The Hermite normal form for certain rank-1 circulant and skew-circulant lattice rules

Stephen Joe

Department of Mathematics, University of Waikato, Private Bag 3105, Hamilton 3240, New Zealand

Abstract

Characterisations are provided of the Hermite normal form of certain integer circulant and skew-circulant matrices. These matrices are associated with rank-1 circulant and skew-circulant lattice rules. Previous computer searches for lattice rules of specified trigonometric degree have indicated that there is some merit in searches of such lattice rules.

We also consider the question of whether a Hermite normal form with the characterisation for these rank-1 circulant lattice rules is actually associated to a circulant lattice rule. Though the answer is negative in the general case, several examples where the answer is positive will be given.

Keywords: Rank-1 circulant lattice rules, Hermite normal form.
2000 MSC: 15B36, 15B05, 65D30

1. Introduction

Here we provide characterisations of the Hermite normal form of certain integer circulant and skew-circulant matrices. We recall:

Definition 1. An $s \times s$ integer matrix H is in *Hermite normal form* (HNF) when H is upper triangular and

$$0 \le h_{ij} < h_{jj} \text{ for } 1 \le i < j \le s.$$

For a given integer matrix B with $|\det(B)| = n$, there is a unique H in HNF such that

$$H = UB \quad \text{with} \quad \det(H) = n,$$

where U is some unimodular matrix (an integer matrix with determinant ± 1). We shall call H the *HNF associated to* B. Information about the HNF may be found in [9], but note that the results there assume a lower triangular HNF obtained by elementary column operations whereas here we assume an upper triangular HNF obtained by elementary row operations. The results there may be easily translated to the situation here.

The integer circulant and skew-circulant matrices of interest here are those associated with rank-1 circulant and skew-circulant lattice rules. Lattice rules are used to approximate the s-dimensional integral

$$\int_{[0,1]^s} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}$$

and make use of n points in $[0,1)^s$ that belong to some *integration lattice*.

Definition 2. An s-dimensional *lattice* is an infinite set of points in $\mathbb{R}^s$ that is closed under addition and subtraction and has no limit points. An *integration lattice* Λ is a lattice that contains $\mathbb{Z}^s$ as a sublattice.

Corresponding to any lattice is a generator matrix.

Definition 3. An $s \times s$ matrix A is termed a *generator matrix* of the s-dimensional lattice Λ when Λ comprises precisely all points of the form

$$\boldsymbol{x} = \sum_{i=1}^{s} \lambda_i \boldsymbol{a}_i = \boldsymbol{\lambda} A,$$

where $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_s) \in \mathbb{Z}^s$ and $\boldsymbol{a}_i$ is the i-th row of A.

Note that in this paper, all points and vectors are written row-wise, so that, for example, $\boldsymbol{x} = (x_1, x_2, \ldots, x_{s-1}, x_s)$. More general information about lattice rules may be found in [7] and [10]. Generator matrices for integration lattices are considered in detail in [4].

Related to A is $B = (A^T)^{-1}$. The matrix B is a generator matrix for the *dual lattice* $\Lambda^\perp$. This dual lattice is conventionally defined by

$$\boldsymbol{p} \in \Lambda^\perp \Leftrightarrow \boldsymbol{p} \cdot \boldsymbol{x} \in \mathbb{Z}\ \forall \boldsymbol{x} \in \Lambda,$$

where $\cdot$ denotes the dot product. If A generates an integration lattice Λ, then all elements of B are integers and $|\det(B)| = n$, where n is the number of points belonging to $[0,1)^s \cap \Lambda$.

For choosing a 'good' lattice rule, some criterion needs to be chosen. Some criteria, such as high trigonometric degree, result in computer searches using B. Computer searches by Cools and Govaert [1], Cools and Lyness [2], and Lyness and Sørevik [5] based on high trigonometric degree showed there was merit in lattice rules for which the associated matrices B were integer circulant or skew-circulant matrices. We refer to these lattice rules as circulant or skew-circulant lattice rules.

