Two Lower Bounds for Random Point Sets via Negative Association

Denys Bulavka, Olivier Devillers, Philippe Duchon, Marc Glisse, Xavier Goaoc

Two Lower Bounds for Random Point Sets via Negative Association*

Denys Bulavka† Olivier Devillers‡ Philippe Duchon§ Marc Glisse¶
Xavier Goaoc‖

Abstract

We present two lower bounds that hold with high probability for random point sets. We first give a new, and elementary, proof that the classical models of random point sets (uniform in a smooth convex body, uniform in a polygon, Gaussian) have a superconstant number of extreme points with high probability. We next prove that any algorithm that determines the orientation of all triples in a planar set of n points (that is, the order type of the point set) from their Cartesian coordinates must read with high probability $4n \log n - O(n \log \log n)$ coordinate bits. This matches previously known upper bounds. Both bounds rely on a method due to Dubhashi and Ranjan (*Random Structures and Algorithms*, 1998) for obtaining concentration results via a *negative association* property.

1 Introduction

The analysis of random point sets is a classical theme in discrete and computational geometry and many statistics have been studied in the course of average-case analysis of geometric algorithms or to better understand what to expect from a typical point set, see *e.g.* [1, 3, 4, 6, 7, 8, 11]. While the simpler results give asymptotic estimates on the expectation of the statistic considered, it is natural to aim for more precise statements, where bounds on the variance or higher moments ensure that the statistic is close to its average with high probability. Such results often follow from recasting the statistic considered as a sum of independent contributions [26], and in many cases establishing this independence leads to substantial technical complications (we will see examples shortly).

Some 25 years ago, Dubhashi and Ranjan [13] established that several of the benefits of independence are also enjoyed by random variables that are *negatively dependent* in the sense that, intuitively, when one is high the others tend to be low (see Section 2 for a formal definition). In this paper, we apply these ideas to analyze random point sets, where negatively dependence is easily found, and prove lower bounds with high probability on the typical number of extreme points and on the typical resolution of the order types.

*Funded by grant ANR-17-CE40-0017 of the French National Research Agency (ANR project ASPAG)

†Department of Applied Mathematics, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic dbulavka@kam.mff.cuni.cz

‡Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France Olivier.Devillers@inria.

§LaBRI, Université de Bordeaux, CNRS, Bordeaux INP, F33504 Talence, France philippe.duchon@u-bordeaux.fr

¶Université Paris-Saclay, CNRS, Inria, Laboratoire de Mathématiques d'Orsay, 91405, Orsay, France Marc.Glisse@inria.fr

‖Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France Xavier.Goaoc@loria.fr

1.1 Context and motivation

Before we state our results let us provide some background.

Orientations and order types. Given three points $p, q, r \in \mathbb{R}^2$, the *orientation* of the triple (p, q, r) is defined as $+1$ if r is to the left of the line (pq), oriented from p to q, -1 if r is to the right of that line, and 0 if r is on that line. More generally, the orientation of a $(d+1)$-tuple $(p_1, p_2, \ldots, p_{d+1})$ of points in $\mathbb{R}^d$ can be defined as

$$\operatorname{orient}(p_1, p_2, \ldots, p_{d+1}) = \operatorname{sign} \det \begin{pmatrix} (p_1)_1 & (p_2)_1 & \ldots & (p_{d+1})_1 \\ (p_1)_2 & (p_2)_2 & \ldots & (p_{d+1})_2 \\ \vdots & \vdots & & \vdots \\ (p_1)_{d+1} & (p_2)_{d+1} & \ldots & (p_{d+1})_{d+1} \\ 1 & 1 & \ldots & 1 \end{pmatrix}$$

Two point sets A and B have *the same order type* if there is a bijection $A \to B$ that preserves all orientations. This defines an equivalence relation on finite point sets, and an *order type* is an equivalence class for that relation. A point set in an order type is also said to *realize* that order type. An order type of point sets in $\mathbb{R}^d$ is *simple* if all orientations are non zero.

The order type of a point set determines many of its properties (*e.g.* its convex hull and convex layers, its k-sets, its triangulations or crossing-free graphs, ...) while being amenable to combinatorial analysis (*e.g.* it enjoys a Ramsey-type theorem [24, §9.3]). A natural question arises:

What can be said about the order type of a random point set?

For instance, Han et al. [19] proved that for random samples of the unit square, a threshold phenomenon occurs with respect to the property of containing all order types of a given size.

Random polytopes and concentration. In stochastic geometry, an established model of *random polytope* is the convex hull of a set of n random points chosen independently from one and the same distribution μ, where μ is either a Gaussian distribution in $\mathbb{R}^d$ (the *Gaussian setting*) or the uniform measure on a compact convex body in $\mathbb{R}^d$, usually assumed to be smooth (the *smooth setting*) or a polytope (the *polytopal setting*). The number of extreme points (or faces of higher dimension) is a natural statistic to investigate; although the estimates of the expectation are classical, bounds on the variance were only obtained more recently and with considerably more effort (see the survey of Reitzner [28, §2.2.4]).

These concentration bounds were used by Goaoc and Welzl [15, Theorem 1.1] to show that the order type of certain random point sets are concentrated. Their proof applies to the Gaussian, smooth and polytopal settings, where the variance of the number of extreme points is known, but they conjecture that the phenomenon is more general [15, Conjecture 1.8]. Interestingly, their proof only uses a consequence of the concentration bounds: that the number of extreme points be *asymptotically almost surely superconstant*. With Theorem 1, we give a simple proof that this is true in the Gaussian, smooth and polygonal settings.

Realization on grids. A perturbation argument shows that any simple order type can be realized on a regular grid. Define the *resolution* of a simple planar order type τ as the smallest integer N such that τ can be realized by a subset of $\{1, 2, \ldots, N\}^2$. The resolution of every order type of size n is at most doubly-exponential in n and some order types attain this

bound [17, 21]. Of the $n^{(3+o(1))n}$ order types [16], at least $n^{(3+o(1))n}$ have resolution $O(n^4)$ [30], and the proportion of n-point order types with polynomial resolution is unknown.

Fabila-Monroy and Clemens [14] proved that for every $\epsilon > 0$, with high probability, a uniform sample U_n of n points in the unit square can be rounded to a regular grid of step size proportional to $n^{-3-\epsilon}$ without changing its order type. This was generalized to higher dimension by Cardinal et al. [10] and the planar analysis was also generalized by van der Hoog et al. [32] into a smoothed analysis. As a consequence, the order type of U_n has resolution $O(n^{3+\epsilon})$ with high probability, and the analysis of [14] can be easily modified to show that with probability $1-o(1)$, reading the first $(3+o(1))\log n$ coordinate bits of each point suffices to determine the order type (Theorem 23 in appendix). Our Theorem 2 provides a lower bound with high probability on the number of bits that need to be read from a random point set to determine its order type, even when each point can be refined independently.

Imprecise geometric data. We are not aware of other probabilistic lower bounds in the "pay per input bit" cost model we use in Theorem 2. We note that it relates to the classical theme in computational geometry of coping with uncertainty in the input geometric data, as pioneered by ϵ-geometry, *e.g.* [18, 27, 29], and explored, more recently, by the development of algorithms for *imprecise point sets*, *e.g.* [9, 12, 22, 23].

1.2 Results

As a warm-up, we revisit the problem of counting the number of extreme points in a random point set. We say that a sequence of random variables X_n is *asymptotically almost surely (a.a.s.) superconstant* if there exists a sequence $(e_n)_{n\in\mathbb{N}}$ such that $\lim_{n\to\infty} e_n = +\infty$ and $\lim_{n\to\infty} \mathbb{P}\left(X_n \geq e_n\right) = 1$. We give a new proof of the following results.

Theorem 1. *Let μ be a Gaussian distribution over $\mathbb{R}^d$ or the uniform distribution on a convex body K in $\mathbb{R}^d$ that is smooth with positive curvature or a polytope. A set of n random points sampled independently from μ has asymptotically almost surely a superconstant number of extreme points.*

Theorem 1 is not novel, as it follows (with sharper bounds) from known bounds on the variance of the number of vertices in a random polytope [28]. The main advantage of our proof is its simplicity. We also note that it actually gives the right asymptotic order of magnitude up to $\log\log$ factors.

