Geometric and Functional Analysis
Vol. 2, No. 4 (1992)

1016-443X/92/0400381-13$1.50+0.20/0

ON THE NUMBER OF CONVEX LATTICE POLYTOPES

I. BÁRÁNY AND A.M. VERSHIK

1. Introduction and Results

A convex polytope $P \subset R^d$ is a lattice polytope if all of its vertices come from the lattice of integers, Z^d. Write $\mathcal{P}$ or $\mathcal{P}_d$ for the set of all convex lattice polytopes with positive volume. Two convex lattice polytopes are said to be *equivalent* if there is a lattice preserving affine transformation $R^d \mapsto R^d$ carrying one to the other. This is clearly an equivalence relation and equivalent polytopes have the same volume. Write $N_d(A)$ for the number of different (i.e., non-equivalent) convex lattice polytopes of volume A in R^d. Arnold [Ar] proved that

$$A^{1/3} \ll \log N_2(A) \ll A^{1/3} \log A \ , \tag{1.1}$$

He conjectured and Konyagin, Sevastyanov [KS] proved that this extends to higher dimension in the following way:

$$A^{\frac{d-1}{d+1}} \ll \log N_d(A) \ll A^{\frac{d-1}{d+1}} \log A \ . \tag{1.2}$$

Actually, the lower bound here is due to Arnold [Ar]. In this paper we improve upon the upper bound giving the right order of magnitude of $\log N_d(A)$.

THEOREM 1.

$$\log N_d(A) \ll A^{\frac{d-1}{d+1}} \ . \tag{1.3}$$

This theorem is proved in the special case $d = 2$ in [BP]. Although the proof given there uses a lemma similar to Theorem 2 below it does not go through in higher dimensions.

The upper bound in (1.1) and (1.2) follows from the fact that the number of vertices of any $P \in \mathcal{P}_d$ is $\ll (\operatorname{vol} P)^{\frac{d-1}{d+1}}$. This is a result of Andrews [An1], other proofs and extensions can be found in [KS] and [Sch]. Using Theorem 1, or rather its proof, we get this as a corollary.

The first named author is partially supported by Hungarian National Science Foundation no. 1907 and 1909.

COROLLARY. *The number of vertices of any $P \in \mathcal{P}_d$ is* $\ll (\operatorname{vol} P)^{\frac{d-1}{d+1}}$.

The main tool in the proof of Theorem 1 is a result about "multi-partitions". Write Z_+^d for the set of positive integer points of R^d, i.e., $z \in Z_+^d$ if every component of z is a positive integer. Given $n = (n_1, \dots, n_d) \in Z_+^d$ we call a set $\{z_1, \dots, z_t\} \subset Z_+^d$ such that $\sum_{i=1}^t z_i = n$ a *multi-partition* of n. The number of distinct multi-partitions of n will be denoted by $p(n)$. The generating function of $p(n)$ is given in Andrews' book [An2] as

$$f(x) = \sum_{n \in Z_+^d} p(n) x^n = \prod_{m \in Z_+^d} (1 - x^m)^{-1}, \tag{1.4}$$

where $x = (x_1, \dots, x_d) \in R^d$ and $x^n = x_1^{n_1} \dots x_d^{n_d}$. It is clear and actually well known, that $f(x)$ is well-defined and finite when all $|x_i| < 1$. To our surprise we could not find the following theorem in the literature.

THEOREM 2.

$$\log p(n) \le (d+1)\big(\zeta(d+1) n_1 \dots n_d\big)^{1/(d+1)} .$$

Here $\zeta(d+1) = \sum_1^\infty k^{-(d+1)}$ is the zeta function.

When $d = 1$, $p(n)$ is the number of partitions of $n \in Z$ and the upper bound from Theorem 2 is very good, cf. [Ra]. In the case $d = 2$ a more precise formula is given in [Au]. In fact, $p(n)$ is determined there with high precision in the range when n_1/n_2 and n_2/n_1 is bounded. It follows from [BP] that $\log p(n)$ is of the order $(n_1 n_2)^{1/3}$ when n_1/n_2^2 and n_2/n_1^2 is bounded, and less than that outside this range. In higher dimensions, $\log p(n)$ is of the order $(n_1 \dots n_d)^{1/(d+1)}$ when none of the n_i is too small. Even the constant in Theorem 2 is best possible, see the Remark at the end of section 2. We mention that the same bound would not apply if $z_i = 0$ were allowed for the components of the constituents of the multi-partition. This can be seen easily by comparing $p(n)$ for $d = 1$ and $d = 2$.