For a circulant lattice rule, the associated B is of the form:

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{s-2} & b_{s-1} \\ b_{s-1} & b_0 & b_1 & \cdots & b_{s-3} & b_{s-2} \\ b_{s-2} & b_{s-1} & b_0 & \cdots & b_{s-4} & b_{s-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_2 & b_3 & b_4 & \cdots & b_0 & b_1 \\ b_1 & b_2 & b_3 & \cdots & b_{s-1} & b_0 \end{bmatrix}, \tag{1}$$

where the $b_0, \ldots, b_{s-1} \in \mathbb{Z}$. Skew-circulant matrices differ from circulant matrices by a change of sign of the elements below the main diagonal. For a skew-circulant lattice rule, B is of the form:

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{s-2} & b_{s-1} \\ -b_{s-1} & b_0 & b_1 & \cdots & b_{s-3} & b_{s-2} \\ -b_{s-2} & -b_{s-1} & b_0 & \cdots & b_{s-4} & b_{s-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -b_2 & -b_3 & -b_4 & \cdots & b_0 & b_1 \\ -b_1 & -b_2 & -b_3 & \cdots & -b_{s-1} & b_0 \end{bmatrix}.$$

For a given n, one may wish to do a computer search through the circulant (or skew-circulant) matrices B with $|\det(B)| = n$ to find good matrices B. The problem is that for a given lattice, there are many choices for B, even if restricted to integer circulant matrices. If U is an $s \times s$ unimodular matrix, then UB generates the same lattice as B. The matrix UB results from performing elementary row operations on B.

For an efficient computer search, it would be useful to have information about which HNFs are associated with circulant or skew-circulant lattice rules, so that we can just search through these lattice rules. This has led to the results in this paper which provide characterisations of the HNF associated to integer circulant and skew-circulant matrices when the HNF is of the form given below in (2). However, the results obtained are not entirely satisfactory. The comments in the next paragraph and the contents of the final section mean that a computer search among HNFs with such a characterisation may include lattice rules which are not circulant and may omit some circulant lattice rules.

Here we restrict ourselves to HNFs which are of the form

$$H = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & h_1 \\ 0 & 1 & 0 & \cdots & 0 & h_2 \\ 0 & 0 & 1 & \cdots & 0 & h_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & h_{s-1} \\ 0 & 0 & 0 & \cdots & 0 & n \end{bmatrix}, \tag{2}$$

where $0 \le h_k < n$, $1 \le k \le s-1$, and $n = |\det(B)|$ is the number of points in the associated lattice rule. Currently, it is not known which circulant and skew-circulant lattice rules have an associated HNF of the form given in (2), though a simple necessary condition for such a circulant or skew-circulant lattice rule is that $\gcd(b_0, b_1, \ldots, b_{s-2}, b_{s-1}) = 1$. Moreover, lattice rules associated to such an HNF have to be what are known as rank-1 lattice rules. When n is square-free, all lattice rules with n points are rank 1 (see Section 9.2 of [10]). Lattice rules of higher rank do not have a HNF of the form (2). We remark that though the interest here is in numerical integration, lattices are of relevance in lattice-based cryptography (for example, see [8] and [12]). In these two references, a HNF of the form (2) is called an 'optimal' HNF.

In the next section, we provide relationships between the $h_1, \ldots, h_{s-1}$ in (2) when H is a Hermite normal form associated with a B for rank-1 circulant and skew-circulant lattice rules. In the final section, we look at the question of whether a Hermite normal form satisfying these relationships (as given in Theorem 1 in the next section) is actually associated to a rank-1 circulant lattice rule. Though the answer is a negative one in the general case, the final section considers several examples where the answer is positive.

2. Main results

The first result we consider is the one for circulant lattice rules.

Theorem 1. *Let H be of the form (2) and suppose it is the HNF associated to a rank-1 circulant lattice rule having n points. Then the elements in the last column of H satisfy the following:*

$$h_1^s \equiv (-1)^s \pmod{n} \tag{3}$$

and

$$h_k \equiv (-1)^{k-1} h_1^k \pmod{n}, \quad 2 \le k \le s-1. \tag{4}$$

Remark 1. Since $0 \le h_k < n$, $1 \le k \le s-1$, then fixing $h_1 \in [1, n-1]$ fixes all the other values $h_2, \ldots, h_{s-1}$.

