmatrix}.$$

The set G generates $P(Q_L)$ under the operation of addition modulo $\mathbb{Z}^s$, but is not sufficient to generate L under addition in $\mathbb{R}^s$. For example, we observe that G is linearly independent over $\mathbb{R}^s$, and hence over $\mathbb{Z}^s$, and that

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{4}{9}g_1 + \frac{11}{9}g_2 - \frac{2}{3}g_3.$$

Since the coefficients in this expression are unique, due to the linear independence of G in $\mathbb{R}^s$, it follows that e_1 is not expressible as a linear combination over $\mathbb{Z}$ of the elements of G. Since $e_1 \in L$ this implies that G is not a generator set for L. To recover a generator set for L from the generator set G for $P(Q_L) \cong L/\mathbb{Z}^s$ we must include elements which span $\mathbb{Z}^s$, such as the standard Cartesian basis vectors

$$g_4 = e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad g_5 = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \qquad g_6 = e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

We begin by reducing the augmented linearly dependent initial generator set to a basis for L, via suitable elementary column operations. Note that the multiplicative factor $\mu = \mathrm{LCM}(m_1, m_2, \ldots, m_6)$, where $g_i = (1/m_i)z_i$ with $z_i \in \mathbb{Z}^s$, is used to convert the problem into an equivalent one whose solution requires only integer arithmetic.

Step 1. Let $\mu = \mathrm{LCM}(6,3,3,1,1,1) = 6$.

Step 2. Let

$$\mu G = \begin{pmatrix} 2 & 2 & -4 & 6 & 0 & 0 \\ -5 & 4 & 4 & 0 & 6 & 0 \\ 3 & 0 & 2 & 0 & 0 & 6 \end{pmatrix}.$$

Reduce μG to a nonsingular generator matrix μA for μL. We have

$$\mu G \sim \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ -5 & 9 & -6 & 15 & 6 & 0 \\ 3 & -3 & 8 & -9 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ -5 & 3 & 0 & 0 & 0 & 0 \\ 3 & -3 & 2 & 0 & 0 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ -2 & 3 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 & 0 \end{pmatrix},$$

and we choose

$$\boldsymbol{C} = \mu \boldsymbol{A} = \begin{pmatrix} 2 & 0 & 0 \\ -2 & 3 & 0 \\ 0 & -1 & 2 \end{pmatrix}.$$

Step 3. Reduce $\mu \boldsymbol{A}$ to Smith normal form, yielding

$$\boldsymbol{T} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix} \quad \text{and} \quad \boldsymbol{Z} = \begin{pmatrix} 0 & 1 & 0 \\ 3 & -1 & 1 \\ -1 & 0 & 0 \end{pmatrix}.$$

Step 4. Let $m = 3 - 1 = 2$, $n_1 = \frac{6}{1} = 6$, $n_2 = \frac{6}{2} = 3$ and $n_3 = \frac{6}{6} = 1$. The rule

$$Q_L(f) = \frac{1}{18} \sum_{j_1=1}^{6} \sum_{j_2=1}^{3} f\left(\frac{j_1}{6} \begin{pmatrix} 0 \\ 3 \\ -1 \end{pmatrix} + \frac{j_2}{3} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right), \tag{3.1}$$

with the summation being performed modulo $\mathbb{Z}^s$, is in canonical form.

Remark. In step 3 of the example, the author used the algorithm of Bradley [1] to compute the matrices $\boldsymbol{T}$ and $\boldsymbol{Z}$. Such calculations are prone to a number of computational difficulties (see, for example, [4]) and the reader is referred to [5, 7] for a discussion of these problems and of the space and time complexities of related algorithms.

We may verify that the right-hand side of (3.1) is indeed a canonical form for Q_L as follows. By [12, Corollary 4.6] the expression is a canonical form for some lattice rule provided only that it is nonrepetitive, that is, that no element $\boldsymbol{x}$ of the abscissa set of the rule is expressible in more than one way in the form

$$\boldsymbol{x} = \sum_{i=1}^{m} j_i \frac{\boldsymbol{z}_i}{n_i} \quad \text{modulo } \mathbb{Z}^s,$$

where $0 \leqslant j_i < n_i$ for $i = 1, \ldots, m$. Clearly this is the case if $\{z_1/n_1, \ldots, z_m/n_m\}$ is linearly independent over $\mathbb{Z}$. The interested reader may verify that this is so in the present case. To establish that the expression in (3.1) is a canonical form for the rule Q_L in particular, it now suffices to show that the integration lattices L_G and L_Z with generator sets $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_6\}$ and $\{z_1/n_1, z_2/n_2, \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ coincide. In fact, we have $\mu^{-1}\boldsymbol{Z}\boldsymbol{T} = \boldsymbol{Z}\boldsymbol{D}^{*-1}$ and, as noted in Section 2, the columns of $\boldsymbol{Z}\boldsymbol{D}^{*-1}$ form a basis for L_Z. Also, by construction the columns of $\boldsymbol{A}$ form a basis for L_G. It is known (see, for example, [3, Ch. 7]) that under these conditions L_G and L_Z coincide if and only if there exists an integer matrix $\boldsymbol{V}$, invertible over $\mathbb{Z}$, such that $\boldsymbol{Z}\boldsymbol{D}^{*-1} = \boldsymbol{A}\boldsymbol{V}$. This is the case if and only if

$$|\det(\boldsymbol{A}^{-1}\boldsymbol{Z}\boldsymbol{D}^{*-1})| = |\det(\mu^{-1}\boldsymbol{A}^{-1}\boldsymbol{Z}\boldsymbol{T})| = 1.$$

The interested reader may verify that this is indeed the case in the present example.

