

RANDOM POINTS AND LATTICE POINTS IN CONVEX BODIES

IMRE BÁRÁNY

ABSTRACT. Assume $K \subset \mathbf{R}^d$ is a convex body and X is a (large) finite subset of K . How many convex polytopes are there whose vertices belong to X ? Is there a typical shape of such polytopes? How well does the maximal such polytope (which is actually the convex hull of X) approximate K ? We are interested in these questions mainly in two cases. The first is when X is a random sample of n uniform, independent points from K . In this case motivation comes from Sylvester's famous four-point problem and from the theory of random polytopes. The second case is when $X = K \cap \mathbf{Z}^d$ where \mathbf{Z}^d is the lattice of integer points in \mathbf{R}^d and the questions come from integer programming and geometry of numbers. Surprisingly (or not so surprisingly), the answers in the two cases are rather similar.

1. SYLVESTER'S FOUR-POINT PROBLEM

The study of random points in convex bodies started with an innocent looking question. The year was 1864. The place was London. The journal was the *Educational Times*. Problem 1941 came from J. J. Sylvester [60]. It read: "Show that the chance of four points forming the apices of a reentrant quadrilateral is $1/4$ if they be taken at random in an indefinite plane." Several answers came in. Most of them were different. In 1865 Sylvester [61] concluded, "This problem does not admit of a determinate solution." The reason is, as we all know by now, in "at random in an indefinite plane", since there is no natural probability measure on it. Sylvester immediately modified the question: Let K be a convex body in the plane and choose four random, independent, and uniform points from K . What is the probability that they form the vertices of a reentrant quadrilateral, or, in recent terminology, that their convex hull is a triangle. Further, for what K is this probability the smallest and the largest.

This question has become known as Sylvester's four-point problem, and it has proved to be extremely fertile. It took more than fifty years (and several erroneous proofs) to find the answer. Blaschke showed in [26] and [27] that the probability in question is largest for a triangle and smallest for the disk (or any ellipse). His solution used the method of symmetrization and "shaking down" that have become standard tools since.

Sylvester's question, and its subsequent solution, determined the direction of research for a long time. Many papers have been written starting with the setting: Let $X_n = \{x_1, \dots, x_n\}$ be a random, independent, uniform sample of n points from

Received by the editors November 2, 2007.

2000 *Mathematics Subject Classification*. Primary 52A22, 52B20.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

some fixed d -dimensional convex body K and let K_n denote the convex hull of X_n . Then K_n is a *random polytope* inscribed in K . Define, in the style of Sylvester's question, $p(K, n)$ as the probability that X_n is in convex position, that is, no x_i lies in the convex hull of the others, or in other words, that K_n has exactly n vertices. In this setting, the four-point problem asks for the determination of (the complement of) $p(K, 4)$. Several results have been achieved about $p(K, n)$ for various convex bodies in \mathbf{R}^d with various values of n . We return to them a little later.

2. RÉNYI AND SULANKE

In 1963 a new question concerning random polytopes appeared in a much quoted paper by Rényi and Sulanke [53]. Apparently, Blaschke played a role at the origin of this new direction, almost fifty years after his solution of Sylvester's four-point problem. Here is how Sulanke remembers it [59].

"My motivation for considering problems on geometric probabilities originated in discussion with W. Blaschke on integral geometry: *Express geometrically invariant properties of figures by their integral invariants*. Alfréd Rényi's idea was to pose problems on geometrical probabilities on the base of invariant measures considered in integral geometry. The probabilistic description of random figures, e.g. distributions, moments, asymptotic coefficients, etc., should yield new integral geometric entities containing information about the geometry of the random figures. This general point of view has been the motivation of all my papers about geometric probabilities. We did not consider, and I did not know, Sylvester's four-point problem."

What Rényi and Sulanke observed is the following. For a fixed convex body $K \subset \mathbf{R}^d$, the random polytopes K_n get closer and closer to K as n gets larger and larger with high probability. So how does the random variable $\text{Vol}(K \setminus K_n)$ behave? Also, how do the polytopal properties of K_n , for instance the number of vertices, behave as n tends to infinity? They determined, asymptotically, the expectation of these random variables when K is a polygon and when K has smooth boundary (see [53]). Their result was the starting point of, and the motivation for, hundreds of papers. Most of them are about expectations of various functionals associated with K_n . More recently there have been several breakthrough results concerning the distribution of these random variables, in particular central limit theorems and large deviations.

3. LATTICE POLYTOPES

In this third introductory section we just state two basic problems.

Integer points in convex bodies, in particular disks, balls, and ellipsoids, have been studied for a long time. The *circle problem* asks for the number of lattice points in the circle rB^2 , of radius r centered at the origin. In this paper we are interested in a different question. Namely, consider the integer convex hull $I(K)$ of a convex body K in \mathbf{R}^d which is defined as the convex hull of $K \cap \mathbf{Z}^d$. Motivation for the definition of $I(K)$ comes from integer programming where one wants to maximize a linear function over all integer points in a fixed convex body K , or, what is the same, over the integer convex hull, $I(K)$.

The integer convex hull is clearly a polytope; moreover, it is a lattice polytope, meaning that all of its vertices belong to \mathbf{Z}^d . How many vertices, edges, facets does

it have, for instance, when $K = rB^d$, and r is large? We will come back to this question later.

In a different direction, V. I. Arnold asked the following beautiful and inspiring question in [3]. How many different lattice polytopes are there? Infinitely many, of course. Refine the question then. Two lattice polytopes are said to be *equivalent* if one can be carried to the other by a lattice preserving affine transformation. This is an equivalence relation, and equivalent polytopes have the same volume. The refined question is this: How many equivalence classes are there in dimension d of volume at most W . The answer will be given in Section 14.

The present survey aims at explaining the recent developments on random polytopes, together with the asymptotic behaviour of the expectations. It will also cover old and new results around Sylvester's question. We will see further that random polytopes and lattice polytopes behave quite similarly, although the proof methods in the two cases are different. As a rule, proofs are not given here, with some exceptions where we felt that a sketch can help the reader to understand the underlying ideas better. In particular, we explain how the economic cap covering theorem can be used to estimate expectations and variances. It is not our intention to present every result here: there are too many of them anyway. Rather we try to emphasize directions, new ideas, basic results, and their consequences.

Work on an extended version of this article is in progress. The interested reader will find detailed proofs and further results there. It is going to be a short book, with the same title as this survey, to be published (expected in 2009) in the series Zürich Lectures in Advanced Mathematics, European Mathematical Society, Zürich.

4. NOTATION

A convex body in \mathbf{R}^d is a convex compact set with non-empty interior. We write \mathcal{K} or \mathcal{K}^d for the family of all convex bodies in \mathbf{R}^d . The family of convex polytopes, to be denoted by $\mathcal{P} = \mathcal{P}^d$, and the family of smooth convex bodies, to be denoted by $\mathcal{C} = \mathcal{C}^d$, will often be treated separately. We assume that each $K \in \mathcal{C}^d$ has twice continuously differentiable boundary whose Gauss curvature is positive everywhere. We will not indicate the dimension if there is no danger of ambiguity.

We write \mathcal{K}_1 , \mathcal{P}_1 and \mathcal{C}_1 for the subfamilies where the volume is equal to 1. This is often very convenient since for $K \in \mathcal{K}_1$ the probability measure and the Lebesgue measure coincide.

As usual, $f_j(P)$ denotes the number of j -dimensional faces of a polytope $P \in \mathcal{P}^d$. We write $\text{Vol } S$ for the volume of a set $S \subset \mathbf{R}^d$. Also, $\text{aff } X$ stand for its affine hull, and $\text{conv } X$ or simply $[X]$ for its convex hull, and $\text{bd}S$ for its boundary.

As usual, we will write $E\phi(K_n)$ for the expectation of the random variable $\phi(K_n)$, and $\text{Var } \phi(K_n)$ for its variance. For instance, $Ef_0(K, n)$ is the expectation of the number of vertices of K_n . Since K_n is very close to K with high probability (as n gets large), we are interested in the difference $\text{Vol}(K \setminus K_n)$, which will be denoted by $E(K, n)$.

On the technical side we will use the “big Oh” and “little oh” notation, together with Vinogradov's very convenient \ll and \gg symbols. So $f(n) \ll g(n)$ means that there are constants c_1 and c_2 such that $f(n) \leq c_2g(n)$ for all $n \geq c_1$. These constants of course do not depend on n . Unless otherwise stated, they only depend on dimension. Sometimes we use $f(n) \sim g(n)$ meaning that $f(n) \ll g(n) \ll f(n)$.

Constants will be denoted by $c, c_i, b_j, D, \alpha, \beta$. They usually depend on dimension and their value may vary from place to place.

To avoid complications with trivialities, we assume throughout that the dimension d is at least two.

5. ASYMPTOTIC EXPECTATIONS

Expectations of $\phi(K_n)$, for certain functionals ϕ , can be computed with high precision when $K \in \mathcal{K}^d$ is smooth and when it is a polytope. The basic method for this appears already in Rényi and Sulanke [53]. We give a quick sketch in the case when ϕ is of the form

$$\phi(K_n) = \sum_{F \in \mathcal{F}} \phi(F),$$

where \mathcal{F} is the set of facets of the polytope K_n . So the method applies, for instance, when ϕ is f_{d-1} , or surface area. Since K_n is a simplicial polytope with probability one, each facet is of the form $[x_{i_1}, \dots, x_{i_d}]$. We write $\mathbf{1}\{A\}$ for the indicator function of the event A . Then, assuming $K \in \mathcal{K}_1$,

$$\begin{aligned} E\phi(K_n) &= \sum_{1 \leq i_1 < \dots < i_d \leq n} \int_K \dots \int_K \mathbf{1}\{[x_{i_1}, \dots, x_{i_d}] \in \mathcal{F}\} \\ &\quad \times \phi[x_{i_1}, \dots, x_{i_d}] dx_1 \dots dx_n \\ &= \binom{n}{d} \int_K \dots \int_K \mathbf{1}\{[x_1, \dots, x_d] \in \mathcal{F}\} \phi([x_1, \dots, x_d]) dx_1 \dots dx_n. \end{aligned}$$

Write $V = \text{Vol } C(x_1, \dots, x_d)$ for the volume of the smaller cap, $C(x_1, \dots, x_d)$, cut off from K by $H = \text{aff}\{x_1, \dots, x_d\}$ (which is a hyperplane, almost surely). Since $F = [x_1, \dots, x_d]$ is a facet if and only if x_{d+1}, \dots, x_n are all on one side of H , we have

$$(5.1) \quad E\phi(K_n) = \binom{n}{d} \int_K \dots \int_K [(1 - V)^{n-d} + V^{n-d}] \phi(F) dx_1 \dots dx_d.$$

Next we use the Blaschke-Petkantschin [54] integral formula

$$E\phi(K_n) = \binom{n}{d} \int_G [(1 - V)^{n-d} + V^{n-d}] \phi^*(F) dH,$$

where the integral is taken over the Grassmannian of all hyperplanes with dH denoting the corresponding measure, and where by the Blaschke-Petkantschin integral formula

$$\phi^*(F) = (d-1)! \int_{K \cap H} \dots \int_{K \cap H} \phi(F) V_{d-1}(F) dx_1 \dots dx_d,$$

with the variables in the last integral coming from $K \cap H$, and $V_{d-1}(F)$ is the surface area of F .

