



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

Chris Pinner

Department of Mathematics, Kansas State University, Manhattan, Kansas
pinner@ksu.edu

Chris Smyth

School of Mathematics, University of Edinburgh, Edinburgh, Scotland U.K.
c.smyth@ed.ac.uk

Received: 2/16/22, Revised: 8/9/22, Accepted: 10/21/22, Published: 11/4/22

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 $D^*(\mathbf{a}) \leq D^{**}(\mathbf{a}) \leq D^{***}(\mathbf{a})$ 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 $n \geq 1$ 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

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

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

$$M(\mathbf{a})M(\mathbf{a})^T = \text{diag}(\|\mathbf{a}\|^2, \|\mathbf{a}_2\|^2, \|\mathbf{a}_3\|^2, \dots, \|\mathbf{a}_n\|^2),$$

so that

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

Here $\|\cdot\|$ 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 $L_{\min}(\mathbf{a})$.

Theorem 1. *For $n \geq 1$ and a vector $\mathbf{a} \in \mathbb{Z}^n$ whose components have greatest common divisor 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 [8]. 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 in Equations (11) and (16) 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, where necessary, 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 Inequalities (3) and Equation (16) only for completeness.

1.2. The Lattice Spanned by the Vector \mathbf{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 $\mathbf{u}_2, \dots, \mathbf{u}_n$ 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 $\mathbf{a}, \mathbf{u}_2, \dots, \mathbf{u}_n$. 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 greatest common divisor of the components of the vector \mathbf{a} .*

This is a known result – see for instance [7, p. 145]. The proof given in Section 8, much simpler than our original one, follows a suggestion of Lenstra (personal communication).

Corollary 1. *For $n = 2$ we have $D_{\min}(\mathbf{a}) = D^\perp(\mathbf{a}) = \|\mathbf{a}\|^2 / g$.*

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

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

In particular, taking $L(\mathbf{a}) = L_{\min}(\mathbf{a})$ gives the lower bound of Theorem 1.

1.3. Background Motivation

This work arose from a preliminary study of the approximation of the (logarithmic) Mahler measure

$$m(F) := \int_0^1 \cdots \int_0^1 \log |F(e^{2\pi i t_1}, \dots, e^{2\pi i t_k})| dt_1 \cdots dt_k \tag{6}$$

of a polynomial $F(z_1, \dots, z_n)$ with complex coefficients, by the Mahler measure of the 1-variable polynomial $F(z^{a_1}, \dots, z^{a_n})$ for a given integer exponent vector $\mathbf{a} := (a_1, \dots, a_n)$. Defining $\mu(\mathbf{a})$ to be the length of the shortest vector in the hyperplane in \mathbb{Z}^n orthogonal to \mathbf{a} , a result of Lawton [6] tells us that

$$\lim_{\mu(\mathbf{a}) \rightarrow \infty} m(F(z^{a_1}, \dots, z^{a_n})) = m(F).$$

It sometimes happens that $m(F(z^{a_1}, \dots, z^{a_n})) = m(F)$ exactly. An example is $F(z_1, z_2) = z_1 + z_2 + 2$ with $a_1 > 0, a_2 > 0$. However, it is of interest to know when this does not happen, so that then $m(F)$ is a limit point of distinct values $m(F(z^{a_1}, \dots, z^{a_n}))$. For this, we need a positive lower bound for $|m(F(z^{a_1}, \dots, z^{a_n})) - m(F)|$. This has been done by Boyd [1, Appendix 2] for the polynomial $F(z_1, z_2) = z_1 + z_2 + 1$. See also [2, pp. 404-5] for a discussion of

this issue. For more general lower bounds (actually asymptotic values) of this kind for 2-variable polynomials, see Condon [5] and Brunault *et al* [3, Theorem 5.1].

Since the integrand in Equation (6) is periodic of period 1 in each variable t_i , we can replace integration over the n -cube by integration over an n -box whose edges have directions $\mathbf{a}, \mathbf{a}_2, \dots, \mathbf{a}_n$ and is long in the \mathbf{a} direction, but short in the other directions. (Here $\mathbf{a}, \mathbf{a}_2, \dots, \mathbf{a}_n$ are as in Equation (1).) We hope to be able to use this to obtain the required lower bound, when it exists.

