Acta Math. Hungar., **137 (1–2)** (2012), 72–81
DOI: 10.1007/s10474-012-0219-2
First published online April 27, 2012

ON A QUESTION OF V. I. ARNOL'D

I. BÁRÁNY[1,2]

[1] Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences,
H-1364 Budapest, Pf. 127, Hungary
e-mail: barany@renyi.hu

[2] Department of Mathematics, University College London,
Gower Street, London, WC1E 6BT, UK

(Received August 1, 2011; revised November 14, 2011; accepted December 8, 2011)

Abstract. We show by a construction that there are at least $\exp\{cV^{(d-1)/(d+1)}\}$ convex lattice polytopes in $\mathbb{R}^d$ of volume V that are different in the sense that none of them can be carried to an other one by a lattice preserving affine transformation.

1. Introduction and main result

In 1980 Arnol'd [2] asked the following question: How many convex lattice polytopes are there in $\mathbb{R}^d$? Infinitely many, of course. So Arnol'd refined the question. He calls two convex lattice polytopes *equivalent* if one can be carried to the other by a lattice preserving affine transformation. This is an equivalence relation and equivalent polytopes have the same volume. Let $N_d(V)$ denote the number of equivalence classes of convex lattice polytopes in $\mathbb{R}^d$ of volume V. Of course, $d!V$ is a positive integer. Arnol'd showed that

$$V^{1/3} \ll \log N_2(V) \ll V^{1/3} \log V.$$

Actually, Arnol'd proved the stronger statement that $\log N_2^+(V) \ll V^{1/3} \log V$ where $N_d^+(V)$ denotes the number of equivalence classes of convex lattice polytopes in $\mathbb{R}^d$ of volume at most V. He asked what happens in higher dimensions and Konyagin and Sevastyanov proved [7] that $\log N_d^+(V) \ll V^{(d-1)/(d+1)} \log V$. This was subsequently improved to $\log N_d^+(V) \ll V^{(d-1)/(d+1)}$ by Bárány and Pach [5] (for $d = 2$) and by Bárány

Key words and phrases: lattice, polytope, integer convex hull, statistics of convex lattice polytopes.

Mathematics Subject Classification: primary 52B20, secondary 11H06.

and Vershik [6] (for $d \geqq 2$). The proof of the lower bound $\log N_d^+(V) \gg V^{(d-1)/(d+1)}$ is quite easy as we will see soon. The main result of this paper is the same lower bound for $\log N_d(V)$:

THEOREM 1.1. $V^{(d-1)/(d+1)} \ll \log N_d(V)$.

In [2] Arnol'd proved this theorem for $d = 2$. For higher dimensions he only says: "Proof of the lower bound: let $x_1^2 + \cdots + x_{d-1}^2 \leqq x_d \leqq A$". The construction for the lower bound to be presented here uses an idea of Arnol'd and several further ingredients. Of course Theorem 1.1 has the following

COROLLARY 1.1. $V^{(d-1)/(d+1)} \ll \log N_d^+(V)$.

A proof is sketched in [3], and another proof is given by Chuanming Zong [9]. We also give a short argument for this corollary.

