LATTICES OF MINIMAL INDEX IN $\mathbb{Z}^n$ HAVING AN ORTHOGONAL BASIS CONTAINING A GIVEN BASIS VECTOR

CHRIS PINNER AND CHRIS SMYTH

ABSTRACT. Given an vector $\underline{a}$ in $\mathbb{Z}^n$, we seek a lattice in $\mathbb{Z}^n$ of smallest index having an orthogonal basis containing $\underline{a}$. We find lower and upper bounds for this index, and develop an algorithm for computing it exactly. Also, we evaluate the index in $\mathbb{Z}^n$ of the lattice whose basis is the union of $\underline{a}$ and a basis for the integer points of the hyperplane $\underline{a}^{\perp}$.

1. INTRODUCTION

Suppose that $n \geq 1$ and we are given a nonzero n-tuple $\underline{a}$ of integers. We are studying the sublattices (n-dimensional subgroups) of $\mathbb{Z}^n$ that have an orthogonal basis that, moreover, have a lattice basis with $\underline{a}$ as one of the basis vectors. It is clear from solving the relevant homogeneous linear equations that such an orthogonal basis can always be constructed, which then, of course, specifies a sublattice, $L_n(\underline{a})$ say, of $\mathbb{Z}^n$. Its index, $D_n(\underline{a})$ in $\mathbb{Z}^n$ say, is the modulus of the determinant $D_n(\underline{a})$ of a matrix $M_n(\underline{a})$, say, whose rows form a basis for the lattice. By orthogonality, $D_n(\underline{a})$ is also the product of the lengths of these basis vectors. The question we are considering here is: what is the minimal index, call it $D_n^{\min}(\underline{a})$ say, of such a sublattice in $\mathbb{Z}^n$? Let us call a lattice with this minimal index $L_n^{\min}(\underline{a})$.

We denote by $\| \underline{a} \|$ the length $\sqrt{a_1^2 + \cdots a_n^2}$ of $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, and by $\mathcal{L}_n(\underline{a})$ the set of lattices in $\mathbb{Z}^n$ having an orthogonal basis containing $\underline{a}$. We let $M_n(\underline{a})$ denote any $n \times n$ matrix with integer entries whose top row is $\underline{a}$, has rows pairwise orthogonal, and determinant of modulus $D_n(\underline{a})$. Often we identify $M_n(\underline{a})$ with the lattice $L_n(\underline{a})$ generated by its rows.

1.1. Lower and upper bounds for $D_n^{\min}(\underline{a})$.

Theorem 1. *Given $n \geq 1$ and a nonzero vector $\underline{a} \in \mathbb{Z}^n$ whose components have* gcd $= g$, *then every lattice $L_n(\underline{a})$ has determinant an integer multiple of $\| \underline{a} \|^2 / g$. On the other hand there is a lattice with an orthogonal basis $M_n(\underline{a})$ such that $D_n(\underline{a}) \leq c_n \, \| \underline{a} \|^{2n-2} \, g$. Here*

Date: 17 September 2019.

2010 *Mathematics Subject Classification.* 11H99.

Key words and phrases. orthogonal lattice, integer sequence.

$c_1 = 1$ *while* c_n *is specified for* $n > 1$ *by*

$$c_{2n} = \frac{c_n^2}{4^{n-1}} \tag{1}$$
$$c_{2n+1} = \frac{c_n \cdot c_{n+1}}{4^{n-1}} \cdot \frac{n+1}{2n+1}.$$

The proof uses a method whereby, given matrices $M_{n'}(\underline{a}')$ and $M_{n''}(\underline{a}'')$ of the kind described above, we can construct a matrix $M_{n'+n''}(\underline{a}'|\underline{a}'')$ of the same kind. The proof will be given in Section 3.

1.2. **The lattice spanned by $\underline{a}$ and the integer points of the hyperplane $\underline{a}^\perp$.** We now look at a simpler problem. Given $\underline{a} \in \mathbb{Z}^n$, we take a basis $\underline{u}_2, \dots, \underline{u}_n$ for the sublattice in $\mathbb{Z}^n$ of the integer solutions to the equation $\underline{a} \cdot \underline{x} = 0$, and consider the lattice $L_n^\dagger(\underline{a})$ spanned by $\underline{a}, \underline{u}_2, \dots, \underline{u}_n$. We define $D_n^\dagger(\underline{a})$ to be the modulus of the determinant of this lattice. It is clear that the modulus of $D_n^\dagger(\underline{a})$ is independent of the choice of this basis.

We also remark that $D_n^\dagger(\underline{a})$ will be unchanged when its columns, including the components of $\underline{a}$, are permuted – see also Subsection 6.1 below. Thus $D_n^\dagger(\underline{a})$ is a function only of the underlying multiset of components of $\underline{a}$.

We can evaluate $D_n^\dagger(\underline{a})$ explicitly.

Theorem 2. *We have* $D_n^\dagger(\underline{a}) = \| \underline{a} \|^2 / g$, *where* g *is the* gcd *of the components of* $\underline{a}$.

Corollary 3. *For* $n = 1$ *and* 2 *we have* $D_n^{\min}(\underline{a}) = \| \underline{a} \|^2 / g$.

