

# Defect of an octahedron in a rational lattice

Mikhail Fadin \*

## Abstract

Consider an arbitrary  $n$ -dimensional lattice  $\Lambda$  such that  $\mathbb{Z}^n \subset \Lambda \subset \mathbb{Q}^n$ . Such lattices are called *rational* and can always be obtained by adding  $m \leq n$  rational vectors to  $\mathbb{Z}^n$ . *Defect*  $d(\mathcal{E}, \Lambda)$  of the standard basis  $\mathcal{E}$  of  $\mathbb{Z}^n$  ( $n$  unit vectors going in the directions of the coordinate axes) is defined as the smallest integer  $d$  such that certain  $(n - d)$  vectors from  $\mathcal{E}$  together with some  $d$  vectors from the lattice  $\Lambda$  form a basis of  $\Lambda$ .

Let  $\|\dots\|$  be  $L^1$ -norm on  $\mathbb{Q}^n$ . Suppose that for each non-integer  $x \in \Lambda$  inequality  $\|x\| > 1$  holds. Then the unit octahedron  $O^n = \{x \in \mathbb{R}^n : \|x\| \leq 1\}$  is called admissible with respect to  $\Lambda$  and  $d(\mathcal{E}, \Lambda)$  is also called defect of the octahedron  $O^n$  with respect to  $\mathcal{E}$  and is denoted as  $d(O_{\mathcal{E}}^n, \Lambda)$ .

Let  $d_n^m = \max_{\Lambda \in \mathcal{A}_m} d(O_{\mathcal{E}}^n, \Lambda)$ , where  $\mathcal{A}_m$  is the set of all *rational* lattices that can be obtained by adding  $m$  rational vectors to  $\mathbb{Z}^n$ :  $\Lambda = \langle \mathbb{Z}^n, a_1, \dots, a_m \rangle_{\mathbb{Z}}$ ,  $a_1, \dots, a_m \in \mathbb{Q}^n$ . In this article we show that there exists an absolute positive constant  $C$  such that for any  $m < n$

$$d_n^m \leq C \frac{n \ln(m+1)}{\ln \frac{n}{m}} \left( \ln \ln \left( \frac{n}{m} \right)^m \right)^2$$

This bound was also claimed in [1], [2], however the proof was incorrect. In this article along with giving correct proof we highlight substantial inaccuracies in those articles.

**Keywords:** Lattice, Defect, Octahedron, System of common representatives

## 1 Definitions, notation and formulation of result

Let  $\Gamma \subset \mathbb{R}^n$  be an arbitrary lattice in an  $n$ -dimensional Euclidean space, and let  $O = (0, 0, \dots, 0) \in \Gamma$  be the point of origin. If  $\Gamma$  is a sublattice of a lattice  $\Lambda$ , then  $\Lambda$  is called a *centering* of the lattice  $\Gamma$ . We are going to investigate the difference between the basis of a lattice and the basis of its centering.

Let us consider a basis  $e_1, \dots, e_n$  of  $\Gamma$ . The set of vectors  $\mathcal{E} = \{e_1, \dots, e_n\}$  will be called a *frame*. The *defect of the frame  $\mathcal{E}$  with respect to the lattice  $\Lambda$*  is defined as the smallest integer  $d$  such that certain  $(n - d)$  vectors from  $\mathcal{E}$  together with some  $d$  vectors from the lattice  $\Lambda$  form a basis of  $\Lambda$ . It is denoted as  $d(\mathcal{E}, \Lambda) = d$ .

An *octahedron* corresponding to the frame  $\mathcal{E}$  is defined as the set

$$O_{\mathcal{E}}^n = \{x \in \mathbb{R}^n : x = \lambda_1 e_1 + \dots + \lambda_n e_n; |\lambda_1| + \dots + |\lambda_n| \leq 1\}.$$

The octahedron  $O_{\mathcal{E}}^n$  is called *admissible* with respect to the lattice  $\Lambda$  if its interior contains no points of the lattice  $\Lambda$ , except for  $O$  and  $\pm e_i$ :

$$O_{\mathcal{E}}^n \cap \Lambda = \{O, e_1, -e_1, \dots, e_n, -e_n\}.$$

---

\*michailfadin@gmail.com; Faculty of Mathematics, National Research University Higher School of Economics, Moscow, 119048, Russia

If the octahedron  $O_{\mathcal{E}}^n$  corresponding to the frame  $\mathcal{E}$  is admissible with respect to the centering  $\Lambda$ , then the quantity  $d(\mathcal{E}, \Lambda)$  is denoted as  $d(O_{\mathcal{E}}^n, \Lambda)$  and is called the *defect of the admissible octahedron  $O_{\mathcal{E}}^n$  in the lattice  $\Lambda$* .

