 EXTRACTA MATHEMATICAE

Article in press
Available online May 21, 2025

On the coordinates of minimal vectors in a Minkowski-reduced basis

Ákos G. Horváth

Department of Algebra and Geometry, Budapest University of Technology
Egry József u. 1*, Budapest, Hungary,* 1111
ghorvath@math.bme.hu

Received October 11, 2024
Accepted May 9, 2025

Presented by J.B. Sancho

Abstract: Finding the shortest non-zero vectors in a lattice is a computationally hard problem (NP-hard in general dimensions), making results in low dimensions particularly important in lattice reduction theory. This paper focuses on the coordinates of minimal lattice vectors when expressed in a Minkowski-reduced basis. By applying Ryskov's findings on admissible centerings and Tammela's work characterizing Minkowski-reduced forms via a finite set of inequalities (up to dimension 6), we demonstrate sharp bounds on the absolute values of these coordinates. Specifically, we show that for dimensions $n \leq 6$, the absolute values of the coordinates of any minimal vector with respect to a Minkowski-reduced basis are bounded by 1 (for $n = 2, 3$), 2 (for $n = 4, 5$), and 3 (for $n = 6$). This refines bounds implicitly available from Tammela's results by combining geometric arguments from lattice theory, admissible centering theory, and reduction theory.

Key words: Dirichlet-Voronoi cell, minimum vector of a lattice, Minkowski-reduction, admissible centering, positive quadratic forms.

MSC (2020): 11H50, 11H55.

1. Introduction

A lattice L is a discrete subgroup of the Euclidean space $\mathbb{R}^n$. Every lattice possesses a basis, a set of linearly independent vectors $\{e_1, \ldots, e_n\}$ such that any vector $v \in L$ can be uniquely written as $v = \sum_{i=1}^{n} z_i e_i$ with integer coefficients $z_i \in \mathbb{Z}$. The integer n is the dimension (or rank) of the lattice. A central theme in the geometry of numbers is lattice reduction, which aims to find a "good" basis for a given lattice, typically consisting of vectors that are relatively short and nearly orthogonal.

Classical reduction theories include those by Hermite [4], Minkowski [7], Korkine-Zolotarev [6], and Venkov [15]. While these notions often coincide in low dimensions (e.g., Minkowski and Hermite reduction are equivalent for $n \leq 6$ [9]), they differ in higher dimensions (e.g., [5]). For a comprehensive overview, see [3].

ISSN: 0213-8743 (print), 2605-5686 (online)

A fundamental problem in lattice theory is finding the shortest non-zero vector(s), known as minimal vectors. The length of a minimal vector is the first successive minimum of the lattice. All classical reduction algorithms implicitly assume this shortest vector problem (SVP) is solvable, although finding minimal vectors is NP-hard under randomized reductions.

The structure defined by the set of minimal vectors is crucial in various fields, including coding theory, discrete geometry, and the study of root lattices. Determining the properties of minimal vectors, such as their coordinates relative to a reduced basis, is therefore of significant interest. This article focuses on bounding these coordinates when the basis is Minkowski-reduced, for dimensions $n \leq 6$. We leverage the theory of admissible centerings and Tammela's characterization of Minkowski-reduced forms to establish our main result, Theorem 3.1.

2. Preliminaries: lattices, reduction, and centerings

Let L be an n-dimensional lattice in $\mathbb{R}^n$. We denote the lattice generated by a basis $\{e_1, \ldots, e_n\}$ as $L[e_1, \ldots, e_n]$. The linear span is denoted by $\mathrm{Lin}[e_1, \ldots, e_n]$.

Definition 2.1. A set of linearly independent lattice vectors $\{f_1, \ldots, f_k\}$ is a *primitive system*, if any lattice vector in their linear span can be expressed as an integer linear combination of them, i.e.,

$$\mathrm{Lin}[f_1, \ldots, f_k] \cap L[e_1, \ldots, e_n] = L[f_1, \ldots, f_k].$$

Equivalently, the set $\{f_1, \ldots, f_k\}$ can be extended to a basis of the lattice L. A single non-zero vector $v \in L$ is primitive if $v/k \notin L$ for any integer $k > 1$. Every subset of a primitive system is also a primitive system, and minimal vectors are always primitive.

Definition 2.2. (Successive minima) Let L be an n-dimensional lattice. The i-th successive minimum $\lambda_i(L)$ $(1 \leq i \leq n)$ is the smallest real number r such that L contains i linearly independent vectors of length at most r. A set of vectors $\{a_1, \ldots, a_n\}$ such that $|a_i| = \lambda_i(L)$ for all i, and $a_1, \ldots, a_i$ are linearly independent vectors achieving the i-th minimum for each i, is called a system realizing the successive minima. Note that a_1 is a minimal vector.

A system realizing successive minima does not necessarily form a basis. Minkowski reduction provides a way to construct a basis related to these minima.

