BASES OF MINIMAL VECTORS IN LATTICES, III

JACQUES MARTINET AND ACHILL SCHÜRMANN

ABSTRACT. We prove that all Euclidean lattices of dimension \( n \leq 9 \) which are generated by their minimal vectors, also possess a basis of minimal vectors. By providing a new counterexample, we show that this is not the case for all dimensions \( n \geq 10 \).

1. Introduction

In their paper [CS95], Conway and Sloane constructed an example of an 11-dimensional lattice generated by its minimal vectors, but having no basis of minimal vectors. They left open the question of the existence of such lattices in lower dimensions. In [Mar07], the first author proved that such lattices do not exist in dimensions \( n \leq 8 \), leaving open their existence in dimension 9 and 10. In this paper we fully resolve this question.

Theorem 1.1. A lattice of dimension \( n \leq 9 \) which is generated by its minimal vectors, has also a basis of minimal vectors. In all dimensions \( n \geq 10 \) there exist lattices which are generated by their minimal vectors, but have no basis of minimal vectors.

For standard terminology on lattices used here and in the sequel we refer the reader to [Mar03]. Given, an \( n \)-dimensional Euclidean vector space \( E \), we say that a lattice \( \Lambda \subset E \) is well rounded if its minimal vectors span \( E \). Any system of \( n \) independent minimal vectors then generates a sublattice \( \Lambda' \) of finite index in \( \Lambda \), referred to as Minkowskian sublattice. We denote by \( i = i(\Lambda) \) the maximal index \([\Lambda : \Lambda']\) for Minkowskian sublattices \( \Lambda' \) of \( \Lambda \).

Our proof of Theorem 1.1 makes use of knowledge about possible values of \( i \) and of the corresponding structures of the set of minimal vectors of \( \Lambda \). Our basic references for this information are [Mar01] (in particular Table 11.1) and [KMS11] (in particular Tables 2 to 10), which extend previous works of Watson, Ryshkov, and Zahareva up to dimension 9. We give a brief sketch of the used results and recall some notations for this paper in Section 2.

We split the proof of Theorem 1.1 into different cases according to the maximal index \( i \) of a putative counterexample. Loosely speaking, proofs are straightforward for lattices having a small or a large maximal index. In
2 JACQUES MARTINET AND ACHILL SCHÜRMANN

“large index” means \( i \geq 10 \): by the results in [KMS11], there exist sufficiently many minimal vectors in these cases, from which bases can be extracted. Some more details are given in Section 4, where we also treat 9-dimensional lattices with maximal index \( i = 7, 8, 9 \). A “small index” in dimension 9 means \( i \leq 4 \), a case that we consider in Section 5.

This leaves us with the two more difficult cases of \( i = 5, 6 \), for which we use some computer assistance. The difficult case with \( n = 9 \) and \( i = 6 \) is treated in Section 6. In Section 7, we reduce the other difficult case with \( n = 10 \) and \( i = 5 \) to the study of just one special type of lattices. It turns out that such lattices do not exist for \( n = 9 \). However, the study of corresponding lattices for \( n = 10 \), lead us to the counterexamples described in Section 8, by which we finish the proof of Theorem 1.1. In Section 3, we not only give some background information on the computer calculations, but we also explain how the same techniques could be used for a general algorithmic approach to the proof of Theorem 1.1. It should be noted that such a fully computerized proof seems practically infeasible and that only the interplay of human reasoning and computer assistance allowed us to obtain the dimension 9 part of the theorem.

### 2. Classification of minimal classes

This paper relies largely on the results in [KMS11]. There we describe all the \( \mathbb{Z}/d\mathbb{Z} \)-codes arising from a pair \( (\Lambda, \Lambda') \) of 9-dimensional lattices, such that \( \Lambda \) is generated by its set \( S = S(\Lambda) \) of minimal vectors and \( \Lambda' \) has a basis \( B = (e_1, \ldots, e_9) \) of vectors of \( S \); here, \( d \) is the annihilator of \( \Lambda/\Lambda' \), and the code words are the elements \( (a_1, \ldots, a_9) \in (\mathbb{Z}/d\mathbb{Z})^9 \) such that \( \frac{a_1 e_1 + \cdots + a_9 e_9}{d} \) belongs to \( \Lambda \). We classify pairs \( (\Lambda, \Lambda') \) according to possible structures of \( \Lambda/\Lambda' \), merely viewed as an abstract Abelian group. Using the standard convention for quoting Abelian groups by their elementary divisors, we speak for example of type \((3, 2)\) for groups of order 6 isomorphic to \( \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). In [KMS11] we show that quotients \( \Lambda/\Lambda' \) may have any possible structure of order up to index 10, or they may be of type \((12), (6, 2), (4, 4), (4, 2, 2)\) or \((2, 2, 2, 2)\) for larger index.

Given a code \( C \), we attach in [KMS11] a unique minimal class \( C_C \) (in the sense of [Mar07, Section 9.1]; cf. Proposition 3.1 in [KMS11]). This is an equivalence class of lattices with the property that for any pair \( (\Lambda, \Lambda') \) defining \( C \), the set \( S(\Lambda) \) contains \( S(\Lambda_0) \) for some lattice \( \Lambda_0 \in C_C \). In other words, the sets of minimal vectors of lattices in \( C_C \), which are well-defined up to \( \text{GL}_n(\mathbb{Z}) \) equivalence, are minimal with respect to inclusion.

The general method that we can use to prove the existence or nonexistence of a type, is to show that the set of lattices realizing a given code or minimal class is non-empty or empty. Instead of working with lattices directly, we work with the space of Gram matrices of lattice bases, that is, with the space of positive definite, real symmetric matrices. The question
of existence or nonexistence of a lattice type can be decided based on polyhedral computations with rational coordinates, hence, with linear algebra that can be rigorously checked using a computer. For a detailed description we refer to [KMS11].

3. A general algorithmic approach

For the proof of Theorem 1.1 presented here we use computer assistance to rule out two difficult cases in dimension 9 in Sections 6 and 7. The used techniques are general enough, however, to allow (in principle) a proof of Theorem 1.1 entirely based on computer reasoning. In dimension $n$ the general algorithmic approach can be split into two main components:

1. For each minimal class of well rounded $n$-dimensional lattices obtain a polyhedral realization space $P$ of Gram matrices.
2. For each face of $P$ obtain a “typical Gram matrix” and check if its minimal vectors generate but do not provide a basis of $\mathbb{Z}^n$.

For $n = 9$, the minimal classes of well rounded lattices are classified in [KMS11]. There, the non-existence or existence of a minimal class is decided by checking if a corresponding polyhedral realization space is empty or not. Thus Step 1 is carried out in [KMS11]. Typical Gram matrices in PARI/GP format [PARI] and additional information can be obtained from the file Gramindex.gp in the “online appendix” of [KMS11].

Below we explain Step 2. For an implementation we used MAGMA [MAGMA], together with the program lrs [LRS] to deal with the necessary polyhedral computations. For the exclusion of specific cases in this paper, we use Step 2 only for a few specific cases: 22 faces in Sections 6 and one face in Section 7.

