ON ARNOLD'S PROBLEM ON THE CLASSIFICATIONS OF CONVEX LATTICE POLYTOPES

CHUANMING ZONG[1]

Abstract. In 1980, V.I. Arnold studied the classification problem for convex lattice polygons of given area. Since then this problem and its analogues have been studied by Bárány, Pach, Vershik, Liu, Zong and others. Upper bounds for the numbers of non-equivalent d-dimensional convex lattice polytopes of given volume or cardinality have been achieved. In this paper, by introducing and studying the unimodular groups acting on convex lattice polytopes, we obtain lower bounds for the number of non-equivalent d-dimensional convex lattice polytopes of bounded volume or given cardinality, which are essentially tight.

1. INTRODUCTION

Let $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d\}$ be an orthonormal basis of the d-dimensional Euclidean space $\mathbb{E}^d$. A convex lattice polytope in $\mathbb{E}^d$ is the convex hull of a finite subset of the integral lattice $\mathbb{Z}^d$. As usual, let P denote a d-dimensional convex lattice polytope, let $v(P)$ denote the volume of P, let $int(P)$ denote the interior of P, and let $|P|$ denote the cardinality of $P \cap \mathbb{Z}^d$. For general references on polytopes and lattice polytopes, we refer to Bárány [2], Barvinok [6], Gruber [7], Ziegler [12] and Zong [13].

Let P_1 and P_2 be d-dimensional convex lattice polytopes. If there is a unimodular transformation σ ($\mathbb{Z}^d$-preserving linear transformation) satisfying

$$P_2 = \sigma(P_1),$$

then we say P_1 and P_2 are equivalent. For convenience, we write $P_1 \sim P_2$ for short. It is easy to see that, if $P_1 \sim P_2$ and $P_2 \sim P_3$, then we have $P_1 \sim P_3$. In addition, if $P_1 \sim P_2$, then we have

$$v(P_1) = v(P_2)$$

and

$$|P_1| = |P_2|.$$

Clearly, the equivalence relation $\sim$ divides convex lattice polytopes into different classes. Using triangulations, it can be easily shown that

$$d! \cdot v(P) \in \mathbb{Z}$$

holds for any d-dimensional convex lattice polytope P. Let $v(d, m)$ denote the number of different classes of the d-dimensional convex lattice polytopes P with $v(P) = m/d!$,

[1] 2010 Mathematics Subject Classification. 52B20, 52C07, 20H05

This work is supported by 973 Program 2011CB302400, the National Natural Science Foundation of China (Grant No. 11071003) and the Chang Jiang Scholars Program of China.

where both d and m are positive integers. In 1980, Arnold [1] studied the values of $v(2,m)$ and proved

$$m^{\frac{1}{3}} \ll \log v(2,m) \ll m^{\frac{1}{3}} \log m.$$

Remark 1. In this paper $f(d,m) \ll g(d,m)$ means that, for fixed positive integer d,

$$f(d,m) \leq c_d \cdot g(d,m)$$

holds for all positive integers m with a suitable constant c_d.

In 1992, Bárány and Pach [4] improved Arnold's upper bound to

$$\log v(2,m) \ll m^{\frac{1}{3}}; \tag{1}$$

Bárány and Vershik [5] generalized (1) to d dimensions by proving

$$\log v(d,m) \ll m^{\frac{d-1}{d+1}}. \tag{2}$$

In [5], the authors attributed

$$\log v(d,m) \gg m^{\frac{d-1}{d+1}} \tag{3}$$

and

$$\log v(d,m) \ll m^{\frac{d-1}{d+1}} \log m$$

to Arnold [1] and Konyagin and Savastyanov [8], respectively. In fact, neither of them contains such proofs. In particular, a proof for (3) seems non-trivial. Therefore, to determine the order of magnitude of $\log v(d,m)$ for fixed d and large m is still a basic open problem.

For convenience, we write

$$g(d,m) = \sum_{j=1}^{m} v(d,j).$$

According to Bárány [2] and [3], Arnold posed the problem to investigate $g(d,m)$ and to determine the order of magnitude of $\log g(d,m)$, and proved that

$$\log g(d,m) \gg m^{\frac{d-1}{d+1}}. \tag{4}$$

In fact, a rigorous proof for this result is missing.

Let $v^*(d,m)$ denote the number of different classes of the d-dimensional centrally symmetric convex lattice polytopes P with $v(P) = m/d!$, let $\kappa(d,w)$ denote the number of different classes of d-dimensional convex lattice polytopes P with $|P| = w$, let $\kappa^*(d,w)$ denote the number of different classes of d-dimensional centrally symmetric convex lattice polytopes P with $|P| = w$, and let $\kappa'(d,w)$ denote the number of different classes of d-dimensional convex lattice polytopes P with $|P| = w$ and $int(P) \cap \mathbb{Z}^d \neq \emptyset$. Then we have $v^*(d,m) = 0$ whenever m is odd and $\kappa^*(d,w) = 0$ if w is even. Therefore in this paper we assume that the m in $v^*(d,m)$ is even and the w in $\kappa^*(d,w)$ is odd.

Remark 2. As usual, in this paper centrally symmetric convex lattice polytopes are those centered at lattice points. In this sense, the unit cube $\{\mathbf{x} \in \mathbb{E}^d : \ 0 \leq x_i \leq 1\}$ is not a centrally symmetric convex lattice polytope, though it is a convex lattice polytope and is centrally symmetric.

