Random points and lattice points in convex bodies

April 28, 2008

1 Introduction

We write $\mathcal{K}$ or $\mathcal{K}^d$ for the set of convex bodies in $\mathbb{R}^d$, that is, compact convex sets with nonempty interior in $\mathbb{R}^d$. Assume $K \in \mathcal{K}$ and $x_1, \ldots, x_n$ are random, independent points chosen according to the uniform distribution in K. The convex hull of these points, to be denoted by K_n, is called a **random polytope** inscribed in K. Thus $K_n = [x_1, \ldots, x_n]$ where $[S]$ stands for the convex hull of the set S. The study of random polytopes began in 1864 with Sylvester's famous "four-point question" [73].

Starting with the work of Rényi and Sulanke in 1964 [56] there has been a lot of research to understand the asymptotic behaviour of random polytopes. Most of it has been concentrated on the expectation of various functionals associated with K_n. For instance the number of vertices, $f_0(K_n)$, or more generally, the number of k-dimensional faces, $f_k(K_n)$, of K_n, or the volume missed by K_n, that is $\mathrm{vol}(K \setminus K_n)$. The latter quantity measures how well K_n approximates K. As usual we will denote the expectation of $f_k(K_n)$ by $\mathbb{E} f_k(K_n)$, and that of $\mathrm{vol}(K \setminus K_n)$ by $\mathbb{E}(K, n)$.

We write $\mathcal{K}_1$ for the set of those $K \in \mathcal{K}$ that have unit volume: $\mathrm{vol}\, K = 1$. This is convenient since then the Lebesgue measure and the uniform probability measure on $K \in \mathcal{K}_1$ coincide. The boundary of K is denoted by $\mathrm{bd}\, K$. We write $\mathrm{aff}\, S$ for the affine hull of S.

Assume $a \in \mathbb{R}^d$ is a unit vector and $t \in \mathbb{R}$. Then the halfspace $H = H(a \le t)$ is defined as

$$H(a \le t) = \{x \in \mathbb{R}^d : a \cdot x \le t\},$$

where $a \cdot x$ is the scalar product of a and x. The bounding hyperplane of this halfspace is denoted by $H(a = t)$.

We will use often the Brunn-Minkowski theorem which says the following. If $K, L \subset \mathbb{R}^d$ are convex sets, then

$$\mathrm{vol}(K + L)^{1/d} \ge (\mathrm{vol}\, K)^{1/d} + (\mathrm{vol}\, L)^{1/d}$$

where $K + L$ is the set of all $k + l$ with $k \in K$ and $l \in L$. For a proof see Schneider's book [64]

The Brunn-Minkowski theorem has an important consequence. Suppose $K \in \mathcal{K}^d$, define $h(t) = \mathrm{vol}_{\,d-1} K \cap H(a = t)$ and assume that $h(t)$ is positive on an interval I.

Lemma 1.1. *The function $t \to h^{1/(d-1)}(t)$ is concave on I.*

2 A general result on $\mathbb{E}(K, n)$

A **cap** of $K \in \mathcal{K}$ is simply a set of the form $C = K \cap H$ where H is a closed halfspace. The width of the cap, $w(C)$ is the usual width of C in the normal direction of H. We define the function $v : K \to \mathbb{R}$ by

$$v(x) = \min\{\text{vol}(K \cap H) : x \in H, \text{ and } H \text{ is a halfspace}\},$$

This function is going to play a central role in what follows. The **minimal cap** belonging to $x \in K$ is a cap $C(x)$ with $x \in C(x)$ and $\text{vol}\, C(x) = v(x)$. The minimal cap $C(x)$ need not be unique, so our notation is a little ambiguous but this will not cause any trouble.

The level sets of v are defined as

$$K(v \geq t) = \{x \in K : v(x) \geq t\}.$$

The **wet part** of K with parameter $t > 0$ is

$$K(t) = K(v \leq t) = \{x \in K : v(x) \leq t\}.$$

The name comes from the mental picture when K is a three dimensional convex body containing t units of water. We call $K(v \geq t)$ the **floating body** of K with parameter $t > 0$ as, in a similar picture, this is the part of K that floats above water (cf [14] and [44]). The floating body is the intersection of halfspaces so it is convex.

The wet part $K(t) = K(v \leq t)$ is a kind of inner parallel body to the boundary of K. We note that the function $v : K \to \mathbb{R}$ is invariant (or rather equivariant) under non-degenerate linear transformations $A : \mathbb{R}^d \to \mathbb{R}^d$. Precisely, with notation $v(x) = v_K(x)$, we have

$$v_{AK}(Ax) = |\det A| v_K(x)$$

since $C_{AK}(Ax) = A(C_K(x))$. This also shows that the quantity

$$\frac{\text{vol}\, K(v \leq t \,\text{vol}\, K)}{\text{vol}\, K} \tag{2.1}$$

is invariant under non-degenerate linear transformations.

The following theorem describes the general behaviour of $\mathbb{E}(K, n)$: The expected missed volume is of the same order of magnitude as the volume of the wet part with $t = 1/n$. This works for general convex bodies $K \in \mathcal{K}$, not only when K is smooth or is a polytope. Precisely, we have

Theorem 2.1. *For every $d \geq 2$ there are constants $c_0, c_1, c_2 > 0$ such that for every $K \in \mathcal{K}_1$ and $n \geq c_0$*

$$c_1 \,\text{vol}\, K(1/n) \leq \mathbb{E}(K, n) \leq c_2 \,\text{vol}\, K(1/n).$$

It will be convenient to use the $\ll$, $\gg$ and $\approx$ notation. For instance, $f(n) \ll g(n)$ means that there is a constant b such that $f(n) \leq bg(n)$ for all values of n. This notation always hides a constant which, as a rule, does not depend on n but may depend on dimension. With this notation, the above theorem can be formulated this way:

Theorem 2.2. *For large enough n and for every $K \in \mathcal{K}_1$*

$$\operatorname{vol} K(1/n) \ll \mathbb{E}(K,n) \ll \operatorname{vol} K(1/n).$$

The content of Theorem 2.2 is that, instead of determining $\mathbb{E}(K,n)$, one can determine the volume of the wet part (which is usually simpler) and obtain the order of magnitude of $\mathbb{E}(K,n)$. The reader will have no difficulty understanding that for the unit ball B^d in $\mathbb{R}^d$ the wet part $B^d(v \le t)$ is the annulus $B^d \setminus (1-h)B^d$ where h is of order $t^{2/(d+1)}$. Thus

$$\mathbb{E}(B^d,n) \approx \operatorname{vol} B^d(1/n) \approx n^{-2/(d+1)}.$$

Similarly, for the unit cube Q^d in $\mathbb{R}^d$ the floating body with parameter t (in the subcube $[0,1/2]^d$) is bounded by the hypersurface $\{x \in \mathbb{R}^d : \prod x_i = d^d t/d!\}$. From this the volume of the wet part can be determined easily:

$$\mathbb{E}(Q^d,n) \approx \operatorname{vol} Q^d(1/n) \approx \frac{(\ln n)^{d-1}}{n}.$$

This shows that the behaviour of $\mathbb{E}(K,n)$ can be very different for different convex bodies: the volume of the wet part varies heavily depending on the boundary structure of K.

3 Economic cap covering of $K(v \le \varepsilon)$

Everything interesting that can happen to a convex body happens near its boundary. The technique of cap-coverings and M-regions is a powerful method to deal with the boundary structure of convex bodies. The proof of the economic cap covering theorem (see [14] and [7]) is based on this technique. It says the following

Theorem 3.1. *Assume $K \in \mathcal{K}_1$ and $0 < \varepsilon < \varepsilon_0 = (d2^d)^{-1}$. Then there are caps $C_1, \dots, C_m$ and pairwise disjoint convex sets $C_i', \dots, C_m'$ such that $C_i' \subset C_i$ for each i and*

(i) $\bigcup_1^m C_i' \subset K(\varepsilon) \subset \bigcup_1^m C_i$,

(ii) $\operatorname{vol} C_i' \gg \varepsilon$ *and* $\operatorname{vol} C_i \ll \varepsilon$ *for each i,*

(iii) for each cap C with $C \cap K(v > \varepsilon) = \emptyset$ there is a C_i containing C.

The meaning is that the caps C_i cover the wet part, but do not “over cover” it. In particular,

$$m\varepsilon \ll \operatorname{vol} K(\varepsilon) \ll m\varepsilon. \tag{3.1}$$

The next corollary expresses a certain concavity property of the function $\varepsilon \to \operatorname{vol} K(\varepsilon)$. It says that, apart from the constant implied by the $\gg$ notation, $\operatorname{vol} K(\varepsilon)$ is a concave function near $\varepsilon = 0$. This will be sufficient for our purposes, that is, for the proof of Theorem 2.2.

Corollary 3.2. *If $K \in \mathcal{K}_1$, $\varepsilon \le \varepsilon_0$, and $\lambda \ge 1$, then*

$$\operatorname{vol} K(\varepsilon) \gg \lambda^{-1} \operatorname{vol} K(\lambda\varepsilon). \tag{3.2}$$

The proof of the above results relies heavily on the Macbeath-regions and their properties. They are defined, with their properties explained, in the next section.

4 Macbeath-regions

Macbeath-regions, or M-regions, for short, were introduced in 1952 by A. M. Macbeath: given a convex body $K \in \mathcal{K}^d$, and a point $x \in K$, the corresponding M-region is, by definition,

$$M(x) = M_K(x) = K \cap (2x - K).$$

So $M(x)$ is, again, a convex set. It is centrally symmetric with centre x. We define the blown-up version of the M-region as follows

$$M(x,\lambda) = M_K(x,\lambda) = x + \lambda\left[(K-x) \cap (x-K)\right].$$

This is just a blown-up copy of $M(x)$ from its center x with scalar $\lambda > 0$.

We define the function $u : K \to \mathbb{R}$ by

$$u(x) = \operatorname{vol} M(x).$$

The level sets of u are defined the same way as those of v:

$$K(u \le t) = \{x \in K : u(x) \le t\},\ K(u \ge t) = \{x \in K : u(x) \ge t\}.$$

We note that the function $u : K \to \mathbb{R}$, just like v, is invariant (or rather equivariant) under non-degenerate linear transformations $A : \mathbb{R}^d \to \mathbb{R}^d$. That is,

$$u_{AK}(Ax) = |\det A| u_K(x)$$

since $M_{AK}(Ax) = A(M_K(x))$. This also shows that the quantity,

$$\frac{\operatorname{vol} K(u \le t \operatorname{vol} K)}{\operatorname{vol} K} \tag{4.1}$$

is invariant under non-degenerate linear transformations, cf (2.1).

M-regions have an important property that can often be used with induction on dimension. Namely, assume H is a hyperplane and $x \in K \cap H$. Then, as it is very easy to see,

$$M_{K\cap H}(x) = M_K(x) \cap H. \tag{4.2}$$

The convexity of $K(u \ge t)$ is not as simple as that of $K(v \ge t)$. It was proved by Macbeath [47]. We state it as a separate lemma.

Lemma 4.1. *The function $u^{1/d} : K \to \mathbb{R}$ is concave. Consequently, the set $K(u \ge t)$ is convex.*

Proof. We check first that $\frac{1}{2}(M(x)+M(y)) \subset M(\frac{1}{2}(x+y))$. So assume $a \in M(x)$, that is $a \in K$ and $a \in 2x - K$, or $a = 2x - k_1$ for some $k_1 \in K$. Similarly $b \in M(y)$ implies $b \in K$ and $b = 2y - k_2$ for some $k_2 \in K$. Then, by the convexity of K, $(a+b)/2 \in K$ and

$$\frac{a+b}{2} = x + y - \frac{k_1+k_2}{2} \in 2\frac{x+y}{2} - K,$$

implying the claim. Now the Brunn-Minkowski inequality together with the containment $\frac{1}{2}(M(x)+M(y)) \subset M(\frac{1}{2}(x+y))$ implies that the function $u^{1/d}$ is concave in the following way.

$$\begin{aligned}
\frac{1}{2}u(x)^{1/d} \quad + \quad & \frac{1}{2}u(y)^{1/d} = \frac{1}{2}\left(\operatorname{vol} M(x)^{1/d} + \operatorname{vol} M(y)^{1/d}\right) \\
\leq \quad & \frac{1}{2}\operatorname{vol}\left(M(x)+M(y)\right)^{1/d} = \operatorname{vol}\left(\frac{M(x)+M(y)}{2}\right)^{1/d} \\
\leq \quad & \operatorname{vol} M\left(\frac{x+y}{2}\right)^{1/d} = u\left(\frac{x+y}{2}\right)^{1/d}.
\end{aligned}$$

Thus, in particular, the level sets $K(u \geq t)$ are convex. $\square$

We need another property of the function u, proved first by S. Stein [72]

Lemma 4.2. *Given* $K \in \mathcal{K}_1$, $\max\{u(x) : x \in K\} > 2^{-d}$.

Proof. The basic observation is that the average of $u(x)$ on $K \in \mathcal{K}_1$ equals 2^{-d}. From this the Lemma follows immediately. In order to determine the average of $u(x)$, let K^* be the set of pairs (x,y) with $x \in K$ and $y \in M(x)$. Since K^* is convex (right?), Fubini's theorem applies:

$$\int_K u(x)dx = \int\int_{K^*} dydx = \int\int_{K^*} dxdy.$$

For fixed $y \in K$, $y \in M(x)$ if and only if $y \in 2x - K$, or, equivalently, $x \in y + \frac{1}{2}(K-y)$. Thus for fixed $y \in K$, $\int_{K^*} dx = 2^{-d}\operatorname{vol} K = 2^{-d}$. $\square$

The computation of $u(x)$ is simpler than that of $v(x)$ since one does not have to minimize. It turns out that $v(x) \approx u(x)$, when x is close to the boundary of K. A word of warning is in place here: closeness to the boundary is to be expressed equivariantly, that is, in terms of how small $v(x)$ or $u(x)$ is as both u and v are affinely equivariant.

We now list several properties of these functions and their interrelations. The proofs are technical and will be given in the next section which can be skipped on first reading. In each one of these lemmas we assume that K is a convex body in $\mathcal{K}_1$ and $\varepsilon_0 = (d2^d)^{-1}$.

Lemma 4.3. *For all* $x \in K$, $u(x) \leq 2v(x)$.

Lemma 4.4. *If* $x, y \in K$ *and* $M(x,1/2) \cap M(y,1/2) \neq \emptyset$, *then*

$$M(y,1) \subset M(x,5).$$

Lemma 4.5. *If $x \in K$ and $v(x) \le \varepsilon_0$, then*

$$C(x) \subset M(x, 2d).$$

Lemma 4.6. *If $x \in K$ and $v(x) \le \varepsilon_0$, then $v(x) \le (2d)^d u(x)$.*

Lemma 4.7. *If $x \in K$ and $u(x) \le (2d)^{-d}\varepsilon_0$, then $v(x) \le (2d)^d u(x)$.*

Lemma 4.8. *When $\varepsilon > 0$, $K(v \ge \varepsilon)$ contains no line segment on its boundary.*

Lemma 4.9. *Assume C is a cap of K and $C \cap K(v \ge \varepsilon) = \{x\}$, a single point. If $\varepsilon \le \varepsilon_0$, then $\operatorname{vol} C \le d\varepsilon$ and*

$$C \subset M(x, 2d).$$

Lemma 4.10. *Every $y \in K(\varepsilon)$ is contained in a minimal cap $C(x)$ with $\operatorname{vol} C(x) = \varepsilon$ and $x \in \operatorname{bd} K(v \ge \varepsilon)$, provided $\varepsilon \le \varepsilon_0$.*

Lemma 4.11. *If $\varepsilon \le \varepsilon_0$, then for every $y \in K(\varepsilon)$ there is an $x \in \operatorname{bd} K(v \ge \varepsilon)$ with $y \in M(x)$.*

Lemma 4.12. *For all $\varepsilon \ge 0$, $K(v \le \varepsilon) \subset K(u \le 2\varepsilon)$. If $\varepsilon \le (2d)^{-d}\varepsilon_0$, then $K(u \le (2d)^{-d}\varepsilon) \subset K(v \le \varepsilon)$.*

The importance of these lemmas lies in the fact that they show $u \approx v$ near the boundary of K in a strong sense. Namely, under the conditions of Lemma 4.5 the minimal cap is contained in a blown up copy of the Macbeath region. On the other hand, "half" of the Macbeath region is contained in the minimal cap. Precisely, if $C = K \cap H(a \le t)$ is a minimal cap, then

$$M(x) \cap H(a \le t) \subset C(x). \tag{4.3}$$

This shows that there is a two-way street between $C(x)$ and $M(x)$: $C(x)$ can be replaced by $M(x)$ and $M(x)$ by $C(x)$ whenever it is more convenient to work with the other one.

5 Proofs of the properties of the M-regions

Lemma 4.3 follows from (4.3).

Proof of Lemma 4.4 from the ground breaking paper by Ewald, Larman, Rogers [28]. Assume a is the common point of $M(x, 1/2)$ and $M(y, 1/2)$. Then

$$a = x + \frac{1}{2}(x - k_1) = y + \frac{1}{2}(k_2 - y)$$

for some $k_1, k_2 \in K$ implying $y = 3x - k_1 - k_2$. Suppose now that $b \in M(y, 1)$. Then $b \in K \subset x + 5(K - x)$ clearly, and $b = y + (y - k_3)$ with some $k_3 \in K$. Consequently

$$\begin{aligned} b &= 2y - k_3 = 6x - 2k_1 - 2k_2 - k_3 \\ &= x + 5\left(x - \left[\frac{2}{5}k_1 + \frac{2}{5}k_2 + \frac{1}{5}k_3\right]\right) \in x + 5(x - K). \end{aligned}$$

□

Lemma 4.5 is also from the Ewald, Larman, Rogers paper. The proof below is a slight improvement on their constant, and comes from an effort to find an affine invariant proof when the statement is affine invariant.

Proof of Lemma 4.5. The basic observation is that if $C(x) = K \cap H(a \leq t)$ is minimal cap, then x is the centre of gravity of the section $K \cap H(a = t)$. This can be checked by a routine variational argument. We first prove the following

Claim 5.1. *Assume $C(x)$ has width w, and K contains a point k in the hyperplane $H(a = t + w)$. Then $C(x) \subset M(x, 2d)$.*

Proof. Assume that, on the contrary, there is a point $z \in C(x)$ which is not in $M(x, 2d)$. Then $z \notin x + 2d(x - K)$ implying

$$z^* = x - \frac{1}{2d}(z - x) \notin K.$$

Let L be the two-dimensional plane containing x, k and z, then $z^* \in L$ as well, and our problem has become a simple plane computation. Fix a coordinate system to L with x lying at the origin and the hyperplane $H(a = t)$ intersecting L in the y axis, as shown in Figure 1.