Remark 2. When s is even, $h_1 = 1$ is a solution of (3), while $h_1 = n-1$ is always a solution since $(n-1)^s \equiv (-1)^s \pmod{n}$. When $h_1 = n-1$, then $(-1)^{k-1} h_1^k \equiv -1 \pmod{n}$ which shows that $h_1 = h_2 = \cdots = h_{s-1} = n-1$.

Remark 3. Bounds on the number of solutions of the equation

$$h_1^s \equiv (-1)^s \pmod{n}$$

are known. For example, if n is prime, Lagrange's theorem shows there are at most s solutions modulo n for h_1 (see [11, Theorem 6.3]).

Before giving the proof, we state in Lemma 1 a property of circulant matrices that is needed in the proof. Such a property may be found in the monograph by Davis [3]. It is a simple consequence of the fact that any circulant matrix may be written as a polynomial of the cyclic permutation matrix T introduced in the proof below. As shown in [5], the Lemma below is also true if occurrences of 'circulant' are replaced by 'skew-circulant'.

Lemma 1. *Let C and D be two circulant matrices of the same size. Then CD is a circulant matrix and $CD = DC$.*

PROOF. For the proof of Theorem 1, we introduce the cyclic permutation matrix

$$T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Clearly, T is a circulant matrix. Then Lemma 1 shows that the powers T^k for $1 \leq k \leq s-1$ are circulant as well. Being a permutation matrix, T is a unimodular matrix and a cofactor expansion down the first column of T shows that $\det(T) = (-1)^{s-1}$. Hence the T^k are also unimodular matrices.

Let B be an $s \times s$ integer circulant matrix and suppose its associated HNF is of the form given in (2). So we can write $H = UB$ for some unimodular matrix U. Then for any k satisfying $1 \leq k \leq s-1$, we have

$$HT^k = UBT^k.$$

For circulant B, Lemma 1 shows that $BT^k = T^kB$. Hence

$$HT^k = U(T^kB) = (UT^k)B.$$

Since UT^k is unimodular, then HT^k and B generate the same lattice. But since H generates the same lattice as B, it then follows that HT^k and H generate the same lattice.

Now we have assumed that H is an HNF of the form given in (2), namely,

$$H = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & h_1 \\ 0 & 1 & 0 & \cdots & 0 & h_2 \\ 0 & 0 & 1 & \cdots & 0 & h_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & h_{s-1} \\ 0 & 0 & 0 & \cdots & 0 & n \end{bmatrix},$$

where $0 \leq h_k < n$, $1 \leq k \leq s-1$, and $n = |\det(B)|$. Let $\boldsymbol{e}_j$ be the j-th standard unit vector (treated as a row vector) and

$$\boldsymbol{h}^T = \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_{s-1} \\ n \end{bmatrix}.$$

This allows us to write

$$H = \left[\boldsymbol{e}_1^T, \boldsymbol{e}_2^T, \ldots, \boldsymbol{e}_{s-1}^T, \boldsymbol{h}^T\right].$$

Then for $1 \leq k \leq s-1$, we have

$$HT^k = \left[\boldsymbol{e}_{s-k+1 \pmod s}^T, \boldsymbol{e}_{s-k+2 \pmod s}^T, \ldots, \boldsymbol{e}_{s-1}^T, \boldsymbol{h}^T, \boldsymbol{e}_1^T, \ldots, \boldsymbol{e}_{s-k}^T \right],$$

where $\boldsymbol{h}^T$ is the k-th column of HT^k, and for convenience of notation, we take $\boldsymbol{e}_0 = \boldsymbol{h}$.

