Studia Scientiarum Mathematicarum Hungarica 29 (1994), 169–175

ON THE COORDINATES OF MINIMUM VECTORS IN n-LATTICES

Á. G. HORVÁTH

Abstract

In this paper the following problem will be discussed: How to find such a basis of an n-lattice in E^n that with respect to this basis the absolute values of the coordinates belonging to the minima of this lattice are "small enough". We prove that in every lattice possessing n linearly independent minima one can find such a basis for which the maximum of the absolute values of the coordinates belonging to a minimum vector is not greater than the maximum of the indices of the admissible centerings of the n-dimensional lattices. This result is not sharp, we prove that in the lower dimensional cases, where $n \leqq 5$ in every lattice with n linearly independent minima there exists a basis for which all the coordinates of the minima are equal to -1, 0 or 1; and in the cases $n = 4$ and 5 the maximal admissible index is equal to 2.

1. Definitions

A lattice in E^n defined by the basis $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ of E^n is the set $L = \sum_{i=1}^{n} x_i \mathbf{a}_i$ of all integral linear combinations of the basis A. A minimum vector (or minimum) of L is one of the shortest non-zero vectors in L. A minimum basis A of L is then such a basis in L for which all the basis vectors $\mathbf{a}_i$ are minimum vectors of L. The common length of the minima is denoted by $\min L$. Let us define now the numbers $L(A)$ and L_n in the following way:

$$(1) \qquad L(A) = L(\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}) := \max\Big\{ |x_i|; \mathrm{m} = \sum_{i=1}^{n} x_i \mathbf{a}_i \in L, |\mathrm{m}| = \min L \Big\}$$

$$(2) \qquad L_n := \sup\Big\{ \min\{L(A) \mid A \text{ is a basis of } L\} \mid L \subset E^n \text{ is a lattice possessing } n \text{ independent minima} \Big\}.$$

1991 *Mathematics Subject Classification.* Primary 52C07; Secondary 11H50.
Key words and phrases. Lattice, minimum vector basis.

Supported by the Hungarian National Found for Scientific Research Grant No. 1615 (1991).

We will use some results from the theory on admissible centerings of n-lattices (see [5], [2]) so we have to recall some further definitions.

The lattice L' is a centering of the lattice L if $L' \supset L$. This centering is admissible iff $\min L' = \min L$. The index of the admissible centering is defined by the number $\mathrm{ind}(L'/L) = v(L)/v(L')$, where $v(L)$ is the volume of a basic parallelepiped in the lattice L. Let V_n be the maximum of the n-dimensional indices for all admissible centerings of all lattices L possessing n linearly independent minima. An important task in the geometry of numbers is to give estimations for the value of V_n. The first results in this field are due to A. Korkine–G. Zolotareff (see [4/a], [4/b]) and H. Minkowski [6]. Later a good estimation was given by Davenport and Watson [2], namely they proved that $V_n \leqq c_n^{n/2}$ where c_n denotes the Hermite constant defined as $\max\{(\min L)^2 \mid L \subset E^n$ is a lattice of determinant $1\}$. There holds $c_n \leqq \leqq 2^{-0.198\ldots}\frac{n}{\pi e}(1+o(1))$ cf. the upper estimate of the packing density of balls in E^n in [3]. In the lower dimensional cases also the exact values of V_n are known due to the results of S. S. Ryškov [7] and N. V. Zaharova-Novikova [8] who discussed the cases $n \leqq 7$ and $n = 8$, respectively.

