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

CHRISTOPHER PINNER AND CHRISTOPHER SMYTH

ABSTRACT. Given a vector $\mathbf{a}$ in $\mathbb{Z}^n$, we seek a lattice in $\mathbb{Z}^n$ of smallest index $D_{\min}(\mathbf{a})$ having an orthogonal basis containing $\mathbf{a}$. We find lower and upper bounds for this index, and develop an algorithm for computing it exactly. The lower bound is provided by evaluation of the index in $\mathbb{Z}^n$ of the lattice $L_n^{\perp}(\mathbf{a})$ whose basis is the union of $\mathbf{a}$ and a basis for the integer points of the hyperplane $\mathbf{a}^{\perp}$. We obtain upper bounds $D^*(\mathbf{a}) \le D^{**}(\mathbf{a}) \le D^{***}(\mathbf{a})$ for $D_{\min}(\mathbf{a})$ by construction of lattices of the required type (the more stars, the simpler the construction). We also study for which $\mathbf{a}$ these lower and upper bounds are sharp, giving particularly detailed results in the case $n = 3$.

1. INTRODUCTION

1.1. **Preliminaries.** Suppose that $n \ge 1$ and we are given a nonzero n-tuple $\mathbf{a}$ of integers. We are studying the full sublattices (n-dimensional subgroups) of $\mathbb{Z}^n$ that have an orthogonal basis with $\mathbf{a}$ as one of the basis vectors; we denote the set of such sublattices by $\mathcal{L}(\mathbf{a})$. It is clear from solving the relevant homogeneous linear equations that such an orthogonal basis can always be constructed, which then specifies a sublattice, $L(\mathbf{a})$ say, of $\mathbb{Z}^n$. Its index in $\mathbb{Z}^n$, $D(\mathbf{a})$ say, is the modulus of the determinant of a matrix

$$M(\mathbf{a}) = \begin{pmatrix} \mathbf{a} \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \vdots \\ \mathbf{a}_n \end{pmatrix} \in \mathcal{L}(\mathbf{a}) \tag{1}$$

say, whose rows form a basis for $L(\mathbf{a})$. By orthogonality,

$$M(\mathbf{a})M(\mathbf{a})^{\mathsf{T}} = \operatorname{diag}(\|\,\mathbf{a}\,\|^2, \|\,\mathbf{a}_2\,\|^2, \|\,\mathbf{a}_3\,\|^2, \cdots, \|\,\mathbf{a}_n\,\|^2),$$

so that

$$D(\mathbf{a}) = \|\,\mathbf{a}\,\| \cdot \|\,\mathbf{a}_2\,\| \cdot \|\,\mathbf{a}_3\,\| \cdots \|\,\mathbf{a}_n\,\| \,. \tag{2}$$

Here $\|\,.\,\|$ denotes Euclidean length. The main question we are considering here is: what is the minimal index, call it $D_{\min}(\mathbf{a})$ say, of such a sublattice in $\mathbb{Z}^n$? Let us call any lattice with this minimal index $L_{\min}(\mathbf{a})$.

Date: 3 December 2021.

2020 *Mathematics Subject Classification.* 11H06,52C07.

Key words and phrases. orthogonal lattice, integer sequence.

Theorem 1. *For $n \geq 1$ and a vector $\mathbf{a} \in \mathbb{Z}^n$ whose components have* gcd *equal to g we have*

$$\frac{\|\mathbf{a}\|^2}{g} \leq D_{\min}(\mathbf{a}) \leq \frac{(n-1)!}{n^{n-2}g^{2n-3}}\|\mathbf{a}\|^{2n-2}. \tag{3}$$

Both inequalities are sharp for $n = 1$ and 2. In Section 3 we shall construct three further upper bounds

$$D^*(\mathbf{a}) \leq D^{**}(\mathbf{a}) \leq D^{***}(\mathbf{a}) \leq \frac{(n-1)!}{n^{n-2}g^{2n-3}}\ \|\mathbf{a}\|^{2n-2} \tag{4}$$

for $D_{\min}(\mathbf{a})$. All three bounds are sharp for some $\mathbf{a}$, as we shall see. An important part of this paper is the description, in Section 5, of an algorithm for evaluating $D_{\min}(\mathbf{a})$. We have implemented the algorithm in Maple [1]. The first part of this algorithm is a routine to compute $D^*(\mathbf{a})$. The algorithm for evaluating $D^*(\mathbf{a})$ is much simpler than that for $D_{\min}(\mathbf{a})$, while $D^{**}(\mathbf{a})$ and $D^{***}(\mathbf{a})$ are given by the explicit formulae (9) and (14) below.

Since multiplying any column of $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$ by -1 preserves the orthogonality of its rows, we can assume that $\mathbf{a} \in (\mathbb{Z}_{\geq 0})^n$. In fact, although $\mathbf{a}$ is written as a vector, $D(\mathbf{a})$ depends only on the multiset of components of $\mathbf{a}$; this is clearly seen by permuting the columns of the matrix $M(\mathbf{a})$ with determinant $\pm D(\mathbf{a})$. Thus we can assume that the components of $\mathbf{a}$ are in (non-strictly) ascending order. Furthermore, because clearly

$$D_{\min}(\mathbf{a}) = gD_{\min}\left(\frac{\mathbf{a}}{g}\right),$$

where g is as in Theorem 1, we can for computational purposes assume that $g = 1$. Indeed, g is included in formulae such as (3) and (14) only for completeness.

1.2. **The lattice spanned by a and the integer points of the hyperplane $\mathbf{a}^\perp$.** For our given $\mathbf{a} \in \mathbb{Z}^n$, we can define a related sublattice of $\mathbb{Z}^n$ as follows. Take a basis $\mathbf{u}_2, \ldots, \mathbf{u}_n$ for the sublattice in $\mathbb{Z}^n$ of the integer solutions to the equation $\mathbf{a} \cdot \mathbf{x} = 0$, and consider the lattice $L^\perp(\mathbf{a})$ spanned by $\mathbf{a}, \mathbf{u}_2, \ldots, \mathbf{u}_n$. We define $D^\perp(\mathbf{a})$ to be the modulus of the determinant of this lattice. It is clear that the modulus of $D^\perp(\mathbf{a})$ is independent of the choice of this basis.

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

We can evaluate $D^\perp(\mathbf{a})$ explicitly.

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

The proof is given in Section 8.

Corollary 3. *For $n = 2$ we have $D_{\min}(\mathbf{a}) = D^\perp(\mathbf{a}) = \|\mathbf{a}\|^2 / g$.*

Since any $L_{\min}(\mathbf{a})$ is a sublattice of $L^\perp(\mathbf{a})$ we have that

$$D^\perp(\mathbf{a}) \mid D_{\min}(\mathbf{a}). \tag{5}$$

This immediately gives the lower bound of Theorem 1.

1.3. **Description of the following sections.** In Section 2 we state some preliminary lemmas. In Section 3 we define and discuss the upper bounds $D^*(\mathbf{a})$, $D^{**}(\mathbf{a})$ and $D^{***}(\mathbf{a})$ for $D_{\min}(\mathbf{a})$, as in (4). We also prove Theorem 1. In Section 4 we discuss the arithmetic of $D(\mathbf{a})$. In Section 5 we describe the algorithms for computing $D^*(\mathbf{a})$ and $D_{\min}(\mathbf{a})$. In Section 6 we gives the results of computing $D_{\min}(\mathbf{a})$ for particular sequences of integer vectors $\mathbf{a}$. In Section 7 we evaluate for many sets of vectors $\mathbf{a} \in \mathbb{Z}^3$. Section 8 is devoted to the proofs of many of our results.

2. Lemmas

The following lemmas are needed for our constructions and proofs.

Lemma 4. *Given integer vectors* $\mathbf{a}' \in \mathbb{Z}_{n'}$, $\mathbf{a}'' \in \mathbb{Z}_{n''}$, *and matrices*

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

the matrix

$$M(\mathbf{a}' \mid \mathbf{a}'') := \begin{pmatrix} \mathbf{a}' & | & \mathbf{a}'' \\ \mathbf{a}'_2 & | & \mathbf{0}'' \\ \mathbf{a}'_3 & | & \mathbf{0}'' \\ \vdots & \vdots & \vdots \\ \mathbf{a}'_{n'} & | & \mathbf{0}'' \\ \mathbf{0}' & | & \mathbf{a}''_2 \\ \mathbf{0}' & | & \mathbf{a}''_3 \\ \vdots & \vdots & \vdots \\ \mathbf{0}' & | & \mathbf{a}''_{n''} \\ \lambda\mathbf{a}' & | & -\mu\mathbf{a}'' \end{pmatrix} \tag{6}$$

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

$$D(\mathbf{a}')D(\mathbf{a}'') \, \| \mathbf{a}' \mid \mathbf{a}'' \|^2 / g'. \tag{7}$$

In the matrix, $\mathbf{0}'$ and $\mathbf{0}''$ are zero vectors of lengths n' and n'' respectively. Note that for $n := n' + n'' \geq 3$ all matrices constructed using (6) will have at least one entry equal to 0.

Proof. The rows of $M(\mathbf{a}' \mid \mathbf{a}'')$ are easily seen to be pairwise orthogonal. Its determinant squared, being the product of the squared lengths of its rows, is

$$\| \mathbf{a}' \mid \mathbf{a}'' \|^2 \cdot (D(\mathbf{a}')^2 / \| \mathbf{a}' \|^2) \cdot (D(\mathbf{a}'')^2 / \| \mathbf{a}'' \|^2) \cdot (\lambda^2 \| \mathbf{a}' \|^2 + \mu^2 \| \mathbf{a}'' \|^2).$$

This simplifies to $\left(\| \mathbf{a}' \mid \mathbf{a}'' \|^2 \, D(\mathbf{a}')D(\mathbf{a}'')/g'\right)^2$, 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*

$$b_1 + b_2 + \cdots + b_k \le \frac{k}{n}(b_1 + b_2 + \cdots + b_n).$$

Furthermore if the b_k are not all equal then the inequality is strict for $k = 1, \ldots, n-1$.