1.4. 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 Inequalities (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 give the results of computing $D_{\min}(\mathbf{a})$ for particular sequences of integer vectors \mathbf{a} . In Section 7 we evaluate it 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 1. *Given row vectors $\mathbf{a}' \in \mathbb{Z}^{n'}$, $\mathbf{a}'' \in \mathbb{Z}^{n''}$, and matrices*

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

the $n \times n$ matrix

$$M(\mathbf{a}' \mid \mathbf{a}'') := \left(\begin{array}{c|c} \mathbf{a}' & \mathbf{a}'' \\ \mathbf{a}'_2 & \mathbf{0}'' \\ \mathbf{a}'_3 & \mathbf{0}'' \\ \vdots & \vdots \\ \mathbf{a}'_{n'} & \mathbf{0}'' \\ \mathbf{0}' & \mathbf{a}''_2 \\ \mathbf{0}' & \mathbf{a}''_3 \\ \vdots & \vdots \\ \mathbf{0}' & \mathbf{a}''_{n''} \\ \lambda \mathbf{a}' & -\mu \mathbf{a}'' \end{array} \right) \tag{7}$$

lies in $\mathcal{L}(\mathbf{a}' \mid \mathbf{a}'')$. Here $n = n' + n''$, with $\lambda = \|\mathbf{a}''\|^2 / g'$ and $\mu = \|\mathbf{a}'\|^2 / g'$, where g' is the greatest common divisor of the components of the vector $(\|\mathbf{a}''\|^2 \mathbf{a}' \mid -\|\mathbf{a}'\|^2 \mathbf{a}'')$. Furthermore, its determinant is

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

In the matrix, $\mathbf{0}'$ and $\mathbf{0}''$ are zero vectors of lengths n' and n'' , respectively. Note that for $n \geq 3$ all matrices constructed using Equation (7) 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 $(\|\mathbf{a}' \mid \mathbf{a}''\|^2 D(\mathbf{a}')D(\mathbf{a}'')/g')^2$, giving the result. □

We note the following trivial result.

Lemma 2. *If $b_1 \leq b_2 \leq \dots \leq b_n$ then for $1 \leq k \leq n$ we have*

$$b_1 + b_2 + \dots + b_k \leq \frac{k}{n}(b_1 + b_2 + \dots + b_n).$$

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

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

Lemma 3. *Given $n \geq 2$, $n - 1$ linearly independent row vectors $\mathbf{a}_2, \dots, \mathbf{a}_n$ in \mathbb{R}^n and an indeterminate row vector $\mathbf{y} = (y_1, \dots, y_n)$ 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 $\mathbf{c} := (c_1, \dots, c_n)$ is orthogonal to the hyperplane $\langle \mathbf{a}_2, \dots, \mathbf{a}_n \rangle$.

(This generalizes the classical formula for the cross product $\mathbf{a}_2 \times \mathbf{a}_3$ in \mathbb{R}^3 .)

Proof. Let $\mathbf{d} = (d_1, \dots, d_n)$ be nonzero and orthogonal to $\langle \mathbf{a}_2, \dots, \mathbf{a}_n \rangle$. 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 $\mathbf{x} = (x_1, \dots, x_n)^T \in \mathbb{R}^n$ is a column vector. Since $\det M(\mathbf{d}) \neq 0$, this equation has a unique solution. Hence this solution is $\mathbf{x} = \mathbf{d}^T$, which is given by Cramer's Rule as

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

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

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 greatest common divisor of its components to make their greatest common divisor equal to 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 $\mathbf{a} = (a_1, \dots, a_n)$. 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 1, applied recursively. The stronger upper bound, $D^*(\mathbf{a})$, is obtained as follows. For $n = 1$ and 2, it is simply $D_{\min}(\mathbf{a})$. 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 formula (8) 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 Expression (8), we define $D^*(\mathbf{a})$ to be the minimum, over all 2-partitions $(\mathbf{a}' \mid \mathbf{a}'')$, of the starred version of (8), namely

$$D^*(\mathbf{a}')D^*(\mathbf{a}'') \|\mathbf{a}'\mathbf{a}''\|^2 / g'. \tag{9}$$

In particular, for $n = 3$ and $\mathbf{a} = (a, b, c)$, we have, explicitly from Lemma 1 using the three 2-partitions of \mathbf{a} , that

$$D^*(\mathbf{a}) = \|\mathbf{a}\|^2 \min(f(a, b, c), f(b, c, a), f(c, a, b)), \tag{10}$$

where

$$f(a, b, c) := \frac{a^2 + b^2}{\gcd(a, b) \gcd(ac, bc, a^2 + b^2)}.$$

The upper bound $D^{**}(\mathbf{a})$ uses Lemma 1 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

$$D^{**}(\mathbf{a}) := \frac{\|\mathbf{a}\|^2}{g_n} \prod_{i=2}^{n-1} \frac{\|\alpha_i\|^2/g_i^2}{\gcd(a_{i+1}/g_{i+1}, \|\alpha_i\|^2/g_i^2)} \tag{11}$$

where we have written α_i and g_i for the truncations

$$\alpha_i := (a_1, a_2, \dots, a_i), \quad g_i := \gcd(a_1, a_2, \dots, a_i), \quad i = 2, \dots, n. \tag{12}$$

Theorem 3. *Given $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ we have*

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

If the a_i grow fast enough so that

$$\frac{\|\alpha_i\|^2}{g_i^2} \geq \frac{\|\alpha_{i-1}\|^4}{g_{i-1}^4} \left(\prod_{j=2}^{i-1} \frac{\|\alpha_j\|^2/g_j^2}{\gcd(a_{j+1}/g_{j+1}, \|\alpha_j\|^2/g_j^2)} \right)^2 \tag{13}$$