Recently, Liu and Zong [10] studies Arnold's problem for the centrally symmetric lattice polygons and the classification problem for convex lattice polytopes of given cardinality by proving

$$m^{\frac{1}{3}} \ll \log v^*(2, m) \ll m^{\frac{1}{3}},$$

$$w^{\frac{1}{3}} \ll \log \kappa(2, w) \ll w^{\frac{1}{3}},$$

$$w^{\frac{1}{3}} \ll \log \kappa^*(2, w) \ll w^{\frac{1}{3}},$$

$$\kappa(d, w) = \infty, \quad if\ w \geq d+1 \geq 4,$$

$$\log \kappa'(d, w) \ll w^{\frac{d-1}{d+1}} \tag{5}$$

and

$$\log \kappa^*(d, w) \ll w^{\frac{d-1}{d+1}}. \tag{6}$$

In Section 2 of this paper we introduce and study unimodular groups acting on convex lattice polytopes. In particular, the orders of these groups are estimated. In Sections 3 and 4, by applying the results obtained in Section 2, we prove the following two theorems:

Theorem 4. *Let $g(d, m)$ denote the number of different classes of the d-dimensional convex lattice polytopes P with $v(P) \leq m/d!$, then*

$$\log g(d, m) \gg m^{\frac{d-1}{d+1}}.$$

Theorem 5. *Let $\kappa^*(d, w)$ denote the number of different classes of d-dimensional centrally symmetric convex lattice polytopes P with $|P| = w$, then*

$$\log \kappa^*(d, w) \gg w^{\frac{d-1}{d+1}}.$$

Theorem 4 confirms (4), which was predicted by Arnold and Bárány. It and (2) together yields the following result.

Theorem A. *Let $g(d, m)$ denote the number of different classes of the d-dimensional convex lattice polytopes P with $v(P) \leq m/d!$, then*

$$m^{\frac{d-1}{d+1}} \ll \log g(d, m) \ll m^{\frac{d-1}{d+1}}.$$

Theorem 5, (5) and (6) together produces the following consequences:

Theorem B. *Let $\kappa^*(d, w)$ denote the number of different classes of d-dimensional centrally symmetric convex lattice polytopes P with $|P| = w$, then*

$$w^{\frac{d-1}{d+1}} \ll \log \kappa^*(d, w) \ll w^{\frac{d-1}{d+1}}.$$

Theorem C. *Let $\kappa'(d,w)$ denote the number of different classes of d-dimensional convex lattice polytopes P with $|P|=w$ and $\mathrm{int}(P)\cap\mathbb{Z}^d\neq\emptyset$, then*

$$w^{\frac{d-1}{d+1}} \ll \log \kappa'(d,w) \ll w^{\frac{d-1}{d+1}}.$$

2. UNIMODULAR GROUPS OF CONVEX LATTICE POLYTOPES

In this section we introduce and study unimodular groups acting on convex lattice polytopes. Several interesting results are proved. In particular, Theorem 3 will be essential for our proofs of both Theorem 4 and Theorem 5.

As usual, a unimodular transformation $\sigma(\mathbf{x})$ of $\mathbb{E}^d$ is a $\mathbb{Z}^d$-preserving linear transformation, i.e.,

$$\sigma(\mathbf{x}) = \mathbf{x}U + \mathbf{v},$$

where U is a $d\times d$ integral matrix satisfying $|det(U)|=1$ and $\mathbf{v}$ is an integral vector. In particular, if U also satisfies $UU'=I$, where U' is the transpose of U and I is the $d\times d$ unit matrix, we call $\sigma(\mathbf{x})$ an orthogonal unimodular transformation. It is known in linear algebra that an orthogonal unimodular keeps the Euclidean distances unchanged.

Let σ_1 and σ_2 be two unimodular transformations in $\mathbb{E}^d$. It is known in linear algebra that both $\sigma_1\cdot\sigma_2$ and σ_1^{-1} are unimodular transformations. Therefore, all unimodular transformations in $\mathbb{E}^d$ form a multiplicative group. We denote it by $\mathbb{G}_d$. Similarly, all orthogonal unimodular transformations in $\mathbb{E}^d$ form a subgroup of $\mathbb{G}_d$. We denote it by $\mathbb{G}'_d$.

Let P be a convex lattice polytope in $\mathbb{E}^d$, and let $\mathbb{P}_d$ denote the family of all d-dimensional convex lattice polytopes. We define

$$\sigma(P)=\{\sigma(\mathbf{x}):\ \mathbf{x}\in P\}.$$

Clearly, $\sigma(P)$ is a convex lattice polytope as well. Then we define

$$G(P)=\{\sigma\in\mathbb{G}_d:\ \sigma(P)=P\}$$

and

$$G'(P)=\{\sigma\in\mathbb{G}'_d:\ \sigma(P)=P\}.$$

It is easy to check that both $G(P)$ and $G'(P)$ are finite subgroups of $\mathbb{G}_d$, and $G'(P)$ is a subgroup of $G(P)$. We call $G(P)$ the *unimodular group* of P and call $G'(P)$ the *orthogonal unimodular group* of P.

Theorem 1. *If $P\in\mathbb{P}_d$ and $\sigma\in\mathbb{G}_d$, then we have*

$$G(\sigma(P))=\sigma G(P)\sigma^{-1}.$$

If $\tau\in\mathbb{G}'_d$, then we have

$$G'(\tau(P))=\tau G'(P)\tau^{-1}.$$

Proof. If $\mu\in G(P)$, then we have

$$\mu(P)=P,$$

$$\sigma\mu\sigma^{-1}(\sigma(P)) = \sigma\mu(P) = \sigma(P)$$

and therefore

$$\sigma G(P)\sigma^{-1} \subseteq G(\sigma(P)). \tag{7}$$

Replacing P and σ by $\sigma(P)$ and σ^{-1} respectively in (7) and noting

$$P = \sigma^{-1}\sigma(P),$$

we get

$$\sigma^{-1}G(\sigma(P))\sigma \subseteq G(P). \tag{8}$$

Combining (7) and (8) we obtain

$$G(\sigma(P)) \subseteq \sigma G(P)\sigma^{-1} \subseteq G(\sigma(P))$$

and

$$G(\sigma(P)) = \sigma G(P)\sigma^{-1}.$$

The orthogonal case can be proved by similar arguments. □

Theorem 2. *Let O_d denote the multiplicative group of orthogonal unimodular transformations of $\mathbb{E}^d$ which keep the origin fixed. Then, we have*