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 $\mathbf{a}_2, \ldots, \mathbf{a}_n$ in $\mathbb{R}^n$ and an indeterminate row vector $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$, expand the determinant $\det M(\mathbf{y})$ of the matrix*

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

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

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

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

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

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

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

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

We see, (from choosing $\mathbf{d} = \mathbf{c}$ in the first place!) that in fact $\mathbf{c}$ is scaled so that its squared length $\| \mathbf{c} \|^2 := \sum_{j=1}^n c_j^2$ is equal to $\det M(\mathbf{c})$.

We note in passing that for $n = 3$ this identity takes the form

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

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

3. The upper bounds $D^*(\mathbf{a})$, $D^{**}(\mathbf{a})$ and $D^{***}(\mathbf{a})$ for $D_{\min}(\mathbf{a})$

Let us fix a nonzero integer vector $\mathbf{a} = (a_1, \ldots, a_n)$. As discussed earlier, we can assume that the components of $\mathbf{a}$ are nonnegative and in nondecreasing order. We first consider $D^*(\mathbf{a})$ and $D^{**}(\mathbf{a})$. They are both derived from Lemma 4, applied recursively. The stronger upper bound, $D^*(\mathbf{a})$, is obtained as follows. If $n = 1$ we have $D^*(\mathbf{a}) = D_{\min}(\mathbf{a}) = g = \| \mathbf{a} \|$ trivially, while if $n = 2$ we easily have $D^*(\mathbf{a}) = D_{\min}(\mathbf{a}) = \| \mathbf{a}/g \|^2 \; g$, where g is the gcd of the coordinates of $\mathbf{a}$. For larger n, we consider all possible 2-partitions $(\mathbf{a}' \mid \mathbf{a}'')$ of the multiset of components of $\mathbf{a}$. (Thus the order of the components of $\mathbf{a}$ is irrelevant here.) The construction of the lemma then gives us a formula (7) for $D(\mathbf{a})$ in terms of $D(\mathbf{a}')$ and $D(\mathbf{a}'')$ corresponding to matrices $M(\mathbf{a})$, $M(\mathbf{a}')$ and $M(\mathbf{a}'')$. Having chosen $M(\mathbf{a}')$ and $M(\mathbf{a}'')$ to be matrices with determinants $D^*(\mathbf{a}')$ and $D^*(\mathbf{a}'')$ respectively, and using (7), we define $D^*(\mathbf{a})$ to be the minimum, over all 2-partitions $(\mathbf{a}' \mid \mathbf{a}'')$, of the starred version of (7), namely

$$D^*(\mathbf{a}')D^*(\mathbf{a}'') \; \| \, \mathbf{a}' | \mathbf{a}'' \, \|^2 \; / g'. \tag{8}$$

The upper bound $D^{**}(\mathbf{a})$ uses Lemma 4 in a simpler way. Throughout the recursive process, $n'' = 1$, and the associated singleton is the largest component of the vector being 2-partitioned.

Define

$$D^{**}(\mathbf{a}) := \frac{||\mathbf{a}||^2}{g_n} \prod_{i=2}^{n-1} \frac{||\boldsymbol{\alpha}_i||^2/g_i^2}{\gcd\left(a_{i+1}/g_{i+1}, ||\boldsymbol{\alpha}_i||^2/g_i^2\right)} \tag{9}$$

where we have written $\boldsymbol{\alpha}_i$ and g_i for the truncations

$$\boldsymbol{\alpha}_i := (a_1, a_2, \ldots, a_i), \quad g_i := \gcd(a_1, a_2, \ldots, a_i), \quad i = 2, \ldots, n. \tag{10}$$

Theorem 7. *Given* $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ *we have*

$$D^*(\mathbf{a}) \le D^{**}(\mathbf{a}).$$

If the a_i *grow fast enough so that*

$$\frac{||\boldsymbol{\alpha}_i||^2}{g_i^2} \ge \frac{||\boldsymbol{\alpha}_{i-1}||^4}{g_{i-1}^4} \left(\prod_{j=2}^{i-1} \frac{||\boldsymbol{\alpha}_j||^2/g_j^2}{\gcd\left(a_{j+1}/g_{j+1}, ||\boldsymbol{\alpha}_j||^2/g_j^2\right)} \right)^2 \tag{11}$$

for all $i = 3, \ldots, n$, *then we have* $D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = D^{**}(\mathbf{a})$.

If the a_i *satisfy*

$$\frac{||\boldsymbol{\alpha}_{i-1}||^2}{g_{i-1}^2} \;\Big|\; \frac{a_i}{\gcd(a_i, g_{i-1})} \tag{12}$$

for all $i = 3, \ldots, n$ *then*

$$D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = \frac{||\mathbf{a}||^2}{g_n}.$$

Noting that $g_i \ge g_n = g$ for all i gives us our third and simplest bound

$$D_{\min}(\mathbf{a}) \le D^*(\mathbf{a}) \le D^{**}(\mathbf{a}) \le D^{***}(\mathbf{a}), \tag{13}$$

where

$$D^{***}(\mathbf{a}) := g^{3-2n}(a_1^2+a_2^2)(a_1^2+a_2^2+a_3^2)\cdots(a_1^2+\cdots+a_n^2). \tag{14}$$

For any a_1, a_2 with $\gcd(a_1,a_2)=1$ we can immediately produce infinitely many cases of equality in (13), as follows.

Corollary 8. *If* $\gcd(a_1,a_2)=1$ *and the* a_i *grow fast enough that*

$$||\boldsymbol{\alpha}_i||^2 \geq ||\boldsymbol{\alpha}_{i-1}||^4 \prod_{j=2}^{i-1} ||\boldsymbol{\alpha}_j||^4,$$

and

$$\gcd(a_i, ||\boldsymbol{\alpha}_{i-1}||^2) = 1,$$

for all $i=3,\ldots,n$*, then*

$$D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = \prod_{i=2}^{n} ||\boldsymbol{\alpha}_i||^2.$$

Similarly if $\gcd(a_1,a_2)=1$ the conditions to produce cases where the lower bound is sharp simplify. Recall these are the cases where the hyperplane orthogonal to $\mathbf{a}$ has an orthogonal basis.

Corollary 9. *If* $\gcd(a_1,a_2)=1$ *and for* $i=3,\ldots,n$

$$||\boldsymbol{\alpha}_{i-1}||^2 \mid a_i,$$

then

$$D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = ||\mathbf{a}||^2.$$

Since $D^{**}(\mathbf{a})$ is defined using one particular sequence of partitions in Lemma 4, while $D^*(\mathbf{a})$ is the minimum of $D(\mathbf{a})$ using all possible such partitions, we clearly have

$$D_{\min}(\mathbf{a}) \leq D^*(\mathbf{a}) \leq D^{**}(\mathbf{a}),$$

as in (4).

From Lemma 5 with $b_i = a_i^2$ $(i=2,\ldots,n)$ and $k=2,\ldots,n$ we obtain the simple bound

$$D^{***}(\mathbf{a}) \leq \frac{(n-1)!}{n^{n-2}g^{2n-3}} \| \mathbf{a} \|^{2n-2},$$

as claimed in (3). Also, the lemma shows that equality can occur here only when all the a_i are equal. Thus, assuming Theorem 7, we have proved both Theorem 1 and (4).

4. The arithmetic of $D(\mathbf{a})$

For a given vector $\mathbf{a} \in \mathbb{Z}^n$, write $\| \mathbf{a} \|^2 = r\ell^2$, where r is the *squarefree part of* $\| \mathbf{a} \|^2$. Then for $M(\mathbf{a})$ as in (1) we see that

$$\| \mathbf{a}_2 \|^2 \cdot \| \mathbf{a}_3 \|^2 \cdots \| \mathbf{a}_n \|^2$$

also has squarefree part equal to r. Thus any prime factor of r is a factor of both $\| \mathbf{a} \|^2$ and some $\| \mathbf{a}_i \|^2$. Let us use this fact to show that $D_{\min}((1,2,3)) = 42$. Now $\| (1,2,3) \|^2 = 14$,

so $\| \mathbf{a}_2 \|^2 \| \mathbf{a}_3 \|^2$ is of the form $14\ell^2$ for some ℓ. Thus $D(\mathbf{a})$ 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 both for

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & -2 & 1 \\ 4 & 1 & -2 \end{pmatrix} \quad \text{and for} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -1 \\ 5 & -4 & 1 \end{pmatrix},$$

each of determinant 42. We remark in passing that this example also shows that a matrix $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$ with $D(\mathbf{a}) = D_{\min}(\mathbf{a})$ need not be unique, even if left multiplication by a signed permutation matrix is considered not to 'essentially change' the matrix.

In fact, using (2), we have the following.

Proposition 10. *For $\mathbf{a}, \mathbf{a}_2, \ldots, \mathbf{a}_n$ as in (1), with $\| \mathbf{a} \|^2 = r\ell^2$ as above, we have that*

$$\| \mathbf{a}_2 \|^2 \cdot \| \mathbf{a}_3 \|^2 \cdots \| \mathbf{a}_n \|^2 = r\ell^2 s^2$$

for some integer s, and $D(\mathbf{a}) = r\ell^2 s$.

We also have the following corollary to Theorem 2 above.