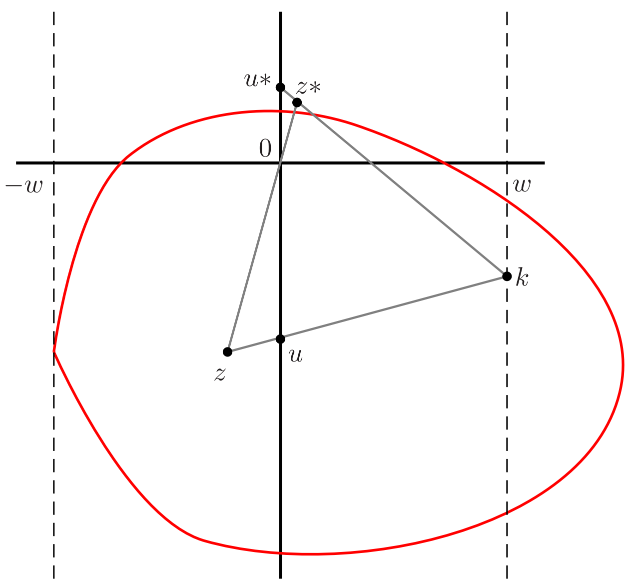

Figure 1

In this setting $z^* = -\frac{1}{2d}z$. The line aff$\{k, z\}$, resp. aff$\{k, z^*\}$ intersects the y axis at the points $u \in K$ (since $k, z \in K$) and $u^* \notin K$ (since $k \in K$ and $z^* \notin K$). As x is the centre of gravity of a $(d-1)$-dimensional section, $(d-1)\|u^*\| > \|u\|$ must hold. Write $k = (k_1, k_2)$ and $z = (z_1, z_2)$; the conditions imply that $k_1 = w$ and $z_1 \in [-w, 0]$. It is not hard to check that

$$\|u\| = \frac{|k_1 z_2 - k_2 z_1|}{k_1 - z_1} \text{ and } \|u^*\| = \frac{|k_1 z_2 - k_2 z_1|}{2dk_1 + z_1}.$$

Then $(d-1)\|u^*\| > \|u\|$ implies $(d-1)(k_1-z_1) > 2dk_1+z_1$ or $-dz_1 > (d+1)k_1$ contradicting $k_1 = w$ and $z_1 \in [-w, 0]$. $\square$

The rest of the proof is what I like to call trivial volume estimates. We show that if $C(x) = K \cap H(a \le t)$ is a minimal cap of width w and $v(x) \le \varepsilon_0$, then the width of K in direction a is at least $2w$. Assume the contrary. We can suppose, by translating K if necessary, that $H(a = 0)$ is the common supporting hyperplane to $C(x)$ and K. Then $w = t$, and we define

$$A(\tau) = \mathrm{vol}_{\,d-1}(K \cap H(a = \tau)).$$

Then $1 = \mathrm{vol}\, K = \int_0^{2w} A(\tau)d\tau$, and $v(x) = \mathrm{vol}\, C(x) = \int_0^w A(\tau)d\tau$. Clearly $A(\tau)$ is positive on an interval $(0, s)$ with $w \le s < 2w$. The Brunn-Minkowski theorem, actually Lemma 1.1, shows that $A(\tau)^{1/(d-1)}$ is a concave function on $[0, s)$. It is easy to see then that $A(2\tau) \le 2^{d-1}A(\tau)$ for all $\tau \in [0, w]$, with strict inequality when $2\tau > s$. Thus

$$1 = \int_0^{2w} A(\tau)d\tau = 2\int_0^w A(2\tau)d\tau < 2^d \int_0^w A(\tau)d\tau = 2^d v(x),$$

contradicting $v(x) \le \varepsilon_0$. $\square$

Lemma 4.6 follows immediately.

Proof of Lemma 4.7. We prove the stronger statement that $u(x) \le (2d)^{-d}\varepsilon$ and $\varepsilon \le \varepsilon_0$ implies $v(x) \le \varepsilon$. This implication is the same as

$$K(u \le (2d)^{-d}\varepsilon) \subset K(v \le \varepsilon),$$

which is the same as

$$K(v \ge \varepsilon) \subset K(u \ge (2d)^{-d}\varepsilon).$$

The advantage of the last formulation is that both sets are convex, and both contain the point where the function u takes its maximum. (The last statement follows from Lemma 4.2.) So it suffices to check that every point on the boundary of $K(v \ge \varepsilon)$ is contained in $K(u \ge (2d)^{-d}\varepsilon)$. But at boundary point, z say, $v(z) = \varepsilon \le \varepsilon_0$, and Lemma 4.6 implies what we need. $\square$

Proof of Lemma 4.8. Let $x, y \in \mathrm{bd}\, K(v \ge \varepsilon)$ and assume $z = \frac{1}{2}(x + y)$ is also in $\mathrm{bd}\, K(v \ge \varepsilon)$. Then there is a minimal cap $C(z)$ of volume ε. $C(z)$ cannot contain x (or y) in its interior as otherwise a smaller "parallel" cap would contain x (or y). Then $C(z)$ must contain both x and y in its bounding hyperplane. Then it is a minimal cap for both x and y. But both x and y cannot be the centre of gravity of the section $K \cap H(a = t)$ at the same time unless $x = y$.

Proof of Lemma 4.9. Denote the set of outer normals to $K(v \ge \varepsilon)$ at $z \in \mathrm{bd}\, K(v \ge \varepsilon)$ by $N(z)$. It is well known (see [58]) that as $K(v \ge \varepsilon)$ is a convex body, $N(z)$ coincides with the cone hull of its extreme rays.

For $b \in S^{d-1}$ define C^b as the unique cap $C^b = K \cap H(b \le t)$ such that $C^b \cap K(v \ge \varepsilon) \ne \emptyset$ but $C^b \cap \mathrm{int}\, K(v \ge \varepsilon) = \emptyset$. Then, by the previous lemma,

$C^b \cap K(a \geq \varepsilon) = \{x\}$. We mention that the function $b \to \operatorname{vol} C^b$ is obviously continuous. We will need a classical result of Alexandrov (see for instance [64]) stating that at almost every point z on the boundary of a convex body the supporting hyperplane is unique. This shows that if $z \in \operatorname{bd} K(v \geq \varepsilon)$ is such a point then $N(z) \cap S^{d-1}$ is a unique vector, to be denoted by $b(z)$. In this case, of course, $\operatorname{vol} C^{b(z)} = \varepsilon$.

Claim 5.2. *If b is the direction of an extreme ray of $N(z)$, then* $\operatorname{vol} C^b = \varepsilon$.

Proof. We prove the claim first for an extremal ray which is exposed as well. This means that there is a vector $w \in S^{d-1}$ such that $w \cdot b = 0$ and $w \cdot x < 0$ for all $x \in N(z)$, $x \neq \lambda b$ $(\lambda > 0)$.

Note that $N(z)$ is the polar of the minimal cone whose apex is z and which contains $K(v \geq \varepsilon)$. Then w is in the polar of $N(z)$, and w is a tangent direction to $K(v \geq \varepsilon)$ at z. So there are points $z(t) \in \operatorname{bd} K(v \geq \varepsilon)$ for all small enough $t > 0$ with

$$\|(z(t) - z) - tw\| = o(t) \text{ as } t \to 0.$$

Choose now a subsequence $z_k \in \operatorname{bd} K(v \geq \varepsilon)$ very close to $z(1/k)$ with unique tangent hyperplane to $K(v \geq \varepsilon)$ (using Alexandrov's theorem). We may assume that $\lim b(z_k)$ exists and equals $b_0 \in S^{d-1}$. It is easily seen that $b_0 \in N(z)$. Assume $b_0 \neq b$. Then, since $b(z_k) \in N(z_k)$,

$$0 \geq b(z_k) \cdot (y - z_k)$$

for every $y \in K(v \geq \varepsilon)$. In particular, for $y = z$ we get

$$0 \geq b(z_k) \cdot (z - z_k) = -\frac{1}{k} b(z_k) \cdot w - o(1/k) > -\frac{2}{k} b_0 \cdot w - o(1/k) > 0$$

for large enough k. A contradiction proving $b_0 = b$. The continuity of the map $b \to \operatorname{vol} C^b$ implies $\operatorname{vol} C^b = \varepsilon$. This finishes the proof of the claim for exposed rays.

A theorem of Straszewicz (see [64] says (in a slightly different form) that the set of extreme rays is the closure of the set of exposed rays. This implies, again by the continuity of the map $b \to \operatorname{vol} C^b$, that for an extreme ray b of $N(z)$, $\operatorname{vol} C^b = \varepsilon$. □

Now let $C = K \cap H(a \leq t)$ be the cap in the statement of the lemma. Then $-a \in N(x)$ and thus $-a$ is in the cone hull of extreme rays of $N(x)$. Thus by Carathédory's theorem $-a$ is in the cone hull of $b_1, \ldots, b_d \in S^{d-1}$ where each b_i represents an extreme ray of $N(z)$. Then C is contained in $\cup C^{b_i}$. This implies that $\operatorname{vol} C \leq d \operatorname{vol} C^{b_i} = d\varepsilon$. Also, each C^{b_i} is a minimal cap, so by Lemma 4.5, it is contained in $M(x, 2d)$. Consequently,

$$C \subset \bigcup_1^d C^{b_i} \subset M(x, 2d).$$

□

Proof of Lemma 4.10. The minimal cap $C(y) = K \cap H(a \le t)$ is internally disjoint from the floating body $K(v \ge \varepsilon)$. Let τ be the maximal number with $H(a \le \tau)$ internally disjoint from $K(v \ge \varepsilon)$. By Lemma 4.8 the cap $C = K \cap H(a \le \tau)$ contains a unique point $x \in \operatorname{bd} K(v \ge \varepsilon)$. The proof of Lemma 4.9 gives that

$$y \in C(y) \subset C \subset \bigcup_1^d C^{b_i}$$

where each C^{b_i} is a minimal cap of x. $\square$

Proof of Lemma 4.11. Assume the contrary and let $y \in K(v \le \varepsilon)$ be a point contained in no $M(x)$ with x from the boundary of $K(v \ge \varepsilon)$. Then $y \notin 2x - K$, or $2x - y \notin K$. This means that the twice blown-up copy, from centre y, of the convex body $K(v \ge \varepsilon)$ is disjoint from K. Then a halfspace, $H(a \le t)$ say, contains K but is disjoint from $K(v \ge \varepsilon)$. We assume, without loss of generality, that $y = 0$. Then the halfspace $H(a \le t/2)$ is disjoint from $K(v \ge \varepsilon)$. So the cap $C = K \cap H(a \le t/2)$ has volume at most $d\varepsilon$ (by Lemma 4.9). At the same time, the width of K in direction a is less than twice the width of C (in the same direction). As we have seen at the end of the proof of Lemma 4.5, this implies that $2^d \operatorname{vol} C > \operatorname{vol} K$ which contradicts the conditions $\operatorname{vol} K = 1$ and $\operatorname{vol} C \le (d2^d)^{-1}$.

Proof of Lemma 4.12. The first statement follows directly from $u(x) \le 2v(x)$. The second was demonstrated in the proof of Lemma 4.7. $\square$

6 Proof of the cap covering Theorem

We start with a definition: if a cap $C = K \cap H(a \le t)$ has width w, then $H(a = t - w)$ is a supporting hyperplane to K. The **centre** of the cap is the centre of gravity of the set $K \cap H(a = t - w)$. The blown-up copy of C from its centre by a factor $\lambda > 0$ is denoted by C^λ. It is clear that C^λ lies between hyperplanes $H(a = t - w)$ and $H(a = t - w + \lambda w)$, and convexity implies that

$$K \cap H(a \le t - w + \lambda w) \subset C^\lambda \tag{6.1}$$

and so $\operatorname{vol} K \cap H(a \le t - w + \lambda w) \le \lambda^d \operatorname{vol} C$.

Choose a system of points $x_1, \ldots, x_m$ on the boundary of the floating body $K(v \ge \varepsilon)$ which is maximal with respect to the property

$$M(x_i, 1/2) \cap M(x_j, 1/2) = \emptyset$$

for each i, j distinct. Such a maximal system is finite since they are pairwise disjoint, all of them are contained in K and $\operatorname{vol} M(x_i, 1/2) = 2^{-d} u(x_i) \ge (4d)^{-d} v(x) = (4d)^{-d} \varepsilon$.

We show next that

$$K(\varepsilon) \subset \bigcup_1^m M(x_i, 5).$$

Indeed, by Lemma 4.11, for each $y \in K(\varepsilon)$ there is an $x \in \operatorname{bd} K(v \geq \varepsilon)$ with $y \in M(x)$. By the maximality of the system $x_1, \dots, x_m$, there is an x_i with $M(x, 1/2) \cap M(x_i, 1/2) \neq \emptyset$. Lemma 4.4 shows then that $y \in M(x_i, 5)$.

We have now a covering of $K(\varepsilon)$ with M-regions. We are going to turn it into a covering with caps. The minimal cap at x_i is given by $C(x_i) = K \cap H(a_i \leq t_i)$, let w_i be its width. Define

$$C_i' = M(x_i, 1/2) \cap H(a_i \leq t_i) \text{ and } C_i = K \cap H(a_i \leq t_i + 5w_i)..$$

It is evident that the C_i' are pairwise disjoint convex sets, each contained in C_i and $\operatorname{vol} C_i' \geq \frac{1}{2} \operatorname{vol} M(x_i, \frac{1}{2}) \geq \frac{1}{2}(4d)^{-d}\varepsilon$ by Lemma 4.6. On the other hand, $M(x_i, 5)$ lies between hyperplanes $H(a_i = t_i - w_i)$ and $H(a_i = t_i + 5w_i)$ and so it is contained in C_i. Finally, (6.1) shows that $\operatorname{vol} C_i \leq 6^d \operatorname{vol} C(x_i) = 6^d \varepsilon$.

So far this is the proof of (i) and (ii) of the theorem. We now show how one can enlarge C_i to satisfy (iii).

This is quite simple. Keep the previous notation except for C_i, which we now define as $C_i = K \cap H(a_i \leq t_i + (10d - 1)w_i)$. The new C_i satisfy (i) and (ii), with a much larger constant but that does not matter. Then $\operatorname{vol} C_i \ll \varepsilon$. Moreover, $M(x_i, 10d) \subset C_i$.

Consider now a cap C, disjoint from $K(v > \varepsilon)$. We may assume that our C is maximal in the sense that $C \cap K(v \geq \varepsilon)$ nonempty. Then by Lemma 4.8 they have a single point, say x, in common, and by Lemma 4.9

$$C \subset M(x, 2d).$$

By the maximality of the system $x_1, \dots, x_m$ there is an x_i with $M(x, 1) \subset M(x_i, 5)$. We claim that $M(x, 2d) \subset M(x_i, 10d)$. This will prove what we need.

The claim follows from a more general statement:

Fact. Assume A and B are centrally symmetric convex sets with centre a and b respectively. If $B \subset A$ and $\lambda \geq 1$, then

$$b + \lambda(B - b) \subset a + \lambda(A - a). \tag{6.2}$$

Proof. We may assume $a = 0$. Let $c \in B$, we have to prove that $b + \lambda(c - b) \in \lambda A$. B is symmetric, so $2b - c \in B \subset A$, and A is symmetric so $c - 2b \in A$. Also, A is convex and $c \in B \subset A$, thus $(1/2)(c + (c - 2b)) = c - b \in A$. Then $c \in A$ and $c - b \in A$ imply $\lambda c \in \lambda A$ and $\lambda(c - b) \in \lambda A$. But $b + \lambda(c - b)$ lies on the segment connecting λc and $\lambda(c - b)$:

$$b + \lambda(b - c) = \frac{1}{\lambda}(\lambda c) + \left(1 - \frac{1}{\lambda}\right)\lambda(c - b) \in A$$

proving the fact. $\square$

Proof of Corollary 3.2. Let $C_1, \dots, C_m$ be the economic cap covering from Theorem 3.1. We will show that, with notation $\mu = \lambda^{1/d}$,

$$K(\lambda\varepsilon) \subset \bigcup_1^m C_i^{\mu}.$$

This will prove what we want, since, by the economic cap covering theorem,

$$\begin{aligned}\operatorname{vol} K(\lambda\varepsilon) &\leq \sum_1^m \operatorname{vol}(C_i^\mu) = \mu^d \sum_1^m \operatorname{vol} C_i \ll \lambda m \varepsilon \\ &\ll \lambda \sum_1^m \operatorname{vol} C_i' \leq \lambda \operatorname{vol} K(\varepsilon).\end{aligned}$$

Consider $x \in K(\lambda\varepsilon)$, we may assume $x \notin \bigcup C_i$. The minimal cap $C(x) = K \cap H(a \leq t)$ has centre z and width w. It is again convenient to assume (and can be reached by translation) that z lies in the hyperplane $H(a = 0)$. Then $w = t$ as well. The segment $[x, z]$ intersects $\operatorname{bd} K(v \geq \varepsilon)$ at the point y, and let $y \in H(a = w')$. Now setting $A(\tau) = \operatorname{vol}_{d-1} K \cap H(a = \tau)$ we have $\varepsilon = v(y) \leq \int_0^{w'} A(\tau) d\tau$, and $\lambda\varepsilon \geq v(x) = \int_0^w A(\tau) d\tau$. We use again Lemma 1.1:

$$\begin{aligned}\lambda\varepsilon &\geq \int_0^w A(\tau) d\tau = \frac{w}{w'} \int_0^{w'} A\left(\frac{w}{w'}\tau\right) d\tau \\ &\geq \frac{w}{w'} \int_0^{w'} \left(\frac{w}{w'}\right)^{d-1} A(\tau) d\tau \geq \left(\frac{w}{w'}\right)^d \varepsilon.\end{aligned}$$

Thus $\mu = \lambda^{1/d} \geq w/w'$ and $w/w' = \|z - x\| / \|z - y\|$, implying

$$\|z - x\| \leq \mu \|z - y\|.$$

Consider now the cap $C_i = K \cap H(a_i \leq t_i)$ that contains y. Let z_i be the centre of C_i and write y_i for the intersection of $[z_i, x] \cap H(a_i = t_i)$. The line $\operatorname{aff}\{z, x\}$ intersects the hyperplanes $H(a_i = t_i)$, $H(a_i = t_i - w_i)$ respectively at y' and z'. It is easy to check that the points z', z, y, y', x come on this order on $\operatorname{aff}\{z, x\}$. Consequently,

$$\frac{\|x - z_i\|}{\|y_i - z_i\|} = \frac{\|x - z'\|}{\|y' - z'\|} \leq \frac{\|x - z\| + \|z - z'\|}{\|y - z\| + \|z - z'\|} \leq \frac{\|x - z\|}{\|y - z\|} \leq \mu.$$

So indeed $x \in \bigcup_1^m C_i^{\lambda\,\mu}$. □

7 Auxiliary lemmas from probability

We will need an upper and lower bound for the quantity $\operatorname{Prob}\{x \notin K_n\}$ where x is a fixed point of K and the random polytope K_n varies. The lower bound is simple: if $C(x)$ is the minimal cap of x, then clearly

$$\operatorname{Prob}\{x \notin K_n\} \geq \operatorname{Prob}\{X_n \cap C(x) = \emptyset\} = (1 - v(x))^n \qquad (7.1)$$

where X_n is the random sample of n points from K.

We mention at once that this implies the lower bound in Theorem 2.2, or, what is the same, in Theorem 2.1:

Proof of the lower bound in Theorem 2.1. Using the above inequality we get, for all $t > 0$ that

$$\begin{aligned}
\mathbb{E}(K,n) &= \int_K \mathrm{Prob}\{x \notin K_n\} dx \ge \int_K (1-v(x))^n dx \\
&\ge \int_{K(t)} (1-v(x))^n dx \ge \int_{K(t)} (1-t)^n dx \ge (1-t)^n \operatorname{vol} K(t).
\end{aligned}$$

Choosing here $t = 1/n$ gives the lower bound with $c_1 = 1/4$ for instance. Note that c_1 is universal: it does not depend on dimension. $\square$

We need an upper bound on $\mathrm{Prob}\{x \notin K_n\}$:

$$\mathrm{Prob}\{x \notin K_n\} \le 2 \sum_{i=0}^{d-1} \binom{n}{i} \left(\frac{u(x)}{2}\right)^i \left(1 - \frac{u(x)}{2}\right)^{n-i}. \tag{7.2}$$

Proof. We are going to use the following equality which is due to Wendel [78]. Assume M is an 0-symmetric d-dimensional convex body, and let X_n be a random sample of uniform, independent points from M. Then

$$\mathrm{Prob}\{0 \notin M\} = 2^{-n+1} \sum_{i=0}^{d-1} \binom{n-1}{i}. \tag{7.3}$$

(I will give a proof of this result at the end of the section.)