Note that without loss of generality we can take  $\Gamma$  to be  $\mathbb{Z}^n$  and the frame  $\mathcal{E}$  to represent the standard basis ( $n$  unit vectors going in the directions of the coordinate axes).

In [6] N.G. Moshchevitin introduced the quantity

$$d_n^* = \max_{\Lambda_a} d(O_{\mathcal{E}}^n, \Lambda_a),$$

where  $\Lambda_a$  runs through lattices that can be obtained by adding one rational vector to  $\mathbb{Z}^n$ , and proved that there exists a positive constant  $C$  such that

$$d_n^* \leq C \frac{n}{\ln n} (\ln \ln n)^2.$$

Then, in the article [7] (see also [8], [10], [11]) A.M Raigorodskii proved that there exists a positive constant  $C$  such that

$$C \frac{n}{\ln n} (\ln \ln n)^2 \leq d_n^*$$

Finally, in the article [1] the quantity  $d_n^m$  – natural generalisation of  $d_n^*$ , was introduced:

$$d_n^m = \max_{\Lambda \in \mathcal{A}_m} d(O_{\mathcal{E}}^n, \Lambda),$$

where  $\mathcal{A}_m$  is the set of all centerings of the integer lattice  $\mathbb{Z}^n$  that can be obtained by adding  $m$  rational vectors:

$$\Lambda = \langle \mathbb{Z}^n, a_1, \dots, a_m \rangle_{\mathbb{Z}}, \quad a_1, \dots, a_m \in \mathbb{Q}^n.$$

In [1], [2] the following bound was claimed.

**Theorem 1.** *There exists an absolute positive constant  $C$  such that*

$$d_n^m \leq C \frac{n \ln(m+1)}{\ln \frac{n}{m}} \left( \ln \ln \left( \frac{n}{m} \right)^m \right)^2$$

for any  $m < n$ .

However, the proof contained several substantial inaccuracies. Eliminating those inaccuracies turned out to be quite challenging. In this article we are going to show the correct proof of this bound and mark substantial inaccuracies in [1], [2]. In order to do it we define the following quantity:

$$\mathcal{D}_n^m = \max_{\Lambda \in \mathcal{A}_m^*} d(O_{\mathcal{E}}^n, \Lambda),$$

where  $\mathcal{A}_m^*$  is the set of all centerings of the integer lattice  $\mathbb{Z}^n$  that can be obtained by adding  $m$  rational vectors whose coordinates' denominators are square-free:  $\Lambda = \langle \mathbb{Z}^n, a_1, \dots, a_m \rangle_{\mathbb{Z}}; a_1, \dots, a_m \in \mathbb{Q}^n$ , there exists a square-free positive integer  $q$  such that  $q \cdot a_1, \dots, q \cdot a_m \in \mathbb{Z}^n$ .

**Theorem 2.** *There exists an absolute positive constant  $C$  such that*

$$\mathcal{D}_n^m \leq C \frac{n \ln(m+1)}{\ln \frac{n}{m}} \left( \ln \ln \left( \frac{n}{m} \right)^m \right)^2$$

for any  $m < n$ .

**Theorem 3.**  $\mathcal{D}_n^m = d_n^m$ .

Note that Theorem 1 is a direct implication of Theorems 2 and 3.

## 2 Proof of Theorem 3

Let  $a_1, \dots, a_m \in \mathbb{Q}^n$  be given vectors. Suppose  $O_{\mathcal{E}}^n$  is admissible with respect to  $\Lambda = \langle \mathbb{Z}^n, a_1, \dots, a_m \rangle_{\mathbb{Z}}$ . Define  $A^*$  as the matrix formed by writing vectors  $a_1, \dots, a_m$  as its rows.

**Lemma 1.** *Let  $\Lambda'$  be a sublattice of  $\Lambda$  such that  $\mathbb{Z}^n \subset \Lambda'$ . Then there exist  $\lambda_1, \dots, \lambda_m \in \mathbb{Q}^n$  such that*

$$\Lambda' = \langle \mathbb{Z}^n, \lambda_1, \dots, \lambda_m \rangle_{\mathbb{Z}}.$$

*Proof.* Let  $b_1, \dots, b_n$  be a basis of  $\Lambda'$ . Obviously,  $\Lambda' = \langle \mathbb{Z}^n, b_1, \dots, b_n \rangle_{\mathbb{Z}}$ . For each  $i$  there exist  $b_i^* \in \mathbb{Z}^n$  such that  $b_i' = b_i + b_i^* \in \langle a_1, \dots, a_m \rangle_{\mathbb{Z}}$ . We have  $\Lambda' = \langle \mathbb{Z}^n, b_1', \dots, b_n' \rangle_{\mathbb{Z}} = \langle \mathbb{Z}^n, c_1 A^*, \dots, c_n A^* \rangle_{\mathbb{Z}}$ , where for each  $i$ ,  $c_i$  is a row of  $m$  integers.