$$|O_d| = 2^d \cdot d!.$$

Proof. Assume that

$$\tau(\mathbf{x}) = \mathbf{x}U + \mathbf{v}$$

is a unimodular transformation of $\mathbb{E}^d$. If it keeps the origin fixed, we get $\mathbf{v} = \mathbf{o}$. If it is orthogonal, we have

$$UU' = I,$$

where I is the $d \times d$ unit matrix, and therefore

$$\sum_{k=1}^{d} u_{ik}u_{jk} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Then, by the assumption that u_{ij} are integers we get

$$u_{ij} \in \{-1, 0, 1\},$$

$$\sum_{j=1}^{d} |u_{ij}| = 1, \quad i = 1, 2, \ldots, d$$

and

$$\sum_{i=1}^{d} |u_{ij}| = 1, \quad j = 1, 2, \ldots, d.$$

In other words, each row (column) of U has exactly one non-zero element, which is either 1 or -1. On the other hand, any matrix of this type is orthogonal unimodular. Then, by computing the number of such matrices it is easy to conclude

$$|O_d| = 2^d \cdot d!.$$

The theorem is proved. $\square$

Corollary 1. *For any d-dimensional centrally symmetric convex lattice polytope P, $|G'(P)|$ is a divisor of $2^d \cdot d!$.*

Proof. Assume that P is centered at a lattice point $\mathbf{u}$. In $\mathbb{E}^d$ we define

$$\tau(\mathbf{x}) = \mathbf{x} - \mathbf{u}.$$

It follows by Theorem 1 that

$$|G'(P)| = |G'(\tau(P))|.$$

On the other hand, $\tau(P)$ is centered at the origin $\mathbf{o}$, $G'(\tau(P))$ is a subgroup of O_d and therefore $|G'(\tau(P))|$ is a divisor of $2^d \cdot d!$. The assertion is proved. $\square$

Let m be a positive integer and let ρ be a real number satisfying $1 \leq \rho \leq \infty$. We define

$$P_{d,m,\rho} = \mathrm{conv}\left\{ \mathbf{z} \in \mathbb{Z}^d : \sum_{i=1}^{d} |z_i|^\rho \leq m^\rho \right\}.$$

One can easily verify that $P_{d,m,\rho}$ is a d-dimensional centrally symmetric convex lattice polytope. In particular, $P_{d,m,1}$ is a lattice cross-polytope, $P_{d,m,2}$ is a lattice ball, and $P_{d,m,\infty}$ is a lattice cube.

Theorem 3. *When d and m are positive integers and ρ is a positive number satisfying $1 \leq \rho \leq \infty$, we have*

$$G\left(P_{d,m,\rho}\right) = G'\left(P_{d,m,\rho}\right) = O_d$$

and

$$\left|G\left(P_{d,m,\rho}\right)\right| = \left|G'\left(P_{d,m,\rho}\right)\right| = 2^d \cdot d!.$$

Proof. First of all, since $P_{d,m,\rho}$ is centrally symmetric and centered at the origin, we have

$$\sigma(\mathbf{o}) = \mathbf{o} \tag{9}$$

for all $\sigma \in G(P_{d,m,\rho})$.

Let $\mathbf{v}$ be a primitive integral vector in $\mathbb{Z}^d$ and let P be a centrally symmetric convex lattice polytope in $\mathbb{E}^d$. We define

$$L(P, \mathbf{v}) = \{z\mathbf{v} : z \in \mathbb{Z}\} \cap P$$

and

$$\ell(P) = \max_{\mathbf{v}}\{|L(P, \mathbf{v})|\},$$

where the maximum is over all primitive integral vectors in $\mathbb{Z}^d$. Recall that $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d\}$ is an orthonormal basis of $\mathbb{E}^d$. We consider two cases as following:

Case 1. $\rho < \infty$. Notice that

$$\sum_{i=1}^{d} |mv_i|^\rho = m^\rho \sum_{i=1}^{d} |v_i|^\rho,$$

it can be easily deduce that

$$\ell(P_{d,m,\rho}) = 2m + 1$$

and

$$|L(P_{d,m,\rho}, \mathbf{v})| = 2m + 1$$

holds if and only if $\mathbf{v} = \pm\mathbf{e}_i$ for some index i. Thus, for any $\sigma \in G(P_{d,m,\rho})$, we have

$$\{\sigma(\mathbf{e}_1), \sigma(\mathbf{e}_2), \ldots, \sigma(\mathbf{e}_d)\} \subset \{\pm\mathbf{e}_1, \pm\mathbf{e}_2, \ldots, \pm\mathbf{e}_d\}. \tag{10}$$

Case 2. $\rho = \infty$. In this case $P_{d,m,\infty}$ is a d-dimensional cube. It has $2d$ facets $\pm F_1$, $\pm F_2$, …, $\pm F_d$, each is a $(d-1)$-dimensional cube. The centers of the facets are $\pm m\mathbf{e}_1$, $\pm m\mathbf{e}_2$, …, $\pm m\mathbf{e}_d$. If $\sigma \in G(P_{d,m,\infty})$, we have

$$\{\sigma(F_1), \sigma(F_2), \ldots, \sigma(F_d)\} \subset \{\pm F_1, \pm F_2, \ldots, \pm F_d\},$$

$$\{\sigma(m\mathbf{e}_1), \sigma(m\mathbf{e}_2), \ldots, \sigma(m\mathbf{e}_d)\} \subset \{\pm m\mathbf{e}_1, \pm m\mathbf{e}_2, \ldots, \pm m\mathbf{e}_d\}$$

and therefore

$$\{\sigma(\mathbf{e}_1), \sigma(\mathbf{e}_2), \ldots, \sigma(\mathbf{e}_d)\} \subset \{\pm\mathbf{e}_1, \pm\mathbf{e}_2, \ldots, \pm\mathbf{e}_d\}. \tag{11}$$