Let $x \in K$ be fixed and define $N(x) = X_n \cap M(x)$. Setting $n(x) = |N(x)|$ we have

$$\begin{aligned}
\mathrm{Prob}\{x \notin K_n\} &= \sum_{m=0}^{n} \mathrm{Prob}\{x \notin K_n | n(x) = m\} \, \mathrm{Prob}\{n(x) = m\} \\
&\le \sum_{m=0}^{n} \mathrm{Prob}\{x \notin N(x) | n(x) = m\} \, \mathrm{Prob}\{n(x) = m\} \\
&= 2 \sum_{m=0}^{n} 2^{-m} \sum_{i=0}^{d-1} \binom{m-1}{i} \mathrm{Prob}\{n(x) = m\}.
\end{aligned}$$

We used Wendel's equality. $\mathrm{Prob}\{n(x) = m\}$ is a binomial distribution with parameter $u = u(x)$. Thus

$$
\begin{aligned}
\text{Prob}\{x \notin K_n\} &\leq 2\sum_{m=0}^{n} 2^{-m} \sum_{i=0}^{d-1} \binom{m-1}{i}\binom{n}{m} u^m (1-u)^{n-m} \\
&= 2\sum_{i=0}^{d-1}\sum_{m=0}^{n} \binom{m-1}{i}\binom{n}{m}\left(\frac{u}{2}\right)^m (1-u)^{n-m} \\
&\leq 2\sum_{i=0}^{d-1}\sum_{m=i+1}^{n} \binom{m}{i}\binom{n}{m}\left(\frac{u}{2}\right)^m (1-u)^{n-m} \\
&= 2\sum_{i=0}^{d-1}\binom{n}{i}\sum_{m=i}^{n} \binom{n-i}{m-i}\left(\frac{u}{2}\right)^m (1-u)^{n-m} \\
&= 2\sum_{i=0}^{d-1}\binom{n}{i}\sum_{k=0}^{n-i} \binom{n-i}{k}\left(\frac{u}{2}\right)^{k+i} (1-u)^{n-i-k} \\
&= 2\sum_{i=0}^{d-1}\binom{n}{i}\left(\frac{u}{2}\right)^{i}\left(1-\frac{u}{2}\right)^{n-i}.
\end{aligned}
$$

□

Proof of Wendel's equality. We start with the following simple fact. Assume $H_1, \dots, H_n$ are hyperplanes in $\mathbb{R}^d$ in general position that is, every d of them has exactly one point in common and no $d+1$ of them intersect. The set $\mathbb{R}^d \setminus \cup_1^n H_i$ is the union of pairwise disjoint, connected open sets, to be called cells. Each cell is a convex polyhedron.

Claim 7.1. *The number of cells is exactly* $\sum_{i=0}^{d}\binom{n}{i}$.

We prove this by induction on d. Everything is clear when $d = 1$. Assume $d > 1$ and the statement is true in R^{d-1}. Let $a \in R^d$ be a unit vector in general position and let C be one of the cells. If $\min\{a \cdot x : x \in C\}$ is finite, then it is reached at a unique vertex of C which is the intersection of some d hyperplanes $H_{i_1}, \dots, H_{i_d}$. There are $\binom{n}{d}$ such minima and each one comes from a different cell. So exactly $\binom{n}{d}$ cells have a finite minimum in direction a. Let K be a number smaller than each of these $\binom{n}{d}$ minima. The rest of the cells are unbounded in direction a, so they all intersect the hyperplane H with equation $a \cdot x = K$. The induction hypothesis can be used in H (which is a copy of R^{d-1}) to show that the number cells, unbounded in direction a is $\sum_{i=0}^{d-1}\binom{n}{i}$. This finishes the proof of the Claim. □

Now for the proof of Wendel's equality. The basic observation is that choosing the points $x_1, \dots, x_n$ and choosing the points $\varepsilon_1 x_1, \dots, \varepsilon_n x_n$ (where each $\varepsilon_i = \pm 1$) are equally likely. So we want to see that, out of the 2^n such choices, how many will not have the origin in their convex hull. If $0 \notin [\varepsilon_1 x_1, \dots, \varepsilon_n x_n]$, then all the $\varepsilon_i x_i$ are contained in the open halfspace $\{x \in \mathbb{R}^d : a \cdot x > 0\}$ for some unit vector $a \in \mathbb{R}^d$. The conditions $a \cdot (\varepsilon_i x_i) > 0$ show that all halfspaces containing each $\varepsilon_i x_i$ ($i = 1, \dots, n$, the ε_i are fixed) have their normal a in the cone

$$\bigcap_1^n \{y \in \mathbb{R}^d : y \cdot (\varepsilon_i x_i) > 0\}.$$

So the question is how many such cones there are. Or, to put it differently, when you delete the hyperplanes $H_i = \{y \in \mathbb{R}^d : y \cdot x_i = 0\}$ $i = 1, \ldots, n$ from R^d you get pairwise disjoint open cones C_α; how many such cones are there? Surprisingly, this number is independent of the the position of the x_i (if they are in general position and, in the given case, they are). We claim that this number is equal to

$$2 \sum_{i=0}^{d-1} \binom{n-1}{i}.$$

This will, of course, prove Wendel's equality (7.3).

Consider the hyperplane $H^* = \{y \in \mathbb{R}^d : y \cdot x_n = 1\}$. The cones C_α come in pairs, C_α together with $-C_\alpha$ and only one of them intersects H^*. So the question is this. If you delete the hyperplanes H_i, $i = 1, \ldots, n-1$ from H^*, how many connected components are left? This is answered by the Claim: there are exactly

$$\sum_{i=0}^{d-1} \binom{n-1}{i}$$

such cells. □

8 Proof of Theorem 2.1

We only have to prove the upper bound. We start with the integral representation of $\mathbb{E}(K, n)$ and use the upper bound from (7.2):

$$\begin{aligned}
\mathbb{E}(K, n) &= \int_K \operatorname{Prob}\{x \notin K\} dx \\
&\leq \int_K 2 \sum_{i=0}^{d-1} \binom{n}{i} \left(\frac{u(x)}{2}\right)^i \left(1 - \frac{u(x)}{2}\right)^{n-i} dx \\
&\leq 2 \sum_{i=0}^{d-1} \binom{n}{i} \int_K \left(\frac{u(x)}{2}\right)^i \left(1 - \frac{u(x)}{2}\right)^{n-i} dx.
\end{aligned}$$

K is the disjoint union of the sets for $\lambda = 1, 2, \ldots, n$

$$K_\lambda = K((\lambda - 1)/n \leq u < \lambda/n).$$

We integrate separately on each K_λ using that, on K_λ, $u(x) < \lambda/(2n)$ and $1 - u(x)/2 \leq \exp\{-(\lambda - 1)/(2n)\}$. Thus

$$\int_{K_\lambda} \left(\frac{u(x)}{2}\right)^i \left(1 - \frac{u(x)}{2}\right)^{n-i} dx \ll \left(\frac{\lambda}{2n}\right)^i \exp\{-(\lambda - 1)/4\} \operatorname{vol} K(u \leq \lambda/n).$$

We continue the inequality for $\mathbb{E}(K,n)$:

$$\begin{aligned}
\mathbb{E}(K,n) &\ll 2\sum_{i=0}^{d-1}\binom{n}{i}\sum_{\lambda=1}^{n}\left(\frac{\lambda}{2n}\right)^{i}\exp\{-(\lambda-1)/4\}\operatorname{vol}K(u\le\lambda/n)\\
&\ll \sum_{\lambda=1}^{n}\sum_{i=0}^{d-1}\binom{n}{i}\left(\frac{\lambda}{2n}\right)^{i}\exp\{-(\lambda-1)/4\}\operatorname{vol}K(u\le\lambda/n)\\
&= \sum_{\lambda=1}^{\Lambda}..+\sum_{\lambda=\Lambda+1}^{n}..
\end{aligned}$$

where $\Lambda=(2d)^{-2d}\varepsilon_0 n=8^{-d}d^{-2d-1}n$ which we take for an integer. Note that $\binom{n}{i}\left(\frac{\lambda}{2n}\right)^{i}\ll\lambda^{i}$. So we have, using Lemma 4.12 and Corollary 3.2

$$\begin{aligned}
\sum_{\lambda=1}^{\Lambda}.. &\ll \sum_{\lambda=1}^{\Lambda}d\lambda^{d-1}\exp\{-(\lambda-1)/4\}\operatorname{vol}K(v\le(2d)^{d}\lambda/n)\\
&\ll \sum_{\lambda=1}^{\Lambda}\lambda^{d-1}\exp\{-(\lambda-1)/4\}\lambda\operatorname{vol}K(v\le 1/n)\\
&\ll \operatorname{vol}K(v\le 1/n).
\end{aligned}$$

Estimating the second sum is simpler since one can use the trivial $\operatorname{vol}K(u\le\lambda/n)\le 1$ and $1/n\le\operatorname{vol}K(u\le 1/n)$ inequalities:

$$\begin{aligned}
\sum_{\Lambda+1}^{n}.. &\ll \sum_{\Lambda+1}^{n}\lambda^{d-1}\exp\{-(\lambda-1)/4\}\operatorname{vol}K(v\le(2d)^{d}\lambda/n)\\
&\ll \sum_{\Lambda+1}^{n}\lambda^{d-1}\exp\{-(\lambda-1)/4\}\\
&\ll \operatorname{vol}K(v\le 1/n).
\end{aligned}$$

Thus we have $\mathbb{E}(K,n)\ll\operatorname{vol}K(1/n)$. □

Remark. This proof comes from the paper Bárány, Larman 1988.

9 Expectation of $f_k(K_n)$

The following simple identity is due to Efron [27] : for $K\in\mathcal{K}_1$

$$Ef_0(K_n)=nE(K,n-1). \tag{9.1}$$

The proof is straightforward:

$$\begin{aligned}
Ef_0(K_n) &= \sum_{i=1}^{n}\operatorname{Prob}\{x_i\text{ is a vertex of }K_n\}\\
&= n\operatorname{Prob}\{x_1\text{ is a vertex of }K_n\}=n\operatorname{Prob}\{x_1\notin[x_2,\dots,x_n]\}\\
&= n\operatorname{Prob}\{x\notin K_{n-1}\}=nE(K,n-1)
\end{aligned}$$

where the last probability is taken with both K_{n-1} and x varying.

Theorem 2.2 determines then the order of magnitude of $Ef_0(K_n)$ as well. The expectation of $f_k(K_n)$ for $k = 1, \dots, d-1$ must be close to that of $Ef_0(K_n)$ since, as n goes to infinity, K_n looks locally like a "random" triangulation of $\mathbb{R}^{d-1}$ where you don't expect vertices of high degree. We have the following result from Bárány [7].

Theorem 9.1. *For large enough n and for all $K \in \mathcal{K}_1$ and for all $k = 0, 1, \dots, d-1$*

$$n \operatorname{vol} K(1/n) \ll Ef_k(K_n) \ll n \operatorname{vol} K(1/n).$$

The lower bound in case $k = 0$ follows, via Efron's identity, from the lower bound in Theorem 2.1. The following fact simplifies the proof of Theorem 9.1.

Lemma 9.2. *For all $0 \le i < j \le d-1$*

$$f_i(K_n) \le \binom{j+1}{i+1} f_j(K_n).$$

Proof. Almost surely K_n is a simplicial polytope. Double counting the pairs (F_i, F_j) where F_i and F_j are faces of dimension i and j of K_n with $F_i \subset F_j$ we have

$$f_i(K_n) = \sum_{F_i} 1 \le \sum_{(F_i, F_j)} 1 = \binom{j+1}{i+1} f_j(K_n).$$

□

So we see that for the upper bound in Theorem 9.1 it suffices to show the following:

Lemma 9.3. *For large enough n and for all $K \in \mathcal{K}_1$*

$$Ef_{d-1}(K_n) \ll n \operatorname{vol} K(1/n).$$

At this point we state an interesting corollary to the economic cap covering theorem which has no direct application in what follows. Some preparation is necessary.

Assume $x_1, \dots, x_k \in K$, set $L = \operatorname{aff}\{x_1, \dots, x_k\}$ and define

$$v(L) = \max\{v(x) \ : x \in L\}.$$

We write K^k for the set of ordered k-tuples $(x_1, \dots, x_k)$ with $x_i \in K$ for each i.

Corollary 9.4. *If $K \in \mathcal{K}_1$, $k = 1, 2, \dots, d$ and $\varepsilon \le \varepsilon_0$, then*

$$\{(x_1, \dots, x_k) \in K^k \ : v(L) \le \varepsilon\} \subset \bigcup_1^m (C_i, \dots, C_i)$$

where $C_1, \dots, C_m$ is the set of caps from the previous theorem.

Proof. This is where we use part (iii) of Theorem 3.1. If $v(L) \le \varepsilon$, then L and $K(v > \varepsilon)$ are disjoint. By separation, there is a halfspace H, containing L which is disjoint from $K(v > \varepsilon)$. Then the cap $C = K \cap H$ is also disjoint from $K(v > \varepsilon)$. Clearly, C contains $x_1, \dots, x_k$. Consider now C_i from the cap covering with $C \subset C_i$: it is evident that

$$(x_1, \dots, x_k) \in (C, \dots, C) \subset (C_i, \dots, C_i).$$

□

We mention that the Corollary implies the following estimate:

$$\text{meas}\{(x_1, \dots, x_k) \in K^k \ : v(L) \le \varepsilon\} \le \varepsilon^{k-1} K(\varepsilon).$$

Indeed, the measure of $\bigcup_1^m (C_i, \dots, C_i)$ is $\ll m\varepsilon^k \ll \varepsilon^{k-1}K(\varepsilon)$ by the economic cap covering theorem.

10 Proof of Lemma 9.3

Given $x_{i_1}, \dots, x_{i_d}$ let $V = V(x_{i_1}, \dots, x_{i_d})$ denote the volume of the smaller cap cut off by $L = \text{aff}\{x_{i_1}, \dots, x_{i_d}\}$ from K. This is well defined almost surely since L is a hyperplane with probability one. Write $\mathcal{F}$ for the set of facets of K_n. Then we have

$$\begin{aligned} Ef_{d-1}(K_n) &= \sum_{1 \le i_1 < \dots < i_d \le n} \text{Prob}\{[x_{i_1}, \dots, x_{i_d}] \in \mathcal{F}\} \\ &= \binom{n}{d} \text{Prob}\{[x_1, \dots, x_d] \in \mathcal{F}\} \\ &= \binom{n}{d} \int_K \dots \int_K [(1-V)^{n-d} + V^{n-d}] dx_1 \dots dx_d. \end{aligned}$$

The last equality follows form the fact that $[x_1, \dots, x_d]$ is a facet of K_n if and only if all other x_i lie on one side of L.

Next we split the domain of integration into two parts: K_1 is the subset of K^d where the function V is smaller than $(c \ln n)/n$, and K_2 is where $V \ge (c \ln n)/n$. The constant c will be specified soon. Clearly $V \le 1/2$. The integrand over K_2 is estimated as follows:

$$\begin{aligned} (1-V)^{n-d} + V^{n-d} &\le \exp\{-(n-d)V\} + 2^{-(n-d)} \\ &\le 2\exp\{-(n-d)(c \ln n)/n\} \\ &= 2n^{-c(n-d)/n} \end{aligned}$$

which is smaller than $n^{-(d+1)}$ if $c = 2(d+1)$ (and $n > 2d$ which we can assume). Then the contribution of the integral on K_2 to $Ef_{d-1}(K_n)$ is at most $1/n$ so it is very small since, trivially, $Ef_{d-1}(K_n)$ is at least one.

Now let h be an integer with $2^{-h} \le (c \ln n)/n$. For each such h let $\mathcal{M}_h$ be the collection of caps $\{C_1, \dots, C_{m(h)}\}$ forming the economic cap covering from Theorem 3.1 with $\varepsilon = 2^{-h}$.

Assume now that $(x_1,\dots,x_d)\in K_1$. We will denote by $C(x_1,\dots,x_d)$ the cap cut off from K by the hyperplane $\operatorname{aff}\{x_1,\dots,x_d\}$, clearly $\operatorname{vol} C(x_1,\dots,x_d) = V(x_1,\dots,x_d)$. We associate with $(x_1,\dots,x_d)$ the maximal h such that, for some $C_i\in\mathcal{M}_h$, $C(x_1,\dots,x_d)\subset C_i$. It follows that

$$V(x_1,\dots,x_d)\le \operatorname{vol} C_i \ll 2^{-h} \tag{10.1}$$

and, by the maximality of h,

$$V(x_1,\dots,x_d)\ge 2^{-h-1} \tag{10.2}$$

since otherwise $C(x_1,\dots,x_d)$ would be contained in a cap from $\mathcal{M}_{h+1}$. We integrate over K_1 by integrating each $(x_1,\dots,x_d)$ on its associated C_i. It is very easy to estimate the integrand on C_i:

$$(1-V)^{n-d}+V^{n-d}\le 2(1-V)^{n-d}\le 2(1-2^{-h-1})^{n-d}\le 2\exp\{-(n-d)2^{-h-1}\}.$$

Thus the integral on $C_i\in\mathcal{M}_h$ is bounded by

$$2\exp\{-(n-d)2^{-h-1}\}(\operatorname{vol} C_i)^d \ll \exp\{-(n-d)2^{-h-1}\}(2^{-h})^d$$

as all the x_i come from C_i. Summing this for all $C_i\in\mathcal{M}_h$ and all $h\ge h_0$ where $h_0=\lfloor (c\ln n)/n\rfloor$ we get that

$$\begin{aligned}
Ef_{d-1}(K_n) &\ll \binom{n}{d}\sum_{h_0}^{\infty}\sum_{C_i\in\mathcal{M}_h}\exp\{-(n-d)2^{-h-1}\}2^{-hd}\\
&\ll \binom{n}{d}\sum_{h_0}^{\infty}\exp\{-(n-d)2^{-h+1}\}2^{-hd}|\mathcal{M}_h|\\
&\ll \binom{n}{d}\sum_{h_0}^{\infty}\exp\{-(n-d)2^{-h+1}\}2^{-h(d-1)}\operatorname{vol} K(2^{-h})
\end{aligned}$$

where the last inequality follows from (3.1).

The rest of the proof is a direct computation. We sum first for $h\ge h_1$ where h_1 is defined by $2^{-h_1}\le 1/n<2^{-h_1+1}$. The sum from h_1 to infinity is estimated via:

$$\begin{aligned}
\sum_{h_1}^{\infty}.. &\le \sum_{h_1}^{\infty}\exp\{-(n-d)2^{-h+1}\}2^{-h(d-1)}\operatorname{vol} K(1/n)\\
&\le \operatorname{vol} K(1/n)\sum_{h_1}^{\infty}2^{-h(d-1)}\le n^{-(d-1)}\operatorname{vol} K(1/n).
\end{aligned}$$

When $h_0\le h<h_1$ we set $h=h_1-k$ so k runs from 1 to $k_1=\log_2\ln n+\ln c$. Corollary 3.2 shows that

$$\operatorname{vol} K(2^{-h})\le \operatorname{vol} K(2^k/n)\ll 2^k\operatorname{vol} K(1/n).$$

Thus

$$\begin{aligned}
\sum_{h_0}^{h_1-1} .. &\ll \sum_{k=1}^{k_1} \exp\{-(n-d)2^{-h_1+k-1}\} 2^{(-h_1+k)(d-1)} 2^k \operatorname{vol} K(1/n) \\
&\ll n^{-(d-1)} \operatorname{vol} K(1/n) \sum_{k=1}^{k_1} \exp\{-(n-d)2^{k-1}/n\} 2^{kd} \\
&\ll n^{-(d-1)} \operatorname{vol} K(1/n) \sum_{k=1}^{\infty} \exp\{-2^{k-2} + dk \ln 2\} \\
&\ll n^{-(d-1)} \operatorname{vol} K(1/n)
\end{aligned}$$

where the last step is easily justified. □

Remark. This proof shows that $Ef_{d-1}(K_n) \ll \operatorname{vol} K(1/n)$. Then $Ef_0(K_n) \ll \operatorname{vol} K(1/n)$ follows from Lemma 9.2. Efron's identity implies that $Ef_0(K_n) \approx E(K, n)$. Thus the proof of Lemma 9.3 is a new proof of the upper bound in Theorem 2.2. We mention further that the proof of $Ef_{d-1}(K_n) \ll \operatorname{vol} K(1/n)$ presented here is new and uses the cap-covering theorem in a different and apparently more effective way than the old proof from Bárány [7].

11 The volume of the wet part

As we have seen in the previous sections, the order of magnitude of $E(K, n)$ and $Ef_k(K_n)$, resp. is equal to that of $\operatorname{vol} K(1/n)$ and $n \operatorname{vol} K(1/n)$. In this section we state several results on the function $t \to \operatorname{vol} K(t)$. In particular, we are interested in the cases when this function is maximal and minimal.

Theorem 11.1. *Assume $K \in \mathcal{K}_1$ and $t \geq 0$ Then*

$$\operatorname{vol} K(t) \gg t \left(\ln \frac{1}{t}\right)^{d-1}. \tag{11.1}$$

This theorem is best possible (apart from the implied constant) as shown by polytopes. We need the following definition. A *tower* of a polytope P is a chain of faces $F_0 \subset F_1 \subset \ldots, \subset F_{d-1}$ where F_i is i-dimensional. Write $T(P)$ for the number of towers of P.