To conclude this introductory section we give a sketch of the proof of Theorem 1. First we find a representative from each equivalence class in the aligned box $T(\gamma) = \{x \in R^d : 0 \le x_i \le \gamma_i \ , \ i = 1, \dots, d\}$ where the volume of $T(\gamma)$ is $\le \operatorname{const} A$. This is done in Theorem 3. Then we prove a statement stronger than required, namely, that the number of convex lattice polytopes lying in $T(\gamma)$ is less than $\exp\{\operatorname{const}(\prod_{i=1}^d \gamma_i)^{1/(d+1)}\}$. The idea is that by a theorem of Minkowski [BF, pp. 118–119] a convex polytope is uniquely determined (up to translation) by the outer normals and $(d-1)$-dimensional volumes of its facets. The outer normal to a facet of a convex lattice polytope $P \subset T(\gamma)$, with its euclidean length equal to the $(d-1)$-dimensional volume of the facet, is a vector from the lattice $\frac{1}{(d-1)!}Z^d$. Moreover, the j-th component of the normal is the volume of the projection, onto the hyperplane $x_j = 0$, of the facet. So the sum of the absolute values of the j-th components of the normals is less than twice $\prod_{i \neq j} \gamma_i$. Then Theorem 2 shows that the number of possible collections of outer normals is bounded by $\exp\left\{\text{const}(\prod_{i=1}^d \gamma_i)^{(d-1)/(d+1)}\right\}$. However, some components of the normals can be equal to 0 which is not allowed in Theorem 2. This causes difficulties and we have to rely on a theorem of Pogorelov [Po] (instead of Minkowski).

A few words are in place here about notation. When $x \in R^d$ we write $x_1, \ldots, x_d$ for its components in the standard basis of R^d. We will use Vinogradov's $\ll$ notation, the implied constants will depend on dimension only.

The paper is organized as follows. The next section contains the proof of Theorem 2. In section 3 we find a representative of each equivalence class in the aligned box $T(\gamma)$. The proof of the main theorem is in section 4. Finally we prove the Corollary and make some further comments.

2. Proof of Theorem 2

We start with taking the logarithm of (1.4).

$$\begin{aligned} \log f(x) &= \log \prod_{m \in Z_+^d} (1-x^m)^{-1} = \sum_{m \in Z_+^d} \log \frac{1}{1-x^m} \\ &= \sum_{m \in Z_+^d} \sum_{k=1}^{\infty} \frac{x^{km}}{k} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{m \in Z_+^d} x^{km} = \sum_{k=1}^{\infty} \frac{1}{k} \prod_{i=1}^{d} \frac{x_i{}^k}{1-x_i{}^k}, \end{aligned} \tag{2.1}$$

where the last equality follows easily from

$$\sum_{m \in Z_+^d} x^{km} = \prod_{i=1}^{d} (x_i{}^k + x_i{}^{2k} + \ldots) = \prod_{i=1}^{d} \frac{x_i{}^k}{1-x_i{}^k},$$

which is true when all $|x_i| < 1$. Now for every $t \in (0,1)$

$$\frac{t^k}{1-t^k} = \frac{t}{1-t} \frac{t^{k-1}}{1+t+\ldots+t^{k-1}} \leq \frac{t}{k(1-t)}.$$

From now on we assume all $x_i \in (0,1)$. Then we get from (2.1) that

$$\begin{aligned}\log f(x) &\le \sum_{k=1}^{\infty} \frac{1}{k} \prod_{i=1}^{d} \frac{x_i}{k(1-x_i)} \\ &= \zeta(d+1) \prod_{i=1}^{d} \frac{x_i}{1-x_i} \ .\end{aligned} \tag{2.2}$$