2. The theorem

THEOREM. *For an arbitrary dimension n $L_n \leqq V_n$ holds, i.e. in every n-lattice possessing n linearly independent minima there exists a basis such that the absolute values of the coordinates belonging to any minimum vector are not greater than V_n.*

PROOF. Let $\pm\mathbf{m}_1, \ldots, \pm\mathbf{m}_\sigma$ be all different minima of the lattice. It is well known that $\sigma \leqq 2^n - 1$ is valid (see [9]). Suppose that the positive volume of the parallelepiped $\pi(\mathbf{m}_1, \ldots, \mathbf{m}_n)$ is not less than the volume of any other n-dimensional parallelepiped spanned by the minimum vectors of L. Then

$$m_l = \sum_{j=1}^{n} \alpha_{lj}\mathbf{m}_j, \qquad \text{where } 1 \leqq l \leqq \sigma \tag{3}$$

and for the rational numbers α_{lj} the following hold:

$$|\alpha_{lj}| \leqq 1, \qquad j = 1, \ldots, n \text{ and } 1 \leqq l \leqq \sigma. \tag{4}$$

(Assuming the contrary we get such a minimum parallelepiped which has a volume greater than that of the parallelepiped $\pi(\mathbf{m}_1, \ldots, \mathbf{m}_n)$.) Consider now such a basis $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ of L in which $\mathbf{m}_1, \ldots, \mathbf{m}_n$ can be expressed as $\mathbf{m}_j = \sum_{i=1}^{n} v_{ji}\mathbf{a}_i$, where the coordinates v_{ji} satisfy the following inequalities:

$$\begin{aligned} &\text{(i)} \quad v_{jj} > 0, \quad j = 1, \ldots, n \qquad v_{ji} = 0 \quad \text{for } 1 \leqq j < i \leqq n \\ &\text{(ii)} \quad 0 \leqq v_{ji} < v_{jj} \quad \text{for } 1 \leqq i < j \leqq n. \end{aligned} \tag{5}$$

The existence of such a basis A is assured in every n-lattice (see [1]). With respect to this basis A the vectors $\mathbf{m}_1, \ldots, \mathbf{m}_\sigma$ can be expressed in the following form:

$$\mathbf{m}_l = \sum_{j=1}^{n} \alpha_{lj}\mathbf{m}_j = \sum_{i=1}^{n}\Big(\sum_{j=i}^{n} \alpha_{lj}v_{ji}\Big)\mathbf{a}_i, \qquad l = 1, \ldots, \sigma. \tag{6}$$

So the absolute values of the coordinates are:

$$p_{li} = \Big|\sum_{j=i}^{n} \alpha_{lj}v_{ji}\Big|. \tag{7}$$

If for any j $(j > i)$ v_{jj} is equal to one then on the base of (5)(ii), we get $v_{ji} = 0$, so for this reason we have:

$$p_{li} \leqq \sum_{\substack{j=i+1 \\ v_{jj}>1}}^{n} |\alpha_{lj}|v_{ji} + |\alpha_{li}|v_{ii} \leqq \sum_{\substack{j=i+1 \\ v_{jj}>1}}^{n} v_{jj} + v_{ii} \leqq \prod_{j=i}^{n} v_{jj} + 1. \tag{8}$$

In the last step we used that for a finite set of integers each greater than 1 their sum is at most their product, where equality holds only if the set consists of one element. If $v_{ii} = 1$ and there are at least two v_{jj}'s with $i+1 \leqq j \leqq n$, $v_{jj} > 1$ then the sum of these v_{jj}'s is strictly less than their product, so in fact

$$\sum_{\substack{j=i+1 \\ v_{jj}>1}}^{n} v_{jj} + v_{ii} \leqq \prod_{j=i}^{n} v_{jj}.$$

The same holds if there is no j such that $i+1 \leqq j \leqq n$, $v_{jj} > 1$. If there is just one such v_{jj}, then in (8) we can use for this j the sharper estimate $|\alpha_{lj}|v_{ji} \leqq v_{ji} < v_{jj}$, hence $|\alpha_{lj}|v_{ji} \leqq v_{jj} - 1$, which gives

$$p_{li} \leqq \prod_{j=i}^{n} v_{jj}. \tag{9}$$

But $\prod_{j=i}^{n} v_{jj}$ is the index of an admissible centering, which completes the proof of the Theorem.

3. The case of the lower dimensions

In this paragraph we prove that the Theorem is not "sharp". It is well known that $V_1 = V_2 = V_3 = 1$ and $V_4 = V_5 = 2$ (see [7]). We verify two statements:

STATEMENT 1. $L_4 = 1$.