Let  $C = \langle c_1, \dots, c_n \rangle_{\mathbb{Z}} \subset \mathbb{Z}^m$ .  $C$  is a submodule of free module  $\mathbb{Z}^m$  of rank  $m$  over principle ring  $\mathbb{Z}$ . Thus  $C$  is a free module over  $\mathbb{Z}$  of rank  $\leq m$ , which means that there exist  $c'_1, \dots, c'_m$  such that  $C = \langle c'_1, \dots, c'_m \rangle_{\mathbb{Z}}$ . Clearly,  $\Lambda' = \langle \mathbb{Z}^n, c_1 A^*, \dots, c_n A^* \rangle_{\mathbb{Z}} = \langle \mathbb{Z}^n, c'_1 A^*, \dots, c'_m A^* \rangle_{\mathbb{Z}}$ . Thus,  $\lambda_i = c'_i A^*$  are desired vectors. □

**Lemma 2.** *There exist a lattice  $\Lambda'$  such that*

- 1)  $\mathbb{Z}^n \subset \Lambda' \subset \Lambda$ ,
- 2) denominators of coordinates of all vectors of  $\Lambda'$  are square-free,
- 3)  $d(\mathcal{E}, \Lambda') = d(\mathcal{E}, \Lambda)$ .

*Proof.* Let  $d(\mathcal{E}, \Lambda) = n - k + 1$ . Then for each  $I = \{i_1, \dots, i_k\} \subset \{1, \dots, n\}$  coordinate vectors  $e_{i_1}, \dots, e_{i_k}$  can not be completed to a basis of  $\Lambda$ , which means that there exists  $x = x_I \in \Lambda$  such that

$$(*) \ x \in \langle e_{i_1}, \dots, e_{i_k} \rangle_{\mathbb{R}}, \text{ but } x \notin \langle e_{i_1}, \dots, e_{i_k} \rangle_{\mathbb{Z}}.$$

Let  $q_I$  be the least common multiple of the denominators of the coordinates of  $x_I$  and let  $p_I$  be the smallest prime divisor of  $q_I$ ,  $u_I = \frac{q_I}{p_I}$ . Then  $u_I x_I$  also satisfies (\*) and its coordinates' denominators are square-free.

Let  $\Lambda' = \langle \mathbb{Z}^n, \{u_{I_j} x_{I_j}\} \rangle_{\mathbb{Z}}$ , where  $I_j$  runs through all  $k$ -element subsets of  $\{1, \dots, n\}$ . Obviously,  $\Lambda'$  satisfies 1) and 2). Since for each  $I = \{i_1, \dots, i_k\} \subset \{1, \dots, n\}$  there exists  $y_I = u_I x_I \in \Lambda'$  which satisfies (\*),  $e_{i_1}, \dots, e_{i_k}$  can not be completed to a basis of  $\Lambda'$ . Thus  $d(\mathcal{E}, \Lambda') \geq n - k + 1 = d(\mathcal{E}, \Lambda)$ . But since  $\Lambda' \subset \Lambda$ , we have  $d(\mathcal{E}, \Lambda') \leq d(\mathcal{E}, \Lambda)$ . Therefore,  $d(\mathcal{E}, \Lambda') = d(\mathcal{E}, \Lambda)$  as desired. □

Theorem 3 directly follows from Lemma 1 and Lemma 2.

## 3 Auxiliary combinatorial constructions

### 3.1 A system of families of sets $\mathfrak{M}$

Let  $a_1, \dots, a_m \in \mathbb{Q}^n$  be given vectors. Let us reduce their coordinates to a least possible common denominator  $q$ . Due to Theorem 3 we may assume that  $q$  is square-free,  $m < n$  (since it suffices to prove Theorem 2). Let  $q = p_1 \cdot p_2 \cdot \dots \cdot p_s$  ( $p_1 \geq p_2 \geq \dots \geq p_s$ ) be the prime factorization of  $q$ . Define  $A$  as the

matrix formed by writing vectors  $q \cdot a_1, \dots, q \cdot a_m$  as its rows. For each  $j$ , the rank of the matrix  $A$  over the field  $\mathbb{Z}_{p_j}$  will be denoted as  $rank_j$ .

Let  $\mathcal{C}_n = \{1, \dots, n\}$  be the set of all coordinate indexes. For each  $j \in \{1, \dots, s\}$  let  $M_j^i$  denote  $rank_j$ -element subsets of  $\mathcal{C}_n$  such that for an arbitrary  $i$  the columns of the matrix  $A$  with numbers from  $M_j^i$  are linearly independent over the field  $\mathbb{Z}_{p_j}$ . For a fixed  $j$ , the family of sets  $M_j^i$  will be denoted as  $\mathcal{M}_j$ . Finally, the system of families of sets  $\mathfrak{M}$  is defined as  $\mathfrak{M} = \{\mathcal{M}_1, \dots, \mathcal{M}_s\}$ .