4. Determination of rank and invariants in the dual lattice

In Section 2 we developed a procedure for the calculation of the rank, the invariants and a canonical form of a lattice rule, given a generator set for the lattice. However, much of the investigation of lattice rules is conducted by examining the *dual* of an integration lattice, rather than the lattice itself. (See, for example, [11].)

Definition 4.1. The *dual lattice* $L^{\perp}$ of a lattice L is given by

$$L^{\perp} = \{\boldsymbol{h} \in \mathbb{R}^s : \boldsymbol{h} \cdot \boldsymbol{x} \in \mathbb{Z} \text{ for all } \boldsymbol{x} \in L\}.$$

Hence there arises the problem of determining the rank and invariants of a lattice rule directly from a generator set of the dual of the corresponding lattice. The techniques used in the preceding sections may be adapted in a straightforward fashion which enables us to solve this problem. We begin by recalling the following results, the first of which is essentially a restatement of [8, Theorem 5.1].

Lemma 4.2. *Let L be an s-dimensional integration lattice with basis $A = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s\}$. Define $\boldsymbol{A} = (a_{ij})$, where a_{ij} denotes the ith component of $\boldsymbol{a}_j$. Then $\boldsymbol{A}$ is invertible and $L^{\perp}$ is a free Abelian group of rank s with basis $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_s\}$, where $\boldsymbol{b}_j$ is the jth column of $\boldsymbol{B} = (\boldsymbol{A}^{\mathrm{T}})^{-1}$.*

Proof. The invertibility of $\boldsymbol{A}$ follows from the fact that A is a basis of L. The relationship between the generator sets A and B was established by [8, Theorem 5.1] and implies that B is linearly independent over $\mathbb{Z}$. Hence the Abelian group

$$L^{\perp} = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_s \rangle$$

is free and of rank s. □

Definition 4.3. The matrix $\boldsymbol{B}$ defined in Lemma 4.2 is called a *generator matrix* of the lattice $L^{\perp}$.

Lemma 4.4 (Lyness [8, Theorem 5.2]). *A nonsingular $s \times s$ matrix $\boldsymbol{A}$ is the generator matrix of an integration lattice L if and only if $\boldsymbol{B} = (\boldsymbol{A}^{\mathrm{T}})^{-1}$ has only integer elements.*

Lemmas 4.2 and 4.4 allow us to restate our problem as follows: given a nonsingular $s \times s$ integer matrix $\boldsymbol{B}$, determine the rank and invariants of the lattice rule whose dual lattice has generator matrix $\boldsymbol{B}$.

Theorem 4.5. *Let $\boldsymbol{B}$ be a nonsingular $s \times s$ integer matrix. Then*

(a) *$\boldsymbol{B}$ is the generator matrix of the dual $L^{\perp}$ of an integration lattice L,*

(b) *the columns $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_s$ of $\boldsymbol{A} = (\boldsymbol{B}^{-1})^{\mathrm{T}}$ form a basis of L,*

(c) *the set $G = \{\boldsymbol{g}_i : \boldsymbol{g}_i \equiv \boldsymbol{a}_i \text{ modulo } \mathbb{Z}^s, \boldsymbol{g}_i \in U^s, i = 1, 2, \ldots, s\}$, where $U^s = [0, 1)^s$, is a generator set for the abscissa group $P(Q_L)$ of the lattice rule Q_L, and*

(d) *a defining set of relators on G for $P(Q_L)$ is given by $R = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_s\}$, where $\boldsymbol{r}_i$ is the ith row of $\boldsymbol{B}$.*

Also, let $\boldsymbol{D} = \operatorname{diag}(d_1, d_2, \ldots, d_s)$, where $d_i \in \mathbb{Z}$, be the Smith normal form of $\boldsymbol{B}^{\mathrm{T}}$, that is, let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be matrices, invertible over $\mathbb{Z}$, such that $\boldsymbol{D} = \boldsymbol{X}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{Y}$ and $d_i | d_{i+1}$ for $i = 1, \ldots, s-1$. Let m denote the number of nonunit elements of $\{d_1, d_2, \ldots, d_s\}$ and let $n_i = d_{s+1-i}$ for $i = 1, 2, \ldots, m$. Then

(e) *m is the rank and $n_1, n_2, \ldots, n_m$ are the invariants of Q_L, ordered so that $n_{i+1} | n_i$ for $i = 1, 2, \ldots, m-1$, and*

(f) *a canonical form for Q_L is given by*

$$Q_L(f) = \frac{1}{N} \sum_{j_1=1}^{n_1} \cdots \sum_{j_m=1}^{n_m} f\left(\frac{j_1}{n_1}\boldsymbol{z}_1 + \cdots + \frac{j_m}{n_m}\boldsymbol{z}_m\right),$$

where $N = \prod_{i=1}^{m} n_i$, $f: \mathbb{R}^s \to \mathbb{R}$ and $\boldsymbol{z}_i$ is the $(s+1-i)$-th column of $\boldsymbol{Y}$.

