Submitted to BIT on 5 May 1998 (Revised 19 February 1999)

A CONSTRUCTIVE APPROACH TO LATTICE RULE CANONICAL FORMS

J. N. LYNESS[1] and S. JOE[2]

[1] *Mathematics and Computer Science Division, Argonne National Laboratory, 9700 South Cass Avenue, Argonne, IL 60439 U.S.A. email: lyness@mcs.anl.gov*

[2] *Department of Mathematics, The University of Waikato, Private Bag 3105, Hamilton, New Zealand. email: stephenj@math.waikato.ac.nz*

Abstract.

The rank and invariants of a general lattice rule are conventionally defined in terms of the group-theoretic properties of the rule. Here we give a constructive definition of the rank and invariants using integer matrices. This underpins a nonabstract algorithm set in matrix algebra for obtaining the Sylow p-decomposition of a lattice rule. This approach is particularly useful when it is not known whether the form in which the lattice rule is specified is canonical or even repetitive. A new set of necessary and sufficient conditions for recognizing a canonical form is given.

AMS subject classification: 65D30.

Key words: Constructing canonical forms, lattice rules, Sylow p-decomposition.

1 Introduction

An s-dimensional *lattice rule* $Q(\Lambda)$ is an equal-weight quadrature rule on $[0,1)^s$ of the form

$$Q(\Lambda)f = \frac{1}{N}\sum_{j=1}^{N} f(\mathbf{x}_j),$$

where $\mathbf{x}_1, \ldots, \mathbf{x}_N$ are all the points of $[0,1)^s$ that belong to an integration lattice Λ. An s-dimensional *integration lattice* is a discrete set of points that is closed under normal addition and subtraction and that contains the unit lattice Λ_0 as a sublattice. Here Λ_0 is the familiar lattice consisting of all points $\mathbf{x} = (x_1, x_2, \ldots, x_s)$, all of whose components x_i are integers. The set of abscissas used for a lattice rule forms an Abelian group under addition modulo 1.

It is known [SL89] that every s-dimensional lattice rule may be written in the form $Qf = \mathcal{Q}[t, D, Z, s]f$, where

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

here t and d_i are positive integers, $\mathbf{z}_i \in \Lambda_0$, and $\{\mathbf{x}\} \in [0,1)^s$ denotes the vector whose components are the fractional parts of the components of $\mathbf{x}$. This form is known as a *t-cycle $D-Z$ form* of an s-dimensional lattice rule [LK95]. The parameters in the abbreviation $\mathcal{Q}[t,D,Z,s]$ are D, which denotes the $t \times t$ diagonal integer matrix having positive diagonal elements d_i, and Z, which denotes the $t \times s$ integer matrix having rows $\mathbf{z}_i$.

The number of distinct quadrature points in a lattice rule is known as the *order* of the rule and is denoted by $\nu(Q)$.

DEFINITION 1.1. *The rule form $\mathcal{Q}[t,D,Z,s]$ is termed* nonrepetitive *when the order of Q is $\nu(Q) = \prod_{i=1}^{t} d_i$.*

On the other hand, a $D-Z$ form may be *repetitive*; that is, the order of the lattice rule is less than $d_1 d_2 \cdots d_t$. (One can show that the number of distinct quadrature points in a repetitive $D-Z$ form is $d_1 d_2 \cdots d_t / k$ for some integer $k > 1$.)

A given lattice rule has many nonrepetitive distinct $D-Z$ forms. In [SL89] a partial solution to this problem of nonuniqueness is given. There it is shown that each lattice rule may be expressed in a nonrepetitive t-cycle $D-Z$ form in which $d_{i+1} \mid d_i$, $i = 1, 2, \ldots, t-1$, and $d_t > 1$ with $t \le s$. Moreover, in such a representation, the values of t and of d_i are unique to the rule Q and are called the *rank* of Q and the *invariants* of Q, respectively. Such a form is termed a *canonical form*. The definitions in [SL89] rely heavily on group theory. In fact, the theory of lattice rules forms an excellent application of Kronecker's celebrated group representation theorem; see, for example, [S86, p. 45 *et seq.*]. However, the practical problem remains of actually calculating a canonical form of a general rule given in $D-Z$ form. This is the problem addressed in this paper.

In a previous paper [LJ96] we treated *prime-power* rules, that is, rules whose order, $\nu(Q)$, is a power of some prime. For these rules the invariants have a nonabstract definition that is closely related to the ideas underlying projection regularity (see [LJ96]). In that less complicated context, a theory was developed that does not rely on group theory or lattice theory at all. We state here a few key definitions and results from that paper.

DEFINITION 1.2. *Let a* prime-power *rule Q have invariants n_i and rank r. Then the form $Q = \mathcal{Q}[r,D,Z,s]$ is termed a* canonical form *of Q if $D = \operatorname{diag}\{n_1, n_2, \ldots, n_r\}$.*

DEFINITION 1.3. *The $t \times t$ integer diagonal matrix $D = \operatorname{diag}\{d_1, d_2, \ldots, d_t\}$ is termed* sequential *when*

$$d_1 \ge d_2 \ge \cdots \ge d_t > 1.$$

THEOREM 1.1. *A necessary and sufficient condition for a $D-Z$ form of a prime-power rule to be canonical is that it be nonrepetitive with sequential D.*

THEOREM 1.2. *A necessary and sufficient condition for a $D-Z$ form of a prime-power rule of order p^γ to be canonical is that D be sequential and the matrix Z be of full rank modulo p.*

For a prime-power rule in nonrepetitive form, it follows from Definition 1.1 that each d_i is a prime power. When D is sequential, this gives $d_{i+1} \mid d_i$, and so the invariants also have this property.