Some remarks are in place here about notation and terminology. A convex polytope $P \subset \mathbb{R}^d$ is a lattice polytope if its vertex set, $\operatorname{vert} P$ is a subset of $\mathbb{Z}^d$, the integer lattice. Write $\mathcal{P}$ or $\mathcal{P}_d$ for the set of all convex lattice polytopes in $\mathbb{R}^d$ with positive volume. The number of vertices of $P \in \mathcal{P}$ is denoted by $f_0(P)$. Throughout the paper we use, together with the usual "little oh" and "big Oh" notation, the convenient $\ll$ symbol, which means, for functions $f, g : \mathbb{R}_+ \to \mathbb{R}_+$, that $f(V) \ll g(V)$ if there are constants $V_0 > 0$ and $c > 0$ such that $f(V) \leqq cg(V)$ for all $V > V_0$. These constants, to be denoted by $c, c_1, \dots, b, b_1, \dots$ may only depend on dimension. The standard basis of $\mathbb{R}^d$ is $e_1, \dots, e_d$, and $|x| = \sqrt{x_1^2 + \cdots + x_d^2}$ is the Euclidean norm of $x = (x_1, \dots, x_d) \in \mathbb{R}^d$, and B^d is the Euclidean unit ball of $\mathbb{R}^d$, and $\operatorname{vol} B_d = \omega_d$. Also $\mathbb{R}_+^d$ denotes the set of $x \in \mathbb{R}^d$ with $x_i \geqq 0$ for every $i \in [d]$. Here $[d] = \{1, 2, \dots, d\}$.

The paper is organized as follows. The integer convex hull and some of its properties are given in the next section. A quick proof of Corollary 1.1 is the content of Section 3. Section 4 presents some auxiliary results. The construction of many non-equivalent convex lattice polytopes is in Section 5. We finish with concluding remarks.

2. The integer convex hull

Suppose $K \subset \mathbb{R}^d$ is a bounded convex set. Its *integer convex hull, $I(K)$*, is defined as

$$I(K) = \operatorname{conv}\left(K \cap \mathbb{Z}^d\right),$$

which is a convex lattice polytope if nonempty. One important ingredient of our construction is

$$Q_r = I\left(rB^d\right) = \operatorname{conv}\left(\mathbb{Z}^d \cap rB^d\right).$$

Trivially $\operatorname{vol} Q_r \leqq \omega_d r^d$. It is proved in Bárány and Larman in [4] that $\operatorname{vol}(rB_d \setminus Q_r) \ll r^{d\frac{d-1}{d+1}}$. The last exponent will appear so often that we write $D = d\frac{d-1}{d+1}$. The number of vertices of Q_r is estimated in [4] as

$$r^D \ll f_0(Q_r) \ll r^D. \tag{2.1}$$

The upper bound is a result of Andrews [1] stating that $f_0(P) \ll (\operatorname{vol} P)^{(d-1/(d+1)}$ for all $P \in \mathcal{P}_d$ with $\operatorname{vol} P > 0$.

We are to establish further properties of Q_r, always assuming that r is large enough.

Lemma 2.1. $(r - \sqrt{d}\,) B^d \subset Q_r$.

Proof. A cap C of B^d is the intersection of B^d with a halfspace H. If $\operatorname{int} C \cap \mathbb{Z}^d = \emptyset$, then $\operatorname{int} C$ cannot contain a translate of the unit cube, implying that the width of C is at most $\sqrt{d}$. □

Lemma 2.2. $(r - 2\sqrt{d}\,) B^d \subset I(Q_r \setminus \operatorname{vert} Q_r)$.

Proof. The previous lemma implies that no vertex of Q_r lies in $(r - \sqrt{d}\,) B^d$. Consequently $(r - \sqrt{d}\,) B^d \subset Q_r \setminus \operatorname{vert} Q_r$. Taking the integer convex hull of both sides and applying Lemma 2.1 to $Q_{r-\sqrt{d}} = I\big((r - \sqrt{d}\,) B^d\big)$ finishes the proof. □

For a lattice polytope $P \in \mathcal{P}$ with $x \in \operatorname{vert} P$ we define

$$\triangle(x) = P \setminus I\big(\operatorname{vert} P \setminus \{x\}\big).$$

It is evident that $\operatorname{vol} \triangle(x)$ is an integer multiple of $1/d!$.

Lemma 2.3. *For every* $x \in \operatorname{vert} Q_r$ $\operatorname{vol} \triangle(x) \ll r^{\frac{d-1}{2}}$ *and* $\big|\triangle(x) \cap \mathbb{Z}^d\big| \ll r^{\frac{d-1}{2}}$.

