The Annals of Probability
1999, Vol. 27, No. 4, 2020–2034

SYLVESTER'S QUESTION: THE PROBABILITY THAT n POINTS ARE IN CONVEX POSITION[1]

BY IMRE BÁRÁNY

Hungarian Academy of Sciences and University College London

For a convex body K in the plane, let $p(n, K)$ denote the probability that n random, independent, and uniform points from K are in convex position, that is, none of them lies in the convex hull of the others. Here we determine the asymptotic behavior of $p(n, K)$ by showing that, as n goes to infinity, $n^2 \sqrt[n]{p(n, K)}$ tends to a finite and positive limit.

1. Introduction. Assume $K \subset R^2$ is a convex compact set with nonempty interior. In what follows we determine, asymptotically, the probability that n random, independent and uniform points from K are in convex position, that is, none of them is in the convex hull of the others. Write $p(n, K)$ for the probability in question.

Work on $p(n, K)$ started a long time ago. In the *Educational Times* in 1864 Sylvester [17] asked what the value of $p(4, K)$ was without specifying K. Several answers came in. Most of them were different. The question was changed. For what K is $p(4, K)$ minimal and maximal. A solution came from Blaschke [6]. For every convex body $K \subset R^2$,

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

Valtr [18] showed that

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

a surprisingly exact result. But since K can be sandwiched between two triangles and since $p(n, \text{triangle})$ is, asymptotically, $(13.5 e^2 n^{-2})^n$, we get that

$$c_1 \le n^2 \sqrt[n]{p(n, K)} \le c_2$$

with universal constants $0 < c_1 < c_2 < \infty$. Our main result is the following theorem.

THEOREM 1. *For every convex set $K \subset R^2$ with* Area $K = 1$,

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

exists and equals $\frac{1}{4} e^2 A^3(K)$ where $A(K)$ is the supremum of the affine perimeter of all convex sets $S \subset K$.

Received December 1997; revised June 1999.

[1] Supported in part by Hungarian Science Foundation Grant T 016391 and by Research Grant of the Academy 96-31/61.

AMS 1991 *subject classifications.* Primary 60D05; secondary 52A22.

Key words and phrases. Convex sets, affine perimeter, random sample, random points in convex position, limit shape.

Write $AP(K)$ for the affine perimeter of K. (The definition is in Section 4). As $p(n, K)$ is invariant under nondegenerate affine transformations, the limit in the theorem equals $\frac{1}{4}e^2A^3(K)/\text{Area } K$ in general.

Theorem 1 of [2] says that there is a unique convex compact $K_0 \subset K$ with $AP(K_0) = A(K)$. The proof of Theorem 1 above gives more than just the asymptotic behavior of $p(n, K)$. Namely, if the random points $x_1, \dots, x_n$ from K are in convex position, then their convex hull is, with high probability, very close to K_0. For the formulation of this "limit shape" result we use $\delta(A, B)$ to denote the Haussdorf distance of $A, B \subset R^2$. Write, further, $\mathscr{C}$ for the collection of convex compact sets $K \subset R^2$ with nonempty interior and X or X_n for the random sample $x_1, \dots, x_n$. In formulae we abbreviate the statement "X_n is in convex position" to "X_n convex."

THEOREM 2. *For every $K \in \mathscr{C}$ and every $\varepsilon > 0$,*

$$\lim_{n \to \infty} \mathbb{P}\big[\delta(\operatorname{conv} X_n, K_0) > \varepsilon | X_n \subset K, X_n \text{ convex}\big] = 0.$$

This theorem is a law of large numbers in the following sense. For $C \in \mathscr{C}$ and a unit vector u, let $C(u) \in C$ denote the point where the linear function ux reaches its maximum on C (assuming this point is unique). Writing $C_n = \operatorname{conv} X_n$, we have from the proof of Theorem 1 that for every unit vector u, the expectation of $C_n(u)$, conditional to X_n being in convex position, equals $K_0(u)$, and Theorem 2 says that $C_n(u)$ is concentrated around its expectation. (One can prove Theorem 2 along these lines; we choose, however, another approach to be used when proving Theorems 3 and 4.) In the case when K is the square we could even prove [4] a central limit theorem for the random variable $C_n(u)$, a result which is similar to that of Sinai [16] for the case of convex lattice polygons lying in a large square. Recent progress in this direction is due to Vershik and Zeitouni [21].

2. Further results. Let $X = X_n$ be again a random sample of n uniform, independent points from $K \in \mathscr{C}$. Define $Q(X)$ as the random collection of all convex polygons spanned by the points of X, that is, $P \in Q(X)$ if and only if $P = \operatorname{conv}\{x_{i_1}, \dots, x_{i_k}\}$ for some k-tuple $x_{i_1}, \dots, x_{i_k} \subset X$ that is in convex position ($k \geq 3$). Without a doubt, the most frequently studied (see [14], [15], [22]) polygon in $Q(X)$ is its largest element which is just $\operatorname{conv} X$. Write $|Q|$ for the number of elements in a set Q. Next we determine the expectation of $|Q(X_n)|$:

THEOREM 3. *For each $K \in \mathscr{C}$ with* Area $K = 1$,

$$\lim_{n \to \infty} n^{-1/3} \log E|Q(X_n)| = 3 \cdot 2^{-2/3}A(K). \tag{2.1}$$

Again, there is a limit shape to the elements of $Q(X)$. One way of formulating this is in the following theorem.