2. Lemmas

Lemma 4. *Given matrices*

$$M_{n'}(\underline{a}') = \begin{pmatrix} \underline{a}' \\ \underline{a}'_2 \\ \underline{a}'_3 \\ \vdots \\ \underline{a}'_{n'} \end{pmatrix} \in \mathcal{L}_{n'}(\underline{a}') \quad \textit{and} \quad M_{n''}(\underline{a}'') = \begin{pmatrix} \underline{a}'' \\ \underline{a}''_2 \\ \underline{a}''_3 \\ \vdots \\ \underline{a}''_{n''} \end{pmatrix} \in \mathcal{L}_{n''}(\underline{a}''),$$

the matrix

$$M_{n'+n''}(\underline{a}' \mid \underline{a}'') := \begin{pmatrix} \underline{a}' & | & \underline{a}'' \\ \underline{a}'_2 & | & \underline{0}'' \\ \underline{a}'_3 & | & \underline{0}'' \\ \vdots & \vdots & \vdots \\ \underline{a}'_{n'} & | & \underline{0}'' \\ \underline{0}' & | & \underline{a}''_2 \\ \underline{0}' & | & \underline{a}''_3 \\ \vdots & \vdots & \vdots \\ \underline{0}' & | & \underline{a}''_{n''} \\ \lambda \underline{a}' & | & -\mu \underline{a}'' \end{pmatrix}$$

lies in $\mathcal{L}_{n'+n''}(\underline{a}'|\underline{a}'')$. *Here* $\lambda = \| \underline{a}'' \|^2 / g'$ *and* $\mu = \| \underline{a}' \|^2 / g'$, *where* g' *is the* gcd *of the components of* $(\| \underline{a}'' \|^2 \, \underline{a}' \mid - \| \underline{a}' \|^2 \, \underline{a}'')$. *Furthermore, its determinant is*

$$D_{n'}(\underline{a}') D_{n''}(\underline{a}'') \, \| \underline{a}' | \underline{a}'' \|^2 / g'. \tag{2}$$

In the matrix, $\underline{0}'$ and $\underline{0}''$ are zero vectors of lengths n' and n'' respectively.

Proof. The rows of $M_{n'+n''}(\underline{a}'|\underline{a}'')$ are easily seen to be pairwise orthogonal. Its determinant squared, being the product of the squared lengths of its rows, is

$$\| \underline{a}' | \underline{a}'' \|^2 \cdot (D_{n'}(\underline{a}')^2 / \, \| \underline{a}' \|^2) \cdot (D_{n''}(\underline{a}'')^2 / \, \| \underline{a}'' \|^2) \cdot (\lambda^2 \, \| \underline{a}' \|^2 + \mu^2 \, \| \underline{a}'' \|^2).$$

This simplifies to $(\| \underline{a}' | \underline{a}'' \|^2 \, D_{n'}(\underline{a}') (D_{n''}(\underline{a}'')/g')^2$, giving the result. □

We note the following trivial result.

Lemma 5. *If* $b_1 \le b_2 \le \cdots \le b_n$ *then for* $1 \le k \le n$ *we have* $b_1 + b_2 + \cdots + b_k \le \frac{k}{n}(b_1 + b_2 + \cdots + b_n)$.

Proof. We clearly have $\frac{1}{k}(b_1 + b_2 + \cdots + b_k) \le \frac{1}{n}(b_1 + b_2 + \cdots + b_n)$. □

Lemma 6. *Given* $n \ge 2$, $n-1$ *linearly independent row vectors* $\underline{a}_2, \ldots, \underline{a}_n$ *in* $\mathbb{R}^n$ *and an indeterminate row vector* $\underline{y} = (y_1, \ldots, y_n)$ *in* $\mathbb{R}^n$, *expand the determinant* $\det M(\underline{y})$ *of the matrix*

$$M(\underline{y}) := \begin{pmatrix} \underline{y} \\ \underline{a}_2 \\ \vdots \\ \underline{a}_n \end{pmatrix}$$

as $\det M(\underline{y}) = \sum_{i=1}^n c_i y_i$. *Then the vector* $\underline{c} := (c_1, \ldots, c_n)$ *is orthogonal to the hyperplane* $\langle \underline{a}_2, \ldots, \underline{a}_n \rangle$.

(This generalises the very well-known formula for the cross product $\underline{a}_2 \times \underline{a}_3$ in $\mathbb{R}^3$.)