Assume that the unimodular transformation σ is defined by

$$\sigma(\mathbf{x}) = \mathbf{x}U + \mathbf{b}.$$

It follows by (9) that $\mathbf{b} = \mathbf{o}$. In both cases, since U is nonsingular, by (10) and (11) we get

$$\sum_{j=1}^{d} |u_{ij}| = 1, \quad i = 1, 2, \ldots, d$$

and

$$\sum_{i=1}^{d} |u_{ij}| = 1, \quad j = 1, 2, \ldots, d.$$

Thus, we obtain

$$G(P_{d,m,\rho}) \subseteq O_d. \tag{12}$$

On the other hand, it is easy to verify that

$$O_d \subseteq G'(P_{d,m,\rho}). \tag{13}$$

As a conclusion of (12) and (13) we get

$$O_d \subseteq G'(P_{d,m,\rho}) \subseteq G(P_{d,m,\rho}) \subseteq O_d$$

and finally

$$G(P_{d,m,\rho}) = G'(P_{d,m,\rho}) = O_d.$$

The second assertion of the theorem follows from Theorem 2. The theorem is proved. □

Remark 3. Let S_d denote the d-dimensional lattice simplex with vertices $\mathbf{e}_1$, $\mathbf{e}_2$, …, $\mathbf{e}_d$ and $\mathbf{o}$. Then we have

$$|G'(S_d)| = d!$$

and

$$|G(S_d)| = (d+1)!.$$

We end this section with the following conjecture:

Conjecture 1. *For any d-dimensional convex lattice polytope P, we have*

$$|G(P)| \leq 2^d \cdot d!.$$

3. PROOF OF THEOREM 4

In this section, applying results about unimodular groups proved in Section 2, we study Arnold's problem and prove Theorem 4.

Proof of Theorem 4. First, for a positive integer r we define (see Figure 1)

$$K_{d,r} = \left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d \geq 0, \ \sum_{i=1}^{d-1} x_i^2 + x_d \leq r^2 \right\}.$$

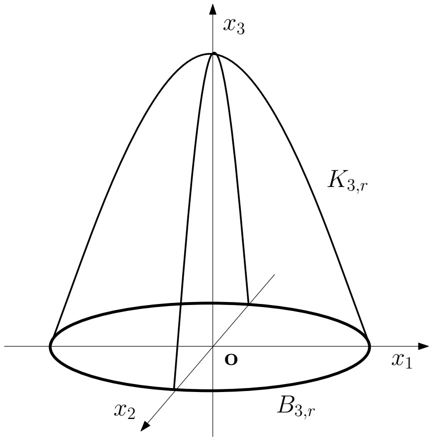

Figure 1

Clearly $K_{d,r}$ is a rotation body of a two-dimensional domain

$$D = \left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d \geq 0, \ x_1^2 \leq r^2 - x_d, \ x_j = 0 \right\}$$

around the x_d axis. Its base is a $(d-1)$-dimensional ball defined by

$$B_{d,r} = \left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d = 0, \ \sum_{i=1}^{d-1} x_i^2 \leq r^2 \right\}.$$

Therefore $K_{d,r}$ is strictly convex, except at its base $B_{d,r}$.

Now, we define

$$P_{d,r} = \mathrm{conv}\left\{ K_{d,r} \cap \mathbb{Z}^d \right\}$$

and define $V_{d,r}$ to be the set of the vertices $\mathbf{v}$ of $P_{d,r}$ satisfying $v_d \neq 0$ and $v_d \neq r^2$. For any point $\mathbf{z} \in B_{d,r} \cap \mathbb{Z}^d$, writing

$$y = \sum_{i=1}^{d-1} z_i^2,$$

the corresponding point $(z_1, z_2, \ldots, z_{d-1}, r^2 - y)$ is on the boundary of $K_{d,r}$ and therefore it is a vertex of $P_{d,r}$. Thus, we have

$$|V_{d,r}| \geq \left| \mathrm{int}(B_{d,r}) \cap \mathbb{Z}^d \right| - 1 \sim \frac{\pi^{\frac{d-1}{2}}}{\Gamma(\frac{d+1}{2})} \cdot r^{d-1} \gg r^{d-1}, \tag{14}$$

where $\Gamma(x)$ is the gamma function.

By deleting i vertices in $V_{d,r}$ from $P_{d,r}$ and considering the convex hulls of the remaining lattice points we get $\binom{|V_{d,r}|}{i}$ different convex lattice polytopes. Taking i from 0 to $|V_{d,r}|$, we obtain

$$\sum_{i=0}^{|V_{d,r}|} \binom{|V_{d,r}|}{i} = 2^{|V_{d,r}|}$$

different convex lattice polytopes. For convenience, we enumerate them as P_1, P_2, $\ldots$, $P_{2^{|V_{d,r}|}}$ and denote the whole family by $\mathcal{F}$.

Let $D_{d,r}$ denote the cylinder defined by

$$\left\{ \mathbf{x} \in \mathbb{E}^d : \ \sum_{i=1}^{d-1} x_i^2 \leq r^2, \ 0 \leq x_d \leq r^2 \right\}.$$

For all $P_i \in \mathcal{F}$ we have

$$v(P_i) \leq v(D_{d,r}) = v(B_{d,r}) \cdot r^2 \leq f(d) \cdot r^{d+1}, \tag{15}$$

where $f(d)$ is a positive constant depends only on d.