Proof. Set $P' := I\big(\operatorname{vert} P \setminus \{x\}\big)$ and let F be a *separating facet* of P' meaning that the hyperplane $\operatorname{aff} F$ strictly separates x and P'. This hyperplane cuts off a small cap C_F from rB^d whose width is less than $2\sqrt{d}$ by the previous lemma. Then the diameter of C_F is at most

$$2\sqrt{(2r - 2\sqrt{d}\,)\, 2\sqrt{d}} < 4d^{1/4}\sqrt{r}.$$

It follows that all such caps C_F are contained in a cap C, centered at $rx/|x|$, and of radius $4d^{1/4}\sqrt{r}$. Then $\triangle(x)$ is contained in C, and the volume of this cap is $\ll r^{\frac{d-1}{2}}$. The second statement follows from the fact that $\big|\triangle(x) \cap \mathbb{Z}^d\big|$ is at most the volume of the Minkowski sum of C and the unit cube. It is not hard to see that this volume is $\ll r^{\frac{d-1}{2}}$. □

3. A quick proof of Corollary 1.1

We are to construct many non-equivalent convex lattice polytopes of volume at most V (when V is large). Choose r so big that $\operatorname{vol} rB^d$ is slightly smaller than V and set $s = \lfloor r \rfloor$. Then Q_r has $\gg r^D$ vertices. Set $G = \{\pm se_1, \dots, \pm se_d\}$.

Here comes Arnol'd idea from [2]. For a subset W of $\operatorname{vert} Q_r \setminus G$ define $Q(W) = I(Q_r \setminus W)$. This is $2^{|\operatorname{vert} Q_r|-2d} \geqq \exp\left\{cV^{(d-1)/(d+1)}\right\}$ convex lattice polytopes (with a suitable $c > 0$, depending only on d). We show that at most $2^d d!$ of the $Q(W)$ are in the same equivalence class.

Assume the lattice preserving affine transformation T maps $Q(W)$ to $Q(W')$. T is of the form $T(x) = Ax + a$ where A is an integral matrix of determinant ± 1 and $a \in \mathbb{Z}^d$. We claim $|Ae_i| = 1$ for all $i \in [d]$. Assume $Ae_i = z \in \mathbb{Z}^d$, then either $|z| = 1$ or $|z| \geqq \sqrt{2}$. As $\pm se_i \in Q(W)$, $\left|T(\pm se_i)\right| \leqq r$. Squaring and expanding gives $(\pm sAe_i + a)^2 = s^2 z^2 \pm 2sz \cdot a + a^2 \leqq r^2$. Summing the two inequalities gives $s^2 z^2 + a^2 \leqq r^2$. Here $s = \lfloor r \rfloor \geqq 0.9r$, and if $z^2 \geqq 2$, we have $1.62r^2 + a^2 \leqq r^2$ which is impossible. So $|z| = 1$ and then $z = \pm e_j$ for some $j \in [d]$. Thus there is a permutation π of $[d]$ with $Ae_i = \pm e_{\pi(i)}$. As $x_i = \pm s$ are supporting hyperplanes to both $Q(W)$ and $Q(W')$, $a = 0$ follows. There are $2^d d!$ such lattice preserving affine transformations, so indeed the equivalence class of $Q(W)$ contains at most $2^d d!$ convex lattice polytopes of the form $Q(W')$. □

Remark. The same method works for the rotational paraboloid given by inequalities $x_1^2 + \dots + x_{d-1}^2 \leqq x_d \leqq r^2$ from Arnol'd paper [2]. Its integer convex hull, P_r, is a convex lattice polytope with $\omega_{d-1} r^{d-1}\big(1 + o(1)\big)$ vertices, and its volume is of order r^{d+1}. Deleting all subsets W of the vertices gives many, namely at least $\exp\left\{cr^{d-1}\right\}$, convex lattice polytopes of the form $I(P_r \setminus W)$, and every equivalence class contains at most $2^{d-1}(d-1)!$ of them.