**Remark.** In [1], [2] there was no reduction to the square-free case (Theorem 3). Instead, matrix  $A$  was considered over rings  $\mathbb{Z}_{p_j^k}$  and most statements were formulated in terms of rings (with the usage of an undefined rank over ring). However, in those terms Theorem 4 as well as auxiliary lemmas afterwards and final constructions in the proof turned out to be wrong. Since even in the square-free case in [1] and [2] there were substantial inaccuracies, in most following remarks we are only going to describe inaccuracies in that case even though all statements in [1], [2] were formulated in the general case.

### 3.2 The relation between the defect and the system $\mathfrak{M}$

Let  $M$  be a subset of  $\mathcal{C}_n$  such that for any  $j \in \{1, \dots, s\}$  there exists  $i \in \{1, \dots, |\mathcal{M}_j|\}$  for which  $M_j^i \subseteq M$ .

**Theorem 4.** Let  $\Lambda = \langle \mathbb{Z}^n, a_1, \dots, a_m \rangle_{\mathbb{Z}}$ . Then the following inequality is satisfied:  $d(\mathcal{E}, \Lambda) \leq |M|$ .

*Proof.* Any point of the lattice  $\Lambda$  can be represented as  $\frac{1}{q} \cdot kA + b$ , where  $k = (k_1, \dots, k_m)$  is a row of  $m$  integer numbers,  $A$  is the matrix defined in the previous section and  $b$  is a vector in  $\mathbb{Z}^n$ .

Consider a subspace of  $\mathbb{R}^n$  spanned by the coordinate axes with indexes that do not belong to  $M$ . Assume that a point  $x = \frac{1}{q} \cdot kA + b$  of the lattice  $\Lambda$  lies in this subspace. Then its coordinates with numbers from  $M$  are equal to zero. Let us fix a number  $j \in \{1, \dots, s\}$ . By definition of  $M$ , there exists a set  $M_j^i = \{v_1, \dots, v_{rank_j}\}$  which is fully embedded in  $M$ . Thus the coordinates of  $x$  numbered as  $v_1, \dots, v_{rank_j}$  are also equal to zero. In other words, coordinates of the vector  $kA$  numbered as  $v_1, \dots, v_{rank_j}$  are divisible by  $q$ , and thus also by  $p_j$ . However, columns of the matrix  $A$  numbered as  $v_1, \dots, v_{rank_j}$  form a maximal linearly independent set of vectors of the matrix  $A$  over the field  $\mathbb{Z}_{p_j}$  (by the definition of the set  $M_j^i$ ). Then all other columns of  $A$  can be expressed over the field  $\mathbb{Z}_{p_j}$  as linear combinations of these  $rank_j$  columns. Therefore, all coordinates of the vector  $kA$  are divisible by  $p_j$ . Since this applies for any  $j \in \{1, \dots, s\}$ , all coordinates of the vector  $kA$  are therefore divisible by  $q$ . Thus  $x \in \mathbb{Z}^n$ , meaning (see [3]) that vectors of the frame  $\mathcal{E}$  with numbers from  $\mathcal{C}_n \setminus M$  can be completed to form a basis of the lattice  $\Lambda$ , and thus we have  $d(\mathcal{E}, \Lambda) \leq |M|$ . □

**Remark.** In [1], [2]  $M$  was defined as a set which for every  $j$  contains some maximum set of indexes of columns which are linear independent over the ring  $\mathbb{Z}_{p_j^k}$ . The same inequality was claimed. One can easily construct a contrexample to this version of the theorem by considering  $n = 2$ ,  $a_1 = (\frac{1}{p^2}, \frac{1}{p^2})$ ,  $a_2 = (\frac{1}{p^2}, \frac{1}{p^2} + \frac{1}{p})$ .

Theorem 4 holds for any  $M$ , allowing us to write  $d(\mathcal{E}, \Lambda) \leq \theta(\mathfrak{M})$ , where  $\theta(\mathfrak{M})$  is the cardinality of the smallest set  $M$ . In the next subsection we are going to recall a problem similar to approximation of  $\theta$ .

### 3.3 A covering problem

Let  $\mathcal{L} = \{L_1, \dots, L_t\}$  be an arbitrary family of subsets of the set  $\mathcal{C}_n$ . Its *system of common representatives (SCR)* is defined as a set  $S \subseteq \mathcal{C}_n$  that includes at least one element from each  $L_i$ . The minimum size of an SCR for  $\mathcal{L}$  is denoted as  $\tau(\mathcal{L})$ . Clearly, the setting in the previous subsection is more general:

instead of a family of sets we consider the system of families of sets  $\mathfrak{M}$ . If we assume that the size of all sets in every family from  $\mathfrak{M}$  equals one, then the set  $M$  defined in the previous subsection is, as a matter of fact, an SCR. Theorem 5 below provides an upper bound on the size of a minimal SCR which will later help us to obtain a bound for  $\theta(\mathfrak{M})$ . A proof and a discussion of this theorem can be found in [5], [9], [12].