THEOREM 4. *For each $K \in \mathscr{C}$ and for each $\varepsilon > 0$,*

$$\lim_{n\to\infty} \frac{E|\{P \in Q(X_n) \colon \delta(P, K_0) > \varepsilon\}|}{E|Q(X_n)|} = 0. \tag{2.2}$$

This paper is closely related to the results of [2] which is about the limit shape of convex lattice polygons contained in K. The lattice is $\frac{1}{n}Z^2$ and the main result is that, as n goes to infinity, the overwhelming majority of the convex lattice polygons contained in K are very close to K_0. Formally, writing $\mathscr{P}_n(K)$ for the convex $\frac{1}{n}Z^2$-lattice polygons contained in $K \in \mathscr{C}$, for every $\varepsilon > 0$,

$$\lim_{n\to\infty} \frac{|\{P \in \mathscr{P}_n(K) \colon \delta(P, K_0) > \varepsilon\}|}{|\mathscr{P}_n(K)|} = 0. \tag{2.3}$$

This is completely parallel to Theorem 4 above. Results of this type were first proved by the author [1] and Vershik [20] for the case when K is the square; later Sinai [16] found stronger forms of the limit shape theorem. The analogue of Theorem 3 is the following result from [2]: Under the assumptions of Theorem 3,

$$\lim_{n\to\infty} n^{-2/3} \log|\mathscr{P}_n(K)| = 3\sqrt[3]{\frac{\zeta(3)}{4\zeta(2)}}\, A(K), \tag{2.4}$$

where $\zeta(s)$ is Riemann's zeta function.

In (2.1) and (2.4) n appears with different exponents. The reason is that in (2.1) the number of random points in K is n while in (2.4) the number of lattice points is n^2. It has been my conviction that random points and lattice points, in relation to convex bodies, behave essentially the same way. The analogy between (2.1) and (2.4) is another confirmation and so is the one between (2.2) and (2.3). In fact, this paper and [2] establish analogous statements for random points and for lattice points in K.

The next section is about higher dimensions. Then we define the affine perimeter and recall several of its properties, mainly from Blaschke's book [6] and from [2], [11]. We also need the special positioning of K and the existence of a small circle rolling freely within K_0. In Section 5 we give the proof of Theorem 1. Theorem 2 is proved in Section 6. The final sections contain proofs (or sketches of proofs) of Theorems 3 and 4.

3. Higher dimensions. The probability $p(n, K)$ can be defined for convex bodies $K \subset R^d$ with $d > 2$ as well. Most of the known results are about the case when $K = B^d$, the Euclidean unit ball. Hostinksy [9] determined $p(5, B^3)$, later Kingman [10] calculated $p(d+2, B^d)$. Miles [13] showed $\lim_{d\to\infty} p(d+3, B^d) = 1$. He conjectured and Buchta [7] showed $\lim_{d\to\infty} p(d+m, B^d) = 1$ for every fixed $m > 3$. Bárány and Füredi [3] proved that $p(n, B^d)$ is close to one as long as $n < d^{-1}2^{d/2}$ and close to zero for $n > d2^{d/2}$.

The results of this paper must have higher-dimensional analogues. However, the proofs given here do not go through. It is not only the unicity of the convex subset of $K \subset R^d$ with maximal affine surface area that is missing. For comments on this, see Remark 1 in [2]. (Actually, the unicity of K_0 is not needed for the proof of Theorem 1.) It is not clear what could replace the multiplicative formula (5.2). Nevertheless I think that for a convex $K \subset R^d$ of volume 1 (with obvious extensions of the definitions),

$$(3.1) \qquad n^{2/(d-1)} \sqrt[n]{p(n,K)} = \mathrm{const}(d) A(K)^{(d+1)/(d-1)}(1+o(1)).$$

There is a similar statement in the theory of best approximation of convex bodies by polytopes. Namely, let S be a convex body with smooth, say $\mathscr{C}^2$, boundary (and Vol $S = 1$) and P_n be a convex polytope with n vertices. When approximation of S by P_n is measured by the volume of their symmetric difference, there is a best approximating polytope P_n^* with n vertices. It is known [8] that

$$(3.2) \qquad n^{2/(d-1)} \mathrm{Vol}(S \,\Delta P_n^*) = \mathrm{const}(d) AP(S)^{(d+1)/(d-1)}(1+o(1)).$$

Moreover, there are indications [8] that the vertices of P_n^* are distributed "uniformly" in a small neighborhood U_n of ∂S. The width of U_n at $z \in \partial S$ is $n^{-2/(d-1)}\kappa^{1/(d+1)}(z)$ where κ is the product curvature. This speculation and (3.1) suggest that the random sample X_n is in convex position and conv X_n is very close to a fixed smooth convex $S \subset K$ with probability $(\mathrm{Vol}\, U_n)^n$. This quantity is the largest when $S = K_0$. Thus X_n is most likely to be close to K_0 when the sample is in convex position. Perhaps this can be used to attack (3.1), the high-dimensional variant of Theorem 3 or its lattice-polytope analogue. Of the latter, it is known that for $K \in \mathscr{C}$ with Vol $K = 1$,

$$0 < c_1 < n^{-d(d-1)/(d+1)} \log |\mathscr{P}_n(K)| < c_2,$$

where $\mathscr{P}_n(K)$ is the set of convex $(1/n)Z^d$-lattice polytopes contained in K [cf. (2.4)]. This follows from the results of [5].

Returning to the planar case, it is very likely that Blaschke's inequality (1.1) extends to

$$p(n, \text{triangle}) \le p(n, K) \le p(n, \text{disk}).$$

4. Affine perimeter. We are going to use the results of [2] on affine perimeter extensively. Given $S \in \mathscr{C}$, choose a subdivision $x_1, \dots, x_m, x_{m+1} = x_1$ of the boundary ∂S and lines L_i supporting S at x_i for all $i \in [m]$ where $[m] = \{1, \dots, m\}$. Write y_i for the intersection of L_i and L_{i+1} (if $L_i = L_{i+1}$, then y_i can be any point between x_i and x_{i+1}). Let T_i denote the triangle with vertices x_i, y_i, x_{i+1} and also its area. The affine perimeter of S is defined as

$$(4.1) \qquad AP(S) = 2 \lim \sum_1^m \sqrt[3]{T_i},$$

where the limit is taken over a sequence of subdivisions with $\max_{1,\dots,m}|x_i - x_{i+1}| \to 0$. The existence of the limit, and its independence of the sequence chosen, follow from the fact that $\sum_1^m \sqrt[3]{T_i}$ decreases as the subdivision is refined. Consequently,