Proof. Let $\underline{d} = (d_1, \ldots, d_n)$ be nonzero and orthogonal to $\langle \underline{a}_2, \ldots, \underline{a}_n \rangle$. Now consider the equation

$$M(\underline{d}) \, \underline{x} = \begin{pmatrix} \sum_{j=1}^n d_j^2 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

where $\underline{x} = (x_1, \ldots, x_n)^{\mathsf{T}} \in \mathbb{R}^n$ is a column vector. Since $\det M(\underline{d}) \ne 0$, this equation has a unique solution. Hence this solution is $\underline{x} = \underline{d}^{\mathsf{T}}$, which is given by Cramer's Rule as

$$d_i = x_i = c_i \left(\frac{\sum_{j=1}^n d_j^2}{\det M(\underline{d})} \right) \qquad (i = 1, \ldots, n).$$

Hence $\underline{c}$ is a nonzero scalar multiple of $\underline{d}$ and so is also orthogonal to $\langle \underline{a}_2, \ldots, \underline{a}_n \rangle$. □

We see, (from choosing $\underline{d} = \underline{c}$ in the first place!) that in fact $\underline{c}$ is scaled so that its squared length $\| \underline{c} \|^2 := \sum_{j=1}^{n} c_j^2$ is equal to $\det M(\underline{c})$. For $n = 3$ we note in passing that this identity takes the form

$$\| \underline{a}_2 \times \underline{a}_3 \|^2 = \det \begin{pmatrix} \underline{a}_2 \times \underline{a}_3 \\ \underline{a}_2 \\ \underline{a}_3 \end{pmatrix}.$$

For our application with $\underline{a} \in \mathbb{Z}^n$, clearly $\underline{c} \in \mathbb{Z}^n$ too, and so we can divide $\underline{c}$ by the gcd of its components to make their gcd $= 1$.

3. Proof of Theorem 1

Proof of Theorem 1. The lower bound for $D^{\min}(\underline{a})$ comes from Theorem 2, since any lattice $L_n(\underline{a})$ is a sublattice of the lattice $L_n^{\dagger}(\underline{a})$ defined in Subsection 1.2. Thus $D_n(\underline{a})$ is a multiple of $D_n^{\dagger}(\underline{a})$.

for the upper bound we proceed by induction. We assume, as we can, that the components of $\underline{a}$ are in (non-strictly) ascending order. We can also clearly assume that $g = 1$, as the result for general g then follows trivially.

Next, we split $\underline{a}$ into two vectors of equal length, or of lengths differing by 1 and use the construction of Lemma 4. Thus for $\underline{a} = (\underline{a}' \mid \underline{a}'')$ of length $2n$, and $\underline{a}'$ and $\underline{a}''$ of length n we have that

$$\begin{aligned} D_{2n}(\underline{a}) &\le D_n(\underline{a}') D_n(\underline{a}'') \, \| \underline{a} \|^2 \\ &\le c_n^2 \, \| \underline{a}' \|^{2n-2} \| \underline{a}'' \|^{2n-2} \| \underline{a} \|^2 \\ &= c_n^2 \left(\| \underline{a}' \|^2 \| \underline{a}'' \|^2 \right)^{n-1} \| \underline{a} \|^2 \\ &\le c_n^2 \left(\frac{\| \underline{a}' \|^2 + \| \underline{a}'' \|^2}{2} \right)^{2n-2} \| \underline{a} \|^2 \end{aligned}$$

using $XY \le ((X+Y)/2)^2$,

$$= \frac{c_n^2}{4^{n-1}} \, \| \underline{a} \|^{4n-2}.$$

Similarly, for $\underline{a} = (\underline{a}' \mid \underline{a}'')$ of length $2n+1$, $\underline{a}'$ of length $n+1$ and $\underline{a}''$ of length n we have that

$$\begin{aligned} D_{2n+1}(\underline{a}) &\leq D_{n+1}(\underline{a}')D_n(\underline{a}'') \parallel \underline{a} \parallel^2 \\ &\leq c_{n+1}c_n \parallel \underline{a}' \parallel^{2n} \parallel \underline{a}'' \parallel^{2n-2} \parallel \underline{a} \parallel^2 \\ &= c_{n+1}c_n \parallel \underline{a}' \parallel^2 \left(\parallel \underline{a}' \parallel^2 \parallel \underline{a}'' \parallel^2 \right)^{n-1} \parallel \underline{a} \parallel^2 \\ &\leq c_{n+1}c_n \parallel \underline{a}' \parallel^2 \left(\frac{\parallel \underline{a}' \parallel^2 + \parallel \underline{a}'' \parallel^2}{2} \right)^{2n-2} \parallel \underline{a} \parallel^2 \\ &= \frac{c_{n+1}c_n}{4^{n-1}} \parallel \underline{a}' \parallel^2 \parallel \underline{a} \parallel^{4n-2} \\ &= \frac{c_{n+1}c_n}{4^{n-1}} \cdot \frac{n+1}{2n+1} \parallel \underline{a} \parallel^{4n}, \end{aligned}$$

on applying Lemma 5 to the squares of the coordinates of $\underline{a}'$.

□

4. The arithmetic of $D_n(\underline{a})$

Now a matrix

$$M(\underline{a}) = \begin{pmatrix} \underline{a} \\ \underline{a}_2 \\ \underline{a}_3 \\ \vdots \\ \underline{a}_n \end{pmatrix} \in \mathcal{L}_n(\underline{a}) \tag{3}$$

has

$$D_n(\underline{a})^2 = \parallel \underline{a} \parallel^2 \parallel \underline{a}_2 \parallel^2 \parallel \underline{a}_3 \parallel^2 \cdots \parallel \underline{a}_n \parallel^2 . \tag{4}$$

Thus any prime factor p of some $\parallel \underline{a}_i \parallel^2$ (which of course is an integer but not necessarily a square) must occur as another prime factor in some $\parallel \underline{a}_j \parallel^2$, since the LHS is a square.