PROOF. We will distinguish two cases.

1. If in the lattice L every linearly independent minimum system is a basis then the absolute values of the examined coordinates are less than two. (This is clear from the proof of the Theorem.)

2. If the lattice L has a minimum system with index 2, then the minima of the lattice can be expressed with respect to the basis constructed above (in the proof of the Theorem), in the following way (where $\mathbf{m}_1$, $\mathbf{m}_2$, $\mathbf{m}_3$, $\mathbf{m}_4$ are the edge vectors of the basic cube; at this time the lattice is the well-known space-centred cubic lattice, see e.g. in [7])

$$\mathbf{m}_1 = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad \mathbf{m}_2 = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad \mathbf{m}_3 = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad \mathbf{m}_4 = \begin{bmatrix}1\\1\\1\\2\end{bmatrix} \quad \mathbf{m}_5 = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \quad \mathbf{m}_6 = \begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

(10)

$$\mathbf{m}_7 = \begin{bmatrix}0\\1\\0\\1\end{bmatrix} \quad \mathbf{m}_8 = \begin{bmatrix}0\\0\\1\\1\end{bmatrix} \quad \mathbf{m}_9 = \begin{bmatrix}0\\1\\1\\1\end{bmatrix} \quad \mathbf{m}_{10} = \begin{bmatrix}1\\0\\1\\1\end{bmatrix} \quad \mathbf{m}_{11} = \begin{bmatrix}1\\1\\0\\1\end{bmatrix} \quad \mathbf{m}_{12} = \begin{bmatrix}1\\1\\1\\1\end{bmatrix},$$

and so the characteristic matrix (see [7]) of the minima can be written in the following form:

$$\begin{bmatrix}1&0&0&1&0&1&0&0&0&1&1&1\\0&1&0&1&0&0&1&0&1&0&1&1\\0&0&1&1&0&0&0&1&1&1&0&1\\0&0&0&2&1&1&1&1&1&1&1&1\end{bmatrix}. \tag{11}$$

But a row-subtraction operation on this matrix is equivalent to a basis-change of the lattice so we get that with respect to a suitable basis the minima of L can be written in the following way:

$$\begin{bmatrix}1&0&0&1&0&1&0&0&0&1&1&1\\0&1&0&1&0&0&1&0&1&0&1&1\\0&0&1&1&0&0&0&1&1&1&0&1\\-1&0&0&1&1&0&1&1&1&0&0&0\end{bmatrix}, \tag{12}$$

so L_4 is equal to one. □

STATEMENT 2. *L_5 is equal to one, too.*

PROOF. Suppose $v(L) = 1$. If the volumes of the minimum parallelepipeds are 1 or -1, then the elements of the characteristic matrix are also 0, 1 or -1. So we can assume that $v(\pi(\mathbf{m}_1, \ldots, \mathbf{m}_5)) = 2$. Then the elements of the characteristic matrix have absolute value at most 2. We distinguish two cases:

1. If the lattice does not have a four-dimensional space-centred cubic sublattice (in this we include that the edge vectors of the cube are minima of the lattice and this sublattice is the intersection of the lattice and a 4-plane), then the setup of the characteristic matrix can be started in the following way:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & \dots \\ 0 & 1 & 0 & 0 & 1 & \dots \\ 0 & 0 & 1 & 0 & 1 & \dots \\ 0 & 0 & 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 2 & \dots \end{bmatrix}. \tag{13}$$