Now consider the first row of HT^k when $1 \leq k \leq s-2$. This row is given by

$$\boldsymbol{r} = [0, 0, \ldots, 0, h_1, 1, 0, \ldots, 0],$$

where h_1 is in the k-th position. As $\boldsymbol{r}$ (considered as a point of a lattice) belongs to the lattice generated by HT^k, it must belong to the lattice generated by H. It then follows from Definition 3 with $\boldsymbol{x} = \boldsymbol{r}$ and $A = H$ that there exist $\lambda_1, \ldots, \lambda_s \in \mathbb{Z}$ such that

$$\begin{aligned} \boldsymbol{r} &= \lambda_1[1, 0, \ldots, 0, h_1] + \lambda_2[0, 1, \ldots, 0, h_2] + \cdots + \lambda_{s-1}[0, 0, \ldots, 0, 1, h_{s-1}] \\ &\quad + \lambda_s[0, 0, \ldots, 0, 0, n] \\ &= \left[\lambda_1, \lambda_2, \ldots, \lambda_{s-1}, \sum_{j=1}^{s-1} \lambda_j h_j + \lambda_s n \right]. \end{aligned}$$

Matching the first $s-1$ components of $\boldsymbol{r}$ yields $\lambda_k = h_1$, $\lambda_{k+1} = 1$, and $\lambda_j = 0$ for $1 \leq j < k$ and $k+1 < j \leq s-1$. Moreover, matching the last component of $\boldsymbol{r}$ yields

$$0 = h_1 h_k + h_{k+1} + \lambda_s n.$$

Hence

$$h_{k+1} = -\lambda_s n - h_1 h_k$$

which leads to

$$h_{k+1} \equiv -h_1 h_k \pmod n.$$

By taking $k = 1, 2, 3, \ldots, s-2$ in turn, we then conclude that

$$h_{k+1} \equiv (-1)^k h_1^{k+1} \pmod n$$

for $1 \leq k \leq s-2$, which shows (4).

To show (3), we see from this last equation with $k = s-2$ that

$$h_1 h_{s-1} \equiv h_1 (-1)^{s-2} h_1^{s-1} \pmod n = (-1)^s h_1^s \pmod n. \tag{5}$$

Now we have

$$HT = \left[\boldsymbol{h}^T, \boldsymbol{e}_1^T, \ldots, \boldsymbol{e}_{s-2}^T, \boldsymbol{e}_{s-1}^T \right].$$

The $(s-1)$-th row of this matrix is given by $[h_{s-1}, 0, \ldots, 0, 0, 1]$. This row (considered as a point of a lattice) must belong to the lattice generated by H. Hence, similar to the above, there exist $\lambda_1, \ldots, \lambda_s \in \mathbb{Z}$ such that

$$[h_{s-1}, 0, \ldots, 0, 0, 1] = \left[\lambda_1, \lambda_2, \ldots, \lambda_{s-1}, \sum_{j=1}^{s-1} \lambda_j h_j + \lambda_s n \right].$$

This then means that $\lambda_1 = h_{s-1}$ and $\lambda_j = 0$ for $2 \le j \le s-1$. The last component of the point on each side of this last equation yields

$$1 = h_{s-1}h_1 + \lambda_s n.$$

Hence $h_{s-1}h_1 = 1 - \lambda_s n$, which leads to

$$h_{s-1}h_1 \equiv 1 \pmod{n}.$$

This together with (5) then shows that

$$(-1)^s h_1^s \equiv 1 \pmod{n},$$

which then leads to (3). This completes the proof. □

Example 1. Let

$$B = \begin{bmatrix} 5 & 33 & 8 \\ 8 & 5 & 33 \\ 33 & 8 & 5 \end{bmatrix}.$$

Then the HNF associated to this circulant B is

$$H = \begin{bmatrix} 1 & 0 & 16789 \\ 0 & 1 & 12281 \\ 0 & 0 & 32614 \end{bmatrix}.$$

One may verify that

$$16789^3 \equiv -1 \pmod{32614} \quad \text{and} \quad 12281 \equiv -16789^2 \pmod{32614}.$$

The result for skew-circulant lattice rules is similar.