Polyhedral realization spaces of minimal classes. A minimal class $C_C$ has a polyhedral “realization space” of Gram matrices attached to it. To see this connection, assume the code $C$ contains $k$ code words $a^{(i)}$, $i = 1, \ldots, k$, the lattice $\Lambda'$ has a basis of minimal vectors $e_1, \ldots, e_n$ of $\Lambda$ and $\Lambda = \langle \Lambda', f_1, \ldots, f_k \rangle$ with

$$f_i = \frac{a_1^{(i)} e_1 + \cdots + a_n^{(i)} e_n}{d},$$

for $i = 1, \ldots, k$. With respect to a fixed chosen basis $B = (b_1, \ldots, b_n)$ of $\Lambda$, the $e_i$ have coordinates $\bar{e}^{(i)} \in \mathbb{Z}^n$, which can be expressed solely in terms of the $a_j^{(i)}$ and $d$. Note that these coordinates are completely independent of the specific lattices $\Lambda$ and $\Lambda'$.

Example. Let us look at a specific case that we consider in Section 7. Let $n = 9$, $d = 5$ and $\Lambda = \langle \Lambda', e \rangle$ with $e$ as in (4). Then we can choose $B = (e, e_2, \ldots, e_9)$ as a basis for $\Lambda$ and the coordinate vector $\bar{e}^{(1)}$ with respect to $B$ is $(5, -1, -1, -2, -2, -2, -2, -2, 0)$. 
Assuming the minimum of \( \Lambda \) is 1, we know that the Gram matrix of \( B \) is contained in the affine subspace

\[
\{ G \in S^n \mid G[\overline{e}(i)] = 1 \text{ for } i = 1, \ldots, n \}
\]

within the space \( S^n \) of real symmetric \( n \times n \) matrices. Here, we make use of the notation \( G[a] \) for \( a^T G a \). The infinitely many linear conditions \( G[a] \geq 1 \) on \( S^n \) that are satisfied for all non-zero integral vectors \( a \), define a set referred to as Ryshkov polyhedron. It is a locally finite polyhedral set (see [Sch09, Chapter 3] for details). Its intersection with (1) is either empty if the code cannot be realized, or it is a polytope \( P \) (convex hull of finitely many Gram matrices) if the code can be realized. In the latter case, the relative interior points (within the affine subspace spanned by the polytope) are Gram matrices from bases of lattices in the minimal class \( \mathcal{C}_C \). Note that all of these lattices have the same set of minimal vectors, so that it is sufficient to know one relative interior Gram matrix, which can be considered “typical” for its class.

**Faces and typical Gram matrices.** For a given minimal class, the boundary of the constructed polytope \( P \) (with respect to the topology of the affine subspace spanned by it) is subdivided into faces, that is, into parts which themselves are polytopes of lower dimension. Each face is uniquely defined by some additional affine equations \( G[a(j)] = 1 \), with coordinate vectors \( a(j) \in \mathbb{Z}^n \). These coordinate vectors are the same for all relative interior Gram matrices of a face and there are only finitely many of them. In terms of corresponding, they give coordinates of additional minimal vectors with respect to the chosen basis.

By considering a typical (any relative interior) Gram matrix for each face of \( P \), one can decide for the corresponding minimal class, whether or not there exist lattices in the class which are generated by minimal vectors but do not provide a basis among them: For each typical Gram matrix \( G \) one has to check whether or not the coordinate vectors \( \{ a \in \mathbb{Z}^n \mid G[a] = 1 \} \) attaining the minimum generate \( \mathbb{Z}^n \) but do not provide a basis for \( \mathbb{Z}^n \).

**Choosing specific faces.** For a full automated proof of Theorem 1.1 the number of cases to be considered would be huge. We use computer assisted checks only for specific cases. In each considered case, the coordinate vectors \( a(j) \) and \( \overline{e}(i) \) of assumed minimal vectors generate but do not provide a basis of \( \mathbb{Z}^9 \).

**Example.** In the case with \( d = 5 \) considered in Section 7, we assume the existence of an additional minimal vector \( x \) (given in (5)) which has coordinates \( a^{(1)} = (-4,0,0,2,2,-1,-1,-1,-1) \) with respect to the basis \( B = (e, e_2, \ldots, e_9) \). Here, \( a^{(1)} \) together with \( \overline{e}(i) \), for \( i = 1, \ldots, 9 \), generate \( \mathbb{Z}^9 \), but no choice of nine of the ten vectors gives a basis for \( \mathbb{Z}^9 \).

Often, the linear conditions we start with imply additional linear conditions \( G[a(j)] = 1 \) with additional coordinate vectors \( a(j) \in \mathbb{Z}^9 \); or in the
language of lattices: the existence of some minimal vectors implies the existence of others. A full list of all implied coordinate vectors can be determined by computing the minimal vectors of a typical Gram matrix. If this full list contains a basis of $\mathbb{Z}^9$, then so do the minimal vectors for all lattices of the considered type. Note that all of these rational linear algebra operations can rigorously be verified using a computer.

Example. In the $n = 9$, $d = 5$ case of Section 7 we find 10 pairs of additional minimal vectors from the Gram matrix in (6). The full list of minimal coordinate vectors obtained in this way contains a basis of $\mathbb{Z}^9$, excluding this case as a counterexample in dimension 9.

**Exploiting polyhedral symmetries.** In higher dimensions, i.e. for $n \geq 9$, the polyhedral computations necessary to decide whether or not a code is realizable can be quite involved. In these cases we can try to exploit available symmetries to make the computations feasible. The automorphism group of the code, yields an automorphism group of the corresponding minimal class:

\[(2) \text{ Aut}_C = \{ U \in \text{GL}_n(\mathbb{Z}) \mid Ue^{(i)} \in \{ e^{(1)}, \ldots, e^{(n)} \} \text{ for all } i = 1, \ldots, n \}\]

The polytope $P \subset S^n$ described above is invariant with respect to this group: We have $U^t P U = P$ for all $U \in \text{Aut}_C$. The same is true for the set of vertices of $P$ and therefore the vertex barycenter of $P$ (if non-empty) is contained in the linear subspace

\[(3) \{ G \in S^n \mid U^t G U = G \text{ for all } U \in \text{GL}_n(\mathbb{Z}) \}\]

of $\text{Aut}_C$-invariant Gram matrices. Thus for checking feasibility of a given code $C$ we can restrict the polyhedral computations and search for an interior point within the linear subspace (3).

Moreover it is also possible to make use of symmetries when considering a fixed code $C_C$, together with some coordinate vectors $a^{(j)}$. Instead of restricting to the invariant linear subspace (3) coming from the symmetry group $\text{Aut}_C$, we can restrict to a corresponding linear subspace obtained from a subgroup of $\text{Aut}_C$, for which also the set of coordinate vectors $a^{(j)}$ is preserved.

Example. In our example with $n = 9$, $d = 5$, the coordinate vectors $\bar{e}^{(i)}$ and $a^{(1)} = (-4, 0, 0, 2, 2, -1, -1, -1, -1)$ are for example invariant with respect to permutations of $e_2, e_3$, of $e_4, e_5$ and of $e_6, e_7, e_8$.