Let us use this fact to show that $D_n^{\min}((1,2,3)) = 42$. Now $\parallel (1,2,3) \parallel^2 = 14$, so $\parallel \underline{a}_2 \parallel^2 \parallel \underline{a}_3 \parallel^2$ is of the form $14\ell^2$ for some ℓ. Thus the $D_n(\underline{a})$ is at least 14ℓ. There is no integer vector orthogonal to $(1,2,3)$ that has squared length equal to 1, 2, 4, 7,or 8. Hence ℓ must be at least 3. This bound is attained for $\begin{pmatrix} 1 & 2 & 3 \\ 1 & -2 & 1 \\ 4 & 1 & -2 \end{pmatrix}$, and also for $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -1 \\ 5 & -4 & 1 \end{pmatrix}$, both of determinant 42. We remark in passing that this example also shows that a matrix $M_n(\underline{a}) \in \mathcal{L}_n(\underline{a})$ with $D_n(\underline{a}) = D_n^{\min}(\underline{a})$ need not be unique, even if left multiplication by a signed permutation matrix is considered not to 'essentially change' the matrix.

We also have the following corollary to Theorem 2 above.

Corollary 7. *The modulus of the determinant $D_n(\underline{a})$ of a matrix $M(\underline{a})$ is divisible by* $\mathrm{lcm}_{i=1}^{n} \| \underline{a}_i \|^2 / g_i$, *where g_i is the* gcd *of the coordinates of $\underline{a}_i$. In particular, if $g_1 = 1$ then $D_n(\underline{a})$ is divisible by $\| \underline{a} \|^2$.*

Note that this last sentence cannot be deduced from equation (4). Here $\underline{a}_1 = \underline{a}$. The proof of this result follows easily from Theorem 2. Since the 2nd, 3rd, ... rows of $M(\underline{a})$ are all orthogonal to $\underline{a}$, all the rows of $M(\underline{a})$ span a sublattice of the matrix discussed in that Theorem. Hence, by the Theorem, the matrix must have determinant a multiple of $\| \underline{a} \|^2 / g_1$. Applying this fact to all rows of $M(\underline{a})$ gives the full result.

5. Algorithms for computing $D_n^{\min *}(\underline{a})$ and $D_n^{\min}(\underline{a})$

5.1. **Computing $\mathbf{D}_n^{\min *}(\underline{a})$.** Let us fix a nonzero integer vector $\underline{a}$. Since multiplying any column of $M_n(\underline{a}) \in \mathcal{L}_n(\underline{a})$ by -1 conserves the orthogonality of its rows, we can assume that $\underline{a} \in (\mathbb{Z}_{\geq 0})^n$. If $n = 1$ we have $D_n^{\min}(\underline{a}) = g = \| \underline{a} \|$ trivially, while if $n = 2$ we have $D_n^{\min}(\underline{a}) = \| \underline{a}/g \|^2 \, g$, where g is the gcd of the coordinates of $\underline{a}$. For larger n we can proceed recursively, using the construction of Lemma 4, to get a good upper bound, $D_n^{\min *}(\underline{a})$ say, for $D_n^{\min}(\underline{a})$. Specifically, we apply that lemma to all possible 2-partitions of $\underline{a}$. Each such 2-partition enables us to write $\underline{a}^* = (\underline{a}' \mid \underline{a}'')$, where the coordinate multisets of $\underline{a}'$ and $\underline{a}''$ correspond to the 2-partition, and $\underline{a}^*$ is a vector whose coordinates are a permutation of those of $\underline{a}$. Then we can define $D_n^{\min *}(\underline{a})$ to be the minimum, over all such 2-partitions, of $D_{n'}^{\min *}(\underline{a}') D_{n''}^{\min *}(\underline{a}'') \, \| \underline{a} \|^2 / g'$, as in (2) of Lemma 4, and with the notation used there.

We have implemented this algorithm in Maple: **Good-upper-bound-for-minimum**$(\underline{a})$. As we shall see in Section 6, $D_n^{\min *}(\underline{a})$ is often equal to $D_n^{\min}(\underline{a})$. However, they are not always equal. For instance, for $\underline{a} = (1, 2, 3)$ the method gives $D_n^{\min *}(\underline{a}) = 70$, coming from the matrix $\begin{pmatrix} 1 & 2 & 3 \\ -2 & 1 & 0 \\ 3 & 6 & 5 \end{pmatrix}$, while in fact, as shown above, $D_n^{\min}(\underline{a}) = 42$.

Although this method does not necessarily give the minimal determinant sought, we can use the upper bound $B := D_n^{\min *}(\underline{a})$ it produces to make the exhaustive search, which we are about to describe, shorter than it otherwise might be.

5.2. **Computing $D_n^{\min}(\underline{a})$.** We work with a matrix of the form (3). We are going to search for all matrices $M_n(\underline{a}) \in \mathcal{L}_n(\underline{a})$ of determinant at most B. (We allow equality so that the search is guaranteed to succeed.)