Here $V^{n-d} \leq 2^{-(n-d)}$, which is very small. Moreover, $(1 - V)^{n-d}$ is small, again, unless $V \leq cn^{-1} \log n$. So the dominating part of the integral comes from hyperplanes H that are close to the boundary of K in the sense that they cut off a cap of small volume from K .

One can give precise estimates for the last integral in several special cases. For instance, when $\phi = f_{d-1}$ (then $\phi(F) = 1$), the above formula can be directly

evaluated for smooth convex bodies, using local Taylor expansion of $\text{bd}K$; see [53] for $d = 2$ and [70] for $d \geq 2$. The result is that for $K \in \mathcal{C}_1$

$$Ef_{d-1}(K_n) = c_d \Omega(K) n^{\frac{d-1}{d+1}} (1 + o(1)),$$

where $\Omega(K)$ is the affine surface area of K .

Rényi and Sulanke [53] used this method to determine $Ef_0(K_n)$ for convex polygons and smooth planar convex bodies. In the plane $f_0(K_n) = f_1(K_n)$, and $E(K, n)$ can be determined from $Ef_0(K_n)$ by Efron's identity [34] stating that for every convex body $K \in \mathcal{K}_1$

$$(5.2) \quad Ef_0(K_n) = nE(K, n - 1).$$

The technique also works in other cases as well. For small dimensions the f -vector is completely determined by f_{d-1} , and $E(K, n)$ can be determined by Efron's identity. Schneider and Wieacker [56] computed the expectation of the mean width, $V_1(K) - EV_1(K_n)$, when $K \in \mathcal{C}^d$, using the above method. Wieacker [70] determined $E(K, n)$ for the case when $K = B^d$, the unit ball of \mathbf{R}^d . But often the integrals are too difficult to handle and a different approach is needed. We return to this question in Section 9.

The limitation of the integral geometric technique is that it can only apply when K is a polytope or has smooth boundary. In the next two sections we describe another method that works, with less precision though, for general convex bodies.

6. EXPECTATIONS AND THE FLOATING BODY

A *cap* of a convex body $K \in \mathcal{K}^d$ is simply $K \cap H$ where H is a (closed) halfspace. Let X_n be a random sample of n uniform, independent points from K . A cap of volume $1/10n$ contains no point from X_n with high probability, while a cap of volume $10/n$ does contain a point from X_n with high probability. This suggests that K_n is close to what remains of K after deleting all caps of volume $1/n$. For the precise formulation, we need some definitions.

First we define the function $v : K \rightarrow \mathbf{R}$ by

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

The level sets of v are defined, as usual, via

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

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 3-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. The floating body is the intersection of halfspaces, so it is convex.

The above philosophy suggests that K_n is close to the floating body $K(v \geq 1/n)$. Even more importantly, $K \setminus K_n$ is close to the wet part $K(1/n)$. This is the content of the following theorem from [18].

Theorem 6.1. *For every convex body $K \in \mathcal{K}_1$,*

$$\text{Vol } K(1/n) \ll E(K, n) \ll \text{Vol } K(1/n).$$

We emphasize again that, here and later on, the constants applied by the \ll notation depend only on dimension. Theorem 6.1 turns out to be useful when considering the f -vector of K_n . Efron's identity (5.2) and Theorem 6.1 give that order of magnitude of $Ef_0(K_n)$ behaves exactly as $n\text{Vol } K(1/n)$. This fact was extended to all f_j in [8].

Theorem 6.2. *For every convex body $K \in \mathcal{K}_1$ and for all $j = 0, 1, \dots, d-1$,*

$$n\text{Vol } K(1/n) \ll Ef_j(K_n) \ll n\text{Vol } K(1/n).$$

The strength of these two theorems lies in the fact that they hold for all convex bodies, not only for smooth ones or for polytopes. Note further that both K_n and $K(1/n)$ are affine equivariants, which is just as well. Theorem 6.1 says that in order to determine the order of magnitude of $E(K, n)$, it suffices to determine the volume of the wet part which is not a random quantity. An analogous statement holds for $Ef_j(K_n)$. So the next question is about the volume of the wet part $\text{Vol } K(t)$. The following is known about it [18].

Theorem 6.3. *For every convex body $K \in \mathcal{K}_1$, and for all positive $t \leq t_0(d) = (2d)^{-2d}$,*

$$t \left(\log \frac{1}{t} \right)^{d-1} \ll \text{Vol } K(t) \ll t^{\frac{2}{d+1}}.$$

The estimate on the right-hand side is essentially the affine isoperimetric inequality, and the best constant is known. The left-hand side inequality is of the right order of magnitude when K is a polytope. It is conjectured that, in the left-hand side inequality, the best constant appears when K is a simplex. What happens between these two special classes (\mathcal{P}^d and \mathcal{C}^d) is not a mystery; it is the usual unpredictable behaviour. Informally stated, $\text{Vol } K(t)$ approximates the upper bound $t^{2/(d+1)}$ and the lower bound $t(\log \frac{1}{t})^{d-1}$ infinitely often, as $t \rightarrow 0$, for a typical (in the Baire category sense) convex body K .

Theorem 6.1 implies that for every convex body $K \in \mathcal{K}_1$,

$$(6.3) \quad \frac{1}{n}(\log n)^{d-1} \ll E(K, n) \ll n^{-\frac{2}{d+1}}.$$

The right-hand side inequality, which is due to Groemer [36], can be formulated more precisely. Among all convex bodies of volume one, $E(K, n)$ is the largest for the Euclidean ball (or any other ellipse) of volume one. We will see in Section 9 that the quantity on the left- (and right-) hand side is the correct order of magnitude for \mathcal{P}_1 , the class of polytopes (and for \mathcal{C}_1 , the smooth convex bodies).

Theorem 6.1 extends to intrinsic volumes as well. But as intrinsic volumes are not invariant under affine transformations, we have to assume that $K \in \mathcal{K}^d$ contains a ball of radius r and is contained in a ball of radius R . Under these conditions the following holds (cf. [8]). For all $j = 1, \dots, d$

$$V_j(K) - V_j(K(v \geq 1/n)) \ll V_j(K) - EV_j(K_n) \ll V_j(K) - V_j(K(v \geq 1/n)),$$

where the implied constants depend on d, r, R . (Here $V_j(K)$ denotes the j th intrinsic volume of K .) But the behaviour of $V_j(K) - V_j(K(v \geq t))$ is not known in general, so we do not have the analogs of Theorem 6.3 or the inequality (6.3).

The proof of Theorems 6.1 and 6.2 is simplified by the following

Fact 6.4. $nE(K, n-1) = Ef_0(K_n) \ll Ef_1(K_n) \ll \dots \ll Ef_{d-1}(K_n)$.

Here the equality is just Efron's identity (5.2). The subsequent inequalities are implied by the fact that K_n is simplicial with probability one, and for a simplicial polytope $f_j(K_n) \leq (j+2)f_{j+1}(K_n)$ when $j = 0, 1, \dots, d-2$. These inequalities follow easily by estimating, in two ways, the number of pairs (F_{j+1}, F_j) where F_j is a j -dimensional face contained in F_{j+1} which is a $j+1$ -dimensional face.

Fact 6.4 implies that, for the proof of Theorems 6.1 and 6.2, it suffices to prove two things:

Lemma 6.5. $\text{Vol } K(1/n) \ll E(K, n)$.

Lemma 6.6. $E f_{d-1}(K_n) \ll n \text{Vol } K(1/n)$.

Lemma 6.5 is very easy to prove. The *minimal cap* belonging to $x \in K$ is a cap $C(x)$ of K with $x \in C(x)$ and $\text{Vol } C(x) = v(x)$. Note that the minimal cap $C(x)$ need not be unique, so our notation is a little ambiguous. Observe that

$$\text{Prob}[x \notin K_n] \geq \text{Prob}[C(x) \cap X_n = \emptyset] = (1 - v(x))^n,$$

which implies that, for every $t \in [0, 1]$,

$$\begin{aligned} E(K, n) &= \int_K \text{Prob}[x \notin K_n] dx \geq \int_K (1 - v(x))^n dx \\ &\geq \int_{K(t)} (1 - t)^n dx = (1 - t)^n \text{Vol } K(t). \end{aligned}$$

Choosing here $t = 1/n$ finishes the proof. (We mention that this method works in a much more general setting as well.)

The proof of Lemma 6.6 is more difficult yet interesting and instructive, so I will give a sketch. It uses the so-called *economic cap covering theorem*, which is stated in the next section. Afterward, we will return to the proof of Lemma 6.6

7. ECONOMIC CAP COVERINGS

The economic cap covering theorem is from [18] and [8]. It says that the wet part $K(t)$ can be covered by caps of volume $\ll t$ economically.

Theorem 7.1. *Given $K \in \mathcal{K}_1$ and a positive $t < (2d)^{-2d}$, there exist caps C_1, \dots, C_m and pairwise disjoint convex sets C'_1, \dots, C'_m with $C'_i \subset C_i$ such that*

- (i) $\bigcup_1^m C'_i \subset K(t) \subset \bigcup_1^m C_i$;
- (ii) $\text{Vol } C_i \ll t$, ($i = 1, \dots, m$), and $\text{Vol } C'_i \gg t$, ($i = 1, \dots, m$);
- (iii) *Every cap C of volume t is contained in some C_i .*

Here (i) and (ii) just say that the C_i cover the wet part, but do not overcover it. These conditions show how many caps are needed in the economic covering:

$$(7.4) \quad \text{Vol } K(t)/t \ll m \ll \text{Vol } K(t)/t.$$

We will write K^d for the set of ordered d -tuples (x_1, \dots, x_d) from K . Recall that such a d -tuple defines, with probability one, the smaller cap $C(x_1, \dots, x_d)$ cut off by the hyperplane $H = \text{aff}\{x_1, \dots, x_d\}$ from K . Its volume is $V = \text{Vol } C(x_1, \dots, x_d)$. Condition (iii) of the economic cap covering theorem directly implies the following

Corollary 7.2. *If $K \in \mathcal{K}_1$ and $t \leq (2d)^{-2d}$, then*

$$\{(x_1, \dots, x_d) \in K^d : V \leq t\} \subset \bigcup_1^m (C_i, \dots, C_i),$$

where C_1, \dots, C_m are from Theorem 7.1.

The next corollary expresses a useful concavity property of the function $t \rightarrow \text{Vol } K(t)$. It says that, apart from the constant implied by the \gg notation, the d th root of $\text{Vol } K(t)$ is a concave function. This will be sufficient for our purposes, that is, for the proof of Lemma 6.6.

Corollary 7.3. *If $K \in \mathcal{K}_1$ and $t \leq (2d)^{-2d}$, and $\lambda \geq 1$, then*

$$\text{Vol } K(t) \gg \lambda^{-d} \text{Vol } K(\lambda t).$$

Theorem 6.1 is based on the idea that $K \setminus K_n$ and the wet part $K(1/n)$ are close to each other. The cap covering theorem can be used to prove that K_n contains the wet part $K(c \log n/n)$ with high probability.

Theorem 7.4. *For every $d \geq 2$ every $c > 1$ there is $c' > 0$ such that for every $K \in \mathcal{K}_1$ and for large enough n*

$$\text{Prob}(K(c' \log n/n) \subset K_n) \geq n^{-c}.$$

This useful fact is proved in [15]. Another and more general proof, using VC-dimension, was given by Van Vu [67].