4. Auxiliary results

We are going to use a beautiful result of Reizner, Schütt, Werner [8]. For a vertex x of a polytope $P \in \mathcal{P}$ we define $\triangle^*(x) = P \setminus \operatorname{conv}\left(\operatorname{vert} P \setminus \{x\}\right)$.

Theorem 4.1. *For every integer $d \geqq 2$ there are constants $b_0, b_1 > 0$ such that the following holds. For every $\varepsilon \in (0, 1/2)$ and for every $P \in \mathcal{P}$ with $f_0(P) \geqq b_0^d/\varepsilon$ there is a set $X \subset \operatorname{vert} P$ of size $|X| \geqq (1-2\varepsilon) f_0(P)$ such that for every $x \in X$*

$$\frac{\operatorname{vol} \triangle^*(x)}{\operatorname{vol} P} \leqq b_1\big(\varepsilon f_0(P)\big)^{-\frac{d+1}{d-1}}.$$

Note that, for a lattice polytope P, $\triangle(x) \subset \triangle^*(x)$ so the last inequality holds with $\triangle(x)$ in place of $\triangle^*(x)$.

The main building block of our construction is $K_r = \mathbb{R}^d_+ \cap rB^d$. The estimate (2.1) shows that $r^D \ll f_0(I(K_r)) \ll r^D$. Applying the above theorem to $P = I(K_r)$ with $\varepsilon = 0.24$, say, shows that at least 52 percent of the vertices of $I(K_r)$ satisfy

$$\operatorname{vol} \triangle(x) \leqq b_1 \left(\frac{1}{4}\big|\operatorname{vert} I(K_r)\big|\right)^{-\frac{d+1}{d-1}} \operatorname{vol} I(K_r) \ll 1.$$

This implies that for this set of vertices $\operatorname{vol} \triangle(x) \leqq \frac{b}{d!}$ where b is a positive integer that depends only on d. Let X be a subset of these vertices, excluding the origin (for reasons that will be clear later), with $|X| = \big\lfloor \frac{1}{2} f_0\big(I(K_r)\big) \big\rfloor$. So what we have now is that

$$\operatorname{vol} \triangle(x) \leqq \frac{b}{d!} \quad \text{for all} \quad x \in X. \tag{4.1}$$

The next lemma is fairly simple.

LEMMA 4.1. *If a segment $[u, v] \subset 2K_r$ contains more than $1.9r$ lattice points, then it is parallel with some e_i or with some $e_i - e_j$, $i \neq j$. In the latter case $\left|\frac{1}{2}(u + v)\right| \leqq 1.5r$.*

PROOF. Let z be the primitive vector in the direction of the segment $[u, v]$. Then $u - v = \lambda z$ with $\lambda > 1.9r$. Further,

$$\operatorname{diam} 2K_r = 2 \operatorname{diam} K_r = 2\sqrt{2}r \geqq |u - v| = \lambda|z| \geqq 1.9r|z|$$

implying that $|z| < \frac{2\sqrt{2}}{1.9} < 1.5$. Such an integer vector can have one or two coordinates equal to ± 1, the rest of the coordinates is zero. It is easy to check that the case $z = e_i + e_j$ cannot occur. Equally easy is to see that if $z = e_i - e_j$, then u is close to $2re_i$ and v is close to $2re_j$, and then the midpoint w of $[u, v]$ is close to the midpoint of $[2re_i, 2re_j]$ which is at distance $2r/\sqrt{2}$ from the origin. This implies $|w| < 1.5r$. We omit the straightforward details. $\square$

We need one more fact which is probably known. Let b be a fixed positive integer. Assume $k_1, \dots, k_m \in [b]$ and $\sum_1^m k_j = M$. For $W \subset [m]$ define $\sigma(W) = \sum_{j \in W} k_j$. We want to give an exponential in m lower bound on the number of sets $W \subset [m]$ with $\sigma(W) \in [\beta M - b, \beta M]$ where $\beta \in (0, 1/2)$. The interval $[\beta M - b, \beta M]$ contains b integers. Note that a shorter interval would not suffice in general, for instance when all $k_j = b$.