**4. Lattices of large index**

For $n = 9$ and “very large” indices, namely for $i(\Lambda) \geq 10$, lattices are generated by minimal vectors, and a basis of minimal vectors is “almost” in evidence on typical Gram matrices from the online appendix of [KMS11]. Indeed, most of the matrices turn out to have diagonal entries equal to the minimum of the lattice we consider, and in one case where a diagonal entry was larger than this minimum, we can easily conclude by listing all minimal vectors of the lattice.
To work with \( i = 7, 8, 9 \) is less simple: in these cases, it may happen that the lattices \( \Lambda \) of a minimal class \( C \) are not generated by their minimal vectors. In fact, in some cases, the only minimal vectors are the nine \( e_i \) spanning the sublattice \( \Lambda' \). Or it may happen that all of the additional minimal vectors do not generate \( \Lambda \), for example if they all lie in \( \Lambda' \). We must in these cases explicitly use the existence of extra minimal vectors.

The following proposition will be used (at least implicitly) from this Section onwards.

**Proposition 4.1.** Let \((\Lambda, \Lambda')\) be a pair of \( n \)-dimensional lattices, where \( \Lambda' \) is generated by minimal vectors \((e_1, \ldots, e_n)\) of \( \Lambda \). Let \( d \) the annihilator of \( \Lambda/\Lambda' \) and let \( x = \sum a_i e_i + \sum a_i e_i \) with \( a_i, d' \in \mathbb{Z} \) and \( d' \mid d \). Then the absolute values of the \( a_i \) are bounded from above by \(|d'|\).

**Proof.** We may suppose that \( d' \) and the \( a_i \) are coprime. Let \( L = \langle \Lambda', x \rangle \) contain \( \Lambda' \) to index \( d' \). Let \( i \) such that \( a_i \neq 0 \). We have

\[
e_i = \frac{-d'x - \sum_{j \neq i} a_j e_j}{a_i},
\]

which shows that \( L \) contains to index \(|a_i|\) the lattice \( M \) generated by \( x \) and the \( e_j, j \neq i \). We have \(|\Lambda : M| = |\Lambda : L| \cdot |L : M| \leq i \), hence

\[
|a_i| = |L : M| \leq \frac{|\Lambda : L|}{i} = d'.
\]

\[\square\]

**Proof of Theorem 1.1 for cyclic quotients of order \( d = 9, 8, 7 \).** We first consider cyclic quotients of order \( d = 9, 8, 7 \), writing \( \Lambda = \langle \Lambda', e \rangle \) for some vector \( e \) of the form \( e = \frac{1}{d}(\sum_{i=1}^{d} a_i e_i) \) with \( a_i \in \mathbb{Z} \). Since quotients \( \mathbb{Z}/d\mathbb{Z} \) do not exist in dimension 8, all \( a_i \) are non-zero and we may choose them modulo \( d \). For every integer \( c \) prime to \( d \) we have \( \Lambda = \langle \Lambda', ce \rangle \), allowing us to choose all \( a_i \) in \( \{1, 2, \ldots, \frac{d}{2}\} \). The \( \mathbb{Z}/d\mathbb{Z} \)-code generated by the word \((a_1, \ldots, a_{d/2})\) is well defined by this sequence up to permutation, that is, it is defined by the numbers \( m_i \) of coefficients \( a_j \) equal to \( i \). The transformation \( e \mapsto ce \) induces an action of \((\mathbb{Z}/d\mathbb{Z})^\times/\{\pm 1\}\) which amounts to a circular permutation of \((m_1, m_2, m_3)\) if \( d = 7 \), of \((m_1, m_2, m_4)\) if \( d = 9 \), and the exchange \( m_1 \leftrightarrow m_3 \) if \( d = 8 \).

Since 7, 8 and 9 are prime powers, the hypothesis “\( \Lambda \) is generated by its minimal vectors” amounts to the existence of a minimal vector \( x \in \Lambda \) which generates \( \Lambda \) modulo \( \Lambda' \). In [KMS11, Table 2] the possible codes are listed, up to a permutation as above, which we have to take into account here. For instance, if \( \Lambda \) is constructed using the code modulo 7 for which \((m_1, m_2, m_3) = (4, 2, 3)\), the hypothesis “\( \Lambda \) is generated by its minimal vectors” implies the existence of a minimal vector \( x \in e + \Lambda' \) for an \( e \) associated with any of the three systems \((m_1, m_2, m_3) = (4, 2, 3), (3, 4, 2) \) and \((2, 3, 4)\), and we must thus consider three cases for one code listed in [KMS11].
Six codes are listed in \cite{KMS11}, Table 2. An inspection of the corresponding Gram matrices shows that a basis of minimal vectors exists for the first five, and that the minimal vectors generate a sublattice of index 3 in the remaining case with \((m_1, m_2, m_3, m_4) = (2, 2, 3, 2)\). So we must assume the existence of at least one additional minimal vector here. As we may permute \(m_1, m_2\) and \(m_4\) in this case, we may assume that \(\Lambda\) contains a minimal vector \(x = \frac{a_1 e_1 + \ldots + a_9 e_9}{9}\) with \(a_1 \equiv a_2 \equiv 1\) mod 9. We have \(|a_i| \leq i = 9\) (because \(i(\Lambda) \leq 9\)), hence \(a_1, a_2 = 1\) or \(-8\). If \(a_1 = a_2 = -8\), then we may write \(e_1 + e_2 + x = \frac{-2 + 9 + \ldots + 9 e_9}{8}\), constructing this way a lattice of index 8 in dimension 8, a contradiction. Hence \(a_1 = 1\), say, and \((x, e_2, \ldots, e_9)\) is a basis of minimal vectors for \(\Lambda\).

For 14 out of the 19 codes listed in \cite{KMS11}, Table 2, Gram matrices show the existence of a basis of minimal vectors. In the remaining 5 cases, \(S(\Lambda)\) generates a lattice of index 8 (for systems \((3, 4, 2, 0)\), \((3, 3, 2, 1)\) and \((3, 2, 2, 2)\)) or 2 (for systems \((2, 4, 2, 1)\) and \((3, 1, 3, 2)\)), which we now consider together with the allowed permutation \((1, 3)\).

In all cases, we have \(m_1 \geq 1\), and the argument used for denominator 9 still works: for \(x\) minimal in \(e + \Lambda'\), we can exclude that two coefficients are equal to \(-7\) (because we would construct in this way an 8-dimensional lattice with \(i = 7\)), so that we may assume that, say, \(a_1 = 1\), and \((x, e_2, \ldots, e_9)\) is then a basis of minimal vectors.

For six out of eight systems \((m_1, m_2, m_3)\), Gram matrices show the existence of a basis of minimal vectors for \(\Lambda\). In the remaining two systems, we have \(S(\Lambda) = S(\Lambda')\), and we must use the hypothesis “\(e + \Lambda'\) contains some minimal vector \(x\)” for all circular permutations of these two systems, namely

\[(5, 2, 2), (2, 5, 2), (2, 2, 5), (4, 2, 3), (3, 4, 2), (2, 3, 4)\].