$$AP(S) = 2\inf\sum_1^m \sqrt[3]{T_i}. \tag{4.2}$$

We record further properties of the map $AP\colon \mathscr{C} \to R$ (see [6], [11]):

$$AP(\lambda S) = \lambda^{2/3} AP(S) \quad \text{when } \lambda > 0, \tag{4.3}$$

$$AP(LS) = (\det L)^{1/3} AP(S) \quad \text{when } L\colon R^2 \to R^2 \text{ is linear}, \tag{4.4}$$

$$AP(S) = \int_{\partial S} \kappa^{1/3}\, ds = \int_0^{2\pi} r^{2/3}\, d\phi, \tag{4.5}$$

where κ is the curvature and $r = r(\phi) = \kappa^{-1}$ is the radius of curvature at the boundary point with outer normal $u(\phi) = (\cos\phi, \sin\phi)$. In (4.5), of course, ∂S has to be sufficiently smooth.

The affine length of a convex curve is defined analogously. We will need the following fact. Given a triangle $T = \operatorname{conv}\{a, b, c\}$, let M be the unique parabola which is tangent to ac at a and to bc at b.

(4.6) Among all convex curves connecting a and b within T the arc of the parabola M is the unique one with maximal affine length, and $AP(M) = 2\sqrt[3]{T}$.

We defined $A(K) = \sup\{AP(S)\colon S \in \mathscr{C}(K)\}$, where $\mathscr{C}(K) = \{S \in \mathscr{C}\colon S \subset K\}$ and cited Theorem 1 of [2] about the existence and unicity of $K_0 \in \mathscr{C}$, $K_0 \subset K$ with $AP(K_0) = A(K)$.

As $p(n, K)$ is invariant under (nondegenerate) affine transformations, we want to choose a "good position" for K. We assume first that Area $K = 1$. Let E be the maximum area ellipse contained in K. It is well known that Area $E \geq \pi/3\sqrt{3}$. Clearly $AP(K_0) = A(K) \geq AP(E)$. The affine isoperimetric inequality implies Area $K_0 \geq$ Area $E \geq \pi/3\sqrt{3}$ and so the maximum area ellipse E_0 in K_0 has area at least $\pi^2/27$.

We say that K is in *special position* if Area $K = 1$ and E_0 coincides with a circle of radius r_0 centered at the origin. Clearly, $r_0 \geq \sqrt{\pi/27} > 1/3$ which implies, in turn, that diam $K < 3$. So we have:

(4.7) Every $K \in \mathscr{C}$ can be brought to special position by a suitable affine transformation. In special position, $r_0 B \subset K_0$ and $K \subset 3B$ (where B is the unit circle centered at the origin).

We will write $\mathscr{C}_s$ for the collection of $K \in \mathscr{C}$ that are in special position. We will need several properties of K_0.

Evidently $\partial K_0 \cap \partial K \neq \emptyset$, as otherwise a slightly enlarged copy of K_0 would be contained in K and would have larger affine perimeter than $A(K)$.

Thus $\partial K_0 \setminus \partial K$ consists of (countably many) convex arcs $A_1, A_2, \ldots$, to be called free arcs. The second property we need is:

(4.8) Each free arc A is an arc of a parabola whose tangents at the endpoints are tangent to K_0 as well.

It is proved in [2] that ∂K_0 contains no line segment on its boundary. This implies that the point $z(\phi) \in \partial K_0$ where the outer normal to K_0 is $u(\phi) = (\cos\phi, \sin\phi)$ is uniquely determined for every $\phi \in [0, 2\pi)$. One can prove more: when $K \in \mathscr{C}_s$, the radius of curvature to K_0 exists and is bounded away from 0 and ∞ at every $z(\phi)$. Of this we only need (and prove):

(4.9) The circle of radius $\rho = 1/240$ rolls freely within K_0 (provided $K \in \mathscr{C}_s$),

that is, for every $z \in K_0$ there is a circle B_z of radius ρ such that $z \in B_z \subset K_0$. We prove (4.9) at the end of this section.

$U_m = \{u_1, \ldots, u_m\}$ is an *ordered* set of unit vectors with $u_i = (\cos\phi_i, \sin\phi_i)$ for $i \in [m]$ (where $[m]$ is a shorthand for $\{1, \ldots, m\}$) if $0 \le \phi_1 < \phi_2 < \cdots < \phi_m < 2\pi$. U_m is *dense* if every arc of the unit circle whose length is $5\pi/m$ contains at least one of the u_i. We say that the points $x_1, \ldots, x_m$ are in *convex position* with respect to $u_1, \ldots, u_m$, (or in u-convex position, for short) if, for every $i \in [m]$,

$$\max\{u_i x_j : j \in [m]\} = u_i x_i.$$

Note that $x_i = x_{i+1}$ is possible. Write T_i for the triangle bounded by the segment $[x_i, x_{i+1}]$ and lines $u_i(x - x_i) = 0$ and $u_{i+1}(x - x_{i+1}) = 0$. We denote the area of this triangle with the same letter T_i. Finally, if $X = \{x_1, \ldots, x_m\}$ is in u-convex position, we define

$$T(X) = T(X, U_m) = 2\sum_1^m \sqrt[3]{T_i}\,.$$

(4.10) For every $\varepsilon > 0$ and every $K \in \mathscr{C}_s$ there is m_0 such that for all $m > m_0$, for all dense ordered set U_m of unit vectors and for all $X = \{x_1, \ldots, x_m\} \subset K$ in u-convex position, $T(X, U_m) \le A(K) + \varepsilon$.