On the other hand, we get, again from (1.4) that $p(n)x^n \le f(x)$. So

$$\log p(n) + \sum_{i=1}^{d} n_i \log x_i \le \log f(x).$$

This, together with (2.2) shows that if all $x_i \in (0,1)$, then

$$\begin{aligned}\log p(n) &\le \sum_{i=1}^{d} n_i \log \frac{1}{x_i} + \zeta(d+1) \prod_{i=1}^{d} \frac{x_i}{1-x_i} \\ &\le \sum_{i=1}^{d} n_i \frac{1-x_i}{x_i} + \zeta(d+1) \prod_{i=1}^{d} \frac{x_i}{1-x_i} \ ,\end{aligned} \tag{2.3}$$

where we used the inequality $\log \frac{1}{t} \le \frac{1}{t} - 1$, valid for every $t \in (0,1)$. Now we try to choose x (with all $x_i \in (0,1)$) so that the right hand side of (2.3) be small. A convenient choice is when all the $d+1$ terms in the right hand side are equal, i.e.,

$$n_1 \frac{1-x_i}{x_i} = \ldots = n_d \frac{1-x_d}{x_d} = \zeta(d+1) \prod_{i=1}^{d} \frac{x_i}{1-x_i} = \lambda \ .$$

A simple computation shows now that

$$\lambda = \left(\zeta(d+1) \prod_{i=1}^{d} n_i \right)^{1/(d+1)} \quad \text{and } x_i = \frac{n_i}{n_i + \lambda}$$

which is indeed between 0 and 1. Then we get in (2.3)

$$\log p(n) \le (d+1)\lambda = (d+1) \left(\zeta(d+1) \prod_{i=1}^{d} n_i \right)^{1/(d+1)} \ . \qquad \square$$

Remark: Using the saddle point method one can actually prove that

$$\log p(n) = (d+1)\left(\zeta(d+1)\prod_{i=1}^{d} n_i\right)^{1/(d+1)}(1+o(1))$$

when all the n_i are equal. We hope to return to this question in the companion paper [BV].

3. Choosing the Proper Polytope

In the proof of Theorem 1 we will need a suitable representative from each equivalence class of $\mathcal{P}$. This will be found as follows. Assume $B = \{b^1, \dots b^d\}$ is a basis of Z^d. Given α and β in R^d define

$$T(B,\alpha,\beta) = \left\{x = \sum_{i=1}^{d} \xi_i b^i \in R^d : \alpha_i \le \xi_i \le \beta_i \text{ for all } i\right\} .$$

$T(B,\alpha,\beta)$ is, obviously, a convex polytope. In fact, it is a parallelotope whose edges are parallel to the b^i. Its volume equals $\prod_{i=1}^{d}(\beta_i - \alpha_i)$. Given $P \in \mathcal{P}$ choose α_i maximal and β_i minimal under the condition that $P \subset T(B,\alpha,\beta)$ for every $i = 1, \dots, d$. Write $T(B,P) = T(B,\alpha,\beta)$ with the extremal α and β which are, of course, uniquely determined. $T(B,P)$ is a lattice parallelotope. We need the following result.

THEOREM 3. *Given $P \in \mathcal{P}$ there is a basis B of Z^d such that*

$$\operatorname{vol} T(B,P) \ll \operatorname{vol} P .$$

Proof: We prove the theorem first when P is centrally symmetric with centre at the origin. In this case, as it is well-known, there is an ellipsoid $E \subset R^d$ centred at the origin such that

$$d^{-1/2}E \subset P \subset E .$$

Apply now a linear transformation τ that carries E to the euclidean unit ball of R^d. We denote this ball by D. Evidently, $L = \tau Z^d$ is a lattice again.

Consider now a basis $\widetilde{B} = \{\tilde{b}^1, \dots, \tilde{b}^d\}$ of L together with a dual basis $C = \{c^1, \dots, c^n\}$. This is defined (see, for instance, [Ca]) so as to satisfy

$\tilde{b}^i c^j = \delta_{ij}$ for all i and j. The dual basis spans a lattice, L^*, which is dual to L in the sense that, for all $x \in L$ and $y \in L^*$, $xy \in Z$. It is also well known that $\det(L)\det(L^*) = 1$ where $\det(L)$ and $\det(L^*)$ are equal to the volume of any basis parallelotope of the lattice L and L^*, respectively.