Recalling the notions of $L(P, \mathbf{v})$ and $\ell(P)$ defined in the proof of Theorem 3, for all $P_i \in \mathcal{F}$ we have

$$\ell(P_i) = r^2 + 1,$$

and

$$L(P_i, \mathbf{v}) = r^2 + 1$$

holds if and only if $\mathbf{v} = \mathbf{e}_d$. Therefore, if $\sigma(P_i) = P_j$ holds for some unimodular transformation σ, we can deduce that

$$\sigma(\mathbf{o}) = \mathbf{o}, \quad \sigma(\mathbf{e}_d) = \mathbf{e}_d,$$

$$\sigma\left(B_{d,r} \cap \mathbb{Z}^d\right) = B_{d,r} \cap \mathbb{Z}^d$$

and hence

$$\sigma \in G\left(\mathrm{conv}\left\{B_{d,r} \cap \mathbb{Z}^d\right\}\right) = G(P_{d-1,r,2}).$$

Let $h(d,r)$ denote the number of the non-equivalent lattice polytopes among $\{P_1, P_2, \ldots, P_{2^{|V_{d,r}|}}\}$, by the $\rho = 2$ case of Theorem 3 we get

$$h(d,r) \geq \frac{2^{|V_{d,r}|}}{|G(P_{d-1,r,2})|} \gg 2^{|V_{d,r}|}. \tag{16}$$

Taking

$$r = \left\lfloor \left(\frac{m}{f(d)}\right)^{\frac{1}{d+1}} \right\rfloor, \tag{17}$$

by (15) we get

$$v(P_i) \leq f(d) \cdot r^{d+1} \leq m$$

and therefore

$$g(d,m) \geq h\left(d,r\right). \tag{18}$$

Then, by (18), (16), (14) and (17) we obtain

$$\log g(d,m) \geq \log h\left(d,r\right) \gg |V_{d,r}| \gg r^{d-1} = \left\lfloor \left(\frac{m}{f(d)}\right)^{\frac{1}{d+1}} \right\rfloor^{d-1} \gg m^{\frac{d-1}{d+1}}.$$

Theorem 4 is proved. □

Remark 4. At the end of [1], Arnold made a remark that "In $\mathbb{Z}^d$, 1/3 is probably replaced by $(d-1)/(d+1)$. Proof of the lower bound: let $x_1^2 + \ldots + x_{d-1}^2 \leq x_d \leq A$." This hint is useful for our construction. However, up to now, we have not been able to prove

$$\log v(d,m) \gg m^{\frac{d-1}{d+1}}.$$

Remark 5. By a similar method, for the centrally symmetric case we can also prove

$$\log\left(\sum_{i=1}^{m} v^*(d,m)\right) \gg m^{\frac{d-1}{d+1}}.$$

4. PROOF OF THEOREM 5

In this section we study the classification problem for convex lattice polytopes of given cardinality. In particular, Theorem 5 is proved.

First, we recall the definitions

$$K_{d,r} = \left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d \geq 0, \ \sum_{i=1}^{d-1} x_i^2 + x_d \leq r^2 \right\}$$

and

$$B_{d,r} = \left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d = 0, \ \sum_{i=1}^{d-1} x_i^2 \leq r^2 \right\}.$$

It is easy to compute that

$$v(K_{d,r}) = \int_0^{r^2} \frac{\pi^{\frac{d-1}{2}}}{\Gamma(\frac{d+1}{2})} \cdot (r^2 - x)^{\frac{d-1}{2}} dx = c_1(d) \cdot r^{d+1}, \tag{19}$$

where

$$c_1(d) = \frac{\pi^{\frac{d-1}{2}}}{\Gamma(\frac{d+3}{2})}.$$

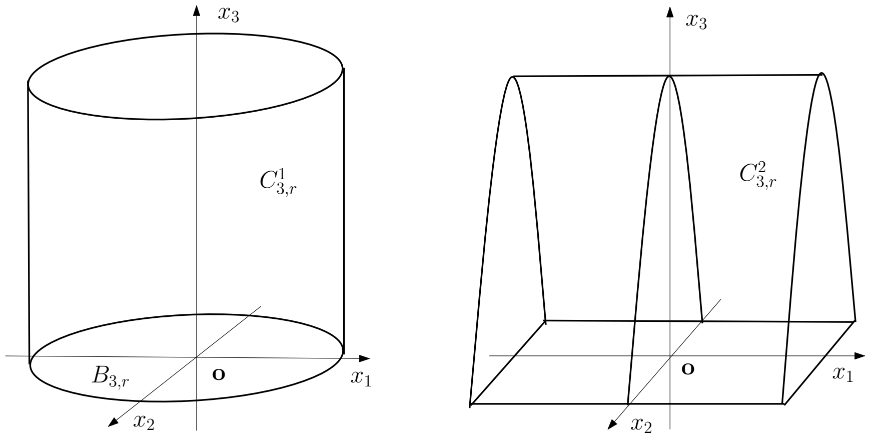

Figure 2

Next, we define

$$C^1_{d,r} = \left\{ \mathbf{x} \in \mathbb{E}^d : \ \sum_{i=1}^{d-1} x_i^2 \leq r^2 \right\},$$

$$C^2_{d,r} = \left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d \geq 0, \ \sum_{i=2}^{d-1} x_i^2 + x_d \leq r^2 \right\}$$

and their intersection

$$C_{d,r} = C^1_{d,r} \cap C^2_{d,r}.$$

In fact, $C^1_{d,r}$ is an infinite cylinder over a base $B_{d,r}$ and $C^2_{d,r}$ is an infinite cylinder over a base

$$\left\{ \mathbf{x} \in \mathbb{E}^d : \ x_d \geq 0, \ x_1 = 0, \ \sum_{i=2}^{d-1} x_i^2 + x_d \leq r^2 \right\},$$

as shown in Figure 2.