DEFINITION 2.3. An ordered basis $\{a_1, \ldots, a_n\}$ of a lattice L is Minkowski-reduced if, for each $i \in \{1, \ldots, n\}$, a_i is a shortest vector among all lattice vectors $v \in L$ such that $\{a_1, \ldots, a_{i-1}, v\}$ can be extended to a basis of L. Equivalently, let a_1 be a minimal vector of L. Let a_2 be a minimal vector among those $v \in L$ such that $\{a_1, v\}$ is a primitive system. Continue this process: a_i is a minimal vector among those $v \in L$ such that $\{a_1, a_2, \cdots a_{i-1}, v\}$ is a primitive system. We call the complete system $\{a_1, a_2, \cdots a_n\}$ a *Minkowski-reduced basis.*

Alternatively, Minkowski reduction can be defined via positive definite quadratic forms. A lattice $L = A\mathbb{Z}^n$ (where A is a matrix of a regular linear transformation of $\mathbb{R}^n$) corresponds to the quadratic form $Q(x) = |Ax|^2 = x^T(A^TA)x$. Two forms Q and Q' are equivalent if to each other if $Q'(x) = Q(U(x))$ for some unimodular transformation U (integer matrix with determinant ± 1). The equivalent forms correspond to distinct bases of the same lattice. A positive quadratic form Q is called *Minkowski-reduced* if $Q(u) \geq Q(e_i)$ holds for $1 \leq i \leq n$ and all integer vectors $u = (u_1, \ldots, u_n)^T \in Y$ with g.c.d.$(u_i, \ldots, u_n) = 1$. Here e_i is the i-th standard basis vector in $\mathbb{Z}^n$.

All lattices have a Minkowski-reduced basis, implying that each positive definite quadratic form is equivalent to a Minkowski-reduced form.

2.1. ADMISSIBLE CENTERINGS. The lattice $L[e_1, \ldots, e_n]$ of dimension n is a *centering* of the lattice $L'[a_1, \ldots, a_n]$ (of the same dimension) if

$$L'[a_1, \ldots, a_n] \subset L[e_1, \ldots, e_n].$$

We have to define first the concept of *admissible centering* of the lattice L' in the case where there is a basis of L' of shortest vectors. (So in the lattice L' there is a *minimum basis*). A lattice L' with a minimum basis *can be centered in an admissible way* by the lattice L, if $\min L' = \min L$. Since there is no minimum basis in all lattices, we can reformulate the definition of admissible centerings, focusing on the idea of successive minima.

DEFINITION 2.4. Take n independent lattice vectors $\{a_1, \ldots, a_n\}$ whose lengths are the successive minima of the lattice $L[e_1, \ldots, e_n]$. We say that $L[e_1, \ldots, e_n]$ is an *admissible centering of* $L'[a_1, \ldots, a_n]$ if for any sequence $1 \leq i_1 < \ldots < i_k \leq n$ of indices in the lattice $\mathrm{Lin}[a_{i_1}, \ldots, a_{i_k}] \cap L[e_1, \ldots, e_n]$ the successive minima are $|a_{i_1}| \leq \ldots \leq |a_{i_k}|$.

Every linearly independent set $\{a_1, \ldots, a_n\}$ of lattice vectors defines a *lattice parallelepiped*

$$\Pi[a_1,\dots,a_n] := \left\{ \sum\nolimits_{i=1}^{n} x_i a_i \ : \ 0 \le x_i < 1 \text{ for all } i \right\}.$$

Let $L'[a_1,\dots,a_n]$ be a lattice with minimum basis $\{a_1,\dots,a_n\}$ and $L[e_1,\dots,e_n]$ one of its admissible centerings. Then there are finitely many points $\{s_1,\dots s_j\}$ of $L[e_1,\dots,e_n]$ in the parallelepiped $\Pi[a_1,\dots,a_n]$ with the following property: The vector system $\{a_1,\dots,a_n,s_1,\dots s_j\}$ generates the lattice $L[e_1,\dots,e_n]$.

In this case, we also say that the parallelepiped $\Pi[a_1,\dots,a_n]$ has an admissible centering. Since in the above case $\Pi[a_1,\dots,a_n]$ is generated by minimum vectors of the lattice, we call it *minimum parallelepiped*.

n	U	V	relevant rows (Coordinates of centering vectors)
2	1	1	$(0,0)$
3	1	1	$(0,0,0)$
4	1	1	$(0,0,0,0)$
4	2	2	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$
5	1	1	$(0,0,0,0,0)$
5	2	2	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},0\right)$
5	2	2	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$
6	1	1	$(0,0,0,0,0,0)$
6	2	2	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},0,0\right)$
6	2	2	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},0\right)$
6	2	2	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$
6	2	4	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},0,0\right), \left(\frac{1}{2},\frac{1}{2},0,0,\frac{1}{2},\frac{1}{2}\right), \left(0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$
6	3	3	$\left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{3}\right)$

Table 1: Relevant rows for $n \le 6$. V is the index, U is the LCM of denominators.