Consider now $T(\widetilde{B}, D) = T(\widetilde{B}, -\alpha, \alpha)$. The facets of $T(\widetilde{B}, -\alpha, \alpha)$ touch the unit ball D and the point $\alpha_i \tilde{b}^i$ is on such a facet. Since the unit normal to this facet is $c^i/\|c^i\|$ we must have $1 = (\alpha_i \tilde{b}^i)(c^i/\|c^i\|) = \alpha_i/\|c^i\|$. Consequently

$$\operatorname{vol} T(\widetilde{B}, D) = \det(L) \prod_{i=1}^{d} 2\alpha_i = \det(L) 2^d \prod_{i=1}^{d} \|c^i\| \ .$$

According to an old theorem of Hermite (see [He] or [Ca]), there is a basis C of the lattice L^* such that $\prod_{i=1}^{d} \|c^i\| \ll \det(L^*)$. Fix a basis C with this property, and compute the corresponding dual basis $\widetilde{B}$ of L. We know then that $\operatorname{vol} T(\widetilde{B}, D) \ll \det(L)\det(L^*) = 1$.

Let us apply now τ^{-1} to $\widetilde{B}$, D, and L. We get a basis $B = \tau^{-1}\widetilde{B}$ of $Z^d = \tau^{-1}L$, and

$$\tau^{-1} T(\widetilde{B}, D) = T(B, E) \ .$$

Moreover, $T(B, P)$ is a lattice polytope which is contained in $T(B, E)$ since $P \subset E$. Now

$$\begin{aligned} \operatorname{vol} T(B, P) &\le \operatorname{vol} T(B, E) = \det \tau^{-1} \operatorname{vol} T(\widetilde{B}, D) \\ &\ll \det \tau^{-1} = \operatorname{vol} E / \operatorname{vol} D \\ &\ll \operatorname{vol} P \ . \end{aligned}$$

This proves the case when P is centrally symmetric.

For a general $P \in \mathcal{P}$ we may assume $0 \in P$. Consider $Q = P - P$. Clearly, Q centrally symmetric and is in $\mathcal{P}$. By a result of [RS], $\operatorname{vol} Q \ll \operatorname{vol} P$. Let now B be the "good" basis for Q whose existence is established above. It will be a good basis for P as well since $T(B, P) \subset T(B, Q)$ and

$$\operatorname{vol} T(B, P) \le \operatorname{vol} T(B, E) \ll \operatorname{vol} Q \ll \operatorname{vol} P.$$ □

Remark: There are other ways to prove Theorem 3. We could, for instance, choose $\widetilde{B}$ to be a Lovász–reduced basis (for the definition see [Lo] or [GLS]), and argue that $\tau^{-1}\widetilde{B}$ satisfies the assertion of the theorem. Or we could take a Korkine–Zolotarov basis of L (see [Ca] or [GLS]). Yet another proof, in two dimensions, is given in [BP].

4. Proof of the Main Theorem

Given any $P \in \mathcal{P}$ with $\operatorname{vol} P = A$ choose a basis B of Z^d according to Theorem 3. Then apply an affine transformation carrying B to the standard basis $\{e^1, \dots, e^d\}$ of Z^d and choose the origin so that the image of $T(B, P)$ is

$$T\big(\{e^1, \dots, e^d\}, 0, \gamma\big)$$

which we will denote by $T(\gamma)$ from now on. We know that for any $P \in \mathcal{P}$ there is a $Q \in \mathcal{P}$, equivalent to P that lies in $T(\gamma)$ where $\gamma \in Z_+^d$ satisfies $\prod_{i=1}^d \gamma_i \ll A$.