Write \(e = \frac{a_1 e_1 + \ldots + a_9 e_9}{9}\) and \(x = \frac{b_1 e_1 + \ldots + b_9 e_9}{9}\), with \(b_i \equiv a_i\) mod 7. Since \(i(\Lambda) = 7\), we have \(b_i = a_i\) or \(b_i = -(7 - a_i)\). Denoting by \(m_i'\) (\(i = 1, \ldots, 6\)) the number of subscripts \(j\) such that \(|b_j| = i\), we have \(m_1' + m_6' = m_1\), \(m_2' + m_5' = m_2\) and \(m_3' + m_4' = m_3\), and \(x + \sum b_i = 6 e_i = \frac{-x + \sum a_i b_i}{6} = \frac{-x + \sum b_i}{6}\). If \(m_i' \geq 1\), say, \(b_1 = 1\), then \((x, e_2, \ldots, e_9)\) is a basis of minimal vectors, so that we may assume that \(m_6' = m_1\). By the equality above, there exist lattices \(L, L'\) with \([L : L'] = 6\) in dimension \(n' = 10 - m_1\), which is possible only if \(10 - m_1 \geq 8\), i.e., \(m_1 = 2\), and then the corresponding system \((M_1, M_2, M_3)\), namely \((1 + m_5', m_2' + m_4', m_3')\) must be one of the six systems listed in \cite{Mar01}. For five out of these six systems, Section 9 of \cite{Mar01} immediately shows that there exists a basis of minimal vectors for \(L\), hence also for \(\Lambda\). We may thus assume that \((M_1, M_2, M_3) = (3, 3, 2)\), hence first that \(m_5' = m_1 = 2\), next that \(m_2' + m_4' = 3\), so that

\[x = \frac{-6(e_1 + e_2) - 5(e_3 + e_4) + 3(e_5 + e_6) + b_7 e_7 + b_8 e_8 + b_9 e_9}{7}\]
with $b_7, b_8, b_9 = 2$ or $-4$. We now write the equality above in the form
\[ 2(x + e_1 + e_2 + e_3 + e_4) - (e_5 + e_6) = \frac{-x + e_3 + e_4 \pm e_7 \pm e_8 \pm e_9}{3}, \]
which shows that $y = \frac{-x + e_3 - 2e_4 \pm e_7 \pm e_8 \pm e_9}{3}$ is minimal. Replacing $x$ by its components on the $e_i$, we obtain
\[ y = \frac{2(e_1 + e_2) + 4e_3 - 3e_4 + e_5 + e_6 \pm e_7 \pm e_8 \pm e_9}{7}, \]
which shows that $(e_1, \ldots, e_8, y)$ is a basis of minimal vectors for a lattice containing $\Lambda'$ to index 7, hence equal to $\Lambda$.

**Proof of Theorem 1.1 for non-cyclic quotients of order $d = 9, 8$.** We now turn to non-cyclic quotients, which are of one of the types $(3, 3)$, $(4, 2)$ or $(2, 2, 2)$.

**Type $(3, 3)$.**\[\text{[KMS11] Table 6}\] shows that $\Lambda$ is of the form $\langle \Lambda', e, f \rangle$ where $e, f$ have denominator 3, where $e$ (resp. $f$) has 6 (resp. 6, 6 or 7) non-zero components. This shows that the $e - e_i$, $i \leq 6$ are minimal, as well as 6 vectors $f \mp e_j$ in the first two cases, so that we obtain a basis of minimal vectors for $\Lambda$ by replacing two convenient vectors $e_k, e_\ell$ by vectors of the form $e - e_i$, $f - e_\ell$. In the third case, we use the fact that there exists some minimal vector $y$ in one of the cosets of $f$, $f + e$ or $f - e$ modulo $\Lambda'$, say, $y \in f + \Lambda'$. (The automorphism group of the code exchanges these three cosets.) We now consider $\Lambda'' = \langle \Lambda', f \rangle$. We have $i(\Lambda'') = 3$ (because $[\Lambda : \Lambda''] = 3$) hence a minimal vector $y \in f + \Lambda'$ must have 7 odd components equal to $\pm 1$ or $\pm 2$, not all equal to $\pm 2$ (as in the proof of Lemma 3.1 in \[\text{[Mar07]}\]), and we obtain a basis of minimal vectors by again replacing two convenient vectors $e_k, e_\ell$ by some vectors $e - e_i$ and $f \mp e_j$.

**Type $(4, 2)$.** Here we have $\Lambda = \langle \Lambda', e, f \rangle$ with $e$ of denominator 4 and $f$ of denominator 2, and there exist minimal vectors $x \in e + \Lambda'$ or $x \in e + f + \Lambda'$ and $y \in f + \Lambda'$ or $y + 2e + \Lambda'$, with $e$ and $f$ as in \[\text{[KMS11] Table 7}\]. Changing the representatives for $\Lambda/\Lambda'$ if need be, we may assume that $x \in e + \Lambda'$ and $y \in f + \Lambda'$, and it suffices to show as for quotients of type $(3, 3)$ that the numerators of $x$ and $y$ have some component equal to $\pm 1$. This is clear for $y$: since $\Lambda''' = \langle \Lambda', f \rangle$ has index 2, the numerator of $y$ has components $\pm 1$ whenever those of $f$ are $\pm 1$. The same is obviously true with $e$ for the first six rows of \[\text{[KMS11] Table 7}\], since $e$ itself is minimal. To deal with the remaining 13 rows, we observe that $\Lambda''' = \langle \Lambda', e \rangle$ has index 4, and that the components of the numerator of $x$ are odd exactly when those of $e$ are. By \[\text{[KMS11] Table 7}\], there are $t \geq 5$ such components. If none was equal to $\pm 1$, there would be $t$ components $\pm 3$ in the numerator of $x$, hence there would exist a pair $L, L'$ of lattices with $[L : L'] = 3$ in dimension $n' = 9 + 1 - t \leq 5$, which would contradict the results of \[\text{[Mar01]}\] Table 11.1.

**Type $(2, 2, 2)$.** This case is dealt with as part \[\text{[Mar07]}\] Lemma 3.1, but proofs are only sketched there. In the following section we give more details for the part needed here, by proving the following proposition.
Proposition 4.2 ([Mar07]). A 2-elementary lattice of maximal index $\nu = 8$ and dimension $n \leq 9$, which is generated by its minimal vectors, has always a basis of minimal vectors.

5. Lattices with 2-elementary quotients

In this section we give detailed proofs for two assertions, which were only sketched in [Mar07], concerning elementary quotients of order 4 and 8. We first consider lattices of index $\nu \leq 4$ and dimension $n \leq 10$, with the usual notation $\Lambda, \Lambda', B = (e_1, \ldots, e_n)$, assuming that $\Lambda$ is generated by its minimal vectors. By showing that these lattices always have a basis of minimal vectors, we obtain a proof for the following proposition, which is even a bit stronger than the assertion of Theorem 1.1 for these indices.

Proposition 5.1 ([Mar07]). A lattice of maximal index $\nu \leq 4$ and dimension $n \leq 10$, which is generated by its minimal vectors, has always a basis of minimal vectors.