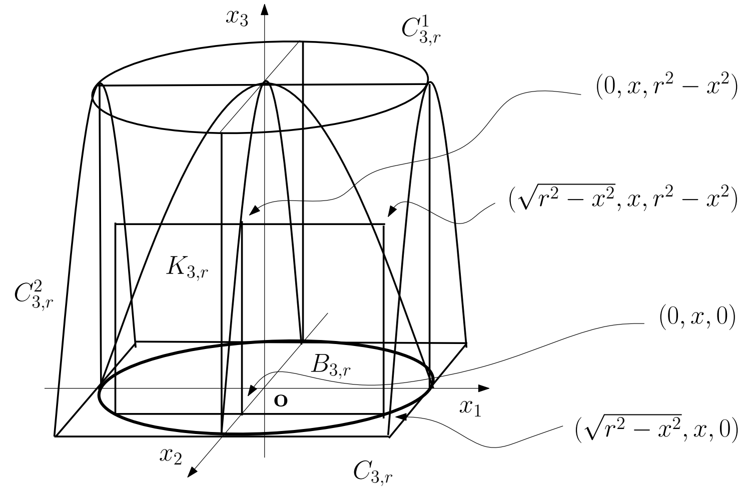

Figure 3

Note that (as illustrated in Figure 3), if

$$x^2 = \sum_{i=2}^{d-1} x_i^2 \tag{20}$$

and

$$(0, x_2, x_3, \ldots, x_{d-1}, 0) \in C_{d,r}, \tag{21}$$

then we have

$$(x_1, x_2, \ldots, x_{d-1}, x_d) \in C_{d,r}$$

provided

$$|x_1| \le \sqrt{r^2 - x^2}$$

and

$$0 \le x_d \le r^2 - x^2.$$

In fact, all the points satisfying both (20) and (21) together form a $(d-2)$-dimensional sphere of radius x which has area measure

$$\frac{(d-2)\pi^{\frac{d-2}{2}}}{\Gamma(\frac{d}{2})} \cdot x^{d-3}.$$

Thus, we get

$$\begin{aligned} v(C_{d,r}) &= \int_0^r \frac{2(d-2)\pi^{\frac{d-2}{2}}}{\Gamma(\frac{d}{2})} \cdot x^{d-3}(r^2 - x^2)^{\frac{3}{2}} dx \\ &= \frac{2(d-2)\pi^{\frac{d-2}{2}}}{\Gamma(\frac{d}{2})} \cdot r^{d+1} \int_0^{\frac{\pi}{2}} \sin^{d-3}\theta \cos^4\theta d\theta \end{aligned}$$

$$\begin{aligned} &= \frac{2(d-2)\pi^{\frac{d-2}{2}}}{\Gamma(\frac{d}{2})}\cdot r^{d+1}\int_0^{\frac{\pi}{2}}\left(\sin^{d-3}\theta-2\sin^{d-1}\theta+\sin^{d+1}\theta\right)d\theta \\ &= c_2(d)\cdot r^{d+1}, \end{aligned} \tag{22}$$

where

$$c_2(d)=\begin{cases} \frac{6(d-2)\pi^{\frac{d-2}{2}}}{(d^2-1)\Gamma(\frac{d}{2})}\cdot\frac{d-4}{d-3}\cdot\frac{d-6}{d-5}\cdots\frac{1}{2}\cdot\frac{\pi}{2} & \text{if } d \text{ is odd;}\\ \frac{6(d-2)\pi^{\frac{d-2}{2}}}{(d^2-1)\Gamma(\frac{d}{2})}\cdot\frac{d-4}{d-3}\cdot\frac{d-6}{d-5}\cdots\frac{1}{2} & \text{if } d \text{ is even.}\end{cases}$$

It follows by $K_{d,r}\subset C_{d,r}$ that

$$c_1(d)<c_2(d). \tag{23}$$

Next, we define

$$Q_{d,r}=\left(\mathrm{int}\left(C^1_{d,r}\right)\cap C^2_{d,r}\right)\cup B_{d,r}, \tag{24}$$

$$H_{d,r}=\mathrm{conv}\left\{\mathbf{z}\in Q_{d,r}\cap\mathbb{Z}^d:\,z_1\le 0\right\} \tag{25}$$

and

$$H'_{d,r}=\mathrm{conv}\left\{\mathbf{z}\in K_{d,r}\cap\mathbb{Z}^d:\,z_1\le 0\right\}.$$

By (19) and (22), we respectively obtain

$$|H_{d,r}|\sim\frac{1}{2}\cdot v(C_{d,r})=\frac{c_2(d)}{2}\cdot r^{d+1} \tag{26}$$

and

$$|H'_{d,r}|\sim\frac{1}{2}\cdot v(K_{d,r})=\frac{c_1(d)}{2}\cdot r^{d+1}. \tag{27}$$

Remark 6. Let $L(\mathbf{x})$ denote the line defined by $\{\mathbf{x}+\lambda\mathbf{e}_d:\ \lambda\in\mathbb{R}\}$, where $\mathbb{R}$ is the real number field. When $\mathbf{z}$ is a lattice point on the boundary of $B_{d,r}$, we have

$$\left|L(\mathbf{z})\cap Q_{d,r}\cap\mathbb{Z}^d\right|=1.$$

Now, we introduce a technical lemma which is useful in the proof of Theorem 5.

Lemma 1. *When r is a sufficiently large integer, for any integer k satisfying $0\le k\le 3r|B_{d,r+1}\cap\mathbb{Z}^d|$, there is a convex lattice polytope P satisfies both*

$$H'_{d,r}\subseteq P\subseteq H_{d,r}$$

and

$$|P|=|H'_{d,r}|+k.$$

Proof. It is well-known that

$$\begin{aligned} \left|B_{d,r+1}\cap\mathbb{Z}^d\right| &= \frac{\pi^{\frac{d-1}{2}}}{\Gamma(\frac{d+1}{2})}\cdot(r+1)^{d-1}+\bigcirc\left((r+1)^{d-2}\right). \\ &= \frac{\pi^{\frac{d-1}{2}}}{\Gamma(\frac{d+1}{2})}\cdot r^{d-1}+\bigcirc\left(r^{d-2}\right). \end{aligned}$$

By (26), (27) and (23), when r is sufficiently large, we get

$$\begin{aligned} |H_{d,r}| - |H'_{d,r}| &\geq \frac{1}{4} \cdot (c_2(d) - c_1(d)) \cdot r^{d+1} \\ &\geq c_3(d) \cdot r^2 \cdot |B_{d,r+1} \cap \mathbb{Z}^d| \\ &\geq 3r |B_{d,r+1} \cap \mathbb{Z}^d|, \end{aligned} \tag{28}$$

where $c_3(d)$ is a constant depends only on d.