Theorem 11.2. *Assume $P \in \mathcal{K}_1$ is a polytope and $t \geq 0$. Then*

$$\operatorname{vol} P(t) = \frac{T(P)}{d^d(d-1)!} t \left(\ln \frac{1}{t}\right)^{d-1} (1 + o(1)).$$

We will only prove a simpler statement. Namely, let Δ_i, $i = 1, \ldots, m(P)$ be simplices triangulating P. Then for all positive $t \leq e^{-d+1} \min \operatorname{vol} \Delta_i$

$$\operatorname{vol} P(t) \ll m(P) t \left(\ln \frac{1}{t}\right)^{d-1} \tag{11.2}$$

The implied constant depends on dimension only.

Concerning the upper bound on the volume of the wet part, the affine isoperimetric inequality of Blaschke [19] expresses an extremal property of ellipsoids (cf. Schütt [69] as well).

Theorem 11.3. *For all convex bodies in* $\mathcal{K}_1$

$$\limsup_{t\to 0} t^{-\frac{2}{d+1}} \operatorname{vol} K(t)$$

is maximal for ellipsoids, and only for ellipsoids.

Corollary 11.4. *For all convex bodies* $K \in \mathcal{K}_1$*, and for all* $t \in (0, t_0)$

$$t\left(\ln \frac{1}{t}\right)^{d-1} \ll \operatorname{vol} K(t) \ll t^{\frac{2}{d+1}},$$

where the implied constants depend only on dimension.

In case of smooth convex bodies in $\mathbb{R}^d$ $\operatorname{vol} K(t)$ can be computed with high precision:

Theorem 11.5. *For a convex body* $K \in \mathcal{K}_1$ *with* $\mathcal{C}^2$ *boundary and positive curvature* κ *at each point of* $\operatorname{bd} K$

$$\operatorname{vol} K(t) = c(d) t^{\frac{2}{d+1}} \int_{\operatorname{bd} K} \kappa^{\frac{1}{d+1}} dz (1 + o(1)).$$

The above results show that one can determine $\operatorname{vol} K(t)$ for smooth convex bodies and for polytopes. What happens between these two extreme classes of convex bodies is not a mystery: it is the usual unpredictable behaviour. Using the above results and a general theorem of Gruber [32] one can show the following.

Theorem 11.6. *Assume* $\omega(t) \to 0$ *and* $\Omega(t) \to \infty$ *as* $t \to 0$*. Then for most (in the Baire category sense) convex bodies in* $\mathcal{K}_1$ *one has, for an infinite sequence* $t \to 0$

$$\operatorname{vol} K(t) \geq \omega(t) t^{\frac{2}{d+1}},$$

and also, for another infinite sequence $t \to 0$*,*

$$\operatorname{vol} K(t) \leq \Omega(t) t \left(\ln \frac{1}{t}\right)^{d-1}.$$

We will only prove Theorems 11.1 and inequality (11.2).

12 Determination of $E(K,n)$ and $Ef_s(K_n)$

The asymptotic determination of these expectations has been achieved only when K is a polytope and when K has smooth boundary. Of course, Corollary 11.4 and Theorem 2.1 imply that

$$\frac{1}{n}(\ln n)^{d-1} \ll E(K,n) \ll n^{-2/(d+1)}$$

for all $K \in \mathcal{K}_1$, and analogous inequalities hold for $f_s(K_n)$.

For the upper bound on $E(K,n)$ more precise information is available: a result of Groemer [29] says the following.

Theorem 12.1. *Among all convex bodies in $\mathcal{K}_1$, $E(K, n)$ is maximal for ellipsoids, and only for ellipsoids.*

For smooth convex bodies $Ef_s(K_n)$ has been determined by Bárány, Schütt, and Reitzner:

Theorem 12.2. *Assume $K \in \mathcal{C}_1$ has positive Gauss curvature at every point on its boundary. Then, for all $s = 0, 1, \dots, d-1$,*

$$Ef_s(K_n) = c(d,s)n^{\frac{d-1}{d+1}} \int_{\operatorname{bd} K} \kappa^{\frac{1}{d+1}} dz(1 + o(1)),$$

where $c(d, s)$ is a positive constant.

The constants $c(d, s)$ come from integrals that represent various moment of random simplices. Most of them are not known explicitly. For polytopes the following result holds.

Theorem 12.3. *Assume $K \in \mathcal{K}_1$ is a polytope and $s = 0, 1, \dots, d-1$. then*

$$Ef_s(K_n) = b(d,s)T(P)(\ln n)^{d-1} + O(\ln^{d-2} \ln \ln n),$$

where $b(d, s)$ is a positive constant.

This is a difficult theorem whose proof is based on work of Affentranger and Wieacker[1] (for simple polytopes) and Bárány and Buchta [12] (for general polytopes). The latter result is proved by showing that most of the vertices (and other faces) of K_n are concentrated in certain small simplices associated with the towers of K. The difference between the polytope and smooth case is shown here very spectacularly: In the smooth case, the vertices are distributed almost evenly near the boundary of K, while for a polytope they are concentrated in the small simplices associated with the towers of K. We mention that Reitzner [54] gives an interesting joint treatment of the smooth and polytope case, based on a Blaschke-Petkantschin type integral formula.

13 Proof of Theorem 11.1

We start with introducing notation. Fix $a \in S^{d-1}$ and let $H(a = t_0)$ be the hyperplane whose intersection with K has maximal $(d-1)$-dimensional volume among all hyperplanes $H(a = t)$. Assume the width of K in direction a is at most $2t_0$: if this were not the case we would take $-a$ instead of a. As a will be fixed during this proof we simply write $H(t) = H(a = t)$. Assume further that $H(0)$ is the tangent hyperplane to K. Define

$$Q(t) = H(t) \cap K \text{ and } q(t) = \operatorname{vol}_{d-1} Q(t).$$

The choice of t_0 insures that for $t \in [0, t_0]$

$$q(t) \geq \left(\frac{t}{t_0}\right)^{d-1} q(t_0) \text{ and } 2t_0 q(t_0) \geq \operatorname{vol} K = 1. \qquad (13.1)$$

Claim 13.1. *For $\varepsilon > 0$ and for $t \in (0, t_0]$*

$$Q(t)\left(u_{Q(t)} \le \frac{\varepsilon}{2t}\right) \subset K(u_K \le \varepsilon) \cap H(t)$$

Proof. We are going to show that $x \in H(t) \cap K$ implies $u_K(x) \le 2tu_{Q(t)}(x)$. This of course proves the lemma.

Note first that $M(x)$ lies between hyperplanes $H(0)$ and $H(2t)$. Thus

$$u(x) = \int_0^{2t} \mathrm{vol}_{d-1}(M(x) \cap H(\tau) d\tau \le 2t\, \mathrm{vol}_{d-1}(M(x) \cap H(t))$$

since $M(x)$ is centrally symmetric so its largest section is the middle one. It is easy to check from the definition of $M(x)$ that

$$M(x) \cap H(t) = M_{Q(t)}(x).$$

Consequently $u(x) \le 2t \,\mathrm{vol}\,_{d-1} M_{Q(t)}(x) = 2tu_{Q(t)}(x)$ $\square$

We show next that for $\varepsilon \in (0, 1]$

$$\mathrm{vol}\, K(u \le \varepsilon) \gg \varepsilon \left(\ln \frac{1}{\varepsilon}\right)^{d-1}. \tag{13.2}$$

Then Lemma 4.12 implies that, for $\varepsilon \le (2d)^{-2d}\varepsilon_0$

$$\mathrm{vol}\, K(v \le \varepsilon) \ge \mathrm{vol}\, K(u \le (2d)^{-d}\varepsilon) \gg \varepsilon \left(\ln \frac{1}{\varepsilon}\right)^{d-1}.$$

When $\varepsilon \ge (2d)^{-2d}\varepsilon_0$ the statement of the theorem follows from the fact that $\varepsilon \to \mathrm{vol}\, K(v \le \varepsilon)$ is an increasing function of ε.

We prove (13.2) by induction on d. The case $d = 1$ trivial. We will need the induction hypothesis in its invariant form (4.1): for $Q \in \mathcal{K}^{d-1}$ and for $\eta \in (0, 1]$

$$\frac{\mathrm{vol}\, Q(u_Q \le \eta \,\mathrm{vol}\, Q)}{\mathrm{vol}\, Q} \ge c_{d-1}\eta \left(\ln \frac{1}{\eta}\right)^{d-2}.$$

We have

$$\begin{aligned}
\mathrm{vol}\, K(u \le \varepsilon) &\ge \mathrm{vol}\, K(u \le \varepsilon) \cap H(a \le t) \\
&= \int_0^{t_0} \mathrm{vol}\,_{d-1} K(u \le \varepsilon) \cap H(t) dt \\
&\ge \int_0^{t_0} \mathrm{vol}\,_{d-1} Q(t)(u_{Q(t)} \le \varepsilon/(2t)) dt
\end{aligned}$$

according to Claim 13.1. Define $\eta = \eta(t) = \varepsilon/(2tq(t))$ and let t_1 be the unique solution to $\eta(t) = 1$ between 0 and t_0. Then $\eta(t) \in (0, 1]$ for $t \in [t_1, t_0]$, so the induction hypothesis implies that, for $t \in [t_1, t_0]$,

$$\mathrm{vol}\,_{d-1} Q(t)(u_{Q(t)} \le \eta q(t)) \ge c_{d-1} q(t) \eta \left(\ln \frac{1}{\eta}\right)^{d-2} = c_{d-1} \frac{\varepsilon}{2t} \left(\ln \frac{2tq(t)}{\varepsilon}\right)^{d-2}.$$

It follows from (13.1) that

$$\frac{2tq(t)}{\varepsilon} \geq \frac{2t^d q(t_0)}{\varepsilon t_0^{d-1}}.$$

The left hand side is larger than 1 on the interval $(t_2, t_0]$ where $t_2 \in [t_1, t_0]$ is defined as follows. The function $t \to 2t^d q(t_0)/(\varepsilon t_0^{d-1})$ is increasing on $[t_1, t_0]$. In view of (13.1), it is larger than $\frac{1}{\varepsilon}$ at $t = t_0$. By (13.1) again, at $t = t_1$ it is smaller than one. Let $t_2 \in (t_1, t_0)$ be the unique number with $2t_2^d q(t_0)/(\varepsilon t_0^{d-1}) = 1$.

We continue with $\operatorname{vol} K(u \leq \varepsilon)$:

$$\begin{aligned} \operatorname{vol} K(u \leq \varepsilon) &\geq \int_{t_1}^{t_0} c_{d-1} \frac{\varepsilon}{2t} \left(\ln \frac{2tq(t)}{\varepsilon} \right)^{d-2} \\ &\geq \int_{t_2}^{t_0} c_{d-1} \frac{\varepsilon}{2t} \left(\ln \left(\frac{2t^d q(t_0)}{\varepsilon t_0^{d-1}} \right) \right)^{d-2} dt, \end{aligned}$$

Finally, the last integral can be determined. We have, with $\mu = \ln \frac{2q(t_0)}{\varepsilon t_0^{d-1}}$,

$$\begin{aligned} \operatorname{vol} K(u \leq \varepsilon) &\geq c_{d-1} \frac{\varepsilon}{2} \int_{t_2}^{t_0} \frac{1}{t} (d \ln t + \mu)^{d-2} d\tau \\ &= \frac{\varepsilon c_{d-1}}{2d(d-1)} (d \ln t_0 + \mu)^{d-1} \geq \frac{c_{d-1}}{2d(d-1)} \varepsilon \left(\ln \frac{1}{\varepsilon} \right)^{d-1} \end{aligned}$$

where the last inequality follows from (13.1). $\square$

Remark. This is the only proof known for Theorem 11.1 and it comes from Bárány, Larman 1988. The best possible constant in the inequality probably goes with the simplex. Note that in the proof we made full use of the two-way street between minimal caps and M-regions.

14 Proof of (11.2)

This is a repetition of the previous computation, just the inequalities go the other direction. We need to know $\operatorname{vol} \Delta(v \leq t)$ where Δ is the d-dimensional simplex:

Lemma 14.1. *For all $t \leq e^{-d+1}$*

$$\frac{\operatorname{vol} \Delta(v \leq t \operatorname{vol} \Delta)}{\operatorname{vol} \Delta} \ll t \left(\ln \frac{1}{t} \right)^{d-1}.$$

We remark that the function on the left hand side of this inequality increases with t while the one on the right hand side increases on $[0, e^{-d+1}]$ and decreases afterwards. That is the reason for the condition $t \leq e^{-d+1}$.

Proof. We may assume that Δ is the simplex whose vertices are the origin and the d basis vectors, $e_1, \ldots, e_d$ of $\mathbb{R}^d$. We give an upper bound on the volume of the wet part which lies below the hyperplane H with equation $\sum \xi_i \leq d/(d+$

1). Denote this part by Δ_0. The minimal cap $C(x)$ of $x = (\xi_1, \dots, \xi_d) \in \Delta_0$ is a simplex with vertices $0, d\xi_1 e_1, \dots, d\xi_d e_d$, because x is the centre of gravity of the section. Then $v(x) = \frac{d^d}{d!} \prod \xi_i$. It follows then that $\operatorname{vol} \Delta_0$ is less than the volume of the set

$$S(T) = \{x \in \mathbb{R}^d : \prod \xi_i \le T,\ \xi_i \in [0,1],\ i = 1, \dots, d\},$$

where $T = \frac{d!}{d^d} t$. The volume of $S(T)$ can be determined precisely: for all $T \in (0,1]$

$$\operatorname{vol} S(T) = T \sum_0^{d-1} \frac{1}{j!} \left(\ln \frac{1}{T} \right)^j .$$

This can be proved by a simple induction on d, we omit the details.

To finish the proof of the claim note that H is parallel with the facet opposite to the vertex at the origin. Also, H contains the centre of gravity of Δ.

Finally, let A be the affine transformation, of determinant one, that carries Δ to a regular simplex. Then $d+1$ congruent copies of $A\Delta_0$, one for each vertex of $A\Delta$ completely cover the wet part of $A\Delta$. So $\operatorname{vol} \Delta(v \le t \operatorname{vol} \Delta)$ is at most $d+1$ times $\operatorname{vol} \Delta_0$. □

Now we turn to the proof of inequality (11.2).

Assume the polytope P is triangulated by simplices Δ_i $i = 1, \dots, m(P)$. Clearly, if $v(x) \le t$, then $v_{\Delta_i}(x) \le t$ for the simplex containing x. Consequently, for all $t \le e^{-d+1} \min \operatorname{vol} \Delta_i$,

$$\begin{aligned} \operatorname{vol} P(v \le t) &\le \sum_1^{m(P)} \operatorname{vol} \Delta_i (v_{\Delta_i} \le t) \le \sum t \left(\ln \frac{\operatorname{vol} \Delta_i}{t} \right)^{d-1} \\ &\le m(P) t \left(\ln \frac{1}{t} \right)^{d-1} . \end{aligned}$$

□

Remarks. These proofs are from Bárány, Larman [14] and from Bárány [7].

15 Proof of Greomer's theorem

We will show Theorem 12.1 (which is Groemer's theorem) in the following, equivalent form.

Theorem 15.1. *Among all convex bodies in $\mathcal{K}_1$, $E \operatorname{vol}(K_n)$ is minimal for ellipsoids, and only for ellipsoids.*

The proof is a neat example of symmetrization. Symmetrization is given by a line L in $\mathbb{R}^d$, and the $d-1$-dimensional subspace, $L^\perp$ orthogonal to it. The symmatral, K^* of a set $K \in \mathcal{K}$ is obtained from K by translating every chord of K, within its own line so that its midpoint lies in $L^\perp$. It is not difficult to see that $K^* \in \mathcal{K}$, again. It is clear that K and K^* have the same volume. We will need the following fact: For every $K \in \mathcal{K}$ there is a sequence of symmetrizations that tend to a Euclidean ball. (A proof can be found in Schneider's book The Brunn-Minkowski theory.)

Given $K \in \mathcal{K}$ and a line $L \in \mathbb{R}^d$, the *mid-point set*, $M(K, L)$, is defined as the set of midpoints of all the chords of K that are parallel with L. We will need the following result.

Lemma 15.2. *Under the above conditions, K is an ellipsoid if and only if $M(K, L)$ is contained in a hyperplane.*

Proof. If K is an ellipse, then $M(K, L)$ lies indeed in a hyperplane. For the opposite direction, the condition implies that, for every line L, symmetrization with respect to L is an affine transformation. Consider the smallest volume ellipsoid, E say, that contains K.

There is nothing to do if $K = E$. If $K \neq E$, then consider the sequence of symmetrizations of K tending to B, the Euclidean ball (of the same volume as K). The sequence of symmatrals is just $K, A_1K, A_2K, \dots$ where each A_i is an affine transformation. Then, for a suitably large m, A_mK lies in the a ball B', concentric with B and only slightly larger, and for m large enough, $\operatorname{vol} B' < \operatorname{vol} E$. Then $A_m^{-1}B'$ is an ellipsoid, containing K having smaller volume than E. A contradiction with the definition of E. $\square$

One more piece of preparation is needed before we can start the proof of Theorem 15.1. Assume $X \subset \mathbb{R}^d$ is convex compact, and let X^0 denote the projection of X onto the hyperplane $x_d = 0$. For $a = (a_1, \dots, a_{d-1}, 0) \in X^0$ we define the upper function as $\overline{x}(a) = \sup\{x_d : (a_1, \dots, a_{d-1}, x_d) \in X\}$ and the lower function as $\underline{x}(a) = \inf\{x_d : (a_1, \dots, a_{d-1}, x_d) \in X\}$. Trivially, $\overline{x}$ is a concave, $\underline{x}$ is a convex function on X^0 and $\overline{x}(a) \leq \underline{x}(a)$ at every $a \in X^0$. Conversely, given functions $\overline{x}$ and $\underline{x}$ on a convex set in the hyperplane $x_d = 0$ with these properties, there is a unique convex set $X \subset \mathbb{R}^d$, whose upper and lower functions are the given ones.

Proof of Groemer's theorem. We first fix points $a_1, \dots, a_n$ in the hyperplane $x_d = 0$. Given $Z = (z_1, \dots, z_n) \in \mathbb{R}^n$, define $C(Z) = \operatorname{conv}\{(a_1, z_1), \dots, (a_n, z_n)\}$ and let $V(Z) = \operatorname{vol} C(Z)$.

Lemma 15.3. *Under the previous condition assume that $Z, Y \in \mathbb{R}$. Then*

$$V\left(\frac{1}{2}(Z + Y)\right) \leq \frac{1}{2}V(Z) + \frac{1}{2}V(Y).$$

Proof. Let $\overline{z}, \underline{z}$, and $\overline{y}, \underline{y}$ respectively, be the upper and lower functions of $C(Z)$ and $C(Y)$. Define $\overline{x}(a) = \frac{1}{2}\overline{z}(a) + \frac{1}{2}\overline{y}(a)$ and $\underline{x}(a) = \frac{1}{2}\underline{z}(a) + \frac{1}{2}\underline{y}(a)$. It is clear that $\overline{x}$ and $\underline{x}$ are the upper and lower functions of a convex set $X \subset \mathbb{R}^d$ for which X^0 coincides with the convex hull of the a_i. Moreover, the definition directly implies that

$$\underline{x}(a_i) \leq \frac{1}{2}(z_i + y_i) \leq \overline{x}(a_i)$$

for all i, so that $C(\frac{1}{2}(Z+Y)) \subset X$. Then $V(\frac{1}{2}(Z+Y)) \le \operatorname{vol} X$. Further,

$$\begin{aligned}
\operatorname{vol} X &= \int (\overline{x}(a) - \underline{x}(a))da \\
&= \int \frac{1}{2}(\overline{z}(a) - \underline{z}(a))da + \int \frac{1}{2}(\overline{y}(a) - \underline{y}(a))da \\
&= \frac{1}{2}(V(Z) + V(Y)).
\end{aligned}$$

This completes the proof of the lemma. □

For the next step of the proof we assume that, together with each point a_i, ($i \in [m]$) an interval $L_i = \{z_i : |z_i - p_i| \le l_i\}$ is given. Then $P = (p_1, \dots, p_n) \in \mathbb{R}^n$ and we set

$$W(P) = \int_{L_i} \dots \int_{L_n} V(Z) dz_1 \dots dz_n.$$

Lemma 15.4. *$W(P) \ge W(0)$ with strict inequality if $V(P) \ne 0$.*

Proof. Substituting $u_i = p_i - z_i$ for z_i in the integral defining $W(P)$ gives

$$W(P) = \int_{|u_i| \le l_1} \dots \int_{|u_n| \le l_n} V(P+U) du_1 \dots du_n.$$

It is straightforward to see that here $V(P+U)$ can be replaced by $V(P-U)$, and then by $V(U-P)$ without changing the value of the integral. Thus

$$\begin{aligned}
W(P) &= \int_{|u_i| \le l_1} \dots \int_{|u_n| \le l_n} \frac{1}{2}(V(U+P) + V(U-P)) dz_1 \dots dz_n \\
&\ge \int_{|u_i| \le l_1} \dots \int_{|u_n| \le l_n} V(U) dz_1 \dots dz_n = W(O),
\end{aligned}$$

where the last inequality follows from Lemma 15.3. If $V(P) \ne 0$, then the inequality $\frac{1}{2}(V(U+P) + V(U-P)) \ge V(U)$ is strict at $U = 0$. □

Finally, let $C \in \mathcal{K}$ be a convex body for which $E \operatorname{vol} K_n$ is minimal among all convex bodies in $\mathcal{K}_1$. (The existence of such a body follows from Blaschke's selection theorem and the continuity of the map $K \to E \operatorname{vol} K_n$, using the Löwner-John ellipsoid.) Assume C is not an ellipsoid. By Lemma 15.2 there is a line L such that the midpoint set $M(C, L)$ does not lie in a hyperplane. We choose the coordinate system so that $L^\perp$ is the hyperplane $x_d = 0$. We choose m chords to C, $L_1, \dots, L_n$, each parallel with with L, and each of positive length so that their midpoints are not contained in a hyperplane. (The condition $n > d$ is used here.) Then $V(P) \ne 0$ where $P = (p_1, \dots, p_n)$ is the vector of midpoints of the chords. Lemma 15.4 shows that $V(P) > V(O)$, and for any other system of m chords, parallel to L, the same inequality holds, but possibly with equality sign.