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

If the a_i satisfy

$$\frac{\|\alpha_{i-1}\|^2}{g_{i-1}^2} \mid \frac{a_i}{\gcd(a_i, g_{i-1})} \tag{14}$$

for all $i = 3, \dots, n$ then

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

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

$$D_{\min}(\mathbf{a}) \leq D^*(\mathbf{a}) \leq D^{**}(\mathbf{a}) \leq D^{***}(\mathbf{a}), \tag{15}$$

where

$$D^{***}(\mathbf{a}) := g^{3-2n}(a_1^2 + a_2^2)(a_1^2 + a_2^2 + a_3^2) \cdots (a_1^2 + \cdots + a_n^2). \tag{16}$$

For any a_1, a_2 with $\gcd(a_1, a_2) = 1$ we can immediately produce infinitely many cases of equality in Inequalities (15), as follows.

Corollary 2. *If $\gcd(a_1, a_2) = 1$ and the a_i grow fast enough that*

$$\|\alpha_i\|^2 \geq \|\alpha_{i-1}\|^4 \prod_{j=2}^{i-1} \|\alpha_j\|^4,$$

and

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

for all $i = 3, \dots, n$, then

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

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

$$\|\alpha_{i-1}\|^2 \mid a_i,$$

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 1, 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 Inequalities (4).

From Lemma 2 with $b_i = a_i^2$ ($i = 2, \dots, n$) and $k = 2, \dots, n$ 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 Inequalities (3). Also, the lemma shows that equality can occur here only when all the a_i are equal. Thus, assuming Theorem 3, we have proved both Theorem 1 and Inequalities (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 Equation (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 Equation (2), we have the following.

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

$$\|\mathbf{a}_2\|^2 \cdot \|\mathbf{a}_3\|^2 \cdots \|\mathbf{a}_n\|^2 = r\ell^2 s^2 \tag{17}$$

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

Proof. Since $g = 1$ we have that $\|\mathbf{a}\|^4$ divides $D(\mathbf{a})^2$ from Division Statement (5), so that $r\ell^2 = \|\mathbf{a}\|^2$ divides $\|\mathbf{a}_2\|^2 \cdot \|\mathbf{a}_3\|^2 \cdots \|\mathbf{a}_n\|^2$, and hence $(r\ell^2)^2$ divides $D(\mathbf{a})^2$. Finally, writing $D(\mathbf{a}) = r\ell^2 s$ say, we have Equation (17). \square

We also have the following corollary to Theorem 2 above.

Corollary 4. *The modulus of the determinant $D(\mathbf{a})$ of a matrix $M(\mathbf{a}) \in \mathcal{L}(\mathbf{a})$ as in Equation (1) is divisible by $\text{lcm}_{i=1}^n(\|\mathbf{a}_i\|^2 / g'_i)$, where g'_i is the greatest common divisor 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 determinant of the matrix must be 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 greatest common divisor of the coordinates of \mathbf{a} . For larger n we can proceed recursively, using the construction of Lemma 1, 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 (8) of Lemma 1, 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 given in Equation (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

$$D(\mathbf{a}) = \|\mathbf{a}\| \cdot \|\mathbf{a}_2\| \cdots \|\mathbf{a}_n\| \leq B. \tag{18}$$

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

$$1 \leq \|\mathbf{a}_2\| \leq \|\mathbf{a}_3\| \leq \cdots \leq \|\mathbf{a}_n\|, \tag{19}$$

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

$$\|\mathbf{a}_{\ell+1}\|^{n-\ell} \leq \|\mathbf{a}_{\ell+1}\| \cdots \|\mathbf{a}_n\| \leq \frac{B}{\|\mathbf{a}\| \cdot \|\mathbf{a}_2\| \cdots \|\mathbf{a}_\ell\|}, \tag{20}$$

giving

$$\|\mathbf{a}_\ell\| \leq \|\mathbf{a}_{\ell+1}\| \leq \left(\frac{B}{\|\mathbf{a}\| \cdot \|\mathbf{a}_2\| \cdots \|\mathbf{a}_\ell\|} \right)^{1/(n-\ell)} =: B_{\ell+1}, \tag{21}$$

say, while for $\ell = 1$

$$1 \leq \|\mathbf{a}_2\| \leq \left(\frac{B}{\|\mathbf{a}\|} \right)^{1/(n-1)} =: B_2, \tag{22}$$

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 $\mathbf{h} = (h_1, \dots, h_n) \in \mathbb{Z}^n$ that are orthogonal to all rows of A and for which $L \leq \|\mathbf{h}\|^2 \leq U$. For suitable L and U such \mathbf{h} can be used for a possible k th 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, \dots, h_j) which are the possible first j components of a row of the kind being sought. The root is unlabelled. Obviously the edges of the tree are between nodes labelled (h_1, \dots, h_{j-1}) and $(h_1, \dots, h_{j-1}, h_j)$.