Now, suppose that we want to design an algorithm (in some standard model of computation, *e.g.* the word-RAM model) that solves some problem an uncertain input point set. The algorithm is free to refine the Cartesian coordinates of each point independently and the complexity is measured by the total number of bits read. For the problem of determining all orientations predicates on the unknown point set (that is, of determining its *labeled order type*, or *chirotope*), a simple greedy algorithm reads on average $4n\log n + O(n)$ bits (see appendix). We prove a matching lower bound with high probability.

Theorem 2. *Let $\mathcal{A}$ be any algorithm that, given a set of points in $[0,1]^2$, determines the orientation of every triple. Let $C_{\mathcal{A}}(n)$ denote the number of coordinate bits read by $\mathcal{A}$ to treat a set of n random points sampled independently and uniformly from $[0,1]^2$.*

(i) $\mathbb{E}\left[C_{\mathcal{A}}(n)\right] \geq 4n\log n - O(n\log\log n)$.

(ii) *For every real $\nu > 1$ there exists a real $c > 1$ such that, for n large enough enough,* $\mathbb{P}\left(C_{\mathcal{A}}(n) < 4n\log n - \nu n \log\log n\right) \leq c^{-n}$.

2 Background: negative association

Let us clarify some terminology and notation. For any integer k we write $[k] = \{1, 2, \ldots, k\}$. A function $f : \mathbb{R}^k \to \mathbb{R}$ is *nondecreasing* if for every $x, y \in \mathbb{R}^k$ we have

$$x_i \leq y_i \quad \text{for} \quad i = 1, 2, \ldots, k \qquad \Rightarrow \qquad f(x_1, x_2, \ldots, x_k) \leq f(y_1, y_2, \ldots, y_k).$$

A function $f : \mathbb{R}^k \to \mathbb{R}$ is *nonincreasing* if $-f$ is nondecreasing. Given a vector $X \in \mathbb{R}^k$ and a subset $I = \{i_1, i_2, \ldots, i_\ell\} \subseteq [k]$ with $i_1 < i_2 < \ldots < i_\ell$, we write $(X_i : i \in I)$ for the vector $(X_{i_1}, X_{i_2}, \ldots, X_{i_\ell})$.

2.1 Definition

We now recall the negative association as defined by Dubhashi and Ranjan [13]. A vector $\mathbf{X} = (X_1, \ldots, X_k)$ of real random variables is *negatively associated* if, for any disjoint sets $I, J \subset [k]$ and any functions $f : \mathbb{R}^{|I|} \to \mathbb{R}$ and $g : \mathbb{R}^{|J|} \to \mathbb{R}$ that are both nonincreasing or both nondecreasing we have

$$\mathbb{E}\left[f(X_i : i \in I)g(X_j : j \in J)\right] \leq \mathbb{E}\left[f(X_i : i \in I)\right] \cdot \mathbb{E}\left[g(X_j : j \in J)\right]. \tag{1}$$

Note that if a vector of real random variables is negatively associated, then any permutation of its coordinates is also negatively associated. We therefore say that a *set* of real random variables is negatively associated when the vector formed by one (or any) ordering of these random variables is negatively associated. Note that if a set of random variables is negatively associated, then so is any of its subsets. All sets of random variables considered are finite.

Negative association is a weakening of the property of independence.

Claim 3. *Any finite set of independent random variables is negatively associated.*

Proof. When $X_1, X_2, \ldots, X_k$ are independent, Condition (1) holds with equality for any disjoint sets I and J and any functions f and g (monotonicity is not even required). □

2.2 Easy ways to find negative association

We recall three easy ways provided by Dubhashi and Ranjan [13] to find negative association. We illustrate each of them on random variables useful to analyze random point sets.

0−1 random variables. A 0−1 *random variable* is a random variable with values in $\{0, 1\}$. For $0-1$ random variables, negative association follows from a very simple *dependence*.

Claim 4. *Let $\mathcal{X}$ be a finite set of $0-1$ random variables. If $\sum_{X\in\mathcal{X}} X$ is always at most 1, then $\mathcal{X}$ is negatively associated.*

Proof. Let R be the random variable defined by $R = 1 - \sum_{X\in\mathcal{X}} X$. Dubhashi and Ranjan [13, Lemma 9] proved that any vector of 0−1 random variables that sum to 1 is negatively associated. This applies to $\mathcal{X} \cup \{R\}$, and its subset $\mathcal{X}$ is therefore also negatively associated. □

Example 5. *Here is a geometric illustration. Let μ be some arbitrary probability distribution over $\mathbb{R}^d$ and let $C_1, C_2, \ldots, C_k$ be pairwise disjoint measurable subsets of $\mathbb{R}^d$. Let p be a random point chosen from μ and let A_i denote the indicator function of $p \in C_i$. Claim 4 ensures that the set $\{A_i\}_{1\leq i\leq k}$ is negatively associated.*

Combining independent sets.

Claim 6 ([13, Proposition 8.1])**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be two sets of random variables. If $\mathcal{X}$ and $\mathcal{Y}$ are independent and each set is negatively associated, then $\mathcal{X} \cup \mathcal{Y}$ is negatively associated.*

Example 7. *Following up on Example 5, now suppose $P = \{p_1, p_2, \ldots, p_n\}$ is a set of n random points independently sampled from μ. For $1 \le i \le n$ and $1 \le j \le k$, let $A_{i,j}$ denote the indicator function of the event that point p_i is contained in set C_j. As noted in Example 5, each set $\{A_{i,j}\}_{1 \le j \le k}$ is negatively associated for $1 \le i \le n$. Since the points are independent, Claim 6 ensures that the whole set $\{A_{i,j}\}_{1 \le i \le n, 1 \le j \le k}$ is negatively associated.*

Transforming disjoint subsets of variables.

Claim 8 ([13, Proposition 8.2])**.** *Let $\mathcal{X} = (X_1, X_2, \ldots, X_k)$ be a vector of random variables, let $I_1, I_2, \ldots, I_\ell$ be pairwise disjoint subsets of $[k]$ and for $1 \le j \le \ell$ let $Y_j = f_j(X_i : i \in I_j)$ where $f_i \colon \mathbb{R}^{|I_i|} \to \mathbb{R}$. If $\mathcal{X}$ is negatively associated and the functions $\{f_j\}_{1 \le j \le \ell}$ are all nondecreasing or all nonincreasing, then $(Y_1, Y_2, \ldots, Y_\ell)$ is negatively associated.*

Example 9. *Following up on Example 7, now for $1 \le j \le k$ let B_j denote the indicator function of the event that set C_j is nonempty. Note that $B_j = \max_{i \in [n]} A_{i,j}$ is a nondecreasing function of $\{A_{i,j}\}_{1 \le i \le n}$. Moreover, these sets of random variables are pairwise disjoint and each is negatively associated. The set $\{B_j\}_{1 \le j \le k}$ is thus negatively associated by Claim 8.*

2.3 A Chernoff-Hoeffding bound from negative association

A striking property of negative association is that it can replace the independence assumption in the Chernoff-Hoeffding inequalities.

Theorem 10. *Let $\mathcal{X} = (X_1, \ldots, X_k)$ be a vector of negatively associated, 0–1 random variables. Let $S = X_1 + X_2 + \ldots + X_k$. For any reals $\delta > 0$ and $0 < \lambda < 1$,*

$$\mathbb{P}\left(S \ge (1+\delta)\mathbb{E}\left[S\right]\right) \le \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mathbb{E}[S]} \quad \text{and} \quad \mathbb{P}\left(S \le (1-\lambda)\mathbb{E}\left[S\right]\right) \le \left(\frac{e^{-\lambda}}{(1-\lambda)^{1-\lambda}}\right)^{\mathbb{E}[S]}.$$

Example 11. *Following up on Example 9, let $B = B_1 + B_2 + \ldots + B_k$ denote the number of regions hit by the random point set P. Since the variables $\{B_j\}_{1 \le j \le k}$ are negatively associated 0–1 random variables, taking $\lambda = \frac{1}{2}$, the probability that B is below half its average is at most $\left(\sqrt{\frac{2}{e}}\right)^{\mathbb{E}[B]} \le 0.86^{\mathbb{E}[B]}$.*

For completeness, we provide a proof of the Chernoff-Hoeffding bound for negative association, as it is only sketched in [13].