**Theorem 5.** *Assume that  $|L_i| \geq k$  for each  $i \in \{1, \dots, t\}$ . Then there exists a constant  $c$  such that*

$$\tau(\mathcal{L}) \leq c \frac{n}{k} \cdot \max \left\{ 1, \ln \frac{tk}{n} \right\}.$$

## 4 Proof of Theorem 2

### 4.1 Outline of the proof

Consider vectors  $a_1, \dots, a_m \in \mathbb{Q}^n$ . Let us construct a system of families of sets  $\mathfrak{M} = \{\mathcal{M}_1, \dots, \mathcal{M}_s\}$  using the method from Subsection 3.1. We would like to prove the inequality

$$\theta(\mathfrak{M}) \leq C \frac{n \ln(m+1)}{\ln \frac{n}{m}} \left( \ln \ln \left( \frac{n}{m} \right)^m \right)^2$$

by applying Theorem 5. Subsection 4.3 is going to contain this proof, and the auxiliary lemmas used in the proof are presented in the following subsection.

### 4.2 Auxiliary Lemmas

**Lemma 3.**  $\det \Lambda = p_1^{-\text{rank}_1} \cdot p_2^{-\text{rank}_2} \cdot \dots \cdot p_s^{-\text{rank}_s}$

*Proof.* Denote  $\Lambda_k = \langle \mathbb{Z}^n, a_1, \dots, a_k \rangle_{\mathbb{Z}}$  for  $0 \leq k \leq m$ . We have  $\Lambda_0 \subset \Lambda_1 \dots \subset \Lambda_m$  and  $\Lambda_k / \Lambda_{k-1} = \langle a_k \rangle$ . Define a number  $q_k$  in the following way. Let  $q \cdot a_k$  not lie in  $\langle q \cdot a_1, \dots, q \cdot a_{k-1} \rangle_{\mathbb{Z}_{p_j}}$  for  $p_j | q_k$  and lie for all other  $p_j$ .

Let  $r$  be integer such that  $0 < r < q_k$ . Suppose that  $r \cdot a_k \in \Lambda_{k-1}$ . There exists  $i$  such that  $p_i | q_k$  but  $(p_i, r) = 1$ . By assumption,  $r \cdot a_k = b_1 \cdot a_1 + \dots + b_{k-1} \cdot a_{k-1}$ , where  $b_1, \dots, b_{k-1}$  are integers. But that means that in  $\mathbb{Z}_{p_i}$  we have  $a_k = r^{-1} b_1 \cdot a_1 + \dots + r^{-1} b_{k-1} \cdot a_{k-1}$  which contradicts the definition of  $q_k$ .

By Chinese Remainder Theorem and definition of  $q_k$  there exist integers  $b_1, \dots, b_{k-1}$  such that each coordinate of  $q \cdot a_k - q b_1 \cdot a_1 - \dots - q b_{k-1} \cdot a_{k-1}$  is divisible by  $\frac{q}{q_k}$  i.e.  $q \cdot a_k - q b_1 \cdot a_1 - \dots - q b_{k-1} \cdot a_{k-1} \in \mathbb{Z}^n$ .

So,  $a_k, 2a_k, \dots, (q_k - 1)a_k \notin \Lambda_{k-1}$  while  $q_k a_k \in \Lambda_{k-1}$ . Thus index of  $\Lambda_{k-1}$  in  $\Lambda_k$  is  $q_k$ . Since  $q \cdot a_k$  cannot be expressed as a linear combination of  $q \cdot a_1, \dots, q \cdot a_{k-1}$  over  $\mathbb{Z}_{p_j}$  for  $p_j | q_k$  and can be expressed as a linear combination of  $q \cdot a_1, \dots, q \cdot a_{k-1}$  over  $\mathbb{Z}_{p_j}$  for all other  $p_j$ ,  $q_1 \cdot \dots \cdot q_m = p_1^{\text{rank}_1} \cdot p_2^{\text{rank}_2} \cdot \dots \cdot p_s^{\text{rank}_s}$ . Then we have  $1 = \det \Lambda_0 = q_1 \det \Lambda_1 = \dots = q_1 \cdot \dots \cdot q_m \cdot \det \Lambda_m = p_1^{\text{rank}_1} \cdot \dots \cdot p_s^{\text{rank}_s} \cdot \det \Lambda$  which concludes the proof. □