Now let C^* be the symmetral of K_0 with respect to $x_d = 0$. When one integrates first over Z with $a_1, \dots, a_n$ fixed, and then over the systems $a_1, \dots, a_n$, it follows that $E \operatorname{vol} C_n > E \operatorname{vol} C_n^*$, contradicting the choice of K_0. □

16 Andrews' theorem: an application of the cap covering technique

In 1963 G. E. Andrews [2] proved the following remarkable theorem.

Theorem 16.1. *Assume $P \subset R^d$ is a lattice polytope of volume $V > 0$. Then*

$$f_{d-1}(P) \ll V^{\frac{d-1}{d+1}}.$$

Alternative proofs were later found by Arnold [4], Konyagin and Sevastyanov [43], Schmidt [62], Bárány and Vershik [18], Reisner, Schütt, Werner [52]. Here is yet another proof, due to Bárány and Larman [15], based on the technique of M-regions.

Proof. We start the proof by fixing $\varepsilon = (2d(10d)^d(d+1)!V)^{-1}$. Note that in this way $\varepsilon V < \varepsilon_0$. Let F be a facet of P and let x_F be the point on $\operatorname{bd} P(v \geq \varepsilon V)$ where the tangent hyperplane to $P(v \geq \varepsilon V)$ is parallel with F. According to Lemma 4.8, x_F is unique. Let C_F stand for the cap cut off from K by the hyperplane parallel to F and passing through x_F.

Lemma 16.2. *For distinct facets F and G of P*

$$M(x_F, 1/2) \cap M(x_G, 1/2) = \emptyset.$$

Proof. To see this assume this intersection is nonempty. Then by Lemma 4.4 $M(x_G, 1) \subset M(x_F, 5)$. Further, Lemma 4.9 shows that

$$G \subset C_G \subset M(x_G, 2d) \subset M(x_F, 10d),$$

where the last containment is a simple consequence of $M(x_G, 1) \subset M(x_F, 5)$. Even simpler is

$$F \subset C_F \subset M(x_F, 2d) \subset M(x_F, 10d).$$

Now $M(x_F, 10d)$ contains both facets F and G so it contains $d+1$ affinely independent lattice points. Thus its volume is at least $1/d!$. Then, using again Lemma 4.9,

$$\begin{aligned} \tfrac{1}{d!} &\leq \operatorname{vol} M(x_F, 10d) = (10d)^d u(x_F) \leq (10d)^d 2v(x_F) \\ &\leq 2(10d)^d d\varepsilon V = \tfrac{1}{(d+1)!}. \end{aligned}$$

A contradiction (due to the choice of ε), finishing the proof. □

So the half M-regions $M(x_F, 1/2)$, for all facets F are pairwise disjoint. Their "half" $M(x_F, 1/2) \cap C(F)$ lies completely in $P(\varepsilon)$. Then, by the equivariant version of Theorem 11.3,

$$\sum \frac{1}{2} \operatorname{vol} M(x_F, 1/2) \leq \operatorname{vol} P(v \leq \varepsilon V) \ll \varepsilon^{\frac{2}{d+1}} V \ll V^{\frac{d-1}{d+1}}.$$

Now, again by Lemma 4.9 and Lemma 4.3,

$$\operatorname{vol} M(x_F, 1/2) = 2^{-d} u(x_F) \geq 2^{-d}(2d)^{-2d} \varepsilon V \gg 1.$$

The last two formulae show that the number of facets of P is is indeed $\ll V^{\frac{d-1}{d+1}}$.
$\square$

Theorem 16.1 implies, via a trick of Andrews [2], the following slightly stronger theorem.

Theorem 16.3. *For a lattice polytope $P \in \mathbb{R}^d$ with volume $V > 0$*

$$f_0(P) \ll V^{\frac{d-1}{d+1}}.$$

In what follows we will consider polytopes Q whose vertices belong to the lattice $\frac{1}{s}\mathbb{Z}^d$ where $s \in \mathbb{N}$. Such a polytope is called a $\frac{1}{s}\mathbb{Z}^d$-lattice polytope. Its volume, relative to the new lattice, is just $s^d \operatorname{vol} Q$, which is the same as the volume of Q when the unit volume is the volume of a basic parallelotope of the new lattice.

Proof of Theorem 16.3. Let Q be the convex hull of $(P \cap \frac{1}{3}\mathbb{Z}^d) \setminus X$ where X is the set of vertices of P. So the vertices of P disappeared, but there are (at least) two new lattice points (from the lattice $\frac{1}{3}\mathbb{Z}^d$) on every edge of P. The volume of Q, relative to the new lattice, is at most $3^d \operatorname{vol} P \ll V$. Also, every vertex of P is separated from Q by a facet of Q, and each one by a different facet. Thus $f_0(P) \le f_{d-1}(Q) \ll V^{\frac{d-1}{d+1}}$. $\square$

We can further strengthen the above theorems using a variant of the above method.

Theorem 16.4. *For a lattice polytope $P \in R^d$ with volume $V > 0$*

$$T(P) \ll V^{\frac{d-1}{d+1}}.$$

Proof. We start with a construction. Given a lattice polytope P in $\mathbb{R}^d$, we construct another polytope $Q \subset P$ which is a $\frac{1}{s(d)}\mathbb{Z}^d$-lattice polytope, together with a map f from the set of towers of P to the vertices of Q mapping distinct towers to distinct vertices. Here $s(d)$ is an integer depending only on d.

Such a construction suffices for the proof of the theorem because then $T(P) \le f_0(Q)$ and $f_0(Q)$ is bounded, by the previous theorem, by $V^{\frac{d-1}{d+1}}$, since the volume of Q, relative to the new lattice is at most $s(d)^d \operatorname{vol} P$.

The construction goes by induction. We start with $d = 2$. Given P, let Q be the $\frac{1}{3}\mathbb{Z}^2$-lattice polygon, constructed in the previous proof. A tower of P is just a vertex v and an edge vu of P. The map f takes this tower to the first vertex of Q after v on the segment $(v, u]$. This vertex is clearly on the segment$(v, (2v + u)/3]$, and we are done with the case $d = 2$.

For the induction step $d - 1 \to d$, consider a facet, F, of P. This facet is a lattice polytope, in the lattice $\mathbb{Z}^d \cap \operatorname{aff} F$. The induction hypothesis guarantees the existence of a $\frac{1}{s(d-1)}\mathbb{Z}^d$-lattice polytope Q_F and a map f_F with the required properties. Shrink the lattice a little further to $\frac{1}{2ds(d-1)}\mathbb{Z}^d$. Then Q_F contains a new lattice point, say z, in its relative interior. We shrink now Q_F, from center z, by a factor of 2, let Q_F^* denote the new polytope. It is easy to see that Q_F^*

is a $\frac{1}{2ds(d-1)}\mathbb{Z}^d$-lattice polytope, $Q_F^* \subset F$, and also, it has no point in common with the relative boundary of F. We set now

$$Q = \text{conv} \bigcup_{\text{all } F} Q_F^*.$$

The next task is to define the map f. Let $F_0, F_1, \ldots, F_{d-1}$ be a tower of P. For simpler notation we write $F = F_{d-1}$. Now $F_0, F_1, \ldots, F_{d-2}$ is a tower of F, so it is mapped by f_F to a unique vertex of Q_F. This vertex goes to a unique vertex, say v, of Q_F^*, during the shrinking by a factor of 2. We can define now f on the tower $F_0, F_1, \ldots, F_{d-1}$: its value is just v. Distinct towers are then mapped to distinct vertices of Q since v lies in the relative interior of F. The construction is finished. $\square$

Remark. Theorems 16.1, 16.3, and 16.4 are best possible, apart from the dimension dependent constant. This will be shown by a construction in the next section (in connection with Theorem 17.1), and also by the integer convex hull of rB^d in Section 21.

17 Arnold's question

In 1980, V I Arnold [4] asked the following question which turned out to be very fertile. How many distinct lattice polytopes are there? Of course, infinitely many, so one has to ask a more subtle question. Write $\mathcal{P}$ or $\mathcal{P}^d$ for the set of all convex lattice polytopes in $\mathbb{R}^d$ of positive volume. Two convex lattice polytopes are *equivalent* if there is a lattice preserving affine transformation $\mathbb{R}^d \to \mathbb{R}^d$ carrying one to the other. This is an equivalence relation, and equivalent polytopes have the same area. Write $N_d(V)$ for the number of different, that is, non-equivalent, convex lattice polytopes form $\mathcal{P}^d$, having volume at most V. Arnold showed that, in the two dimensional case, (we write A instead of V for the area)

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

He conjectured and Konyagin and Sevastyanov [43] proved that

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

The log factor can be removed. This was done in [17] for the case $d = 2$, and in [18] for the general case.

Theorem 17.1.

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

The lower bound is easier and follows from the following construction of Arnold [4]. We explain it first in the planar case. Consider the parabola (t, t^2) when $t \in [0, T]$ and T is an even integer. Write $E = \{(t, t^2), t \in [0, T] \text{ even}\} \cup \{(0, T^2)\}$ and $D = \{(t, t^2), t \in [0, T] \text{ odd}\}$. Each subset V of D defines a convex lattice polygon $\text{conv}\{W \cup E\}$. These $2^{T/2}$ convex lattice polygons are distinct (that is, no two of them are equivalent), and their area is less than T^3. So with

$A = T^3$ we have $2^{T/2} = \exp\{\frac{1}{2}\log 2A^{1/3}\}$ convex lattice polytopes of area at most A. Out of this collection of convex lattice polygons one can even produce the same number of distinct convex lattice polygons with the same area. This can be achieved by cutting off a small lattice triangle, with one vertex at $(0, T^2)$, from each polygon.

The higher dimensional construction is very similar and based on the lattice points lying on the paraboloid $x_d = x_1^2 + \cdots + x_{d-1}^2$ with $x_d \leq T^2$. The reader will have no difficulty reconstructing this example.

We mention that the convex hull of all the integer points on the above parabola (resp., paraboloid) is the example showing that the estimate given by Andrews theorem (Theorem 16.1) is best possible.

A further example will come from Theorem **??** in Section 21.

The proof for the upper bound is more difficult and will be given, first for the planar case, and then for the general one, in the next two section. One of the main tools is a result about "multi–partitions" which we state and prove here.

Write $\mathbb{Z}_+^d$ for the set of positive integer points of R^d, i. e., $z \in \mathbb{Z}_+^d$ if every component of z is a positive integer. Given $n = (n_1, \ldots, n_d) \in \mathbb{Z}_+^d$ we call a set $\{z_1, \ldots, z_t\} \subset Z_+^d$ 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 $p(n)$ or $p_d(n)$ if we want to specify dimension. The generating function of $p(n)$ is given in Andrews' book [3] as

$$f(x) = 1 + \sum_{n \in Z_+^d} p(n) x^n = \prod_{m \in \mathbb{Z}_+^d} (1 - x^m)^{-1}, \tag{17.1}$$

where $x = (x_1, \ldots, x_d) \in R^d$ and $x^n = x_1^{n_1} \ldots x_d^{n_d}$. Actually, this is very easy to check as well. It is clear and actually well known, that $f(x)$ is well–defined and finite when all $|x_i| < 1$. We will prove

Theorem 17.2. $\log p(n) \leq (d+1)\left(\zeta(d+1) n_1 \ldots n_d\right)^{1/(d+1)}$.

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

When $d = 1$, $p(n) = p_1(n)$ is the number of partitions of $n \in Z$ and the upper bound from Theorem 2 is very good but, of course, much more precise aymptotic formula is known (cf. [50]). There are asymptotic formulae for $p_d(n)$ (when $d \geq 2$) as well [48], [81], [82], but all of them are valid for some values of the parameters $n = (n_1, \ldots, n_d)$, typically when all ratios n_i/n_j are bounded. In this case the asymptotic formulae (in [48], for instance) imply that

$$\log p(n) = (d+1)\left(\zeta(d+1) n_1 \ldots n_d\right)^{1/(d+1)} (1 + o(1)).$$

This shows that the estimate given in Theorem 17.2 is best possible. However, $\log p_d(n)$ is much smaller than the upper bound when the smallest n_i is very small.

We mention that the same estimation 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 $p_d(1, n, \ldots, n)$ with $p_{d-1}(n, \ldots, n)$.

Proof. We start with taking the logarithm of equation (17.1).

$$\begin{aligned}\log f(x) &= \log \prod_{m\in\mathbb{Z}_+^d} (1-x^m)^{-1} = \sum_{m\in\mathbb{Z}_+^d} \log \frac{1}{1-x^m} \qquad (17.2)\\ &= \sum_{m\in\mathbb{Z}_+^d} \sum_{k=1}^{\infty} \frac{x^{km}}{k} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{m\in\mathbb{Z}_+^d} x^{km} = \sum_{k=1}^{\infty} \frac{1}{k} \prod_{i=1}^{d} \frac{x_i{}^k}{1-x_i{}^k},\end{aligned}$$

where the last equality follows easily from

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

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

$$\frac{t^k}{1-t^k} = \frac{t}{1-t} \frac{t^{k-1}}{1+t+\dots+t^{k-1}} \le \frac{t}{k(1-t)}.$$

From now on we assume all $x_i \in (0,1)$. Then we get from (17.2) that

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

On the other hand, we see from (17.1) that $p(n)x^n \le f(x)$. So

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

Thus for all $x_i \in (0,1)$, we have

$$\begin{aligned}\log p(n) &\le \sum_{i=1}^{d} n_i \log \frac{1}{x_i} + \zeta(d+1) \prod_{i=1}^{d} \frac{x_i}{1-x_i} \qquad (17.3)\\ &\le \sum_{i=1}^{d} n_i \frac{1-x_i}{x_i} + \zeta(d+1) \prod_{i=1}^{d} \frac{x_i}{1-x_i},\end{aligned}$$

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 last line in (17.3) is as small as possible. A convenient choice is when all the $d+1$ terms there are equal, i.e.,

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

A simple computation shows now that

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

which is indeed between 0 and 1. Then we get in (17.3)

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

18 Proof of Theorem 17.1, the planar case

In this section we give the proof of the two-dimensional case of Theorem 17.1. It is slightly different and simpler than the case of higher dimensions, which is considered in the next section.

We need a definition that will be useful later as well. Given $z \in \mathbb{Z}^d$ the width of a set $K \in \mathcal{K}$ is defined as

$$w(K, z) = \max\{z(x - y) : x, y \in K\},$$

and the lattice width of K as

$$w(K) = \min\{w(K, z) : z \in \mathbb{Z}^d,\ z \neq 0\}. \tag{18.1}$$

It is not hard to check that the minimum exists. The vector z in which the minimum is reached is the lattice width direction of K. When K is a lattice polytope, its lattice width plus 1 is equal to the minimal number of parallel (consecutive) lattice hyperplanes that intersect K. An important property of the lattice width is that is is invariant under lattice preserving affine transformations.

The box of $\gamma = (\gamma_1, \dots, \gamma_0) \in \mathbb{Z}^d_+$ is defined as

$$\mathrm{Box}(\gamma) = \{x \in \mathbb{R}^d : 0 \leq x_i \leq \gamma_i \text{ for all } i\}.$$

The volume of $\mathrm{Box}(\gamma)$ is $\prod_1^d \gamma_i$, which will be denoted simply by Γ. Recall that $\mathcal{P}^d$ stands for the set of all convex lattice polytopes of positive volume in $\mathbb{R}^d$.

The so called Box Lemma is important for the proof of Theorem 17.1.

Lemma 18.1. *For every $P \in \mathcal{P}^d$ there exist another $Q \in \mathcal{P}^d$ equivalent to P such that $Q \subset \mathrm{Box}(\gamma)$ for a suitable $\gamma \in \mathbb{Z}^d_+$ with $\Gamma \ll \mathrm{vol}\, P$.*

Proof for the $d = 2$ case. (The general case is proved in the Section 19.) Let w be the lattice width of $P \in \mathcal{P}^2$ with $A = \mathrm{Area}\, P > 0$. We can assume that the lattice width direction of P is $(0, 1)$, and that P lies between lines $y = 0$ and $y = w$. Let ℓ be the length of the longest segment in which a horizontal lattice line intersect K. There are parallel tangent lines to K at the two endpoints of this longest segment. We may assume (possibly after applying a suitable lattice preserving affine transformation) that the slope of this line is at least one. Then P is contained in a parallelogram, (see Fig. **??**). It follows that $\frac{1}{2}\ell w \leq A \leq \ell w$.

Using the notations of Fig. **??**, $\ell + x \geq w$ as otherwise the width of P in direction $(1, 0)$ would be smaller than w. Next we check the width in direction $(1, 1)$, which is at most $(\ell + x + w) - 2x = \ell - x + w \geq w$ implying $\ell \geq x$. This shows that $2\ell \geq w$. Consequently P lies in $\mathrm{Box}(\ell + x, w) \subset \mathrm{Box}(3\ell, w)$. The last box has area $3\ell w \leq 6A$ and contains P. $\square$

The number of boxes of area $6A$ is less than $(6A)^2$, by a very generous estimate. Thus the following result suffices for the proof of Theorem 17.1.

Lemma 18.2. *Each box of area A contains at most $\exp\{cA^{1/3}\}$ convex lattice polygons, where c is a universal constant.*

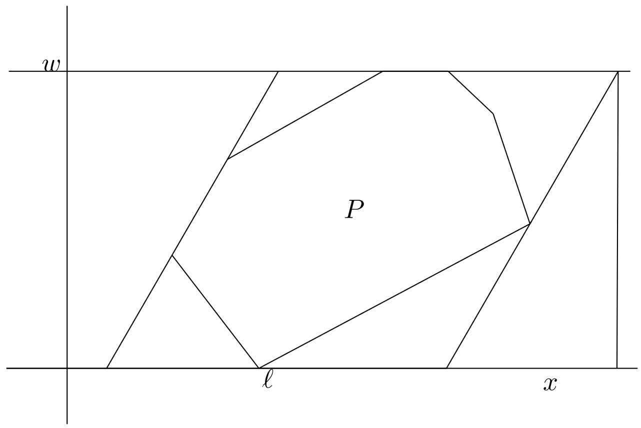

Figure 1: P and the enclosing parallelogram.

Proof. Fix $\gamma \in \mathbb{Z}^2_+$ with $\Gamma \le A$ and consider some $P \in \mathcal{P}^2$ lying in $\mathrm{Box}(\gamma)$. Define, for $\varepsilon = (\varepsilon_1, \varepsilon_2) \in \{-1, +1\}^2$, the convex polyhedron

$$P_\varepsilon = P + \{x \in \mathbb{R}^2 : \varepsilon_i x_i \ge 0 \text{ for } i = 1, 2\}.$$

P_ε is an infinite convex polyhedron whose vertices are from $\mathbb{Z}^2 \cap \mathrm{Box}(\gamma)$. Write $N_\varepsilon(\gamma)$ for the number of such polyhedra.