Corollary 11. *The modulus of the determinant $D(\mathbf{a})$ of a matrix $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$ as in (3) is divisible by $\operatorname{lcm}_{i=1}^{n}(\| \mathbf{a}_i \|^2 / g_i')$, where g_i' is the* gcd *of the coordinates of $\mathbf{a}_i$.*

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

5. Algorithms for computing $D^*(\mathbf{a})$ and $D_{\min}(\mathbf{a})$

5.1. **Computing $D^*(\mathbf{a})$.** Let us fix a nonzero integer vector $\mathbf{a}$ of length n. If $n = 1$ we have $D^*(\mathbf{a}) = D_{\min}(\mathbf{a}) = g = \| \mathbf{a} \|$ trivially, while if $n = 2$ we have $D^*(\mathbf{a}) = D_{\min}(\mathbf{a}) = \| \mathbf{a}/g \|^2 \, g$, where g is the gcd of the coordinates of $\mathbf{a}$. For larger n we can proceed recursively, using the construction of Lemma 4, to get a good upper bound, $D^*(\mathbf{a})$ say, for $D_{\min}(\mathbf{a})$. Specifically, we apply that lemma to all possible 2-partitions of $\mathbf{a}$. Each such 2-partition enables us to write $\mathbf{a}^* = (\mathbf{a}' \mid \mathbf{a}'')$, where the coordinate multisets of $\mathbf{a}'$ and $\mathbf{a}''$ correspond to the 2-partition, and $\mathbf{a}^*$ is a vector whose coordinates are a permutation of those of $\mathbf{a}$. Then we can define $D^*(\mathbf{a})$ to be the minimum, over all such 2-partitions, of

$$D^*(\mathbf{a}') D^*(\mathbf{a}'') \, \| \mathbf{a} \|^2 / g',$$

as in (7) of Lemma 4, and with the notation used there.

We have implemented this algorithm in Maple: **Find-D^*($\mathbf{a}$)**. As we shall see in Section 6, $D^*(\mathbf{a})$ is often equal to $D_{\min}(\mathbf{a})$. However, they are not always equal. For instance, for

$\mathbf{a} = (1, 2, 3)$ the method gives $D^*(\mathbf{a}) = 70$, coming from the matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ -2 & 1 & 0 \\ 3 & 6 & 5 \end{pmatrix},$$

while in fact, as shown above, $D_{\min}(\mathbf{a}) = 42$.

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

5.2. **Computing $D_{\min}(\mathbf{a})$.** We work with a matrix of the form (1). The basic idea is to search for all matrices $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$ of determinant at most B, starting with $B := D^*(\mathbf{a})$. (We allow equality so that the search is guaranteed to succeed.)

We want

$$D(\mathbf{a}) = \| \mathbf{a} \| \cdot \| \mathbf{a}_2 \| \cdots \| \mathbf{a}_n \| \leq B. \tag{15}$$

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

$$1 \leq \| \mathbf{a}_2 \| \leq \| \mathbf{a}_3 \| \leq \cdots \leq \| \mathbf{a}_n \|, \tag{16}$$

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

$$\| \mathbf{a}_{\ell+1} \|^{n-\ell} \leq \| \mathbf{a}_{\ell+1} \| \cdots \| \mathbf{a}_n \| \leq \frac{B}{\| \mathbf{a} \| \| \mathbf{a}_2 \| \cdots \| \mathbf{a}_\ell \|}, \tag{17}$$

giving

$$\| \mathbf{a}_\ell \| \leq \| \mathbf{a}_{\ell+1} \| \leq \left(\frac{B}{\| \mathbf{a} \| \| \mathbf{a}_2 \| \cdots \| \mathbf{a}_\ell \|} \right)^{1/(n-\ell)} =: B_{\ell+1}, \tag{18}$$

say, while for $\ell = 1$

$$1 \leq \| \mathbf{a}_2 \| \leq \left(\frac{B}{\| \mathbf{a} \|} \right)^{1/(n-1)} =: B_2, \tag{19}$$

say.

A routine called **Row-finder**(A, L, U) is the most important one for finding the minimum $D_{\min}(\mathbf{a})$. Here A is a $(k-1) \times n$ integer matrix whose top row is $\mathbf{a}$ and whose rows are mutually orthogonal. Here $k \geq 2$ and $\mathbf{a} \in (\mathbb{Z}_{\geq 0})^n$, with components in nondecreasing order. Its purpose is to find all possible vectors $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}^n$ that are orthogonal to all rows of A and for which $L \leq \| \mathbf{h} \|^2 \leq U$. For suitable L, U such $\mathbf{h}$ 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 $(h_1, \ldots, h_{j-1}, h_j)$.

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 $\mathbf{a}$. To

construct all possible kth rows $\mathbf{h}$ 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 $\mathbf{a}$ are in nondecreasing order, $m_{k-1} = n$, the nonzero length of $\mathbf{a}$. The aim is to construct all $\mathbf{h}$ orthogonal to all rows of E (and hence of A), and with $\| \mathbf{h} \|^2 \leq U$. Having constructed such an $\mathbf{h}$, it is rejected if $\| \mathbf{h} \|^2 < L$, 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

$$h_j^2 \leq U - (h_1^2 + h_2^2 + \cdots h_{j-1}^2). \tag{20}$$

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 $\mathbf{e} = (e_1, \ldots, e_{j+1}, 0, \ldots, 0)$ 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 $\mathbf{e} = (e_1, \ldots, e_j, 0, \ldots, 0)$ 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 (20). 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 $\mathbf{a}$ has some equal components. This speedup is particularly effective for $\mathbf{a} = (1, 1, \ldots, 1)$ – 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**$(\mathbf{a})$, finds an $n \times n$ integer matrix whose first row is $\mathbf{a}$, whose rows are mutually orthogonal and whose determinant is as small as possible. It starts searching for such a matrix of determinant at most B, where B is the smallest integer we know of where $B = D(\mathbf{a})$ for some matrix $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$. We start with

$B := D^*(\mathbf{a})$, obtained using **Find-D^***$(\mathbf{a})$. 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 $\mathbf{a}$, with the nodes at level i labelled $A_i := (\mathbf{a}, \mathbf{a}_2, \dots, \mathbf{a}_i)$, and joined to the node labelled $A_{i-1} = (\mathbf{a}, \mathbf{a}_2, \dots, \mathbf{a}_{i-1})$. We then find all possible 2nd rows $\mathbf{a}_2$ using **Row-finder**$((\mathbf{a}), 1, U/\|\mathbf{a}\|)$. For $3 \le i \le n-1$ it finds all possible ith rows using

$$\textbf{Row-finder}(A_{i-1}, \|a_{i-1}\|, B_i) \tag{21}$$

from (18). The final row $\mathbf{a}_n$ is uniquely determined by the other $n-1$ rows, and is in fact specified by Lemma 6. It should satisfy

$$\|\mathbf{a}_{n-1}\| \quad \le \quad \|\mathbf{a}_n\| \quad \le \quad B_n \qquad \text{(defined by (18))},$$

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 new value $D(\mathbf{a}) < B$ is found along the way, then we can trim the search tree by redefining B as this $D(\mathbf{a})$ in the equations of Section 5.2.

The output of **Put-rows-together**$(\mathbf{a})$ is $D_{\min}(\mathbf{a})$, along with a matrix $M_{\min}(\mathbf{a})$, say, with determinant of modulus $D_{\min}(\mathbf{a})$.

6. Heinz encoding of integer multisets, and integer sequences

6.1. **Permuting or changing signs of the components of a, or removing its zeros.** Now multiplication of any $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$ on the right by a signed permutation matrix, while not changing $D(\mathbf{a})$, will in general change the order and the signs of (some) elements of $\mathbf{a}$. Thus we can confine our attention to $\mathbf{a}$ with nonnegative components. Also, since $D(\mathbf{a})$ depends only on the multiset of its components, we can choose the order of these components, so that they are in nondecreasing order.

If our given integer vector $\mathbf{a}$ contains no zero entries, then we can construct a matrix $M(\mathbf{a}^\#)$ from a matrix $M(\mathbf{a})$, where $\mathbf{a}^\# \in \mathbb{Z}^{n+\ell}$ is $\mathbf{a}$ with ℓ zeros added, as follows. We add ℓ extra rows and columns to $M(\mathbf{a})$, with an $\ell \times \ell$ identity matrix on the diagonal and all other new entries equal to 0. This construction of $M(\mathbf{a}^\#)$ shows immediately that $D_{\min}(\mathbf{a}^\#) \le D_{\min}(\mathbf{a})$. We suspect that they are actually equal, but, somewhat to our surprise, have not been able to prove this. Thus we state the following.

Open Problem. Find an example of a nonzero vector $(a_1, \dots, a_n) \in \mathbb{Z}^n$ with the property that

$$D_{\min}(0, a_1, \dots, a_n) < D_{\min}(a_1, \dots, a_n).$$

Alternatively, prove that no such vector exists.

Assuming our suspicion, we can confine our attention to those $\mathbf{a} \in \mathbb{N}^n$ whose components are in nonstrictly increasing order.