In this paper we exploit the previous work of [LJ96] on prime-power rules to provide a corresponding theory for general rules. Specifically, we use a matrix-based presentation of the Kronecker theorem mentioned above. This allows us to express the $D - Z$ form of a rule Q as a sum of the $D - Z$ forms of the "Sylow p-components" of the rule Q. These Sylow p-components are themselves lattice rules of prime-power order. Section 2 is devoted to this decomposition, Theorem 2.5 being the key result. This theorem is well known in the context of the decomposition of finite Abelian groups. What is new here is the specification of a $D - Z$ form for each Sylow p-component.

In Section 3 we *define* the rank and invariants of the general rule in terms of the rank and invariants of the component rules; we define a canonical form; and we show how it may be obtained from a general $D - Z$ form. These particular definitions are constructive. In Section 4, we complete the theory by providing in Theorem 4.5 a necessary and sufficient condition for a $D - Z$ form to be canonical.

2 The Sylow p-Component Rule Forms

In this section we introduce notation and algorithmic rules for handling $D - Z$ forms, and we use these to express a rule form as a sum of Sylow p-component rule forms. The transformations listed in the following theorem are well known and have been widely used in previous work such as [SL89] and [SJ94].

THEOREM 2.1. *The rule $Q = \mathcal{Q}[t, D, Z, s]$ given in (1.1) is unaltered if Z is modified by applying one of the following transformations or a sequence of them.*

(a) *Replace $\mathbf{z}_i$ by $\ell\mathbf{z}_i$ for ℓ an integer satisfying $\gcd(\ell, d_i) = 1$.*

(b) *Replace $\mathbf{z}_i$ by $\mathbf{z}_i + d_i\mathbf{x}$ for $\mathbf{x} \in \Lambda_0$.*

(c) *Replace $\mathbf{z}_i$ by $\mathbf{z}_i + (md_i/d_j)\mathbf{z}_j$ for $j \neq i$, m an integer, and $d_j \mid md_i$.*

Other transformations that allow one to change D and Z by consistent row interchange, removal of common factors, and removal of redundant rows are listed in [LJ96]. In this paper we do not use them explicitly. However, two more transformations are given in Theorem 2.3 below.

We now introduce the sum of lattice rules. This is a simple concept.

DEFINITION 2.1. The sum *of two s-dimensional integration lattices Λ_1 and Λ_2 is a lattice Λ that comprises all points and only points expressible in the form*

$$\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2,$$

where $\mathbf{x}_i \in \Lambda_i$, $i = 1, 2$.

Colloquially, Λ is the smallest lattice that contains both Λ_1 and Λ_2.

DEFINITION 2.2. *The* sum

$$Q = Q_1 + Q_2$$

of two s-dimensional lattice rules Q_1 and Q_2 is the rule Q obtained from the sum of the corresponding integration lattices for Q_1 and Q_2.

This definition extends to the sum of more than two lattice rules in an obvious way. It follows immediately that when

$$Q_1 f = \frac{1}{\nu(Q_1)} \sum_{j=1}^{\nu(Q_1)} f(\mathbf{x}_j) \text{ and } Q_2 f = \frac{1}{\nu(Q_2)} \sum_{k=1}^{\nu(Q_2)} f(\mathbf{y}_k), \tag{2.1}$$

their sum is

$$Qf = (Q_1 + Q_2)f = \frac{1}{\nu(Q_1)\nu(Q_2)} \sum_{k=1}^{\nu(Q_2)} \sum_{j=1}^{\nu(Q_1)} f(\{\mathbf{x}_j + \mathbf{y}_k\}), \tag{2.2}$$

and

$$\nu(Q_1 + Q_2) \leq \nu(Q_1)\nu(Q_2), \tag{2.3}$$

with equality being valid if $\nu(Q_1)$ and $\nu(Q_2)$ are relatively prime. In the situation where there is equality, the sum is a direct sum; the reader is referred to [JS94] or [SJ94, pp. 53–57] for further details about direct sums in this context.

LEMMA 2.2. *The sum of two rules having forms $\mathcal{Q}[t_1, D_1, Z_1, s]$ and $\mathcal{Q}[t_2, D_2, Z_2, s]$, respectively, may be expressed in the form $\mathcal{Q}[t_3, D_3, Z_3, s]$ with $t_3 = t_1 + t_2$, $D_3 = \operatorname{diag}\{D_1, D_2\}$, and*

$$Z_3 = \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix}.$$

PROOF. The result is readily proved by using (1.1), (2.1), and (2.2) with $Q_1 = \mathcal{Q}[t_1, D_1, Z_1, s]$ and $Q_2 = \mathcal{Q}[t_2, D_2, Z_2, s]$. □

It is a short step from dealing with the sum of two rules $Q_1 f$ and $Q_2 f$ to the "sum" of two forms $\mathcal{Q}[t_1, D_1, Z_1, s]$ and $\mathcal{Q}[t_2, D_2, Z_2, s]$ that represent them. One may re-express Lemma 2.2 using the following definition.

DEFINITION 2.3. *A relation*

$$\mathcal{Q}[t_3, D_3, Z_3, s] \equiv \mathcal{Q}[t_1, D_1, Z_1, s] + \mathcal{Q}[t_2, D_2, Z_2, s]$$

is valid if and only if the rules represented satisfy $Q_3 = (Q_1 + Q_2)$.

This paper relies heavily on this notation and definition. Each relation of this type could be verified by expanding each term in the form of (1.1), but this formalism makes such verification unnecessary.

We note that, while the sum of two rules is well defined, the sum of two forms is not. For example, in Lemma 2.2 one could equally well have set $D_3 = \operatorname{diag}\{D_2, D_1\}$ and

$$Z_3 = \begin{pmatrix} Z_2 \\ Z_1 \end{pmatrix}.$$

We now present a pair of transformations using this notation. These two transformations, which are discussed and illustrated in [L93], are reasonably straightforward to establish.