The modified version of this notation for a lattice formed by successive minimum vectors of the lattice is used, too. Ryskov [11] proved that in a given dimension, all combinatorial types of admissible centering arise as the admissible centering of a minimum parallelepiped. Hence, the relative connection between the two lattices can always be described as an admissible centering of a lattice with a minimum basis. If a given dimension, the admissible centerings are classified, then we know the possible connections between the given lattice $L[e_1, \dots, e_n]$ and its sublattices $L'[a_1, \dots, a_n]$. The Table 1 that displays the results of Ryskov contains the most important geometric data of the admissible centerings of a minimum parallelepiped. The points $\{s_1, \dots s_j\}$ defining the centering of the parallelepiped $\Pi[a_1, \dots, a_n]$ clearly have rational coordinates with respect to the basis $\{a_1, \dots, a_n\}$. The least common multiple U of the denominators of the coordinates of the points $\{s_1, \dots s_j\}$ divides the determinant

$$V = [L : L'[a_1, \dots, a_n]] = \mathrm{vol}(\Pi[a_1, \dots, a_n])/\mathrm{vol}(\Pi[e_1, \dots, e_n]).$$

The *index* (or the volume ratio of the centering) V is an integer related to U. The *relevant rows* contain the coordinates of the fundamental centering vectors $\{s_1, \dots s_j\}$ with respect to the basis $\{a_1, \dots, a_n\}$. Table 1 summarizes the data for $n \leq 6$. Ryskov also gave in [11] similar tables for dimension seven, and Zakharova and Novikova for dimension eight in [16], but there is no similar table in higher dimensions.

2.2. Characterization of the Minkowski reduction via inequalities. A key result, known for $n \leq 6$, characterizes Minkowski-reduced bases using finite set of conditions. Let Q be the quadratic form associated to the basis $\{e_1, \dots, e_n\}$. This basis is Minkowski-reduced if and only if:

1. $Q(e_{i+1}) \geq Q(e_i)$ for $1 \leq i \leq n-1$.
2. $Q(u) \geq Q(e_i)$ for specific vectors $u = \sum_{j=1}^{n} u_i e_i$ can be transformed into a column of the matrix in Table 2, by permuting the coordinates of u and omitting the signs of these coordinates, while $\mathrm{g.c.d}(u_i, \dots, u_n) = 1$.

The checking inequalities in Table 2 was announced by Minkowski for $n \leq 6$ and proved by Minkowski for $n \leq 4$ ([8]), Ryskov (in [10]) and later Afflerbach (in [1]) for $n = 5$ and by Tammela for $n = 6$. Tammela in [14] slightly refined and extended the result to the case $n = 7$.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 3 \end{pmatrix}$$

Table 2: Checking inequalities of reduction when $n \leq 6$.

The result says that $\{e_1, \ldots, e_n\}$ forms a Minkowski-reduced basis in its lattice $L[e_1, \ldots, e_n]$ if for the above finite number of inequalities $Q(u) \geq Q(e_i)$ holds with the vectors permitted by the table. Conversely, if we find a vector u that is allowed by the table and for which the inverse inequality is satisfied, the base under consideration is not Minkowski-reduced; the lattice vector u is a better choice for the reduction algorithm than the choice given by the corresponding element of the base.

$$\left(\begin{array}{ccccccccc||ccccccccc||ccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 2 & 2 & 0 & 0 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 3 & 0 & 0 & 0 & 3 & 2 & 3 & 4 & 3 & m & 0 & 3 & 4 & 4 & 3 \end{array}\right)$$

Table 3: Checking inequalities of the relevants of the Dirichlet-Voronoi cell.

Crucially, minimal vectors of a lattice are relevant vectors for its Dirichlet-Voronoi (DV) cell centered at the origin. Tammela [13] proved that for $n \leq 6$, if $\{e_1, \ldots, e_n\}$ is a Minkowski-reduced basis, the coordinates $(x_1, \ldots, x_n)$ of any relevant vector of the DV cell (and thus any minimal vector $m = \sum_{i=1}^{n} x_i e_i$), up to permutation and signs, correspond to a column in a specific,

larger table (Table 3, which combines Table 2 with vectors relevant for the DV cell). (In the process, we have to exclude the last column $(1,1,1,1,2,m)^T$ of the second part, partitioned by two vertical doubled lines in the table). The first chunk in Table 2 coincides with Table 2, this part is needed to find the reduced basis. The second part contains the possible vectors that may be shorter than the longest basis vector included in the reduced basis. In the n-dimensional case, we have to consider only those columns of the table in which the number of non-zero coordinates does not exceed n.

Since every vector of minimum length is a relevant vector of the Dirichlet-Voronoi cell of the origin, the coordinates of these vectors (apart from their sign and the possible permutations) with respect to a Minkowski-reduced basis are included in the columns of the table.

We note that the book by Achill Schürmann [12] contains more recent results on 7-dimensional Minkowski-reduced forms, but our proof would lead to a highly complicated discussion in the case of 7-dimensional lattices. Therefore, in this paper, we only focus on the six-dimensional case.

3. Main result and preparatory lemmas

Let $n \leq 6$ and assume that the lattice $L[e_1, \ldots, e_6]$ is spanned by a Minkowski-reduced basis. Combining the results on admissible centerings with the results of reduction theory, we can prove a sharpening of Tammela's result on the coordinates of the minimum vectors. Table 3 shows that the maximum absolute value of the coordinates in 5 or 6 dimensions can be 3 or 4. In the following Theorem we obtain sharp bounds.

Theorem 3.1. *Let L be an n-dimensional lattice, where $n \leq 6$, $m = \sum_{i=1}^{n} x_i e_i$ be an arbitrary minimal vector of L, where $\{e_1, \ldots, e_n\}$ is a Minkowski-reduced basis of the lattice. Then, for an arbitrary index i, the following inequalities are satisfied:*

$$|x_i| \leq \begin{cases} 1 & \text{if } n = 2, 3\,, \\ 2 & \text{if } n = 4, 5\,, \\ 3 & \text{if } n = 6\,. \end{cases}$$

First, we highlight some easy geometric observations which we repeatedly use in our proof:

1. $\mathrm{vol}(L) = \det(\{e_1, \ldots, e_n\}) = 1$

2. The minimal vector $m = \sum x_i e_i$ under investigation has $x_i \neq 0$ for all i. If some $x_k = 0$, the problem reduces to a lower-dimensional one, and the bounds would hold by induction.
3. $|m| = \lambda_1(L) = 1$.