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 ℓ th row has ‘nonzero length’ (the length excluding its trailing zeroes on the right) denoted by 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 k th rows \mathbf{h} we classify the n columns of E , indexed by j , into four types. Defining $m_0 := 0$, we have

- type 1 : $m_{\ell-1} < j < m_\ell - 1$;
- type 2 : $m_{\ell-1} < j = m_\ell - 1$;
- type 3 : $m_{\ell-1} + 1 < j = m_\ell$;
- type 4 : $m_{\ell-1} + 1 = j = m_\ell$.

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, \dots, h_{j-1}) , to find all possible h_j we need to have

$$h_j^2 \leq U - (h_1^2 + h_2^2 + \dots + h_{j-1}^2). \tag{23}$$

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, and from the row $\mathbf{e} = (e_1, \dots, e_{j+1}, 0, \dots, 0)$ of E of nonzero length $j + 1$, we have the constraint

$$h_1e_1 + \dots + h_{j-1}e_{j-1} + h_je_j + h_{j+1}e_{j+1} = 0,$$

where $e_{j+1} \neq 0$ and h_1, \dots, h_{j-1} are known. Thus one has to find all integer solutions h_j, h_{j+1} to this equation, subject to $h_j^2 + h_{j+1}^2 \leq U - (h_1^2 + h_2^2 + \dots + h_{j-1}^2)$. 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 $\mathbf{e} = (e_1, \dots, e_j, 0, \dots, 0)$ of E of nonzero length j such that $e_j \neq 0$ and

$$h_1e_1 + \dots + h_{j-1}e_{j-1} + h_je_j = 0.$$

Thus h_j is uniquely determined by (h_1, \dots, h_{j-1}) . It must be an integer, and satisfy Inequality (23). 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 $\mathbf{a} = (1, 1, \dots, 1)$ – 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**($(\mathbf{a}), 1, B/\|\mathbf{a}\|$). For $3 \leq i \leq n - 1$ it finds all possible i th rows using

$$\mathbf{Row-finder}(A_{i-1}, \|a_{i-1}\|, B_i) \tag{24}$$

from Inequalities (21). The final row \mathbf{a}_n is uniquely determined by the other $n - 1$ rows, and is in fact specified by Lemma 3. It should satisfy

$$\|\mathbf{a}_{n-1}\| \leq \|\mathbf{a}_n\| \leq B_n \quad (\text{defined by Inequalities (21)}),$$

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 \mathbf{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 $D_{\min}(\mathbf{a}^\#) \leq D_{\min}(\mathbf{a})$. 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} , labelled so that $n_1 \leq n_2 \leq \dots \leq n_k$, its *Heinz number* is defined as $\prod_{i=1}^k p_{n_i}$, where p_n denotes the n th prime. This gives a bijection between such multisets and \mathbb{N} . See for instance sequence A344616 in [9]. 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, 42, 11, 40, 29, 50, 25, 20, 12, 65, 20, 24, 13, 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, 78, 20, 132, 21, 145, 22, 66, 41, 205, 22, 104, 16, 170,

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, 70, 11, 40, 29, 50, 25, 20, 12, 65, 20, 24, 13, 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, 130, 20, 132, 21, 145, 22, 66, 41, 205, 22, 104, 16, 170,

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 $n = 30, 42, 70, \dots$. 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 $\mathbf{1}_n := (1, 1, \dots, 1) \in \mathbb{Z}_n$ our program gives that, for $n = 1, 2, \dots, 13$,

$$D_{\min}(\mathbf{1}_n) = D^*(\mathbf{1}_n) \tag{25}$$

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 Division Statement (5). We do not know whether Equation (25) 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 $n = 1, \dots, 13$ for both the sequences A327267 and A328666 above.

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

$$D_{\min}((1, 2, 3, \dots, n)) = 1, 5, 42, 90, 990, 5733, 6720, 39168, \tag{26}$$

(A327269), while

$$D^*((1, 2, 3, \dots, n)) = 1, 5, 70, 150, 1650, 35490, 147000, 2142000. \tag{27}$$

Concerning elapsed timings, the computations for Equation (26) on a desktop Mac, using Maple, took under 1 second for $n \leq 5$, and 18 seconds, 73 seconds and 3688 seconds for $n = 6, 7, 8$ respectively. The computations for Equation (27) were much faster: less than 1 second for $n \leq 6$, with 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

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

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 $M(\mathbf{1}_{2^k})$ using Lemma 2, in particular (8) with $\mathbf{a}' = \mathbf{a}'' = \mathbf{1}_{2^k} \in \mathbb{Z}^{2^k}$ and $g' = 2^k$. This shows that $S_2^*(k+1) \leq 2S_2^*(k)^2$. Using $S_2^*(0) = 1$ this gives $S_2(k) \leq S_2^*(k) \leq 2^{2^k-1}$. We see that we have equality for $k \leq 3$. 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 $D_{\min}(\mathbf{a}) = D^{***}(\mathbf{a})$. The proofs are given in Sections 8.3 and 8.4.