Claim 18.3. $\log N_\varepsilon(\gamma) \ll \Gamma^{1/3}$.

Proof. It suffices to prove this with $\varepsilon = (-1, +1)$ since all the $N_\varepsilon(\Gamma)$ are equal. In this case each P_ε can be translated, by a vector form $\mathbb{Z}^2$, so that its infinite horizontal edge coincides with the negative half of the x axis, and its infinite vertical edge coincides with the vertical halfline starting at $\beta = (\beta_1, \beta_2) \in \mathbb{Z}^2 \cap \mathrm{Box}(\gamma)$. Let P^*_ε denote this translated copy. At most Γ such translations result in the same P^*_ε.

Observe next that each multipartition of β produces such a P^*_ε by ordering the vectors in the multipartition by increasing (or rather non-decreasing) slope. Sometimes two multipartitions give rise to the same P^*_ε, for instance when the same vector appears twice. But certainly, the number of multipartitions of β is not smaller than the number of P^*_ε with fixed β. Thus Theorem 17.2 applies:

$$\begin{aligned} N_{(-1,1)}(\gamma) &\le \sum_{\beta \in \mathbb{Z}^2 \cap \mathrm{Box}(\gamma)} \Gamma \exp\{3\zeta(3)(\beta_1\beta_2)^{1/3}\} \\ &\le \Gamma^2 \exp\{3\zeta(3)\Gamma^{1/3}\}. \end{aligned} \tag{18.2}$$

This finishes the proof of the claim. □

We are almost done. It is clear that P determines the four infinite polyhedra P_ε uniquely. Conversely, four polyhedra P_ε with distinct ε determine $P \in \mathcal{P}^2$ uniquely if they determine a convex lattice polygon at all. Thus $N(\gamma) \le N_\varepsilon(\gamma)^4$, and the theorem follows from Claim 18.3. □

19 Proof of Theorem 17.1, the general case

We prove first the Box Lemma for general d. We formulate it in a different way, more suitable for the proof.

Assume $B = \{b^1, \dots b^d\}$ is a basis of $\mathbb{Z}^d$. Given α and β in $\mathbb{R}^d$ define

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

$T(B, \alpha, \beta)$ 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 $K \in \mathcal{K}^d$ choose α_i maximal and β_i minimal under the condition that $K \subset T(B, \alpha, \beta)$ for every $i = 1, \dots, d$. Write $T(B, K) = T(B, \alpha, \beta)$ with the extremal α and β which are, of course, uniquely determined. We need the following result.

Theorem 19.1. *Given $P \in$
cP^d there is a basis B of $\mathbb{Z}^d$ such that*

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

Note that this theorem immediately implies the Box Lemma. One just applies a lattice preserving affine transformation carrying $T(B, P) = T(B, \alpha, \beta)$ to $\operatorname{Box}(\gamma)$ where $\gamma = \beta - \alpha$.

Proof. We prove the theorem first when P is centrally symmetric with centre at the origin. In this case, as is well–known, there is an ellipsoid $E \subset \mathbb{R}^d$ 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 $\mathbb{R}^d$. We denote this ball by D. Evidently, $L = \tau\mathbb{Z}^d$ is a lattice again.

Consider now a basis $\hat{B} = \{\hat{b}^1, \dots, \hat{b}^d\}$ of L together with a dual basis $C = \{c^1, \dots, c^n\}$. This is defined (see, for instance, [25]) so as to satisfy $\hat{b}^i c^j = \delta_{ij}$ 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 $y \in L^*$, $xy \in \mathbb{Z}$. It is also well known that $\det(L)\det(L^*) = 1$ where $\det(L)$ and $\det(L^*)$ are equal to the volume of a basis parallelotope of the lattice L and L^*, respectively.

The definition of $T(B, K)$ extends without any difficulty to the case when the underlying lattice is L and not $\mathbb{Z}^d$. So we can consider $T(\hat{B}, D) = T(\hat{B}, -\alpha, \alpha)$. The facets of $T(\hat{B}, -\alpha, \alpha)$ touch the unit ball D and the point $\alpha_i \hat{b}^i$ is on such a facet. Since the unit normal to this facet is $c^i/\|c^i\|$ we must have $1 = (\alpha_i \hat{b}^i)(c^i/\|c^i\|) = \alpha_i/\|c^i\|$. Consequently

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

According to an old theorem of Hermite (see [34] or [25]), 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 $\hat{B}$ of L. Then $\operatorname{vol} T(\hat{B}, D) \ll \det(L)\det(L^*) = 1$.

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

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

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

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

This proves the case when P is centrally symmetric.

The general case $P \in \mathcal{P}^d$ follows now easily. We assume $0 \in P$ and consider $Q = P - P$. Clearly, Q is centrally symmetric and is in $\mathcal{P}^d$. By a result of Rogers and Shephard [60], $\operatorname{vol} Q \ll \operatorname{vol} P$. Let now B be the "good" basis for Q whose existence is established above. It is a good basis for P as well since $T(B, P) \subset T(B, Q)$ and

$$\operatorname{vol} T(B,P) \leq \operatorname{vol} T(B,E) \ll \operatorname{vol} Q \ll \operatorname{vol} P. \quad \square$$

Remark. There are other ways to prove Theorem 3. We could, for instance, choose C to be a Lovász–reduced basis of the dual lattice ,(for the definition see [45] or [31]), and argue that $\tau^{-1}\hat{B}$ satisfies the assertion of the theorem. Or we could take a Korkine–Zolotarov basis of L^* (see [25] or [31]).

Proof of Theorem 17.1, general case. By the Box Lemma we may assume that the given $P \in \mathcal{P}^d$ with $\operatorname{vol} P \leq V$ lies in $\operatorname{Box}(\gamma)$ where $\gamma \in \mathbb{Z}^d_+$ satisfies $\Gamma = \prod_{i=1}^d \gamma_i \ll V$.

Fix now $\gamma \in \mathbb{Z}^d_+$ 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 $\operatorname{Box}(\gamma)$. We are going to show the following fact, analogous to Lemma 18.2

Lemma 19.2. $\log N(\gamma) \ll \Gamma^{\frac{d-1}{d+1}}$.

This will prove the theorem since the number of $\gamma \in \mathbb{Z}^d_+$ with $\Gamma \ll V$ is less than V^d as one can easily check. (Their number is, actually, $O(V(\log V)^{d-1})$ but that makes no difference in this case.)

Let the convex lattice polytope P lie in $\operatorname{Box}(\gamma)$. Consider, just like in the planar case, the 2^d unbounded polyhedra

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

where $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_d) \in \mathbb{R}^d$ with $\varepsilon_i = +1$ or -1. These 2^d polyhedra determine P uniquely. Conversely, 2^d such polyhedra determine P uniquely if they determine a polytope at all.

Define $N_\varepsilon(\gamma)$ as the number of different polyhedra P_ε coming from a lattice polytope in $T(\gamma)$. The following lemma is similar to Lemma 18.2 but for its proof different ideas are needed.

Lemma 19.3. $\log N_\varepsilon(\gamma) \ll \Gamma^{\frac{d-1}{d+1}}$.

Lemma(19.2) follows from here the same way as in the planar case. Thus the theorem is proved once Lemma 19.3 is demonstrated.

Proof. By symmetry, it is be enough to show the lemma when $\varepsilon = (1, \dots, 1)$. In this case we denote P_ε simply by P_+.

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

$$P^* = \{x \in \mathbb{R}^d : \pi_i(x) \in \pi_i(P_+) \text{ for all } i\}.$$

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

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

They determine P^* uniquely. P_i is a $(d-1)$-dimensional polytope lying in box $\pi_i \operatorname{Box}(\gamma)$ which is an aligned box in $(d-1)$-dimensions that has $(d-1)$-volume Γ/γ_i. Write $N^*(\gamma)$ for the number of different profiles of all convex lattice polytopes $P \subset \operatorname{Box}(\gamma)$. An easy induction, using Lemma 19.2 as the induction hypothesis, shows that

$$\log N^*(\gamma) \ll \sum_{i=1}^{d} (\Gamma/\gamma_i)^{\frac{d-2}{d}} \ll \Gamma^{\frac{d-2}{d}}. \tag{19.1}$$

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

Fix now a profile P^* coming from some $P \subset \operatorname{Box}(\gamma)$, and write $N_+(P^*)$ for the number of different polyhedra with profile P^*.

Claim 19.4. $\log N_+(P^*) \ll \Gamma^{\frac{d-1}{d+1}}$.

This will prove Lemma 19.3 because

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

Proof of Claim 19.4. Now we 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 $\mathbb{Z}^d$ (actually in $\mathbb{Z}^d_+$). F is a $(d-1)$-dimensional lattice polytope in the sublattice, of $\mathbb{Z}^d$, orthogonal to $v(F)$. The determinant of this sublattice is $\|v(F)\|$. Whence

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

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 ith component of $u(F)$ is equal to

$\mathrm{vol}_{d-1}\, \pi_i(F)$ as the reader can easily check. Since all the bounded facets of P_+ lie in $\mathrm{Box}(\gamma)$ we get

$$\sum_F u_i(F) = \sum_F \mathrm{vol}\ _{d-1}\pi_i(F) \le \pi_i(\mathrm{Box}(\gamma)) = \Gamma/\gamma_i. \tag{19.2}$$

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

$$\sum_{u \in U} u_i \le (d-1)!\Gamma/\gamma_i. \tag{19.3}$$

(Of course, U is special with respect to γ.) We need the unicity part of the following result of Pogorelov [49].

Lemma 19.5. *Given a profile P^* and vectors $u^1, \dots, u^k \in \mathbb{R}^d_+$, no two of them parallel, there is a unique unbounded polyhedron P_+ with profile P^* and having exactly 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 [49], 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 $U = \{u^1, \dots, u^k\} \subset \mathbb{Z}^d_+$, 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 $\mathrm{vol}_{d-1} F_j = \frac{1}{(d-1)!}\|u^j\|$. Not every such P_+ is a lattice polyhedron, but certainly all P_+ coming from a lattice polytope P can be represented this way. Consequently

$$N_+(P^*) \le \text{number of special sets } U \text{ satisfying (19.3)}.$$

Finally, define $n \in \mathbb{Z}^d_+$ by $n_i = (d-1)!\Gamma/\gamma_i$. According to Theorem 17.2 the number of special sets satisfying (19.3) is

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

This proves Claim 19.4 which, in turn, proves Lemma 19.3 and Lemma 19.2, finishing the proof of Theorem 17.1. □

Remark. Lemma 19.2 implies rather quickly Andrews theorem in the following way. Assume $P \in \mathcal{P}^d$, we suppose it is contained in $\mathrm{Box}(\gamma)$ with $\Gamma \le \mathrm{vol}\, P$. Write X for the set of vertices of P. Then $\mathrm{conv}\, Y$ is a convex lattice polytope for each nonempty $Y \subset X$. This is $2^{|X|} - 1$ distinct lattice polytopes in Box(γ). By Lemma 19.2, the total number of lattice polytopes in Box(γ) is at most $\exp\{\text{const}\Gamma^{(d-1)/(d+1)}\}$, implying

$$f_0(P) = |X| \ll (\operatorname{vol} P)^{\frac{d-1}{d+1}}.$$

Proof of Lemma 19.5. Set $e = (1, \ldots, 1) \in \mathbb{R}^d$ and denote by $H_j(\omega_j)$ the hyperplane orthogonal to u^j and intersecting the line $\{\tau e \in \mathbb{R}^d : \tau \in R\}$ at the point $\omega_j e$. Let $H_j^-(\omega_j)$ be the halfspace bounded by $H_j(\omega_j)$ and containing the infinite ray pointing in the direction $-e$. Any P_+ with bounded facets orthogonal to u^j $(j = 1, \ldots, k)$ is of the form

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

where the parameter ω is from $\mathbb{R}_+^k$. 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 existence. We choose a sufficiently large compact set $C \subset \mathbb{R}_+^k$ by requiring two things. The first is that for $\omega \in C$ the set $P^* \cap H_j(\omega_j)$ is nonvoid which means that $\omega_j \le M_j$ for some suitable M_j. The second is that the $(d-1$-volume of $P^* \cap H_j(\omega_j)$ is at most $\sum_1^k ||u_j||$, which means that $m_j \le \omega_j$ with a suitable m_j. Note that with $\omega_j < m_j$ the $(d-1)$-volume of the bounded facets is larger than $\sum_1^k ||u_j||$.

Define Ω as the set of those $\omega \in C$ for which the $(d-1)$-volume of $F_j(\omega)$ is at most $\|u^j\|$ $(j = 1, \ldots, k)$. The set Ω is clearly compact. It is nonempty because the ω when each $H_j(\omega_j)$ is tangent to P^* belongs to Ω. So the continuous function $g : \Omega \to \mathbb{R}$ 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 $\operatorname{vol}_{d-1} F_j(\omega) < \|u^j\|$ 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 $\operatorname{vol}_{d-1} F_j(\omega') < \|u^j\|$. On the other hand, for $i \neq j$, $F_i(\omega') \subset F_i(\omega)$ and so $\operatorname{vol}_{d-1} F_i(\omega') \le \operatorname{vol}_{d-1} F_i(\omega)$. 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 $P(\omega^*)$ and let $\delta = \max_j(\omega_j - \omega_j^*)$. We assume $\delta > 0$ (otherwise exchange the names). Denote by J the set of those indices j for which $\delta = \omega_j - \omega_j^*$ 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 $\omega_i = \omega_i^*$. Clearly $Q(\omega) = \bigcap_j H_j^-(\omega_j - \delta)$ is a subset of $P(\omega^*)$.

Denote by $\bar{F}_j$ (and F_j) the facet of $P(\omega^*)$ (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 $P(\omega^*)$. 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 have

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

and similarly

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

As $\omega_m^* \geq \omega_m - \delta$, we have $F_j \subset \bar{F}_j$. This inclusion is proper because $\omega_i^* > \omega_i - \delta$ 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. $\square$

20 Approximation

There are two types of problems in the theory of approximation of a convex body $K \in \mathcal{K}$ by polytopes belonging to a certain class $\mathcal{P}$ of polytopes. The first type is asking for a lower bound, that is, a statement of the form: no polytope $P \in \mathcal{P}$ approximates K better than some function of K and $\mathcal{P}$. The second is asking for the existence of a polytope $P \in \mathcal{P}$ which approximates K well, hopefully as well as the previous function. To be less vague, we consider inscribed polytopes only (that is $P \subset K$) and we measure approximation by the relative missed volume, that is, by

$$\mathrm{appr}(K, P) = \frac{\mathrm{vol}(K \setminus P)}{\mathrm{vol}\, K}.$$

To give a specific example, let $K \in \mathcal{K}_1$ be a convex body with $\mathcal{C}^2$ boundary and Gauss curvature $\kappa > 0$ everywhere. Its affine surface area, $\Omega(K)$, is defined as $\int_{\mathrm{bd}\, K} \kappa^{1/(d+1)}$. The following two results are from Gruber [33]. If P_n is an inscribed polytope with n vertices, then

$$\mathrm{appr}(K, P_n) \geq \mathrm{del}_{d-1} \Omega(K)^{(d-1)/(d+1)} n^{-2/(d-1)} (1 + o(1)). \tag{20.1}$$

where the more or less explicit constant del_{d-1} depends only on d. This is a first type statement. A second type one is that, under the same conditions, there is an inscribed polytope P_n^* with n vertices, such that

$$\mathrm{appr}(K, P_n^*) \leq \mathrm{del}_{d-1} \Omega(K)^{(d-1)/(d+1)} n^{-2/(d-1)} (1 + o(1)), \tag{20.2}$$

where even the constant is the same as in (20.1).

In this section we show how the cap-covering technique can be used to attack both type of approximation problems. As expected, the results do not give precise constants but tell the right order of magnitude.

We start with the problem of the second type. C. Schütt [69] proved two very neat and general results.

Theorem 20.1. *Given $K \in \mathcal{K}_1$ and $t \in (0, t_0]$ (where t_0 depends only on the dimension), there is a polytope P with $K(v \geq t) \subset P \subset K$ for which*

$$f_0(P) \ll \frac{\operatorname{vol} K(t)}{t}.$$

Theorem 20.2. *Given $K \in \mathcal{K}_1$ and $t \in (0, t_0]$ (where t_0 depends only on the dimension), there is a polytope P with $K(v \geq t) \subset P \subset K$ for which*

$$f_{d-1}(P) \ll \frac{\operatorname{vol} K(t)}{t}.$$

This means that $\operatorname{appr}(K, P) \leq \operatorname{vol} K(t)$ and the lost volume is "t per vertex", and "t per facet", respectively. We will see below that, for smooth bodies, this is the best possible order of magnitude. One may wonder whether the same result holds with $T(P) \ll \frac{\operatorname{vol} K(t)}{t}$. If it does, it contains both theorems above.

Schütt's proof of these theorems is direct and technical. Here I present a simple argument showing the power and efficacy of the cap covering method. Nevertheless, this argument gives weaker constants than Schütt's original theorem and does not extend to approximation by circumscribed polytopes (cf [69]).

We mention that Theorem 20.1, for instance, gives the order of magnitude in the formula (20.2). Indeed, by Theorem 11.5, $K(t)$ is of order $t^{2/(d+1)}$, so $n = f_0(P)$ in Theorem 20.1 is $\ll t^{-(d-1)/(d+1)}$ and $\operatorname{appr}(K, P) \ll K(t) \approx t^{2/(d+1)}$. Thus P is an inscribed polytope on n vertices satisfying $\operatorname{appr}(K, P) \leq \operatorname{const}(K) n^{-2/(d-1)}$. Even $\operatorname{const}(K) \leq c_d \int \kappa^{1/(d+1)}$ follows from Theorem 11.5.

For both theorems, start with setting $\tau = d^{-1} 6^{-d} t$ and choose a system of points $\{x_1, \ldots, x_m\}$ from $\operatorname{bd} K(v \geq \tau)$ maximal with respect to the property that the sets $M(x_i, 1/2)$ are pairwise disjoint. The economic cap covering argument shows that

$$m \ll \frac{\operatorname{vol} K(\tau)}{\tau} \leq \frac{\operatorname{vol} K(t)}{\tau} \ll \frac{\operatorname{vol} K(t)}{t}.$$

Proof of Theorem 20.2. Let $C(x_i)$ be a minimal cap, and define

$$P = K \setminus \cup_1^m C(x_i)^6.$$

We will show that (1) no $z \in \operatorname{bd} K$ belongs to P, and (2) $K(v \geq t) \subset P$. This is clearly sufficient.