Proof. Note first that $T(X)$ is the affine perimeter of a convex body $M(X)$. Here $M(X)$ is bounded by parabola-arcs touching edges $[y_i, v_i]$ and $[v_i, y_{i+1}]$ of T_i at y_i and y_{i+1} (where v_i is the third vertex of T_i). Assume (4.10) is false. Then there is a sequence of U's and X's with larger and larger m's so that $T(X) \ge A(K_0) + \varepsilon$. Choose a convergent subsequence of the $M(X)$'s. Clearly, the limit M is a convex subset of K. Since the affine perimeter is upper semicontinuous (this was proved in more general form by Lutwak [12]), $AP(M) \ge AP(K_0) + \varepsilon$, a contradiction.

Proof of (4.9) Fix an x, y coordinate system and consider the parabola M_t whose equation is

$$y = g_t(x) = 118(x - t)^2$$

with $t \in [-1/6, 1/6]$. As $K \in \mathscr{C}_s$, $\partial K_0 \cap \{(x, y): x \in [-1/3, 1/3]\}$ is the graph of two functions; let $f(x)$ be the smaller. Then f is evidently convex and $f(x) < g_t(x)$ for all $x \in [-1/3, 1/3]$. Set $m_t = \min\{g_t(x) - f(x): x \in [-1/3, 1/3]\}$.

The set $C_t = \{x \in [-1/3, 1/3]: m_t = g_t(x) - f(x)\}$ is nonempty and closed. Further, there is a unique tangent to f at $x \in C_t$ and it is parallel to the tangent of g_t at x. We claim C_t is connected. Assume not, then there is an open interval (x_1, x_2) disjoint from C_t but with $x_1, x_2 \in C_t$. However, replacing the piece of ∂K_0 between $(x_1, f(x_1))$ and $(x_2, f(x_2))$ with the arc of the parabola $g_t(x) - m_t$ would produce, by (4.6), a larger affine perimeter contradicting the maximality of K_0.

Thus C_t is either a point or an interval. Increasing the coefficient 118 to 120 in the definition of M_t ensures that C_t is a single point for every $t \in [-1/6, 1/6]$. Assume the coefficient is 120 and keep the notation the same. Then $t \mapsto C_t$ is a point-to-point map. We claim it is continuous.

Assume t_j is a sequence with limit t_0. Then C_{t_j} has a convergent subsequence with limit x_0, say. It is easy to see that $x_0 \in C_{t_0}$ holds. However, C_{t_j} cannot have two distinct accumulation points showing that the map in question is, indeed, continuous.

A simple inspection, using the special position of K, shows that $C_{-1/6} < -1/120$ and $C_{1/6} > 1/120$. Thus the parabola $g_t(x) - m_t$ slides freely on ∂K_0 between $x = -1/120$ and $1/120$. The circle of radius $1/240$ rolls freely within the parabola M_t, so it also rolls freely on ∂K_0 on the interval $[-1/120, 1/120]$. Since we can fix the coordinate system arbitrarily to the origin we get that the same circle rolls freely within K_0. $\square$

5. Proof of Theorem 1. Fix K in special position and let $X_n = \{x_1, \dots, x_n\}$ be an n-sample of random, independent, uniform points from K. Let m be large (it will depend on $\varepsilon > 0$ to be given later) and U_m be an ordered, dense set of unit vectors. Define $i(j)$ by $u_j x_{i(j)} = \max\{u_j x_i: i \in [n]\}$. Clearly, $i(j)$ is well defined with probability 1 and the points $x_{i(1)}, \dots, x_{i(m)}$ are in convex position with respect to $u_1, \dots, u_m$. Repetitions may, however, occur but only in contiguous intervals. So let $y_1, \dots, y_k$ be the collection of the distinct $x_{i(j)}$'s in their original order. To fix the notation, assume y_h is maximal for $u_{i_{h-1}+1}, u_{i_{h-1}+2}, \dots, u_{i_h}$ while $h \in [k]$. Write $Y = \{y_1, \dots, y_k\}$. We also say, with a slight but convenient abuse of language, that Y is in u-convex position and that Y is the u-max of X, in notation: $Y = u\text{-max } X$. Now $p(n, K)$ can be computed as

$$
\begin{aligned}
p(n,K) &= \mathbb{P}[X \text{ convex}] = \int_{X \text{ convex}} \cdots \int dx_1 \dots dx_n \\
&= \sum_{k=3}^{m} \sum \binom{n}{k} \int_{Y\, u\text{-convex}} \cdots \int \mathbb{P}[X \text{ convex}, Y = u\text{-max } X]\, dy_1 \cdots dy_k,
\end{aligned}
\tag{5.1}
$$

where the second sum is taken over all possible choices of $1 \le i_1 < \cdots < i_k \le m$ and the probability under the integral is understood with Y fixed and $X \setminus Y$ varying so that X is in convex position and Y is the u-max of X.

The points of $X \setminus Y$ have to lie in the triangles T_h with $h \in [k]$ where T_h is bounded by the segment $[y_h, y_{h+1}]$ and by the lines $u_{i_h}(x - y_h) = 0$ and $u_{i_{h+1}}(x - y_{h+1}) = 0$. Writing p_h for the number of points of $X \setminus Y$ lying in T_h, we have

$$\begin{aligned}
&\mathbb{P}[X \text{ convex}, Y = u\text{-max } X] \\
&\quad = \sum\nolimits^* \mathbb{P}[X \text{ convex}, Y = u\text{-max } X \,|\, |X \cap T_h| = p_h(\forall h)] \\
&\qquad \times \mathbb{P}[|X \cap T_h| = p_h(\forall h)] \qquad\qquad (5.2)\\
&\quad = \sum\nolimits^* \binom{n-k}{p_1, \dots, p_k} \prod_1^k (T_h \cap K)^{p_h} \\
&\qquad \times \mathbb{P}[p_h \text{ points for a convex chain in } T_h \cap K],
\end{aligned}$$

where Σ^* is taken over all $p_1, \dots, p_k$ that sum to $n - k$. The conditional probability can be replaced by the product since the events happening in distinct triangles are independent. We have to explain what stands after the last $\mathbb{P}$ in (5.2): we say that points $z_1, \dots, z_p$ form a convex chain in $T \cap K$ where T is a triangle with distinguished vertices $z_0, z_{p+1} \in K$ if all the z_i are in $T \cap K$ and $\operatorname{conv}\{z_0, z_1, \dots, z_p, z_{p+1}\}$ has $p + 2$ vertices. In our case the distinguished vertices are, of course, y_h and y_{h+1}. Now $\mathbb{P}[p$ points form a convex chain in $T \cap K]$ is meant with p random, independent points drawn uniformly from $T \cap K$. This probability is known when $T \subset K$; it is proved in [4] (see also [19] for a related statement) that

$$\mathbb{P}[p \text{ points form a convex chain in } T] = \frac{2^p}{p!(p+1)!}. \qquad (5.3)$$