LEMMA 4.2. *For all positive integers b, m and for all $\beta \in (0, 1/2)$ the following holds. Given a sequence $k_1, \dots, k_m$ with all $k_j \in [b]$ and $\sum_1^m k_j = M$,* *the number of sets* $W \subset [m]$ *satisfying* $\sigma(W) \in [\beta M - b, \beta M]$ *is at least* $\beta^b 2^{\beta m}$.

PROOF. Fix $\beta \in (0, 1/2)$. The sets $P_i = \{ j \in [m] : k_j = i \}$ form a partition of $[m]$. Set $p_i = |P_i|$ and $q_i = \lfloor \beta p_i \rfloor$. We are going to choose q_i^* elements from P_i with $q_i \leqq q_i^* \leqq q_i + 1$ for all i so that $\sum_1^b i q_i^* \in [\beta M - b, \beta M]$. As $\sum_1^b i q_i \leqq \beta M \leqq \sum_1^b i(q_i + 1)$, and the difference of the upper and lower bounds here is $\binom{b}{2}$, there is such a choice of q_i^*. We fix such a choice.

The number of sets $W \subset [m]$ with exactly q_i^* elements from P_i is $\prod_1^b \binom{p_i}{q_i^*}$. Here $\binom{p_i}{q_i^*} \geqq \binom{p_i}{q_i}$ since $\beta < 1/2$, and $\binom{p_i}{q_i} \geqq \left(\frac{p_i}{q_i}\right)^{q_i}$. Moreover $\frac{p_i}{q_i} \geqq \frac{p_i}{\beta p_i} = \frac{1}{\beta}$. Thus

$$\prod_1^b \binom{p_i}{q_i^*} \geqq \left(\frac{1}{\beta}\right)^{\sum q_i} \geqq \left(\frac{1}{\beta}\right)^{\beta m - b} \geqq \beta^b \left(\frac{1}{\beta}\right)^{\beta m} > \beta^b 2^{\beta m}. \quad \square$$

5. The construction

The building block of the construction is the convex lattice polytope $I(K_r) = I(rB^d \cap \mathbb{R}_+^d)$. As r grows, more and more lattice points enter the ball rB^d and so $I(K_r)$, sometimes many of them with the same r. That is why we modify our construction a little. Order the lattice points in $\mathbb{R}_+^d$ as $x_0, x_1, x_2, \dots$ with the only condition that $|x_i| \leqq |x_j|$ for $i \leqq j$. Define $K^n = \operatorname{conv}\{x_0, x_1, \dots, x_n\}$.

Set $r = |x_n|$. Then K^n is close to K_r and $n = \omega_d r^d \big(1 + o(1)\big)$ and $\operatorname{vol} K^n = \omega_d r^d \big(1 + o(1)\big)$. Moreover, all the estimates and lemmas of Section 2 remain valid for K^n because no proof (not even in [4]) considers whether a particular lattice point is on the boundary of rB^d or not.

The function $n \to \operatorname{vol} I(K^n)$ is increasing, of order r^d, with jumps at least $1/d!$ and at most $O\big(r^{(d-1)/2}\big)$ in view of Lemma 2.3. The function $n \to f_0\big(I(K^n)\big)$ is of order r^D with jumps at most 1 and at least $-cr^{(d-1)/2}$ for a suitable $c > 0$ depending only on d, again by Lemma 2.3. Consequently for every large enough V there is n such that with $r = |x_n|$

$$0 \leqq 2^d \operatorname{vol} K^n - V - \frac{1}{5d!} f_0(K^n) \ll r^{(d-1)/2}.$$