Fix now $\gamma \in Z_+^d$ and set $\Gamma = \prod_{i=1}^d \gamma_i$. Write $N(\gamma)$ for the number of convex lattice polytopes (not necessarily with positive volume) that lie in $T(\gamma)$. We are going to show that

$$\log N(\gamma) \ll \Gamma^{\frac{d-1}{d+1}} . \tag{4.1}$$

This will prove the theorem since the number of $\gamma \in Z_+^d$ with $\Gamma \ll A$ is less than A^d as one can easily check.

Let the convex lattice polytope P lie in $T(\gamma)$ and consider the 2^d unbounded polyhedra

$$P_\varepsilon = P + \{x \in R^d : \varepsilon_i x_i \le 0 \text{ for all } i\}$$

where $\varepsilon = (\varepsilon_1, \dots, \varepsilon_d) \in R^d$ with $\varepsilon_i = +1$ or -1. These 2^d polyhedra determine P uniquely. Define $N_\varepsilon(\gamma)$ as the number of different polyhedra $\mathcal{P}_\varepsilon$ coming from a lattice polytope in $T(\gamma)$. We will show that, for fixed ε,

$$\log N_\varepsilon(\gamma) \ll \Gamma^{\frac{d-1}{d+1}}. \tag{4.2}$$

This will clearly prove (4.1). By symmetry, it will be enough to show (4.2) when $\varepsilon = (1, \dots, 1)$. In this case we denote P_ε simply by P_+.

Let pr_i be the orthogonal projection onto the hyperplane $x_i = 0$. Define

$$P^* = \big\{x \in R^d : \operatorname{pr}_i(x) \in \operatorname{pr}_i(P_+) \text{ for all } i\big\} .$$

This unbounded polyhedron is called the *profile* of P or P_+. The lattice polytopes P_i $(i = 1, \dots, d)$ are defined as

$$P_i = P^* \cap T(\gamma) \cap \{x \in R^d : x_i = 0\}.$$

They determine P^* uniquely. P_i is a $(d-1)$–dimensional polytope lying in $\mathrm{pr}_i T(\gamma)$, an aligned box in $(d-1)$–dimensions that has volume Γ/γ_i. Write $N^*(\gamma)$ for the number of different profiles of the convex lattice polytopes $P \subset T(\gamma)$. An easy induction, using (4.1) as the inductional hypothesis, shows that

$$\log N^*(\gamma) \ll \sum_{i=1}^{d} (\Gamma/\gamma_i)^{\frac{d-2}{d}} \ll \Gamma^{\frac{d-2}{d}}.$$

(A little extra care is needed when $d = 2$. Then $\log N^*(\gamma) = \log(\gamma_1\gamma_2)$ and this works for the remainder of the proof.)

Fix now a profile P^* coming from some $P \subset T(\gamma)$, and write $N_+(P^*)$ for the number of different polyhedra with profile P^*. We will prove now that

$$\log N_+(P^*) \ll \Gamma^{\frac{d-1}{d+1}} \tag{4.3}$$

Since $N_+(\gamma) = \sum_{P^*} N_+(P^*) \le N^*(\gamma) \exp\{c\Gamma^{\frac{d-1}{d+1}}\}$, this will prove (4.2).

Let us now have a closer look at the bounded facets of P_+. Notice, first, that if P_+ has no bounded facets, then $P_+ = P^*$. Assume now that P_+ has a bounded facet F. As P is a lattice polytope there is a unique outer normal $v(F)$ to F which is a primitive vector in Z^d (actually in Z^d_+). F is a $(d-1)$–dimensional lattice polytope in the sublattice, of Z^d, orthogonal to $v(F)$. The determinant of this sublattice is $\|v(F)\|$. Whence

$$\mathrm{vol}_{d-1} F = \frac{z}{(d-1)!} \|v(F)\| ,$$

for some positive integer z. So the facet F determines the vector $u(F) = \frac{z}{(d-1)!} v(F) \in \frac{1}{(d-1)!} Z^d$, which, in turn, gives the outer normal and the $(d-1)$–dimensional volume of F. Moreover, the i–th component of $u(F)$ is equal to $\mathrm{vol}_{d-1}\mathrm{pr}_i(F)$ as the reader can easily check. Since all the bounded facets of P_+ lie in $T(\gamma)$ we get

$$\sum_F u_i(F) = \sum_F \mathrm{vol}_{d-1}\mathrm{pr}_i(F) \le \mathrm{pr}_i\big(T(\gamma)\big) = \Gamma/\gamma_i .$$

We call a finite subset U of Z^d_+ *special* if, for all $i = 1, \dots, d$

$$\sum_{u \in U} u_i \le (d-1)!\Gamma/\gamma_i. \tag{4.4}$$

(Of course, U is special with respect to γ.) We need the unicity part of the following result of Pogorelov.