Here is a quick sketch of the proof. First assume that $z_1, \dots, z_p$ are drawn from the unit square and seek the probability that they, together with $(0,0)$ and $(1,1)$ form a convex chain in the triangle $\operatorname{conv}\{(0,0),(1,0),(1,1)\}$. The vertical and horizontal lines through the z_j have p^2 intersection points, arranged in a matrix. Every one of the $p!$ diagonals (i.e., one point from every vertical and every horizontal line) of this matrix is equally likely but only one of them is an increasing chain from $(0,0)$ to $(1,1)$. So $z_1, \dots, z_p$ is an increasing chain with probability $1/p!$. Now an increasing chain is just an ordered set of $(p+1)$ positive vectors. It turns out all of their permutations are equally likely. Clearly all of them are increasing but only one is convex. This gives $(p!(p+1)!)^{-1}$ for the probability in the square. The case of the triangle now follows readily.

We are going to estimate $p(n, K)$ first from above and then from below. We use (5.1) and (5.2). Assume a small positive ε is given, and choose m_0 according to (4.1) and let $m > m_0$.

For the upper estimate we assume first that K is a convex polygon (in special position). Let U_m be an ordered, dense set of unit vectors with the extra condition that the outer unit normals to the edges of K are all contained in U_m. This implies $T_h \cap K = T_h$ and so we can apply (5.3). (This is the only point where K has to be a polygon.) We continue (5.2) using (5.3),

$$(5.4)\quad \mathbb{P}[X \text{ convex}, Y = u\text{-max } X] \le (n-k)! \sum{}^{*} \prod_{1}^{k} \frac{(2T_h)^{p_h}}{p_h!^2 (p_h+1)!}$$

with the previous remark about Σ^*. Here $(2T_h)^{p_h}(p_h!^2(p_h+1)!)^{-1} \le (2e^3 T_h p_h^{-3})^{p_h}$ and it is easy to show that the product, over $h = 1, \dots, k$, of the last expression is maximal, subject to the condition $\Sigma p_h = n - k$, when

$$p_h = \frac{\sqrt[3]{T_h}}{\sum_{j=1}^{k} \sqrt[3]{T_j}} (n-k).$$

(To see this, consider p_h a positive real variable and determine the conditional maximum of the logarithm of the product, the condition being $\Sigma p_h = n - k$.) We have then

$$\prod_{1}^{k} \frac{(2T_h)^{p_h}}{p_h!^2(p_h+1)!} \le \prod_{1}^{k} (2e^3 T_h p_h^{-3})^{p_h}$$
$$\le \left(\frac{2e^3 \left(\sum_1^k \sqrt[3]{T_h} \right)^3}{(n-k)^3} \right)^{n-k} \le \left(\frac{e^3 T(Y)^3}{4(n-k)^3} \right)^{n-k},$$

where $T(Y)$ is to be understood as $2\Sigma \sqrt[3]{T_h}$, or as $T(x_{i(1)}, \dots, x_{i(m)})$ possibly with repeated elements. We continue (5.4) by observing that the number of terms in the sum is $\binom{n-1}{k-1}$,

$$\mathbb{P}[X \text{ convex}, Y = u\text{-max } X]$$
$$(5.5)\quad \le (n-k)! \binom{n-1}{k-1} \left(\frac{e^3 T(Y)^3}{4(n-k)^3} \right)^{n-k}$$
$$\le n \binom{n-1}{k-1} \left(\frac{e^2 T(Y)^3}{4(n-k)^2} \right)^{n-k}.$$

According to (4.10) and the choice of m, $T(Y) \le A(K) + \varepsilon$. Returning now to (5.1) we see that each integral is bounded by the right-hand side of the last formula with $T(Y)$ replaced by $A(K) + \varepsilon$. The number of terms of the second sum in (5.1) is equal to the number of ways to partition $[m]$ into k contiguous intervals, that is, $\binom{m}{k}$. So we infer

$$\mathbb{P}[X \text{ convex}] \le \sum_{k=3}^{m} \binom{m}{k}\binom{n}{k} n \binom{n-1}{k-1} \left(\frac{e^2 (A(K)+\varepsilon)^3}{4(n-k)^2} \right)^{n-k}$$
$$\le 2^m n^{2m} \left(\frac{e^2 (A(K)+\varepsilon)^3}{4(n-m)^2} \right)^{n-m}.$$

Here m is fixed and depends only on ε, so for large enough n we have

$$n^2 \sqrt[n]{p(n,K)} \le \frac{e^2}{4} (A(K) + 2\varepsilon)^3.$$

Now let $K \in \mathscr{C}$ be arbitrary with area $K = 1$. Choose a convex polygon P containing K so that $A(P) \le A(K) + \varepsilon$. Writing Z_n for a random n-tuple of points from P we have

$$\begin{aligned} p(n,K) &= \mathbb{P}[X_n \text{ convex in } K] = \mathbb{P}[Z_n \text{ convex in } P | Z_n \subset K] \\ &= \frac{\mathbb{P}[Z_n \text{ convex in } P \text{ and } Z_n \subset K]}{\mathbb{P}[Z_n \subset K]} \\ &\le \left(\frac{\text{Area } P}{\text{Area } K} \right)^n \mathbb{P}[Z_n \text{ convex in } P] \\ &= (\text{Area } P)^n p(n,P) \le (\text{Area } P)^n \left(\frac{e^2 (A(P) + 2\varepsilon)^3}{4n^2 \text{ Area } P} \right)^n \\ &\le \left(\frac{e^2 (A(K) + 3\varepsilon)^3}{4n^2} \right)^n. \end{aligned} \tag{5.6}$$