6.2. **Heinz encoding.** Given a finite multisubset $\{n_1, n_2, \dots, n_k\}$ of $\mathbb{N}$, 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 $\mathbb{N}$. See for instance sequence A344616 in [2]. Thus we can re-cast the values

of $D_{\min}(\mathbf{a})$ for multisets $\mathbf{a}$ 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 $D(k\mathbf{a}) = kD(\mathbf{a})$ 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

$$0, 1, 2, 2, 3, 5, 4, 6, 4, 10, 5, 6, 6, 17, 13, 8, 7, 18, 8, 22, 10, 26, 9, 42, 6, 37, 12,$$
$$18, 10, \underline{42}, 11, 40, 29, 50, 25, 20, 12, 65, 20, 24, 13, \underline{42}, 14, 54, 34, 82, 15, 32,$$
$$8, 38, 53, 38, 16, 78, 34, 114, 34, 101, 17, 30, 18, 122, 12, 48, 15, 30, 19, 102,$$
$$85, \underline{78}, 20, 132, 21, 145, 22, 66, 41, 205, 22, 104, 16, 170, \ldots .$$

This is sequence A327267. The information on this sequence also has a link to a table of the corresponding matrices of minimal determinant. We can do the same thing for the values of $D^*(\mathbf{a})$, obtaining the sequence $\{S^*(n)\}_{n\in\mathbb{N}}$ say, beginning

$$0, 1, 2, 2, 3, 5, 4, 6, 4, 10, 5, 6, 6, 17, 13, 8, 7, 18, 8, 22, 10, 26, 9, 42, 6, 37, 12,$$
$$18, 10, \underline{70}, 11, 40, 29, 50, 25, 20, 12, 65, 20, 24, 13, \underline{105}, 14, 54, 34, 82, 15,$$
$$32, 8, 38, 53, 38, 16, 78, 34, 114, 34, 101, 17, 30, 18, 122, 12, 48, 15, 30, 19,$$
$$102, 85, \underline{130}, 20, 132, 21, 145, 22, 66, 41, 205, 22, 104, 16, 170, \ldots .$$

This is sequence A328666. 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 $n = 30, 42, 70, \ldots$. This list of values of n is sequence A348557.)

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

6.3. **Further examples.** For $\mathbf{1}_n := (1, 1, \ldots, 1) \in \mathbb{Z}_n$ our program gives that, for $n = 1, 2, \ldots, 13$,

$$D_{\min}(\mathbf{1}_n) = D^*(\mathbf{1}_n) \tag{22}$$

with the values

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

(sequence A327271). Note that $\|\mathbf{1}_n\|^2 = n \mid A327271(n)$, in accordance with (5). We do not know whether (22) holds for all n. Since $(\mathbf{1}_n)$ corresponds under Heinz encoding to the integer $p_1^n = 2^n$, these are the values of $S(2^n) = S^*(2^n)$ for $n = 1, \ldots, 13$ for both the sequences A327267 and A328666 above.

For $(1, 2, 3, \ldots, n) \in \mathbb{Z}^n$, our program gives for $n = 1, 2, \ldots, 8$ that

$$D_{\min}((1, 2, 3, \ldots, n)) = 1, 5, 42, 90, 990, 5733, 6720, 39168, \tag{23}$$

(A327269), while

$$D^*((1, 2, 3, \ldots, n)) = 1, 5, 70, 150, 1650, 35490, 147000, 2142000. \tag{24}$$

Concerning elapsed timings, the computations for (23) on my desktop Mac, using Maple, took under 1 second for $n \le 5$, and 18 seconds, 73 seconds and 3688 seconds for $n = 6, 7, 8$ respectively. The computations for (24) were much faster: less than 1 second for $n \le 6$, 4 seconds for $n = 7$ and 46 seconds for $n = 8$.

Since $(1, 2, 3, \dots, n)$ corresponds to the integer $p_1 p_2 \cdots p_n$ in Heinz encoding, we have

$$S(p_1 p_2 \cdots p_n) = D_{\min}((1, 2, 3, \dots, n)).$$

Now take n to be of the form $n = 2^{2^k}$. We have that

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

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 $M(\mathbf{1}_{2^{k+1}})$ from two copies of a $2^k \times 2^k$ matrix $M(\mathbf{1}_{2^{k+1}})$ using Lemma 5, in particular equation (7) with $\mathbf{a}' = \mathbf{a}'' = \mathbf{1}_{2^k} \in \mathbb{Z}^{2^k}$ 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 A058891), or conceivably even that $S_2(k) = 2^{2^k - 1}$ for all k.

7. Some $n = 3$ results

7.1. **Results for some families.** In this section we discuss $D_{\min}(\mathbf{a})$ for various families of $\mathbf{a} \in \mathbb{Z}^3$. Different families give examples of $D_{\min}(\mathbf{a}) = D^{\perp}(\mathbf{a}) = ||\mathbf{a}||^2$, $D_{\min}(\mathbf{a}) = D^*(\mathbf{a})$, $D_{\min}(\mathbf{a}) < D^*(\mathbf{a})$, $D_{\min}(\mathbf{a}) = D^{**}(\mathbf{a})$ and $D_{\min}(\mathbf{a}) = D^{***}(\mathbf{a})$. Proofs are given in Section 8.4.

Theorem 12. *Let α, β be in $\mathbb{Z}$ and $\mathbf{a} = (b, a, \alpha a + \beta b)$ with $\gcd(a, b) = 1$.*

If $\beta a \equiv \alpha b \mod (\alpha^2 + \beta^2 + 1)$ then

$$D_{\min}(\mathbf{a}) = ||\mathbf{a}||^2. \tag{25}$$

More generally, if

$$4||\mathbf{a}||^2 \ge \frac{(\alpha^2 + \beta^2 + 1)^4}{\gcd(\alpha^2 + \beta^2 + 1, \beta a - \alpha b)^2} \tag{26}$$

then

$$D_{\min}(\mathbf{a}) = ||\mathbf{a}||^2 \frac{(\alpha^2 + \beta^2 + 1)}{\gcd(\alpha^2 + \beta^2 + 1, \beta a - \alpha b)}. \tag{27}$$

When $\alpha, \beta \ne 0$, and we have strict inequality in (26), and a/b is not equal to $\alpha/\beta, -(1+\beta^2)/\alpha\beta$ or $-\alpha\beta/(1+\alpha^2)$, we are guaranteed that $D_{\min}(\mathbf{a}) < D^*(\mathbf{a})$.

When (26) does not hold, (27) still gives an upper bound for $D_{\min}(\mathbf{a})$.

Thus we readily obtain infinitely many examples with $D_{\min}(\mathbf{a}) < D_{\min}^*(\mathbf{a})$, including cases where $D_{\min}(\mathbf{a}) = ||\mathbf{a}||^2$:

Corollary 13. *Suppose that $\mathbf{a} = (b, a, a + b)$ with $a, b \in \mathbb{N}$, $b \le a$ and $\gcd(a, b) = 1$. Then*

$$D_{\min}(\mathbf{a}) = ||\mathbf{a}||^2 \begin{cases} 1 & \text{if } a \equiv b \mod 3, \\ 3 & \text{otherwise,} \end{cases}$$

whereas

$$D^*(\mathbf{a}) = ||\mathbf{a}||^2 \begin{cases} \frac{1}{2}(a^2+b^2) & \text{if } a, b \text{ both odd,} \\ \min\left\{(a^2+b^2), \frac{1}{2}a^2+ab+b^2\right\} & \text{if } a \text{ even and } b \text{ odd,} \\ \min\left\{(a^2+b^2), \frac{1}{2}b^2+ab+a^2\right\} & \text{if } b \text{ even and } a \text{ odd.} \end{cases}$$

The next result is another case where we can check all the exceptions to (26).

Corollary 14. *Suppose that* $\mathbf{a} = (b, a, 2a+b)$ *with* $a, b \in \mathbb{N}$ *and* $\gcd(a,b) = 1$. *Then*

$$D_{\min}(\mathbf{a}) = ||\mathbf{a}||^2 \begin{cases} 1 & \text{if } a \text{ is even and } 3 \mid (a+b), \\ 2 & \text{if } a \text{ is odd and } 3 \mid (a+b), \\ 3 & \text{if } a \text{ is even and } 3 \nmid (a+b), \\ 6 & \text{if } a \text{ is odd and } 3 \nmid (a+b), \end{cases}$$

apart from $(1,1,3), (3,1,5), (2,3,8), (4,3,10)$, *whereas*

$$D^*(\mathbf{a}) = ||\mathbf{a}||^2 \min\left\{ \frac{a^2+b^2}{\gcd(5, 2a+b)}, \frac{5a^2+4ab+b^2}{\gcd(5,b)}, \frac{4a^2+4ab+2b^2}{\gcd(2,b)^2} \right\}.$$

We have other families with $D_{\min}(\mathbf{a}) < D^*(\mathbf{a})$, as the next result shows.

Corollary 15. *Suppose that* $\mathbf{a} = (b^2, ab, a^2)$ *with* a, b *in* $\mathbb{N}$, $b \le a$, $\gcd(a,b) = 1$. *Then*

$$D_{\min}(\mathbf{a}) = 2||\mathbf{a}||^2,$$

whereas

$$D^*(\mathbf{a}) = (a^2+b^2)||\mathbf{a}||^2.$$

When $a \ge 2$, these are cases where $D_{\min}(\mathbf{a}) < D^*(\mathbf{a})$. We saw in Theorem 7 that $D_{\min}(\mathbf{a}) = D^*(\mathbf{a})$ for $\mathbf{a} = (a_1, a_2, a_3)$ whenever a_3/g is suitably large relative to a_1/g_2 and a_2/g_2. In the $n = 3$ case we are able to save a factor of 4 in (11), as follows.

Proposition 16. *Suppose that* $\mathbf{a} = (ec, ac, b)$ *with* $a, b, c, e \in \mathbb{N}$, $\gcd(a,e) = 1$ *and* $\gcd(b,c) = 1$.

If $(a^2+e^2) \mid b$ *then* $D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = ||\mathbf{a}||^2$.

More generally, if

$$4||\mathbf{a}||^2 \ge \frac{(a^2+e^2)^4}{\gcd(b, a^2+e^2)^2}, \tag{28}$$

then

$$D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = ||\mathbf{a}||^2 \frac{(a^2+e^2)}{\gcd(b, a^2+e^2)}. \tag{29}$$

When (28) *does not hold,* (29) *still gives an upper bound.*

For $e = 1$ and $a = 1, 2$ we are able to check all the exceptions to (28), as follows.