THEOREM 2.3. *When m and n are relatively prime,*

$$\mathcal{Q}[1, mn, \mathbf{z}, s] \equiv \mathcal{Q}[1, m, \mathbf{z}, s] + \mathcal{Q}[1, n, \mathbf{z}, s] \tag{2.4}$$

and

$$\mathcal{Q}[1, m, \mathbf{z}_1, s] + \mathcal{Q}[1, n, \mathbf{z}_2, s] \equiv \mathcal{Q}[1, mn, m\mathbf{z}_2 + n\mathbf{z}_1, s]. \tag{2.5}$$

This notation is convenient for manipulating rule forms. A trivial iterated application of Lemma 2.2 provides a decomposition of any t-cycle $D - Z$ form into the sum of 1-cycle $D - Z$ forms as follows:

$$\mathcal{Q}[t, D, Z, s] \equiv \mathcal{Q}[1, d_1, \mathbf{z}_1, s] + \mathcal{Q}[1, d_2, \mathbf{z}_2, s] + \cdots + \mathcal{Q}[1, d_t, \mathbf{z}_t, s], \tag{2.6}$$

where, as before, $\mathbf{z}_j$ denotes the jth row of Z. Further decomposition is possible when $\det D$ has more than one prime factor.

LEMMA 2.4. *Let* $\det D$ *have the prime factorization* $\det D = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_q^{\gamma_q}$, *and let d_i have the prime factor decomposition*

$$d_i = p_1^{\gamma_{1,i}} p_2^{\gamma_{2,i}} \cdots p_q^{\gamma_{q,i}}, \quad i = 1, 2, \ldots, t. \tag{2.7}$$

Then

$$\mathcal{Q}[1, d_i, \mathbf{z}_i, s] \equiv \mathcal{Q}[1, p_1^{\gamma_{1,i}}, \mathbf{z}_i, s] + \mathcal{Q}[1, p_2^{\gamma_{2,i}}, \mathbf{z}_i, s] + \cdots + \mathcal{Q}[1, p_q^{\gamma_{q,i}}, \mathbf{z}_i, s]. \tag{2.8}$$

PROOF. This follows by repeated application of (2.4) above. □

It is well known that when p is prime, $\mathcal{Q}[1, p^\gamma, \mathbf{z}, s]$ represents a *cyclic* rule. Surveys on cyclic rules may be found in [N78] and [N92]. The decompositions (2.6) and (2.8) are very well known in terms of the underlying group theory. The formulation given here will allow us to write down the actual cyclic rules involved in the decomposition, in terms of the parameters in D and Z. These results apply as written in cases in which $\gamma_{j,i} = 0$, giving $p_j^{\gamma_{j,i}} = 1$. The final forms may include forms $\mathcal{Q}[1, 1, \mathbf{z}_i, s]$, which may be included or discarded at will.

The conventional definition of the order of an element of an Abelian group under addition modulo 1 is also used in our context. Thus we have the following definition.

DEFINITION 2.4. *A point* $\mathbf{x}$ *is of order* n *when* $n\mathbf{x} \in \Lambda_0$ (*and n is the smallest positive integer for which this is true*).

We now introduce the Sylow p-component of a rule Q. This is defined as follows.

DEFINITION 2.5. *The Sylow p-component of a lattice rule Q is a lattice rule whose abscissa set comprises all points of the abscissa set of Q that are of order p^γ for any nonnegative integer γ.*

This corresponds precisely to the Sylow p-subgroup of a given group, the group elements being members of the respective abscissa sets. We note some simple standard properties.

(a) The trivial Sylow p-component with $p = 1$ is $\mathcal{Q}[1, 1, Z, s]$, which represents only the single point $\mathbf{0}$, the origin.

(b) When Q is a prime-power rule, it has only one nontrivial Sylow p-component, which coincides with Q.

(c) When $Q = \mathcal{Q}[t, D, Z, s]$, the only nontrivial Sylow p-components are those corresponding to any primes p that occur as a factor of $\det D$.

It follows that, using (2.6) and (2.8), we may set

$$\mathcal{Q}[t, D, Z, s] \equiv \sum_{i=1}^{t} \sum_{j=1}^{q} \mathcal{Q}[1, p_j^{\gamma_{j,i}}, \mathbf{z}_i, s] = \sum_{j=1}^{q} S^{(j)},$$

where we have *defined* a rule $S^{(j)}$ by one of its $D - Z$ forms, namely,

$$S^{(j)} := \sum_{i=1}^{t} \mathcal{Q}[1, p_j^{\gamma_{j,i}}, \mathbf{z}_i, s] \equiv \mathcal{Q}[t, D^{(j)}, Z, s],$$

with

$$D^{(j)} = \operatorname{diag}\{d_1^{(j)}, d_2^{(j)}, \ldots, d_t^{(j)}\} = \operatorname{diag}\{p_j^{\gamma_{j,1}}, p_j^{\gamma_{j,2}}, \ldots, p_j^{\gamma_{j,t}}\}. \tag{2.9}$$

Clearly $S^{(j)}$ contains only points that belong to Q, and it contains only points of order p_j^{γ} for various integers γ. No other Sylow p-component contains a point of order p_j^{γ} for any γ, except for the origin. Taken together, these facts establish the following theorem.

THEOREM 2.5. *Any rule Q may be expressed as the sum of all its Sylow p-components. There is a Sylow p_j-component $S^{(j)}$ for every p_j occurring in the prime factor decomposition of $\nu(Q)$. When $Q = \mathcal{Q}[t, D, Z, s]$, one form for $S^{(j)}$ is*

$$S^{(j)} = \mathcal{Q}[t, D^{(j)}, Z, s], \tag{2.10}$$

where $D^{(j)}$ is given in (2.9).

Note that in this $D - Z$ form of the Sylow p_j-component rule, the parameters t, Z, and s are the same as those in the $D - Z$ form for Q, and the elements of $D^{(j)}$ are obtained from those of D by retaining only the p_j component of each element.

