Discrete Comput Geom 1:315–319 (1986)

Discrete & Computational Geometry

Random Polytopes in the d-Dimensional Cube

Z. Füredi*

Mathematical Institute of the Hungarian Academy of Sciences, 1364 Budapest, P.O. Box 127, Hungary

Abstract. Let C^d be the set of vertices of a d-dimensional cube, $C^d = \{(x_1, \ldots, x_d)\colon x_i = \pm 1\}$. Let us choose a random n-element subset $A(n)$ of C^d. Here we prove that Prob(the origin belongs to the conv $A(2d + x\sqrt{2d})) = \Phi(x) + o(1)$ if x is fixed and $d \to \infty$. That is, for an arbitrary $\varepsilon > 0$ the convex hull of more than $(2+\varepsilon)d$ vertices almost always contains 0 while the convex hull of less than $(2-\varepsilon)d$ points almost always avoids it.

1. Convex Hull of Subsets of Vertices

Let C^d denote the set of vertices of a d-dimensional cube, $C^d \subset \mathbb{R}^d$, $C^d = \{(x_1, \ldots, x_d)\colon x_i = \pm 1\}$. Let $A(n)$ be a random n-element subset of C^d. We have $\binom{2^d}{n}$ possibilities for $A(n)$, hence Prob($A(n)$ has property π) = (# of n-tuples of C^d with property π)$\Big/\binom{2^d}{n}$. The threshold function of the property π is n_d if for every $\varepsilon > 0$ we have

$$\text{Prob}(A((1+\varepsilon)n_d) \text{ has property } \pi) \to 1 \qquad \text{whenever} \quad d \to \infty$$

and

$$\text{Prob}(A((1-\varepsilon)n_d) \text{ has property } \pi) \to 0 \qquad \text{whenever} \quad d \to \infty.$$

J. Mycielski posed the following problem: How large should we choose n so that conv $A(n)$, the convex hull of $A(n)$, contains almost surely the origin 0 [2]? P. Erdös conjectured that the threshold function of this property is $O(d)$ [2]. This was proved by Komlós [5] in 1980.

---

* Present address: Department of Mathematics, M.I.T., Room 2-380, Cambridge, MA 02139, USA.

Theorem 1.1 [5]. *$1.3d < n_d < 4.4d$, i.e.,*

$$\lim_{d\to\infty} \mathrm{Prob}(0 \in \mathrm{conv}\, A(1.3d)) = 0$$

and

$$\lim_{d\to\infty} \mathrm{Prob}(0 \in \mathrm{conv}\, A(4.4d)) = 1.$$

Here we improve this result. Denote $1/\sqrt{2\pi}\int_{-\infty}^{c} e^{-x^2/2}\,dx$ by $\Phi(c)$, as usual.

Theorem 1.2. *Let c be a real number. Then*

$$\lim_{d\to\infty} \mathrm{Prob}(0 \in \mathrm{conv}\, A(2d + c\sqrt{2d})) = \Phi(c).$$

Corollary 1.3. *$n_d = 2d$.*

Our results are strongly related to an old theorem of Wendel [7] (see Theorem 4.1). More results and an extensive literature about random polytopes can be found in a recent paper of Buchta and Müller [1]. See also Mycielski [6].

2. Lemmas

P. Erdös conjectured that a random ± 1 matrix is almost always regular. This was proved by Komlós [4] in 1967:

Lemma 2.1 [4]. *Let M be a $d \times d$ random ± 1 matrix (i.e., every entry a_{ij} is chosen independently and with probabilities* $\mathrm{Prob}(a_{ij} = 1) = \mathrm{Prob}(a_{ij} = -1) = \frac{1}{2}$). *Then*

$$\mathrm{Prob}(M \textit{ is regular}) > 1 - O(1/\sqrt{d}). \tag{1}$$

Komlós conjectures that one can replace $O(1/\sqrt{d})$ by $O(1/(1+\varepsilon)^d)$ for some positive ε. The following lemma is a simple generalization of a result due to Harding [3]. Let $P = \{p_1, p_2, \ldots, p_n\} \subset \mathbb{R}^d$ be a point-set ($p_i = p_j$ is possible). The partition $P = U \cup V$ is *induced by a hyperplane* if there exists a hyperplane $H \subset \mathbb{R}^d$ such that $P \cap H = \emptyset$ and H splits every segment $[u, v]$ for $u \in U$, $v \in V$. Denote by $h(P)$ the number of such partitions of P, $h(d, n) = \max\{h(P) : P \subset \mathbb{R}^d, |P| = n\}$. Harding proved that

$$h(d, n) = \binom{n-1}{d} + \cdots + \binom{n-1}{0}.$$

Denote by $a(k, P)$ the number of affine dependent k-tuples of P. The lower bound in the following lemma is an easy consequence of a theorem of Winder [8] (see also Zaslavsky [9]).

Lemma 2.2. *For every $P\subset\mathbb{R}^d$, $|P|=n$ we have*

$$h(d,n)-\sum_{2\le k\le d+1} a(k,P)\leq h(P)\leq h(d,n)=\sum_{k\le d}\binom{n-1}{k}. \tag{2}$$

This lower bound is not the best possible, but it is sufficient for our purposes.