Let $\mathbf{m}_l$ be an arbitrary minimum vector, where $5 < l \leqq \sigma$. Then the coordinates of this minima can be seen from (6), we have:

$$m_{il} = \sum_{j=i}^{n} \alpha_{lj} v_{ji} = \sum_{j=i}^{5} \alpha_{lj} v_{ji}, \tag{14}$$

where $v_{11} = \dots = v_{44} = v_{5i} = 1$ if $1 \leqq i < 5$, $v_{55} = 2$ and the other v_{ji} are equal to zero. So we get the following simple equalities:

$$m_{il} = \alpha_{li} + \alpha_{l5}, \qquad m_{5l} = 2\alpha_{l5}. \tag{15}$$

Clearly we may assume $m_{5l} \geqq 0$. First assume that $m_{5l} = 2$, hence $\alpha_{l5} = 1$. At this time we have the possibility for the choice of the values of the other coordinates 0, 1, 2, respectively. It is clear that we do not have a minimal vector in the lattice mod (2) equivalent to one of the vectors $\mathbf{m}_1, \dots, \mathbf{m}_5$. So the number of the 1's among the first four coordinates is two or three. Now we examine two cases:

(a) If there is a zero among the first 4 coordinates;
then there is a sublattice L_1 of L which is a space-centred cubic 4-sublattice in L (e.g. if $m_{1l} = 0$, then the vectors $\mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4, \mathbf{m}_l$ form a minimum system with index 2, and the sublattice L_1 is spanned by the vectors $\mathbf{a}_2, \dots, \mathbf{a}_5$).

(b) If there are two or three 1's among the first 4 coordinates and the others are equal to 2;
then also there is a space-centred cubic 4-sublattice of the lattice L, for example if $\mathbf{m}_l = [2, 1, 1, 1, 2]^T$ or $\mathbf{m}_l = [2, 2, 1, 1, 2]^T$ then the sublattice spanned by the vectors $\mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \mathbf{a}_1 + \mathbf{a}_5$ contains the minimum-parallelepiped $\pi(\mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4, \mathbf{m}_l)$ with volume two. So this sublattice is a space-centred cubic lattice, too.

From this reason if $m_{5l} = 2$ then $\mathbf{m}_l = \mathbf{m}_5$.

Secondly we assume that $m_{5l} = 1$. At this time $\alpha_{l5} = \frac{1}{2}$ and the coordinates m_{il}, $1 \leqq i < 5$, are equal to zero or one.

Lastly if $m_{5l} = 0$ it may be seen that the other coordinates of this minimum are -1, 0 or 1 (e.g. if $m_{1l} = 2$, then the vectors $\mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4, \mathbf{m}_l$ form a

minimum system of index 2 in the sublattice spanned by the vectors $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$, $\mathbf{e}_4$).

So in the case of 1 the characteristic matrix can be written in the following form:

$$(16) \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} \\ A \\ \\ \end{bmatrix} \begin{bmatrix} \\ A' \\ \\ \end{bmatrix},$$

where A is a $(0, \pm 1)$ matrix in which the elements of the last row are equal to zero, and the matrix A' is a $(0, 1)$ one. It can easily be seen by the subtraction of the first row from the last one that this matrix is equivalent to a $(0, \pm 1)$ one.

2. Consider now the case that the lattice L has a space-centred cubic 4-sublattice. Then the characteristic matrix is the following:

$$(17) \qquad \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} & & \\ & A & \\ & & \\ & B & \\ 1 & \cdots & 1 \end{bmatrix},$$

where A has three rows and B is a one-row vector. If an element of B is equal to 2 resp. -2, then B does not have any negative resp. positive coordinate. In fact, otherwise the columns of the characteristic matrix containing the two mentioned elements of B together with $\mathbf{m}_1$, $\mathbf{m}_2$, $\mathbf{m}_3$ form a submatrix with determinant of absolute value greater than 2. So, if B is not a $(0, \pm 1)$ vector, we may assume that the coordinates of B are either positive or zero resp. either negative or zero. Subtracting the last row from, resp. adding the last row to the row containing B we get that B becomes a $(0, \pm 1)$ vector. Therefore we may assume B is a $(0, \pm 1)$ vector. Assume that A has such an element (for example in the first row) whose absolute value is greater than one. But this element must be a coordinate of a minimum vector $\mathbf{m} = [x_1\, x_2\, x_3\, x_4\, 1]^T$ so the parallelepiped $\pi = \pi[\mathbf{m}, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4, \mathbf{m}_5]$ is a minimum one. But after doing the suitable column-subtractions we have