To see (1), assume $z \in \operatorname{bd} K$. By Lemma 4.11 there is $x \in \operatorname{bd} K(v \geq \tau)$ such that $z \in M(x)$. By the maximality of the system $x_1, \ldots, x_m$, there is an x_i with $M(x, 1/2) \cap M(x_i, 1/2) \neq \emptyset$. By Lemma 4.4, $M(x) = M(x, 1) \subset M(x_i, 5)$, implying

$$z \in M(x) \subset M(x_i, 5) \cap K \subset C(x_i)^6.$$

To check that (2) also holds, note that $\operatorname{vol} C(x_i) \leq d\tau$ by Lemma 4.9. So we have

$$\operatorname{vol} C(x_i)^6 \leq 6^d \operatorname{vol} C(x_i) \leq 6^d d\tau = t,$$

so $v(x) \leq t$ for every point x cut off from K by one of the caps $C(x_i)^6$. $\square$

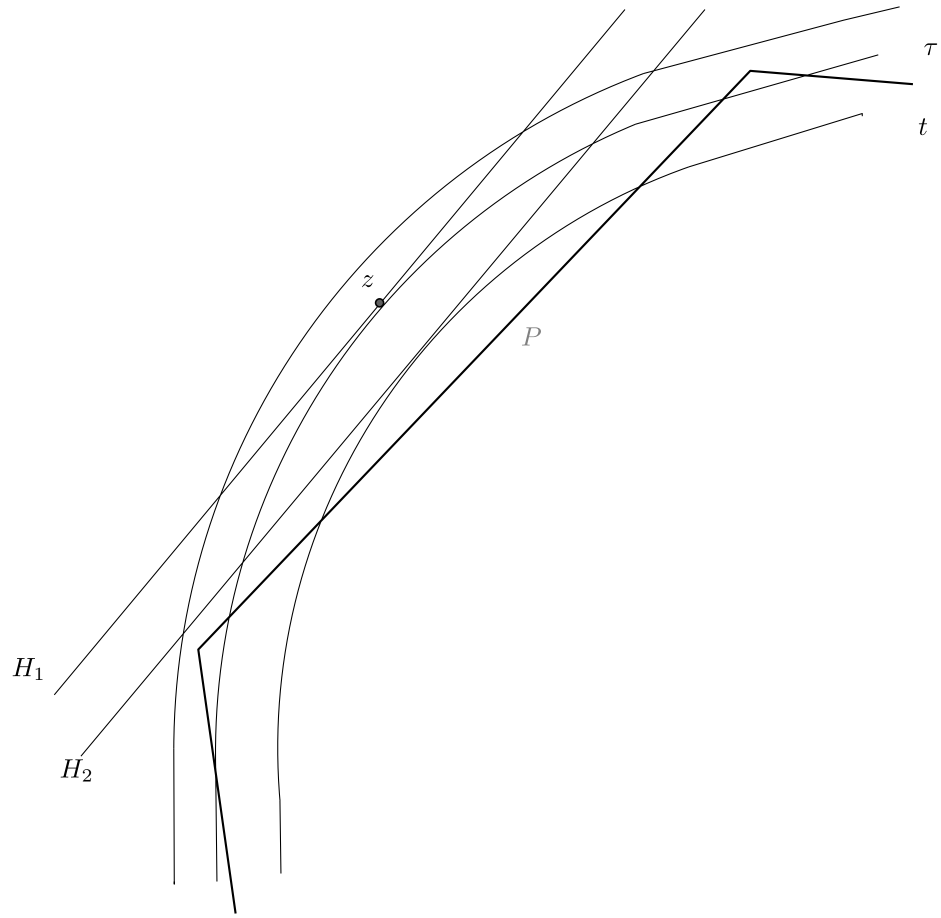

Figure 2: When P does not contain $K(t)$.

Proof of Theorem 20.1. Let y_i be an arbitrary point from $M(x_i, 1)$. (One is tempted to choose y_i from the boundary of K but that is not important here.) Define

$$P = \mathrm{conv}\{y_1, y_2, \ldots, y_m\}.$$

Clearly $P \subset K$. So we have to show $K(v \geq t) \subset P$. Assume the contrary: then there is a halfspace H_1 disjoint from P whose bounding hyperplane is tangent to $K(v \geq t)$. Note that no y_i is in H_1, see Fig. 2. Let H_2 be the halfspace whose bounding hyperplane is parallel to that of H_1, and which is tangent to $K(v \geq \tau)$ at the point z, say. Set $C_j = K \cap H_j$, $j = 1, 2$. Lemma 4.9 says that $\mathrm{vol}\, C_2 \leq d\tau$, and $\mathrm{vol}\, C_1 \geq t = d6^d\tau$.

By the maximality of the x_i, $M(z, 1/2)$ intersects some $M(x_i, 1/2)$ and, in view of Lemma 4.4, again, $M(x_i, 1) \subset M(z, 5)$. Also, $M(z, 5) \cap K$ is contained in $C_2^6 \cap K$ which is a cap of K whose volume is at most $6^d\, \mathrm{vol}\, C_1 \leq d6^d\tau$, by Lemma 4.9. Now $C_2^6 \subset C_1$ follows from the construction and from $\mathrm{vol}\, C_1 \geq d6^d\tau$. By the construction $y_i \in M(x_i)$, and so $y_i \in C_1 \subset H_1$. A contradiction. $\square$

We turn now to the first type of approximation question. We will consider here the family of all polytopes inscribed in K with at most n s-dimensional faces. Denote this class of polytopes by $\mathcal{P}_n(K,s)$. The usual question of approximation by inscribed polytopes with at most n vertices, the case $\mathcal{P}_n(K,0)$ in our notation, is well understood, see (20.1) and (20.2) above. In the same paper Gruber [33] proves an asymptotic formula for circumscribed polytopes with at most n facets, and in [46], Ludwig gives exact asymptotic formulae for the unrestricted case with n vertices and n facets, respectively. (Approximation is measured as the relative volume of the symmetric difference of P and K.)

Is there a similar estimate for $\mathcal{P}_n(K,s)$ when $0 < s < d-1$? Or a weaker one, giving the order of magnitude of $\operatorname{appr}(K,P)$? This unusual approximation question has come up in connection with the integer convex hull (cf [15]). We will see how it is used there in Section 21.

Again, M-regions and cap coverings are going to help. Here we present the basic ideas of the proof in the case when $K = B^d$, the unit ball $\mathbb{R}^d$: this extends without serious difficulty to convex bodies whose product curvature is separated from 0 and ∞. It should be mentioned that K. Böröczky Jr in [20] has worked out several other cases of this type, for instance, inscribed, circumscribed, and unrestricted polytopes with at most n s-dimensional faces (again when $0 < s < d-1$). His approach is different: it is based on local quadratic approximation of the boundary and uses power diagrams.

Here is the result on approximation by polytopes in $\mathcal{P}_n(B^d,s)$ for the unit ball.

Theorem 20.3. *For every $s = 0,1,\dots,d-1$ and for every polytope $P \in \mathcal{P}_n(B^d,s)$, and for large n*

$$\operatorname{appr}(B^d,P) \gg n^{-\frac{2}{d-1}}.$$

The proof below is based on an idea from [15] which is used there when $s = d-1$. This particular case, when $K = B^d$, was first proved by Rogers [59]. We mention that the theorem holds for smooth convex bodies, not only for the Euclidean ball. But the technique and the arguments are simpler and cleaner in the case of B^d. The interested reader will have no difficulty in extending the proof below to smooth convex bodies.

Proof. We may suppose that

$$\operatorname{vol}(B^d \setminus P) \le b_1 n^{-\frac{2}{d-1}}$$

for any particular constant b_1 of our choice (b_1 depending on d), as otherwise there is nothing to prove. We assume further that $s \ge 1$, the case $s = 0$ being covered by (20.1) and (20.2). We can and do suppose further that all vertices of P are on the boundary of B^d.

Let $F_1,\dots,F_n$ denote the s-dimensional faces of P and let z_i be the nearest point of F_i to the origin. The minimal cap $C(z_i)$ has width h_i. It is not hard to check that $F_i \subset C(z_i)$. Also, $\operatorname{vol}(C(z_i) \setminus P) \ge \frac{1}{2}\operatorname{vol} C(z_i)$. This means that $\operatorname{vol} C(z_i)$ must be small, and so h_i must be small. Consequently, $\operatorname{vol} C(z_i) \approx h_i^{\frac{d+1}{2}}$, as a quick computation reveals.

Choose next a subsystem $\{x_{i_1}, \ldots, x_{i_m}\}$ from the x_i which is, as we are used to it by now, maximal with respect to the property that the M-regions $M(x_{i_j}, 1/2)$ are pairwise disjoint. To have simple notation set $z_j = x_{i_j}$ and also $h_j = h_{i_j}$ with minimal abuse. By Lemma 4.4, every $C(x_i)$ is contained in some $M(z_j, 5)$. So writing V for the set of vertices of P we clearly have

$$V \subset \cup_1^n F_i \subset \cup_1^n C(x_i) \subset \cup_1^m M(z_j, 5).$$

As we observed before, half of $C(x_i)$ is outside of P. The sets $M(z_j, 1/2)$ are pairwise disjoint, and half of $C(z_j) \cap M(z_j, 1/2)$ is outside of P which gives a lower bound for $\mathrm{vol}(B^d \setminus P)$:

$$\sum_1^m h_j^{\frac{d+1}{2}} \ll \mathrm{vol}(B^d \setminus P) \leq b_1 n^{-\frac{2}{d-1}},$$

where h_j denotes the width of the cap $C(z_j)$.

Fix $\rho = b_2 n^{-\frac{1}{d-1}}$, where $b_2 = b_2(d)$ is to be defined later. We want to show that the set $V + \rho B^d$ covers at most half of $S^{d-1} = \mathrm{bd}\, B^d$. We estimate the surface area of this set by that of $S^{d-1} \cap \cup_1^m (M(z_j, 5) + \rho B^d)$. For a particular z_j, $M(z_j, 5) + \rho B^d$ is contained in a cap, centered at z_j, with radius $\ll \rho + \sqrt{h_j}$. Thus the surface area of S^{d-1}, covered by $V + \rho B^d$ is at most

$$\begin{aligned}
&\ll \sum_1^m \left(\rho + h_j^{\frac{1}{2}}\right)^{d-1} = \sum_{j=1}^m \sum_{k=0}^{d-1} \binom{d-1}{k} \rho^{d-1-k} h_j^{\frac{k}{2}} \\
&= \sum_{k=0}^{d-1} \binom{d-1}{k} \rho^{d-1-k} \left(\sum_{j=1}^m h_j^{\frac{k}{2}} \right) \\
&\leq \sum_{k=0}^{d-1} \binom{d-1}{k} \rho^{d-1-k} m \left(\frac{1}{m} \sum_{j=1}^m h_j^{\frac{d+1}{2}} \right)^{\frac{k}{d+1}} \\
&= m \left(\rho + \left(\frac{1}{m} \sum_1^m h_j^{\frac{d+1}{2}} \right)^{\frac{1}{d+1}} \right)^{d-1},
\end{aligned}$$

where we used the inequality between the kth and $(d+1)$st means.

The last expression is smaller than half the surface area of S^{d-1} if the constants b_1, b_2 are chosen suitably. Indeed, as $m \leq n$,

$$\rho = b_2 n^{-\frac{1}{d-1}} \leq b_2 m^{-\frac{1}{d-1}},$$

and since $\sum_{j=1}^m h_j^{\frac{d+1}{2}} \leq b_1 n^{-\frac{2}{d-1}}$,

$$\left(\frac{1}{m} \sum h_j^{\frac{d+1}{2}} \right)^{\frac{1}{d+1}} \leq b_1^{\frac{1}{d+1}} m^{-\frac{1}{d-1}}.$$

We just proved that $V + \rho B^d$ covers at most half of S^{d-1}. But then

$$S^{d-1} \setminus (V + \frac{\rho}{2} B^d)$$

contains many pairwise disjoint caps of radius $\rho/2$. This is shown by a greedy algorithm: assume the centers $y_p \in S^{d-1} \setminus (V + \rho B^d)$ of these caps C_p have been chosen for $p = 1, 2, \ldots, q$ and the caps are pairwise disjoint. The caps with centres y_p and radius ρ cover at most

$$q\rho^{d-1} \operatorname{vol}_{d-1} S^{d-1}$$

of S^{d-1}. So as long as this is smaller than the surface area of

$$S^{d-1} \setminus (V + \rho B^d),$$

there is room to choose the next center y_{q+1}. The algorithm produces as many as $\gg \rho^{-(d-1)} \approx n$ pairwise disjoint caps. They are all disjoint from P, so the volume missed by P is

$$\sum \operatorname{vol} C_p \gg n\rho^{d+1} \gg n^{-\frac{2}{d-1}},$$

finishing the proof of Theorem 20.3. □

21 The integer convex hull

The "integer convex hull" of $K \in \mathcal{K}^d$ is, by definition,

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

which is clearly a convex lattice polytope if it is non-empty. How many vertices does $I(K)$ have? Motivation for the question comes from different sources: integer programming (cf. [26], [13]), classical enumeration problems ([37],[62], or more generally [77],[74]), and from the theory of random polytopes (see later).

In this section we determine the order of magnitude of $f_s(I(K))$ when $K = rB^d$, the Euclidean ball of radius r, centered at the origin. Write $P_r = I(rB^d)$. For the case $d = 2$ it is shown in [5] that

$$0.33r^{2/3} \le f_0(P_r) \le 5.55r^{2/3}. \tag{21.1}$$

The limit, as $R \to \infty$, of the average of $r^{-2/3} f_0(P_r)$, on an interval $[R, R + H]$, is determined by Balog and Deshoullier [6], and turns out to be $3.453\ldots$, (H must be large). Our main result extends (21.1) to any $d \ge 2$ and to any $f_s(P_r)$ with $s = 0, \ldots, d-1$.

Theorem 21.1. *For every $d \ge 2$ for every $s \in \{0, \ldots, d-1\}$*

$$r^{d\frac{d-1}{d+1}} \ll f_s(P_r) \le r^{d\frac{d-1}{d+1}}. \tag{21.2}$$

We mention that this theorem is valid not only for $K = rB^d$ but more generally for rC where $C \in \mathcal{K}$ is a convex body with smooth, $\mathcal{C}_2$ say, boundary, and product curvature κ separated from 0 and infinity, and $0 \in \operatorname{int} C$. In this case the constants implied by the $\ll$ notation depend on d and also on how well

κ is separated from 0 and infinity. The proof for the general case is very similar to that of $C = B^d$. We choose to give it for B^d because this way the idea is clearer and we don't have use local approximation of $\operatorname{bd} C$ by a paraboloid.

The upper bound follows from Theorem 16.4, which is a slightly stronger version of Andrews theorem. Indeed, trivially, $f_s(P) \le T(P)$ for every s and every polytope P. We don't even need $C = B^d$.

We give a simple proof for $f_0(P_r) \ll r^{d\frac{d-1}{d+1}}$ since we will need it later. Define first $h = c(d)r^{-\frac{d-1}{d+1}}$ where the constant $c(d)$ is sepcified soon. Let $z \in \mathbb{Z}^d$ be a lattice point at distance $r-h$ at most from the origin. It is easy to check that $\operatorname{vol} M(z) \ge 2^d$ (if the constant $c(d)$ in the definition of h is chosen large enough). $M(z)$ is centrally symmetric with center z. By Minkowski's theorem it contains a lattice point $y \ne z$. Then it contains $2z - y \in \mathbb{Z}^d$ as well. Thus z is the midpoint of the segment $[y, 2z-y]$. Consequently it cannot be a vertex of P_r. Then all vertices of P_r lie in the annulus $rB^d \setminus (r-h)B^d$. By classical results about the circle problem (see for instance [**?**])

$$|\mathbb{Z}^d \cap rB^d| = \operatorname{vol} B^d r^d + o(r^{d\frac{d-1}{d+1}}).$$

this implies that the annulus contains $\ll r^{d\frac{d-1}{d+1}}$ lattice points, showing, in turn, that $f_0(P_r) \ll r^{d\frac{d-1}{d+1}}$.

The proof of the lower bounds is based on

Theorem 21.2. *For every $d \ge 2$*

$$\operatorname{vol}(rB^d \setminus P_r) \ll r^{d\frac{d-1}{d+1}}.$$

Proof of Theorem 21.1 from Theorem 21.2. This is based on the approximation result of Theorem 20.3 and is quite easy. Setting $f_0(P_r) = n$ the approximation result says that

$$\begin{aligned} n^{-\frac{2}{d-1}} &\ll \operatorname{appr}(rB^d, P_r) = \frac{\operatorname{vol}(rB^d \setminus P_r)}{\operatorname{vol} rB^d} \\ &\ll \frac{r^{d\frac{d-1}{d+1}}}{r^d} = r^{-\frac{2d}{d+1}}. \end{aligned}$$

From this $n \gg r^{d\frac{d-1}{d+1}}$ immediately follows. □

Remark. The inequality given in Theorem 21.2 is best possible, apart from the implied constant, and the corresponding inequality follows quickly from this proof. Indeed, if one had the bound $\operatorname{vol}(rB^d \setminus P_r) \ll r^D$, then with $n = f_0(P_r)$ we had $n^{-2/(d-1)} \ll r^{D-d}$ from (20.1). The upper bound in Theorem 21.1 shows that $n \ll r^{d\frac{d-1}{d+1}}$. Thus

$$r^{\frac{1}{2}(d-1)(d-D)} \ll n \ll r^{d\frac{d-1}{d+1}},$$

implying $D \ge d\frac{d-1}{d+1}$.

Before the proof of Theorem 21.2 we introduce notation and terminology. We write $\mathbb{P}$ for the set of primitive vectors $z \in \mathbb{Z}^d$. Recall that $z \in \mathbb{Z}^d$ is called *primitive* if the greatest common divisor of its components is 1. Each facet of P_r has a unique outward normal vector which is primitive, and for $p \in \mathbb{P}$ we denote this facet (if it exists) by $F(p)$. It lies in the hyperplane $H(p) = \operatorname{aff} F(p)$ which cuts of a small cap $C(p)$ from rB^d. Clearly,

$$\mathbb{Z}^d \cap \operatorname{int} C(p) = \emptyset. \tag{21.3}$$

Let $\rho = \rho(p)$ be the radius of the $(d-1)$-ball $H(p) \cap rB^d$ and let $h = h(p)$ be the width, in direction p, of the cap $C(p)$. Then

$$\rho^2 = (2r - h)h \text{ and so } rh \ll \rho^2 \ll rh. \tag{21.4}$$

Write $||x||$ for the Euclidean length of $x \in \mathbb{R}^d$. Letting Area to denote $(d-1)$-dimensional volume, we have

$$\operatorname{Area} F(p) = \ell(p)|p| \ll \rho^{d-1}. \tag{21.5}$$

Here $||p||$ is, in fact, the determinant of the lattice $\mathbb{Z}^d \cap H(p)$, and so

$$\ell(p) \in \frac{1}{(d-1)!}\mathbb{Z}_+.$$

Proof of Theorem 21.2. We begin with a simple lemma.

Lemma 21.3. *The contribution to* $\operatorname{vol}(rB^d \setminus P_r)$ *of the caps* $C(p)$ *with* $h(p) \leq r^{-\frac{d-1}{d+1}}$ *is* $\ll r^{d\frac{d-1}{d+1}}$.

Proof. Everything that is contained in such a $C(p)$ is also contained in

$$rB^d \setminus (r - r^{-\frac{d-1}{d+1}})B^d$$

whose volume is just $\left(r^d - (r - r^{-\frac{d-1}{d+1}})^d\right) \operatorname{vol} B^d \ll r^{d\frac{d-1}{d+1}}$. □

From now on we can only consider facets $F(p)$ with

$$h(p) \geq r^{-\frac{d-1}{d+1}}. \tag{21.6}$$

We are going to use the Flatness Theorem (cf. [39] or [38]) saying that the lattice width of a lattice point free convex body (in $\mathbb{R}^d$) is at most $c_0 d^2$ where c_0 is a universal constant. Applying this to $C(p)$, or rather to $\operatorname{int} C(p)$ which is lattice point free by (21.3), we get a primitive vector $q \in \mathbb{Z}^d$ such that

$$\max\{q(x-y)\, x, y \in C(p)\} \leq c_0 d^2. \tag{21.7}$$

Case 1: when $h(p) \leq c_0 d^2 ||p||^{-1}$. In this case p is the flatness direction for $C(p)$ (since consecutive lattice hyperplanes with normal $p \in \mathbb{P}$ are at distance $||p||^{-1}$ apart). Then $\rho^2 \ll rh \ll r||p||^{-1}$ and

$$\operatorname{Area} F(p) = \ell(p)||p|| \ll \rho^{d-1} \ll (r||p||^{-1})^{\frac{d-1}{2}},$$

implying

$$\ell(p) \ll r^{\frac{d-1}{2}}||p||^{-\frac{d+1}{2}}.$$

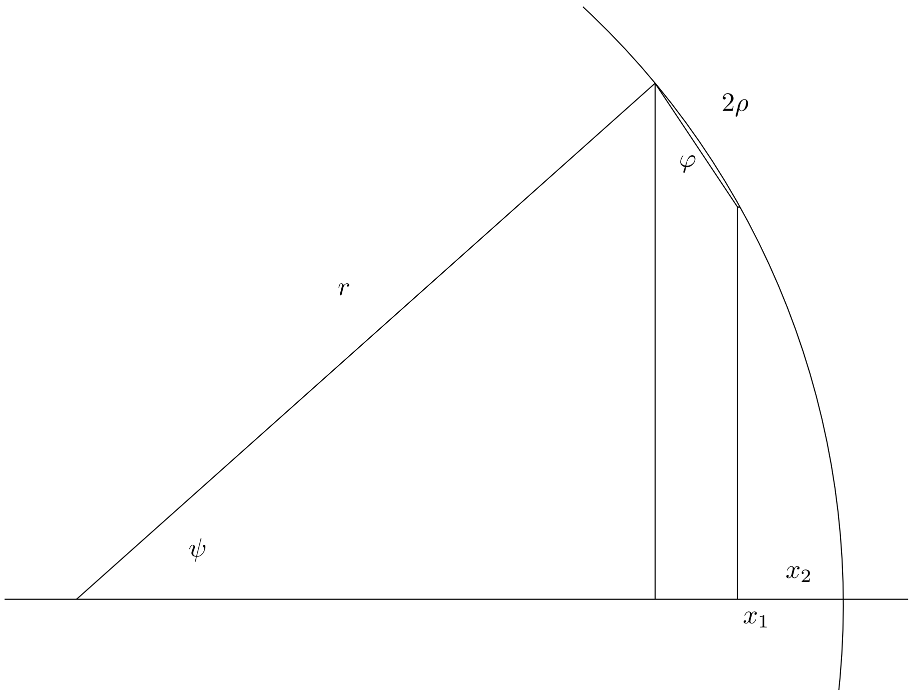

Figure 3: The section in the plane of 0, q, and the centre of $C(p)$.