Theorem 4. *Let $\alpha, \beta \in \mathbb{Z}$ and $\mathbf{a} = (b, a, \alpha a + \beta b)$ with $\gcd(a, b) = 1$.*

If $\beta a \equiv \alpha b \pmod{\alpha^2 + \beta^2 + 1}$ then

$$D_{\min}(\mathbf{a}) = \|\mathbf{a}\|^2. \tag{28}$$

More generally, if

$$4\|\mathbf{a}\|^2 \geq \frac{(\alpha^2 + \beta^2 + 1)^4}{\gcd(\alpha^2 + \beta^2 + 1, \beta a - \alpha b)^2} \tag{29}$$

then

$$D_{\min}(\mathbf{a}) = \|\mathbf{a}\|^2 \frac{(\alpha^2 + \beta^2 + 1)}{\gcd(\alpha^2 + \beta^2 + 1, \beta a - \alpha b)}. \tag{30}$$

When $\alpha, \beta \neq 0$, and we have strict inequality in Condition (29), and a/b is not equal to $\alpha/\beta, -(1 + \beta^2)/\alpha\beta$ or $-\alpha\beta/(1 + \alpha^2)$, we ensure that $D_{\min}(\mathbf{a}) < D^(\mathbf{a})$.*

When Condition (29) does not hold, Equation (30) 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 5. *Suppose that $\mathbf{a} = (b, a, a + b)$ with $a, b \in \mathbb{N}$, $b \leq a$ and $\gcd(a, b) = 1$.*

Then

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

whereas

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

The next result is another case where we can check all the exceptions to Condition (29).

Corollary 6. *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 7. *Suppose that $\mathbf{a} = (b^2, ab, a^2)$ with $a, b \in \mathbb{N}$, $b \leq a$, and $\gcd(a, b) = 1$. Then*

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

whereas

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

When $a \geq 2$, these are cases where $D_{\min}(\mathbf{a}) < D^*(\mathbf{a})$. We saw in Theorem 3 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 Condition (13), as follows.

Proposition 2. *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

$$4\|\mathbf{a}\|^2 \geq \frac{(a^2 + e^2)^4}{\gcd(b, a^2 + e^2)^2}, \tag{31}$$

then

$$D_{\min}(\mathbf{a}) = D^*(\mathbf{a}) = \|\mathbf{a}\|^2 \frac{(a^2 + e^2)}{\gcd(b, a^2 + e^2)}. \tag{32}$$

When Inequality (31) does not hold, Equation (32) still gives an upper bound.

For $e = 1$ and $a = 1, 2$ we are able to check all the exceptions to Inequalities (31), as follows.

Corollary 8. For b, c in \mathbb{N} with $\gcd(b, c) = 1$

$$D_{\min}(c, c, b) = D^*(c, c, b) = \|\mathbf{a}\|^2 \begin{cases} 1 & \text{if } 2 \mid b, \\ 2 & \text{if } 2 \nmid b, \end{cases} \tag{33}$$

and

$$D_{\min}(c, 2c, b) = D^*(c, 2c, b) = \|\mathbf{a}\|^2 \begin{cases} 1 & \text{if } 5 \mid b, \\ 5 & \text{if } 5 \nmid b, \end{cases} \tag{34}$$

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

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

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

is equal to the right-hand side of Equation (32). Otherwise we can rearrange: for example, $(1, a, 1)$, $(1, a, a)$ should be treated as the cases $(1, 1, a)$, $(a, a, 1)$ of Equation (33). The others: $(1, 2, 3)$, $(1, 2, 4)$ and $(1, 2, 7)$, are cases of Corollaries 5 or 7 or Subsection 7.2.

Likewise

$$D_{\min}(c, 3c, b) = D^*(c, 3c, b) = \|\mathbf{a}\|^2 \frac{10}{\gcd(b, 10)}, \tag{35}$$

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 5 and 7. We find that Equation (35) holds for all $(1, 3, b)$ with $b \neq 1, 2, 3, 4, 7, 9, 19, 23, 29$.

Corollary 5 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 2, as follows.

Corollary 9. 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 $2 \parallel k$ (that is, $2 \mid k$ but $2^2 \nmid k$) 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 4 to improve upon $D^*(\mathbf{a})$, as follows.