Theorem 2. *Let H be of the form* (2) *and suppose it is the HNF associated to a rank-*1 *skew-circulant lattice rule having n points. Then the elements in the last column of H satisfy the following:*

$$h_1^s \equiv -1 \pmod{n}$$

and

$$h_k \equiv h_1^k \pmod{n}, \quad 2 \le k \le s-1.$$

Proof. For this proof, the circulant matrix T in the proof of the previous theorem has to be replaced by the skew-circulant matrix

$$\hat{T} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -1 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

As $\hat{T}$ is a skew-circulant matrix, Lemma 1 shows that the powers $\hat{T}^k$ for $1 \le k \le s-1$ are as well. A cofactor expansion down the first column of $\hat{T}$ shows that $\det(\hat{T}) = (-1)^s$. Hence $\hat{T}$ and the $\hat{T}^k$ are unimodular. As in the previous proof, we conclude that $H\hat{T}^k$ generates the same lattice as H.

With

$$H = \left[\boldsymbol{e}_1^T, \boldsymbol{e}_2^T, \ldots, \boldsymbol{e}_{s-1}^T, \boldsymbol{h}^T \right],$$

then for $1 \le k \le s-1$, we have

$$H\hat{T}^k = \left[-\boldsymbol{e}_{s-k+1 \pmod s}^T, -\boldsymbol{e}_{s-k+2 \pmod s}^T, \ldots, -\boldsymbol{e}_{s-1}^T, -\boldsymbol{h}^T, \boldsymbol{e}_1^T, \ldots, \boldsymbol{e}_{s-k}^T \right],$$

where $\boldsymbol{e}_0 = \boldsymbol{h}$. The full details of the rest of the proof are then similar to those given in the proof of the previous theorem and so are omitted. □

3. The sufficiency of the characterisation for circulant lattice rules

In this section, we look at the question of whether a Hermite normal form of the form (2) and that satisfies the relationships (3) and (4) of Theorem 1 is actually associated to a rank-1 circulant lattice rule. In other words, whether such a HNF is the HNF of an integer circulant matrix.

Unfortunately, it is not difficult to see that the answer is negative in the general case. In the case $s = 2$, suppose we have

$$H = \begin{bmatrix} 1 & h_1 \\ 0 & n \end{bmatrix},$$

where $h_1^2 \equiv 1 \pmod n$. Now for $s = 2$, an integer circulant matrix has to be of the form

$$B = \begin{bmatrix} b_0 & b_1 \\ b_1 & b_0 \end{bmatrix},$$

where $b_0, b_1 \in \mathbb{Z}$. Since $n = |\det(B)| = \left|b_0^2 - b_1^2\right|$, n has to be expressible as a difference of two squares. This means that $n \not\equiv 2 \pmod 4$; see [11, Problem 25 of Exercise 8.1]).

Even if n is the determinant of an integer circulant matrix, the answer is still negative in the general case. To see this, suppose

$$H = \begin{bmatrix} 1 & 1 \\ 0 & b_0^2 - b_1^2 \end{bmatrix},$$

where $b_0, b_1 \in \mathbb{Z}$ with $0 < b_1 < b_0$. Then this H satisfies the relationship (3) of Theorem 1. If this H is associated to an integer circulant matrix B, there must exist a unimodular matrix U such that $H = UB$ or $B = U^{-1}H$. However, it is easily checked that

$$B = \begin{bmatrix} b_0 & b_1 \\ b_1 & b_0 \end{bmatrix} = \begin{bmatrix} b_0 & -1/(b_0+b_1) \\ b_1 & 1/(b_0+b_1) \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & b_0^2 - b_1^2 \end{bmatrix}.$$

For this U^{-1}, its inverse U does not have integer entries and hence is not a unimodular matrix. So the given H cannot be the HNF associated to an integer circulant matrix.

We now give some examples of H of the form (2) that satisfy the relationships (3) and (4) of Theorem 1 and which are associated to circulant matrices having a known form. Here we shall make use of some of the matrices considered in Newman [6]. As we saw above in the case $s = 2$, the determinant of an integer circulant matrix can take on only certain values. The paper of Newman [6] considers the possible values of the determinant of integer circulant matrices.

Suppose we have an H of the form (2) such that the relationships (3) and (4) of the theorem (with $\det H = n$) are satisfied. If we can find an integer circulant matrix B with $\det(B) = n$ and an integer matrix W such that $WH = B$, then H must be the HNF associated to B. To see this, we note that $WH = B$ or $H = W^{-1}B$. Since W is an integer matrix with $\det(W) = 1$, then W^{-1} is a unimodular matrix.