Proof of Theorem 10. We follow the proof from the textbook of Motwani and Raghavan [25], making changes as appropriate. We let $p_i = \mathbb{P}\left(X_i = 1\right) = \mathbb{E}\left[X_i\right]$ and $m = \sum_{1 \le i \le k} p_i = \mathbb{E}\left[S\right]$.

Upper bound. Let $t > 0$ be some real to be chosen later. The conditions $S \ge (1+\delta)\mathbb{E}\left[S\right]$ and $e^{tS} \ge e^{t(1+\delta)\mathbb{E}[S]}$ are equivalent, and Markov's inequality yields

$$\mathbb{P}\left(S \ge (1+\delta)\mathbb{E}\left[S\right]\right) = \mathbb{P}\left(e^{tS} \ge e^{t(1+\delta)\mathbb{E}[S]}\right) \le \frac{\mathbb{E}\left[e^{tS}\right]}{e^{t(1+\delta)\mathbb{E}[S]}}.$$

Since the $\{X_i\}_{1\leq i\leq k}$ are negatively associated and $x \mapsto e^{tx}$ is increasing, Equation (1) yields

$$\mathbb{E}\left[e^{tS}\right] = \mathbb{E}\left[e^{\sum_i tX_i}\right] = \mathbb{E}\left[\prod_i e^{tX_i}\right] \leq \prod_i \mathbb{E}\left[e^{tX_i}\right].$$

Since X_i is a $0-1$ random variable, we have

$$\mathbb{E}\left[e^{tX_i}\right] = (1-p_i) + p_i e^t = 1 + p_i(e^t - 1) \leq e^{p_i(e^t-1)},$$

where the last inequality only uses the fact that $1 + u \leq e^u$ holds for any $u \in \mathbb{R}$. Combining these three steps, we obtain that

$$\mathbb{P}\left(S \geq (1+\delta)\mathbb{E}\left[S\right]\right) \leq \frac{\prod_{i=1}^{k} e^{p_i(e^t-1)}}{e^{t(1+\delta)\mathbb{E}[S]}} = \frac{e^{(e^t-1)\mathbb{E}[S]}}{e^{t(1+\delta)\mathbb{E}[S]}} = e^{(e^t-1-(1+\delta)t)\mathbb{E}[S]},$$

holds for any $t > 0$. Taking $t = \ln(1+\delta)$ yields the announced upper bound.

Lower bound. The proof is similar. For any $t > 0$ we have

$$\mathbb{P}\left(S \leq (1-\lambda)\mathbb{E}\left[S\right]\right) = \mathbb{P}\left(e^{-tS} \leq e^{-t(1-\lambda)\mathbb{E}[S]}\right) \leq \mathbb{E}\left[e^{-tS}\right] e^{t(1-\lambda)\mathbb{E}[S]},$$

and, again, since the $\{X_i\}_{1\leq i\leq k}$ are negatively associated and $x \mapsto e^{-tx}$ is decreasing, Equation (1) yields

$$\mathbb{E}\left[e^{-tS}\right] \leq \prod_i \mathbb{E}\left[e^{-tX_i}\right] = \prod_i (1 - p_i + p_i e^{-t}) \leq e^{-(1-e^{-t})\mathbb{E}[S]}.$$

Hence, for any $t > 0$ we have $\mathbb{P}\left(S \leq (1-\lambda)\mathbb{E}\left[S\right]\right) \leq \left(e^{e^{-t}-1+t(1-\lambda)}\right)^{\mathbb{E}[S]}$ and taking $t = -\ln(1-\lambda)$ yields the announced lower bound. □

3 Warm-up: superconstant number of extreme points made easy

Let us now show how Theorem 1 follows from Theorem 10 with little effort.

For P a finite point set in $\mathbb{R}^d$, we let $f_0(P)$ denote its number of extreme points. A *cap* for a subset $U \subset \mathbb{R}^d$ is the intersection of U with a closed halfspace. We say that a set C is a cap for a measure if C is a cap for the support of that measure.

Proposition 12. *Let μ be a probability measure in $\mathbb{R}^d$. Suppose that for n large enough, there exist $k(n)$ pairwise disjoint caps for μ, each of μ-measure at least $m(n)$. If $k(n) = \omega(1)$ and $m(n) \geq \frac{\log 3}{n}$, then the number of extreme points among n random points chosen independently from μ is at least $\frac{k(n)}{3}$ with probability $1 - o(1)$.*

Proof. Let us consider some large enough n. Let $k = k(n)$ and let $C_1^n, C_2^n, \ldots, C_k^n$ be pairwise disjoint caps, each of μ-measure at least $m(n)$. Let P_n be a set of n random points chosen independently from μ. For $1 \leq j \leq k$, let B_j denote the indicator function that $C_j^n \cap P_n$ is nonempty. Let $B = B_1 + B_2 + \ldots + B_k$ and remark that $f_0(P_n) \geq B$. Indeed, any cap C_j^n that

contains at least one point of P_n must contain the point of P_n that is extreme in the direction of the inner normal to the halfspace that cuts out the cap. As the caps C_j^n are pairwise disjoint, no two of them can contain the same extreme point.

Let us compute $\mathbb{E}\left[B\right]$. Each B_i has the same distribution, governed by

$$\mathbb{P}\left(B_i{=}1\right) = \mathbb{E}\left[B_i\right] = 1-(1-\mu(C_i^n))^n \geq 1-(1-m(n))^n.$$

Using that $(1-x)^n \leq e^{-nx}$ for any $0<x<1$, we obtain

$$\mathbb{E}\left[B\right] \geq k(n)\left(1-(1-m(n))^n\right) \geq k(n)\left(1-e^{-nm(n)}\right).$$

Since $m(n) \geq \frac{\log 3}{n}$ then for n large enough we have $\mathbb{E}\left[B\right] \geq \frac{2}{3}k(n)$.

The set of $0-1$ random variable $\{B_j\}_{1\leq j\leq k}$ is negatively associated. This follows from Claims 4, 6 and 8 as explained in Example 9. We can therefore apply the lower bound of Theorem 10, with $\lambda = \frac{1}{2}$, to obtain that, for n large enough

$$\mathbb{P}\left(f_0(P_n){\leq}\frac{k(n)}{3}\right) \leq \mathbb{P}\left(B{\leq}\frac{k(n)}{3}\right) \leq \mathbb{P}\left(B{\leq}\frac{\mathbb{E}\left[B\right]}{2}\right) \leq \left(\sqrt{\frac{2}{e}}\right)^{\mathbb{E}[B]} \leq 0.86^{\mathbb{E}[B]}.$$

Since $\mathbb{E}\left[B\right] \geq \frac{2}{3}k(n) = \omega(1)$, for n large enough, we have $\mathbb{P}\left(f_0(P_n) \leq \frac{k(n)}{3}\right) = o(1)$. □

To prove Theorem 1 it remains to construct families of caps and apply Proposition 12. We do that for each type of measure separately.

3.1 Uniform distribution on a smooth convex body

Given a convex body $K \subset \mathbb{R}^d$, we say that K has the *rolling balls property* if there are two constants $r_{\min}$ and $r_{\max}$ such that for all point p on the boundary ∂K of K there are two balls $\mathbf{B}^p_{\min}$ and $\mathbf{B}^p_{\max}$, of radii $r_{\min}$ and $r_{\max}$, tangent in p with $\mathbf{B}^p_{\min} \subset K \subset \mathbf{B}^p_{\max}$ (see Figure 1). In particular a smooth convex body whose curvature is bounded from below and above by two strictly positive finite constants has the rolling ball property.