8. PROOF OF LEMMA 6.6

We are going to use (5.1) with $\phi = f_{d-1}$ in which case $\phi(F) = 1$ if F is a facet of K_n and 0 otherwise.

$$(8.5) \quad Ef_{d-1}(K_n) = \binom{n}{d} \int_K \dots \int_K [(1 - V)^{n-d} + V^{n-d}] dx_1 \dots dx_d.$$

We split the domain of integration into two parts: K^* is the subset of K^d , where the function V is smaller than $(c \log n)/n$, and K^0 is where $V \geq (c \log n)/n$. The constant c will be chosen large but depending only on d . Clearly, $V \leq 1/2$. The integrand over K^0 is small:

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

which is smaller than $n^{-(d+1)}$ if c is chosen large enough (depending only on d). Then the contribution of the integral on K^0 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 $2^{-h} \leq (c \log n)/n$. 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 7.1 with $t = 2^{-h}$.

Assume now that $(x_1, \dots, x_d) \in K^*$. The cap $C(x_1, \dots, x_d)$ has volume V . We associate with (x_1, \dots, x_d) the maximal h such that, for some $C_i \in \mathcal{M}_h$, $C(x_1, \dots, x_d) \subset C_i$. Such a maximal h exists by (iii) of Theorem 7.1. It follows that

$$V = \text{Vol } C(x_1, \dots, x_d) \leq \text{Vol } C_i \ll 2^{-h}$$

and, by the maximality of h ,

$$V = \text{Vol } C(x_1, \dots, x_d) \geq 2^{-h-1},$$

since otherwise $C(x_1, \dots, x_d)$ would be contained in a cap from \mathcal{M}_{h+1} .

For such an (x_1, \dots, x_d) , we have

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

Instead of integrating over K^* , we integrate each (x_1, \dots, x_d) on its associated $C_i \in \mathcal{M}_h$. In formula (8.5) the integral on $C_i \in \mathcal{M}_h$ is bounded by

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

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

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

where the last inequality follows from (7.4).

The rest of the proof is a direct computation using properties of the cap covering. We sum first for $h \geq h_1$, where h_1 is defined by $2^{-h_1} \leq 1/n < 2^{-h_1+1}$. The sum from h_1 to infinity is estimated via

$$\begin{aligned} \sum_{h_1}^{\infty} \dots &\leq \sum_{h_1}^{\infty} \exp\{-(n-d)2^{-h+1}\} 2^{-h(d-1)} \text{Vol } K(1/n) \\ &\leq \text{Vol } K(1/n) \sum_{h_1}^{\infty} 2^{-h(d-1)} \leq n^{-(d-1)} \text{Vol } K(1/n). \end{aligned}$$

When $h_0 \leq h < h_1$, we set $h = h_1 - k$ so k runs from 1 to $k_1 = \log \log n + \log c$. Corollary 7.3 shows that $\text{Vol } K(2^{-h}) \leq \text{Vol } K(2^k/n) \ll 2^{kd} \text{Vol } K(1/n)$. Thus,

$$\begin{aligned} \sum_{h_0}^{h_1-1} \dots &\ll \sum_{k=1}^{k_1} \exp\{-(n-d)2^{-h_1+k-1}\} 2^{(-h_1+k)(d-1)} 2^{kd} \text{Vol } K(1/n) \\ &\ll n^{-(d-1)} \text{Vol } K(1/n) \sum_{k=1}^{k_1} \exp\{-(n-d)2^k/n\} 2^{k(d-1)} 2^{kd} \\ &\ll n^{-(d-1)} \text{Vol } K(1/n), \end{aligned}$$

where the last step is justified easily.

Remark. This proof shows the power and usefulness of the economic cap covering theorem. It gives a new method for estimating integrals of the type (8.5): instead of integrating over all d -tuples from K , we split integration on suitably chosen caps from \mathcal{M}_h . On each cap the integral can be estimated directly. The computation is then reduced to estimating an infinite sum which can be done by standard methods using properties of the cap covering.

9. FURTHER EXPECTATIONS

The integral geometric technique of Section 5 did not work for $Ef_0(K_n)$ or for $E(K, n)$. Determining them had been an open problem for some time. The solution in the case when $K \in \mathcal{C}_1$ came from Bárány [9], and somewhat more generally from Schütt [57]. The cap covering technique was used in [9] to show that K_n behaves essentially independently in the vicinity of two points from $\text{bd}K$ when n is large enough. The method is a combination of the integral geometric approach with this independence structure. The result is similar to $Ef_{d-1}(K_n)$, only the constants differ. For all $K \in \mathcal{C}_1$,

$$Ef_0(K_n) = c_0 \Omega(K) n^{\frac{d-1}{d+1}} (1 + o(1)),$$

where $\Omega(K)$ is the affine surface area of K and c_0 is a constant depending only on d . By Efron's identity, the analogous result holds for $E(K, n)$.

We write P instead of K when the mother body is a polytope, and write P_n instead of K_n for the corresponding random polytope. In the case of simple polytopes, Affentranger and Wieacker [1] extended the integral geometric approach to the case when $\phi(F)$ (F is a facet of P_n) is of special form, namely, when $\phi(F) = (w(F)V_{d-1}(F))^q$. Here $w(F)$ is the width of the cap cut off by $\text{aff}(F)$ from P , in the direction of the outer normal to F , and q is a positive integer. Using this result, the case of general, non-simple polytopes was solved by Bárány and Buchta [14]:

Theorem 9.1. *For a polytope $P \in \mathcal{K}_1$*

$$E(P, n) = \frac{T(P)}{(d+1)^{d-1}(d-1)!} \frac{\log^{d-1} n}{n} (1 + o(1)).$$

Here $T(P)$ is the number towers of P , where a tower of P is a chain $F_0 \subset F_1 \subset \dots \subset F_{d-1}$, where F_i is an i -dimensional face of P .

The main novelty in the proof of Theorem 9.1 is that most of the volume missed by P_n is concentrated in small simplices associated with the towers of P . Another feature of the proof is “independence of shape”: the missed volume near a fixed point of the boundary is almost independent of other parts of the boundary. This implies that what happens in one of those small simplices is essentially independent of what happens in another small simplex. Then the missed volume in each small simplex is the same and can be determined from the result of Affentranger and Wieacker [1].

The difference between the random polytopes K_n (coming from $K \in \mathcal{C}^d$) and P_n (coming from $P \in \mathcal{P}^d$) is beautifully highlighted here. The vertices of K_n are distributed almost uniformly near the boundary of K , their density depends on the local curvature. The vertices of P_n are distributed in the small simplices. In both cases, the independence of shape phenomenon prevails.

Recently, Matthias Reitzner [49] found a way to extend the integral geometric method so that it becomes applicable in many more cases. To explain what the main novelty is, assume that the convex hull of the random points $x_1, \dots, x_k \in X_n$ determines a $(k-1)$ -face, F , of K_n . Let L be the orthogonal complement of F , and let K'_n be the projection of K_n onto L . It is clear that F is a $(k-1)$ -face of K_n if and only if the projection of F onto L is a vertex of K'_n . This transforms the determination of $Ef_{k-1}(K_n)$ into a lower-dimensional problem, provided all positions of $\text{aff}F$, together with the choice of k uniform, independent points in

$K \cap \text{aff} F$ are taken into account. The method leads, again, to Blaschke-Petkantschin type integral geometric formulae. After lengthy and non-trivial computations, these formulae can be evaluated in the case when K is smooth and when K is a simple polytope. (The extension to the non-simple case uses the independence structure and the small simplices from [14].) The outcome is that $E f_j(K_n)$ is asymptotically equal to $c_j \Omega(K) n^{(d-1)/(d+1)}$ for convex bodies in \mathcal{C}_1 , and to $b_j T(P) (\log n)^{d-1}$ for polytopes $P \in \mathcal{P}^d$, with constant depending on j and d .

10. VARIANCES

Many papers have been devoted to determine the expectation of various functionals of K_n . Yet until quite recently, very little has been known about the distribution of these functionals. A few notable exceptions will be mentioned in Section 11. Wieacker and Weil, in their survey article [69] in 1993 complain that “the determination of the variance, for instance, is a major open problem.”

The first result in this direction is due to Küfer [45]. He shows the upper bound $O(n^{-(d+3)/(d+1)})$ for the variance of the missed volume when the mother body is the unit ball. He extends this result for spherically symmetric distributions with regularly varying tails.

The first general result concerning variances comes from a remarkable paper of M. Reitzner [50]. He has established an upper bound on the variance of the volume of K_n (which is the same as the variance of the missed volume) and on $f_j(K_n)$ in the case of smooth convex bodies K :

$$\begin{aligned} \text{Var Vol } K_n &\leq c(K) n^{-(d+3)/(d+1)}, \\ \text{Var } f_j(K_n) &\leq c(K) n^{(d-1)/(d+1)}, \end{aligned}$$

where the constants $c(K)$ depend on K and dimension only. These estimates are based on the jackknife inequality of Efron and Stein [35], which implies (we omit the details) that

$$\text{Var Vol } K_n \leq (n+1) E(\text{Vol } K_{n+1} - \text{Vol } K_n)^2.$$

On the next page we give a short sketch of the method. It starts, quite naturally, with a coupling argument since K_{n+1} is just the convex hull of K_n and x_{n+1} , the last point from the random sample X_{n+1} . For simpler notation we write y for x_{n+1} . Let \mathcal{F} be the collection of those facets F of K_n for which y is not on the same side of the hyperplane $\text{aff} F$ as K_n . Clearly, $\mathcal{F} = \emptyset$ if $y \in K_n$. We write $[n]$ for the set $\{1, \dots, n\}$. The difference $K_{n+1} \setminus K_n$ is the union of (pairwise internally disjoint) simplices $[F, y]$ with $F \in \mathcal{F}$. For a d -subset I of $[n]$, let F_I denote the convex hull of $\{x_i : i \in I\}$. Then, with \sum_I denoting summation over all d -element subsets of $[n]$,

$$\begin{aligned} \text{Vol } K_{n+1} - \text{Vol } K_n &= \sum_{F \in \mathcal{F}} \text{Vol } [F, y] \\ &= \sum_I \mathbf{1}\{F_I \in \mathcal{F}\} \text{Vol } [F_I, y] \leq \sum_I \mathbf{1}\{F_I \in \mathcal{F}\} V(F_I), \end{aligned}$$

where $V(F_I)$ denotes the volume of the cap $C(F_I)$ containing y which is cut off by the hyperplane $\text{aff} F_I$. (This is well defined if $F_I \in \mathcal{F}$ and is irrelevant otherwise.) Now

$$(\text{Vol } K_{n+1} - \text{Vol } K_n)^2 = \sum_I \sum_J \mathbf{1}\{F_I \in \mathcal{F}\} V(F_I) \mathbf{1}\{F_J \in \mathcal{F}\} V(F_J).$$

By symmetry we can assume that $V(F_I) \geq V(F_J)$ at the price of a factor 2. When integrating, we can assume, again by symmetry, that $I = [d]$, $I \cap J = [k]$ and $J = [k] \cup \{d+1, \dots, 2d-k\}$ and $k \in \{0, 1, \dots, d\}$. Write $F = F_I$ and $G = F_J$ with these I and J . So we have

$$E(\text{Vol } K_{n+1} - \text{Vol } K_n)^2 \leq 2 \sum_{k=0}^d \binom{n}{d} \binom{d}{k} \binom{n-d}{d-k} \int_K \dots \int_K \mathbf{1}\{F \in \mathcal{F}\} \\ \times V(F) \mathbf{1}\{G \in \mathcal{F}\} V(G) \mathbf{1}\{V(F) \geq V(G)\} dx_1 \dots dx_n dy$$

with the extra condition that $y \in C(F) \cap C(G)$. Consider now the above integral for a fixed k . Using Theorem 7.4, it is not hard to see that this integral is concentrated on the part where $V(F) \leq (c \log n)/n$. Since $F \in \mathcal{F}$, the variables x_{2d-k+1}, \dots, x_n all lie in the complement of $C(F)$, their total contribution is at most $(1 - V(F))^{n-(2d-k)}$. This shows that the integral for a fixed k is at most

$$\int_K \dots \int_K (1 - V(F))^{n-2d+k} V(F) V(G) \mathbf{1}\{y \in C(F) \cap C(G)\} \\ \times \mathbf{1}\{V(G) \leq V(F) \leq \frac{c \log n}{n}\} dx_1 \dots dx_{2d-k} dy.$$

When K is smooth, the last integral can be estimated using local approximation of K and integral geometric methods. This is what happens in [50]. But the cap covering technique, the one used in Section 8 works just as well. Moreover, it works not only for smooth convex bodies, but for polytopes as well. The outcome is that for a polytope $K \in \mathcal{P}_1$

$$(10.6) \quad \text{Var Vol } K_n \leq c(K) \frac{1}{n^2} (\log n)^{d-1},$$

and the constant $c(K)$ is proportional to the number of towers of K . The variance of $f_j(K_n)$ can also be estimated analogously. In that case we have, with the same remark about $c(K)$ as above,

$$\text{Var } f_j(K_n) \leq c(K) (\log n)^{d-1}.$$

These results are stated, without proof, in Bárány and Reitzner [22].