EXAMPLE 2.1. Consider the $D - Z$ form $\mathcal{Q}[3, D, Z, 3]$ with

$$D = \begin{bmatrix} 2 \times 5 & 0 & 0 \\ 0 & 2 \times 3^4 \times 5^2 & 0 \\ 0 & 0 & 5 \end{bmatrix}, \quad Z = \begin{bmatrix} 11 & 6 & 1 \\ 1 & 4 & 8 \\ 2 & 5 & 9 \end{bmatrix}. \tag{2.11}$$

With $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$, it then follows that $D - Z$ forms for the Sylow p_j-components are given by $S^{(j)} = \mathcal{Q}[3, D^{(j)}, Z, 3]$, where

$$D^{(1)} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad D^{(2)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3^4 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad D^{(3)} = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5^2 & 0 \\ 0 & 0 & 5 \end{bmatrix}. \tag{2.12}$$

Note that each form has the same Z matrix, which is the one in the original $D - Z$ form. □

This last theorem is one of the key results in the theory of lattice rules. It is familiar in a group theory context and, in that context, may be established more quickly and more elegantly than the derivation given above. But here we have obtained a simple calculable $D - Z$ representation of each Sylow p-component without demanding that Q be given in canonical form (see the next section) or even in nonrepetitive form. It is immediately available given any $D - Z$ representation of Q. That is, it provides a constructive example of the Kronecker decomposition theorem.

In view of (2.3), we have

$$\nu(Q) = \prod_{j=1}^{q} \nu(S^{(j)}); \tag{2.13}$$

and, following the notation of (2.7) and (2.9), we have

$$\det D = \prod_{j=1}^{q} \det D^{(j)}. \tag{2.14}$$

This leads to the following theorem.

THEOREM 2.6. *In the notation of the previous theorem, the form* $\mathcal{Q}[t, D, Z, s]$ *is nonrepetitive if and only if every component form* $\mathcal{Q}[t, D^{(j)}, Z, s]$ *is nonrepetitive.*

PROOF. We exploit (2.13) and (2.14) above. First we note that, whether or not any of these forms are repetitive, we have

$$\nu(S^{(j)}) \leq \det D^{(j)} \text{ for all } j, \tag{2.15}$$

so it follows that

$$\nu(Q) = \prod_{j=1}^{q} \nu(S^{(j)}) \leq \prod_{j=1}^{q} \det D^{(j)} = \det D. \tag{2.16}$$

When all the forms for $S^{(j)}$ are nonrepetitive, the relation in (2.15) is an equality. This produces an equality in (2.16), which shows that the form for Q is also nonrepetitive. Conversely, if one of the forms for $S^{(j)}$ is repetitive, there is one value of j for which the relation in (2.15) is a strict inequality; this makes the relation in (2.16) a strict inequality, showing that the form for Q is also repetitive. □

3 Canonical Form of a General Lattice Rule

In [LJ96], the *rank* and *invariants* for prime-power rules are defined in a nonabstract manner. Some of their properties are recalled in the introduction. In this section we exploit these definitions to define the same quantities in the context of a general lattice rule. The link that enables the broadening of the definition is Theorem 2.5, which asserts that any rule may be decomposed into a sum

$$Q = S^{(1)} + S^{(2)} + \cdots + S^{(q)} \tag{3.1}$$

of its Sylow p_j-components $S^{(j)}$, $j = 1, 2, \ldots, q$. Each component is a prime-power rule, and its rank and invariants satisfy the sequential and divisibility conditions mentioned in Theorem 1.1 and the discussion preceding it. Let $S^{(j)}$ have rank and invariants

$$r^{(j)}; \quad n_1^{(j)}, n_2^{(j)}, \ldots, n_s^{(j)}. \tag{3.2}$$

Here it is convenient to include the trivial invariants, that is,

$$n_i^{(j)} = 1, \quad i = r^{(j)} + 1, \ldots, s. \tag{3.3}$$

DEFINITION 3.1. *The* rank *and* invariants *of a general lattice rule Q are*

$$r = \max(r^{(1)}, r^{(2)}, \ldots, r^{(q)}) \text{ and } n_i = n_i^{(1)} n_i^{(2)} \cdots n_i^{(q)}, \quad i = 1, 2, \ldots, r, \tag{3.4}$$

where $r^{(j)}$ and $n_i^{(j)}$ are respectively the rank and invariants of the Sylow p_j-components of Q as specified in (3.1), (3.2), *and* (3.3) *above.*

This definition comprises a nonabstract realization of a standard definition based on group theory.

DEFINITION 3.2. *Let Q have invariants n_i and rank r. Then any form $Q = \mathcal{Q}[r', D, Z, s]$ is termed a* canonical form *of Q if $D = \mathrm{diag}\{n_1, n_2, \ldots, n_{r'}\}$, so long as $r' \in [r, s]$.*

(When $r' > r$, this is known as a padded version because1 each of the final $r' - r$ elements of D is 1 and the final $r' - r$ rows of Z are arbitrary.)

Thus, by definition, we see that, as in the case of the simpler prime-power rule, a canonical $D - Z$ form is one in which the elements of D are the actual invariants of the rule.

THEOREM 3.1. *A canonical form $\mathcal{Q}[r, D, Z, s]$ has the following properties:*

(a) $n_{i+1} \mid n_i$, $i = 1, 2, \ldots, r - 1$;

(b) $\mathcal{Q}[r, D, Z, s]$ *is nonrepetitive.*

PROOF. The first property is inherited from the corresponding property for each of the Sylow p-components through (3.4). The second property may be established as follows. If $\mathcal{Q}[r, D, Z, s]$ were repetitive, the transformations of Theorem 2.1 could be used to reduce it to a nonrepetitive form $\mathcal{Q}[r', D', Z', s]$ with $\det D' < \det D$. For a nonrepetitive form, $\nu(Q) = \det D'$; but for a canonical form, $\det D = \nu(Q)$. Since $\det D' \neq \det D$, it follows that a canonical form cannot be repetitive. □

COROLLARY 3.2. *In a canonical form, $\mathbf{z}_i / n_i$ is semiproper, that is,* $\gcd(Z_{i1}, \ldots, Z_{is}, n_i) = 1$.