To estimate from below we do not need the auxiliary polygon. Shrink first K and K_0 (from the origin) by a factor $\lambda < 1$ so that

$$AP(\lambda K_0) = \lambda^{2/3} AP(K_0) > AP(K_0) - \varepsilon.$$

We will fix a large m soon. Define z_h as the point where $u_h x$ reaches its maximum in λK_0 where we simply define $u_h = [\cos(2\pi h/m), \sin(2\pi h/m)]$ for all $h \in [k]$. Let $T_h(z)$ be the triangle bounded by the segment $[z_h, z_{h+1}]$ and lines $u_h(x - z_h) = 0$ and $u_{h+1}(x - z_{h+1}) = 0$. Choose m so large that, for all $h \in [m]$, the third vertex, v_h, of $T_h(z)$ (the intersection of the two lines) is in K and, further, the length of the edges $[z_h, v_h]$ and $[v_h, z_{h+1}]$ is at least $(\lambda/240)\tan(\pi/m) > 1/80m$, since λ can be chosen as close to 1 as you wish. [The existence of such an m follows from (4.9).] Finally, let B_h be the circle of radius $1/100m^3$ with $z_h \in B_h \subset \lambda K_0$.

Since we are to estimate $p(n, K)$ from below we concentrate on the large terms in (5.1) and (5.2). We only consider the terms with $k = m$ and will only integrate over $y_h \in B_h$. Then, since B_h is very small, $y_1, \dots, y_m$ are in

u-convex position. Moreover, all vertices of the triangles $T_h = T_h(y)$ belong to K. Thus $T_h(y) \cap K = T_h(y)$ and (5.3) can be used, again. Further, since y_h is in B_h and the length of an edge of $T_h(z)$ is at least $1/80m$, a little elementary geometry reveals that

$$T_h(y) \geq T_h(z)\left(1 - \frac{1}{7m}\right).$$

Using this in (5.2) we see that, assuming $y_h \in B_h$,

$$\begin{aligned} &\mathbb{P}[X \text{ convex}, Y = u\text{-max } X] \\ &\quad \geq \sum{}^* \binom{n-m}{p_1, \dots, p_m} \prod_1^m T_h(y)^{p_h} \\ (5.7) \qquad &\quad\quad \times \mathbb{P}[p_h \text{ points form a convex chain in } T_h(y)] \\ &\quad \geq (n-m)! \sum{}^* \left(1 - \frac{1}{7m}\right)^{n-m} \prod_1^m \frac{(2T_h(z))^{p_h}}{p_h!^2(p_h+1)!}. \end{aligned}$$

The factors in the product are at least $(2T_h(z))^{p_h}(p_h+1)!^{-3} \geq (2e^3 T_h(z)(p_h+1)^{-3})^{(p_h+1)}$. The last expression is maximal, under the condition $\Sigma(p_h+1) = n$, when

$$p_h + 1 = \frac{\sqrt[3]{T_h(z)}}{\sum_{j=1}^m \sqrt[3]{T_j(z)}} n.$$

Using this and some simple estimates, it is easy to see that the maximal value of the last product in (5.7) is at least

$$\left(\frac{e^3\left(2\Sigma\sqrt[3]{T_h(z)}\right)^3}{4n^3}\right)^n \geq \left(\frac{e^3(A(K) - 2\varepsilon)^3}{4n^3}\right)^n.$$

Recall that only the case $k = m$ is considered in (5.1), and only one term from the sum in (5.2). Using the last inequality in (5.7) and (5.1) yields

$$\begin{aligned} p(n,K) &\geq \binom{n}{m}(n-m)!\left(\frac{e^3(A(K)-2\varepsilon)^3}{4n^3}\right)^n \left(1 - \frac{1}{7m}\right)^{n-m} \\ &\quad \times \left[\pi(100m^3)^{-2}\right]^m \\ &\geq \frac{1}{m!}\left(\frac{e^2(A(K)-2\varepsilon)^3}{4n^2}\right)^n \left(1 - \frac{1}{7m}\right)^{n-m} \left[\pi(100m^3)^{-2}\right]^m, \end{aligned}$$

where the square bracket comes from integrating over B_h m times. Then, for large enough n,

$$n^2 \sqrt[n]{p(n,K)} \geq \frac{e^2}{4}(A(K) - 3\varepsilon)^3,$$

proving the theorem. □

6. Proof of Theorem 2. We need further results from [2]. Assume first that K is in special position, and a small $\varepsilon > 0$ is given. Recall the notation $\mathscr{C}(K) = \{S \in \mathscr{C}: S \subset K\}$. Lemma 5 from [2] states the following:

(6.1) There are halfplanes $H_1, \dots, H_p$, each with $(1 - \varepsilon/24)K_0 \not\subset H_i$, and points $z_1, \dots, z_q \in K \cap \partial(1 + \varepsilon/24)K_0$, where p and q are at most const$/\varepsilon$, such that the following holds. For every $C \in \mathscr{C}(K)$ with $\delta(C, K_0) > \varepsilon$, either there is an $i \in [p]$ with $C \subset H_i$ or there is an $j \in [q]$ with $z_j \in C$.