Proposition 3. *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*

$$D_{\min}(\mathbf{a}) \leq \frac{\|\mathbf{a}\|^2(a^2 + b^2 + 1)}{g^*} < D^*(\mathbf{a}). \tag{36}$$

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

$$D_{\min}(\mathbf{a}) \leq D^*(\mathbf{a}) = \frac{1}{2}(a^2 + b^2)\|\mathbf{a}\|^2. \tag{37}$$

There are cases where the Inequalities (36) and (37) are sharp, but also cases where they can be improved. For $b = 1$, Proposition 3 becomes

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

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

Similarly, Corollary 7 with $b = 1$ can be thought of as the $k = 2$ case of $(1, a, a^k)$. Applying Proposition 2 will give us cases of equality in Inequalities (15), 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 4. *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 for $i = 1, 2$ other rows (x_i, y_i, z_i) 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 4 we can assume that

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

$$\begin{aligned} |l_1|az_2 + |l_2|az_1 &< \frac{(a^2 + 1)^{1/2}((a^k + \delta)^2 + a^2)^{1/2}(a^2 + L')}{\|\mathbf{a}\|L} + 2z_1 z_2 \\ &< \frac{a(a^2 + 3)}{L} + 2z_1 z_2 \end{aligned}$$

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

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

For a given $\ell, z, \gcd(\ell, z) = 1$, 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

$$x^2 + y^2 + z^2 = (a\ell - \delta z)^2 + (\ell + a^{k-1}z)^2 + z^2 < G(a^2 + L')/L. \tag{38}$$

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

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

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. When a is odd G_1 is even, but G is even if and only if z is even.

We see that, for $k = 2$, if we have an a with ℓ, z and G satisfying Inequality (38) then any $a' \equiv \pm a \pmod G$ with the same z and $\ell' = \pm\ell$ will give $G \mid G'$ and

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

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

For example, $a = 18, z = 2, \ell = -1, G = 11$ gives $a \equiv \pm 4 \pmod{11}$, and $a = 16, z = 1, \ell = 2, G = 14$ gives $a \equiv \pm 2 \pmod{14}$, examples mentioned above. The smallest factor encountered for $a \leq 401$ was $a = 289$ with $z = 32, \ell = -41, G = 378434$, or $z = 9, \ell = 7, G = 18433$, (saving a factor $0.01499\dots$) with ratios $2(\ell^2 + z^2)/G = 0.01429\dots$ or $0.01410\dots$ for $a \equiv \pm 289 \pmod{378434}$ or $a \equiv \pm 289 \pmod{18433}$. 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 can clearly assume that $g = 1$, as the result for arbitrary g then follows immediately. Next, we easily see that the lattice $L^\perp(\mathbf{a})$ consists of the vectors $\mathbf{x} \in \mathbb{Z}^n$ for which $\mathbf{a} \cdot \mathbf{x}$ is a multiple of $\|\mathbf{a}\|^2$. Then choose $\mathbf{u} \in \mathbb{Z}^n$ such that $\mathbf{a} \cdot \mathbf{u} = 1$, so that for the factor group $\mathbb{Z}^n/L^\perp(\mathbf{a})$ we can take as coset representatives $L^\perp(\mathbf{a}) + j\mathbf{u}, j = 0, 1, \dots, \|\mathbf{a}\|^2 - 1$. Thus it has cardinality $\|\mathbf{a}\|^2$, which, by (for instance) [4, Lemma 1 of Chapter 1], is also $D^\perp(\mathbf{a})$. \square

8.2. Proof of Theorem 3

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 i th column $(a_i, 0, \dots, 0)^\top$ and then an i th 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 $\gcd(a_i/g_i, \|\alpha_{i-1}\|^2/g_i g_{i-1}) = d_i$, 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

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

using Equation (2). Hence

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

and the claimed upper bound is plain.

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

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

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

$$a_n^2 x_n^2 = |a_1 x_1 + \dots + a_{n-1} x_{n-1}|^2 \leq \|\alpha_{n-1}\|^2 (x_1^2 + \dots + x_{n-1}^2)$$

and

$$x_1^2 + \dots + x_n^2 \geq \frac{a_n^2 x_n^2}{\|\alpha_{n-1}\|^2} + x_n^2 = \frac{\|\alpha_n\|^2}{\|\alpha_{n-1}\|^2} x_n^2 \geq \frac{\|\alpha_n\|^2/g_n^2}{\|\alpha_{n-1}\|^2/g_{n-1}^2}.$$

Hence if we have two such rows then

$$\det(A_n)^2 \geq \|\alpha_n\|^2 \left(\frac{\|\alpha_n\|^2/g_n^2}{\|\alpha_{n-1}\|^2/g_{n-1}^2} \right)^2,$$

exceeding the square of our upper bound if Condition (13) holds for $i = n$. Thus if (13) 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 $(a_n, 0, \dots, 0, b)^\top$ attached to a matrix whose first row is (a_1, \dots, a_{n-1}) and the first $(n - 1)$ rows are mutually orthogonal. Since the last row is orthogonal to the second through $(n - 1)$ st rows, it must be a multiple of the first row $\lambda \left(\frac{a_1}{g_{n-1}}, \dots, \frac{a_{n-1}}{g_{n-1}} \right)$. To be orthogonal to the first row, λ and b must satisfy

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

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, \dots, a_{n-1}) . Since A_2 gives the minimal determinant for $n = 2$, the Condition (13) for $i = 3, \dots, n$ successively shows that one cannot beat the determinant of A_3, \dots, A_n for dimensions $3, \dots, n$.