We need several lemmas.

LEMMA 3.2. (VOLUME AND CENTERING DENOMINATORS) *If a parallelepiped* $\Pi[a_1, \ldots, a_n]$ *has a* k*-dimensional centered face of denominator* 2 *then its volume is even.*

Proof. If the centered face is $\Pi[a_1, \ldots, a_k]$ then the coordinates of the vector $b = (1/2)(a_1 + \ldots + a_k) \in L[e_1, \ldots, e_n]$ are integers, respectively. Hence the volume of $\Pi[b, a_2, \ldots, a_n]$ is also an integer. But

$$\begin{aligned} \mathrm{vol}(\Pi[b, a_2, \ldots, a_n]) &= \det[b, a_2, \ldots, a_n] \\ &= (1/2)\det[a_1 + \ldots + a_k, a_2, \ldots, a_n] \\ &= (1/2)\mathrm{vol}(\Pi[a_1, a_2, \ldots, a_n]) \end{aligned}$$

proves the statement. ∎

LEMMA 3.3. *For all indices* i *the inequality* $|x_i| \leq 4$ *holds.*

Proof. The minimum vectors of the lattice $L[e_1, \ldots, e_n]$ are relevant vectors of the Dirichlet-Voronoi cell of the origin, so by Theorem 2 in [13] the absolute value of the coordinates of the minimum vectors with respect to a Minkowski-reduced basis can be found in that modification of Table 3 in which the last column of the middle part is omitted. Hence for all i we have $|x_i| \leq 4$. ∎

LEMMA 3.4. (LEXICOGRAPHICAL MINIMALITY) *Let* $\{e_1, e_2, \ldots e_6\}$ *be a Minkowski-reduced basis of the lattice then in the proof of the theorem we can assume that* $|e_1| = |e_2| = |e_3| = |e_4| = |m| = 1$.

Proof. We recall a result of G. Csóka [2]. It says that in an n-dimensional lattice with $n \leq 6$, the Minkowski-reduced basis is the lexicographical minima of the set of such bases, which are ordered by the increasing lengths of their elements. (Observe that this theorem is a consequence of the fact (is proved by Ryskov) that the domains of the Minkowski-reduced forms, Hermite-reduced

forms, and $L^\star$-reduced forms are agreed for $n \leq 6$.) From this, the first four elements of a Minkowski-reduced basis give a primitive system of successive minimum vectors. So, Ryskov's affinity sends these vectors to a primitive system of minimum vectors of the image lattice without changing the coordinates of a minimum vector. ∎

LEMMA 3.5. (PRIMITIVE SYSTEMS AND REDUCTION VECTORS) *Assume that the lattice $L := L[e_1, \ldots, e_n]$ is spanned by the Minkowski-reduced basis $\{e_1, \ldots, e_n\}$, where $n \leq 6$. Let $\{e_1, \ldots, e_{n-2}, x\}$ be a primitive system with the vector $x = \sum_{i=1}^{n} x_i e_i$, having the property that $x_n \neq 0$. (Clearly, we have that $|e_1| \leq \ldots \leq |e_{n-1}| \leq |x|$.) There is a column $\alpha := \alpha_1 e_1 + \cdots + \alpha_{n-1} e_{n-1} + \alpha_n e_n$ in the n-dimensional part of Table 2 for which also holds that*

$$\alpha = \sum_{i=1}^{n-2} y_i e_i \; + \; y_{n-1} x,$$

consequently simultaneously hold the equalities

$$\alpha_{n-1} = y_{n-1} x_{n-1} \qquad \text{and} \qquad \alpha_n = y_{n-1} x_n$$

with such non-zero integers which absolute values are in Table 2.

Proof. With a suitable affinity φ we define a lattice of form $L^\star = \varphi(L)$ in which $\{e_1 \ldots e_{n-2}, x\}$ is a primitive system (hence $L[e_1, \ldots e_{n-2}, x]$ is a common complete sublattice both of L and $L^\star$) and the minimum value of the length of those vectors which don't belong to $L[e_1, \ldots e_{n-2}, x]$ is greater than $|x|$. Then $\{e_1 \ldots e_{n-2}, \varphi(e_{n-1})\}$ in its lattice couldn't be a Minkowski-reduced basis ($\varphi(e_{n-1}) \notin L[e_1, \ldots e_{n-2}, x]$) hence there is such a column $\alpha := \alpha_1 e_1 + \ldots + \alpha_{n-1}\varphi(e_{n-1}) + \alpha_n \varphi(e_n)$ in the n-dimensional part of Table 2, which exclude $\varphi(e_{n-1})$ from the possible Minkowski-reduced basis elements. But the vector in $L^\star$ corresponding to α has to be shorter then $\varphi(e_{n-1})$. Hence it is in $\mathrm{Lin}[e_1, \ldots e_{n-2}, x] \cap L = \mathrm{Lin}[e_1, \ldots e_{n-2}, x] \cap L^\star$ (the common lattice layer of L and $L^\star$) implying that $\alpha = y_1 e_1 + \ldots + y_{n-2} e_{n-2} + y_{n-1} x$ where y_i's are all non-zero integers as we stated.