Corollary 13. *Let μ be the uniform distribution on K, a convex body with the rolling ball property. There exists a constant C depending on K such that a set of n points i.i.d. from μ has at least $C \cdot n^{\frac{d-1}{d+1}}$ extreme points with probability $1-o(1)$.*

Proof. Given a cap defined as the intersection of a convex U with a halfspace H^+, we let w denote the largest distance between H and a point of $U \cap H^+$ and its diameter v to be the diameter of $U \cap H$. If U is a ball, we have $w = \Theta(\frac{v^2}{r})$, $v = \Theta(\sqrt{wr})$ and $\mu(U \cap H^+) = \Theta(wv^{d-1}) = \Theta(r^{-1}v^{d+1}) = \Theta(r^{\frac{d-1}{2}}w^{\frac{d+1}{2}})$ (see Figure 1).

First, we consider $(p_i)_{i\in[k]}$ an ϵ-sampling of ∂K, i.e. the balls $\mathbf{B}\left([p_i,\epsilon]\right)$ of radius ϵ and centered on $(p_i)_{i\in[k]}$ are disjoint, and no disjoint ball of radius ϵ can be added. Thus the balls with the same centers and radius 2ϵ cover ∂K and we can deduce

$$\mathrm{Vol}_{d-1}\left(\partial K\right) \leq \sum_{i=1}^{k} \mathrm{Vol}_{d-1}\left(\mathbf{B}\left([p_i,2\epsilon]\right) \cap \partial K\right) \leq \sum_{i=1}^{k} \mathrm{Vol}_{d-1}\left(\partial\mathbf{B}\left([p_i,2\epsilon]\right)\right) \leq \Theta(k\epsilon^{d-1}).$$

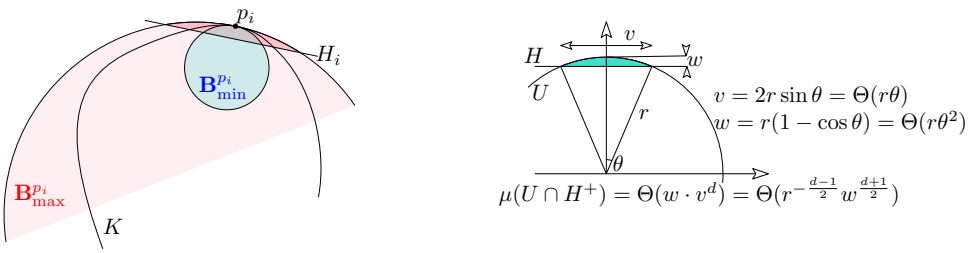

Figure 1: Cap of a smooth convex body with the rolling ball property.

Since K is considered of constant size, we have $k = \Omega(\epsilon^{1-d})$.

For each p_i we can consider $\mathbf{B}^{p_i}_{\min}$, $\mathbf{B}^{p_i}_{\max}$, and H_i the hyperplane parallel to the tangent plane in p_i that cuts $\mathbf{B}^{p_i}_{\max}$ in a ball of radius ϵ. Then

$$\mu(K \cap H_i^+) \geq \mu(\mathbf{B}^{p_i}_{\min} \cap H_i^+) \simeq \left(\frac{r_{\min}}{r_{\max}}\right)^{\frac{d-1}{2}} \mu(\mathbf{B}^{p_i}_{\max} \cap H_i^+) = \Theta\left(\left(\frac{r_{\min}}{r_{\max}}\right)^{\frac{d-1}{2}} r_{\max}^{-1} \epsilon^{d+1}\right) = \Theta(\epsilon^{d+1})$$

since $r_{\min}$ and $r_{\max}$ are constants. Choosing ϵ to be $\Theta(n^{-\frac{1}{d+1}})$ with a suitable constant, we get that the volume of the caps $K \cap H_i^+$ is larger that $\frac{\log 3}{n}$. Altogether, we can apply Proposition 12 and get that $k = \Omega(\epsilon^{1-d}) = \Omega\left(n^{\frac{d-1}{d+1}}\right)$ with high probability. □

3.2 Gaussian distributions

We now turn our attention to Gaussian distributions in $\mathbb{R}^d$. Since the extreme points are unchanged under affine transform, we consider the standard normal distribution $\mathcal{N}(0, I_d)$. The number of extreme points among n points chosen i.i.d. from $\mathcal{N}(0, I_d)$ has expectation and variance $\Theta\left(\log^{\frac{d-1}{2}} n\right)$ [28]. Our lower bound requires little effort and is close to optimal.

Corollary 14. *The number of extreme points among n random points chosen independently from $\mathcal{N}(0, I_d)$ is $\Omega\left(\left(\frac{\log n}{\log\log n}\right)^{\frac{d-1}{2}}\right)$ with probability $1-o(1)$.*

Proof. Let $\mu = \mathcal{N}(0, I_d)$. Let us fix $n \geq d+1$ and let P_n be a set of n random points chosen independently from μ. The fact that μ is supported on all of $\mathbb{R}^d$ makes it impossible to construct more than two disjoint caps for μ. We handle this by truncating μ so that the law of the number of extreme points does not change much. Specifically, for any real $r > 0$, let $\mathbf{B}_r$ denote the closed ball of radius r centered at the origin and let $\overline{\mathbf{B}}_r$ denote its complement. We let μ_r denote the conditioning of μ to lie in $\mathbf{B}_r$ and we let $Q_{r,n}$ denote a set of n random points chosen independently from μ_r. We note that the number of extreme points of P_n conditioned on $P_n \subseteq \mathbf{B}_r$ has the same law as the number of extreme points of $Q_{r,n}$:

$$\forall m \in [n], \qquad \mathbb{P}\left(f_0(P_n) = m \middle| P_n \subseteq \mathbf{B}_r\right) = \mathbb{P}\left(f_0(Q_{r,n}) = m\right).$$

First, we compute $\mu(\overline{\mathbf{B}}_r)$. To do so, we make a change of variable to represent a point as $t \cdot u$ where $t \in \mathbb{R}^+$ and $u \in \mathbb{S}^{d-1}$ the unit sphere. The Jacobian of this change of variable is $t^{d-1}J(u)$,

where J does not depend on t, see [5]. We also use the incomplete gamma function given by $\Gamma(s,x)=\int_x^\infty t^{s-1}e^t\mathrm{d}t$. Now,

$$\mu(\overline{\mathbf{B}}_r)=\frac{\int_{x\in\overline{\mathbf{B}}_r}e^{-\frac{\|x\|^2}{2}}\mathrm{d}x}{\int_{x\in\overline{\mathbf{B}}_0}e^{-\frac{\|x\|^2}{2}}\mathrm{d}x}=\frac{\int_r^\infty\int_{u\in\mathbb{S}^{d-1}}e^{-\frac{t^2}{2}}t^{d-1}J(u)\mathrm{d}u\mathrm{d}t}{\int_0^\infty\int_{u\in\mathbb{S}^{d-1}}e^{-\frac{t^2}{2}}t^{d-1}J(u)\mathrm{d}u\mathrm{d}t}=\frac{\int_{\frac{r^2}{2}}^\infty x^{\frac{d}{2}-1}e^{-x}\mathrm{d}x}{\int_0^\infty x^{\frac{d}{2}-1}e^{-x}\mathrm{d}x}=\frac{\Gamma(\frac{d}{2},\frac{r^2}{2})}{\Gamma(\frac{d}{2})}$$

where we have made the change of variables $x=\frac{t^2}{2}$. If d is even, let $l=\frac{d}{2}-1$, otherwise let $l=\frac{d}{2}-\frac{1}{2}$ The incomplete gamma function satisfies the following recurrence relation $\Gamma(s+1,x)=s\Gamma(s,x)+x^se^{-x}$, hence

$$\Gamma\left(\tfrac{d}{2},\tfrac{r^2}{2}\right)=\Gamma\left(\tfrac{d}{2}-l,\tfrac{r^2}{2}\right)\prod_{i=1}^{l}\left(\tfrac{d}{2}-i\right)+e^{-\frac{r^2}{2}}\sum_{i=1}^{l}\left(\tfrac{r^2}{2}\right)^{\frac{d}{2}-i}\prod_{j=1}^{i-1}\left(\tfrac{d}{2}-j\right)=\Theta\left(e^{-\frac{r^2}{2}}\left(\tfrac{r^2}{2}\right)^{\frac{d}{2}-1}\right)$$

$$\text{since }\Gamma\left(1,\tfrac{r^2}{2}\right)=\int_{\frac{r^2}{2}}^\infty e^{-t}\mathrm{d}t=e^{-\frac{r^2}{2}}\text{ and }\Gamma\left(\tfrac{1}{2},\tfrac{r^2}{2}\right)=\sqrt{2}\int_r^\infty e^{-\frac{t^2}{2}}\mathrm{d}t=\Theta\left(\frac{e^{-\frac{r^2}{2}}}{r}\right).$$