Plainly, when Condition (14) holds, the upper bound equals the lower bound. Moreover, since $a_i/g_i \geq \|\alpha_{i-1}\|^2/g_{i-1}^2$, we have $\|\alpha_i\|^2/g_i^2 > a_i^2/g_i^2 \geq \|\alpha_{i-1}\|^4/g_{i-1}^4$ and Condition (13) automatically holds. \square

8.3. Proof of Theorem 4

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

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

we have

$$\begin{aligned} x_1 x_2 + y_1 y_2 + z_1 z_2 &= (\beta z_1 - t_1 a)(\beta z_2 - t_2 a) + (\alpha z_1 + t_1 b)(\alpha z_2 + t_2 b) + z_1 z_2 \\ &= \frac{\|\mathbf{a}\|^2}{\alpha^2 + \beta^2 + 1} (U_1 U_2 + t_1 t_2) \end{aligned}$$

and

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

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

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

and Condition (29) 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' . \square

8.4. Proofs of Other $n = 3$ Results

In this section, the proofs of formulae for $D^*(\mathbf{a})$ follow directly from Equation (10).

Proof of Corollary 5. For $a \equiv b \pmod 3$ or $\|\mathbf{a}\|^2 = 2(a^2 + ab + b^2) \geq 3^4/4$, the claim follows from Theorem 4. The remaining case $(1, 2, 3)$ checks out, since we saw in Section 4 that $D_{\min}((1, 2, 3)) = 42$. \square

Proof of Corollary 6. 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 4. The remaining cases can be checked from sequence A327267 in [9], as discussed in Section 6. \square

Proof of Corollary 7. 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 $2\|\mathbf{a}\|^2$. \square

Proof of Proposition 2. 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

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

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

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

where

$$U_i := \frac{(a^2 + e^2)}{a\|\mathbf{a}\|} \left(x_i + \frac{bew_i}{a^2 + e^2}\right), \quad i = 1, 2, \tag{39}$$

and

$$x_i^2 + y_i^2 + z_i^2 = \frac{\|\mathbf{a}\|^2}{(a^2 + e^2)} (U_i^2 + w_i^2). \tag{40}$$

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 Inequalities (31),

$$\det(A)^2 \geq \frac{4w_1^2w_2^2\|\mathbf{a}\|^6}{(a^2 + e^2)^2} \geq \frac{4\|\mathbf{a}\|^6}{(a^2 + e^2)^2} \geq \left(\|\mathbf{a}\|^2 \frac{(a^2 + e^2)}{\gcd(b, a^2 + e^2)}\right)^2. \tag{41}$$

□

Proof of Corollary 8. 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 9. 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 2.

Set

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

Next, note that for $\varepsilon = \pm 1$ and $k \geq 4$ we have

$$\gcd(a^k + \varepsilon b^k, a^2 + b^2) = \gcd(a^{k-2} - \varepsilon b^{k-2}, a^2 + b^2) = \gcd(a^{k-4} + \varepsilon b^{k-4}, a^2 + b^2).$$

Using this identity we see that for $k \geq 5$ with k odd or $2 \parallel k$ we have the identity $\gcd(a^k - b^k, a^2 + b^2) = d$, and for $k \geq 4$ with k odd or $4 \mid k$ we have similarly $\gcd(a^k + b^k, a^2 + b^2) = d$. Thus from Proposition 2 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 3. Taking $\alpha = a, \beta = -b$ in Theorem 4 we have

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

and

$$D_{\min}(\mathbf{a}) \leq \|\mathbf{a}\|^2 \frac{a^2 + b^2 + 1}{g^*}, \tag{42}$$

while, using Equation (10),

$$D^*(\mathbf{a}) = \|\mathbf{a}\|^2 \min \left\{ \frac{a^2 + b^2}{\gcd(2, a^2 + b^2)}, \frac{a^2 + (a^2 - b^2)^2}{\gcd(b, a^2 + 1)}, \frac{b^2 + (a^2 - b^2)^2}{\gcd(a, b^2 + 1)} \right\}. \tag{43}$$

Since $(a^2 - b^2)^2 \geq (a + b)^2 > a^2 + b^2 + 1$ the two right-most terms of Equation (43) certainly exceed the upper bound in Inequality (42). 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 Equation (43) also exceeds the bound in Inequality (42), 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 in Inequality (42) is only $(a^2 + b^2 + 1)\|\mathbf{a}\|^2$ while the first term in Equation (43) gives $D^*(\mathbf{a}) = \frac{1}{2}(a^2 + b^2)\|\mathbf{a}\|^2$. \square

In cases such as $(1, a, a^3)$, $(1, a, a^3 \pm 1)$ and $(1, a, a^2 - 1)$ where Inequality (31) does not hold, the proof of Proposition 2 gives us bounds on the size of the entries of a matrix beating our bound. The same could be done for Theorem 4.