Now we prove the existence of a lattice $L^\star$ with the above properties. Since $\{e_1, \ldots, e_{n-2}, x\}$ is a primitive system we have g.c.d$(x_{n-1}, x_n) = 1$. By our assumption $x_n \neq 0$. Let $z = z_1 + z_2$ be an orthogonal decomposition of $z \in \mathbb{R}^n$, where $z_1 \in \mathrm{Lin}[e_1, \ldots, e_{n-2}, x]$. If $x_{n-1} = 0$ then $L[e_1, \ldots e_{n-2}, x] = L[e_1, \ldots e_{n-2}, e_n]$ holds and e_{n-1} each vector is in the form

$$v = v_1 e_1 + \ldots + v_{n-1} e_{n-1} + v_{n-1} x + k e_{n-1} \qquad \text{with a } \; k \in \mathbb{Z}.$$

Let $\varphi(z) := z_1 + (1+\varepsilon)z_2$ be an affinity with an arbitrary positive ε. Then, for $k \neq 0$, $\varphi(v)$ is equal to $v_1e_1 + \ldots + v_{n-1}e_{n-1} + v_{n-1}x + k\varphi(e_{n-1})$ and for $v \in L \setminus L[e_1, \ldots, e_{n-2}, x]$ the minimal value of $|\varphi(v)|$ is equal to $|\varphi(e_{n-1})|$ since the basis $\{e_1 \ldots e_n\}$ is a Minkowski-reduced one. Clearly, we can choose ε on such a way that the condition $|\varphi(e_{n-1})| > |x|$ also holds. In the other case, when $x_{n-1} \neq 0$ we have $e_{n-1} = \frac{1}{x_{n-1}}(x - x^\star - x_ne_n) \in L[e_1, \ldots, e_n]$, where $x^\star \in L[e_1, \ldots, e_{n-2}]$. Since the coordinates of $x - x^\star$ are integers (with respect to the basis $\{e_1, \ldots, e_n\}$) we get that $|x_{n-1}| = 1$. Hence $x = x^\star \pm e_{n-1} + x_ne_n$ with a non-zero integer x_n. Hence $L[e_1, \ldots e_{n-2}, x, e_{n-1}]$ is an sublattice of L of index $|x_n|$. Apply the above affinity to this lattice with such ε that the minimum value of the lengths $|\varphi(v)|$ of the lattice vector v of the set $L \setminus L[e_1, \ldots, e_{n-2}, x]$ will be grater than $|x|$. Since $\{e_1, \ldots, e_{n-2}, e_{n-1}\}$ is a primitive system of L then it is also a primitive system of $L[e_1, \ldots e_{n-2}, x, e_{n-1}]$. Thus $\{e_1, \ldots, e_{n-2}, \varphi(e_{n-1})\}$ is a primitive system of $\varphi(L[e_1, \ldots e_{n-2}, x, e_{n-1}])$ but couldn't be a Minkowski-reduced basis in this lattice because of $|\varphi(e_{n-1})| > |x|$, as the required affinity exists in this case, too. ∎

Remark 3.6. (Coordinates when basis vectors are minimal) The assertion of Theorem 3.1 is evident if $\{e_1, \ldots, e_n\}$ is a basis consisting of minimal vectors. In fact,

$$\mathrm{vol}(\Pi[e_1, \ldots, e_{i-1}, m, e_{i+1} \ldots e_n]) = |x_i|\mathrm{vol}(\Pi[e_1, \ldots, e_n]).$$

Using this equality, $|x_i|$ can only be one of the allowed volumes in Table 1. However, this is greater than three only in one case, when $n = 6$ and the volume of the parallelepiped $\Pi[e_1, \ldots, e_{i-1}, m, e_{i+1} \ldots e_n]$ is 4. This case can occur in a specific structure (related to $D_6^\star$). Ryskov showed ([11] Theorem 6) then the five-dimensional sublattice $L'[e_1, \ldots, e_{i-1}, e_{i+1} \ldots e_n]$ contains a four-dimensional body-centered cubic lattice L'' whose index is 2 in $L'[e_1, \ldots, e_{i-1}, e_{i+1} \ldots e_n]$. Then, however, we have the inequality:

$$\begin{aligned} 4 = {} & \mathrm{vol}(\Pi[e_1, \ldots, e_{i-1}, m, e_{i+1} \ldots e_n] \\ & \geq |x_i|\mathrm{ind}(L''/L'[e_1, \ldots, e_{i-1}, e_{i+1} \ldots e_n]) = 2|x_i|, \end{aligned}$$

i.e., $|x_i| \leq 2$ for all i.

4. Proof of Theorem 3.1

Proof. Let $\{e_1, \ldots, e_n\}$ be a Minkowski-reduced basis and $m = \sum x_ie_i$ is a minimum vector in the lattice $L = [e_1, \ldots, e_n]$. Assume that the volume of the

parallelepiped $\Pi[e_1, \ldots, e_n]$ equals 1. By Lemma 3.4, we can assume that the coordinates x_i are non-zero and the first four elements of the basis are minimum vectors. By Remark 3.6, the statement is trivial in dimensions $n \leq 4$; hence, we have to investigate only the cases $n = 5$ and $n = 6$, respectively.