The upper bounds imply a strong law of large numbers for the corresponding functionals.

What about lower bounds for the variances? In [51] Reitzner gives a matching lower bound when $K \in \mathcal{C}_1$:

$$\text{Var Vol } K_n \geq c(K) n^{-(d+3)/(d+1)}, \\ \text{Var } f_j(K_n) \geq c(K) n^{(d-1)/(d+1)}.$$

These lower bounds have been extended to every convex body $K \in \mathcal{K}_1$ in the following form:

$$(10.7) \quad \text{Var Vol } K_n \gg \frac{1}{n} \text{Vol } K(1/n), \\ \text{Var } f_j(K_n) \gg \text{Vol } K(1/n).$$

The proof is given in [22]. It is based on properly decomposing the variance (just as in [51]), and on the cap covering technique combined with a little convex geometry.

The last results suggest that, in general,

$$\begin{aligned}\text{Var Vol } K_n &\sim \frac{1}{n} \text{Vol } K(1/n), \text{ and} \\ \text{Var } f_j(K_n) &\sim \text{Vol } K(1/n)\end{aligned}$$

for all convex bodies in \mathcal{K}_1 , with the implied constants depending only on dimension. This is confirmed in the case when K is in \mathcal{P}_1 or in \mathcal{C}_1 by the previously given upper bounds. Also, it can be proved in the planar case with ad hoc methods.

11. CENTRAL LIMIT THEOREMS

The few exceptions where the variance had been known are connected to the few cases when the central limit theorem had been established. One of them is Groeneboom's result [37] proving a central limit theorem in the following form. For a polygon P in the plane, the distribution of $f_0(P_n)$ is close to normal. Namely, if P has r vertices, then

$$\frac{f_0(P_n) - \frac{2}{3}r \log n}{\sqrt{\frac{10}{27}r \log n}} \rightarrow \mathcal{N}(0, 1)$$

in distribution, where $\mathcal{N}(0, 1)$ is the standard normal distribution. Further, Cabo and Groeneboom [31] proved for a polygon P of area 1, in a version suggested by Buchta [30], that

$$\frac{(1 - \text{Vol } P_n) - \frac{2}{3}r \frac{\log n}{n}}{\sqrt{\frac{28}{27}r \frac{\log n}{n^2}}} \rightarrow \mathcal{N}(0, 1),$$

again in distribution. Groeneboom showed the central limit theorem for the case of the unit disk and f_0 , with the variances evaluated numerically. Hsing [40] proved that, with $K = B^2$ the unit disk,

$$\frac{(\pi - \text{Vol } K_n) - c_1 n^{-2/3}}{\sqrt{c_2 n^{-5/3}}} \rightarrow \mathcal{N}(0, 1)$$

in distribution, again, with more or less explicit constants c_1 and c_2 . The asymptotic distribution of the Hausdorff distance between a planar convex body K and K_n has been determined with high precision by Bräker, Hsing, and Bingham in [28].

A general central limit theorem was proved by Matthias Reitzner in [51]. It applies in the case when $K \in \mathcal{C}_1$, and it is about the Poisson random polytope Π_n (and not the usual random polytope K_n). The Poisson polytope is defined by $\Pi_n = [K \cap X(n)]$, where $X(n)$ is a Poisson process of intensity n . For an alternative definition, let N be a random variable which is Poisson distributed with mean n . Then K_m is equal to $\Pi_n | N = m$. Reitzner proved the central limit theorem for $\text{Vol } \Pi_n$ and $f_j(\Pi_n)$, a remarkable achievement, in the following form.

Theorem 11.1. *There is a function $\varepsilon(n)$, tending to zero as $n \rightarrow \infty$, such that for every $K \in \mathcal{C}_1$,*

$$\left| \text{Prob} \left(\frac{\text{Vol } \Pi_n - E \text{Vol } \Pi_n}{\sqrt{\text{Var } \text{Vol } \Pi_n}} \leq x \right) - \Phi(x) \right| \leq c(K) \varepsilon(n),$$

and for all $j = 0, \dots, d-1$

$$\left| \text{Prob} \left(\frac{f_j(\Pi_n) - E f_j(\Pi_n)}{\sqrt{\text{Var } f_j(\Pi_n)}} \leq x \right) - \Phi(x) \right| \leq c(K) \varepsilon(n),$$

where $c(K)$ is a constant depending only on K .

Here $\varepsilon(n) = n^{-1/2+1/(d+1)}(\log n)^c$ where c depends only on d .

The basic idea of the proof is to use a central limit theorem with weak dependence (instead of the usual independence condition). This idea was actually suggested by Avram and Bertsimas in [4], and the right central limit theorem for this purpose is Rinott’s theorem [52] (or another one by Baldi and Rinott [5]), which is often the convenient form of C. Stein’s version of the central limit theorem.

The weak dependence is given by the so-called *dependency graph*, which is defined as follows: Let $\zeta_i, i \in W$, be a finite collection of random variables. The graph $G = (W, E)$ is said to be a dependency graph for ζ_i if for any pair of disjoint sets $W_1, W_2 \subset W$, such that no edge in E goes between W_1 and W_2 , the sets of random variables $\{\zeta_i : i \in W_1\}$ and $\{\zeta_i : i \in W_2\}$ are independent.

Theorem 11.2 (Rinott). *Let $\zeta_i, i \in W$, be random variables having a dependency graph G . Set $\zeta = \sum_{i \in W} \zeta_i$ and $\sigma^2(\zeta) = \text{Var } \zeta$. Denote the maximal degree of G by D and suppose that $|\zeta_i - E\zeta_i| \leq M$ almost surely. Then*

$$\left| \text{Prob} \left(\frac{\zeta - E\zeta}{\sqrt{\text{Var } \zeta}} \leq x \right) - \Phi(x) \right| \leq \frac{1}{\sqrt{2\pi}} \frac{DM}{\sigma(\zeta)} + 16 \frac{|W|^{\frac{1}{2}} D^{\frac{3}{2}} M^2}{\sigma^2(\zeta)} + 10 \frac{|W| D^2 M^3}{\sigma^3(\zeta)}.$$

When using this theorem, one has to construct the dependency graph, define the random variables ζ_i , and prove the necessary properties. Also, one needs a lower bound on $\text{Var } \zeta$.

Here is a sketch of how the construction goes for the case of $\text{Vol } \Pi_n$. Set $T = (c \log n)/n$ where c is a large constant, and take an economic cap covering of the wet part $K(v \leq T)$, with covering caps C_1, \dots, C_m . Introduce the condition $K(v \geq T) \subset \Pi_n$ and denote it by A . (By Theorem 7.4, $K(v \geq T) \subset K_n$ happens with very high probability. It is not hard to see that condition A holds with high probability as well.)

First we prove the central limit theorem under condition A . Choose a subset $S_i \subset C_i \cap K(v \leq T)$ so that the S_i are pairwise internally disjoint and their union is $K(v \leq T)$. This is clearly possible. The random variables are $\zeta_i = \text{Vol}(S_i \cap \Pi_n)$. The vertex set of the graph G is then $[m]$. In order to define the edges of G , let L_i be the set of points $x \in K(v \leq T)$ *visible from S_i within $K(v \leq T)$* . This means that $x \in L_i$ if there is $a \in S_i$ such that the segment $[x, a] \subset K(v \leq T)$, or, what is the same, $[x, a] \cap K(v > T) = \emptyset$. Now two vertices $i, j \in [m]$ form an edge in G if there is a point visible within $K(v \leq T)$ from both S_i and S_j , that is, $L_i \cap L_j \neq \emptyset$. It is not hard to see that the maximal degree of G is bounded by a constant that depends only on d . (The proof is based on the fact that only a bounded number of caps can have a common point, which follows from $K \in \mathcal{C}^d$.) The next lemma shows that G is the independence graph with random variables ζ_i .

Lemma 11.3. *Assume condition A holds. Given disjoint subsets W_1, W_2 of W with no edge between them, the random variables $\{\zeta_i : i \in W_1\}$ are independent of the random variables $\{\zeta_j : j \in W_2\}$.*

The explanation is simple. Under condition A the random variable ζ_i is determined by those facets of Π_n that intersect S_i . Thus each vertex b on such a facet is visible from an $a \in S_i$ within $K(v \leq T)$. So all vertices that belong to a facet intersecting S_i come from L_i . If there is no edge between W_1 and W_2 , then $\bigcup\{L_i : i \in W_1\}$ and $\bigcup\{L_j : j \in W_2\}$ are disjoint, and so the corresponding variables are independent, due to a basic property of the Poisson process.

It is also clear that, under condition A , $\zeta = \sum \zeta_i = \text{Vol } \Pi_n - \text{Vol } K(v \geq T)$. The lower bound (10.7) on the variance $\text{Var Vol } K_n$ carries over to that of Π_n showing that $\text{Var Vol } \Pi_n \geq c(K)n^{-(d+3)/(d+1)}$. Also, $\text{Vol } S_i \leq \text{Vol } C_i \leq (c \log n)/n$. Thus, Rinott's theorem applies, and a quick check proves Theorem 11.1 under condition A .

The next task is to remove condition A . This can be done by the following *transference lemma* from [25], which has been used in an implicit form in [51] and in [68], and perhaps elsewhere as well.

Lemma 11.4. *Let ξ_n and ξ'_n be two series of random variables with means μ_n and μ'_n , variances σ_n^2 and σ'^2_n , respectively. Assume that there are functions $\varepsilon_1(n)$, $\varepsilon_2(n)$, $\varepsilon_3(n)$, $\varepsilon_4(n)$, all tending to zero as n tends to infinity such that*

- (i) $|\mu'_n - \mu_n| \leq \varepsilon_1(n)\sigma_n$.
- (ii) $|\sigma'^2_n - \sigma_n^2| \leq \varepsilon_2(n)\sigma_n^2$.
- (iii) For every x , $|\text{Prob}(\xi'_n \leq x) - \text{Prob}(\xi_n \leq x)| \leq \varepsilon_3(n)$.
- (iv) For every x ,

$$\left| \text{Prob}\left(\frac{\xi'_n - \mu'_n}{\sigma'_n} \leq x\right) - \Phi(x) \right| \leq \varepsilon_4(n).$$

Then there is a positive constant C such that for every x ,

$$\left| \text{Prob}\left(\frac{\xi_n - \mu_n}{\sigma_n} \leq x\right) - \Phi(x) \right| \leq C \sum_{i=1}^4 \varepsilon_i(n).$$

It is quite easy, though technical, to finish the proof of the central limit theorem for $\text{Vol } \Pi_n$. The proof for $f_j(\Pi_n)$ goes along very similar lines.