PROOF. Suppose $\mathbf{z}_i/n_i$ were not semiproper, so that $\gcd(Z_{i1},\ldots,Z_{is},n_i)=\lambda$ for some $\lambda>1$. Then we could replace $\mathbf{z}_i$ by $\mathbf{z}_i'=\mathbf{z}_i/\lambda$ and n_i by $n_i'=n_i/\lambda$, and so the form would be repetitive, which contradicts Theorem 3.1. $\square$

Clearly the rank and invariants of any rule Q exist and are unique, since the expansion (3.1) is unique, each component has unique invariants, and these are assembled in a determinate way in (3.4). It is straightforward to show that every rule Q has a canonical form. This follows from the existence of concrete realizations of each step in the definitions.

THEOREM 3.3. *When $Q=\mathcal{Q}[r,D,Z,s]$ is a canonical form of Q, then $\mathcal{Q}[r,D^{(j)},Z,s]$ is a canonical form of $S^{(j)}$, its Sylow p_j-component.*

The proof of this result is straightforward and is omitted.

We now describe in detail how a canonical form of a general rule Q may be constructed from any $D-Z$ form. When $Q=\mathcal{Q}[t,D,Z,s]$, we first invoke Theorem 2.5, which asserts that each Sylow p_j-component is $S^{(j)}=\mathcal{Q}[t,D^{(j)},Z,s]$, where, as usual, $D^{(j)}$ comprises the p_j-components of D.

If each $D^{(j)}$ is sequential and each $D-Z$ form is nonrepetitive, the original $D-Z$ form is already canonical. Otherwise, it is necessary to form a new representation for $S^{(j)}$ that is sequential and nonrepetitive. This can be accomplished by using the transformations of Theorem 2.1 and the others mentioned just after that theorem. In [LJ96] a procedure for doing this is given as part of the proof of Theorem 3.7.

EXAMPLE 3.1. Here we obtain sequential nonrepetitive representations for the Sylow p_j-components of the rule given by the $D-Z$ form in Example 2.1. There the $D-Z$ forms for the three Sylow p_j-components given in (2.12) are not sequential, and all involved the same matrix Z given in (2.11). We now individually treat the $D-Z$ form for each Sylow p_j-component. We make each sequential by reordering rows and removing rows for which the corresponding diagonal element of D is 1. This gives immediately $D-Z$ forms for the three Sylow p_j-components given by $S^{(j)}=\mathcal{Q}[t^{(j)},D^{(j)},\tilde{Z}^{(j)},3]$, where

$$t^{(1)}=2,\quad D^{(1)}=\begin{bmatrix}2&0\\0&2\end{bmatrix},\qquad \tilde{Z}^{(1)}=\begin{bmatrix}11&6&1\\1&4&8\end{bmatrix},$$
$$t^{(2)}=1,\quad D^{(2)}=\begin{bmatrix}3^4\end{bmatrix},\qquad \tilde{Z}^{(2)}=\begin{bmatrix}1&4&8\end{bmatrix},$$
$$t^{(3)}=3,\quad D^{(3)}=\begin{bmatrix}5^2&0&0\\0&5&0\\0&0&5\end{bmatrix},\quad \tilde{Z}^{(3)}=\begin{bmatrix}1&4&8\\11&6&1\\2&5&9\end{bmatrix}.$$

Finally (and optionally), we may use Theorem 2.1(b) to reduce the size of the elements in the $\tilde{Z}^{(j)}$-matrices. We then obtain $D-Z$ forms for the three Sylow p_j-components given by $S^{(j)}=\mathcal{Q}[t^{(j)},D^{(j)},Z^{(j)},3]$, where

$$Z^{(1)}=\begin{bmatrix}1&0&1\\1&0&0\end{bmatrix},\quad Z^{(2)}=\begin{bmatrix}1&4&8\end{bmatrix},\quad Z^{(3)}=\begin{bmatrix}1&4&8\\1&1&1\\2&0&4\end{bmatrix}.$$

It is not difficult to see that $Z^{(1)}$ is of full rank modulo 2 and that $Z^{(2)}$ is of full rank modulo 3. It then follows from Theorems 1.1 and 1.2 that the representations for $S^{(1)}$ and $S^{(2)}$ are nonrepetitive.

$Z^{(3)}$ is not of full rank modulo 5. This could be ascertained by calculating $\det Z^{(3)}$, but it is immediately apparent that the last row of $Z^{(3)}$, $\mathbf{z}_3^{(3)}$, is equal to the sum of the first two rows modulo 5. Hence the representation for $S^{(3)}$ is repetitive. Using Theorem 2.1(c), we may replace $\mathbf{z}_3^{(3)}$ by $\mathbf{z}_3^{(3)} - \mathbf{z}_2^{(3)} = [1, -1, 3]$. In turn, this may be replaced by $\mathbf{z}_3^{(3)} - \mathbf{z}_1^{(3)} = [0, -5, -5]$, which is equal modulo 5 to $[0, 0, 0]$. Discarding this zero vector, we obtain the sequential nonrepetitive form for $S^{(3)}$ given by $\mathcal{Q}[2, D^{(3)}, Z^{(3)}, 3]$, where

$$D^{(3)} = \begin{bmatrix} 5^2 & 0 \\ 0 & 5 \end{bmatrix}, \quad Z^{(3)} = \begin{bmatrix} 1 & 4 & 8 \\ 1 & 1 & 1 \end{bmatrix}. \quad \square$$

When all the Sylow p_j-components are in sequential nonrepetitive form, we assemble them, row by row. It is convenient in this description to provide, for each Sylow p_j-component, an s-cycle $D - Z$ form. One way of doing this is to append an appropriate number of zero vectors to the Z-matrix and a corresponding identity matrix to D.