3. Proof of Theorem 1.2

The first observation is that we can neglect those $A(n)$'s which contain a pair of opposite vertices because the probability of this event tends to 0 when $d\to\infty$. In fact, we have

$$\operatorname{Prob}(A(n)\cap(-A(n))\neq\varnothing)\le\frac{2^d\binom{2^d}{n-2}}{\binom{2^d}{n}}<\frac{n^2}{2^d}=o(1)\qquad\text{if}\quad n=O(d)\text{ and }d\to\infty. \tag{3}$$

The main idea in our argument is that we obtain a random n-set A in two steps. First we choose n pairs from the 2^{d-1} pairs of the form $\{x,-x\}$, $x\in C^d$. Then we choose an element from each pair. Let H be a hyperplane of $\mathbb{R}^d$ in general position with respect to C^d, $0\notin H$. For $x\in C^d$ we denote the point $H\cap(0,x)$ by $\pi(x)$.

Lemma 3.1. *Let $x_1,\dots,x_n\in C^d$, $\Pi=\{\pi(x_i)\colon 1\leq i\leq n\}$ and*

$$Y=\{\{y_1,\dots,y_n\}\colon y_i=x_i\text{ or }-x_i\}.$$

Then # (members of Y whose convex hull avoids 0) $=2h(\Pi)$.

Proof. If the convex hull of $\{y_1,\dots,y_n\}$ avoids 0 then there exists a hyperplane H_0 through 0 such that it separates $\{y_1,\dots,y_n\}$ from $\{-y_1,\dots,-y_n\}$. Hence $H_0\cap H$ induces a partition of Π. Moreover, the converse is also true, every induced partition yields two members of Y. □

Using Lemma 2.2 for $n=2d+c\sqrt{2d}$ we get

$$\operatorname{Prob}(0\notin\operatorname{conv}A(n))=\frac{1}{2^n\binom{2^{d-1}}{n}}\sum 2h(\Pi)\leq\frac{h(d,n)}{2^{n-1}}$$

$$=\frac{1}{2^{n-1}}\sum_{i<n/2-(c\sqrt{n})/2}\binom{n-1}{i}=\Phi(-c)+O\left(\frac{1}{n}\right).$$

(Actually we have calculated $\operatorname{Prob}(0\notin\operatorname{conv}A(n)|A\cap(-A)=\varnothing)$ and used (3).)

Moreover, (3) implies

$$\operatorname{Prob}(0\notin\operatorname{conv}A(n))\geq\frac{h(d,n)}{2^{n-1}}-\frac{1}{2^{n-1}\binom{2^{d-1}}{n}}\sum_{\Pi}\sum_{1\leq k\leq d}a(k,\Pi). \tag{4}$$

Here Komlós' theorem (i.e., Lemma 2.1) implies

$$\frac{1}{\binom{2^{d-1}}{n}} \sum a(k, \Pi) \leqslant O\left(\frac{1}{\sqrt{d}}\right)\binom{n}{d}.$$

Similarly

$$\frac{1}{2^{d-1}} \sum_{\Pi} a(k, \Pi)$$

$$= \binom{n}{k} \text{Prob}(k \text{ random } \pm 1 \text{ sequences of length } d \text{ are linearly dependent})$$

$$\leq \binom{n}{k} O\left(\frac{1}{\sqrt{d}}\right).$$

Hence (4) gives

$$\text{Prob}(0 \notin \text{conv } A(n)) \geqslant \frac{h(d, n)}{2^{n-1}} - \frac{\sum_{i \leqslant d} \binom{n}{i}}{2^{n-1}} O\left(\frac{1}{\sqrt{d}}\right) = \Phi(-c) + O\left(\frac{1}{n}\right) - O\left(\frac{1}{\sqrt{d}}\right).$$

4. Final Remarks

If Komlós' conjecture is true, then the method given above yields, for $n = O(d)$,

$$\text{Prob}(0 \notin \text{conv } A(n)) = \frac{h(n, d)}{2^{n-1}} + O(d^2/(1+\varepsilon)^d).$$

Of course, this method can be used in all cases when the underlying set of the points T is symmetric, and Prob($x_1, \ldots, x_d$, T are linearly dependent) $= 1 - o(1)$, for example,

Theorem 4.1 (Wendel [7]). *Let B^d denote the d-dimensional ball. Let us choose an n-element set P randomly. Then*

$$\text{Prob}(0 \notin \text{conv } P) = h(d, n)/2^{n-1}.$$

Actually, Wendel used a similar inductional method (but he did not need our lemmas except the equality $h(P) = h(d, n)$ for affine independent n-sets $P \subset \mathbb{R}^d$). Finally, it is easy to see that in our case ($n \sim 2d$, $d \to \infty$) we have

$$\text{Prob}(0 \in \text{int conv } P) - \text{Prob}(0 \in \text{conv } P) \to 0.$$

References

1. C. Buchta and J. Müller, Random polytopes in a ball, *J. Appl. Probab.* **21** (1984), 753-762.
2. P. Erdös and J. Mycielski, private communication.
3. E. F. Harding, The number of partitions of a set of n points in k dimensions induced by hyperplanes, *Proc. Edinburgh Math. Soc.* (2) **15** (1966/67), 285-289.
4. J. Komlós, On the determinant of (0, 1)-matrices, *Studia Sci. Math. Hungar.* **2** (1967), 7-21.
5. J. Komlós, unpublished.
6. J. Mycielski, On random convex hulls, *Colloq. Math.*, to appear.
7. J. G. Wendel, A problem in geometric probability, *Math. Scand.* **11** (1962), 109-111.
8. R. O. Winder, Partitions of N-space by hyperplanes, *SIAM J. Appl. Math.* **14** (1966), 811-818.
9. T. Zaslavsky, *Facing up to Arrangements: Face-count Formulas for Partitions of Space by Hyperplanes*, Memoir 154, American Mathematical Society, Providence, RI, 1975.

Received November 12, 1985.