Next comes the central limit theorem for K_n , and one would like to use the transference lemma between K_n and Π_n , or rather, between $\text{Vol } K_n$ and $\text{Vol } \Pi_n$. The difficult point is to prove condition (ii), that is, the corresponding variances are very close to each other. This was achieved by Van Vu in [68] using his tail estimates from [67]. Here is Van Vu's remarkable central limit theorem.

Theorem 11.5. *There is a function $\varepsilon(n)$, tending to zero as $n \rightarrow \infty$, such that for every $K \subset \mathcal{C}_1$,*

$$\left| \text{Prob}\left(\frac{\text{Vol } K_n - E\text{Vol } K_n}{\sqrt{\text{Var Vol } K_n}} \leq x\right) - \Phi(x) \right| \leq c(K)\varepsilon(n),$$

and for all $j = 0, \dots, d - 1$,

$$\left| \text{Prob}\left(\frac{f_j(K_n) - Ef_j(K_n)}{\sqrt{\text{Var } f_j(K_n)}} \leq x\right) - \Phi(x) \right| \leq c(K)\varepsilon(n),$$

where $c(K)$ is a constant depending only on K .

Here $\varepsilon(n) = n^{-1/(d+1)+o(1)}$.

The method has been extended to other cases as well, for instance when K is a polytope. The following central limit theorem has been proved by Reitzner and Bárány in [22].

Theorem 11.6. *There is a function $\varepsilon(n)$, tending to zero as $n \rightarrow \infty$, such that for every polytope $K \subset \mathcal{P}_1$,*

$$\left| \text{Prob}\left(\frac{\text{Vol } K_n - E\text{Vol } K_n}{\sqrt{\text{Var Vol } K_n}} \leq x\right) - \Phi(x) \right| \leq c(K)\varepsilon(n),$$

and for all $j = 0, \dots, d - 1$,

$$\left| \text{Prob} \left(\frac{f_j(K_n) - E f_j(K_n)}{\sqrt{\text{Var } f_j(K_n)}} \leq x \right) - \Phi(x) \right| \leq c(K)\varepsilon(n),$$

where $c(K)$ is a constant depending only on K .

Here $\varepsilon_i(n)$ is of order $(\log n)^{-\frac{d-1}{2}+o(1)}$, and $c(K)$ is a constant times a power of the number of towers of K . We describe the proof in a nutshell. It uses the transference lemma several times. First, one works with Poisson polytopes Π_n , under the condition that Π_n is sandwiched between the floating bodies $K(v \geq s)$ and $K(v \geq T)$, where $T = (\alpha \log \log n)/n$ and $s = \mathbf{1}/(n \log^\beta n)$, where α and β are suitable constants depending only on dimension. Note that both s and T are very close to $1/n$. The sandwiching happens with high probability. The vertex set of dependency graph G is defined similarly, using a cap covering of $K(v \leq T)$ consisting of caps C_1, \dots, C_m , just S_i is a subset of $C_i \cap K(s \leq v \leq T)$. A pair $i, j \in [m]$ is an edge of G , a point $b \in K(s \leq v \leq T)$ is visible from both S_i and S_j within $K(v \leq T)$. This time it is harder to give an upper bound on the maximal degree, D , of G .

Theorem 11.7. $D \ll T(K)^4(\log \log n)^{4(d-1)}$.

Of course, $\zeta_i = \text{Vol}(\Pi_n \cap K(v \leq T))$, and again $\zeta = \text{Vol } \Pi_n - \text{Vol } K(v \geq T)$. The variance is known (see the previous section). All conditions of Rinott’s theorem are satisfied. Its conclusion gives the central limit theorem for $\text{Vol } \Pi_n$ under the condition of sandwiching. Removing this condition is technical and lengthy. The transference lemma is applied again, this time between $\text{Vol } \Pi_n$ and $\text{Vol } K_n$, which is technical and exhausting but there are no serious difficulties. (The case of $f_j(K_n)$ is worse.)

Finally, we mention one of the geometric lemmas that is crucial for the proof. Given $z \in K(v \leq T)$, define $S(z, T)$ as the set of points $x \in K$ that see z within $K(v \leq T)$, that is, the segment $[z, x]$ is disjoint from $K(v > T)$. We need a bound on the volume of $S(z, T)$, assuming that $K \in \mathcal{P}_1$.

Lemma 11.8. *If $0 < 2v(z) \leq T \leq 1/2$, then*

$$\text{Vol } S(z, T) \ll F(P) T \log^{d-1} \left(\frac{T}{v(z)} \right).$$

Note that the inequality $\text{Vol } S(z, T) \ll F(P) T (\log 1/T)^{d-1}$ follows immediately from the fact that $S(z, T) \subset P(v \leq T)$. The improvement from $1/T$ to $T/v(z)$ (which is an improvement only if $v(z) > T^2$) is a significant step in the proof of Theorem 11.6.

One remark is in place here. Perhaps it is more natural to work with Poisson polytopes Π_n than with ordinary random polytopes.

12. TAIL ESTIMATES

Let Y_n be a functional on the random polytope K_n , for instance $Y_n = \text{Vol } K_n$. We have seen that its expectation can be determined with high precision, its variance can be estimated quite well, and Y_n obeys the central limit theorem near its expectation. The next target is to estimate the tail probabilities

$$\text{Prob}(|Y_n - EY_n| \geq T).$$

Of course, a precise and complete description of the tail probability would tell almost everything one may wish to know about Y_n . But such a description is, in general, hopeless. Still, one can prove good estimates on these probabilities. For instance, the inequality

$$\text{Prob}(|Y_n - EY_n| \geq \sqrt{\lambda \text{Var } Y_n}) \leq c_1 \exp\{-c_2 \lambda\}$$

would say that Y_n has exponential, or sub-Gaussian tail. (Here c_1, c_2 are positive constants.) Such an inequality would have important consequences on the higher moments of Y_n , or the concentration of Y_n around its expectations, etc.

An inequality of exponential type has been proved by Van Vu in the breakthrough paper [67]. To present his results, we assume that $K \in \mathcal{K}_1$, $z \in K(v \leq t)$ with $t \in (0, (2d)]^{-2d}$. Recall the definition from the previous section:

$$S(z, t) = \{x \in K : [x, z] \cap K(v > t) = \emptyset\}.$$

So $S(z, t)$ is the set of points, *visible from z within $K(v \leq t)$* . Also, $S(z, t)$ is the union of all caps of volume t that contain z . Next define

$$g(t) = \sup_{z \in K(v \leq t)} \text{Vol } S(z, t).$$

Note that for $K \in \mathcal{C}_1$, $g(t) \sim t$, while for a polytope K , $g(t) \sim t(\log 1/t)^{d-1}$. This follows since for a polytope, $\text{Vol } S(z, t)$ is maximal when z is a vertex, and the union of $S(z, t)$ over all vertices z of K contains $K(v \leq t)$. Finally, set

$$\tilde{V} = \tilde{V}(n, t) = 36ng^2(t)\text{Vol } K(t),$$

which, as we will see soon, is not far from the variance. Here is Van Vu’s exponential tail inequality.

Theorem 12.1. *Assume $K \in \mathcal{K}_1$. Then there are positive constants α, c, t_0 such that the following holds. For every $t \in ((\alpha \log n)/n, t_0]$ and every $\lambda \in (0, n\text{Vol } K(t)]$, we have*

$$\text{Prob}\left(|\text{Vol } K_n - E\text{Vol } K_n| \geq \sqrt{\lambda \tilde{V}}\right) \leq 2 \exp\{-\lambda/4\} + \exp\{-ctn\}.$$

It is hard to appreciate the importance of this result at first sight. We present some of its consequences. Set $t = (\alpha \log n)/n$ and define with this value of t

$$\tilde{V}_n = \tilde{V}(n, t) = \tilde{V}(n, (\alpha \log n)/n).$$

Corollary 12.2. *Assume $K \in \mathcal{K}_1$. Then the k th moment, M_k , of $\text{Vol } K_n$ satisfies*

$$M_k = O(\tilde{V}_n^{k/2}).$$

In particular, for a polytope, $M_k = O(n^{-2}(\log n)^{3kd/2})$.

Note that for the variance (which is the second moment), this estimate is just a little weaker than the truth (10.6) and (10.7). Another consequence is the concentration of $\text{Vol } K_n$ near its expectation which we present for the polytopal case.

Corollary 12.3. *Assume $K \in \mathcal{K}_1$ and $f(n) = \delta(n)n^2(\log n)^{-3d-1/2}$, where $\delta(n)$ is a function tending to zero arbitrarily slowly. Then, almost surely,*

$$\lim_{n \rightarrow \infty} \left| \frac{\text{Vol } K_n}{E\text{Vol } K_n} - 1 \right| f(n) = 0.$$

In the case when $K \in \mathcal{C}_1$, Corollary 12.2 gives an estimate for the variance which is a power of a $\log n$ factor off the true variance. For this case, Van Vu proves a more precise version of Theorem 12.1.

Theorem 12.4. *Assume $K \in \mathcal{C}_1$. Then there are positive constants α, c such that the following holds. For every $\lambda \in \left(0, \alpha n^{\frac{(d-1)(d+3)}{(d+1)(3d+5)}}\right]$ and with $\tilde{V} = 4\alpha n^{\frac{d+3}{d+1}}$, we have*

$$\text{Prob}\left(|\text{Vol } K_n - E\text{Vol } K_n| \geq \sqrt{\lambda \tilde{V}}\right) \leq 2 \exp\{-\lambda/4\} + \exp\{-cn^{(d-1)/(3d+5)}\}.$$

We state, rather informally, the two consequences of this theorem that are analogous to the two corollaries above. If $K \in \mathcal{C}_1$, then the k th moment, M_k , of $\text{Vol } K_n$ satisfies

$$M_k = O\left(n^{\frac{k}{2} \frac{d+3}{d+1}}\right).$$

Note that this estimate gives the right order of magnitude for the variance. For the concentration of $\text{Vol } K_n$ we have

$$\lim_{n \rightarrow \infty} \left| \frac{\text{Vol } K_n}{E\text{Vol } K_n} - 1 \right| \delta(n) n^{(d+3)/(d+1)} (\log n)^{-1/2} = 0$$

for any function $\delta(n)$ tending to zero as $n \rightarrow \infty$.

The proof of Theorem 12.1 is based on a divide-and-conquer martingale technique due to Van Vu [65] and Kim and Vu [43]. It is a strengthening of Azuma’s inequality, and it has proved very powerful in other cases as well (cf. [66], [43]). The method works for other functionals such as $f_j(K_n)$ although there are serious difficulties and new ideas are needed. Also, the proof of Theorem 12.4 is not straightforward. Several novel ideas are used, including interesting geometric properties of the wet part and of $S(z, t)$. The interested reader is advised to read Van Vu’s excellent paper [68].