We fix this n and the corresponding $r = |x_n|$ and define $Q = 2K^n$, which is a homothetic copy of K^n by blow-up factor 2 and center 0. Further, x is a vertex of Q iff $x/2$ is a vertex of $I(K^n)$. The estimate (2.1) shows that

$$r^D \ll f_0(Q) = f_0(K^n) \ll r^D.$$

For $x \in \operatorname{vert} Q$ define

$$\triangle(x) = \triangle_Q(x) = Q \setminus I(Q \setminus \{x\}).$$

$\triangle(x)$ is a translate of $\triangle_{K^n}(x/2)$ (by the vector $x/2$). This implies that for all $x \in \operatorname{vert} Q$

$$\frac{1}{d!} \leqq \operatorname{vol} \triangle(x) \ll r^{\frac{d-1}{2}}.$$

The advantage of the blow-up factor 2 in the definition of Q is that for distinct $x, y \in \operatorname{vert} Q$, $\triangle(x)$ and $\triangle(y)$ are internally disjoint, that is, $\operatorname{int} \triangle(x) \cap \operatorname{int} \triangle(y) = \emptyset$ when $x, y \in \operatorname{vert} Q$ are distinct.

We use next the Reizner–Schütt–Werner theorem in the form of (4.1): There is $X \subset \operatorname{vert} Q$, $|X| = \left\lfloor \frac{1}{2} f_0(Q) \right\rfloor$, and $0 \notin X$ such that $\operatorname{vol} \triangle(x) \leqq b/d!$ for all $x \in X$ where b is a positive integer depending only on d. Set $|X| = m$ and $M = \sum_{x \in X} \operatorname{vol} \triangle(x)$. Clearly $m/d! \leqq M \leqq bm/d!$.

Our target is to find many lattice polytopes contained in Q that have volume very close to, and slightly larger than, V. To this end we define $\mathcal{H}$ as the collection of all $W \subset X$ with

$$\operatorname{vol} \Big(Q \setminus \bigcup_{x \in W} \triangle(x) \Big) \in \Big[V, V + \frac{b}{d!} \Big],$$

or, what is the same, $\sum_{x \in W} \operatorname{vol} \triangle(x) \in [\operatorname{vol} Q - V - b/d!, \operatorname{vol} Q - V]$.

CLAIM 5.1. *There is $c > 0$, depending only on d such that $|\mathcal{H}| \geqq \exp \left\{ cV^{(d-1)/(d+1)} \right\}$.*

PROOF. We are going to use Lemma 4.2, this time not with integral k_j but with $\operatorname{vol} \triangle(x)$, $x \in X$ instead. These numbers are not integers but positive integer multiples of $1/d!$ which makes no difference. We define β via $\beta M = \operatorname{vol} Q - V$ and check, first, that $\beta < 1/2$.

As $(d-1)/2 < D = d(d-1)/(d+1)$ for all $d \geqq 2$, $r^{(d-1)/2} = o(r^D)$, and we have

$$\operatorname{vol} Q - V = \frac{1}{5d!} f_0(K^n) + O\big(r^{(d-1)/2}\big) = \frac{1}{5d!} f_0(K^n) \big(1 + o(1)\big).$$

On the other hand $M \geqq m/d! = \left\lfloor \frac{1}{2} f_0(K^n) \right\rfloor / d!$. Thus $\beta = (\operatorname{vol} Q - V)/M < 1/2$, indeed.

We show next that $\beta \geqq \frac{1}{3b}$. Just as before

$$\operatorname{vol} Q - V = \frac{1}{5d!} f_0(K^n) \big(1 + o(1)\big), \quad \text{and} \quad M \leqq bm/d! = b \left\lfloor \frac{1}{2} f_0(K^n) \right\rfloor /d!,$$

showing that $\beta \geqq \frac{1}{3b} > 0$ indeed.