From the form of H, we see that the first $s-1$ columns of W are identical to those of B. So the first $s-1$ columns of W are integers if B is a circulant matrix of the form (1). More specifically, we have

$$w_{k,j} = b_{(j-k) \bmod s}, \quad 1 \le k \le s, \quad 1 \le j \le s-1.$$

From (1) we see that the elements of B in the last column are given by

$$b_{k,s} = b_{s-k}, \quad 1 \le k \le s.$$

Then by considering the last column of $B = WH$, we have for $1 \le k \le s$,

$$b_{k,s} = b_{s-k} = \sum_{j=1}^{s-1} w_{k,j} h_j + w_{k,s} n = \sum_{j=1}^{s-1} b_{(j-k) \bmod s} h_j + w_{k,s} n.$$

So for $1 \le k \le s$, the elements in the last column of W are given by

$$\begin{aligned} w_{k,s} &= \frac{b_{s-k} - \sum_{j=1}^{s-1} b_{(j-k) \bmod s} h_j}{n} \\ &= \frac{b_{s-k} - \sum_{j=1}^{k-1} b_{s+j-k} h_j - \sum_{j=k}^{s-1} b_{j-k} h_j}{n}, \end{aligned} \tag{6}$$

with the usual convention that empty sums have the value zero. If we have $w_{k,s} \in \mathbb{Z}$ for $1 \le k \le s$, then W is an integer matrix. In this case, H is the HNF associated to the integer circulant matrix B.

Example 2. Let q be a positive integer and let H be the $s \times s$ matrix given by

$$H = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & qs(s-1)-1 \\ 0 & 1 & 0 & \cdots & 0 & qs(s-2)-1 \\ 0 & 0 & 1 & \cdots & 0 & qs(s-3)-1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & qs-1 \\ 0 & 0 & 0 & \cdots & 0 & qs^2 \end{bmatrix}. \tag{7}$$

The first $s-1$ entries in the last column are given by $h_k = qs(s-k)-1$, $1 \le k \le s-1$. For positive integer m, we have

$$\begin{aligned} h_1^m &= (qs(s-1)-1)^m = \sum_{i=0}^{m} \binom{m}{i} (qs(s-1))^i (-1)^{m-i} \\ &\equiv \sum_{i=0}^{1} \binom{m}{i} (qs(s-1))^i (-1)^{m-i} \pmod{qs^2} \\ &= \left((-1)^m + mqs(s-1)(-1)^{m-1}\right) \pmod{qs^2} \\ &\equiv \left((-1)^m - mqs(-1)^{m-1}\right) \pmod{qs^2}. \end{aligned}$$

With $m = s$ and $m = k$, we obtain

$$h_1^s \equiv (-1)^s \pmod{qs^2} \quad \text{and} \quad (-1)^{k-1} h_1^k \equiv (-1 - kqs) \pmod{qs^2}.$$

Since $h_k = qs(s-k) - 1 \equiv (-qsk - 1) \pmod{qs^2}$, we see that the h_k satisfy both (3) and (4) of Theorem 1 with $n = qs^2$.

As we shall show below, the H given above is the HNF associated with the integer circulant matrix B having

$$b_0 = q+1, \quad b_1 = q-1, \quad b_j = q, \quad 2 \le j \le s-1,$$

when s is odd or both s and q are even. The matrix H has determinant $n = qs^2$ as does the integer circulant matrix B. This latter result and this circulant matrix may be found in the proof of Theorem 4 in [6].

To verify that this H is indeed the HNF associated to this B, we make use of (6) and show that all the values of $w_{k,s}$ are integers. Because b_0, b_1, and the other b_j, $2 \le j \le s-1$, have differing values, we need to use (6) with the three possible values of b_{s-k}.