We choose $r(n)=\sqrt{2\log n+d\log\log n+\Theta(1)}$ so that $\mu(\overline{\mathbf{B}}_{r(n)})=\frac{1}{n\log n}$. The size of $\overline{\mathbf{B}}_{r(n)}\cap P_n$ is a sum of independent, $0-1$ random variables, namely the indicator functions that each point is in $\overline{\mathbf{B}}_{r(n)}$. That size has average $\frac{1}{\log n}$ and applying Theorem 10 with $\delta=\log n-1$ we obtain

$$\mathbb{P}\left(P_n\not\subseteq\mathbf{B}_{r(n)}\right)=\mathbb{P}\left(|\overline{\mathbf{B}}_{r(n)}\cap P_n|\geq 1\right)\leq\left(\frac{e^{\log n-1}}{(\log n)^{\log n}}\right)^{\frac{1}{\log n}}\leq\frac{e}{\log n}.$$

$$\text{Altogether,}\quad\forall m\in[n],\qquad\mathbb{P}\left(f_0(P_n)\geq m\right)\geq\left(1-\frac{e}{\log n}\right)\mathbb{P}\left(f_0(Q_{r(n),n})\geq m\right),\tag{2}$$

and it remains to apply Proposition 12 to $\mu_{r(n)}$.

Now, we proceed by lower bounding the μ_r-measure of a cap. For any real $a>0$ the μ-measure of the halfspace $H_a=\{(x_1,\ldots,x_d)\in\mathbb{R}^d\colon x_1\geq a\}$ is given by [20, Ch. 2, Sec. 3]

$$\mu(H_a)=\frac{1}{\sqrt{2\pi}}\int_a^\infty e^{-\frac{x^2}{2}}\mathrm{d}x\geq\left(\frac{1}{a}-\frac{1}{a^3}\right)\frac{1}{\sqrt{2\pi}}e^{-\frac{a^2}{2}}.$$

$$\text{Then,}\qquad\mu_r(H_a)\geq\mu(H_a)-\mu(\overline{\mathbf{B}}_{r(n)})\geq\left(\frac{1}{a}-\frac{1}{a^3}\right)\frac{1}{\sqrt{2\pi}}e^{-\frac{a^2}{2}}-\frac{1}{n\log(n)}.$$

Taking $a=\sqrt{2\log(n)-\log\log n-\log(25\pi)}$ and using that for $a\geq\sqrt{2}$ we have $(\frac{1}{a}-\frac{1}{a^3})\geq\frac{1}{2a}$ we obtain that, for n large enough, $\mu_{r(n)}(H_a)$ verifies the hypothesis of Proposition 12 :

$$\mu_{r(n)}(H_a)\geq\frac{1}{2\sqrt{2\log n-\log\log n-\log(25\pi)}}\frac{1}{\sqrt{2\pi}}\frac{\sqrt{\log n}\sqrt{25\pi}}{n}-\frac{1}{n\log n}\geq\frac{5}{4n}-\frac{1}{n\log n}\geq\frac{\log 3}{n}.$$

The halfspace $H(a)$ cuts out a cap of angle $\theta(n)\in[0,\frac{\pi}{2}]$ on $\partial\mathbf{B}_{r(n)}$:

$$\theta(n)=\arccos\left(\frac{a}{r(n)}\right)=\arccos\left(\frac{\sqrt{2\log n-\log\log n-\log(25\pi)}}{\sqrt{2\log n+d\log\log n+O(1)}}\right)$$

$$=\arccos\left(1-\frac{(d-1)\log\log n}{4\log n}+O\left(\frac{1}{\log n}\right)\right)=\sqrt{\frac{(d-1)\log\log n}{2\log n}}+O\left(\frac{1}{\sqrt{\log n}}\right).$$

Consider an inclusion-maximal family of k disjoint caps of angle θ. Let V_d denote the d-volume of the unit sphere of $\mathbb{R}^d$. The $(d-1)$-volume of the boundary of $\mathbf{B}_{r(n)}$ is $dV_d r(n)^{d-1}$. The $(d-1)$-volume of the boundary of a caps of angle θ is[1] smaller than $V_{d-1}\left(\tan(2\theta)r(n)\right)^{d-1}$. Doubling the opening angle θ of each caps covers the sphere $\partial\mathbf{B}_{r(n)}$, so $k \geq \sqrt{\pi}d\left(\frac{1}{4\theta}\right)^{d-1}$. Proposition 12 ensures that $Q_{r(n),n}$ has at least $\frac{1}{3}k \geq \frac{\sqrt{\pi}d}{3}\left(\frac{(d-1)\log n}{8\log\log n}\right)^{\frac{d-1}{2}} + O(1)$ extreme points with probability $1-o(1)$. Theorem 1 for the case where μ is a Gaussian distribution then follows from Equation (2). □

3.3 The uniform distribution in a polygon

Let T denote the triangle with vertices $(0,0)$, $(0,1)$ and $(1,0)$ and let μ_T be the uniform distribution on T. For any subset $P \subseteq T$ we write $\widehat{P} = P \cup \{(1,0),(0,1)\}$. The number of extreme points among n points chosen i.i.d. from μ_T has expectation and variance $\Theta(\log n)$ [28]. Our lower bound requires little effort and is close to optimal.

Corollary 15. *Let P_n be a set of n random points chosen independently from μ_T. The number of extreme points in $\widehat{P}_n$ is $\Omega\left(\frac{\log n}{\log\log n}\right)$ with probability $1-o(1)$.*

Proof. Let $\mu = \mu_T$. For $0 < t < 1$, let F_t denote the region $\{(x,y) \in \mathbb{R}^2 \mid x+y \leq 1, xy \geq \frac{t}{2}\}$. Let μ_t denote the uniform distribution on F_t, renormalized so as to be a probability measure. Let P_n be a set of n random points chosen independently from μ. Let $Q_{t,n}$ be a set of n random points chosen independently from μ_t. We note that

$$\forall m \in [n], \qquad \mathbb{P}\left(f_0(\widehat{P}_n) = m \middle| P_n \subseteq F_t\right) = \mathbb{P}\left(f_0(\widehat{Q}_{t,n}) = m\right),$$

For $t = t(n) = \frac{2}{n\log^2 n}$ we have $\mu(F_{t(n)}) \geq 1 - \frac{1}{n\log n}$. Indeed, *c.f.* Figure 2,

$$\begin{aligned} 1-\mu(F_t) &= 2\left(\tfrac{1}{2}\left(\sqrt{\frac{t}{2}}\right)^2 + \int_{\sqrt{\frac{t}{2}}}^1 \frac{t}{2}x\mathrm{d}x\right) = \frac{t}{2} + t\left(\log 1 - \log\sqrt{\frac{t}{2}}\right) \\ &= -\frac{t}{4}\log t + \left(\frac{1}{2} + \frac{1}{2}\log 2)\right)t = \frac{1}{n\log n}\left(\tfrac{1}{2} + O\left(\tfrac{\log\log n}{\log n}\right)\right). \end{aligned}$$

As a consequence, $\mathbb{P}\left(P_n \subseteq F_{t(n)}\right) \geq 1 - \frac{e}{\log n}$ and

$$\forall m \in [n], \qquad \mathbb{P}\left(f_0\left(\widehat{P}_n\right) \geq m\right) \geq \left(1 - \frac{e}{\log n}\right)\mathbb{P}\left(f_0\left(\widehat{Q}_{t(n),n}\right) \geq m\right). \tag{3}$$

So let us place some caps on the arc of hyperbola $xy = \frac{t(n)}{2}$ bounding $F_{t(n)}$.