Now equation (21.6) and the condition $h(p) \le c_0 d^2 ||p||^{-1}$ imply that $||p|| \ll r^{\frac{d-1}{d+1}}$. We write $b = b(d)$ for the implied constant. The lost volume in Case 1 is

$$\begin{aligned} &\ll \sum_p \operatorname{Area} F(p)h(p) \ll \sum_{p\in\mathbb{P}} \ell(p) \ll \sum_{||p||\le br^{\frac{d-1}{d+1}}} r^{\frac{d-1}{2}} ||p||^{-\frac{d+1}{2}} \\ &\ll r^{\frac{d-1}{2}} \int_0^{br^{\frac{d-1}{d+1}}} x^{-\frac{d+1}{2}} x^{d-1} dx \ll r^{d\frac{d-1}{d+1}} \end{aligned} \qquad (21.8)$$

where in the last steps we extended the sum from $p \in \mathbb{P}$ to $p \in \mathbb{Z}^d$, and then estimated the sum by the corresponding integral.

Case 2: when $h(p) > c_0 d^2 ||p||^{-1}$. Then some $q \in \mathbb{Z}^d$, distinct from p, is the flatness direction of $C(p)$.

Assume $C(p)$ is between hyperplanes $qx = \ell_1$ and $qx = \ell_2$ with $\ell_1, \ell_2 \in (0, ||q||r]$ and $\ell_2 - \ell_1 \le c_0 d^2$. Set $k_i = |q|r - \ell_i$ and $x_i = k_i/|q|$, $(i = 1, 2)$. Consider the two-dimensional plane containing $0, q$, and the centre of $C(p)$.

We show first that ϕ and ψ (see Fig. 3) gets small as r gets large. Indeed, assuming $x_2 > 0$, and using (21.6)

$$\sin\phi = \frac{x_1 - x_2}{2\rho} = \frac{x_1 - x_2}{2\sqrt{(2r-h)h}} \le \frac{k_1 - k_2}{2||q||\sqrt{rh}} \le \frac{c_0 d^2}{2||q||\sqrt{r \cdot r^{-\frac{d-1}{d+1}}}} \ll r^{-\frac{1}{d+1}}$$

since $||q|| \ge 1$. This holds even if $x_2 = 0$ since then $\sin\phi < x_1/\rho$ and the same estimate works.

As ϕ and ψ (see Fig. 3) again) are almost equal, the previous inequality implies

$$x_1 = r(1-\cos\psi) \le r\sin^2\phi \ll r^{\frac{d-1}{d+1}}.$$

Next we estimate ρ. As $\cos\phi > 1/2$ for large enough r, we get

$$\begin{aligned}\rho &< \sqrt{(2r-x_1)x_1} - \sqrt{(2r-x_2)x_2} \\ &= \frac{(2r-x_1)x_1-(2r-x_2)x_2}{\sqrt{(2r-x_1)x_1}+\sqrt{(2r-x_2)x_2}} \le \frac{(2r-x_1-x_2)(x_1-x_2)}{\sqrt{r}(\sqrt{x_1}+\sqrt{x_2})} \\ &\le 2\sqrt{r}\frac{k_1-k_2}{||q||}\frac{\sqrt{||q||}}{\sqrt{k_1}+\sqrt{k_2}} \ll \sqrt{\frac{r}{||q||k_1}}. \qquad (21.9)\end{aligned}$$

The same estimate follows almost the same way when $x_2 = 0$. We only have to start with $\rho < 2\sqrt{(2r-x_1)x_1}$.

It follows from (21.9 that $h \ll \rho^2 r^{-1} \ll (||q||k_1)^{-1}$. Now (21.6) shows $k_1||q|| \ll r^{\frac{d-1}{d+1}}$. Set now $k = \lceil k_1 \rceil$. As p is not a flatness direction, $1 \le k_1 - k_2 \le k_1$. So $k \ge 1$ and

$$k||q|| \ll r^{\frac{d-1}{d+1}}.$$

Collect the $F(p)$ with fixed flatness direction q and fixed k into groups. The missed volume in the corresponding caps is

$$\ll \sum \mathrm{Area}\, F(p)h(p) \le S \max h(p) \qquad (21.10)$$

where S is the surface area of rB^d between hyperplanes $qx = \ell_1$ and $qx = \ell_2$. Since ϕ is small,

$$\begin{aligned}S &\le 2\left([(2r-x_1)x_1]^{\frac{d-1}{2}} - [(2r-x_2)x_2]^{\frac{d-1}{2}}\right)\mathrm{Area}\, B^{d-1} \\ &\ll \left(\sqrt{(2r-x_1)x_1} - \sqrt{(2r-x_2)x_2}\right)((2r-x_1)x_1)^{\frac{d-2}{2}} \\ &\ll \sqrt{\frac{r}{||q||k}}\left(\frac{rk}{||q||}\right)^{\frac{d-2}{2}}.\end{aligned}$$

where we used the estimate in (21.9). Evidently $\max h(p) \le \rho^2/r \ll (||q||k)^{-1}$. We continue (21.10):

$$\ll \frac{1}{|q|k}\sqrt{\frac{r}{||q||k}}\left(\frac{rk}{||q||}\right)^{\frac{d-2}{2}} = r^{\frac{d-1}{2}}||q||^{-\frac{d+1}{2}}k^{\frac{d-5}{2}}.$$

This is to be summed for all $k = 1, 2, \ldots$ and $q \in \mathbb{Z}^d$ primitive with $k||q|| \le R$ where $R \ll r^{\frac{d-1}{d+1}}$. Then the total missed volume is

$$\begin{aligned}&\ll r^{\frac{d-1}{2}}\sum_{k=1}^{R}\sum_{q\in\mathbb{Z}^d}^{\frac{R}{k}}||q||^{-\frac{d+1}{2}}k^{\frac{d-5}{2}} \ll r^{\frac{d-1}{2}}\sum_{k=1}^{R}\int_{x\in R^d,\ ||x||\le\frac{R}{k}}||x||^{-\frac{d+1}{2}}k^{\frac{d-5}{2}}dx \\ &\ll r^{\frac{d-1}{2}}\sum_{k=1}^{R}k^{\frac{d-5}{2}}\int_0^{\frac{R}{k}}t^{d-1}t^{-\frac{d+1}{2}}dt \ll r^{\frac{d-1}{2}}\sum_{k=1}^{R}k^{\frac{d-5}{2}}\left(\frac{R}{k}\right)^{\frac{d-1}{2}} \\ &= r^{\frac{d-1}{2}}R^{\frac{d-1}{2}}\sum_{k=1}^{R}k^{-2} \ll (rR)^{\frac{d-1}{2}} \ll r^{d\frac{d-1}{d+1}}.\end{aligned}$$

Here, again, we replaced the sum over $q \in \mathbb{P}$ with sum over $q \in \mathbb{Z}^d$, which was estimated by the corresponding integral. $\square$

Remark 1. This proof shows the inequality $f_0(P_r) \ll r^{d\frac{d-1}{d+1}}$ (which is case $s = 0$ of Theorem 21.1) directly. Actually, it shows the stronger result that

$$|\partial P_r \cap Z^d| \ll r^{d\frac{d-1}{d+1}}.$$

To see this one has to use the simple fact

$$|F(p) \cap Z^d| \ll \frac{\mathrm{Area}\, F(p)}{||p||}$$

valid for every facet $F(p)$ of P_r. This gives, in Case 1,

$$\sum_p |F(p) \cap Z^d| \ll \sum_p \frac{\mathrm{Area}\, F(p)}{||p||} \ll \sum_p \frac{\rho(p)^{d-1}}{||p||} \ll \sum_p r^{\frac{d-1}{2}} ||p||^{-\frac{d+1}{2}},$$

which is $\ll r^{d\frac{d-1}{d+1}}$, according to (21.8). Case 2 is even simpler. Then

$$|F(p) \cap Z^d| \ll \frac{\mathrm{Area}\, F(p)}{||p||} \ll \mathrm{Area}\, F(p) h(p) \ll \mathrm{vol}\, C(p)$$

and the estimates in the end of Case 2 can be applied. Finally, if $h(p) \le r^{-\frac{d-1}{d+1}}$, the total number of lattice points in the annulus $rB^d \setminus (r - r^{-\frac{d-1}{d+1}})B^d$ is at most $r^{d\frac{d-1}{d+1}}$, as we have checked it before Theorem 21.2.

References

[1] Affentranger, F., Wieacker, J.A.: On the convex hull of uniform random points in a simple d-polytope. Discrete Comp. Geom., **6**, 291–305 (1991).

[2] Andrews, G.E.: A lower bound for the volumes of strictly convex bodies with many boundary points. Trans. AMS, **106**, 270–279 (1993).

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

[4] Arnold, V.I.: Statistics of integral convex polytopes. (in Russian) Funk. Anal. Pril., **14**, 1–3 (1980). English translation: Funct. Anal. Appl., **14**, 79–84 (1980).

[5] Balog, A., Bárány, I.: On the convex hull of the integer points in a disc, DIMACS Series , Vol **6** (1991) *Discrete and Computational Geometry*, 39–44.

[6] Balog, A., Deshouillers, J-M.: On some convex lattice polytopes, *Number theory in progress* **2** (Zakopane 1997), 591–606, de Gruyter, Berlin 1999.

[7] Bárány, I.: Intrinsic volumes and f-vectors of random polytopes. Math. Annalen, **285**, 671–699 (1989).

[8] Bárány, I.: Random polytopes in smooth convex bodies. Mathematika, **39**, 81–92 (1992).

[9] Bárány, I.: The technique of M-regions and cap-coverings: a survey. Rendiconti Palermo, **65**, 21–38 (1999).

[10] Bárány, I.: Sylvester's question: the probability that n points are in convex position. Annals of Prob., **27**, 2020–2034 (2000).

[11] Bárány, I.: A note on Sylvester's four-point problem., Studia Math. Hung., **38**, 2020–2034 (2001).

[12] Bárány, I., Buchta, Ch.: Random polytopes in a convex polytope, independence of shape, and concentration of vertices. Math. Annalen, **297**, 467–497 (1993).

[13] Bárány, I., Howe, R., Lovász, L.: On integer points in polyhedra: a lower bound, *Combinatorica*, **12** (1992), 135–142.

[14] Bárány, I., Larman, D.G.: Convex bodies, economic cap coverings, random polytopes. Mathematika, **35**, 274–291 (1988).

[15] Bárány, I,. Larman, D.G.: The convex hull of the integer points in a large ball. Math. Annalen, **312**, 167–181 (1998).

[16] Bárány, I., Reitzner, M.: Central limit theorems for random polytopes in convex polytopes. manuscript (2005).

[17] I. Bárány and J. Pach, On the number of convex lattice polytopes, *Comb. Prob. Comp.*, **1**(1991), 295–302.

[18] Bárány, I., Vershik, A. M.: On the number of convex lattice polytopes. GAFA Journal, **12**, 381-393 (1992).

[19] Blaschke, W.: Affine Differentialgeometrie. Springer, Berlin, (1923).

[20] Böröczky, K. Jr: Polytopal approximation bounding the number of k-faces. J. Appr. Theory, **102**, 263–285 (1999).

[21] Bräker, H., Hsing, T., Binham, N.H.: On the Hausdorff distance between a convex set and the an interior random convex hull. Adv. in Appl. Probab., **30**, 295–316 (1998).

[22] Buchta, Ch.: An identity relating moments of functionals of convex hulls. Discrete Comp. Geom., **33**, 125–142 (2005).

[23] Cabo, A.J., Groeneboom, P.: Limit theorems for functionals of convex hulls, Probab. Theory. Rel. Fields, **100**, 31–55 (1994).

[24] Calka, P., Schreiber, T.: Large deviation probabilities for the number of vertices of random polytopes in the ball, to appear in Ann. Probab., (2005).

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

[26] Cook, W., Hartman, M., Kannan, K., McDiarmid, C.: On integer points in polyhedra, *Combinatorica*, **12** (1992), 27–37.

[27] Efron, B.: The convex hull of a random set of points. Biometrika, **52**, 331–343 (1965).

[28] Ewald, G., Larman, D.G., Rogers, C.A.: The directions of the line segments and of the r-dimensional balls on the boundary of a convex body in Euclidean space. Mathematika, **17**, 1–20 (1970).

[29] Groemer, H.:On the mean value of the volume of a random polytope in a convex set. Archiv Math., **25**, 86–90 (1997).

[30] Groeneboom, P.: Limit theorems for convex hulls, Probab. Theory. Rel. Fields, **79**, 327–368 (1988).

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

[32] Gruber, P.M.: In most cases approximation is irregular. Rend. Circ. Mat. Torino, **41**, 19–33 (1983).

[33] Gruber, P.M.: Asymptotic estimates for best and stepwise approximation of convex bodies II. Forum Math., **5**, 521–538 (1993).

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

[35] Hsing, T.: On the asymptotic distribution of th area outside a random convex hull in a disk. Ann. Appl. Probab., **4**, 478–493 (1994).

[36] Ivanov, B. A.: Exceptional directions for a convex body. (in Russian), Mat. Zametki, **20**, 365–371 (1976). English translation: Math. Notes **20**, 763–765 (1976).

[37] Jarnik, V.: Über Gitterpunkte und konvex Kurven, *Math. Z.*, **2** (1925), 500-518.

[38] Kannan, R., Lovász, L.: Covering minima and lattice point free convex bodies, *Annals of Math.* **128** (1988), 577–602.

[39] Khintchine, A.: A qualitative formulation of Kronecker's theory of approximation, *Izv. Akad. Nauk SSSR Ser. Mat.*, **12** (1948), 113–122. (in Russian)

[40] Kim, J.H., Vu, V.H.: Concentration of multivariate polynomials and its applications, Combinatorica, **20**, 417–434 (2000).

[41] Klee, V.: Research problem No.5. Bull. AMS, **62**, 419 (1957).

[42] Klee, V.: Can the boundary of a d–dimensional convex body contain segment in all directions? Amer. Math. Monthly, **76**, 408–410 (1969).

[43] Konyagin, S.B., Sevastyanov, S.V.: Estimation of the number of vertices of a convex integral polyhedron in terms of its volume. (in Russian) Funk. Anal. Pril., **18**, 13–15 (1984). English translation: Funct. Anal. Appl., **18**, 11–13 (1984).

[44] Leichtweiss, K.: Affine geometry of convex bodies. Barth, Heidelberg, (1998).

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

[46] Ludwig, M.: Asymptotic approximation of smooth convex bodies by general polytopes. Mathematika, **46**, 103–125 (1999).

[47] Macbeath, A.M.: A theorem on non-homogeneous lattices. Annals of Math., **56**, 269–293 (1952).

[48] Meinardus, G., Zur additiven Zahlentheorie in mehreren Dimensionen, *Math. Annalen*, **132** (1957), 333–346.

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

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

[51] Raynaud, H.: Sur l'enveloppe convexe des nuages de points aléatoires dans $\mathbb{R}^n$. J. Appl. Probab., **7**, 35–48 (1970).

[52] Reisner, S., Schütt, C., Werner, E.:

[53] Reitzner, M.: Random polytopes and the Efron-Stein jackknife inequality. Ann. Probab., **31**, 2136–2166 (2003).

[54] Reitzner, M.: The combinatorial structure of random polytopes. Adv. Math., **191**, 178–208 (2005).

[55] Reitzner, M.: Central limit theorems for random polytopes. Preprint (2005).

[56] Rényi, A., Sulanke, R.: Über die konvexe Hülle von n zufällig gewählten Punkten. Z. Wahrsch. Verw. Geb., **2**, 75-84 (1963).

[57] Rinott, Y.: On normal approximation rates for certain sums of dependent random variables. J. Comput. Appl. Math., **55**, 135–143 (1994).

[58] Rockafellar, T.R.: Convex analysis. Princeton (1970).

[59] Rogers, C.A., *The volume of a polyhedron inscribed in a sphere.* J. London Math. Soc., **28** (1953), 410–416.

[60] Rogers, C.A., and Shephard, G.C., The difference body of a convex body, *Arch. Math.*, **8** (1957), 220–223.

[61] Santaló, L.A.: Integral geometry and geometric probability. Addison-Wiley, Reading MA (1976).

[62] Schmidt, W.: Integral points on surfaces and curves. Monatshefte Math., **99**, 45–82 (1985).

[63] Schneider, R.: Kinematic measures for sets of colliding convex bodies. Mathematika, **25**, 1–12 (1978).

[64] Schneider, R.: Convex bodies: the Brunn-Minkowski theory. Encyclopedia Math. Appl. vol 44. Cambridge University Press, Cambridge (1993).

[65] Schneider, R.: Measures in convex geometry. Rend. Istit. Mat. Univ. Trieste, Suppl., Vol XXIX, 215–265 (1998).

[66] Schneider, R.: Convex bodies in exceptional relative positions. J. London Math. Soc., (1999).

[67] Schneider, R.: Discrete aspects of stochastic geometry. in: Goodman, J.E., O'Rourke, J. (eds.) Handbook of Discrete and Computational Geometry, CRC Press, Boca Raton, 255–278 (2004).

[68] Schütt, C.: Random polytopes and affine surface area. Math. Nachr., **170**, 227–249 (1994).

[69] Schütt, C.: Floating bodies, illumination bodies, and polytopal approximation. in: Ball, K. M. (ed.) Convex Geometric Analysis, Cambridge, Math. Sci. Res. Inst. Publ. **43**, 203–229 (1999).

[70] Schütt, C.: Random polytopes and affine surface area. Math. Nachr., **170**, 227–249 (1994).

[71] Schütt, C., Werner, E.: Polytopes with vertices chosen randomly from the boundary of a convex body. Geometric and Functional Analysis, Lecture Notes in Math. **1807**, 241–422, Springer, Berlin, (2003).

[72] Stein, S., The symmetry function in a convex set, 1954

[73] Sylvester, J.J.: Question 1491. Educational Times, London, April (1864).

[74] Vinogradov, I. M.: On the number of integer points on a sphere, *Izv. Akad.Nauk SSSR Ser. Mat.*, **27** (1963), 957–986. (in Russian)

[75] Vu, V.H.: Concentration of non-Lipschitz functions and applications. Random Struct. Alg., **20**, 262–316 (2002).

[76] Vu, V.H.: Sharp concentration of random polytopes, to appear in GAFA Journal (2005).

[77] Walfisz, A.: Gitterpunkte in mehrdimensionalischen Kugeln, Panstwowe Wydawnictwo Naukowe, Warszawa, 1957.

[78] Wendel, J.G.: A problem in geometric probability. Math. Scand., **11**, 109–111 (1962).

[79] Wieacker, J.A.: Einige Probleme der polyedrische approximation. Diplomarbeit, Albert-Ludwigs-Universität, Freiburg im Breisgau, (1978).

[80] W. Weil, J. A. Wieacker: *Stochastic geometry.* In: Gruber, P.M., Wills, J. (eds.) Handbook of convex geometry, North-Holland, Amsterdam, 1391–1438 (1993).

[81] Wright, E.M., Partitions of multi–partite numbers, *Proc. Amer. Math. Soc.*, **7** (1956), 880–890.

[82] Wright, E.M., Partitions of large bipartites, *Amer. J. Math.*, **80** (1958), 643–658.

[83] Zalgaller, V. A.: k–dimensional directions singular for a convex body F in R^n. (in Russian), Zapiski Sem. Leningrad., **27**, 67–72 (1972). English translation: J. Soviet Math., **3**, 437–441 (1972).