The Sylow p_j-components, now in the form $\mathcal{Q}[s, \bar{D}^{(j)}, \bar{Z}^{(j)}, s]$, may be re-expressed as

$$\sum_{i=1}^{s} \mathcal{Q}[1, \bar{d}_i^{(j)}, \bar{\mathbf{z}}_i^{(j)}, s].$$

Since the ordering is immaterial, we may express Q in the form

$$\sum_{i=1}^{s} \left(\sum_{j=1}^{q} \mathcal{Q}[1, \bar{d}_i^{(j)}, \bar{\mathbf{z}}_i^{(j)}, s] \right).$$

The inner sum may be assembled to give $\mathcal{Q}[1, \bar{d}_i, \bar{\mathbf{z}}_i, s]$, where $\bar{d}_i = \prod_{j=1}^{q} \bar{d}_i^{(j)}$. This assembly process may be carried out by making repeated use of the relation (2.5). We then obtain the rule form for Q given by $\mathcal{Q}[s, \bar{D}, \bar{Z}, s]$, where $\bar{D} = \operatorname{diag}\{\bar{d}_i\}$ and

$$\bar{Z} = \begin{bmatrix} \bar{\mathbf{z}}_1 \\ \bar{\mathbf{z}}_2 \\ \vdots \\ \bar{\mathbf{z}}_s \end{bmatrix}.$$

Reference to Definition 3.2 confirms that this is a canonical form, with $r' = s$. The rank, r, of the rule Q is given by the largest integer i for which $\bar{d}_i > 1$. Hence, the form obtained by removing the last $s - r$ rows of $\bar{Z}$ and making a similar curtailment to $\bar{D}$ is also canonical.

EXAMPLE 3.2. We continue the previous example by assembling the three Sylow p_j-components to obtain a canonical form. Since all forms are now rank 2 or less, we may use two cycle forms, namely, $S^{(j)} = \mathcal{Q}[2, \bar{D}^{(j)}, \bar{Z}^{(j)}, 3]$, where

$$\bar{D}^{(1)} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad \bar{Z}^{(1)} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

$$\bar{D}^{(2)} = \begin{bmatrix} 3^4 & 0 \\ 0 & 1 \end{bmatrix}, \quad \bar{Z}^{(2)} = \begin{bmatrix} 1 & 4 & 8 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\bar{D}^{(3)} = \begin{bmatrix} 5^2 & 0 \\ 0 & 5 \end{bmatrix}, \quad \bar{Z}^{(3)} = \begin{bmatrix} 1 & 4 & 8 \\ 1 & 1 & 1 \end{bmatrix}.$$

We now reconstruct the original rule Q from these three forms of the Sylow p_j-components. We have $\bar{d}_1 = 2 \times 3^4 \times 5^2 = 4050$ and $\bar{d}_2 = 2 \times 5 = 10$. Moreover, by using (2.5) twice, we obtain

$$\bar{\mathbf{z}}_1 = 2 \times \left(5^2 \times [1,4,8] + 3^4 \times [1,4,8]\right) + 3^4 \times 5^2 \times [1,0,1] = [2237, 848, 3721]$$

and

$$\bar{\mathbf{z}}_2 = 2 \times (5 \times [0,0,0] + [1,1,1]) + 5 \times [1,0,0] = [7,2,2].$$

Thus a canonical $D - Z$ form for the rule is given by $\mathcal{Q}[2, \bar{D}, \bar{Z}, 3]$, where

$$\bar{D} = \begin{bmatrix} 4050 & 0 \\ 0 & 10 \end{bmatrix}, \quad \bar{Z} = \begin{bmatrix} 2237 & 848 & 3721 \\ 7 & 2 & 2 \end{bmatrix}. \quad \Box$$

4 Recognizing a Canonical Form

Although we can always obtain a canonical form for a lattice rule, it is sometimes difficult to *recognize* whether a *given* form $\mathcal{Q}[t, D, Z, s]$ is a canonical form. Of course, a canonical form has some obvious properties. These appear in the following definition.

DEFINITION 4.1. *The form $\mathcal{Q}[t, D, Z, s]$ is termed a* candidate form *if $t \le s$, each $\mathbf{z}_i/d_i$ is semiproper, and*

$$d_{i+1} \mid d_i, \quad i = 1, 2, \ldots, t-1.$$

Trivially, a form that is not a candidate form cannot be a canonical form.

THEOREM 4.1. *If $Q = \mathcal{Q}[t, D, Z, s]$ is a candidate form, then $\mathcal{Q}[t, D^{(j)}, Z, s]$ is a candidate form of $S^{(j)}$, its Sylow p_j-component.*

PROOF. The divisibility property follows from that of Q. Since $\mathbf{z}_i/d_i$ is semiproper and $d_i^{(j)}$ is a factor of d_i, $\mathbf{z}_i/d_i^{(j)}$ is also semiproper. $\Box$

In Theorem 3.1 and Corollary 3.2 we established that a canonical form satisfies the conditions to be a candidate form and is, in addition, nonrepetitive. The following theorem establishes the converse of this statement.

THEOREM 4.2. *A nonrepetitive candidate form is canonical.*

PROOF. When $\mathcal{Q}[t, D, Z, s]$ is nonrepetitive, $\mathcal{Q}[t, D^{(j)}, Z, s]$, the form for the Sylow p_j-component of Q, is also nonrepetitive (Theorem 2.6). When

$\mathcal{Q}[t, D, Z, s]$ is a candidate form, the previous theorem shows that $\mathcal{Q}[t, D^{(j)}, Z, s]$ is also. Thus, the elements $d_i^{(j)}$ of $D^{(j)}$ satisfy $d_{i+1}^{(j)} \mid d_i^{(j)}$, and since $S^{(j)}$ is a prime-power rule, the element $d_i^{(j)}$ is the ith invariant of $S^{(j)}$. By definition, the ith invariant of Q is

$$n_i = \prod_{j=1}^{q} d_i^{(j)}.$$

This coincides with d_i, the ith element of D. Thus D contains the invariants of Q, and this is the sole condition for $\mathcal{Q}[t, D, Z, s]$ to be a canonical form of Q. □

In some of the theory one comes across representations $Q[s, D, Z, s]$ in which Z is unimodular. A unimodular matrix is one whose determinant is ± 1. Any $D-Z$ form in which Z is unimodular is nonrepetitive (see [LK95, Theorem 2.2]). Thus, in particular, we have the following.