Here is a large deviation theorem, due to Calka and Schreiber [32], which is similar to Theorem 2.11 from Van Vu’s paper [67]. It is about the number of vertices of K_n when the underlying body $K = B^d$. Write Z_n for $f_0(K_n)$ in this case. The result says that for every $\varepsilon > 0$,

$$\liminf_{n \rightarrow \infty} \frac{1}{\log n} \log(-\log \text{Prob}\{|Z_n - EZ_n| > \varepsilon EZ_n\}) \geq \frac{d-1}{3d+5}.$$

There is another approach to random polytopes, using Poisson approximation and the theory of stochastic processes, which is beyond the scope of this survey. The generic result of this approach can be summarized as follows: The random point measures induced by the vertices of the convex hull of a Poisson sample from the unit ball, when properly rescaled and centered, converge to those of a mean zero Gaussian field. Such a result gives more than just, say, the central limit theorem for the number of vertices of the convex hull. However, it does not seem to cover other functionals such as $\text{Vol } K_n$ or $f_j(K_n)$. For more information, see, e.g., Penrose and Yukich [47] and the references therein.

13. THE INTEGER CONVEX HULL

We return now to the question posed in Section 3. Recall that the integer convex hull, $I(K)$, of a (large) convex body $K \in \mathcal{K}^d$ has been defined as

$$I(K) = \text{conv}(K \cap \mathbf{Z}^d) = [K \cap \mathbf{Z}^d].$$

Define $\mathcal{Z}^d \subset \mathcal{P}^d$ as the family of lattice polytope (with positive volume). Thus $I(K) \in \mathcal{Z}^d$, if K is “large”. We are interested in the number of vertices, $f_0(I(K))$. For simplicity we consider the case $K = rB^d$, r large. (Other smooth convex bodies behave very similarly.)

We start by quoting a beautiful theorem of G. E. Andrews [2] from 1963.

Theorem 13.1. *For all $P \in \mathcal{Z}^d$,*

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

The proof is not easy. By now there are several other proofs available, by Konyagin and Sevastyanov [44], Schmidt [55], Bárány and Vershik [24], Bárány and Larman [19], and Reisner, Schütt and Werner [48]. All of them are based on different ideas and none of them is simple.

The following even more general statement was proved in [44] and [19]. For all $P \in \mathcal{Z}^d$

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

For simpler notation write $P_r = I(rB^d)$. The result implies, of course, that

$$f_j(P_r) \ll r^{d(d-1)/(d+1)}.$$

It was proved in [6] (case $d = 2$) and in [19] that

$$(13.8) \quad f_j(P_r) \gg r^{d(d-1)/(d+1)}.$$

The proof in [19] is based on estimating the volume missed by P_r , which is defined, as expected, as $M_r = \text{Vol } rB^d - \text{Vol } P_r$.

Lemma 13.2. $M_r \ll r^{\frac{d-1}{d+1}}$.

The proof of the lemma relies on the Flatness Theorem (cf. [42], [41]) saying that the lattice width of a convex body $K \in \mathcal{K}^d$ with $K \cap \mathbf{Z}^d = \emptyset$ is bounded by a number depending only on d . The proof of (13.8) is finished by invoking a result from the theory of approximation of convex bodies by polytopes. It is well known that a polytope with n vertices and inscribed in B^d misses $\gg n^{-\frac{2}{d-1}}$ volume of B^d . After suitable scaling we get

$$(f_0(P_r))^{-\frac{2}{d-1}} \ll \frac{M_r}{\text{Vol } rB^d} \ll r^{d\frac{d-1}{d+1}-d} = r^{-\frac{2d}{d+1}},$$

directly implying (13.8).

The method works for $f_j(P_r)$ as well (by suitably extending the approximation result from vertices to j -dimensional faces), and gives

$$f_j(P_r) \gg r^{d\frac{d-1}{d+1}}.$$

The example P_r shows that the exponent in Andrews’ theorem is best possible. Another, earlier example of the same type was given by V. I. Arnold in [3]. We explain it in the planar case; extending it to higher dimensions is left to the reader. Let P be the convex hull of the points (x, x^2) , where $x \in \mathbf{Z}$ and $-(n-1)/2 \leq x \leq (n-1)/2$ when n is odd, and $-(n-2)/2 \leq x \leq n/2$ when n is even. Trivially, $f_0(P) = n$. It is easy to check that the area of P is very close to $n^3/12$.

Actually, the result $f_j(P_r) \sim r^{d\frac{d-1}{d+1}}$ is what one would expect if random polytopes and the integer convex hull of convex bodies (of rB^d in particular) behave similarly. For proper scaling we have to assume that $n = \text{Vol } rB^d \sim r^d$. The expected number of vertices of the random polytope K_n in rB^d (or, what is the same, in B^d) is of order

$n^{(d-1)/(d+1)} \sim r^{d \frac{d-1}{d+1}}$. Note however, that while $E f_0(K_n)$ is known asymptotically, only the order of magnitude of $f_0(P_r)$ has been established. A little more is known in the planar case. Balog and Deshoullier [7] determined the limit, as $R \rightarrow \infty$ of the average of $r^{-2/3} f_0(P_r)$ on the interval $r \in [R, R + H]$. Here H slowly goes to infinity with R .

Motivation for considering the integer convex hull comes from the geometry of numbers, the circle problem, and from integer programming. In integer programming one wants to know that $I(K)$ does not have too many vertices, assuming, say, that K is a rational polytope. This simply means that K is given by m inequalities with integral coefficients. The size of such an inequality is the number of bits necessary to encode it as a binary string. Then the size of the rational polytope is the sum of the sizes of the defining inequalities. Cook, Hartman, Kannan, and McDiarmid [33] showed that for a rational polytope $K \in \mathcal{P}^d$ of size ϕ ,

$$f_0(I(K)) \leq 2m^d (12d^2 \phi)^{d-1}.$$

Most likely, the inequality $f_j(I(K)) \ll \phi^{d-1}$ holds for all $j = 1, \dots, d-1$ as well (with the implied constant depending on d and m), but there is no proof in sight.

The above inequality for $f_0(I(K))$ is best possible, as shown by Bárány, Howe, and Lovász in [17]. The construction uses algebraic number theory. Further, it shows that the estimate $f_j(I(K)) \ll \phi^{d-1}$, for all j , is best possible, if true.

There is a further parallel between random polytopes and the integer convex hull, to be more precise, the *randomized integer convex hull*. Randomization is introduced here since the usual integer convex hull of an individual convex body may have few vertices. For instance, if Q is an aligned cube (or box) in \mathbf{R}^d , then $I(Q)$ always has 2^d vertices, while the integer convex hull of a randomly rotated copy of Q can have many more vertices. For randomization, the lattice \mathbf{Z}^d is replaced by L , a randomly translated and rotated copy of \mathbf{Z}^d , and we investigate the randomized integer convex hull

$$I_L(K) = \text{conv}(K \cap L)$$

for a fixed convex body K . More precisely, for a translation vector $t \in [0, 1]^d$ and a rotation $\rho \in SO(d)$ around the origin, we set $L_{t,\rho} = \rho(\mathbf{Z}^d + t)$, and define

$$\mathcal{L} = \{L_{t,\rho} : t \in [0, 1]^d, \rho \in SO(d)\}.$$

A natural probability measure on \mathcal{L} is defined as the product of the Lebesgue measure on $[0, 1]^d$ and of the normalized Haar measure on $SO(d)$. This measure is invariant under isometries of \mathbf{R}^d .

If the convex body K is too flat, it may not contain a single lattice point. That is why we need to assume that our convex body K is round. We say that $K \in \mathcal{K}^d$ is D -rounded if K contains a ball of radius r and is contained in a concentric ball of radius R and $R/r \leq D$. It is clear that $\text{Vol } I(K) > 0$, and then $I(K) \in \mathcal{Z}^d$, if $K \in \mathcal{K}$ is D -rounded and has large enough volume. The next result is from Bárány and Matoušek [20].

Theorem 13.3. *Given d and D , there exist positive constants c_0 , depending only on d and D , such that for all D -rounded $K \in \mathcal{K}^d$ with $\text{Vol } K > c_0$,*

$$\text{Vol } K(v < 1) \ll E f_0(I_L(K)) \ll \text{Vol } K(v < 1)$$

where the implied constants depend only on d and D .

When comparing the randomized integer convex hull with a random polytope in K , the proper scaling is again $\text{Vol } K = n$. Under this convention, case $j = 0$ of Theorem 6.2 says that

$$\text{Vol } K(v < 1) \ll Ef_0(K_n) \ll \text{Vol } K(v < 1)$$

as $n \rightarrow \infty$, with the implied constants depending only on d . This inequality and Theorem 13.3 show a strong analogy between random polytopes and the randomized integer convex hull. Most likely, $Ef_j(I_L(K))$ behaves like $Ef_j(K_n)$ for all j , but a proof looks hopeless for the time being.

We mention that the analogy, surprisingly, does not extend to the expected missed area, which is just $E\text{Vol}(K \setminus I_L(K))$. In the case when, say, $Q \in \mathcal{K}^2$ is a square of (large) area A , the expected missed area of $I(Q)$ is of order $(\log A)^2$, while with the proper normalization $n = A$, $E(Q, n)$ is only of order $\log A$. Details can be found in [20]. When working on the expected missed area, we encountered (and solved) the following interesting question, a relative of Buffon's needle problem. Given a convex body $C \in \mathcal{K}^2$, determine the probability that $L \cap C$ is lattice-point free when $L \in \mathcal{L}$ is a random lattice.

14. ARNOLD'S QUESTION

Recall that two convex lattice polytopes, $P, Q \in \mathcal{Z}^d$, are said to be equivalent if there is a lattice-preserving affine transformation $T : \mathbf{R}^d \rightarrow \mathbf{R}^d$ such that $TP = Q$. Equivalent polytopes have the same volume. Let $N_d(V)$ denote the number of equivalence classes whose volume is at most V . In [3] Arnold asks for the determination of $\log N_d(V)$. He proves that, in the planar case,

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

as V goes to infinity. Arnold's proof is based on the estimate in Theorem 13.1 in the planar case (that he found independently of Andrews [2]), and on the *square lemma*. This lemma states that every convex lattice polygon of area V is contained in an aligned square of side length $36V$. From this, the upper bound follows easily.

Arnold's question turned out to be fertile, and Konyagin and Sevastyanov [44] proved Theorem 13.1, again independently of Andrews [2]. They used it, together with an extension of the square lemma, to show that

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

The extra log factor was removed by Bárány and Vershik in [24]. (In the planar case this had been done earlier in [21].)

Theorem 14.1. *When $d \geq 2$ and $V \rightarrow \infty$, then*

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

The proof is based on several ideas from number theory, convexity, and geometry of numbers. It uses the following extension of the square lemma. First, let \mathbf{Z}_+^d be the set of all $a = (a_1, \dots, a_d) \in \mathbf{Z}^d$ where each $a_i > 0$. Next, given $a \in \mathbf{Z}_+^d$, we define the box of a as

$$\text{Box}(a) = \{x \in \mathbf{R}^d : 0 \leq x_i \leq a_i\}.$$

For simplicity set $\prod a = \prod_1^d a_i$. Here is the *box lemma* which replaces the square lemma in the proof.

Lemma 14.2. *For every $P \in \mathcal{Z}^d$ there is an $a \in \mathbf{Z}_+^d$ with $\prod a \ll \text{Vol } P$ such that an equivalent copy of P is contained in $\text{Box}(a)$. The implied constant depends only on d .*

As the number of boxes with $\prod a \ll V$ is less than V^d (actually, much less), the next step in the proof of the upper bound in Theorem 14.1 is the following fact.