Corollary 17. *For b, c in $\mathbb{N}$ with $\gcd(b,c)=1$*

$$D_{\min}(c,c,b) = D^*(c,c,b) = ||\mathbf{a}||^2 \begin{cases} 1 & \text{if } 2 \mid b, \\ 2 & \text{if } 2 \nmid b, \end{cases} \tag{30}$$

and

$$D_{\min}(c,2c,b) = D^*(c,2c,b) = ||\mathbf{a}||^2 \begin{cases} 1 & \text{if } 5 \mid b, \\ 5 & \text{if } 5 \nmid b, \end{cases} \tag{31}$$

except for $(1,2,b)$ with $b=1,2,3,4$ or 7 and $(2,4,1)$.

Of course Proposition 16 is appropriate only when $D^*(\mathbf{a}) = ||\mathbf{a}||^2 B^*$, where B^*, defined as the minimum of

$$\frac{(a^2+e^2)}{\gcd(b,a^2+e^2)}, \frac{(b^2+a^2c^2)}{\gcd(a,b)^2\gcd(e,b^2+a^2c^2)}, \text{ and } \frac{(b^2+e^2c^2)}{\gcd(e,b)^2\gcd(a,b^2+e^2c^2)},$$

is equal to the right-hand side of (29). Otherwise we can rearrange: e.g., $(1,a,1)$, $(1,a,a)$ should be treated as the cases $(1,1,a)$, $(a,a,1)$ of (30). The others: $(1,2,3)$, $(1,2,4)$ and $(1,2,7)$, are cases of Corollaries 13 or 15 or §7.2.

Likewise

$$D_{\min}(c,3c,b) = D^*(c,3c,b) = ||\mathbf{a}||^2 \frac{10}{\gcd(b,10)}, \tag{32}$$

for all $\gcd(b,c)=1$ with $5 \mid b$, or with $2 \mid b$ and $10c^2+b^2 \geq 625$, or with $10c^2+b^2 \geq 2500$. Some of these fall outside our list of 6000 but we can check for $c=1$ where we already know the exceptions $(1,3,4)$, $(1,3,9)$ from Corollaries 13 and 15. We find that (32) holds for all $(1,3,b)$ with $b \neq 1,2,3,4,7,9,19,23,29$.

Corollary 13 can be thought of as the case $k=1$ for the families $(b,a,a^k \pm b^k)$. For k sufficiently large these will be cases where we can apply Proposition 16, as follows.

Corollary 18. *Suppose that $\mathbf{a} = (b,a,a^k \pm b^k)$ with $a > b \geq 1$, $\gcd(a,b)=1$, $k \geq 2$.*

(a) *If $4 \mid k$ then*

$$D_{\min}(b,a,a^k-b^k) = D^*(b,a,a^k-b^k) = ||\mathbf{a}||^2,$$

(b) *If $2 \parallel k$ then*

$$D_{\min}(b,a,a^k+b^k) = D^*(b,a,a^k+b^k) = ||\mathbf{a}||^2.$$

(c) *In the remaining cases, if $k \geq 3$ then*

$$D^*(b,a,a^k \pm b^k) = ||\mathbf{a}||^2 \begin{cases} \frac{1}{2}(a^2+b^2) & \text{if } a \text{ and } b \text{ are odd}, \\ (a^2+b^2) & \text{if } a \text{ or } b \text{ is even}, \end{cases}$$

while if $k \geq 4$ then

$$D_{\min}(\mathbf{a}) = D^*(\mathbf{a}).$$

If $k = 3$ there are cases with $D_{\min}(\mathbf{a}) \neq D^*(\mathbf{a})$, but they are not so common. For example for $2 \leq a \leq 1000$ we have

$$D_{\min}(1, a, a^3 + 1) < D^*(1, a, a^3 + 1)$$

only when $a = 12, 14, 18, 86, 438, 508, 672, 968, 997, 998$, and

$$D_{\min}(1, a, a^3 - 1) < D^*(1, a, a^3 - 1)$$

only when $a = 2, 8, 22, 68, 658$. Of course there may well be infinitely many such a.

This just leaves $k = 2$ and $\mathbf{a} = (b, a, a^2 - b^2)$. When a, b have opposite parity we can use Theorem 12 to improve upon $D^*(\mathbf{a})$, as follows.

Proposition 19. *Suppose that* $\mathbf{a} = (b, a, a^2 - b^2)$ *with* $a > b \geq 1$ *and* $\gcd(a, b) = 1$. *Put* $g^* := \gcd(a, b^2 + 1) \cdot \gcd(b, a^2 + 1)$.

If a, b *have opposite parity, or are both odd with* $g^* \geq 3$, *then*

$$D_{\min}(\mathbf{a}) \leq \frac{||\mathbf{a}||^2(a^2 + b^2 + 1)}{g^*} < D^*(\mathbf{a}). \tag{33}$$

If a, b *are both odd with* $g^* = 1$ *then we only have*

$$D_{\min}(\mathbf{a}) \leq D^*(\mathbf{a}) = \frac{1}{2}(a^2 + b^2)||\mathbf{a}||^2. \tag{34}$$

There are cases where (33) and (34) are sharp, but also cases where they can be improved. For $b = 1$, Proposition 19 becomes

$$D_{\min}(1, a, a^2 - 1) \leq D^{\bigstar}(1, a, a^2 - 1) := ||\mathbf{a}||^2 \begin{cases} \frac{1}{2}(a^2 + 1) & \text{if } a \text{ is odd,} \\ \frac{1}{2}(a^2 + 2) & \text{if } a \text{ is even.} \end{cases}$$

For $a = 2, .., 401$ we have $D_{\min}(1, a, a^2 - 1) = D^{\bigstar}(1, a, a^2 - 1)$ only 62 out of 200 times for a even and 90 out of 200 times for a odd. Moreover if we beat $D^{\bigstar}(1, a, a^2 - 1)$ for a particular a then we can expect to beat it for a whole arithmetic progression. For example, when $a \equiv \pm 4 \mod 11$ or $a = \pm 2 \mod 14$ we will beat it by a factor tending to $\frac{10}{11}$ and $\frac{5}{7}$ respectively.

Similarly, Corollary 15 with $b = 1$ can be thought of as the $k = 2$ case of $(1, a, a^k)$. Applying Proposition 16 will give us cases of equality in (13), once $k \geq 4$. In fact, unlike the situation for $(1, a, a^3 \pm 1)$, the same is true for $(1, a, a^3)$, although crude size considerations are not enough there.

Proposition 20. *Suppose that* $\mathbf{a} = (1, a, a^k)$ *with* $a \geq 1$. *If* $k \geq 3$ *then*

$$D_{\min}(1, a, a^k) = D^*(1, a, a^k) = D^{***}(1, a, a^k) = (1 + a^2)||\mathbf{a}||^2.$$

7.2. **Computations for** $(1, a, a^3 \pm 1)$ **and** $(1, a, a^2 - 1)$**.** Suppose that $\mathbf{a} = (1, a, a^k + \delta)$, with $a^k + \delta = a^3 \pm 1$ or $a^2 - 1$ and that we have a 3×3 matrix A with pairwise orthogonal rows, first row $\mathbf{a}$ and other rows (x_i, y_i, z_i) $(i = 1, 2)$ with $\gcd(x_i, y_i, z_i) = 1$, $z_i \geq 0$. Then, from $x_i + ay_i + z_i(a^k + \delta) = 0$, we have

$$x_i = -\delta z_i + a\ell_i, \quad y_i = -\ell_i - a^{k-1}z_i, \quad \gcd(\ell_i, z_i) = 1.$$

If $|\det(A)| < ||\mathbf{a}||^2(a^2+L')/L$, where for $k=3$ we have $L'=1$ and $L=1$ or 2 as a is even or odd, and for $k=2$ we have $L=2$ and $L'=1$ or 2 as a is odd or even, then from Lemma 21 we can assume that

$$1 \le z_1 z_2 < \frac{(a^2+1)(a^2+L')}{2L\sqrt{(a^k+\delta)^2+a^2+1}} < \frac{(a^{2-\frac{k}{2}}+1)^2}{2L},$$

$$\begin{aligned}|l_1|az_2 + |\ell_2|az_1 &< \frac{(a^2+1)^{1/2}((a^k+\delta)^2+a^2)^{1/2}(a^2+L')}{||\mathbf{a}||L} + 2z_1z_2 \\ &< \frac{a(a^2+3)}{L} + 2z_1z_2\end{aligned}$$

and writing z for the minimum of z_1, z_2 and ℓ for the corresponding ℓ_i, that

$$1 \le z \le \frac{(a^{2-\frac{k}{2}}+1)}{\sqrt{2L}}, \qquad |\ell| < \frac{(a^2+3)}{zL} + 2.$$

For a given ℓ, z, $\gcd(\ell, z) = 1$, the matrix becomes

$$\begin{pmatrix} 1 & a & a^k+\delta \\ -\delta z + a\ell & -\ell - a^{k-1}z & z \\ X/G & Y/G & Z/G \end{pmatrix},$$

where

$$\begin{aligned} X &= \ell(a^k+\delta) + z(a + a^{k-1}(a^k+\delta)), \\ Y &= \ell a(a^k+\delta) - z(1+\delta(a^k+\delta)), \\ Z &= -\ell(a^2+1) + z(a\delta - a^{k-1}), \\ G &= \gcd(X,Y,Z). \end{aligned}$$

with the matrix having determinant of absolute value $||\mathbf{a}||(x^2+y^2+z^2)/G$. Then one checks whether

$$x^2+y^2+z^2 = (a\ell-\delta z)^2 + (\ell + a^{k-1}z)^2 + z^2 < G(a^2+L')/L. \tag{35}$$

Writing $aX - Y = z||\mathbf{a}||^2$, $(a^{k-1}-a\delta)Y - (1+\delta(a^k+\delta))Z = \ell||\mathbf{a}||^2$ we have

$$G \mid G_1 := \gcd(||\mathbf{a}||^2, Z), \quad G = \begin{cases} \frac{1}{2}G_1 & \text{if } a \text{ and } z \text{ are odd,} \\ G_1 & \text{else,} \end{cases}$$

the latter since $2 \parallel ||\mathbf{a}||^2$ and $X(a^2+1) + Z(a^k+\delta) = az||\mathbf{a}||^2$, where $\gcd(a^2+1, ||\mathbf{a}||^2) = 2$ for a odd and 1 for a even, and when a is odd G_1 is even, but G is even iff z is even.