The proof given in [Mar07] is only sketched for non-cyclic quotients. We complete it in this section. By the 10-dimensional lattice described in Section 8, it turns out that Proposition 5.1 is best possible, because it has maximal index $\nu = 5$. Thus our new 10-dimensional counterexample is minimal for both the dimension and the maximal index. We note that the 11-dimensional lattice constructed in [CS95] has maximal index $\nu = 3$.

Proof of Proposition 5.1. Lattices with maximal index $\nu = 2$, and generated by their minimal vectors are easily proved to possess a basis of minimal vectors, regardless of the dimension: indeed $\Lambda$ is generated over $\Lambda'$ endowed with a basis $B = (e_1, \ldots, e_n)$ of minimal vectors by one minimal vector $x = a_1e_1 + \cdots + a_ne_n$ with $|a_j| \leq 2$, hence with some $a_i$ equal to $\pm 1$; replacing $e_i$ by $x$ in $B$ yields a basis of minimal vectors.

When $\Lambda/\Lambda'$ is cyclic of order $d = 3$ or 4, it is proved in [Mar07] that $\Lambda$ possesses a minimal vector of the form $x = \frac{a_1e_1 + \cdots + a_ne_n}{d}$ with at least one $a_i$ equal to $\pm 1$, so that replacing $e_i$ by $x$ in $B$ gives us a basis of minimal vectors.

Assume now that $\Lambda/\Lambda'$ is 2-elementary of order 4. Then we have $\Lambda = \Lambda' \cup (e + \Lambda') \cup (f + \Lambda') \cup (g + \Lambda')$ where $e, f, g \in \Lambda$ have denominators 2 and numerators 0 or 1 when expressed with respect to the basis $B'$ of $\Lambda'$, and $e + f + g \in \Lambda'$.

There is a well-defined partition of $\{1, \ldots, n\}$ into subsets $I_1, I_2, I_3, I_4$ such that

$$e = \frac{1}{2} \sum_{i \in I_1 \cup I_2} e_i \quad \text{and} \quad f = \frac{1}{2} \sum_{i \in I_2 \cup I_3} e_i$$

(hence $g = \frac{1}{2} \sum_{i \in I_1 \cup I_3} e_i$). We set $p_k = |I_k|, m_1 = p_1 + p_2, m_2 = p_2 + p_3,$ and $m = p_1 + p_2 + p_3$ (thus $p_4 = n - m$). Note that at least two of the intervals $I_1, I_2, I_3$ are non-empty.
Permuting \(e, f, g\) if necessary, we may assume that the cosets of \(e\) and \(f\) contain minimal vectors

\[
x = \frac{a_1e_1 + \cdots + a_ne_n}{2} \quad \text{and} \quad y = \frac{b_1e_1 + \cdots + b_ne_n}{2}.
\]

By Proposition 4.1, we have

\[
a_i = \pm 1 \text{ if } i \in I_1 \cup I_2 \quad \text{and} \quad a_i = 0, \pm 2 \text{ otherwise}.
\]

We now construct a basis of minimal vectors for \(\Lambda\) by considering successively two cases.

Case 1. Assume first that some \(a_i, i \in I_3\) or some \(b_i, i \in I_1\) is equal to \(\pm 2\).

Exchanging \(x\) and \(y\), negating \(y\), and permuting some \(e_i\) if necessary, we may assume that \(b_1 = 2\) and \(a_1 = 1\). Then

\[
4x + 2y = 4e_1 + \sum_{i \geq 2} (2a_i + b_i)e_i
\]

and we obtain

\[
x - e_1 = -\frac{2y + \sum_{i \geq 2} c_i e_i}{4}
\]

where \(c_i = 2a_i + b_i\) is odd for \(i \in I_2 \cup I_3\). We have thus constructed a sublattice \(L' = \langle \Lambda', x - e_1 \rangle\) of \(\Lambda = \langle \Lambda', e, f \rangle\) such that \(\Lambda/L'\) is cyclic, which implies the existence of a minimal basis for \(\Lambda\) since we assume \(n \leq 10\).

Case 2. Assume now that all \(a_i\) for \(i \in I_3\) and all \(b_i\) for \(i \in I_1\) are zero. Then we obtain a basis of minimal vectors for \(\Lambda\) by replacing one \(e_i\) by \(x\) and one \(e_j\) by \(y\) where \(i, j\) are chosen in two distinct intervals \(I_k\).

We can now also deal with the Type \((2, 2, 2)\) case at the end of Section 4 by proving the proposition about elementary quotients \(\Lambda/\Lambda'\) of order 8 in dimension \(n \leq 9\).

**Proof of Proposition 4.2.** One easily checks that binary codes of dimension 3 and length \(\ell \leq 9\) (and even \(\ell \leq 10\)) are of weight \(wt \leq 4\). Hence if \(\Lambda/\Lambda'\) is of type \((2, 2, 2)\), one may write \(\Lambda\) in the form \(\Lambda = \langle \Lambda', e, f \rangle\) where \(g\) is of the form \(g = \frac{e_{i_1} + e_{i_2} + e_{i_3} + e_{i_4}}{2}\), and there exist minimal vectors \(x \in e + \Lambda'\) and \(y \in f + \Lambda'\). We now consider the two cases in the proof of Proposition 5.1 for the lattice \(L = \langle \Lambda', e, f \rangle\).

If Case 1 holds, there exists \(L' \subset L\) such that \(\Lambda/L'\) is of type \((4, 2)\), and then the existence of a basis of minimal vectors has been proved in Section 4. If Case 2 holds, we first construct as above a basis for \(L\) by replacing two vectors \(e_i, e_j\) by \(x, y\), and then a basis for \(\Lambda\) by replacing by \(g\) some \(e_{i_k}\) which belongs to the numerator of \(g\) but not to those of \(e\) and \(f\).

**Remark.** When \([\Lambda/\Lambda']\) is elementary of order 4, the existence of a basis of minimal vectors for \(\Lambda\) could have been proved without assuming the condition \(n \leq 10\), as asserted in [Mar07], but with a less simple proof.
6. LATTICES OF MAXIMAL INDEX 6

We may write $\Lambda = \langle \Lambda', e \rangle$ where $e = \sum_{i=1}^{9} a_i e_i$ with increasing $a_i \in \{0,1,2,3\}$ and $(e_1,\ldots,e_9)$ is a basis for $\Lambda'$. For $i = 0,1,2,3$, we denote by $m_i$ the number of $a_j$ equal to $i$ and set $m = m_1 + m_2 + m_3$. We have $m = 8$ (six systems $(m_1,m_2,m_3)$ listed in [Mar01 Table 11.1]) or $m = 9$ (20 systems listed in [KMS11 Table 2]). We assume that $\Lambda$ is generated by its minimal vectors, which amounts to the existence of either a minimal vector $x = \sum_{i=1}^{9} b_i e_i \in e + \Lambda'$ (then, $b_i \equiv a_i \mod 6$ and $|b_i| \leq 6$), or the existence of two minimal vectors $y = \sum_{i=1}^{9} c_i e_i \in 2e + \Lambda'$ and $z = \sum_{i=1}^{9} d_i e_i \in 3e + \Lambda'$, with $c_i \equiv a_i \mod 3$ and $d_i \equiv a_i \mod 2$.