An application of Lemma 4.2 shows that $|\mathcal{H}| \geqq \beta^b 2^{\beta m} \geqq (3b)^{-b} 2^{m/3b}$. We are done since b depends only on d and $m \gg r^D \gg V^{(d-1)/(d+1)}$. $\square$

Here comes the last step of the construction. Given $W \in \mathcal{H}$, let $t = t(W)$ be defined by

$$\mathrm{vol}\left(Q \setminus \bigcup_{x \in W} \triangle(x)\right) = V + \frac{t}{d!}.$$

Then $0 \leqq t \leqq b$. The simplex $S(t) = \mathrm{conv}\,\{0, te_1, e_2, \dots, e_d\}$ has volume $t/d!$. We assume r is large, much larger than b. For $W \in \mathcal{H}$ define

$$P(W) = \left(Q \setminus \bigcup_{x \in W} \triangle(x)\right) \setminus S(t).$$

We have now constructed the set $P(W)$ for every $W \in \mathcal{H}$. It is evident that each $P(W)$ is a convex lattice polytope of volume V.

We show finally that a positive fraction of these convex lattice polytopes are non-equivalent. Let $s = \lfloor r \rfloor$. It is clear that Q has d edges, namely $[0, 2se_i]$, $i \in [d]$, that contain $2s + 1$ lattice points. Some of these edges become shorter in $P(W)$, yet each $P(W)$ contains an edge $E_i \subset [0, 2se_i]$ with at least $2s - b \geqq 1.9r$ lattice points on it ($i \in [d]$).

Claim 5.2. *$P(W)$ has no edge containing $1.9r$ lattice points apart from $E_1, \dots, E_d$.*

Proof. If $[u, v]$ is such an edge, then its midpoint lies in $1.5rB^d$, by Lemma 4.1. In view of Lemma 2.2

$$2\left(r - 2\sqrt{d}\,\right) B^d \cap \mathbb{R}^d_+ \subset P(W) \cup L(t),$$

and so $[u, v]$ cannot be an edge. $\square$

Suppose now that $P(W)$ and $P(W')$ are equivalent ($W, W' \in \mathcal{H}$), and T is the lattice preserving affine transformation carrying $P(W)$ to $P(W')$. By the claim, T maps the edges $E_1, \dots, E_d$ of $P(W)$ to the edges $E'_1, \dots, E'_d$ of $P(W')$. Thus T must permute these edges. Moreover, $T(0) = 0$ follows from $\bigcap \mathrm{aff}\, E_i = \bigcap \mathrm{aff}\, E'_i = \{0\}$. Thus T is a lattice preserving linear transformation that permutes the elements of the basis $e_1, \dots, e_d$. There are exactly $d!$ such lattice preserving linear transformations.

This proves that there are at most $d!$ convex lattice polytopes of the form $P(W)$, $W \in \mathcal{H}$ that are equivalent. Consequently

$$\log N_d(V) \geqq \log\left(\frac{1}{d!}|\mathcal{H}|\right) \gg V^{(d-1)/(d+1)} - \log d! \gg V^{(d-1)/(d+1)}. \quad \square$$

6. Concluding remarks

There is a modification of this construction in which no two polytopes are equivalent, showing directly that $N_d(V) \geqq |\mathcal{H}|$. To describe it we define $G_1 = \{se_1\}$, $G_2 = \{se_2, (s-1)e_2\}$, ..., $G_d = \{se_d, \dots, (s-d-1)e_d\}$. For each $W \in \mathcal{H}$ we consider the convex lattice polytope

$$P^*(W) = I\Big(P(W) \setminus \bigcup_1^d G_i\Big).$$

We claim that no two of these convex lattice polytopes are equivalent. Suppose T is a lattice preserving affine transformation carrying $P^*(W)$ to $P^*(W')$. Again, $E_i^* = I(E_i \setminus G_i)$ is an edge of $P^*(W)$, and the same way as before, $T(0) = 0$ and T must permute the e_i. But now the last point (away from the origin) of the edge E_i^* is $(s-i)e_i$ and so T must carry E_i^* to $E_i'^*$ for all $i \in [d]$. Thus T is the identity, and then $W = W'$.