Proof. Assertions (a) and (b) follow immediately from Lemmas 4.2 and 4.4, whilst (c) is little more than a restatement of Theorem 2.3 of [12]. To establish (d) we let $\boldsymbol{R} = \boldsymbol{A}^{-1} = \boldsymbol{B}^{\mathrm{T}}$ and observe that R is a defining set of relators on $P(Q_L)$ as a consequence of the argument of Theorem 2.9. We then obtain (e) and (f) directly from Theorem 2.9. □

Example 4.6. We consider again the example of Section 3. In that case, we had

$$\boldsymbol{A} = \frac{1}{6}\begin{pmatrix} 2 & 0 & 0 \\ -5 & 3 & 0 \\ 3 & -3 & 2 \end{pmatrix}.$$

Consequently,

$$\boldsymbol{B}^{\mathrm{T}} = \boldsymbol{A}^{-1} = \begin{pmatrix} 3 & 0 & 0 \\ 5 & 2 & 0 \\ 3 & 3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

and hence Q_L is of rank 2 with invariants $n_1 = 6$ and $n_2 = 3$.

5. Concluding remarks

In this paper we have established procedures for the determination of the rank, the invariants and a canonical form for a lattice quadrature rule, given a generator set for either the integration lattice or its dual. These procedures have been implemented by the author as Fortran subroutines. At the present time, the subroutines which compute Smith and Hermite normal forms are based on the algorithms described in [1]. However, as noted in [4], subroutines based on these algorithms are susceptible to integer overflow when dealing with matrices of even moderate size. Thus, when dealing with lattice rules of large order the use of more robust algorithms such as those described in [5] should be considered.

Note. After the author had finished this work he learnt from Prof. I.H. Sloan that Dr. J.N. Lyness and Dr. P. Keast had recently submitted for publication a paper [9] in which the Smith normal form of a matrix is employed to obtain similar results to those contained in this paper.

Acknowledgements

The author is grateful to Prof. I.H. Sloan, Dr. S.A.R. Disney and Dr. S. Joe of the University of New South Wales and Prof. H. Niederreiter of the Austrian Academy of Sciences for their helpful comments, and to Dr. J. Cannon of the University of Sydney for Ref. [7]. The work was carried out as part of a doctoral program under the supervision of Prof. Sloan and Dr. Disney. The comments of an anonymous referee helped to improve significantly the exposition of the work.

References

[1] G.H. Bradley, Algorithms for Hermite and Smith normal matrices and linear diophantine equations, *Math. Comp.* **25** (1971) 897–907.

[2] J.J. Cannon, An introduction to the group theory language, Cayley, in: M.D. Atkinson, Ed., *Computational Group Theory: Proc. London Math. Soc. Symp. on Computational Group Theory* (Academic Press, London, 1984) 145–183.

[3] B. Hartley and T.O. Hawkes, *Rings, Modules and Linear Algebra* (Chapman and Hall, London and New York, 1970).

[4] G. Havas and L.S. Sterling, Integer matrices and Abelian groups, in: E.W. Ng, Ed., *Symbolic and Algebraic Computation*, Lecture Notes in Computer Science **72** (Springer, Berlin, 1979) 431–451.

[5] 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.
[6] N. Jacobson, *Basic Algebra*, Vol. 1 (Freeman, New York, 2nd ed., 1985).
[7] R. Kannan and A. Bechem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, *SIAM J. Comput.* **8** (1979) 499–507.
[8] J.N. Lyness, An introduction to lattice rules and their generator matrices, *IMA J. Numer. Anal.* **9** (1989) 405–419.
[9] J.N. Lyness and P. Keast, Application of the Smith normal form to the structure of lattice rules, *SIAM J. Matrix Anal Appl.*, to appear.
[10] I.H. Sloan, Lattice methods for multiple integration, *J. Comput. Appl. Math.* **12 & 13** (1985) 131–143.
[11] I.H. Sloan and P.J. Kachoyan, Lattice methods for multiple integration: theory, error analysis and examples, *SIAM J. Numer. Anal.* **24** (1987) 116–128.
[12] I.H. Sloan and J.N. Lyness, The representation of lattice quadrature rules as multiple sums, *Math. Comp.* **52** (1989) 81–94.
[13] D.A. Smith, A basis algorithm for finitely generated Abelian groups, *Math. Algorithms* **1** (1966) 13–26.
[14] H.J.S. Smith, On systems of indeterminate equations and congruences, *Philos. Trans. Roy. Soc. London Ser. A* **151** (1861) 293–326.
[15] B.L. van der Waerden, *Moderne Algebra*, Vol. 2 (Springer, Berlin, 1931) (German); English translation (Ungar, New York).