Let us first consider the case when there is a minimal vector $x \in e + \Lambda'$, with, say, $b_i = 1$ or $-5$ for $i \leq m_1$, $b_i = 2$ or $-4$ for $m_1 < i \leq m_1 + m_2$, $b_i = 3$ if $m_1 + m_2 < i \leq m$ (and we then may assume that $b_i = +3$). If $b_i = 1$ for some $i$, then a basis of minimal vectors trivially exists. Otherwise, the argument used in the section above to deal with denominator 7 will show the existence of a pair $(L,L')$ of lattices with $z = 5$ in dimension $10 - m_1$, which is possible only if $m_1 \leq 2$ and leaves us with the three systems $(2,5,2)$, $(2,4,3)$, and $(1,5,4)$.

In the first case, $z = \frac{e_1 + e_2 + e_3 + e_9}{2}$ is minimal, and we have

$$x = \frac{4(z - e_1 - e_2 + b'_1 e_3 + \cdots + b'_6 e_9)}{3}$$

for some $b'_i$ equal to 1 or $-2$, among which at least three must be odd. Replacing $e_9$ by $z$ in $(e_1,\ldots,e_9)$ and one $e_i$ with $3 \leq i \leq 7$ by $x$, we obtain a basis of minimal vectors for $\Lambda$.

The same argument works in the third case, taking $z = \frac{e_1 + e_7 + e_8 + e_9}{2}$.

In the second case, $y = \frac{e_1 + e_2 + e_3 + e_4 + e_6 + 2e_9}{3}$ is minimal, we have

$$x = \frac{4(y \pm e_1 \pm e_2 \pm e_3 \pm e_5 \pm e_7 \pm e_8 \pm e_9 \pm b'_1 e_3 + \cdots + b'_6 e_9)}{2}$$

(with $b'_i = 0, \pm 1$ or 3), and we obtain a basis of minimal vectors for $\Lambda$ by replacing $e_1$ by $x$ and $e_9$ by $y$.

From now on we assume that $e + \Lambda'$ does not contain any minimal vector, and work with the minimal vectors $y \in 2e + \Lambda'$ and $z \in 3e + \Lambda'$. Proposition [L1] shows that we have $|c_i| \leq 3$ and $|d_j| \leq 2$. By the results of [Mar01] and [KMS11] for $m = 8$ (resp. 9), there exist 6 (resp. 20 minimal classes), among which 5, those with $s > 14$ (resp. 4, those with $s > 17$) contain minimal vectors in $e + \Lambda'$. So we are left with 1 (resp. 15) minimal classes.

We can get rid of the remaining minimal class with $m = 8$ and of the two minimal classes with $m = 9$ and $s = 17$ by the following argument, which is valid for any dimension: assume that we have $m_1 + m_2 = 6$ and that $3e + \Lambda$ contains some minimal vector $z$; then a vector of the form $y = \pm e_1 \pm \cdots \pm e_8 \pm 2e_9$ is minimal, and since the numerator of $z$ has component $d_m = \pm 1$, $(y, e_2, \ldots, e_{m-1}, z, \ldots)$ is a basis of minimal vectors for $\Lambda$. 

We could get rid in a similar way (by a slightly more complicated argument) of the four minimal classes with $m = 9$ and $s = 15$, but it appears to be very difficult to construct bases of minimal vectors by elementary arguments for the 9 minimal classes with $m = 9$, for which $s(\Lambda) = s(\Lambda') = 9$ is possible. So in this case we used the general approach described in Section 3 to exclude the existence of lattices that are generated by minimal vectors, but which do not have a basis among them.

In fact, we ran a computer calculation on all 2574 possible cases with additional minimal vectors $y \in 2e + \Lambda'$ and $z \in 3e + \Lambda'$, having coefficients $|c_i| \leq 3$ and $|d_j| \leq 2$, and falling into one of the 15 cases with $d = 6$ and $s \leq 17$ listed in [KMS11, Table 2]. Using the general approach of Section 3, these computations show that all but 22 of these cases are infeasible, that is, lattices respectively Gram matrices with these parameters do not exist. All of the 22 feasible cases turn out to have parameters $m_1 = 5$ and $m_2 = 4$. Considering the corresponding Gram matrices displayed in the file Gramindex.gp in the online appendix of [KMS11] shows that in all of these cases, the set of minimal vectors also contains a basis of minimal vectors. By this we complete the proof of Theorem 1.1 for lattices of index 6.

7. Lattices of maximal index 5

We consider lattices of dimension $n$ ($n$ will be 8, 9 or 10) of the form $\Lambda = (\Lambda', e, e')$ where

$$e = \frac{e_1 + \cdots + e_{m_1} + 2(e_{m_1+1} + \cdots + e_{m_1+m_2})}{5},$$

$$e' = \frac{2(e_1 + \cdots + e_{m_1}) - (e_{m_1+1} + \cdots + e_{m_1+m_2})}{5},$$

and $B = (e_1, \ldots, e_n)$ is a basis for $\Lambda'$. From [Mar01], we know that $\ell := m_1 + m_2$ is at least 8, that if $\ell = 8$ (resp. $\ell = 9$) we must have $2 \leq m_1 \leq 6$ (resp. $1 \leq m_1 \leq 9$), and that lattices with $(m_1, m_2) = (2, 6), (4, 4), (6, 2), (1, 8)$ or $(8, 1)$ necessarily have bases of minimal vectors. In the remaining cases, we must use the hypothesis that $\Lambda$ is generated by its minimal vectors, which amounts to saying that there exists some minimal vector in one of the two cosets $e + \Lambda'$ or $2e + \Lambda'$ modulo $\Lambda'$, and since we may exchange $e$ and $e'$ (see [Mar01], Example 3.3), we may and shall assume that the coset of $e$ contains some minimal vector $x$. This vector must be of the form

$$x = \frac{1}{5} \sum_{i=1}^{n} a_i e_i$$

where the $a_i$ satisfy the following congruences modulo 5: $a_i \equiv 1$ if $i \leq m_1$, $a_1 \equiv 2$ if $m_1 < i \leq \ell$, and $a_i \equiv 0$ if $i > \ell$, and are bounded from above by 5 (because $i(\Lambda) = 5$).

Assuming that $n \leq 9$, we shall now derive a contradiction from the assumptions.
(1) there exists a vector $x$ as above, and
(2) $\Lambda$ has no basis of minimal vectors.

First observe that $\alpha_i = 1$ is impossible, since replacing $e_i$ by $x$ yields
a basis of minimal vectors for $\Lambda$. We may thus assume that $\alpha_i = -4$ for
$1 \leq i \leq m_1$.