We see that, for $k=2$, if we have an a with ℓ, z and G satisfying (35) then any $a' \equiv \pm a \mod G$ with the same z and $\ell' = \pm\ell$ will give $G \mid G'$ and

$$\lim_{a'\to\infty} \frac{(a'\ell' - \delta z)^2 + (\ell' + a'z)^2 + z^2}{G(a'^2+L')/2} = \frac{2(\ell^2+z^2)}{G},$$

saving in the limit at least this factor on $D^{\bigstar}(\mathbf{a})$.

For example $a=18$, $z=2$, $\ell=-1$, $G=11$ gives the $a \equiv \pm 4 \mod 11$, and $a=16$, $z=1$, $\ell=2$, $G=14$, gives the $a \equiv \pm 2 \mod 14$, examples mentioned above. The smallest factor encountered for $a \le 401$ was $a=289$ with $z=32$, $\ell=-41$, $G=378434$, or $z=9$,

$\ell = 7$, $G = 18433$, (saving a factor $0.01499\ldots$) with ratios $2(\ell^2 + z^2)/G = 0.01429\ldots$ or $0.01410\ldots$ for the $a \equiv \pm 289 \mod 378434$ or $a \equiv \pm 289 \mod 18433$. There may well be arithmetic progressions of a saving an arbitrarily small factor.

8. Proofs

8.1. **Proof of Theorem 2.**

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 $m = \min(a_1, \ldots, a_n)$. Our induction hypothesis is that there is an $\varepsilon = \pm 1$ such that for $i = 1, \ldots, n$ the cofactor A_i of the ith element a_i of the top row of $D^\perp(\mathbf{a})$ is equal to εa_i. Then the result follows on expanding $D^\perp(\mathbf{a})$ by its top row: $D^\perp(\mathbf{a}) = \sum_{i=1}^n a_i A_i$.

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

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

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 $\mathbf{a}$ with minimum element strictly less than m. Consider an integer vector $\mathbf{a}$ 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

$$mx_1 + a_2 x_2 + a_3 x_3 + \cdots + a_n x_n = 0, \tag{36}$$

which we can write as

$$mx_0 + rx_2 + a_3 x_3 + \cdots + a_n x_n = 0, \tag{37}$$

where $x_0 = x_1 + kx_2$. Then, by the induction hypothesis, we can assume that for the vector $\mathbf{a}' = (m, r, a_3, \dots, a_n)$ that the ith cofactor A_i' of $D^{\perp}(\mathbf{a}')$ 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 $\mathbf{u}' = (u_0, u_2, u_3, \dots, u_n)$ of (37) there is a basis solution $\mathbf{u} = (u_0 - ku_2, u_2, u_3, \dots, u_n)$ of (36). Thus the cofactors A_i of (36) are given by $A_1 = A_1' = \varepsilon m$, while for $j = 3, \dots, n$ 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 $A_2 = A_2' + kA_1' = \varepsilon(r + km) = \varepsilon a_2$. This proves the inductive step. □

8.2. **Proof of Theorem 7.**

Set

$$A_2 := \begin{pmatrix} a_1 & a_2 \\ a_2/g_2 & -a_1/g_2 \end{pmatrix}, \quad \det(A_2)^2 = \frac{||\boldsymbol{\alpha}_2||^4}{g_2^2},$$

and for $i = 3, \dots, n$, obtain A_i from A_{i-1} by appending an ith column $(a_i, 0, \dots, 0)^{\mathsf{T}}$ and then an ith row

$$\frac{a_i/g_i}{d_i}(a_1/g_{i-1}, \dots, a_{i-1}/g_{i-1}), -\frac{||\boldsymbol{\alpha}_{i-1}||^2/g_i g_{i-1}}{d_i},$$

where

$$d_i := \gcd(a_i/g_i, ||\boldsymbol{\alpha}_{i-1}||^2/g_{i-1}^2).$$

Here we have used the fact that $\gcd(a_i/g_i, ||\boldsymbol{\alpha}_{i-1}||^2/g_i g_{i-1}) = d_i$, which we leave as an exercise for the reader to check. Then A_i is an integer matrix with first row $(a_1, a_2, \dots, a_i)$ and i mutually orthogonal rows with

$$\det(A_i)^2 = ||\boldsymbol{\alpha}_i||^2 \left(\frac{\det(A_{i-1})^2}{||\boldsymbol{\alpha}_{i-1}||^2} \right) \frac{||\boldsymbol{\alpha}_{i-1}||^2 ||\boldsymbol{\alpha}_i||^2}{g_{i-1}^2 g_i^2 d_i^2} = \frac{||\boldsymbol{\alpha}_i||^4}{g_i^2 g_{i-1}^2 d_i^2} \det(A_{i-1})^2,$$

using (2). Hence

$$|\det(A_i)| = \frac{\displaystyle\prod_{j=2}^{i} ||\boldsymbol{\alpha}_j||^2}{g_i \displaystyle\prod_{j=2}^{i-1} g_j^2 d_{j+1}}$$

and the claimed upper bound is plain.

Suppose we have a matrix A with n mutually orthogonal rows, first row $(a_1, \dots, a_n)$ and a subsequent row $(x_1, x_2, \dots, x_n)$ with $x_n \neq 0$. From $\sum_{j=1}^{n} a_j x_j = 0$ we have

$$\frac{a_n}{g_n} x_n = -\frac{g_{n-1}}{g_n} \left(\frac{a_1}{g_{n-1}} x_1 + \cdots + \frac{a_{n-1}}{g_{n-1}} x_{n-1} \right)$$

and, since $\gcd(a_n, g_{n-1}) = g_n$, that $\frac{g_{n-1}}{g_n} \mid x_n$.

Applying the Cauchy-Schwarz inequality gives

$$a_n^2 x_n^2 = |a_1 x_1 + \cdots + a_{n-1} x_{n-1}|^2 \leq ||\boldsymbol{\alpha}_{n-1}||^2 (x_1^2 + \cdots + x_{n-1}^2)$$

and

$$x_1^2 + \cdots + x_n^2 \geq \frac{a_n^2 x_n^2}{||\boldsymbol{\alpha}_{n-1}||^2} + x_n^2 = \frac{||\boldsymbol{\alpha}_n||^2}{||\boldsymbol{\alpha}_{n-1}||^2} x_n^2 \geq \frac{||\boldsymbol{\alpha}_n||^2/g_n^2}{||\boldsymbol{\alpha}_{n-1}||^2/g_{n-1}^2}.$$

Hence if we have two such rows then

$$\det(A_n)^2 \geq ||\boldsymbol{\alpha}_n||^2 \left(\frac{||\boldsymbol{\alpha}_n||^2/g_n^2}{||\boldsymbol{\alpha}_{n-1}||^2/g_{n-1}^2} \right)^2,$$

exceeding the square of our upper bound if (11) holds for $i = n$.

Hence if (11) holds an optimal matrix can have at most one of the lower rows ending in something non-zero. We assume the last column takes the form $(a_n, 0, \ldots, 0, b)^{\mathsf{T}}$ attached to a matrix whose first row is $(a_1, \ldots, a_{n-1})$ and the first $(n-1)$ rows mutually orthogonal. Since the last row is orthogonal to the 2nd through $(n-1)$st rows, it must be a multiple of the first row $\lambda \left(\frac{a_1}{g_{n-1}}, \ldots, \frac{a_{n-1}}{g_{n-1}} \right)$. To be orthogonal to the first row the λ and b must satisfy

$$\lambda \left(\frac{g_{n-1}}{g_n} \right) \frac{||\boldsymbol{\alpha}_{n-1}||^2/g_{n-1}^2}{d_n} = -b \, \frac{a_n/g_n}{d_n}$$

and λ must be a multiple of $a_n/d_n g_n$ and the last row a multiple of the last row of A_n. So for a minimal determinant we can assume that the last row and column of A are the same as A_n and the first $(n-1)$ rows and columns are a set of mutually orthogonal vectors with first row $(a_1, \ldots, a_{n-1})$. Since A_2 gives the minimal for $n = 2$, the condition (11) for $i = 3, \ldots, n$ successively shows that one cannot beat the determinant of $A_3, \ldots, A_n$ for dimension $3, \ldots, n$.