We want

$$D_n(\underline{a}) = \| \underline{a} \| \| \underline{a}_2 \| \ldots \| \underline{a}_n \| \leq B. \tag{5}$$

By permuting the $n-1$ bottom rows, if necessary, we can assume that

$$1 \leq \| \underline{a}_2 \| \leq \| \underline{a}_3 \| \leq \cdots \leq \| \underline{a}_n \|, \tag{6}$$

so that, for $2 \leq \ell \leq n-1$ we have

$$\| \underline{a}_{\ell+1} \|^{n-\ell} \leq \| \underline{a}_{\ell+1} \| \cdots \| \underline{a}_n \| \leq \frac{B}{\| \underline{a} \| \| \underline{a}_2 \| \cdots \| \underline{a}_\ell \|}, \tag{7}$$

giving

$$\| \underline{a}_\ell \| \leq \| \underline{a}_{\ell+1} \| \leq \left(\frac{B}{\| \underline{a} \| \| \underline{a}_2 \| \cdots \| \underline{a}_\ell \|} \right)^{1/(n-\ell)} =: B_{\ell+1}, \tag{8}$$

say, while for $\ell = 1$

$$1 \leq \| \underline{a}_2 \| \leq \left(\frac{B}{\| \underline{a} \|} \right)^{1/(n-1)} =: B_2, \tag{9}$$

say.

Our most important subroutine for finding the true minimum $D_n^{\min}(\underline{a})$ which we call **Row-finder**(A, L, U). Here A is a $(k-1) \times n$ integer matrix whose top row is $\underline{a}$ and whose rows are mutually orthogonal. Here $k \geq 2$ and $\underline{a} \in (\mathbb{Z}_{\geq 0})^n$, with components in nondecreasing order. Its purpose is to find all possible vectors $\underline{h} = (h_1, \ldots, h_n) \in \mathbb{Z}^n$ that are orthogonal to all rows of A and for which $L \leq \| \underline{h} \|^2 \leq U$. For suitable L, U such $\underline{h}$ can be used for a possible kth row of A. Its essential structure is a depth-first search on the tree with nodes of depth given by the column index j, and each node labelled by integer vectors $(h_1, \ldots, h_j)$ which are the possible first j components of a row of the kind being sought. The root is unlabeled. Obviously the edges of the tree are between nodes labelled $(h_1, \ldots, h_{j-1})$ and $(h_1, \ldots, h_j)$.

As a first step the matrix A is replaced by an integer echelon form matrix E, obtained from A by integer row operations and whose ℓth row has 'nonzero length' (i.e., the length excluding its trailing zeroes on the right) is denoted m_ℓ. The rows of E are ordered so that these nonzero lengths strictly increase with ℓ. Note that the $(k-1)$-th row of E is $\underline{a}$. To construct all possible kth rows $\underline{h}$ we classify the n columns of E, indexed by j, into four types. Defining $m_0 := 0$, we have

$$\begin{aligned}
&\text{type 1 :} && m_{\ell-1} < j < m_\ell - 1; \\
&\text{type 2 :} && m_{\ell-1} < j = m_\ell - 1; \\
&\text{type 3 :} && m_{\ell-1} + 1 < j = m_\ell; \\
&\text{type 4 :} && m_{\ell-1} + 1 = j = m_\ell.
\end{aligned}$$

For given column j, row ℓ is chosen to be the least ℓ such that j is of one of these types. Since the components of $\underline{a}$ are in nondecreasing order, $m_{k-1} = n$, the nonzero length of $\underline{a}$. The aim is to construct all $\underline{h}$ orthogonal to all rows of E (and hence of A), and with $\| \underline{h} \|^2 \leq U$. Having constructed such an $\underline{h}$, it is rejected if $\| \underline{h} \|^2 < L$, and so then the algorithm backtracks. Assuming that we are at a node labelled $(h_1, \ldots, h_{j-1})$, to find all possible h_j we need to have

$$h_j^2 \leq U - (h_1^2 + h_2^2 + \cdots h_{j-1}^2). \tag{10}$$

Furthermore: for j of type 1 we can simply choose all h_j satisfying that inequality.

For j of type 2, and so $j+1$ of type 3, we have, from the row $\underline{e} = (e_1, \ldots, e_{j+1}, 0, \ldots, 0)$ of E of nonzero length $j+1$ the constraint

$$h_1 e_1 + \cdots + h_{j-1} e_{j-1} + h_j e_j + h_{j+1} e_{j+1} = 0,$$

where $e_{j+1} \neq 0$ and $h_1, \ldots, h_{j-1}$ are known. Thus one has to find all integer solutions h_j, h_{j+1} to this equation, subject to $h_j^2 + h_{j+1}^2 \leq U - (h_1^2 + h_2^2 + \cdots h_{j-1}^2)$. This is readily done by a straightforward subroutine. Again, if there are no solutions, the algorithm backtracks.

Finally, if j is of type 4 one has a row $\underline{e} = (e_1, \ldots, e_j, 0, \ldots, 0)$ of E of nonzero length j such that $e_j \neq 0$ and

$$h_1 e_1 + \cdots + h_{j-1} e_{j-1} + h_j e_j = 0,$$

Thus h_j is uniquely determined by $(h_1, \ldots, h_{j-1})$ and must be an integer, and satisfy the inequality (10). Otherwise this branch of the tree ends, and again the algorithm backtracks.