We mention further that Arnol'd's suggestion, the paraboloid $x_1^2 + \dots + x_{d-1}^2 \leqq x_d \leqq A$, would work in a similar way. Also, an analogous construction applies to centrally symmetric (or, what is the same in this context, 0-symmetric) convex lattice polytopes. Define $M_d(V)$ as the number of equivalence classes of 0-symmetric convex lattice polytopes. In this case, of course, V is a positive integer multiple of $2/d!$

THEOREM 6.1. $V^{(d-1)/(d+1)} \ll \log M_d(V) \ll V^{(d-1)/(d+1)}$.

SKETCH OF PROOF. The upper bound follows from $M_d(V) \leqq N_d(V)$. For the lower bound let E be the ellipsoid

$$x_1^2 + \dots + x_d^2 - \left(\frac{1}{d} - \frac{2}{d^3}\right)(x_1 + \dots + x_d)^2 \leqq \frac{2}{d}.$$

The longest axis of E is in direction $e = (1, 1, \dots, 1)$, and is of length $\sqrt{d}$. All other axes are of length $\sqrt{2/d}$. Let K be the intersection of E with the cube $\{x \in \mathbb{R}^d : -1 \leqq x_i \leqq 1, i \in [d]\}$. The integer convex hull of rK is the starting point of the construction. Theorem 5 of [4] shows that $r^D \ll f_0(I(rK)) \ll r^D$. Set $Q = 2I(rK)$. For an 0-symmetric subset W of $\operatorname{vert} Q$, $I(Q \setminus W)$ is an 0-symmetric convex lattice polytope and $r^d \ll \operatorname{vol} Q \ll r^d$. Choosing r carefully, and using Lemma 4.2, one can show again that exponentially many of them have volume between V and $V + b$. Each such $P(W)$ near the vertices $\pm\lfloor r \rfloor e$ looks like a coordinate octant. To reach exactly V volume one should delete copies of a suitable $S(t)$ at these vertices. □

Acknowledgements. Support from ERC Advanced Research Grant No. 267165, and from Hungarian National Research Grants K 83767 and NK 78439 is acknowledged with thanks.

References

[1] G. E. Andrews, A lower bound for the volumes of strictly convex bodies with many boundary points, *Trans. Amer. Math. Soc.*, **106** (1993), 270–279.
[2] V. I. Arnol'd, Statistics of integral convex polytopes, *Funk. Anal. Pril.*, **14** (1980), 1–3 (in Russian). English translation, *Funct. Anal. Appl.*, **14** (1980), 79–84.
[3] I. Bárány, Random points and lattice points in convex bodies, *Bull. Amer. Math. Soc.*, **45** (2008), 339–365.
[4] I. Bárány and D. G. Larman, The convex hull of the integer points in a large ball, *Math. Annalen*, **312** (1998), 167–181.
[5] I. Bárány and J. Pach, On the number of convex lattice polygons, *Combinatorics, Probability, and Computation*, **1** (1992), 295–302.
[6] I. Bárány and A. Vershik, On the number of convex lattice polytopes, **24** (2004), 171–185.
[7] S. Konyagin and S. V. Sevastyanov, Estimation of the number of vertices of a convex integral polyhedron in terms of its volume, *Funk. Anal. Pril.*, **18** (1984), 13–15 (in Russian). English translation, *Funct. Anal. Appl.*, **18** (1984), 11–13.
[8] Sh. Reizner, C. Schütt and E. Werner, Dropping a vertex or a facet from a convex polytope, *Forum Mathematicum*, **13** (2001), 359–378.
[9] C. Zong, On Arnold's problem on the classifications of convex lattice polytopes, manuscript (2011), arXiv:1107.2966.