To simplify the notation, for $i = 4, 2, 3, 5$, set
$$
\Sigma_i = \sum_{|a_k|=i} e_k \quad \text{and} \quad m'_i = |\{k \mid |a_k| = i\}|;
$$
we thus have $m'_4 = m_1$, $m'_2 + m'_3 = m_2$, $m'_5 = n - \ell$, and
$$
x = -\frac{4\Sigma_4 + 2\Sigma_2 - 3\Sigma_3 + 5\Sigma_5}{5} \quad \text{and} \quad e = \frac{\Sigma_4 + 2(\Sigma_2 + \Sigma_3)}{5}.
$$

We now write down two identities which will allow us to make use of in-
equalities involving denominators 4 and 2 first, and then 3:
$$
x + \Sigma_4 + \Sigma_3 - \Sigma_5 = \frac{-x + \Sigma_3 + \Sigma_5 + 2\Sigma_2}{4}
$$
$$
2x + \Sigma_4 + \Sigma_3 - \Sigma_2 - 2\Sigma_5 = \frac{x - \Sigma_4 - \Sigma_2 - \Sigma_5}{3}.
$$

From the classification of lattices of maximal index 2 and 4 (resp. 3); see
[Mar01] Theorem 2.2 and Table 11.1), we deduce the inequalities
$$
m'_3 + m'_5 \geq 3, \ m'_3 + m'_5 + 2m'_2 \geq 7 \text{ and } m'_3 + m'_5 + m'_2 \geq 6
$$
(resp. $m'_4 + m'_2 + m'_5 \geq 5$).

If $m'_3 + m'_5 = 3$, then $f = \frac{-x + \Sigma_3 + \Sigma_5}{2}$ belongs to $\Lambda$, and a short calculation shows that $f = 2e - \Sigma_2$. Hence replacing in $B$ an $e_i$ with $a_i = -3$ or 5 by
$f$, we obtain a lattice containing $\Lambda'$ and
$$
e = 6e - 5e = 3(f + \Sigma_2) - (\Sigma_4 + 2\Sigma_2 + 2\Sigma_3),
$$

hence the lattice $\Lambda$, which shows that in this case, $\Lambda$ possesses a basis of minimal vectors.

If $m'_3 + m'_5 + 2m'_2 = 7$, let $f = \frac{-x + \Sigma_3 + \Sigma_5 + 2\Sigma_2}{4}$, and let $y$ be a vector $e_i$ with $a_i = -3, 2$ or 5. Then $f - y$ is minimal, and a short calculation shows that $f = e$. Hence replacing in $B$ a convenient $e_i \neq y$ by $f - y$, we again obtain $\Lambda$.

If $m'_4 + m'_2 + m'_5 = 5$, let $g = \frac{x - \Sigma_4 - \Sigma_2 - \Sigma_5}{3}$, and let $y$ be a vector $e_i$ with $a_i = -4, 2$ or 5. Then $g + y$ is minimal, and we have this time $2g = -e + \Sigma_4$, which again shows the existence in this case of a basis of minimal vectors for $\Lambda$.

Summarizing, we have:

Lemma 7.1. Let $\Lambda$ be a lattice of maximal index 5 generated by its minimal vectors but having no basis of minimal vectors. Then $\Lambda$ is generated by a basis $B = (e_1, \ldots, e_n)$ of minimal vectors for a lattice $\Lambda'$ of index 5 in $\Lambda$ and a minimal vector $x$ as in (*) which satisfies the conditions
$$
m'_3 + m'_5 \geq 4, \ m'_3 + m'_5 + 2m'_2 \geq 8 \text{ and } m'_4 + m'_2 + m'_5 \geq 6.
$$
Corollary 7.2. Let $\Lambda$ be a lattice of dimension $\leq 9$ and maximal index 5 generated by its minimal vectors but having no basis of minimal vectors. Then $\Lambda$ has the invariants $m_1 = 3$, $m_2 = 5$ and has a minimal vector $x$ with invariants $m'_2 = 2$ and $m'_3 = 3$.

Proof. We know that $n = 8$ is impossible. Adding the first and the third inequality in Proposition 7.1, we get $\ell \geq 10 - 2m'_5$. Hence we must have $n = 9$ and $m'_5 = 1$, thus $\ell = 8$. Adding the last two inequalities, we get $\ell + 2m'_2 \geq 14 - 2m'_5$, hence $m'_2 \geq 2$. From $m'_2 \geq 4 - m'_5 = 3$, we get $m'_2 \geq 5$, and since $m'_2 = 6$ is excluded, we are left with $m_2 = 5$, which implies $m_1 = 3$, $m'_2 = 2$ and $m'_3 = 3$.

To prove the existence of a basis of minimal vectors for lattices of index $i = 5$, it now suffices to consider the case when we may write

$$e = \frac{e_1 + e_2 + e_3 + 2(e_4 + e_5 + e_6 + e_7 + e_8)}{5} \quad \text{and}$$

$$x = \frac{-4(e_1 + e_2 + e_3) + 2(e_4 + e_5) - 3(e_6 + e_7 + e_8) + 5e_9}{5}.$$  

Here the consideration of denominators 2, 3 or 4 as above does not produce obvious new minimal vectors. We therefore use the general algorithmic approach of Section 3 to deal with this case. As already described there, choosing $B = (e, e_2, \ldots, e_9)$ as a basis, we obtain coordinates $\bar{e}^{(1)} = (5, -1, -1, -2, -2, -2, -2, -2, 0)$ for $e_1$ and $a^{(1)} = (-4, 0, 0, 2, 2, -1, -1, -1, -1)$ for $x$. Assuming a minimum of 1, we get ten linear conditions $G[\bar{e}^{(i)}] = 1$, $i = 1, \ldots, 9$, $G[a^{(1)}] = 1$ for Gram matrices $G$ on the Ryshkov polyhedron (the set of Gram matrices in $S^9$ with $G[z] \geq 1$ for all $z \in \mathbb{Z}^9$). We can make use of some symmetry, as the set of coordinate vectors $\bar{e}^{(i)}$ and $a^{(1)}$ is invariant with respect to permutations of $e_2, e_3$, of $e_4, e_5$ and of $e_6, e_7, e_8$. This yields four additional linear conditions, and we obtain a polytope with 25 vertices satisfying all of the prescribed equations. Its vertex barycenter scaled by 900 is the Gram matrix

$$\begin{pmatrix}
1104 & 54 & 54 & 552 & 552 & 528 & 528 & 528 & 312 \\
54 & 900 & 66 & 27 & 27 & -142 & -142 & -142 & 267 \\
54 & 66 & 900 & 27 & 27 & -142 & -142 & -142 & 267 \\
552 & 27 & 27 & 900 & 138 & 102 & 102 & 102 & -87 \\
552 & 27 & 27 & 138 & 900 & 102 & 102 & 102 & -87 \\
528 & -142 & -142 & 102 & 102 & 900 & 216 & 216 & 186 \\
528 & -142 & -142 & 102 & 102 & 216 & 900 & 216 & 186 \\
528 & -142 & -142 & 102 & 102 & 216 & 216 & 900 & 186 \\
312 & 267 & 267 & -87 & -87 & 186 & 186 & 186 & 900
\end{pmatrix}.$$
From it we obtain a list of ten additional coordinate vectors $a^{(j)}$ which are minimal (satisfying $G[a^{(j)}] = 1$):

$(-1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$,  $(−1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$,  $(−1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$,

$(−2, 1, 0, 1, 1, 1, 1, 1, 0, 0)$,  $(−2, 0, 1, 1, 1, 1, 1, 1, 0, 0)$,  $(−2, 0, 0, 1, 1, 0, 0, 0, 0, 0)$,

$(−2, 0, 0, 1, 1, 0, 0, 0, 0, 0)$,  $(−3, 1, 1, 1, 1, 1, 1, 0, 0, 0)$,  $(−3, 0, 0, 1, 1, 1, 1, 1, 0, 0)$.