**Lemma 4.** *Let  $j \in \{1, \dots, s\}$ ,  $p_j \geq 5$  and let  $v_1, \dots, v_l$  be  $l$  integers,  $0 \leq l < \text{rank}_j$ ,  $1 \leq v_i \leq n$ , such that columns of the matrix  $A$  (see Subsection 3.1) numbered as  $v_1, \dots, v_l$  are independent over  $\mathbb{Z}_{p_j}$ . Let  $\tilde{M}_j$  be the set of indexes of columns which are linearly independent with columns numbered  $v_1, \dots, v_l$  over  $\mathbb{Z}_{p_j}$ . The following inequality holds:*

$$\left| \tilde{M}_j \right| \geq \frac{1}{2} \cdot \frac{\ln p_j^{\text{rank}_j - l}}{\ln \ln p_j^{\text{rank}_j - l}}.$$

**Remark.** In [1],[2] in the formulation of the lemma in the inequality there was  $m$  instead of  $rank_j$ . However, this version of the lemma obviously does not hold: for instance, with fixed  $p_j$  and limitlessly increasing  $m$ , the right-hand side is limitlessly increasing while the left-hand side can be constant. We introduced Lemma 3 in order to show a correct proof of the correct version of the lemma.

*Proof.* It suffices to prove the lemma in the case  $m = rank_j, q = p_j$ . Let  $\Lambda'$  be a lattice obtained by the intersection of  $\Lambda$  with subspace spanned by the coordinate axes numbered by elements of  $\tilde{M}_j$ . We define family of vectors  $a_k^i$  ( $i = 0, \dots, l; k = 1, \dots, m$ ) using the following algorithm.

- Put  $a_k^0 = a_k$ ,
- If for each  $k$  the  $v_i^{th}$  coordinate of  $a_k^{i-1}$  is integer then let  $a_k^i = a_k^{i-1}$ .
- Otherwise for some  $k$   $v_i^{th}$  coordinate of  $p_j \cdot a_k^{i-1}$  is not divisible by  $p_j$ . Thus for each  $r$  there exists integer  $c_r^i$  such that the  $v_i^{th}$  coordinate of  $a_r^{i-1} + c_r^i \cdot a_k^{i-1}$  is an integer. Let  $a_k^i = a_r^{i-1} + c_r^i \cdot a_k^{i-1}$ .

Obviously,  $rank_{\mathbb{Z}_{p_j}}(\{p_j \cdot a_k^i\}) \geq rank_{\mathbb{Z}_{p_j}}(\{p_j \cdot a_k^{i-1}\}) - 1$ . Thus  $rank_{\mathbb{Z}_{p_j}}(\{p_j \cdot a_k^l\}) \geq rank_j - l$ .

Consider vectors  $p_j \cdot a_k^l$ . By the construction, coordinates numbered by  $v_1, \dots, v_l$  of these vectors are equal to zero in  $\mathbb{Z}_{p_j}$ . By definition, all columns of matrix  $A$  with indexes from  $\tilde{M}_j$  can be expressed over  $\mathbb{Z}_{p_j}$  as linear combinations of columns numbered by  $v_1, \dots, v_l$ . Since vectors  $p_j \cdot a_k^l$  are linear combinations of  $p_j \cdot a_1, \dots, p_j \cdot a_m$  we obtain that coordinates numbered by elements of  $\tilde{M}_j$  of these vectors are equal to zero in  $\mathbb{Z}_{p_j}$ . That means that for every  $k$  there exists an integer vector  $t_k$  such that all coordinates numbered by elements of  $\tilde{M}_j$  of  $a_k^l + t_k$  are equal to zero. Note that  $rank_{\mathbb{Z}_{p_j}}(\{p_j \cdot (a_k^l + t_k)\}) = rank_{\mathbb{Z}_{p_j}}(\{p_j \cdot a_k^l\}) \geq rank_j - l$  and  $x_k = a_k^l + t_k \in \Lambda'$ .

Let  $n^* = |\tilde{M}_j|$  and let  $\mathbb{Z}^{n^*}$  be the subspace of  $\mathbb{Z}^n$  spanned by the coordinate axes with indexes from  $\tilde{M}_j$ . Applying Lemma 1 for lattice  $\Gamma = \langle \mathbb{Z}^{n^*}, x_1, \dots, x_m \rangle_{\mathbb{Z}}$  we obtain  $p^{l-rank_j} \geq \det \Gamma \geq \det \Lambda'$ . Since unit octahedron  $O_{\mathcal{E}}^{n^*}$  is admissible in  $\Lambda'$  we can apply Minkowski's Theorem (see [3]):

$$Vol(O_{\mathcal{E}}^{n^*}) = \frac{2^{|\tilde{M}_j|}}{|\tilde{M}_j|!} \leq 2^{|\tilde{M}_j|} \cdot \det \Lambda' \leq \frac{2^{|\tilde{M}_j|}}{p_j^{rank_j-l}} \implies |\tilde{M}_j|! \geq p_j^{rank_j-l} \implies |\tilde{M}_j| \geq \frac{1}{2} \cdot \frac{\ln p_j^{rank_j-l}}{\ln \ln p_j^{rank_j-l}}.$$