Corollary 4.3. *A candidate form $Q[s, D, Z, s]$ in which Z is unimodular is a canonical form.*

A mild generalization of this corollary is as follows.

Theorem 4.4. *A candidate form $Q[t, D, Z, s]$ in which Z contains a $t \times t$ unimodular submatrix is a canonical form.*

Proof. Suppose Z contains a $t \times t$ submatrix that is unimodular. Then from this form, we can construct a candidate form $\mathcal{Q}[s, D', Z', s]$ in which D' has a further $s-t$ diagonal elements, each of which is 1, and Z' has an extra $s-t$ rows, each of the form $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ with a unit occurring in each of the $s-t$ columns not included in the unimodular submatrix of Z. Since $\det Z' = 1$, we have Z' unimodular, and so the form $\mathcal{Q}[s, D', Z', s]$ is canonical.

Recalling Definition 3.2, we see that since $Q[s, D', Z', s]$ is canonical, the invariants of Q are the diagonal elements of D' and the rank is the number of nontrivial invariants. However, the representation $Q[t, D, Z, s]$ has a matrix D containing all of these nontrivial invariants and represents Q. Applying Definition 3.2 directly establishes the result. □

One simple special case of this theorem is the situation in which Z is *column-permuted unit upper triangular* (cpuut), that is, where there exists an $s \times s$ permutation matrix P such that ZP is unit upper triangular. This form is discussed in great detail in [LJ96], where it is used as the basis for a classification of prime-power rules. This last theorem shows that a candidate form in which Z is cpuut is a canonical form.

We now seek a criterion by which one may recognize whether a candidate form is in fact a canonical form. Like any other rule form, the candidate form represents a rule Q, which has Sylow p_j-components as detailed in Section 2. However, the $D-Z$ representation $S^{(j)} = \mathcal{Q}[t, D^{(j)}, Z, s]$ inherits from D the property that $d_{i+1}^{(j)} \mid d_i^{(j)}$. Hence there exists a parameter $t^{(j)}$ such that the elements $d_i^{(j)}$ are 1 for $i > t^{(j)}$; and the form may be reduced to

$$S^{(j)} = \mathcal{Q}[t^{(j)}, \bar{D}^{(j)}, \bar{Z}^{(j)}, s], \tag{4.1}$$

where $\bar{Z}^{(j)}$ is a $t^{(j)} \times s$ submatrix of Z obtained by removing the final $t - t^{(j)}$ rows and $\bar{D}^{(j)}$ is a similarly curtailed version of $D^{(j)}$. According to Theorem 1.2, a necessary and sufficient condition for this form to be nonrepetitive is that $\bar{Z}^{(j)}$ be of full rank modulo p_j. And according to Theorem 2.6, the necessary and sufficient condition for $\mathcal{Q}[t, D, Z, s]$ to be nonrepetitive is that all the above forms for $S^{(j)}$, $j = 1, 2, \ldots, q$, are nonrepetitive. This leads to the following theorem.

THEOREM 4.5. *Let $\mathcal{Q}[t, D, Z, s]$ be a candidate form, and let the prime factor decomposition of* $\det D$ *require precisely q distinct primes $p_1, p_2, \ldots, p_q$. Let $t^{(j)}$ be the largest index i for which d_i contains a factor p_j. Then a necessary and sufficient condition for $\mathcal{Q}[t, D, Z, s]$ to be a* canonical form *of Q is that for $j = 1, 2, \ldots, q$ the first $t^{(j)}$ rows of Z form a matrix of full rank modulo p_j.*

EXAMPLE 4.1. Consider the candidate $D - Z$ form $\mathcal{Q}[3, D, Z, 3]$ with

$$D = \begin{bmatrix} 2 \times 3^4 \times 5^2 & 0 & 0 \\ 0 & 2 \times 5 & 0 \\ 0 & 0 & 5 \end{bmatrix}, \quad Z = \begin{bmatrix} 7 & 4 & 8 \\ 11 & 16 & 1 \\ 4 & 8 & 11 \end{bmatrix}. \tag{4.2}$$

Let us set $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$. Then $t^{(1)} = 2, t^{(2)} = 1$, and $t^{(3)} = 3$; and

$$\begin{aligned} D^{(1)} &= \mathrm{diag}\{2, 2, 1\}, & \bar{D}^{(1)} &= \mathrm{diag}\{2, 2\}, \\ D^{(2)} &= \mathrm{diag}\{3^4, 1, 1\}, & \bar{D}^{(2)} &= \mathrm{diag}\{3^4\}, \\ D^{(3)} &= \mathrm{diag}\{5^2, 5, 5\}, & \bar{D}^{(3)} &= \mathrm{diag}\{5^2, 5, 5\}, \\ \bar{Z}^{(1)} &= \begin{bmatrix} 7 & 4 & 8 \\ 11 & 16 & 1 \end{bmatrix}, & \bar{Z}^{(1)} \pmod 2 &= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \\ \bar{Z}^{(2)} &= \begin{bmatrix} 7 & 4 & 8 \end{bmatrix}, & \bar{Z}^{(2)} \pmod 3 &= \begin{bmatrix} 1 & 1 & 2 \end{bmatrix}, \\ \bar{Z}^{(3)} &= \begin{bmatrix} 7 & 4 & 8 \\ 11 & 16 & 1 \\ 4 & 8 & 11 \end{bmatrix}, & \bar{Z}^{(3)} \pmod 5 &= \begin{bmatrix} 2 & 4 & 3 \\ 1 & 1 & 1 \\ 4 & 3 & 1 \end{bmatrix}. \end{aligned}$$

It is immediately clear that $\bar{Z}^{(1)} \pmod 2$ and $\bar{Z}^{(2)} \pmod 3$ are of full rank. One may verify that $\det \bar{Z}^{(3)} = 900 \equiv 0 \pmod 5$. The theorem then asserts that the $D - Z$ form is not a canonical form. A canonical form of this rule is given in Section 5. (The reader may verify that the $D - Z$ form is canonical if the first row of Z is replaced by $[\ 7 \quad 5 \quad 8\ ]$.) □

The next result is related to Theorem 3.2 of [L93].