Let us shorten $t = t(n)$. Every point on that hyperbola has coordinates $(t^a, \frac{1}{2}t^{1-a})$ for $a \in I$ where I is the interval solution of $t^a + \frac{1}{2}t^{1-a}$. It can be checked that $[0.1, 1.1] \subset I$ when $t < 0.2$. The cap that cuts the hyperbola in the points with parameters v and $w = v + \delta$, with $\delta > 0$, thus contains the triangle these two points span with the point with parameter $u = v + \frac{\delta}{2}$. The

[1] the volume of a cap is smaller than the volume of the intersection of the hyperplane tangent to $\partial\mathbf{B}_{r(n)}$ at the center of the cone with the cone of angle 2θ.

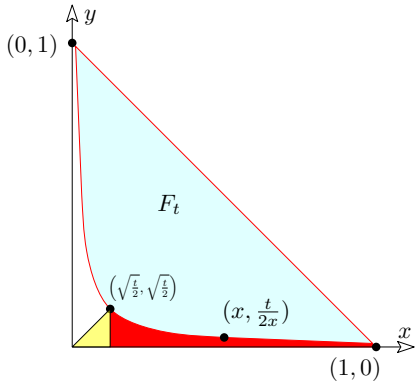

Figure 2: For the proof of Corollary 15 The area of $T \setminus F_t$ is twice the red and yellow areas.

area A of this triangle satisfies that

$$2A = \det \begin{pmatrix} x_v - x_u & x_w - x_u \\ y_v - y_u & y_w - y_u \end{pmatrix} = (t^v - t^u)(\tfrac{1}{2}t^{1-w} - \tfrac{1}{2}t^{1-u}) - (\tfrac{1}{2}t^{1-v} - \tfrac{1}{2}t^{1-u})(t^w - t^u)$$

$$\frac{4A}{t} = t^{v-w} - t^{v-u} - t^{u-w} - t^{w-v} + t^{u-v} + t^{w-u} \quad = \; t^{-\delta} - 2t^{-\delta/2} - t^{\delta} + 2t^{\delta/2}$$

Note that this area is independent of v. Since $\delta > 0$, we have $A \geq \frac{1}{8}t(n)^{1-\delta}$ when $t(n)$ is small enough. For $\delta = \frac{2\log\log n + 2\log 2 + \log\log 3}{\log n + 2\log\log n - \log 2} = O\left(\frac{\log\log n}{\log n}\right)$ we have

$$A \geq \frac{1}{8}t(n)^{1-\delta} \geq \frac{1}{8}\left(n\log^2 n\right)^{\delta-1} = \frac{\log 3}{n}.$$

Since interval $I \ni a$ has length 1, we can construct $\frac{1}{\delta} = \Omega\left(\frac{\log n}{\log\log n}\right)$ disjoint caps for $\mu_{t(n)}$ each with measure at least $\frac{\log 3}{n}$, so Proposition 12 ensures that $\widehat{Q}_{t,n}$ has at least $\Omega\left(\frac{\log n}{\log\log n}\right)$ extreme points with probability $1 - o(1)$. With Equation (3), this implies the statement. □

In Corollary 15, every point of P_n that is extreme in $\widehat{P}_n$ is extreme in a direction in which the extreme point of T is $(0, 0)$. This allows to analyze polygons one triangle at a time.

Corollary 16. *Let μ be the uniform distribution on a convex polygon $K \subset \mathbb{R}^2$ and let P_n be a set of n random points chosen independently from μ. The number of extreme points in P_n is $\Omega\left(\frac{\log n}{\log\log n}\right)$ with probability $1 - o(1)$.*

Proof. Let T' be the triangle formed by three consecutive vertices κ_1, κ_2 and κ_3 of K. Let $P'_n = P_n \cap T'$ and let $\widehat{P'}_n = P'_n \cup \{\kappa_1, \kappa_3\}$. Let V denote the set of directions in which the extreme point of K is κ_2. Observe that if $P_n \cap T'$ is nonempty, then the points of P_n extreme in a direction of V are exactly the points of P'_n extreme in $\widehat{P'}_n$.

Let n' denote the size of P'_n. Conditioned on the value of n', the number of points of P'_n extreme in $\widehat{P'}_n$ is bounded from below by Corollary 15 since nondegenerate affine transforms preserve extreme points. The average of n' is $\mu(T')n$, and since n' is a sum of independent $0-1$ random variables, the Chernoff-Hoeffding bound ensures that it is at least $\frac{\mu(T')}{2}n$ with

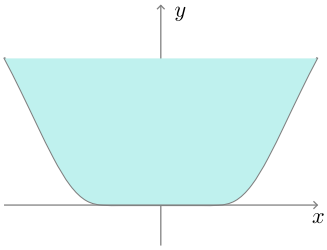

Figure 3: The graph of e^{-1/x^2} is C^2 while having unbounded radius of curvature at $x = 0$.

probability at least $1 - 0.86^{\mu(T')n} = 1 - o(1)$. Altogether, $\widehat{P'}_n$ has $\Omega\left(\frac{\log n}{\log\log n}\right)$ extreme points with probability $1 - o(1)$ and the statement follows. □

3.4 More general measures

Corollaries 13 and 16 generalize to probability measures that are not uniform, but have a density function that takes values in some interval $[c_1, c_2]$, $0<c_1<c_2<\infty$. Does Theorem 2 generalize to probability distributions uniform on more general convex sets (see *e.g.* Figure 3)?

Consider a compact, convex body $K \subset \mathbb{R}^d$ and let μ be the uniform probability distribution on K. Fix some $0 < t < 1$, and let W_t denote the union of all the halfspaces of μ-measure at most t. The region $K_t = K \setminus W_t$ is the *floating body* of K with parameter t. Our proofs of Corollaries 14 and 15 restrict the measure to a floating body with a parameter that ensures that K_t has μ-measure at least $1-\frac{1}{n\log n}$ and, for the polygonal setting, has controlled curvature. This is naturally inspired by the classical relation between floating bodies and random polytopes(see *e.g* [28, §2.2.3]). There are good estimates on the volume of K_t for general K [2], and K_t is known to be strictly convex and, in general, more regular than K [31], but it seems a more precise control is required.

Question 17. *Are there $r_{\min}(t)$ and $r_{\max}(t)$ such that for every compact convex set K, the floating body K_t has the rolling balls property with parameters $r_{\min}(t)$ and $r_{\max}(t)$? What are these functions?*

One could also go in the other direction:

Question 18. *Given $r_{\min}$ and $r_{\max}$, what is the largest real $a(r_{\min}, r_{\max})$ such that any compact convex set K contains a convex set K' such that K' has the rolling balls property with parameters $r_{\min}$ and $r_{\max}$ and the volume of K' is at least $a(r_{\min}, r_{\max})$ times that of K?*

4 Determining planar order types, two bits at a time

Let $P = \{p_1, p_2, \ldots, p_n\}$ be an *arbitrary* set of n points in the unit square, no three aligned. Knowing k bits of a coordinate of p_i means that this coordinate belongs to an interval of length 2^{-k}. For $i \in [n]$, we define $L(i)$ as the smallest k such that *at least one* horizontal or vertical segment of length 2^{-k} starting in p_i is *disjoint* from *all* lines $p_a p_b$ with $a, b \in [n] \setminus \{i\}$ (see Figure 4-left).