Actually, Lemma 5 in [2] is stated without $\varepsilon/24$ (in "there exists $\eta > 0$" form) but the same proof with simple and generous computations shows the validity of (6.1). The second thing we need is a pointed version of the existence and unicity of K_0 (Theorem 4 in [2]):

(6.2) For every $K \in \mathscr{C}$ and every $z \in K$ there is a unique $K_0(z) \in \mathscr{C}(K)$ containing z such that $AP(K_0(z)) > AP(S)$ for every convex $S \in \mathscr{C}(K)$ with $z \in S$, different from $K_0(z)$.

Assume now n is large, X_n is a random n-sample from K, write $C_n =$ conv X_n. Let E_i and F_j, respectively, denote the event that $X_n \subset H_i$, and $z_j \in C_n$, and G the event that X_n is in convex position. We want to bound

$$\mathbb{P}[\delta(C_n, K_0) > \varepsilon | G] = \frac{\mathbb{P}[\delta(C_n, K_0) > \varepsilon \text{ and } G]}{\mathbb{P}[G]}.$$

By (6.1), the numerator is smaller than

$$\sum_1^p \mathbb{P}[E_i \cap G] + \sum_1^q \mathbb{P}[F_j \cap G].$$

The unicity of K_0 and (6.2) imply the existence of $\eta > 0$ such that $A(K \cap H_i) + 3\eta < A(K)$ and $AP(K_0(z_j)) + 4\eta < A(K)$. Now for large enough n, Theorem 1 ensures

$$\mathbb{P}[G] \geq \left(\frac{e^2 (A(K) - \eta)^3}{4n^2} \right)^n. \tag{6.3}$$

Next we estimate $\mathbb{P}[E_i \cap G]$. Using Theorem 1 we have

$$\begin{aligned} \mathbb{P}[E_i \cap G] &= \mathbb{P}[X_n \subset H_i \text{ and } X_n \text{ convex}] \\ &= \mathbb{P}[X_n \text{ convex} | X_n \subset H_i] \mathbb{P}[X_n \subset H_i] \\ &= p(n, K \cap H_i) \left(\frac{\text{Area}(K \cap H_i)}{\text{Area } K} \right)^n \\ &\leq \left(\frac{e^2 (A(K \cap H_i) + \eta)^3}{4n^2 \text{ Area}(K \cap H_i)} \right)^n \left(\frac{\text{Area}(K \cap H_i)}{\text{Area } K} \right)^n \\ &= \left(\frac{e^2}{4n^2} (A(K \cap H_i) + \eta)^3 \right)^n < \left(\frac{e^2}{4n^2} (A(K) - 2\eta)^3 \right)^n. \end{aligned} \tag{6.4}$$

Estimating $\mathbb{P}[F_j \cap G]$ is similar but one has to be more careful. We have to repeat the proof of Theorem 1, upper bound, with the extra condition $z_j \in C_n$. (For the sake of simplicity we ignore the use of the auxiliary polygon.) At the very start of the proof we defined $x_{i(1)}, \dots, x_{i(m)}$ which was abbreviated as Y after getting rid of repetitions. This gives rise to the convex polygon (which clearly depends only on Y),

$$P(Y) = \{x \colon u_h(x - x_{i(h)}) \le 0 \text{ for } h \in [m]\}.$$

Now the proof goes unchanged up to (5.5), this time with the condition $z_j \in C_n$ which implies $z_j \in P(Y)$ because $C_n \subset P(Y)$. We claim that $T(Y) - \eta < AP(K_0(z_j))$ provided m is large enough.

The proof is almost identical to that of (4.10). Assume the claim is false. Then there is a sequence of Y's with larger and larger m's so that $T(Y) - \eta \ge AP(K_0(z_j))$. Define the convex body $M(Y)$ as in (4.10). Then $M(Y) \subset P(Y)$ and $AP(M(Y)) = T(Y)$. Choose a convergent subsequence of the $M(Y)$'s with limit $M \in \mathscr{C}(K)$. Evidently $z_j \in M$. Since the affine perimeter is upper semicontinuous (see [12]), $AP(M) - \eta \ge AP(K_0(z_j))$, a contradiction.

Now, with the claim just proved, the inequality $T(Y) < AP(K_0(z_j)) + \eta < A(K) - 3\eta$ can be used in (5.5). So we have, repeating the same steps,

$$\mathbb{P}[F_j \cap G] \le \left(\frac{e^2 (A(K) - 2\eta)^3}{4n^2} \right)^n.$$

Now (6.2), (6.3) and (6.4) show

$$\mathbb{P}[\delta(C_n, K_0) > \varepsilon | G] \ge (p + q) \left(\frac{A(K) - 2\eta}{A(K) - \eta} \right)^{3n},$$

which is very small when n is large. □

7. Proof of Theorem 3.

We are to estimate

$$\begin{aligned} E|Q(X_n)| &= \sum_{k=3}^{n} \sum_{x_{i_1}, \dots, x_{i_k}} \mathbb{P}[x_{i_1}, \dots, x_{i_k} \text{ convex}] \\ &= \sum_{k=3}^{n} \binom{n}{k} \mathbb{P}[y_1, \dots, y_k \text{ convex}] \end{aligned} \tag{7.1}$$

where $y_1, \dots, y_k$ are random, independent, uniform points from K. Given $\varepsilon > 0$, choose n_0, by Theorem 1, so large that for $m \ge n_0$,

$$\left(\frac{e^2 A(K)^3 (1 - \varepsilon)}{4m^2} \right)^m \le p(m, K) \le \left(\frac{e^2 A(K)^3 (1 + \varepsilon)}{4m^2} \right)^m. \tag{7.2}$$

Let $k = \sqrt[3]{2^{-2}A(K)^3(1-\varepsilon)n}$ and assume k is an integer and n is so large that $k > n_0$. Then the kth term in the last line of (7.1) is at least

$$\exp\{3 \cdot 2^{-2/3}A(K)n^{1/3}(1-\varepsilon)\},$$

as one can easily check.