THEOREM 4.6. *Suppose we have the two candidate forms*

$$Q = \mathcal{Q}[t, D, Z, s] \text{ and } Q' = \mathcal{Q}[t, D', Z, s]$$

such that the elements of D satisfy

$$d_i = p_1^{\gamma_{1,i}} p_2^{\gamma_{2,i}} \cdots p_q^{\gamma_{q,i}}.$$

If the elements of D' satisfy

$$d'_i = p_1^{\lambda_{1,i}} p_2^{\lambda_{2,i}} \cdots p_q^{\lambda_{q,i}},$$

where

$$\lambda_{j,i} = \begin{cases} 1, & \textit{when } \gamma_{j,i} \geq 1, \\ 0, & \textit{when } \gamma_{j,i} = 0, \end{cases}$$

then either both candidate forms are canonical or neither is canonical.

PROOF. In the notation of (4.1), we see from Theorem 4.5 that the requirement is that certain submatrices of Z, namely, $\bar{Z}^{(j)}$, $j = 1, 2 \ldots, q$, be respectively of full rank modulo p_j. The matrix $\bar{Z}^{(j)}$ depends only on the value of $t^{(j)}$, which in turn depends only on which d_i have a p_j factor and not what the p_j factor is. □

Thus, in the example given above, the results about the form being canonical or not are unchanged when D is altered to any matrix of the form $\mathrm{diag}\{2^{\alpha_1}3^{\beta_1}5^{\gamma_1},\ 2^{\alpha_2}5^{\gamma_2},\ 5^{\gamma_3}\}$ with $\alpha_1 \geq \alpha_2 > 0$, $\beta_1 > 0$, $\gamma_1 \geq \gamma_2 \geq \gamma_3 > 0$, but Z remains as before.

5 Miscellaneous Results

This section contains a few special results that are relevant when s or t is small. Since they are the basis of no further theory, the proofs, which are not deep, are omitted. They may help in special cases to obtain a result without using the general approach. They are all concerned with cases in which a form is altered or reduced without altering the Z-matrix.

THEOREM 5.1. *Given a candidate form $\mathcal{Q}[t, D, Z, s]$, the first invariant of the rule Q is $n_1 = d_1$.*

COROLLARY 5.2. *When $t = 1$, a candidate form is a canonical form.*

LEMMA 5.3. *Let $\mathcal{Q}[2, D, Z, s]$ be a candidate form with $d_2 = \prod_{j=1}^{q} p_j^{\gamma_{j,2}}$. Its canonical form is $\mathcal{Q}[2, \tilde{D}, Z, s]$, where $\tilde{d}_1 = d_1$, $\tilde{d}_2 = \prod_{j=1}^{q} p_j^{\gamma_{j,2}(r_j-1)}$ with $r_j =$* rank $Z \pmod{p_j}$.

This lemma is an almost trivial consequence of Theorem 4.5. The factor $(r_j - 1)$ is simply a device to remove, from the product, terms for which $r_j = 1$.

THEOREM 5.4. *Let a prime-power rule S of order p^γ have a repetitive $D - Z$ form given by $\mathcal{Q}[t, D, Z, s]$. Let Z be of rank $\tilde{t}$ modulo p, where $\tilde{t} < t$. Let the $\tilde{t} \times s$ matrix $\tilde{Z}$ obtained from Z by removing the final $t - \tilde{t}$ rows also be of rank $\tilde{t}$ modulo p. Then*

$$S = \mathcal{Q}[t, \tilde{D}, Z, s],$$

where $\tilde{D} = \mathrm{diag}\{d_1, d_2, \ldots, d_{\tilde{t}}, 1, \ldots, 1\}$, is a canonical form.

This last result can be useful in cases where, in a $D - Z$ form of a Sylow p-component, one prefers not to alter Z. Such a situation occurs in the example in the preceding section. There $\det \bar{Z}^{(3)} \equiv 0 \pmod 5$, but the first two rows are linearly independent. Because, in the example, all three Sylow p_j-components can be expressed by using the same matrix Z, the final canonical form can be expressed in $D - Z$ form in (4.2) by retaining this matrix Z but changing d_3 from 5 to 1. Then the redundant third row can be removed, leaving a canonical

$D - Z$ form with

$$D = \begin{bmatrix} 2 \times 3^4 \times 5^2 & 0 \\ 0 & 2 \times 5 \end{bmatrix}, \quad Z = \begin{bmatrix} 7 & 4 & 8 \\ 11 & 16 & 1 \end{bmatrix}.$$

Acknowledgments

The first author was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Computational and Technology Research, U.S. Department of Energy, under Contract W-31-109-Eng-38. It is a pleasure to acknowledge the support of the School of Mathematics of the University of New South Wales, where some of this work was conceived, and to thank Dr I. H. Sloan for several illuminating conversations.

REFERENCES

[JS94] S. Joe and I. H. Sloan, *The direct sum of lattice rules*, Department of Mathematics and Statistics Research Report No. 30, 1994, The University of Waikato, Hamilton.

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

[LJ96] J. N. Lyness and S. Joe, *Triangular canonical forms for lattice rules of prime-power order*, Math. Comp. **65** (1996), pp. 165–178.

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

[N78] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), pp. 957–1041.

[N92] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, 1992.

[S86] A. Schrijver, *Theory of linear and integer programming*, Wiley, New York, 1986.

[SJ94] I. H. Sloan and S. Joe, *Lattice methods for multiple integration*, Clarendon Press, Oxford, 1994.

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