The search tree can be trimmed when the matrix A has some equal columns. For two such columns $j < j'$ say, we can assume that $h_j \geq h'_j$. This applies in particular when $k = 2$ and $\underline{a}$ has some equal components. This speedup is particularly effective for $\underline{a} = (1, 1, \ldots, 1)$ – see Subsection 6.3.

The output of **Row-finder**(A, L, U) is a (possibly empty) list of rows orthogonal to the rows of A, and of squared length between L and U. They are restricted to those rows whose first nonzero component is positive.

The main program, **Put-rows-together**$(\underline{a})$, finds all $n \times n$ integer matrices whose first row is $\underline{a}$, whose rows are mutually orthogonal and whose determinant is at most $B := D_n^{\min *}(\underline{a})$ in modulus. Since we know that there is at least one such matrix, the program will find the smallest one. This program is also structured as a depth-first tree search, but this time using the row index i as the depth. The root at $i = 1$ is labelled $\underline{a}$, with the nodes at level i labelled $A_i := (\underline{a}, \underline{a}_2, \ldots, \underline{a}_i)$, and joined to the node labelled $A_{i-1} = (\underline{a}, \underline{a}_2, \ldots, \underline{a}_{i-1})$. We then find all possible 2nd rows $\underline{a}_2$ using **Row-finder**$((\underline{a}), 1, U/ \| \underline{a} \|)$. For $3 \leq i \leq n-1$ it finds all possible ith rows using

$$\textbf{Row-finder}(A_{i-1}, \| a_{i-1} \|, B_i) \tag{11}$$

from (8). The final row $\underline{a}_n$ is uniquely determined by the other $n-1$ rows, and is in fact specified by Lemma 6. It should satisfy

$$\| a_{n-1} \| \quad \leq \quad \| \underline{a}_n \| \quad \leq \quad B_n \qquad \text{(defined by (8))},$$

so that the sequence of row lengths (after the first) is (non-strictly) increasing, and the final determinant is at most B in modulus. Otherwise, backtrack. If any value $D_n(\underline{a}) < D_n^{\min *}(\underline{a})$ is found along the way, then we can trim the search tree by replacing $D_n^{\min *}(\underline{a})$ by $D_n(\underline{a})$ in the definition of $B := D_n^{\min *}(\underline{a})$ in the equations of Section 5.2.

The output of **Put-rows-together**$(\underline{a})$ is $D_n^{\min}(\underline{a})$, along with a matrix $M_n^{\min}(\underline{a})$ with determinant of modulus $D_n^{\min}(\underline{a})$.

6. Heinz encoding of integer multisets, and integer sequences

6.1. **Permuting or changing signs of the components of $\underline{a}$, or removing its zeros.** Now multiplication of any $M_n(\underline{a}) \in \mathcal{L}_n(\underline{a})$ on the right by a signed permutation matrix, while not changing $D_n(\underline{a})$, will in general change the order and the signs of (some) elements of $\underline{a}$. Thus we can confine our attention to $\underline{a}$ with nonnegative components. Also, $D_n(\underline{a})$

depends only on the multiset of its components. Thus we can choose the order of these components, so that, e.g., they are in nondecreasing order.

If our given integer vector $\underline{a}$ contains $\ell > 0$ zero entries, then we can construct a matrix $M_n(\underline{a})$ from a matrix $M_{n-\ell}(\underline{a}^{\#})$, where $\underline{a}^{\#} \in \mathbb{Z}^{n-\ell}$ is $\underline{a}$ with its zeros removed, as follows. We add ℓ extra rows and columns to $M(\underline{a}^{\#})$, with an $\ell \times \ell$ identity matrix on the diagonal and all other new entries equal to 0. This construction of $M_n(\underline{a})$ shows immediately that $D_n^{\min}(\underline{a}) \le D_n^{\min}(\underline{a}^{\#})$. We conjecture that they are actually equal, but, somewhat to our surprise, have not been able to prove this.

Assuming this conjecture, we can confine our attention to those $\underline{a} \in (\mathbb{Z}_{>0})^n$ whose components are in nonstrictly increasing order.

6.2. **Heinz encoding.** Given a finite multisubset $\{n_1, n_2, \ldots, n_k\}$ of $\mathbb{Z}_{>0}$, its *Heinz number* is defined as $\prod_{i=1}^{k} p_{n_i}$, where p_n denotes the nth prime. This gives a bijection between such multisets and $\mathbb{Z}_{>0}$. See for instance OEIS A122111 [2]. Thus we can re-cast the values of $D_n^{\min}(\underline{a})$ for multisets $\underline{a}$ as an integer sequence $\{S(n)\}_{n\in\mathbb{N}}$ say. Note that $S(p_k) = k$, and $S(p_k p_{k'}) = (k^2 + k'^2)/\gcd(k, k')$. Also, because $D_n(k\underline{a}) = kD_n(\underline{a})$ we have

$$S(p_{k\ell_1} p_{k\ell_2} \cdots p_{k\ell_r}) = kS(p_{\ell_1} p_{\ell_2} \cdots p_{\ell_r}).$$

In particular, $S(p_k^r) = kS(2^r)$.