$$(18) \qquad v(\pi) = |\det \begin{bmatrix} x_1 & 0 & 0 & 1 & 0 \\ x_2 & 1 & 0 & 1 & 0 \\ x_3 & 0 & 1 & 1 & 0 \\ x_4 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}| = |2x_1 - x_4| > 2,$$

where x_4 is 0 or ± 1 and this is a contradiction. For this reason A is a $(0, \pm 1)$ matrix. Thus the only element of the characteristic matrix, which is not 0

or ± 1 is $m_{44} = 2$. Subtract now the first row from the fourth row. Then we get a $(0, \pm 1)$ matrix, unless some minimum vector $\mathbf{m} = [x_1\, x_2\, x_3\, x_4\, 1]^T$ has $x_4 = -x_1 = \pm 1$. However, this case leads to a contradiction by (18). So we have verified this case and the statement, too. □

REMARK. The statement of the theorem is interesting in case of the well-known reduced bases (Minkowski, Hermite, Korkine–Zolotareff) only weaker statements are expected.

REFERENCES

[1] CASSELS, J. W. S., *An introduction to the geometry of numbers*, Die Grundlehren der math. Wissenschaften, Bd. 99, Springer-Verlag, Berlin, 1959. *MR* **28** #1175

[2] DAVENPORT, H. and WATSON, G. L., The minimal points of a positive definite quadratic form, *Mathematika* **1** (1954), 14–17. *MR* **16** – 18

[3] FEJES TÓTH, G., New results in the theory of packing and covering, *Convexity and its applications*, Birkhäuser, Basel–Boston, 1983, 318–359. *MR* **85i**: 52007

[4/A] KORKINE, A. and ZOLOTAREFF, G., Sur les formes quadratiques, *Math. Ann.* **6** (1873), 366–390. *Jb. Fortschritte Math.* **5**, 109

[4/B] KORKINE, A. and ZOLOTAREFF, G., Sur les formes quadratiques positives, *Math. Ann.* **11** (1877), 242–292. *Jb. Fortschritte Math.* **9**, 139

[5] GRUBER, P. M. and LEKKERKERKER, C. G., *Geometry of numbers*, 2nd ed., North-Holland Mathematical Library, Vol. 37, North-Holland, Amsterdam, 1987. *Zbl* **611** #10017. See also *Zbl* **198**, 380

[6] MINKOWSKI, H., Diskontinuitätsbereich für arithmetische Äquivalenz, *J. Reine Angew. Math.* **129** (1905), 220–274. *Jb. Fortschritte Math.* **37**, 251

[7] RYŠKOV, S. S., On the problem of determining perfect quadratic forms of several variables, Number theory, mathematical analysis and their applications, *Trudy Mat. Inst. Steklov* **142** (1976), 215–239, 270–271 (in Russian). *MR* **58** #27807

[8] ZAKHAROVA, N. V., Centerings of eight-dimensional lattices that preserve a frame of successive minima, Geometry of positive quadratic forms, *Trudy Mat. Inst. Steklov* **152** (1980), 97–123, 237 (in Russian). *MR* **82k**:10033 Correction: Novikova, N. V., Three admissible centerings of eight-dimensional lattices, Deposited in VINITI, No. 4842-81 Dep., 1981, I. 8 (in Russian).

[9] VORONOÏ, G., Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier Mémoire: Sur quelques propriétés des formes quadratiques positives parfaites, *J. Reine Angew. Math.* **133** (1908), 97–156. *Jb. Fortschritte Math.* **38**, 261

(Received August 15, 1990)

BUDAPESTI MŰSZAKI EGYETEM
GÉPÉSZMÉRNÖKI KAR
GEOMETRIA TANSZÉK
EGRI JÓZSEF U. 1. H. ÉP. II. 22
H–1521 BUDAPEST
HUNGARY