For $k = s$, we have from (6) that

$$\begin{aligned} w_{s,s} &= \frac{b_0 - \sum_{j=1}^{s-1} b_j h_j}{qs^2} \\ &= \frac{(q+1) - (q-1)h_1 - q\sum_{j=2}^{s-1} h_j}{qs^2} \\ &= \frac{(q+1) - (q-1)(qs(s-1)-1) - q\sum_{j=2}^{s-1}(qs(s-j)-1)}{qs^2}. \end{aligned}$$

One may verify that this last expression simplifies to $1 - q(s-1)/2$ which is integer when s is odd or both s and q are even.

For $k = s-1$, we have from (6) that

$$\begin{aligned} w_{s-1,s} &= \frac{b_1 - \sum_{j=1}^{s-2} b_{j+1}h_j - b_0 h_{s-1}}{qs^2} \\ &= \frac{q - 1 - q\sum_{j=1}^{s-2} h_j - (q+1)h_{s-1}}{qs^2} \\ &= \frac{q - 1 - q\sum_{j=1}^{s-2}(qs(s-j)-1) - (q+1)(qs-1)}{qs^2}. \end{aligned}$$

This last expression simplifies to $-q(s-1)/2$ which is integer when s is odd or both s and q are even.

For $1 \le k \le s-2$, we have from (6) that

$$\begin{aligned} w_{k,s} &= \frac{b_{s-k} - \sum_{j=1}^{k-1} b_{s+j-k}h_j - \sum_{j=k}^{s-1} b_{j-k}h_j}{qs^2} \\ &= \frac{q - q\sum_{j=1}^{k-1} h_j - (q+1)h_k - (q-1)h_{k+1} - q\sum_{j=k+2}^{s-1} h_j}{qs^2} \\ &= \frac{q - q\sum_{j=1}^{k-1}(qs(s-j)-1) - (q+1)(qs(s-k)-1)}{qs^2} \\ &\quad - \frac{(q-1)(qs(s-k-1)-1) - q\sum_{j=k+2}^{s-1}(qs(s-j)-1)}{qs^2}. \end{aligned}$$

This last expression also simplifies to $-q(s-1)/2$. Hence the H given in (7) is indeed the HNF associated to an integer circulant matrix when s is odd or both s and q are even.

Example 3. The previous example requires that s be odd or that both s and q are even for the H given in (7) to be the HNF associated to the integer circulant matrix having

$$b_0 = q+1, \quad b_1 = q-1, \quad b_j = q, \quad 2 \le j \le s-1.$$

In the case $s = 2$, we have

$$\begin{bmatrix} q+1 & q-1 \\ q-1 & q+1 \end{bmatrix} = \begin{bmatrix} q+1 & -q/2 \\ q-1 & 1-q/2 \end{bmatrix} \begin{bmatrix} 1 & 2q-1 \\ 0 & 4q \end{bmatrix}.$$

So when q is even, this last matrix is the HNF associated to the integer circulant matrix on the left-hand side of this last equation. However, when q is odd, we have

$$\begin{bmatrix} q+1 & q-1 \\ q-1 & q+1 \end{bmatrix} = \begin{bmatrix} (q+1)/2 & (1-q)/2 \\ (q-1)/2 & (3-q)/2 \end{bmatrix} \begin{bmatrix} 2 & 2q-2 \\ 0 & 2q \end{bmatrix}.$$

This last matrix is the HNF of the generator matrix for what is called a rank-2 lattice rule. Since $\gcd(b_0, b_1) = \gcd(q+1, q-1) = 2$ when q is odd, the comments

in Section 1 show why we do not have a HNF associated to a rank-1 circulant lattice rule.

Numerical calculations for $s = 6$ show that the previous example cannot be extended to the case of even s when q is odd.