Defining $S(1) = 0$, the first terms of the sequence are

$$0, 1, 2, 2, 3, 5, 4, 6, 4, 10, 5, 6, 6, 17, 13, 8, 7, 18, 8, 22, 10, 26, 9, 42, 6, 37, 12, 18, 10, \underline{42}, 11, 40,$$

$$29, 50, 25, 20, 12, 65, 20, 24, 13, \underline{42}, 14, 54, 34, 82, 15, 32, 8, 38, 53, 38, 16, 78, 34, 114, 34, 101,$$

$$17, 30, 18, 122, 12, 48, 15, 30, 19, 102, 85, \underline{78}, 20, 132, 21, 145, 22, 66, 41, 205, 22, 104, 16, 170,$$

This is sequence A327267 of OEIS [2]. We can do the same thing for the values of $D_n^{\min *}(\underline{a})$, obtaining the sequence $\{S^*(n)\}_{n\in\mathbb{N}}$ say, beginning

$$0, 1, 2, 2, 3, 5, 4, 6, 4, 10, 5, 6, 6, 17, 13, 8, 7, 18, 8, 22, 10, 26, 9, 42, 6, 37, 12, 18, 10, \underline{70}, 11, 40,$$

$$29, 50, 25, 20, 12, 65, 20, 24, 13, \underline{105}, 14, 54, 34, 82, 15, 32, 8, 38, 53, 38, 16, 78, 34, 114, 34, 101,$$

$$17, 30, 18, 122, 12, 48, 15, 30, 19, 102, 85, \underline{130}, 20, 132, 21, 145, 22, 66, 41, 205, 22, 104, 16, 170,$$

This is sequence A327268 of OEIS [2]. The first value of n for which these sequences differ is $n = 30 = p_1 p_2 p_3$ corresponding to the vector $(1, 2, 3)$. We saw above that $S^*(30) = 70$ while $S(30) = 42$. (The underlined numbers are the first three where the two sequences differ, namely for $n = 30, 42$ and 70.) The sequence A327274 is a list of those n for which $S^*(n) < S(n)$.

Theorem 2 also gives rise to an integer sequence via Heinz encoding. Thus if $\underline{a} \in \mathbb{Z}^r$ has positive integer components whose Heinz encoding is n, the sequence $S^{\dagger}(n)$ can be defined as $D_r^{\dagger}(\underline{a})$, which, by Theorem 2, equals $\|\underline{a}\|^2 / g$. This is sequence A289507 of OEIS.

6.3. **Further examples.** For the vector $(1,2,3,\dots,n) \in \mathbb{Z}^n$, our program gives for $n = 1,2,\dots,8$ that

$$D_n^{\min}((1,2,3,\dots,n)) = 1,5,42,90,990,5733,6720,39168,$$

(OEIS A327269) while

$$D_n^{\min *}((1,2,3,\dots,n)) = 1,5,70,150,1650,35490,147000,2142000.$$

(OEIS A327270). Since $(1,2,3,\dots,n)$ corresponds to the integer $p_1p_2\cdots p_n$ in Heinz encoding, we have

$$S(p_1p_2\cdots p_n) = D_n^{\min}((1,2,3,\dots,n))$$

in A327268 above, while

$$S^*(p_1p_2\cdots p_n) = D_n^{\min *}((1,2,3,\dots,n))$$

in A327269.

On the other hand, for $(1,1,\dots,1) \in \mathbb{Z}^n$ our program gives for $n = 1,2,\dots,13$ that

$$D_n^{\min}((1,1,\dots,1)) = D_n^{\min *}((1,1,\dots,1))$$

with the values

$$1,2,6,8,40,48,336,128,864,1280,8448,3072,39936.$$

(OEIS A327271). Since $(1,1,\dots,1)$ corresponds to the integer $p_1^n = 2^n$, these are the values of $S(2^n) = S^*(2^n)$ for $n = 1,\dots,12$ for both the sequences A327267 and A327268 above.

Now take n to be a power of 2, say $n = 2^k$, giving

$$S(2^{2^k}) = S^*(2^{2^k}) = 1,2,8,128 \quad \text{for} \quad k = 0,1,2,3.$$

Put $S_2(k) := S(2^{2^k})$ and $S_2^*(k) := S^*(2^{2^k})$. Then construct a $2^{k+1}\times 2^{k+1}$ matrix $M_{2^{k+1}}((1,1,\dots,1))$ from two copies of a $2^k \times 2^k$ matrix $M_{2^{k+1}}((1,1,\dots,1))$ using Lemma 5, in particular equation (2) with $\underline{a}' = \underline{a}'' = (1,1,\dots,1) \in \mathbb{Z}^{2^k}$ and $g' = 2^k$. This shows that $S_2^*(k+1) \le 2S_2^*(k)^2$. Using $S_2^*(0) = 1$ this gives $S_2(k) \le S_2^*(k) \le 2^{2^k-1}$. We see that we have equality for $k \le 3$. We may in fact have $S_2^*(k) = 2^{2^k-1}$ for all k (essentially OEIS A058891), or conceivably even that $S_2(k) = 2^{2^k-1}$ for all k.