Lemma 19. *Any algorithm that determines the orientation of every triple of P must read, for every i, at least $L(i) - 1$ bits of each coordinate of p_i.*

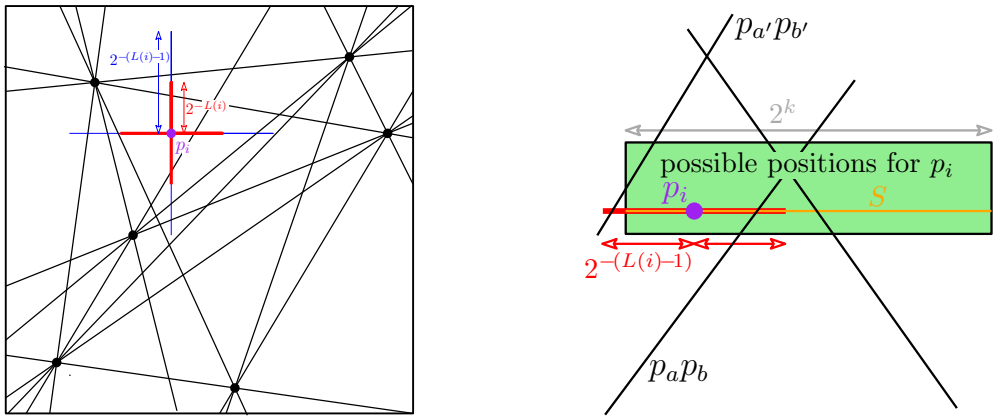

Figure 4: Left: definition of $L(i)$; Right: for the proof of Lemma 19.

Proof. Assume that we know k bits of the x-coordinate of the point p_i. The set of possible positions for p_i then contains a horizontal segment S of length 2^{-k} containing p_i. In fact, it would be exactly such a segment if we knew the y-coordinate of p_i to infinite precision.

By definition of $L(i)$, the two horizontal segments of length $2^{-(L(i)-1)}$ starting in p_i both intersect some line p_ap_b with $a, b \in [n] \setminus \{i\}$ (the lines are different for the two segments). If $2^{-k} \geq 2 \cdot 2^{-(L(i)-1)}$, then the segment S contains at least one of these horizontal segments, and is also intersected by some line p_ap_b with $a, b \in [n] \setminus \{i\}$. Since the possible positions of p_i contain S, this means that the bits read so far from p_i do not suffice to determine the orientation of the triple (p_i, p_a, p_b), even if p_a and p_b were known to infinite precision. □

The rest of this section analyzes the random variable $L(\cdot)$ when P is a uniform sample of the unit square. The variables $L(i)$ have the same distribution, so we only study one of them.

Lemma 20. $\forall \nu > 1,\ \exists c' > 0$ *such that* $\mathbb{P}\left(L(1) \leq 2\log n - \nu \log\log n\right) \leq 2^{-c'n}$.

Lemma 20 readily implies the lower bound announced in Theorem 2 on the average number of bits read by any algorithm that determines all orientations.

Proof of Theorem 2. All n variables $L(i)$ have the same expectation and by Lemma 19, any algorithm that determines the chirotope of P must read at least a total of $2(\sum_i L(i) - 1)$. Statement (ii) follows via a union bound.

For Statement (i), it suffices to determine $\mathbb{E}\left[L(1)\right]$, which rewrites as $\mathbb{E}\left[L(1)\right] = \sum_{k\geq 0} \mathbb{P}\left(L(1) \geq k\right)$. Note that $\mathbb{P}\left(L(1) \geq k\right)$ decreases with k.

Let us fix some $\nu > 1$. By Lemma 20, there is a constant $c' > 0$ such that the first $2\log n - \nu \log\log n$ terms are at least $1 - 2^{-c'n}$. Keeping only these terms, we get

$$\mathbb{E}\left[L(1)\right] \geq (1 - 2^{-c'n})\,(2\log n - \nu\log\log n) \geq (1 - 2^{-c'n})2\log n - \nu\log\log n.$$

For large n, $2^{-c'n+1}\log n < \log\log n$ so Statement (i) follows by linearity of expectation. □

The end of the paper is devoted to the proof of Lemma 20.

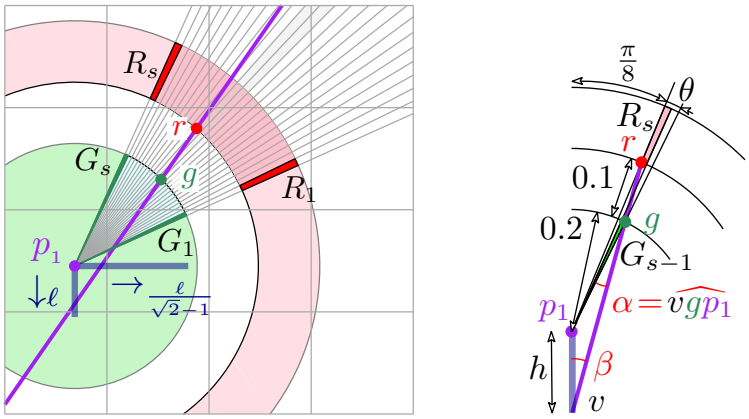

Figure 5: Left: Subdivision in cones around p_1. Right: For the proof of Lemma 21

4.1 The geometric discretization

Our approach is to look for lines passing close to p_1, as such lines are likely to force $L(1)$ to be large. Formally, let $\uparrow_\ell$, $\leftarrow_\ell$, $\downarrow_\ell$ and $\rightarrow_\ell$ denote the segments of length ℓ with p_1 as, respectively, lowest, rightmost, highest and leftmost point. To ensure that $L(1) \geq k$, it suffices that $P \setminus \{p_1\}$ contains two points that define a line intersecting each of these segments for $\ell = 2^{-k}$. To analyze the probability that such pairs of points exist, we discretize the region around p_1. We spell out the analysis for $\downarrow_{2^{-k}}$ and $\rightarrow_{2^{-k}}$, the other two segments being handled similarly.

Let us consider a green disk of center p_1 and radius 0.2 and a red annulus with center p_1 and radii 0.3 and 0.4. We choose a diagonal direction $(\pm 1, \pm 1)$ in which the boundary of the unit square is furthest away from p_1; For the rest of the section we assume this direction is $(1, 1)$ but the other cases are symmetric. We divide the cone of half-angle $\pi/8$ around that direction into s sectors of angle $\frac{\pi}{4s}$ each. We label $G_1, G_2, \dots G_s$ (resp. $R_1, R_2, \dots R_s$) the intersection of each of our angular sectors with the green disk minus p_1 (resp. the red annulus), in counterclockwise order (see Figure 5-left).

Lemma 21. *If $s \geq 32$, for any point $g \in G_i$ and $r \in R_{i+1}$, the line (gr) intersects $\downarrow_{\frac{\pi}{s}}$.*

Proof. The vertical distance $h = p_1 v$ between p_1 and (gr) is maximal when g and r are placed in the corners of G_{s-1} and R_s on circles of radii 0.2 and 0.3 (see Figure 5-right).

Let us relate this maximal distance h to $\theta = \widehat{gp_1 r}$. With the notations of the figure, considering the triangle vp_1g we have $\beta + \alpha + (\frac{7\pi}{8} - \theta) = \pi$ and deduce $\theta = \beta + \alpha - \frac{\pi}{8}$. The law of sines in the triangle vp_1r and Pythagoras' theorem give

$$\sin\beta = \frac{p_1 r}{vr} \sin\frac{7\pi}{8} = \frac{0.3 \sin\frac{\pi}{8}}{\sqrt{(0.3\cos\frac{3\pi}{8})^2 + (0.3\sin\frac{3\pi}{8} + h)^2}} = \frac{0.3\sin\frac{\pi}{8}}{\sqrt{0.09 + h^2 + 0.6h\cos\frac{\pi}{8}}}$$

and $\sin\alpha = \frac{h}{p_1 g} \sin\beta = \frac{h}{0.2}\sin\beta$. And θ as a function of h (for θ sufficiently small):

$$\theta = \arcsin\left(\frac{0.3}{\sqrt{0.09+h^2+0.6h\cos\frac{\pi}{8}}}\sin\frac{\pi}{8}\right) + \arcsin\left(\frac{0.3}{\sqrt{0.09+h^2+0.6h\cos\frac{\pi}{8}}}\frac{h}{0.2}\sin\frac{\pi}{8}\right) - \frac{\pi}{8}.$$