Plainly when condition (12) holds the upper bound equals the lower bound. Moreover, since $a_i/g_i \geq ||\boldsymbol{\alpha}_{i-1}||^2/g_{i-1}^2$, we have $||\boldsymbol{\alpha}_i||^2/g_i^2 > a_i^2/g_i^2 \geq ||\boldsymbol{\alpha}_{i-1}||^4/g_{i-1}^4$ and condition (11) automatically holds. □

8.3. **Proof of Theorem 12.**

Suppose that $\mathbf{a} = (b, a, \alpha a + \beta b)$ with $\gcd(a, b) = 1$ and that A is a matrix with pairwise orthogonal rows, first row $\mathbf{a}$ and other rows $(x_i, y_i, z_i)\,(i = 1, 2)$. From $bx_i + ay_i + (\alpha a + \beta b)z_i = 0$ we have

$$x_i = -\beta z_i + t_i a, \quad y_i = -\alpha z_i - t_i b.$$

If either $t_i = 0$ then A essentially reduces to

$$A' = \begin{pmatrix} b & a & \alpha a + \beta b \\ -\beta & -\alpha & 1 \\ X/\ell & Y/\ell & Z/\ell \end{pmatrix}, \quad \begin{aligned} X &= a(\alpha^2 + \beta^2 + 1) - \beta Z \\ Y &= -b(\alpha^2 + \beta^2 + 1) - \alpha Z \\ Z &= \beta a - \alpha b \end{aligned}$$

where

$$\ell = \gcd(X, Y, Z) = \gcd(\alpha^2 + \beta^2 + 1, \alpha b - \beta a)$$

and

$$\det(A') = ||\mathbf{a}||^2(\alpha^2 + \beta^2 + 1)/\ell.$$

Suppose now that A has $t_1 t_2 \neq 0$. Setting

$$U_i = \left((\alpha^2 + \beta^2 + 1)z_i - (\beta a - \alpha b)t_i \right) / ||\mathbf{a}||$$

we have

$$\begin{aligned} x_1x_2+y_1y_2+z_1z_2 & \\ &= (\beta z_1 - t_1 a)(\beta z_2 - t_2 a) + (\alpha z_1 + t_1 b)(\alpha z_2 + t_2 b) + z_1 z_2 \\ &= \frac{||\mathbf{a}||^2}{\alpha^2+\beta^2+1}\left(U_1U_2 + t_1t_2\right) \end{aligned}$$

and

$$x_i^2+y_i^2+z_i^2 = \frac{||\mathbf{a}||^2}{\alpha^2+\beta^2+1}\left(U_i^2+t_i^2\right).$$

Hence, from the orthogonality of the second and third rows and writing $W = U_1/t_1$, the matrix has

$$\begin{aligned} \det(A)^2 &= \frac{||\mathbf{a}||^6}{(\alpha^2+\beta^2+1)^2}(U_1^2+t_1^2)(U_2^2+t_2^2) \\ &= \frac{t_1^2t_2^2||\mathbf{a}||^6}{(\alpha^2+\beta^2+1)^2}\left(2+W^2+W^{-2}\right) \geq \frac{4t_1^2t_2^2||\mathbf{a}||^6}{(\alpha^2+\beta^2+1)^2}, \end{aligned}$$

and condition (26) ensures that we cannot beat $|\det(A')|$.

The conditions $\alpha, \beta \neq 0$ and $a/b \neq \alpha/\beta$, $-(1+\beta^2)/\alpha\beta$ or $-\alpha\beta/(1+\alpha^2)$, ensure that A' has no zero entries, so that $D^*(\mathbf{a})$ does not come from A'. □

8.4. **Proofs of other $n = 3$ results.**

Proof of Corollary 13. For $a \equiv b \mod 3$ or $||\mathbf{a}||^2 = 2(a^2+ab+b^2) \geq 3^4/4$, the claim follows from Theorem 12. The remaining case $(1, 2, 3)$ checks. □

Proof of Corollary 14. For $6 \mid (a-2b)$ or $\gcd(6, a-2b) = 3$ and $||\mathbf{a}||^2 = 5a^2+4ab+2b^2 \geq 36$, or $\gcd(6, a-2b) = 2$ and $||\mathbf{a}||^2 \geq 81$, or $\gcd(6, a-2b) = 1$ and $||\mathbf{a}||^2 \geq 324$, the claim follows from Theorem 12. The remaining cases can be checked in the list. □

Proof of Corollary 15. We achieve $2||\mathbf{a}||^2$ with

$$\begin{pmatrix} b^2 & ab & a^2 \\ a & -(a+b) & b \\ a & a-b & -b \end{pmatrix}.$$

If the other rows are (x_i, y_i, z_i) then, since $b^2x_i + aby_i + a^2z_i = 0$, we must have $a \mid x_i$ and $b \mid z_i$. If an $x_i = 0$ we reduce to

$$\begin{pmatrix} b^2 & ab & a^2 \\ 0 & -a & b \\ a(a^2+b^2) & -b^3 & -ab^2 \end{pmatrix},$$

giving us the claimed value for $D^*(\mathbf{a})$. Likewise if $z_i = 0$. So suppose that the $x_i, z_i \neq 0$. Then $x_i^2+y_i^2+z_i^2 \geq (a^2+b^2)$, with $(a^2+b^2)^2 > (b^4+a^2b^2+a^4) = ||\mathbf{a}||^2$. So the determinant is greater than $||\mathbf{a}||^2$ and hence at least $2||\mathbf{a}||^2$. □

Proof of Proposition 16. Suppose that $x_i, y_i, z_i\,(i=1,2)$ are the second and third rows of an integer matrix A with pairwise orthogonal rows and first row (ec, ac, b). If $z_i = 0$ we reduce to

$$\begin{pmatrix} ec & ac & b \\ a & -e & 0 \\ be/G' & ba/G' & -c(a^2+e^2)/G' \end{pmatrix}, \qquad \begin{aligned} G' :=&\ \gcd(b, a^2+e^2), \\ |\det(A)| =&\ ||\mathbf{a}||^2(a^2+e^2)/G'. \end{aligned}$$

Otherwise, since $ecx_i + acy_i + bz_i = 0$, we have $c \mid z_i$ and can write

$$ex_i + ay_i = -bw_i, \quad z_i = cw_i, \quad w_i \neq 0.$$

So

$$\begin{aligned} x_1x_2 + y_1y_2 + z_1z_2 &= x_1x_2 + \frac{(bw_1 + ex_1)}{a}\frac{(bw_2 + ex_2)}{a} + w_1w_2c^2 \\ &= \frac{(a^2+e^2)}{a^2}\left(x_1 + \frac{bew_1}{a^2+e^2}\right)\left(x_2 + \frac{bew_2}{a^2+e^2}\right) + \frac{w_1w_2||\mathbf{a}||^2}{a^2+e^2} \\ &= \frac{||\mathbf{a}||^2}{a^2+e^2}\left(U_1U_2 + w_1w_2\right), \end{aligned}$$

where

$$U_i := \frac{(a^2+e^2)}{a||\mathbf{a}||}\left(x_i + \frac{bew_i}{a^2+e^2}\right), \quad i = 1, 2, \tag{38}$$

and

$$x_i^2 + y_i^2 + z_i^2 = \frac{||\mathbf{a}||^2}{(a^2+e^2)}\left(U_i^2 + w_i^2\right). \tag{39}$$

Orthogonality gives $U_1U_2 = -w_1w_2$, and with $U_1 = w_1W$,

$$\begin{aligned} \frac{\det(A)^2}{||\mathbf{a}||^2} &= (x_1^2+y_1^2+z_1^2)(x_2^2+y_2^2+z_2^2) \\ &= \frac{||\mathbf{a}||^4}{(a^2+e^2)^2}(U_1^2+w_1^2)\ \left(\frac{w_1^2w_2^2}{U_1^2} + w_2^2\right) \\ &= \frac{w_1^2w_2^2||\mathbf{a}||^4}{(a^2+e^2)^2}\left(2 + W^2 + \frac{1}{W^2}\right) \geq \frac{4w_1^2w_2^2||\mathbf{a}||^4}{(a^2+e^2)^2}. \end{aligned}$$

Hence by (28)

$$\det(A)^2 \geq \frac{4w_1^2w_2^2||\mathbf{a}||^6}{(a^2+e^2)^2} \geq \frac{4||\mathbf{a}||^6}{(a^2+e^2)^2} \geq \left(||\mathbf{a}||^2\frac{(a^2+e^2)}{\gcd(b, a^2+e^2)}\right)^2. \tag{40}$$

□

Proof of Corollary 17. For $a = 1$ we just need to check $(1, 1, 1)$. For $a = 2$ we are left to check the b, c with $5c^2 + b^2 \leq 156$ and $5 \nmid b$. □

Proof of Corollary 18. When $4 \mid k$ we have $a^2+b^2 \mid a^k-b^k$ and when $2 \parallel k$ we have $a^2+b^2 \mid a^k+b^k$ and (a) and (b) follow from Proposition 16.

Set

$$d = \begin{cases} 1 & \text{if } a \text{ or } b \text{ is even} \\ 2 & \text{if } a \text{ and } b \text{ are odd.} \end{cases}$$

For $k \geq 5$ with k odd or $2 \parallel k$ we have $\gcd(a^k-b^k, a^2+b^2) = d$ and for $k \geq 4$ with k odd or $4 \mid k$ we have $\gcd(a^k+b^k, a^2+b^2) = d$, so from Proposition 16 we will have

$$D_{\min}(b, a, a^k \pm b^k) = D^*(b, a, a^k \pm b^k) = ||\mathbf{a}||^2(a^2+b^2)/d$$

as long as

$$4||\mathbf{a}||^2 \geq (a^2+b^2)^4/d^2.$$

For $k \geq 4$ and $\mathbf{a} = (b, a, a^k+b^k)$ we have

$$||\mathbf{a}||^2 > (a^k+b^k)^2 \geq (a^4+b^4)^2$$

and for $k \geq 5$ and $\mathbf{a} = (b, a, a^k-b^k)$ we have

$$\begin{aligned} ||\mathbf{a}||^2 &> (a^k-b^k)^2 \geq (a^5-b^5)^2 \\ &= (a-b)^2(a^4+a^3b+a^2b^2+ab^3+b^4)^2 > (a^4+b^4)^2. \end{aligned}$$