7. Proof of Theorem 2

Proof. First of all, we note that we can assume that $g = 1$, as the result for arbitrary g then follows easily. We can also assume that all the a_i are nonnegative, as again the general case then follows easily. We use strong induction on $m = \min(a_1,\dots,a_n)$. Our induction hypothesis is that there is an $\varepsilon = \pm 1$ such that for $i = 1,\dots,n$ the cofactor A_i of the ith element a_i of the top row of $D_n^\dagger(\underline{a})$ is equal to εa_i. Then the result follows on expanding $D_n^\dagger(\underline{a})$ by its top row: $D_n^\dagger(\underline{a}) = \sum_{i=1}^n a_iA_i$.

For the base case $m = 1$, we can assume without loss of generality that $a_1 = 1$. Then for $\underline{x} = (x_1,\dots,x_n) \in \mathbb{Z}$ with $\underline{a}\cdot\underline{x} = 0$, $x_2,\dots,x_n$ can be chosen arbitrarily, giving $x_1 = -\sum_{i=2}^n a_ix_i$. Thus we can take as a basis of solutions of $\underline{a}\cdot\underline{x} = 0$ the vectors

$$\underline{u}_j = (-a_j,0,\dots,0,1,0,\dots,0) \ (j = 2,\dots,n),$$

where the '1' is in the jth place. Hence we see that $A_1 = 1 = a_1$ while for $j \geq 2$ we have

$$A_j = (-1)^{j-1} \begin{vmatrix} -a_2 & 1 & & & & & & \\ -a_3 & & 1 & & & & & \\ \cdot & & & \cdot & & & & \\ \cdot & & & & \cdot & & & \\ \cdot & & & & & \cdot & & \\ -a_{j-1} & & & & & & 1 & \\ -a_j & & & & & & & \\ -a_{j+1} & & & & & & & 1 \\ \cdot & & & & & & & \\ \cdot & & & & & & & \\ \cdot & & & & & & & \\ -a_n & & & & & & & \end{vmatrix},$$

where the blank entries are 0. From this we readily obtain $A_j = a_j$. (So $\varepsilon = 1$ for our particular choice of basis.)

Now assume that $m \geq 2$ and that the induction hypothesis holds for all $\underline{a}$ with minimum element strictly less than m. Consider an integer vector $\underline{a}$ with minimum element equal to m. Without loss of generality we can assume that $a_1 = m$. Furthermore, since not all the a_i are divisible by m we can assume, again without loss of generality, that $a_2 = km + r$, where $1 \leq r < m$. Now consider our equation

$$mx_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = 0, \tag{12}$$

which we can write as

$$mx_0 + rx_2 + a_3x_3 + \cdots + a_nx_n = 0, \tag{13}$$

where $x_0 = x_1 + kx_2$. Then, by the induction hypothesis, we can assume that for the vector $\underline{a}' = (m, r, a_3, \ldots, a_n)$ that the ith cofactor A'_i of $D_n^\dagger(\underline{a}')$ with respect to its top row is, for some $\varepsilon = \pm 1$, equal to $\varepsilon a_i (i \neq 2)$ and εr for $i = 2$. Now, using $x_1 = x_0 - kx_2$, we see that for each basis solution $\underline{u}' = (u_0, u_2, u_3, \ldots, u_n)$ of (13) there is a basis solution $\underline{u} = (u_0 - ku_2, u_2, u_3, \ldots, u_n)$ of (12). Thus the cofactors A_i of (12) are given by $A_1 = A'_1 = \varepsilon m$, while for $j = 3, \ldots, n$ we have $A_j = A'_j$ again, obtained by adding k times the jth column of A_j to its first column. Finally, taking the signs of A'_1 and A'_2 into account, we have $A_2 = A'_2 + kA' = \varepsilon(r + km) = \varepsilon a_2$. This proves the inductive step. □

8. The constants c_n.

We note finally that, apart from $c_3 = 2/3$, all the c_n's in Theorem 1 are reciprocals of integers. In fact all the nc_n's are reciprocals of integers for $n \geq 4$. To see this, put $u_n = \frac{1}{nc_n}$. Then from equation (1) we have $u_1 = 1$ and for $n > 1$ that

$$\begin{aligned} u_{2n} &= n2^{2n-3}u_n^2 \\ u_{2n+1} &= n2^{2n-2}u_nu_{n+1}. \end{aligned} \tag{14}$$

Thus $u_2 = u_3 = 1/2$ while all u_n for $n \geq 4$ clearly form an integer sequence

$1, 2, 6, 24, 128, 512, 2560, 15360, 110592, 884736, 8257536, 88080384, 1073741824,$
$8589934592, 77309411328, 773094113280, 8589934592000, 103079215104000,$
$1360645639372800, 19593297206968320, 307792887033102336, 4924686192529637376, \ldots.$

References

[1] Maple 2019, www.maplesoft.com.
[2] N. J. A. Sloane, editor, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org

Department of Mathematics, Kansas State University, Manhattan, Kansas, USA 66506
E-mail address: pinner@ksu.edu

School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, Edinburgh EH9 3FD, Scotland, U.K.
E-mail address: c.smyth@ed.ac.uk