LEMMA. *Given a profile P^* and vectors $u^1, \dots, u^k \in R^d_+$, no two of them parallel, there is a unique unbounded polyhedron P_+ with profile P^* and having k bounded facets $F_1, \dots, F_k$ such that, for $j = 1, \dots, k$, the outer normal to P_+ at F_j is u^j and the $(d-1)$–dimensional volume of F_j is $\|u^j\|$.*

A more general result in three–dimensional space is given in Pogorelov's book [Po, page 542], and the proof there goes through in higher dimensions. For the convenience of the reader we reproduce Pogorelov's proof at the end of this section.

This means that, given P^* and a special $U = \{u^1, \dots, u^k\} \subset Z^d_+$, there is a unique unbounded polyhedron P_+ with k bounded facets $F_1, \dots, F_k$ such that u^j is an outer normal to F_j and $\text{vol}_{d-1} F_j = \frac{1}{(d-1)!}\|u^j\|$. Not every such P_+ is a lattice polyhedron, but certainly all P_+ coming from a lattice polytope P can be represented this way. Consequently

$$N_+(P^*) \le \text{number of special sets } U \text{ satisfying (4.4)} \,. \tag{4.5}$$

Finally, define $n \in Z^d_+$ by $n_i = (d-1)!\Gamma/\gamma_i$. According to Theorem 2 the number of special sets satisfying (4.4) is

$$\begin{aligned}\sum_{\substack{m \le n \\ m \in Z^d_+}} p(m) &\le \sum_{\substack{m \le n \\ m \in Z^d_+}} \exp\left\{(d+1)\Big(\zeta(d+1)\prod_{i=1}^d m_i\Big)^{1/d+1}\right\} \\ &\le \Big(\prod_{i=1}^d n_i\Big) \exp\left\{(d+1)\Big(\zeta(d+1)\prod_{i=1}^d n_i\Big)^{1/d+1}\right\} \\ &= (d-1)!^d\Gamma^{d-1} \exp\left\{(d+1)\big(\zeta(d+1)(d-1)!^d\Gamma^{d-1}\big)^{1/d+1}\right\}\end{aligned} \tag{4.6}$$

This together with (4.5) proves (4.3). □

Proof of the Lemma: Set $e = (1, \dots, 1) \in R^d$ and denote by $H_j(\omega_j)$ the hyperplane orthogonal to u^j and intersecting the line $\{\tau e \in R^d : \tau \in R\}$ at the point $\omega_j e$. Let us denote by $H_j^-(\omega_j)$ the halfspace bounded by $H_j(\omega_j)$ and containing infinite ray pointing in the direction $-e$. Any P_+ with bounded facets orthogonal to u^j $(j = 1, \dots, k)$ is of the form

$$P(\omega) = P^* \cap \bigcap_{j=1}^k H_j^-(\omega_j)$$

where the parameter ω is a point from R^k_+. Write $F_j(\omega)$ for the intersection of $P(\omega)$ with $H_j(\omega_j)$. Note that $F_j(\omega)$ may be empty.