Hence we have

$$4||\mathbf{a}||^2 > 4(a^4+b^4)^2 \geq (a^2+b^2)^4,$$

since $4(x^2+1)^2 \geq (x+1)^4$ for $x \geq 1$. □

Proof of Proposition 19. Taking $\alpha = a$, $\beta = -b$ in Theorem 12 we have

$$\gcd(\alpha^2+\beta^2+1, \beta a - \alpha b) = \gcd(a^2+b^2+1, 2ab) = g^*$$

and

$$D_{\min}(\mathbf{a}) \leq ||\mathbf{a}||^2 \frac{a^2+b^2+1}{g^*}, \tag{41}$$

while

$$D^*_{\min}(\mathbf{a}) = ||\mathbf{a}||^2 \min\left\{ \frac{a^2+b^2}{\gcd(2, a^2+b^2)}, \frac{a^2+(a^2-b^2)^2}{\gcd(b, a^2+1)}, \frac{b^2+(a^2-b^2)^2}{\gcd(a, b^2+1)} \right\}. \tag{42}$$

Since $(a^2-b^2)^2 \geq (a+b)^2 > a^2+b^2+1$ the two terms on the right of (42) certainly exceed (41). If a,b have opposite parity then $2 \mid \gcd(a, b^2+1)$ or $\gcd(b, a^2+1)$, and the first term on the right of (42) also exceeds (41), since $(a^2+b^2)||\mathbf{a}||^2 > \frac{1}{2}(a^2+b^2+1)||\mathbf{a}||^2$. Likewise if a, b are both odd and $\gcd(a, b^2+1)\gcd(b, a^2+1) \geq 3$, since $\frac{1}{3}(a^2+b^2+1)||\mathbf{a}||^2 < \frac{1}{2}(a^2+b^2)||\mathbf{a}||^2$. Finally, if a, b are odd and $g^* = 1$ our bound (41) is only $(a^2+b^2+1)||\mathbf{a}||^2$ while the first term in (42) gives $D^*_{\min}(\mathbf{a}) = \frac{1}{2}(a^2+b^2)||\mathbf{a}||^2$. □

In cases such as $(1, a, a^3)$, $(1, a, a^3 \pm 1)$ and $(1, a, a^2-1)$ where (28) does not hold, the proof of Proposition 16 gives us bounds on the size of the entries of a matrix beating our bound. The same could be done for Theorem 12.

For the proof of Proposition 20, we need the following result.

Lemma 21. *Suppose that A is a 3×3 matrix with pairwise orthogonal rows, with first row $\mathbf{a}=(ec,ac,b)$, $\gcd(a,e)=\gcd(b,c)=1$, and other rows (x_i,y_i,z_i), $i=1,2$. If*

$$|\det(A)|\le ||\mathbf{a}||^2 B,$$

then $c\mid z_i$, $ex_i\equiv -b(z_i/c) \mod a$, and $y_i=-(b(z_i/c)+ex_i)/a$, where

$$|z_1z_2|\le \frac{c^2(a^2+e^2)B}{2||\mathbf{a}||},\qquad |x_1x_2|\le \frac{(b^2+a^2c^2)B}{2||\mathbf{a}||},$$

and

$$|x_1z_2|+|x_2z_1|\le \frac{c(a^2+e^2)^{1/2}(b^2+a^2c^2)^{1/2}B}{||\mathbf{a}||}.$$

Proof. The first inequality follows from (40). Similarly, setting

$$V_i:=\frac{(b^2+a^2c^2)}{a||\mathbf{a}||}\left(w_i+\frac{bex_i}{b^2+a^2c^2}\right),\quad x_i^2+y_i^2+z_i^2=\frac{||\mathbf{a}||^2}{b^2+a^2c^2}(V_i^2+x_i^2),$$

and with U_i as in (38) and (39), we have

$$x_1x_2+y_1y_2+z_1z_2=\frac{||\mathbf{a}||^2}{b^2+a^2c^2}\left(V_1V_2+x_1x_2\right)=\frac{||\mathbf{a}||^2}{be}\left(U_1V_2-x_1w_2\right).$$

Hence, with $Hx_1=V_1$,

$$\begin{aligned}\det(A)^2&=\frac{||\mathbf{a}||^6}{(b^2+a^2c^2)^2}\left(V_1^2+x_1^2\right)\left(\frac{x_1^2x_2^2}{V_1^2}+x_2^2\right)\\&=\frac{x_1^2x_2^2||\mathbf{a}||^6}{(b^2+a^2c^2)^2}\left(2+H^2+H^{-2}\right)\ge\frac{4x_1^2x_2^2||\mathbf{a}||^6}{(b^2+a^2c^2)^2},\end{aligned}$$

and, with $K^2|x_1w_1w_2|=U_1^2|x_2|$,

$$\begin{aligned}\det(A)^2&=\frac{||\mathbf{a}||^6}{(a^2+e^2)(b^2+a^2c^2)}\left(U_1^2+w_1^2\right)\left(\frac{x_1^2w_2^2}{U_1^2}+x_2^2\right)\\&=\frac{||\mathbf{a}||^6}{(a^2+e^2)(b^2+a^2c^2)}\left(x_1^2w_2^2+x_2^2w_1^2+|x_1x_2w_1w_2|(K^2+K^{-2})\right)\\&\ge\frac{(|x_1w_2|+|x_2w_1|)^2||\mathbf{a}||^6}{(a^2+e^2)(b^2+a^2c^2)},\end{aligned}$$

and the claims are plain. □

Proof of Proposition 20. Since $\gcd(a^k,a^2+1)=1$ we have

$$D_{\min}(1,a,a^k)=||\mathbf{a}||^2(a^2+1)$$

as long as

$$4||\mathbf{a}||^2=4(a^{2k}+a^2+1)\ge(a^2+1)^4.$$

This holds for $k\ge 4$ and $a\ge 2$.

Checking $(1,1,1)$ and $(1,2,8)$ suppose that $\mathbf{a}=(1,a,a^3)$ with $a\ge 3$. Suppose that matrix A has pairwise orthogonal rows, first row $\mathbf{a}$ and other rows (x_i,y_i,z_i). From x_i+

$ay_i + a^3 z_i = 0$ we have $a \mid x_i$ and write $x_i = a\ell_i$, $y = -\ell_i - a^2 z_i$. If $z_i = 0$ we get $|\det(A)| = ||\mathbf{a}||(a^2+1)$ so we assume that the $z_i \geq 1$ with $|\det(A)| < ||\mathbf{a}||^2(a^2+1)$. By Lemma 21 we have

$$z_1 z_2 < \frac{(a^2+1)^2}{2||\mathbf{a}||} < a, \quad |\ell_1| z_2 + |\ell_2| z_1 < \frac{(a^2+1)^{3/2}(a^6+a^2)^{1/2}}{a||\mathbf{a}||} < a^2 + 2,$$

i.e. we can assume that $z_1 z_2 < a$ and $|\ell_1| z_2 + |\ell_2| z_1 \leq a^2 + 1$. Writing

$$x_1 x_2 + y_1 y_2 + z_1 z_2 = (a^2+1)\ell_1\ell_2 + (a^4+1) z_1 z_2 + a^2(\ell_1 z_2 + \ell_2 z_1),$$

plainly $\ell_1, \ell_2 \geq 0$ leads to $x_1x_2 + y_1y_2 + z_1z_2 \geq (a^4+1)$ and $\ell_1, \ell_2 < 0$ to $x_1x_2 + y_1y_2 + z_1z_2 \geq (a^2+1) + (a^4+1) - a^2(a^2+1) = 2$. So, from the orthogonality of the second and third rows, we can assume that $\ell_1 \geq 0$, $\ell_2 \leq 0$. Writing

$$0 = x_1 x_2 + y_1 y_2 + z_1 z_2 = (a^2+1)\ell_1\ell_2 + (a^4-1) z_1 z_2 + (a^2+1)(\ell_1 z_2 + \ell_2 z_1) + E,$$

we have

$$E := 2z_1 z_2 - \ell_1 z_2 - \ell_2 z_1 \equiv 0 \mod a^2 + 1,$$

with

$$E = 2z_1 z_2 - |\ell_1| z_2 + |\ell_2| z_1 \leq 2(z_1 - |\ell_1|) z_2 + (a^2 + 1) < 2a + a^2 + 1 < 2(a^2+1),$$

and

$$E \geq (2z_2 + |\ell_2|) z_1 - (a^2+1) > -(a^2+1).$$

Hence we are left with $E = 0$, or $E = a^2 + 1$ when $\ell_1 \leq z_1$.

If $E = 0$ we have $\ell_1 z_2 + \ell_2 z_1 = 2 z_1 z_2$ and $\ell_1\ell_2 + (a^2+1) z_1 z_2 = 0$. Assuming that $\gcd(x_i, y_i, z_i) = 1$ we have $\gcd(\ell_i, z_i) = 1$ and $z_1 \mid \ell_1 z_2$, $z_2 \mid \ell_2 z_1$ and $z_1 z_2 \mid \ell_1\ell_2$ give $z_1 = z_2 = 1$, $\ell_2 = 2 - \ell_1$ and $(\ell_1 - 1)^2 = a^2 + 2$, which plainly has no solution.

If $E = a^2 + 1$, $\ell_1 \leq z_1$ we get $(a^2+1)(z_1 z_2 - 1) = \ell_1|\ell_2| - 1$ where

$$-1 \leq \ell_1|\ell_2| - 1 \leq z_1|\ell_2| - 1 \leq (a^2+1) - 1.$$

Hence for this to be a multiple of $a^2 + 1$ we must have $z_1 = z_2 = 1$ and $\ell_1 = 1$, $\ell_2 = -1$ and $a^2 + 1 = 2$. So this also does not occur for $a > 1$.

□

9. Acknowledgements

We are pleased to acknowledge the financial assistance of the Edinburgh Mathematical Society Research Support Fund for the visit of the first author to Edinburgh, where some of this work was carried out. Also, we thank Craig Spencer for the computations in Corollary 18 for $k = 2, 3$.

References

[1] Maple 2021, Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario. Available at https://maplesoft.com.
[2] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, N. J. A. Sloane, editor, 2020. Available at https://oeis.org.

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

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