The final inequality follows from the condition  $p_j \geq 5$ . The lemma is proved. □

**Lemma 5.** *The following inequality holds:  $s \leq n$ .*

*Proof.* The octahedron  $O_{\mathcal{E}}^n$  is admissible with respect to the lattice  $\Lambda$ ,  $\det \Lambda \leq \frac{1}{q}$  (follows from Lemma 3). Thus, from Minkowski's Theorem, we have:

$$\frac{2^n}{n!} \leq \frac{2^n}{q} \implies q \leq n!,$$

and  $q = p_1 \dots p_s \geq s!$ , which proves the lemma. □

### 4.3 A bound for $\theta(\mathfrak{M})$

Consider the system of families of sets  $\mathfrak{M}_0 = \{\mathcal{M}_1, \dots, \mathcal{M}_t\}$ , where  $t$  is the maximum index such that  $p_t \geq \frac{n}{m}$ . We can assume that  $n$  is sufficiently large. We can also assume that  $m \ll e^{(\ln n)^{1/3}}$  (otherwise the desired bound is trivial).

Let us start by defining  $L_j$  (for each  $j$  such that  $|M_j^1| = m$ ) as the union of all sets from the family  $\mathcal{M}_j \in \mathfrak{M}_0$ . Consider a family of sets  $\mathcal{L} = \{L_{i_1}, \dots, L_{i_r}\}$ . Let us build a minimal SCR  $\mathcal{L}$  (§3.3) and estimate the cardinality of this SCR or, in other words, obtain a bound for  $\tau(\mathcal{L})$ . Applying Lemma 4 with  $l = 0$  we obtain  $|L_{i_j}| \geq \frac{1}{2} \cdot \frac{\ln p_{i_j}^m}{\ln \ln p_{i_j}^m}$ . Here we choose  $n$  to be sufficiently large for the inequality  $p_{i_j} > \frac{n}{m} > 5$  to be satisfied. For sufficiently large values of  $x$ , the function  $\frac{\ln x}{\ln \ln x}$  is increasing, therefore we can write

$$|L_{i_j}| \geq \frac{1}{2} \cdot \frac{\ln \left(\frac{n}{m}\right)^m}{\ln \ln \left(\frac{n}{m}\right)^m}.$$

Let

$$k = \frac{1}{2} \cdot \frac{\ln \left(\frac{n}{m}\right)^m}{\ln \ln \left(\frac{n}{m}\right)^m}.$$

From Lemma 5 we have  $r \leq t \leq s \leq n$ , and thus Theorem 5 yields

$$\tau(\mathcal{L}) = O\left(\frac{n}{k} \ln k\right) = O\left(\frac{n}{\ln \left(\frac{n}{m}\right)^m} \cdot \left(\ln \ln \left(\frac{n}{m}\right)^m\right)^2\right).$$

Let  $\tau_1 = \tau(\mathcal{L})$ , and let us denote the elements of the corresponding SCR as  $v_1^1, \dots, v_{\tau_1}^1$ .

For each  $j \in \{i_1, \dots, i_r\}$  consider an element  $v_{\nu(j)}^1$  that lies in the set  $L_j$ . Clearly, this element lies in a number of sets  $M_j^i$  in the family  $\mathcal{M}_j$ . For each identified set  $M_j^i$ , replace  $M_j^i$  by  $M_j^i \setminus \{v_{\nu(j)}^1\}$ . Now delete all other  $M_j^i$  from  $\mathcal{M}_j$  (if  $\mathcal{M}_j$  became empty or now contains only empty sets then we delete it from  $\mathfrak{M}_0$ ) and rename sets which are left (which contain  $v_{\nu(j)}^1$ ) so that  $\mathcal{M}_j = \{M_j^1, \dots, M_j^{h(j)}\}$ . Define  $L_j$  (for  $j$  such that  $|M_j^1| = m - 1$ ) as union of all sets of  $\mathcal{M}_j$ .

From Lemma 4 with  $l = 1$  or  $0$  (depending on  $\text{rank}_j$ ), we have

$$|L_j| \geq \frac{1}{2} \cdot \frac{\ln \left(\frac{n}{m}\right)^{m-1}}{\ln \ln \left(\frac{n}{m}\right)^{m-1}}.$$

Let  $\{v_1^2, \dots, v_{\tau_2}^2\}$  be an SCR for  $\mathcal{L}$ . As before, Lemma 4 and Theorem 5 yield

$$\tau(\mathcal{L}) = O\left(\frac{n}{\ln \left(\frac{n}{m}\right)^{m-1}} \cdot \left(\ln \ln \left(\frac{n}{m}\right)^m\right)^2\right).$$