THE FIVE-DIMENSIONAL CASE. We cannot examine the coordinates similarly, as in the case of $n = 4$, so we must consider separate cases in the proof.

- The case of the fifth coordinate x_5. Consider the four-dimensional minimum parallelepiped $\Pi[m, e_1, e_2, e_3]$. Its edges have length 1, so the corresponding vector system is a system of successive minima. Then e_4 be a fifth successive minima, so the lattice $L[e_1, \ldots, e_5]$ is an admissible centering of the lattice $L[m, e_1, e_2, e_3, e_4]$. Hence $\mathrm{vol}(L[m, e_1, e_2, e_3, e_4]) = |x_5| \leq 2$ by Table 1.

- The case of the fourth coordinate x_4. If $\{e_1, e_2, e_3, m\}$ IS A PRIMITIVE SYSTEM then there is a Minkowski-reduced basis with first four elements $\{e_1, e_2, e_3, m\}$. We use Lemma 3.5 with the choice $x = m$, so the coefficients x_i are non-zero integers. The 5-dimensional part of Table 2 gives that for all i we have $|\alpha_i| \leq 2$, and since $|y_4| \geq 1$ we get $|x_4| \leq 2$, too. Assume now that $\{e_1, e_2, e_3, m\}$ IS NOT A PRIMITIVE SYSTEM in $L[e_1, \ldots, e_5]$. Then $L[e_1, \ldots, e_5] \cap \mathrm{Lin}(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3, \mathrm{m})$ is an admissible centering of $L[e_1, e_2, e_3, m]$. Hence the lattice $L[e_1, \ldots, e_5] \cap \mathrm{Lin}(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3, \mathrm{m})$ is a body-centered cubic lattice of dimension four and volume 2. Since e_4 is a fifth vector with the minimal length for which $\{e_1, e_2, e_3, e_4^\star, e_4\}$ should form a basis (there is no admissible centering with volume 4), we can conclude by Lemma 3.4 that e_5 is also a minimum vector. We can finish the proof of this case using the result of the Remark 3.6, so in this case, we also get that $|x_4| \leq 2$.

- Clearly, to prove that $|x_i| \leq 2$ for $i = 1, 2, 3$ the argument of $i = 4$ can be applied again.

THE CASE OF DIMENSION SIX. We will use that the statement is true for $n \leq 5$. Let $\{e_1, \ldots, e_6\}$ be a Minkowski-reduced basis and let $m = \sum_{i=1}^{6} x_i e_i$ be a minimal vector with non-zero integer coefficients. We distinguish two cases (with several subcases).

I: If $\{e_1, \ldots, e_4, m\}$ is a primitive system, then $|e_5| = 1$ and $\Pi[e_1, \ldots, e_5, m]$ is a minimum parallelepiped with volume $|x_6|$. By Lemma 3.3, $|x_6| \leq 4$ and we have to prove that $|x_6| \neq 4$. By Table 1, the only lattice centred by volume 4 is the 6-dimensional cubic lattice. Ryskov showed (see [11] Theorem

6) that this centering has only one metric realization in which the sixth vector e_6 must be minimal vector, too. Therefore, we have $|e_6| = 1$. We can again use the last argument of Remark 3.6 to show that all coordinates of m are less than or equal to 3, as we stated.

II: If $\{e_1, \ldots, e_4, m\}$ is not a primitive system, then the face $\Pi[e_1, \ldots, e_4, m]$ is a centered facet of the parallelepiped $\Pi[e_1, \ldots, e_4, m, e_5]$. By Lemma 3.2 $|x_6| = \mathrm{vol}(\Pi[e_1, \ldots, e_4, m, e_5])$ is an even number. (Note that in this case the columns of Table 1 cannot be directly referenced because $|e_5| > 1$.) According to Lemma 3.3, the value of $|x_6|$ is 2 or 4.

- Suppose first that $|x_6| = 2$. Then there is a lattice vector $e_5^\star \in L[e_1, \ldots, e_4, m]$ for which the system $\{e_1, \ldots, e_4, e_5^\star\}$ is a primitive system. Based on Table 1, there are two essentially distinct options for generating this vector, either $e_5^\star = 1/2(e_1 + \ldots + e_4 + m) + z$ where $z \in L[e_1, \ldots, e_4]$ or

$$e_5^\star = 1/2(e_1 + \ldots + e_{i-1} + e_{i+1} + \ldots + e_4 + m) + z$$

, where $z \in L[e_1, \ldots, e_{i-1}, e_{i+1}, \ldots e_4]$.