For convenience, we write $P_0 = H_{d,r}$ and let $\overline{P}$ denote the set of the vertices of P. If $\mathbf{v}_0 \in \overline{P_0} \setminus H'_{d,r}$, we define

$$P_1 = \mathrm{conv}\left\{(P_0 \cap \mathbb{Z}^d) \setminus \{\mathbf{v}_0\}\right\}.$$

Inductively, if P_i has been defined and $\mathbf{v}_i \in \overline{P_i} \setminus H'_{d,r}$, we construct

$$P_{i+1} = \mathrm{conv}\left\{(P_i \cap \mathbb{Z}^d) \setminus \{\mathbf{v}_i\}\right\}.$$

Thus, we have constructed a finite sequence of convex lattice polytopes P_0, P_1, P_2, …, $P_\ell = H'_{d,r}$ which satisfies both

$$P_0 \supset P_1 \supset \ldots \supset P_{\ell-1} \supset P_\ell = H'_{d,r}$$

and

$$|P_i| - |P_{i+1}| = 1, \quad i = 0, 1, 2, \ldots, \ell - 1.$$

By (28) it follows that

$$\ell \geq 3r \left|B_{d,r+1} \cap \mathbb{Z}^d\right|.$$

The assertion is proved. □

Proof of Theorem 5. First, we recall that

$$P_{d,r} = \mathrm{conv}\left\{K_{d,r} \cap \mathbb{Z}^d\right\}. \tag{29}$$

Let w be a large odd integer and let r be the integer satisfying

$$|P_{d,r}| \leq \frac{w}{2} < |P_{d,r+1}|. \tag{30}$$

By (19) we get

$$r^{d+1} \ll w \ll r^{d+1}. \tag{31}$$

We write

$$P^1_{d,r+1} = \{\mathbf{x} \in P_{d,r+1} : \ x_d \geq 2r + 1\}$$

and

$$P^2_{d,r+1} = \{\mathbf{x} \in P_{d,r+1} : \ x_d \leq 2r\}.$$

It is easy to see that

$$|P_{d,r}| = \left|P^1_{d,r+1}\right|$$

and therefore

$$|P_{d,r+1}| - |P_{d,r}| = \left|P^2_{d,r+1}\right| \le (2r+1)\left|B_{d,r+1} \cap \mathbb{Z}^d\right|. \tag{32}$$

We write

$$u = w - 2|P_{d,r}| + \left|B_{d,r} \cap \mathbb{Z}^d\right|. \tag{33}$$

By (30) and (32) we get

$$u < 2\left(|P_{d,r+1}| - |P_{d,r}|\right) + \left|B_{d,r} \cap \mathbb{Z}^d\right| \le 5r\left|B_{d,r+1} \cap \mathbb{Z}^d\right|. \tag{34}$$

Let $V'_{d,r}$ denote the set of the vertices $\mathbf{v}$ of $P_{d,r}$ satisfying both $v_d \neq 0$ and $v_1 \ge 1$, and let $L(\mathbf{x})$ denote the line $\{\mathbf{x} + \lambda \mathbf{e}_d : \ \lambda \in \mathbb{R}\}$ as defined in Remark 6. By convexity, for all $\mathbf{z} \in B_{d,r} \cap \mathbb{Z}^d$ with $z_1 \ge 1$ we have

$$\left|L(\mathbf{z}) \cap V'_{d,r}\right| \le 1.$$

Thus we get

$$\left|V'_{d,r}\right| < \frac{1}{2}\left|B_{d,r} \cap \mathbb{Z}^d\right| \tag{35}$$

and

$$\begin{aligned}\left|V'_{d,r}\right| &\ge \frac{1}{2} \cdot \left(\left|\mathrm{int}(B_{d,r}) \cap \mathbb{Z}^d\right| - \left|B_{d-1,r} \cap \mathbb{Z}^d\right|\right)\\ &\ge \frac{1}{3} \cdot \left(\frac{\pi^{\frac{d-1}{2}}}{\Gamma(\frac{d+1}{2})} \cdot r^{d-1} - \frac{\pi^{\frac{d-2}{2}}}{\Gamma(\frac{d}{2})} \cdot r^{d-2}\right)\\ &\gg r^{d-1}.\end{aligned} \tag{36}$$

With these preparations, we proceed to construct the expected convex lattice polytopes.

Step 1. Let $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_j$ be j points in $V'_{d,r}$ and define

$$P'_{d,r} = \mathrm{conv}\left\{P_{d,r} \setminus \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_j\}\right\}. \tag{37}$$

We have

$$\left|P'_{d,r}\right| = |P_{d,r}| - j. \tag{38}$$

By (34) and (35) we get

$$\begin{aligned}\frac{u}{2} + j &\le \frac{5}{2}r\left|B_{d,r+1} \cap \mathbb{Z}^d\right| + \frac{1}{2}\left|B_{d,r} \cap \mathbb{Z}^d\right|\\ &< 3r\left|B_{d,r+1} \cap \mathbb{Z}^d\right|.\end{aligned}$$