For the case $s = 4$, we do find that the matrix product

$$\begin{bmatrix} q+1 & q-1 & q & (1-3q)/2 \\ q & q+1 & q-1 & (1-3q)/2 \\ q & q & q+1 & (-1-3q)/2 \\ q-1 & q & q & (1-3q)/2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 4q-1 \\ 0 & 1 & 0 & 8q-1 \\ 0 & 0 & 1 & 12q-1 \\ 0 & 0 & 0 & 16q \end{bmatrix} \tag{8}$$

is given by

$$\begin{bmatrix} q+1 & q-1 & q & q \\ q & q+1 & q-1 & q \\ q & q & q+1 & q-1 \\ q-1 & q & q & q+1 \end{bmatrix}. \tag{9}$$

When q is odd, then $(\pm 1 - 3q)/2$ is an integer. Moreover, one may verify that $(4q-1)^4 \equiv 1 \pmod{16q}$, $8q-1 \equiv -(4q-1)^2 \pmod{16q}$, and $12q-1 \equiv (4q-1)^3 \pmod{16q}$. In other words, the elements of the last column of the second matrix in (8) satisfy the relationships (3) and (4) of Theorem 1. Then a matrix of this form is the HNF associated to the integer circulant matrix given in (9) when q is odd.

Example 4. For the final example, consider

$$H = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & n-1 \\ 0 & 1 & 0 & \cdots & 0 & n-1 \\ 0 & 0 & 1 & \cdots & 0 & n-1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & n-1 \\ 0 & 0 & 0 & \cdots & 0 & n \end{bmatrix}.$$

As mentioned in the second Remark after Theorem 1, the values $n-1$ in the last column of H satisfy the relationships (3) and (4) of Theorem 1. Now suppose n is such that $\gcd(n, s) = 1$. Then it is claimed that this H is the HNF of the integer circulant matrix B given by

$$b_0 = b_1 = \cdots = b_{r-1} = q + 1, \quad b_r = b_{r+1} = \cdots = b_{s-1} = q,$$

where $n = qs + r$ for integers q and r with $1 \le r \le s - 1$.

To verify this claim, we again look at the elements in the last column of W where $WH = B$ and show they are all integers. We have $h_j = n - 1$ for $1 \le j \le s - 1$. Each row of B has r values of $q + 1$ and $s - r$ values of q.

In the case when $1 \le k \le s - r$, we have $b_{s-k} = q$. This leaves r values of $q + 1$ and $s - r - 1$ values of q in the k-th row of B. It then follows from (6)

that

$$\begin{aligned} w_{k,s} &= \frac{q - r(q+1)(n-1) - (s-r-1)q(n-1)}{n} \\ &= \frac{-qsn + qn - rn + qs + r}{n} = -qs + q - r + 1 \in \mathbb{Z}, \end{aligned}$$

where we have made use of $n = qs + r$.

Similarly, when $s - r + 1 \le k \le s$, we have $b_{s-k} = q + 1$. This leaves $r - 1$ values of $q + 1$ and $s - r$ values of q in the k-th row of B. From (6), we then obtain

$$\begin{aligned} w_{k,s} &= \frac{q + 1 - (r-1)(q+1)(n-1) - (s-r)q(n-1)}{n} \\ &= \frac{-qsn + qn - rn + n + qs + r}{n} \in \mathbb{Z}. \end{aligned}$$

References

[1] R. Cools and H. Govaert, *Five- and six-dimensional lattice rules generated by structured matrices*, J. Complexity **19** (2003) 715–729.

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

[3] P.J. Davis, *Circulant Matrices*, Wiley, New York, 1979.

[4] J.N. Lyness, *An introduction to lattice rules and their generator matrices*, IMA J. Numer. Anal. **9** (1989) 405–419.

[5] J. N. Lyness and T. Sørevik, *Four-dimensional lattice rules generated by skew-circulant matrices*, Math. Comp. **73** (2003) 279–295.

[6] M. Newman, *On a problem suggested by Olga Taussky-Todd*, Illinois J. Math. **24** (1980) 156–158.

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

[8] M. Rose, T. Plantard, and W. Susilo, *Improved BDD cryptosystems in general lattices*, in: F. Bao and J. Weng (Eds.), ISPEC 2011, Lecture Notes in Computer Science **6672** (2011), 152–167.

[9] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, New York, 1986.

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

[11] J.J. Tattersall, *Elementary Number Theory in Nine Chapters*, Cambridge University Press, New York, 1999.

[12] V.E. Tourloupis, *Hermite normal forms and its cryptographic applications*, Master of Computer Science thesis, University of Wollongong (2013), http://ro.uow.edu.au/theses/3788.