- If $e_5^\star = \sum_{i=1}^4((x_i + 1)/2 + k_i)e_i + (x_5/2)e_5 + (x_6/2)e_6$, with integer coordinates, we apply Lemma 3.5 with $x := e_5^\star$. This means that we have an integer vector α for which by the integer coefficient y_{n-1} hold simultaneously two equalities, $\alpha_5 = y_5(x_5/2)$ and $\alpha_6 = y_5$, respectively. Since $|\alpha_6| = |y_5| \leq 3$ and $|\alpha_5| = |y_5||x_5/2| \leq 3$ we have the possibilities: $|y_5| = 3$ and $|x_5| \leq 2$; $|y_5| = 2$ and $|x_5| \leq 3$; or $|y_5| = 1$ and $|x_5| \leq 6$, respectively. By Lemma 3.3, we have to exclude only the case when $|x_5| = 4$. Assume indirectly that $|x_5| = 4$ and consider the system $\{e_1, e_2, e_3, m, e_6\}$. Since $e_5^\star$ has integer coordinates with respect to the original basis, we get x_4 is odd. Since g.c.d$(x_4, x_5) = 1$, therefore $\{e_1, e_2, e_3, m, e_6\}$ is a primitive system in $L[e_1, \ldots, e_6]$. Consequently,

$$\mathrm{Lin}[e_1, e_2, e_3, m, e_6] \cap L[e_1, e_2, e_3, e_6, e_4, e_5] = \mathrm{Lin}[e_1, e_2, e_3, m, e_6]$$

and $e_4 \notin \mathrm{Lin}[e_1, e_2, e_3, m, e_6]$. We can apply Lemma 3.5 such that $x := e_6$. (The affinity of the proof of Lemma 3.5 takes e_4 to e_4', e_5 to e_5', and does not change the vectors e_1, e_2, e_3, m, e_6, nor the coordinates of m). It follows that there is an integer vector

$$\beta = \beta_1 e_1 + \beta_2 e_2 + \beta_3 e_3 + \beta_6 e_6 + \beta_4 e_4' + \beta_5 e_5' \in L[e_1, e_2, e_3, m, e_6]$$

with coordinates from Table 2. Thus for all i we have $|\beta_i| \leq 3$ is an integer. Since

$$m = m' = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4' + x_5e_5' + x_6e_6\,,$$
$$\beta = y_1e_1 + y_2e_2 + y_3e_3 + y_4m + y_6e_6$$

implying that $|\beta_5| = |y_4x_5| \leq 3$ and $|\beta_4| = |y_4x_4|$. But $|x_5| = 4$ hence the first inequality leads to three possibilities. These correspond to the values $k = 1, 2$ or 3 concerning the equality $|y_4| = k/4$. ($k = 0$ implies that $\beta \in L[e_1, e_2, e_3, e_6]$ therefore in this case we cannot choose e_6 to be the sixth element of a Minkowski-reduced basis). But $|y_4x_4|$ is also an integer; hence, x_4 is even, which is a contradiction with the fact that x_4 is odd. Finally, we have got that $|x_5| \leq 3$. But $|x_5| = 2$ because it is non-zero and even. Let us investigate now the first four coordinates. By the above argument $|y_4| = k/2$ where $k = 1, 2$ or 3. Since x_4 is odd then $k = 2$, $|y_4| = 1$ and $3 \geq |\beta_4| = |x_4|$ proves the required inequality for the fourth coordinate x_4, too. The first four coordinates are equivalent to our arguments, so in this case, the equality $|x_i| \leq 3$ holds for all i, too.

- Secondly, assume that

$$e_5^\star = \sum_{i=2}^{4}((x_i + 1)/2 + k_i)e_i + (x_5/2)e_5 + e_6,$$

hence $e_5^\star$ gives a admissible centering of the minimal 4-dimensional parallelepiped $\Pi[e_2, e_3, e_4, m]$. This means that $e_5^\star$ is a minimal vector, and $\{e_1, e_2, e_3, e_4, e_5^\star\}$ is a primitive system of minimal vectors. So e_5 is a minimal vector, too. Since $\{e_1, e_2, e_3, e_4, e_5, e_5^\star\}$ is a basis, then e_6 is a minimal vector, and we can apply the result of Remark 3.6. Hence, the absolute values of the coordinates of m are less or equal to 3 in this subcase, too.

- Secondly, assume that $|x_6| = 4$. (Remember that $\{e_1, \ldots, e_4, m\}$ is not a primitive system in this case.) Recall that the parallelepiped $\Pi[e_1, \ldots, e_4, m, e_5]$ has volume 4. Let a_5 be a sixth vector whose length is the sixth successive minimum of the lattice concerning the system $\{e_1, \ldots, e_4, m\}$ of minimum vectors. The volume of the parallelepiped $\Pi[e_1 \ldots, e_4, m, a_5]$ is less or equal to 4 because its admissible centering is the lattice $L[e_1 \ldots, e_6]$.

  - If $\mathrm{vol}(\Pi[e_1, \ldots, e_4, m, a_5]) = 2$ and the vector $e_5^\star$ centers the facet $\Pi[e_1, \ldots, e_4, m]$ then we get that $\{e_1, \ldots, e_4, a_5, e_5^\star\}$ is a basis. If $|e_5^\star| \leq$

$|a_5|$ then we get $|a_5| \geq |e_5^\star| \geq |e_5|$ implying that $|a_5| = |e_5|$. Now $\{e_1, \dots, e_4, m, e_5\}$ is a system of successive minimum vectors, and so the centering of $\Pi[e_1, \dots, e_4, m, e_5]$ is the admissible centering of the cubic lattice with index 4. But there is no minimum vector with coordinate 4 in this lattice, giving a contradiction. So we have $|e_5^\star| > |a_5|$ and so $\{e_1, \dots, e_4, a_5, e_5^\star\}$ is an ordered basis. Hence, again, $|a_5| = |e_5|$ leads to the same contradiction as above.