Lemma 14.3. *For every $a \in \mathbf{Z}_+^d$ the number of convex lattice polytopes contained in $\text{Box}(a)$ is at most*

$$\exp \left\{ c_d \left(\prod a \right)^{\frac{d-1}{d+1}} \right\},$$

where c_d is a constant depending only on d .

The proof of this lemma is quite intricate, using ideas from generating functions, convex geometry, and geometry of numbers. It is too involved to be explained here.

The proof of the lower bound in Theorem 14.1 is easier. Consider $P \in \mathcal{Z}^d$ with $n = f_0(P) \gg (\text{Vol } P)^{\frac{d-1}{d+1}}$, for instance P_r , the integer convex hull of rB^d . Let X be the set of vertices of P . For each non-empty subset Y of X , $\text{conv} Y$ is a convex lattice polytope in \mathbf{R}^d , of volume at most $\text{Vol } P$. There are $2^n - 1$ such polytopes. It is not hard to see that most of them are d -dimensional and very few of them are equivalent. This shows the lower bound in Theorem 14.1.

We remark that this argument can be turned around and used for the proof of Andrews' Theorem 13.1. Suppose that $P \in \mathcal{Z}^d$ and $\text{Vol } P \leq V$. By Lemma 14.2 we can assume that P lies in some $\text{Box}(a)$ with $\prod a \ll V$. Again, let X be the set of vertices of P . For each (non-empty) subset Y of X , $\text{conv} Y$ is a convex polytope in $\text{Box}(a)$. These polytopes are all distinct and their number is $2^{|X|} - 1$. By Lemma 14.3,

$$2^{|X|} - 1 \leq \exp \left\{ c_d \left(\prod a \right)^{\frac{d-1}{d+1}} \right\} \ll \exp \left\{ c'_d V^{\frac{d-1}{d+1}} \right\}$$

with a suitable constant c'_d , implying, in turn, that $|X| = f_0(P) \ll V^{\frac{d-1}{d+1}}$.

Theorem 14.1 immediately raises the following problem. Decide whether

$$\lim_{V \rightarrow \infty} V^{-\frac{d-1}{d+1}} \log N_d(V)$$

exists or not. Determine the limit if it exists. This problem looks hard. The answer is not known even in the planar case. Even if this problem is too hard, we may be able to see how many convex lattice polytopes there are in $\text{Box}(a)$. The planar version of this question will be considered in the remainder of this section.

We set up the problem a little differently. Define the lattice \mathbf{Z}_t as $\frac{1}{t}\mathbf{Z}^2$, t is large, so \mathbf{Z}_t is a shrunken copy of \mathbf{Z}^2 . Let $K \in \mathcal{K}^2$ be a convex body, and define $\mathcal{P}(K, t)$ as the family of all convex \mathbf{Z}_t -lattice polygons that are contained in K . How many such polygons are there, and what do they look like? This beautiful and inspiring question is due to A. M. Vershik.

It comes as a pleasant surprise that $\log |\mathcal{P}(K, t)|$ can be determined quite precisely. The following result is from [11].

Theorem 14.4. *For every $K \in \mathcal{K}^2$*

$$\lim_{t \rightarrow \infty} t^{-2/3} \log |\mathcal{P}(K, t)| = 3 \sqrt[3]{\frac{\zeta(3)}{4\zeta(2)}} A^*(K).$$

Here $A^*(K)$ is the supremum (actually, maximum) of the affine perimeter that a convex body contained in K can have. See Blaschke [27], or Bárány [11] for the definition and properties of affine perimeter. It is shown in [11] that there is a unique convex body $K_0 \subset K$ whose affine perimeter equals $A^*(K)$. The correspondence $K \mapsto K_0$ gives a map $\mathcal{K}^2 \rightarrow \mathcal{K}^2$ which is affinely equivariant, that is, for every non-degenerate affine transformation T , $(TK)_0 = T(K_0)$. The unique K_0 has interesting properties. For instance, it contains no line segments on its boundary, and its boundary is a parabola arc whenever it lies in the interior of K . See [11] and [12] for further properties of K_0 .

The convex polygons in $\mathcal{P}(K, t)$ have a limit shape: almost all of them are very close to K_0 . This is the content of the next theorem, where $\text{dist}(X, Y)$ denotes the Hausdorff distance of $X, Y \subset \mathbf{R}^2$.

Theorem 14.5. *For every $K \in \mathcal{K}^2$ and every $\varepsilon > 0$,*

$$\lim_{t \rightarrow \infty} \frac{|\{P \in \mathcal{P}(K, t) : \text{dist}(P, K_0) < \varepsilon\}|}{|\mathcal{P}(K, t)|} = 1.$$

This theorem was first proved in the case when K is the unit square. Then K_0 is bounded by four parabola arcs, each touching consecutive edges of the unit square at their midpoints. This case was proved by Vershik in [63] and Bárány in [10]. Sinai in [58] gave a probabilistic proof, together with a central limit theorem on the distribution of the convex \mathbf{Z}_t -lattice polygons lying in the vicinity of K_0 . The case of general $K \in \mathcal{K}^2$ comes from [11].

More recently, Vershik and Zeitouni [64] established central limit theorems and large deviation results about how big a fraction of $\mathcal{P}(K, t)$ is close to K_0 .

15. BACK TO SYLVESTER

Recall the definition from Section 1: for $K \in \mathcal{K}$, $p(K, n)$ denotes the probability that X_n , a random sample of n independent, uniform points from K , is in convex position. Blaschke's solution [26] to Sylvester's four-point problem is that for every convex body $K \in \mathcal{K}^2$

$$p(\text{triangle}, 4) \leq p(K, 4) \leq p(\text{disk}, 4).$$

Of course, $p(K, n)$ can be defined for convex bodies $K \in \mathcal{K}^d$ with $d > 2$ as well. Most of the known results are about the case when $K = B^d$, the Euclidean unit ball: Hostinsky [38] determined $p(B^3, 5)$, later Kingman [39] calculated $p(B^d, d+2)$. Miles [46] showed $\lim_{d \rightarrow \infty} p(B^d, d+3) = 1$. He conjectured and Buchta [29] showed $\lim_{d \rightarrow \infty} p(B^d, d+m) = 1$ for every fixed $m > 3$. Bárány and Füredi [16] proved that $p(B^d, n)$ is close to one as long as $n < d^{-1}2^{d/2}$ and close to zero for $n > d2^{d/2}$.

Returning to the planar case, Valtr [62] showed in 1997 that

$$p(\text{triangle}, n) = \frac{2^n(3n-3)!}{(n-1)!^3(2n)!},$$

a surprisingly exact result.

Theorems 14.4 and 14.5 offer a new way to look at Sylvester's four-point problem. We can determine the size of $\mathcal{P}(K, t)$ with high precision, and the typical shape of a polygon in it. So we may be able to do the same when the points are chosen randomly from K . This is indeed the case for $K \in \mathcal{K}^2$. Even the probability $p(K, n)$ can be determined [12]:

Theorem 15.1. *For every $K \in \mathcal{K}_1^2$*

$$\lim n^2 \sqrt[n]{p(K, n)}$$

exists and equals $\frac{e^2}{4}(A^(K))^3$.*

Here $A^*(K)$ is the same as in Theorem 14.4. Moreover, conditional on X_n being in convex position, the polygon $\text{conv} X_n$ is very close K_0 , the unique convex subset of K having maximal affine perimeter.

The proof of Theorem 15.1 is based on various properties of K_0 and an interesting probabilistic/geometric lemma. The setting is this. Let T be a triangle with two distinguished vertices a, b . Again, X_n is a random sample from T . We say that X_n *forms a convex chain* in T if the points of X_n together with a and b are in convex position. The lemma (from [62] and [12]) says that the probability that X_n forms a convex chain in T is equal to

$$\frac{2^n}{n!(n+1)!},$$

again, a surprisingly exact result.

Theorem 14.4 has its analog in the random case. Let $Q(X_n)$ be the random collection of all convex polygons spanned by the points of X_n , i.e., $P \in Q(X_n)$ if and only if $P = \text{conv}\{x_{i_1}, \dots, x_{i_k}\}$ for some k -tuple $x_{i_1}, \dots, x_{i_k} \subset X$ that is in convex position ($k \geq 3$). The expectation of $|Q(X_n)|$ can be determined, cf. [12]:

Theorem 15.2. *For each $K \in \mathcal{K}_1^2$ we have*

$$\lim_{n \rightarrow \infty} n^{-1/3} \log E|Q(X_n)| = 3 \cdot 2^{-2/3} A^*(K).$$

Again, there is a limit shape to the elements of $Q(X_n)$: the overwhelming majority of the polygons in $Q(X_n)$ are very close to K_0 . Also, a version of the central limit theorem can be proved in this case [23].

Something can be saved in higher dimensions. It is shown in [13] that for $K \in \mathcal{K}_1^d$

$$c_1 \leq n^{\frac{2}{d-1}} \sqrt[n]{p(K, n)} \leq c_2$$

with positive constants c_1, c_2 that depend on dimension only.

ACKNOWLEDGMENTS

Part of this paper was written on a pleasant and fruitful visit by the author to the Institute for Advanced Study at the Hebrew University in Jerusalem. Thanks are due to the excellent ambiance and working conditions there. The author is indebted to Matthias Reitzner for useful comments on an earlier version of this paper. Partial support from Hungarian National Foundation Grants T 062321 and T 060427, and from the European Community Research project “Discrete and Convex Geometry” is also acknowledged.

ABOUT THE AUTHOR

Imre Bárány is at the Rényi Institute of the Hungarian Academy of Sciences (in Budapest), and is a professor at University College London. His research interest is discrete and convex geometry, and its applications. He was an invited speaker at the ICM 2002 in Beijing.