Repeating this procedure  $m$  times we obtain the following set:

$$M' = \{v_1^1, \dots, v_{\tau_1}^1\} \sqcup \{v_1^2, \dots, v_{\tau_2}^2\} \sqcup \dots \sqcup \{v_1^m, \dots, v_{\tau_m}^m\}.$$

Let  $M^* = \bigcup_{p_i < \frac{n}{m}} M_i^1$ ,  $M = M' \cup M^*$ . From the prime number theorem (see [4]) and inequality  $\text{rank}_i \leq m$ ,  $|M^*| = O\left(m \frac{n}{m \ln(n/m)}\right) = O\left(\frac{n}{\ln(n/m)}\right) = O\left(\frac{n \ln(m+1)}{\ln \frac{n}{m}} \left(\ln \ln \left(\frac{n}{m}\right)^m\right)^2\right)$ . It is clear that  $\theta(\mathfrak{M}) \leq |M|$ , i.e., we can write

$$\theta(\mathfrak{M}) - |M^*| \leq O\left(\frac{n}{\ln\left(\frac{n}{m}\right)^m} \cdot \left(\ln \ln\left(\frac{n}{m}\right)^m\right)^2\right) + O\left(\frac{n}{\ln\left(\frac{n}{m}\right)^{m-1}} \cdot \left(\ln \ln\left(\frac{n}{m}\right)^m\right)^2\right) + \dots + O\left(\frac{n}{\ln\left(\frac{n}{m}\right)} \cdot \left(\ln \ln\left(\frac{n}{m}\right)^m\right)^2\right).$$

To simplify the right-hand side of this asymptotic inequality, it is sufficient to compute the sum of the following expressions:

$$\frac{1}{\ln\left(\frac{n}{m}\right)^r} = \frac{1}{r} \cdot \frac{1}{\ln\left(\frac{n}{m}\right)}, \quad r = 1, \dots, m.$$

Writing this sum as  $O\left(\frac{\ln(m+1)}{\ln\left(\frac{n}{m}\right)}\right)$  proves the theorem.

**Remark.** In [1], [2]  $M$  was constructed in a different (and incorrect) way. On each turn for each  $p_j \geq \frac{n}{m}$  index of some new column (independent over  $\mathbb{Z}_{p_j}$  with chosen for  $p_j$  before) was added to  $M$ . This was possible due to the incorrect version of Lemma 4: with correct version of it we can only guarantee  $k = \frac{1}{2} \cdot \frac{\ln\left(\frac{n}{m}\right)}{\ln \ln\left(\frac{n}{m}\right)}$  on each turn of this algorithm and thus the bound for  $|M|$  becomes much weaker than required to prove Theorem 2.

## Acknowledgements

I would like to thank A.M Raigorodskii for productive discussions about [1],[2], helpful suggestions and proofreading.

## References

- [1] A.A. Bagan, A.M. Raigorodskii, *Defect of an admissible octahedron in a centering of an integer lattice generated by a given number of vectors*, Math. Notes, 99 (2016), N3, 457–459
- [2] A.A. Bagan, A.M. Raigorodskii, *Defect of an admissible octahedron in a centering obtained by adding rational vectors to an integer lattice*, Moscow Journal of Combinatorics and Number Theory, 5 (2015), N 1-2, 3-13
- [3] J.W.S. Cassels, *An introduction to the geometry of numbers*, Springer Berlin Heidelberg, 1996, 344 p.
- [4] A. Karatsuba, *Basic analytic number theory*, Springer Berlin Heidelberg, 2012, 222 p.
- [5] N.N. Kuzyurin, *The asymptotic investigation of the problem of covering*, Probl. Kibern., 1980, N37, 19–56.
- [6] N.G. Moshchevitin, *The defect of an admissible octahedron in a lattice*, Math. Notes, 58 (1995), N4, 558–568.
- [7] A.M. Raigorodskii, *The defects of admissible balls and octahedra in a lattice, and systems of generic representatives*, Mat. Sb., 189 (1998), N6, 117–141.
- [8] A.M. Raigorodskii, *On a problem in the geometry of numbers*, Proc. National Acad. Sci. Belarus, 15 (2007), N1, 111–117.



- [9] A.M. Raigorodskii, *Systems of common representatives in combinatorics and their application to geometry*, MCCME, Moscow, Russia, 2009.
- [10] A.M. Raigorodskii, *The defects of admissible sets in a lattice, and systems of common representatives*, Beiträge zur zahlentheoretischen Analysis, Grazer Math. Berichte, N338 (1999), 31–62.
- [11] A.M. Raigorodskii, *A probabilistic approach to the problem of the defects of admissible sets in a lattice*, Math. Notes, 68 (2000), N6, 910–916.
- [12] A.M. Raigorodskii, *Systems of common representatives*, Fundam. Prikl. Mat., 5 (1999), N3, 851–860.