So all 9-dimensional lattices generated by minimal vectors of type $e_i$ and $x$ as above, have ten additional pairs of minimal vectors, and among them we find always a basis of minimal vectors. Take for example $(e - e_4, e_2, ..., e_9)$. We have thus proved that 9-dimensional lattices of maximal index $\tau = 3$, and which are generated by their minimal vectors, indeed have bases of minimal vectors.

Here is a “check” for the obtained result: The 20 linear conditions of minimal vectors $S$ have rank 19. Up to scaling, there is therefore a unique perfection relation (cf. [BM09]) between the 20 orthogonal projections $p_y$ (in direction $y$) associated to these vectors. Setting $S = S_1 \cup S_2$ with $S_1 = \{\pm e_1, \ldots, \pm e_9, \pm x\}$, we find that this relation has the simple form

$$\sum_{y \in S_1/\{\pm\}} p_y = \sum_{y \in S_2/\{\pm\}} p_y.$$  \hfill (7)

By [BM09] Lemma 2.9, this implies the identity

$$\sum_{y \in S_1/\{\pm\}} N(y) = \sum_{y \in S_2/\{\pm\}} N(y)$$

between norms. This implies (still assuming that $\min \Lambda = N(e_i)$) that all vectors in $S_2$ are actually minimal, so that we obtain a simple proof using calculations “by hand” only. Note however, that guessing the necessary identity (7) would have been difficult without the help of a computer!

8. A 10-DIMENSIONAL COUNTEREXAMPLE

To complete the proof of Theorem 1.1 for $\tau = 5$, it only remains to exhibit a 10-dimensional counterexample. With the notations of the previous section, we give one with parameters $m_1 = 3$, $m_2 = 7$ and $m_3 = 3$, $m'_3 = 4$. With respect to the basis $(e, e_2, \ldots, e_{10})$ we consider coordinates $\bar{e}^{(1)} = (-5, 1, 1, 2, 2, 2, 2, 2, 2)$ for $e_1$ and $a = (-4, 0, 0, 2, 2, 1, 1, 1, 1)$ for an additional minimal vector $x$ that generates the lattice $\Lambda$ together with the $e_i$. We can make use of some symmetry, as the set of coordinate vectors $(\bar{e}^{(i)}, i = 1, \ldots, 10, \text{and} a)$ is invariant with respect to permutations of $e_2, e_3$, of $e_4, e_5, e_6$ and of $e_7, e_8, e_9, e_{10}$. Assuming a fixed minimum, all of these linear conditions turn out to define a polytope of Gram matrices with 154 vertices. Its vertex barycenter is a Gram matrix which we can scale to have integral coordinates and minimum 6209280. Up to isometry, it defines a lattice $\Lambda$ having only the $s = 11$ pairs of minimal vectors that we assumed.
from the beginning (namely \(x\) and the ten vectors \(e_i\)). It is readily verified that any system of 10 independent vectors extracted from this set generates a sublattice \(L\) of \(\Lambda\) with \(\Lambda/L\) cyclic of order 2, 3, 4 or 5, but not 1.

Since the vertex barycenter of the “realization polytope” mentioned above has quite inconvenient coordinates, we provide below a slightly nicer counterexample in the same polytope. An analysis of the 154 vertices shows that it is possible to take some of the midpoints of two vertices as an interior point. All of these counterexamples have the same parameters. Among them, there is a unique one that we can scale to have integral coordinates and minimum 48:

\[
\begin{pmatrix}
88 & -3 & -3 & 40 & 40 & 40 & 26 & 26 & 26 & 26 \\
-3 & 48 & 10 & 5 & 5 & 5 & -13 & -13 & -13 & -13 \\
-3 & 10 & 48 & 5 & 5 & 5 & -13 & -13 & -13 & -13 \\
40 & 5 & 5 & 48 & 14 & 14 & 4 & 4 & 4 & 4 \\
40 & 5 & 5 & 14 & 48 & 14 & 4 & 4 & 4 & 4 \\
40 & 5 & 5 & 14 & 14 & 48 & 4 & 4 & 4 & 4 \\
26 & -13 & -13 & 4 & 4 & 4 & 48 & 8 & 8 & 8 \\
26 & -13 & -13 & 4 & 4 & 4 & 8 & 48 & 8 & 8 \\
26 & -13 & -13 & 4 & 4 & 4 & 8 & 8 & 48 & 8 \\
26 & -13 & -13 & 4 & 4 & 4 & 8 & 8 & 8 & 48
\end{pmatrix}
\]

**Acknowledgments**

We would like to thank the anonymous referee for his helpful comments. The second author would like to thank the Institut de Mathématiques at Université Bordeaux 1 for its great hospitality during two visits, on which major parts of this work were created.

**References**

[BM09] A.-M. Bergé and J. Martinet, *On perfection relations in lattices*, Contemp. Math., 493 (2009), 29–49; preprint at [arXiv:math/0611220](http://arxiv.org/abs/math/0611220).

[CS95] J.H. Conway and N.J.A. Sloane, *A lattice without a basis of minimal vectors*, Mathematika 42 (1995), 175–177.

[Mar01] J. Martinet (with an appendix by Christian Batut), *Sur l’indice d’un sous-réseau*, Réseaux Euclidiens designs sphériques et forms modulaires, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001, pp. 163–211.

[Mar03] J. Martinet, *Perfect lattices in Euclidean spaces*, Springer, Berlin, 2003.

[Mar07] J. Martinet, *Bases of minimal vectors in lattices, I*, Archiv Math. 89 (2007), 404–410.

[KMS11] W. Keller, J. Martinet and A. Schürmann (with an appendix by M. Dutour Sikirić) *On classifying Minkowskian sublattices*, Math. Comp., to appear; preprint at [arXiv:0904.3110](http://arxiv.org/abs/0904.3110).

[Sch09] A. Schürmann, *Computational geometry of positive definite quadratic forms*, AMS, Providence, 2009.

**Software**

[LRS] *lrs* by D. Avis, ver. 4.2., [http://cgm.cs.mcgill.ca/~avis/C/lrs.html](http://cgm.cs.mcgill.ca/~avis/C/lrs.html).
[MAGMA] MAGMA — high performance software for Algebra, Number Theory, and Geometry, ver. 2.13. [http://magma.maths.usyd.edu.au/]

[PARI] PARI/GP, a computer algebra system designed for fast computations in number theory. [http://pari.math.u-bordeaux.fr/]

Institut de Mathématiques, 351, cours de la Libération, 33405 Talence cedex, France
E-mail address: Jacques.Martinet@math.u-bordeaux1.fr

Institute of Mathematics, University of Rostock, 18051 Rostock, Germany
E-mail address: achill.schuermann@uni-rostock.de