To bound $E|Q(X_n)|$ from above, choose n so large that

$$k_0 = \sqrt[3]{2^{-2}A(K)^3(1+\varepsilon)n}$$

is much larger than n_0. We can estimate the sum in the last line of (7.1) as

$$\begin{aligned} E|Q(X_n)| &\le \sum_{k=3}^{n_0}\binom{n}{k} + \sum_{n_0+1}^{n}\binom{n}{k}p(k,K) \\ &\le n_0\binom{n}{n_0} + \sum_{n_0}^{n}\binom{n}{k}\left(\frac{e^2A(K)^3(1+\varepsilon)}{4k^2}\right)^k \\ &\le n_0\binom{n}{n_0} + \sum_{n_0}^{n}\left(\frac{en}{k}\right)^k\left(\frac{e^2A(K)^3(1+\varepsilon)}{4k^2}\right)^k, \end{aligned}$$

where we used (7.2) as well. The maximal term in the second sum occurs at $k = k_0$ and turns out to be smaller than $\exp\{3 \cdot 2^{-2/3}A(K)n^{1/3}(1+\varepsilon)^{1/3}\}$, yielding

$$\begin{aligned} E|Q(X_n)| &\le n^{n_0} + n\exp\{3 \cdot 2^{-2/3}A(K)n^{1/3}(1+\varepsilon)^{1/3}\} \\ &\le \exp\{3 \cdot 2^{-2/3}A(K)n^{1/3}(1+\varepsilon)\}. \end{aligned}$$ □

8. Proof of Theorem 4. We have to estimate the expectation of the number of $P \in Q(X_n)$ that satisfy $\delta(P, K_0) > \varepsilon$. We use (6.1) and estimate the expectations of $P \in Q(X_n)$ satisfying $P \subset H_i$, and $z_j \in P$, respectively.

The previous section contains bounds for $\mathbb{P}[X_k \subset H_i,\ X_k \text{ convex}]$ and also for $\mathbb{P}[z_j \in X_k,\ X_k \text{ convex}]$. Using them the way we computed $E|Q(X_n)|$, there is no difficulty completing the proof. □

Acknowledgments. My thanks are due to Rick Vitale who suggested that the random analogue of (2.1), that is, Theorem 4, may be true. Actually, it was his question and my conviction (that random points and lattice points behave similarly in generic convex bodies) that led to the results of this paper. I also thank Pavel Valtr for comments and suggestions and for careful checking of the manuscript.

REFERENCES

[1] BÁRÁNY, I. (1995). The limit shape of convex lattice polygons. *Discrete Comput. Geom.* **13** 270–295.

[2] BÁRÁNY, I. (1997). Affine perimeter and limit shape. *J. Reine Angew. Math.* **484** 71–84.

[3] BÁRÁNY, I. and FÜREDI, Z. (1988). On the shape of the convex hull of random points. *Probab. Theory Related Fields* **77** 231–240.

[4] BÁRÁNY, I., ROTE, G., STEIGER, W. and ZHANG, C. (1999). A central limit theorem for random convex chains. *Discrete Comput. Geom.* To appear.

[5] BÁRÁNY, I. and VERSHIK, A. M. (1992). On the number of convex lattice polytopes. *GAFA J.* **2** 381–293.

[6] BLASCHKE, W. (1923). *Vorlesungen über Differenzialgeometrie II. Affine Differenzialgeometrie*. Springer, Berlin.

[7] BUCHTA, C. (1986). On a conjecture of R. E. Miles about the convex hull of random points. *Monatsh. Math.* **102** 91–102.

[8] GRUBER, P. M. (1993). Aspects of approximation of convex bodies. In *Handbook of Convex Geometry* 1391–1438. North-Holland, Amsterdam.

[9] HOSTINSKY, B. (1925). Sur les probabilités géométriques. *Publ. Fac. Sci. Univ. Brno.*

[10] KINGMAN, J. F. C. (1969). Random secants of a convex body. *J. Appl. Probab.* **6** 660–672.

[11] LEICHTWEISS, K. (1986). Zur Affinoberfläche konvexer Körper. *Manuscripta Math.* **56** 429–464.

[12] LUTWAK, E. (1991). Extended affine surface area. *Adv. Math.* **85** 39–68.

[13] MILES, R. E. (1971). Isotropic random simplices. *Adv. in Appl. Probab.* **3** 353–382.

[14] RÉNYI, A. and SULANKE, R. (1963). Über die konvexe Hülle von n zufällig gewählten Punkten. *Z. Wahrsch. Verw. Gebiete* **2** 75–84.

[15] SCHNEIDER, R. (1988). Random approximation of convex sets. *J. Microscopy* **151** 211–227.

[16] SINAI, YA. G. (1994). Probabilistic approach to analyse the statistics of convex polygonal curves. *Funct. Anal. Appl.* **28** 41–48 (in Russian).

[17] SYLVESTER, J. J. (1864). Problem 1491. *The Educational Times* (April, 1864), London.

[18] VALTR, P. (1996). The probability that n random points in a triangle are in convex position. *Combinatorica* **16** 567–574.

[19] VALTR, P. (1997). Catalan numbers via random planar point sets. *Bolyai Soc. Math. Stud.* **6**, 441–443.

[20] VERSHIK, A. M. (1994). The limit shape for convex lattice polygons and related topics. *Funct. Anal. Appl.* **28** 16–25 (in Russian).

[21] VERSHIK, A. M. and ZEITOUNI, O. (1999). Large deviations in the geometry of convex lattice polygons. *Israel J. Math.* **109** 13–28.

[22] WEIL, W. and WIEACKER, J. A. (1993). Stochastic geometry. In *Handbook of Convex Geometry* 1391–1438. North-Holland, Amsterdam.

MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
POB 127
BUDAPEST 1364
HUNGARY
E-MAIL: BARANY@MATH-INST.HU.

DEPARTMENT OF MATHEMATICS
UNIVERSITY COLLEGE LONDON
GOWER STREET
LONDON WC1E 6BT
UNITED KINGDOM