According to Lemma 1, there is a convex lattice polytope P satisfies both

$$H'_{d,r} \subseteq P \subseteq H_{d,r} \tag{39}$$

and

$$|P| = \left|H'_{d,r}\right| + \frac{u}{2} + j. \tag{40}$$

Step 2. We construct

$$P' = P \cup P'_{d,r}. \tag{41}$$

It is easy to see that P' is a convex lattice polytope. By (38) and (40) we get

$$|P'| = |P_{d,r}| + \frac{u}{2}. \tag{42}$$

Step 3. We define

$$P_{\mathbf{v}_1,\ldots,\mathbf{v}_j} = P' \cup \{-P'\}. \tag{43}$$

Clearly $P_{\mathbf{v}_1,\ldots,\mathbf{v}_j}$ is a centrally symmetric convex lattice polytope centered at the origin. By (42) and (33) we get

$$\begin{aligned}\left|P_{\mathbf{v}_1,\ldots,\mathbf{v}_j}\right| &= 2\left(|P_{d,r}| + \frac{u}{2}\right) - \left|B_{d,r}\cap\mathbb{Z}^d\right| \\ &= 2|P_{d,r}| + u - \left|B_{d,r}\cap\mathbb{Z}^d\right| \\ &= 2|P_{d,r}| + w - 2|P_{d,r}| + \left|B_{d,r}\cap\mathbb{Z}^d\right| - \left|B_{d,r}\cap\mathbb{Z}^d\right| \\ &= w.\end{aligned}$$

Step 4. Taking all possible subsets of $V'_{d,r}$, we get $2^{|V'_{d,r}|}$ centrally symmetric convex lattice polytopes of cardinality w. For convenience, we enumerate them by P_1, P_2, …, $P_{2^{|V'_{d,r}|}}$ and denote the whole family by $\mathcal{F}$.

Now, we study the equivalence relation among $\mathcal{F}$.

Recalling the definitions of $L(P,\mathbf{v})$ and $\ell(P)$ in the proof of Theorem 3, for any $P_i\in\mathcal{F}$ we have

$$\ell(P_i) = 2r^2+1$$

and

$$L(P_i,\mathbf{v}) = 2r^2+1$$

holds if and only if $\mathbf{v}=\pm\mathbf{e}_d$. Therefore, if $\sigma(P_i)=P_j$ holds for some unimodular transformation σ, we have

$$\sigma(\mathbf{o}) = \mathbf{o}$$

and

$$\sigma(\mathbf{e}_d)\in\{\mathbf{e}_d,-\mathbf{e}_d\}.$$

Let H be a $(d-1)$-dimensional hyperplane which contains the origin of $\mathbb{E}^d$, but not $\mathbf{e}_d$. By projecting $P_i\cap H\cap\mathbb{Z}^d$ onto the plane $\{\mathbf{x}\in\mathbb{E}^d:\ x_d=0\}$, keeping (24), (25), (29), (37), (39), (41), (43) and Remark 6 in mind, it follows that

$$\left|P_i\cap H\cap\mathbb{Z}^d\right| \le \left|B_{d,r}\cap\mathbb{Z}^d\right|,$$

where the equality holds if and only if

$$H = \left\{\mathbf{x}\in\mathbb{E}^d:\ x_d=0\right\}.$$

Thus, we get

$$\sigma\left(B_{d,r}\cap\mathbb{Z}^d\right) = B_{d,r}\cap\mathbb{Z}^d$$

and therefore

$$\sigma \in G\left(\mathrm{conv}\left\{B_{d,r} \cap \mathbb{Z}^d\right\}\right) = G(P_{d-1,r,2}).$$

Consequently, by the $\rho = 2$ case of Theorem 3, we get

$$\kappa^*(d,w) \geq \frac{|\mathcal{F}|}{2|G(P_{d-1,r,2})|} = \frac{2^{|V'_{d,r}|}}{2^d \cdot (d-1)!}.$$

By (36) and (31), we deduce

$$\log \kappa^*(d,w) \gg |V'_{d,r}| \gg r^{d-1} \gg w^{\frac{d-1}{d+1}}.$$

The proof is complete. □

Acknownledgement. I am grateful to Professor Imre Bárány for some email discussion on this topic.

References

[1] V.I. Arnold, Statistics of integral convex polygons, (in Russian), *Funk. Anal. Pril.* **14** (1980), 1-3. English translation: Funct. Anal. Appl. **14** (1980), 79-81.

[2] I. Bárány, Random points and lattice points in convex bodies. *Bull. Amer. Math. Soc.* (N.S.) **45** (2008), 339-365.

[3] I. Bárány, Extremal problems for convex lattice polytopes: a survey, *Contemp. Math.* **453** (2008), 87-103.

[4] I. Bárány and J. Pach, On the number of convex lattice polygons, *Comb. Probab. Comput.* **1** (1992), 295-302.

[5] I. Bárány and A.M. Vershik, On the number of convex lattice polytopes, *Geom. Funct. Anal.* **2** (1992), 381-393.

[6] A. Barvinok, Lattice points and lattice polytopes, *Handbook of Discrete and Computational Geometry*, CRC Press, (2004), 133-152.

[7] P.M. Gruber, *Convex and Discrete Geometry*, Springer-Verlag, Berlin, 2007.

[8] S.B. Konyagin and K.A. Sevastyanov, A bound, in terms of its volume, for the number of vertices of a convex polyhedron when the vertices have integer coordinates, (in Russian), *Funk. Anal. Pril.* **18** (1984), 13-15. English translation: Funct. Anal. Appl. **18** (1984), 11-13.

[9] J.C. Lagarias and G.M. Ziegler, Bounds for lattice polytopes containing a fixed number of interior points in a sublattice, *Canadian J. Math.* **43** (1991), 1022-1035.

[10] H. Liu and C. Zong, On the classifications of convex lattice polytopes, *Adv. Geom.* in press.

[11] O. Pikhurko, Lattice points in lattice polytopes, *Mathematika*, **48** (2001), 15-24.

[12] G.M. Ziegler, *Lectures on Polytopes*, Springer-Verlag, New York, 1995.

[13] C. Zong, What is known about unit cubes, *Bull. Amer. Math. Soc.* **42** (2005), 181-211.

School of Mathematical Sciences, Peking University, Beijing 100871, People's Republic of China
E-mail address: cmzong@math.pku.edu.cn