- If $\mathrm{vol}(\Pi[e_1, \dots, e_4, m, a_5]) = 4$, then the centering is combinatorially agreed with the centering of the 6-dimensional cube with index 4. Hence, a 4-dimensional centered face by index 2 contains a_5 as an edge vector. Let x be the shortest half diagonal of this face. It is shorter than the half-diagonal of a brick with the same edge lengths and longer than a_5. Thus $|a_5|^2 \leq |x|^2 \leq (3 + |a_5|^2)/4$ so $|a_5|^2 = 1$ and the successive minimum vector is a minimum vector. The lattice $L[e_1, \dots, e_4, m, a_5]$ is the 6-dimensional cubic lattice and $L[e_1, \dots, e_4, e_5, e_6]$ is its admissible centering. In this lattice, the Minkowski reduced basis is minimal, so we can apply Remark 3.6 again. ∎

The sharpness of the bounds is shown by explicit examples: For $n = 4, 5$, the centred cubic lattice of dimension n gives sharp bound. This generated by the Minkowski-reduced basis $\{a_1, \dots, a_{n-1}, \frac{1}{2}\sum_{i=1}^n a_i\}$, where $\{a_1, \dots a_n\}$ is an orthonormed basis of $\mathbb{R}^n$. For $n = 6$ consider the lattice $L'[a_1, \dots a_n]$ with associated quadratic form

$$f(x) = \frac{9}{10}\sum_{i=1}^n x_i^2 + \frac{1}{10}\left(\sum_{i=1}^n x_i\right)^2 .$$

Hence we have that

$$\langle a_i, a_j \rangle = \begin{cases} 1 & \text{if } i = j\,, \\ \frac{1}{10} & \text{if } i = j\,. \end{cases}$$

The lattice $L'[a_1, \dots a_n]$ has an admissible centering with the vector $\frac{1}{3}\sum_{i=1}^n a_i$ getting a lattice with Minkowski-reduced basis $\left\{a_1, \dots, a_{n-1}, \frac{1}{3}\sum_{i=1}^n a_i\right\}$. In $L\left[a_1, \dots, a_{n-1}, \frac{1}{3}\sum_{i=1}^n a_i\right]$ the n-th coordinate of the minimal vector a_n is equal to 3.

References

[1] L. Afflerbach, Minkowskische Reduktionsbedingungen für positiv definite quadratische Formen in 5 Variablen, *Monatsh. Math.* **94** (1982), 1 – 8.

[2] G. Csóka, On an extremal property of Minkowski-reduced frames (Russian), *Studia Sci. Math. Hungar.* **13** (1978), 469 – 475.

[3] P.M. Gruber, C.G. Lekkerkerker, "Geometry of numbers", Second Edition, North-Holland Math. Library, 37, North-Holland Publishing Co., Amsterdam, 1987.

[4] C. Hermite, Extraits de lettres de M.Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre, *J. Reine Angew. Math.* **40** (1850), 279 – 290.

[5] Á.G. Horváth, On n-dimensional Minkowski-reduced and Hermite-reduced lattice bases (Hungarian), *Mat. Lapok* **33** (1982/86), 93 – 98.

[6] A. Korkine, G. Zolotareff, Sur les formes quadratiques (French), *Math. Ann.* **6** (1873), 336 – 389.

[7] H. Minkowski, "Geometrie der Zahlen", Teubner-Verlag, 1896.

[8] H. Minkowski, Sur la reduction des formes quadratiques positives quaternaries, in "Gesammelte Abhandlungen I", Teubner, Leipzig-Berlin, 1911, 145 – 148.

[9] S.S. Ryskov, On Hermite, Minkowski and Venkov reduction of positive quadratic forms in n variables (Russian), *Soviet Math. Dokl.* **13** (1972), 1676 – 1679.

[10] S.S. Ryskov, The theory of Hermite-Minkowski reduction of positive definite quadratic forms (Russian), *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **33** (1973), 37 – 64.

[11] S.S. Ryskov, On the problem of finding perfect quadratic forms in higher space (in Russian), *Trudy Mat. Inst. Steklov.* **142** (1976), 215 – 239.

[12] A. Schürmann, "Computational geometry of positive definite quadratic forms: polyhedral reduction theories, algorithms, and applications", Univ. Lecture Ser., 48, American Mathematical Society, Providence, RI, 2009.

[13] P.P. Tammela, On reduction theory of positive quadratic forms (Russian), *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **50** (1975), 6 – 96, 195.

[14] P.P. Tammela, The minkowski reduction domain for positive quadratic forms of seven variables (Russian), *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **67** (1977), 108 – 143, 226.

[15] B.A. Venkov, On the reduction of positive quadratic forms. *Izv. Akad. Nauk SSSR Ser. Mat.* **4/1** (1940), 37 – 52.

[16] N.V. Zakharova, Centerings of eight-dimensional lattices that preserves a frame of successive minima, Geometry of positive quadratic forms (Russian), *Trudy Mat. Inst. Steklov.* **152** (1980), 97 – 123, 237. Correction: N.V. Novikova, Three admissible centerings of eight-dimensional lattices (Russian), *Deposited in VINITI* No. 4842-81, Dep. 1981, I.8.