For the proof of Proposition 4, we need the following result.

Lemma 4. *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*

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

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

$$|z_1 z_2| \leq \frac{c^2(a^2 + e^2)B}{2\|\mathbf{a}\|}, \quad |x_1 x_2| \leq \frac{(b^2 + a^2 c^2)B}{2\|\mathbf{a}\|},$$

and

$$|x_1 z_2| + |x_2 z_1| \leq \frac{c(a^2 + e^2)^{1/2}(b^2 + a^2 c^2)^{1/2}B}{\|\mathbf{a}\|}.$$

Proof. The first inequality follows from Inequalities (41). Similarly, setting

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

and with U_i as in Equation (39) and Equation (40), we have

$$x_1 x_2 + y_1 y_2 + z_1 z_2 = \frac{\|\mathbf{a}\|^2}{b^2 + a^2 c^2} (V_1 V_2 + x_1 x_2) = \frac{\|\mathbf{a}\|^2}{be} (U_1 V_2 - x_1 w_2).$$

Hence, with $Hx_1 = V_1$,

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

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

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

and the claims are plain. □

Proof of Proposition 4. 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

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

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

Checking $(1, 1, 1)$ and $(1, 2, 8)$ suppose that $\mathbf{a} = (1, a, a^3)$ with $a \geq 3$. Suppose that matrix A has pairwise orthogonal rows, first row \mathbf{a} and other rows (x_i, y_i, z_i) . From $x_i + ay_i + a^3z_i = 0$ we have $a \mid x_i$ and write $x_i = al_i, y = -l_i - a^2z_i$. If $z_i = 0$ we get $|\det(A)| = \|\mathbf{a}\|(a^2 + 1)$ so we restrict our attention to the $z_i \geq 1$ with $|\det(A)| < \|\mathbf{a}\|^2(a^2 + 1)$. By Lemma 4 we have

$$z_1z_2 < \frac{(a^2 + 1)^2}{2\|\mathbf{a}\|} < a, \quad |\ell_1|z_2 + |\ell_2|z_1 < \frac{(a^2 + 1)^{3/2}(a^6 + a^2)^{1/2}}{a\|\mathbf{a}\|} < a^2 + 2;$$

that is, we can assume that $z_1z_2 < a$ and $|\ell_1|z_2 + |\ell_2|z_1 \leq a^2 + 1$. Writing

$$x_1x_2 + y_1y_2 + z_1z_2 = (a^2 + 1)\ell_1\ell_2 + (a^4 + 1)z_1z_2 + a^2(\ell_1z_2 + \ell_2z_1),$$

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

$$0 = x_1x_2 + y_1y_2 + z_1z_2 = (a^2 + 1)\ell_1\ell_2 + (a^4 - 1)z_1z_2 + (a^2 + 1)(\ell_1z_2 + \ell_2z_1) + E,$$

we have

$$E := 2z_1z_2 - \ell_1z_2 - \ell_2z_1 \equiv 0 \pmod{a^2 + 1},$$

with

$$E = 2z_1z_2 - |\ell_1|z_2 + |\ell_2|z_1 \leq 2(z_1 - |\ell_1|)z_2 + (a^2 + 1) < 2a + a^2 + 1 < 2(a^2 + 1),$$

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 $\ell_1 z_2 + \ell_2 z_1 = 2z_1 z_2$ 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 $a > 1$. \square

Acknowledgements. We are grateful to the referee for carefully reading our submitted manuscript and making some helpful remarks. Also, 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. Finally, we thank Craig Spencer for the computations in Corollary 9 for $k = 2, 3$.

References

- [1] D. Boyd, Speculations concerning the range of Mahler's measure, *Canad. Math. Bull.* **24** (1981), no. 4, 453–469.
- [2] D. Boyd and M. Mossinghoff, Small limit points of Mahler's measure, *Exp. Math.* **14** (2005), no. 4, 403–414.
- [3] F. Brunault, A. Guilloux, M. Mehrabdollahei, R. Pengo, Limits of Mahler measures in multiple variables, <https://arxiv.org/pdf/2203.12259.pdf>.
- [4] J. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1959.
- [5] J. Condon, Asymptotic expansion of the difference of two Mahler measures, *J. Number Theory* **132** (2012), no. 9, 1962–1983.
- [6] W. Lawton, A problem of Boyd concerning geometric means of polynomials, *J. Number Theory* **16** (1983), no. 3, 356–362.
- [7] H. Lenstra Jr., Lattices, in *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, 127–181, Math. Sci. Res. Inst. Publ., **44**, Cambridge Univ. Press, Cambridge, 2008.
- [8] *Maple 2021*, Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario, 2021, available at <https://maplesoft.com>.
- [9] *The On-Line Encyclopedia of Integer Sequences*, N. J. A. Sloane, editor, OEIS Foundation Inc., 2020, available at <https://oeis.org>.