We first prove the existence. We choose a sufficiently large compact set $C \subset R^k_+$ by requiring, say, that for $\omega \in C$ the set $P^* \cap H_j(\omega_j)$ be nonvoid. Define Ω as the of those $\omega \in C$ for which the $(d-1)$–volume of $F_j(\omega)$ is at most $\|u^j\|$ $(j = 1, \ldots, d)$. The set Ω is clearly compact and nonempty. So the continuous function $g : \Omega \mapsto R$ defined by

$$g(\omega) = \sum_{j=1}^{k} \omega_j$$

takes its minimum at some point in Ω which we denote by ω, too. We claim that $P(\omega)$ has the required properties. Assume not, then $\mathrm{vol}_{d-1} F_j(\omega) < \|u^j\|$ for some j. Decrease ω_j a little and leave the other ω_i unchanged. Let ω' be the new ω. It follows from continuity that $\mathrm{vol}_{d-1} F_j(\omega') < \|v^j\|$. On the other hand, for $i \neq j$, $F_i(\omega') \subset F_i(\omega)$ and so $\mathrm{vol}_{d-1} F_i(\omega') \leq \mathrm{vol}_{d-1} F_i(\omega)$. Thus $\omega' \in \Omega$. But $g(\omega') < g(\omega)$, a contradiction.

Now for unicity. This time we include the ω_j corresponding to the unbounded facets of P^* into ω. Then, of course, we include their outer normals into U as well. Suppose there are two solutions $P(\omega)$ and $P(\bar{\omega})$ and let $\delta = \max_j(\omega_j - \bar{\omega}_j)$. We assume $\delta > 0$ (otherwise exchange the names). Denote by J the set of those indices j for which $\delta = \omega_j - \bar{\omega}_j$ and set $Q(\omega) = P(\omega) - \delta e$. J is nonempty but does not contain the indices corresponding to the unbounded facets since for those $\omega_i = \bar{\omega}_i$. Clearly $Q(\omega) = \bigcap_j H_j^-(\omega_j - \delta)$ is a subset of $P(\bar{\omega})$.

Denote by $\bar{F}_j$ (and F_j) the facet of $P(\bar{\omega})$ (and $Q(\omega)$, respectively,) that corresponds to the index $j \in \{1, \ldots, k\}$. Two facets, $\bar{F}_j$ and $\bar{F}_i$ are said to be *adjacent* if they intersect in a $(d-2)$–dimensional face of $P(\bar{\omega})$. We claim that, for $j \in J$, $\bar{F}_j$ is adjacent only to facets $\bar{F}_i$ with $i \in J$. Assume, on the contrary, that there are indices $j \in J$ and $i \notin J$ such that $\bar{F}_j$ and $\bar{F}_i$ are adjacent. We know that

$$\bar{F}_j = H_j(\bar{\omega}_j) \cap \bigcap_{m=1}^{k} H_m^-(\bar{\omega}_m) \ ,$$

and similarly

$$F_j = H_j(\bar{\omega}_j) \cap \bigcap_{m=1}^{k} H_m^-(\omega_m - \delta) \ .$$

As $\bar{\omega}_m \geq \omega_m - \delta$, we have $F_j \subset \bar{F}_j$. This inclusion is proper because $\bar{\omega}_i > \omega_i - \delta$ and $\bar{F}_j$ is adjacent to $\bar{F}_i$. But then $\mathrm{vol}_{d-1}F_j < \mathrm{vol}_{d-1}\bar{F}_j$, a contradiction.

The claim implies that all indices are in J. But this contradicts the fact that an index corresponding to an unbounded facet is not in J. □

5. Final remarks

The above proof gives the following theorem. Let $\Gamma \in Z_+$ and define $\mathcal{P}_d(\Gamma)$ as the set of all convex lattice polytopes lying in an aligned box $T(\gamma)$ for some $\gamma \in Z_+^d$ with $\prod_{i=1}^d \gamma_i \leq \Gamma$.

THEOREM 4.

$$\log |\mathcal{P}_d(\Gamma)| \ll \Gamma^{\frac{d-1}{d+1}} .$$

The Corollary follows from here easily. Indeed, let $P \subset T(\gamma)$ be a convex lattice polytope with $\prod \gamma_i \leq \Gamma$ and write V for the set of vertices of P. Then $\mathrm{conv}\, W \subset T(\gamma)$ is a convex lattice polytope, again, for every nonempty subset $W \subset V$. This way we get $2^{|V|}-1$ distinct lattice polytopes, so

$$2^{|V|} - 1 \leq \left|\mathcal{P}_d(\Gamma)\right| .$$

Thus Theorem 4 implies that $|V| \ll \Gamma^{\frac{d-1}{d+1}}$.