REFERENCES

- [1] Affentranger, F., Wieacker, J.A.: On the convex hull of uniform random points in a simple d -polytope. *Discrete Comp. Geom.*, **6** (1991), 291–305. MR1098810 (92c:52004)
- [2] Andrews, G.E.: A lower bound for the volumes of strictly convex bodies with many boundary points. *Trans. Amer. Math. Soc.*, **106** (1993), 270–279. MR0143105 (26:670)
- [3] Arnold, V.I.: Statistics of integral convex polytopes. (in Russian) *Funk. Anal. Pril.*, **14**, 1–3 (1980). English translation: *Funct. Anal. Appl.*, **14** (1980), 79–84. MR575199 (81g:52011)
- [4] Avram, F., Bertsimas, D.: On central limit theorems in geometrical probability. *Ann. Appl. Probab.*, **3** (1993), 1033–1046. MR1241033 (95d:60022)
- [5] Baldi, P., Rinott, Y.: On normal approximations of distributions in terms of dependency graphs. *Ann. Probab.*, **17** (1989), 1646–1650. MR1048950 (91c:60024)
- [6] Balog, A., Bárány, I.: On the convex hull of the integer points in a disk, in: *Discrete and Computational Geometry* (eds. J.E. Goodman, R. Pollack, and W. Steiger), DIMACS Series no. **6** (1991), 39–44. MR1143287 (93b:11083)
- [7] Balog, A., Deshouliers, J-M.: On some convex lattice polytopes. in: *Number theory in progress, Vol. 2* (Zakopane-Kościelisko, 1997), 591–606, de Gruyter, Berlin, 1999. MR1689533 (2000f:11083)
- [8] Bárány, I.: Intrinsic volumes and f -vectors of random polytopes. *Math. Annalen*, **285** (1989), 671–699. MR1027765 (91c:52008)
- [9] Bárány, I.: Random polytopes in smooth convex bodies. *Mathematika*, **39** (1992), 81–92. MR1176473 (93k:52002)
- [10] Bárány, I.: The limit shape of convex lattice polygons, *Discrete Comp. Geom.*, **13** (1995), 270–295. MR1318778 (95m:52037)
- [11] Bárány, I.: Affine perimeter and limit shape, *J. Reine Angew. Math.*, **484** (1997), 71–84. MR1437299 (98a:52026)
- [12] Bárány, I.: Sylvester’s question: the probability that n points are in convex position. *Annals of Prob.*, **27** (2000), 2020–2034. MR1742899 (2001a:60010)
- [13] Bárány, I.: A note on Sylvester’s four-point problem. *Studia Math. Hung.*, **38** (2001), 2020–2034. MR1877770 (2002m:60020)
- [14] Bárány, I., Buchta, Ch.: Random polytopes in a convex polytope, independence of shape, and concentration of vertices. *Math. Annalen*, **297** (1993), 467–497. MR1245400 (95g:52005)
- [15] Bárány, I., Dalla, L.: Few points to generate a random polytope, *Mathematika*, **44** (1997), 325–331. MR1600549 (99b:52008)
- [16] Bárány, I., Füredi, Z.: On the shape of the convex hull of random points, *Prob. Theory Rel. Fields*, **77** (1988), 231–240. MR927239 (89g:60030)
- [17] Bárány, I. Howe, R., Lovász, L.: On integer points in polyhedra: a lower bound. *Combinatorica*, **12** (1992), 135–142. MR1179250 (93g:52012)
- [18] Bárány, I., Larman, D.G.: Convex bodies, economic cap coverings, random polytopes. *Mathematika*, **35** (1988), 274–291. MR986636 (90c:52020)
- [19] Bárány, I., Larman, D.G.: The convex hull of the integer points in a large ball. *Math. Annalen*, **312** (1998), 167–181. MR1645957 (99i:52014)
- [20] Bárány, I., Matoušek, J.: The randomized integer hull. *Discr. Comp. Geom.*, **33** (2005), 3–25. MR2104706 (2006b:52003)
- [21] Bárány, I., Pach, J.: On the number of convex lattice polygons, *Combinatorics, Probability, and Computation*, **1** (1992), 295–302. MR1211319 (93m:52017)
- [22] Bárány, I., Reitzner, M.: Central limit theorems for random polytopes in convex polytopes. manuscript (2007)
- [23] Bárány, I., Rote, G., Steiger, W., Zhang, C.: A central limit theorem for random convex chains. *Discrete Comp. Geom.*, **30** (2000), 35–50.
- [24] Bárány, I., Vershik, A.M.: On the number of convex lattice polytopes. *GAFJ Journal*, **12** (1992), 381–393. MR1191566 (93k:52013)
- [25] Bárány, I., Vu, H.V.: Central limit theorems for Gaussian polytopes. *Annals of Prob.*, **35** (2007), 1593–1621. MR2330981
- [26] Blaschke, W.: Über affine Geometrie XI: Lösung des “Vierpunktproblem” von Sylvester aus der Theorie der geometrischen Wahrscheinlichkeiten. *Leipziger Berichte*, **69** (1917), 436–453.
- [27] Blaschke, W.: *Affine Differentialgeometrie*. Springer, Berlin, (1923).

- [28] Bräker, H., Hsing, T., Bingham, N.H.: On the Hausdorff distance between a convex set and an interior random convex hull. *Adv. in Appl. Probab.*, **30** (1998), 295–316. MR1642840 (99f:60020)
- [29] Buchta, C.: On a conjecture of R.E. Miles about the convex hull of random points, *Monatsh. Math.*, **102** (1986), 91–102. MR861933 (88f:60016)
- [30] Buchta, C.: An identity relating moments of functionals of convex hulls. *Discrete Comput. Geom.* **33** (2005), 125–142. MR2105754 (2005j:60022)
- [31] Cabo, A. J., Groeneboom, P.: Limit theorems for functionals of convex hulls. *Probab. Theory Relat. Fields*, **100** (1994), 31–55. MR1292189 (95g:60017)
- [32] Calka, P., Schreiber, T.: Large deviation probabilities for the number of vertices of random polytopes in the ball, *Adv. in Appl. Probab.*, **38** (2006), 47–58. MR2213963 (2007a:60011)
- [33] Cook, W., Hartman, M., Kannan, R., McDiarmid, C.: On integer points in polyhedra. *Combinatorica*, **12** (1992), 27–37. MR1167473 (93e:52025)
- [34] Efron, B.: The convex hull of a random set of points. *Biometrika*, **52** (1965), 331–343. MR0207004 (34:6820)
- [35] Efron, B., Stein, C.: The jackknife estimate of variance. *Ann. Statist.*, **9** (1981), 586–596. MR615434 (82k:62074)
- [36] Groemer, H.: On the mean value of the volume of a random polytope in a convex set. *Archiv Math.*, **25** (1997), 86–90. MR0341286 (49:6036)
- [37] Groeneboom, P.: Limit theorems for convex hulls. *Probab. Theory Relat. Fields*, **79** (1988), 327–368. MR959514 (89j:60024)
- [38] Hostinsky, B.: Sur les probabilités géométriques. *Publ. Fac. Sci. Univ. Brno* (1925).
- [39] Kingman, J. F. C.: Random secants of a convex body. *J. Appl. Probab.*, **6** (1969), 660–672. MR0254891 (40:8098)
- [40] Hsing, T.: On the asymptotic distribution of the area outside a random convex hull in a disk. *Ann. Appl. Probab.*, **4** (1994), 478–493. MR1272736 (95d:60047)
- [41] Kannan, R., Lovász, L.: Covering minima and lattice point free convex bodies. *Annals of Math.*, **128** (1988), 577–622. MR970611 (89i:52020)
- [42] Khintchin, A.: A quantitative formulation of Kronecker’s theory of approximation. (in Russian) *Izv. Akad. Nauk SSSR, Ser. Mat.*, **12** (1948), 113–122. MR0024925 (9:569d)
- [43] Kim, J.H., Vu, V.H.: Concentration of multivariate polynomials and its applications. *Combinatorica*, **20** (2000), 417–434. MR1774845 (2002b:05123)
- [44] 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** (1984), 13–15. English translation: *Funct. Anal. Appl.*, **18** (1984), 11–13. MR739085 (86g:52020)
- [45] Küfer, K.-H.: On the approximation of the ball by random polytopes. *Adv. Applied Probab.*, **26** (1994), 876–892. MR1303867 (96j:60012)
- [46] Miles, R. E., Isotropic random simplices. *Adv. Appl. Probab.*, **3** (1971), 353–382. MR0309164 (46:8274)
- [47] Penrose, M.D., Yukich, J.E.: Normal approximation in geometric probability. Stein’s method and applications, 37–58, Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap., 5, Singapore Univ. Press, Singapore, 2005. MR2201885 (2007f:60015)
- [48] Reisner, Sh., Schütt, C., Werner, E.: Dropping a vertex or a facet from a polytope. *Forum Math.*, **13** (2001), 359–378. MR1831090 (2002f:52003)
- [49] Reitzner, M.: The combinatorial structure of random polytopes. *Adv. Math.*, **191** (2005), 178–208. MR2102847 (2005k:52015)
- [50] Reitzner, M.: Random polytopes and the Efron-Stein jackknife inequality. *Ann. Probab.*, **31** (2003), 2136–2166. MR2016615 (2005b:60026)
- [51] Reitzner, M.: Central limit theorems for random polytopes. *Probab. Theory Relat. Fields*, **133** (2005), 483–507. MR2197111 (2007d:52005)
- [52] Rinott, Y.: On normal approximation rates for certain sums of dependent random variables. *J. Comput. Appl. Math.*, **55** (1994), 135–143. MR1327369 (96m:60057)
- [53] Rényi, A., Sulanke, R.: Über die konvexe Hülle von n zufällig gewählten Punkten. *Z. Wahrsch. Verw. Geb.*, **2** (1963), 75–84. MR0156262 (27:6190)
- [54] Santaló, L.A.: Integral geometry and geometric probability. Addison-Wiley, Reading MA (1976). MR0433364 (55:6340)
- [55] Schmidt, W.: Integral points on surfaces and curves. *Monatshefte Math.*, **99** (1985), 45–82. MR778171 (86d:11081)

- [56] Schneider, R., Wieacker, J.A.: Random polytopes in a convex body. *Z. Wahrsch. Verw. Gebiete*, **52** (1980), 69–73. MR568260 (81f:52008)
- [57] Schütt, C.: Random polytopes and affine surface area. *Math. Nachr.*, **170** (1994), 227–249. MR1302377 (95k:52007)
- [58] Sinai, Ya. G.: Probabilistic approach to analyse the statistics of convex polygonal curves. (in Russian) *Funk. Anal. Appl.* **28**, 41–48 (1994). English translation: *Funct. Anal. Appl.*, **28** (1994), 108–113. MR1283251 (95f:52015)
- [59] Sulanke, R.: Letter to the author, 2004
- [60] Sylvester, J.J.: Question 1491. *Educational Times*, London, April (1864).
- [61] Sylvester, J.J.: Report of the British Association, **35** (1865), 8–9.
- [62] Valtr, P.: The probability that n random points in a triangle are in convex position. *Combinatorica*, **16** (1996), 567–574. MR1433643 (97k:60030)
- [63] Vershik, A.M.: The limit shape for convex lattice polygons and related topics. (in Russian) *Funk. Anal. Appl.*, **28** (1994), 16–25. English translation: *Funct. Anal. Appl.*, **28** (1994), 13–20. MR1275724 (95i:52010)
- [64] Vershik A.M., Zeitouni, O.: Large deviation in the geometry of convex lattice polygons. *Israel J. Math.*, **109** (1999), 13–27. MR1679585 (2000i:52014)
- [65] Vu, V.H.: On the concentration of multivariate polynomials with small expectations. *Random Struct. Alg.*, **16** (2000), 344–363. MR1761580 (2001g:60060)
- [66] Vu, V.H.: Concentration of non-Lipschitz functions and applications. *Random Struct. Alg.*, **20** (2002), 262–316. MR1900610 (2003c:60053)
- [67] Vu, V.H.: Sharp concentration of random polytopes. *Geom. Funct. Anal.*, **15** (2005), 1284–1318. MR2221249 (2007f:52012)
- [68] Vu, V.H.: Central limit theorems for random polytopes in a smooth convex set. *Adv. Math.*, **207** (2006), 221–243. MR2264072 (2007k:60039)
- [69] W. Weil, J.A. Wieacker: *Stochastic geometry*. In: Gruber, P.M., Wills, J. (eds.) *Handbook of convex geometry*, North-Holland, Amsterdam, 1391–1438 (1993). MR1243013 (95a:60014)
- [70] Wieacker, J.A.: Einige Probleme der polyedrische approximation. Diplomarbeit, Albert-Ludwigs-Universität, Freiburg im Breisgau, (1978)

RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, P. O. BOX 127,
1364 BUDAPEST, HUNGARY; AND DEPARTMENT OF MATHEMATICS, UNIVERSITY COLLEGE LONDON,
GOWER STREET, LONDON WC1E 6BT, ENGLAND

E-mail address: `barany@renyi.hu`

E-mail address: `barany@math.ucl.ac.uk`