The proof of Theorem 1 and the lower bound in (1.2) show that $\log p(n)$ is of the order $A^{1/(d+1)}$ for some values of $n \in Z_+^d$ with $\prod n_i \leq A$. And if $\log p(n)$ were smaller for all n, then using this smaller bound in (4.6) we would get a smaller bound for $\log N_d(A)$, a contradiction.

We think it would be interesting to study the family $\mathcal{Q}_d$ of "dually integral" polytopes. A polytope Q is in $\mathcal{Q}_d$ if the outer normal $u(F)$ to its facet F, with its length equal the $(d-1)$–volume of the facet, is in Z_+^d for every facet F. According to a theorem of Minkowski (see [BF]) such a polytope is uniquely determined (up to translation) by the set

$$U(Q) = \{u(F) : F \text{ is a facet of } Q\} .$$

It is clear, further, that $\sum_{u \in U(Q)} u = 0$. There is an equivalence relation on $\mathcal{Q}_d$, namely, two polytopes P and $Q \in \mathcal{Q}_d$ are equivalent if there is a lattice preserving affine tranformation τ such that $\tau(U(P)) = U(Q)$. It is not difficult to see that equivalent polytopes have the same volume. Moreover,

$\mathcal{P}_d$ is contained in $\mathcal{Q}_d$. We hope to return to the determination of the number of equivalent classes of dually integral polytopes of fixed volume in the near future.

Acknowledgement

Part of this work was done while both authors were visiting the Mittag–Leffler Institute in Stockholm. We thank the institute for financial support and for providing excellent conditions for research. We also thank László Lovász and Endre Makai Jr. for informative discussions.

References

[An1] G.E. Andrews, A lower bound for the volumes of strictly convex bodies with many boundary points, Trans. Amer. Math. Soc. 106 (1965), 270–273.

[An2] G.E. Andrews, Theory of partitions, Addison–Wiley, 1973.

[Ar] V.I. Arnold, Statistics of integral convex polytopes, (in Russian) Funk. Anal. Pril. 14 (1980), 1–3.

[Au] G. Auluck, On partitions of bipartite numbers, Proc. Cambridge Phyl. Soc. 49 (1953), 72–80.

[BP] I. Bárány, J. Pach, On the number of convex lattice polytopes, Comb. Prob. Comp. (1991), to appear.

[BV] I. Bárány, A.M. Vershik, The limit shape of convex lattice polygons in a square, (1992), in preparation.

[BF] T. Bonnesen, W. Fenchel, Theorie der konvexen Körper, Springer, 1974.

[Ca] J.W.S. Cassels, An introduction to the geometry of numbers, Cambridge Univ. Press, 1965.

[GLS] M. Grötschel, L. Lovász, L. Schrijver, Combinatorial optimization and the ellipsoid method, Springer, 1987.

[He] C. Hermite, Second letter to Jacobi, Oeuvres, I, J. Math. 40 (1905), 122–135.

[KS] S.B. Konyagin, K.A. Sevastyanov, Estimation of the number of vertices of a convex integral polyhedron in terms of its volume, (in Russian), Funk. Anal. Pril. 18 (1984), 13–15.

[Lo] L. Lovász, An algorithmic theory of numbers, graphs, and convexity, Regional Conferences in Applied Math. 50, 1986.

[Po] A.V. Pogorelov, Exterior geometry of convex surfaces, (in Russian), Nauka, 1969.

[Ra] H. Rademacher, Topics in analytic number theory, Springer, 1973.

[RS] C.A. ROGERS, G.C. SHEPHARD, The difference body of a convex body, Arch. Math. 8 (1957), 220–223.

[Sch] W. SCHMIDT, Integral points on surfaces and curves, Monatshefte. Math. 99 (1985), 45–82.

Imre Bárány
Mathematical Institute of the
Hungarian Academy of Sciences
POB 127
1364 Budapest, Hungary

Anatoly M. Vershik
Department of Mathematics
University of Saint Petersburg
Bibliot. Sq. 2
198904 Saint Petersburg, Russia

Submitted: February 1992