This function $h \mapsto \theta(h)$ verifies $\theta(h) > \frac{h}{2}$ when $\theta(h) \in [0, 0.05]$. Since θ is the angle of *two* sectors, we have $\theta = 2\frac{\pi}{4s}$. For $s \geq 32$ we have $\frac{\pi}{2s} < 0.05$ and $h < \frac{\pi}{s}$. □

Altogether, we can bound $L(1)$ from below by a simple balls-in-bins condition:

Corollary 22. *Assume that $k \geq 3$ and that $s = 2^{k+2}$. If there exist i, i' in $[s]$ such that P intersects each of the four regions G_i, R_{i+1}, $G_{i'}$, and $R_{i'-1}$, then $L(1) \geq k$.*

Proof. First, note that if a line (gr) with $g \in G_i$ and $r \in R_{i+1}$ intersects $\downarrow_\ell$, then it must also intersect $\rightarrow_{\frac{\ell}{\sqrt{2}-1}}$ (see Figure 5-left). Now, let $g \in G_i \cap P$ and $r \in R_{i+1} \cap P$. Since $s \geq 32$, Lemma 21 ensures that the line (gr) intersects $\downarrow_{\frac{\pi}{s}}$. This line also intersects $\downarrow_\ell$ and $\rightarrow_\ell$ with $\ell = \frac{\pi}{(\sqrt{2}-1)s}$. A symmetry with respect to the line of slope 1 through p_1 gives the intersection with the two other segments from the points in $G_{i'}$ and $R_{i'-1}$. Since $\frac{\pi}{(\sqrt{2}-1)} \leq 8$, the existence of i and i' ensures that all four horizontal and vertical segments of length $\frac{8}{s} = 2^{-k+1}$ starting in p_i are intersected by some lines spanned by $P \setminus \{p_1\}$, so $L(1) > k - 1$. □

The existence of i with $P \cap G_i \neq \emptyset$ and $P \cap R_i \neq \emptyset$ is a *bichromatic birthday problem.*

4.2 The probabilistic analysis

We now analyze the probability that a random point set satisfies the conditions of Corollary 22.

The random variables. Let $\mathcal{O}$ denote the event that there exist a, b in $[s]$ such that each of G_a, R_{a+1}, G_b, R_{b-1} is hit by P. To analyze $\mathbb{P}\left(\mathcal{O}\right)$ we introduce for $i \in [s]$ and $j \in [n-1]$, the random variables

$$\begin{array}{l|l|l} A_{i,j} = \mathbb{1}_{p_{j+1} \in G_i} & B_i = \max_{j \in [n-1]} A_{i,j} & B = \sum_{i \in [s]} B_i \\ A'_{i,j} = \mathbb{1}_{p_{j+1} \in R_i} & B'_i = \max_{j \in [n-1]} A'_{i,j} & B' = \sum_{i \in [s]} B'_i \end{array}$$

(Note that, for a better bookkeeping, we index the events associated with p_j by $j-1$ because p_1 is already chosen.) In plain English, B_i is the indicator variable that G_i is non-empty, and B counts the number of non-empty regions G_i. The B'_i and B' variables do the same for the regions R_i. The definition of the regions ensures that each is fully contained in the unit square, that all G_i have the same area, and that all R_i have the same area. So all the $\{A_{i,j}\}_{i,j}$ are identically distributed, and so are the $\{A'_{i,j}\}_{i,j}$, the $\{B_i\}_i$, and the $\{B'_i\}_i$.

Concentration from negative association. The set of $0-1$ random variable $\{B_i\}_{1 \leq i < n}$ is negatively associated, and so is $\{B'_i\}_{1 \leq i < n}$. This follows from Claims 4, 6 and 8 as explained in Example 9. We can therefore apply the lower bound of Theorem 10, with $\lambda = \frac{1}{2}$, to obtain that

$$\mathbb{P}\left(B \leq \frac{\mathbb{E}\left[B\right]}{2}\right) \leq 0.86^{\mathbb{E}[B]} \quad \text{and similarly} \quad \mathbb{P}\left(B' \leq \frac{\mathbb{E}\left[B'\right]}{2}\right) \leq 0.86^{\mathbb{E}[B']}.$$

Let $\mathcal{G}$ denote the event $\mathcal{G} = \{B \geq \mathbb{E}\left[B\right]/2 \text{ and } B' \geq \mathbb{E}\left[B'\right]/2\}$. A union bound yields

$$\mathbb{P}\left(\mathcal{G}\right) \geq 1 - \left(0.86^{\mathbb{E}\left[B\right]} + 0.86^{\mathbb{E}\left[B'\right]}\right)$$

Estimating $\mathbb{E}\left[\mathbf{B}\right]$ and $\mathbb{E}\left[\mathbf{B}'\right]$. Each G_i has area c_1/s, and each R_i has area c_2/s with $c_1 = \frac{\pi}{200}$ and $c_2 = \frac{7\pi}{800}$. Thus, $A_{i,j}$ and $A'_{i,j}$ are $0-1$ random variables, taking value 1 with probability, respectively, c_1/s and c_2/s. For fixed i, the $\{A_{i,j}\}_{j\in[n-1]}$ are independent. Choosing $s = \frac{n^2}{\log^\nu n}$, we have

$$\mathbb{E}\left[B_i\right] = \mathbb{P}\left(B_i = 1\right) = 1 - \left(1 - \frac{c_1}{s}\right)^{n-1} \geq 1 - e^{-c_1\frac{n-1}{s}} \geq c_1\frac{n-1}{s} - \frac{1}{2}\left(c_1\frac{n-1}{s}\right)^2$$
$$= c_1\frac{n}{s} - \frac{1}{2}\left(c_1\frac{n-1}{s}\right)^2 - \frac{c_1}{s} = c_1\frac{\log^\nu n}{n} - O\left(\frac{\log^{2\nu} n}{n^2}\right).$$

the first and second inequalities coming, respectively, from the facts that for every $t \geq 0$ we have $1-t \leq e^{-t}$ and for every $t \in [0,1]$ we have $1-e^{-t} \geq t - \frac{t^2}{2}$. Then, we plugged in $s = \frac{n^2}{\log^\nu n}$. The same computation gives $\mathbb{E}\left[B'_i\right] \geq c_2\frac{\log^\nu n}{n} - O\left(\frac{\log^{2\nu} n}{n^2}\right)$. Since the B_i are identically distributed, and so are the B'_i, we have

$$\mathbb{E}\left[B\right] = s\mathbb{E}\left[B_i\right] \geq c_1 n - O\left(\log^\nu n\right) \quad \text{and} \quad \mathbb{E}\left[B'\right] = s\mathbb{E}\left[B'_i\right] \geq c_2 n - O\left(\log^\nu n\right).$$

The bichromatic birthday conditioned on the values of B and B'. For two integers γ and ρ let us consider the event $\mathcal{G}_{\gamma,\rho} = \{B = \gamma, B' = \rho\}$ and define $f(\gamma,\rho) = \mathbb{P}\left(\mathcal{O}|\mathcal{G}_{\gamma,\rho}\right)$. The function $f(\gamma,\rho)$ is increasing in both variables (the more occupied regions there are, the more likely it is that the collisions we desire occur). Assume the γ occupied green regions have been chosen. Let T_+ (resp. T_-) denote the set of red regions in sectors following counterclockwise (resp. clockwise) the sectors whose green regions have been chosen. Since the green regions in the boundary angular sectors may be among those chosen, we have $\gamma - 1 \leq |T_+|, |T_-| \leq \gamma$. We now pick the ρ red regions to be occupied. Let E_+ (resp. E_-) denote the event that a region of T_+ (resp. T_-) has been chosen among the ρ red regions. Pretend, for the sake of the analysis, that we choose the red regions one by one. If none of the first i regions chosen is in T_+, then next one has to be picked from the $s-i$ unpicked regions, at least $\gamma - 1$ of which are in T_+. Thus,

$$1 - \mathbb{P}\left(E_+\right) \leq \prod_{i=0}^{\rho-1}\left(1 - \frac{\gamma-1}{s-i}\right) = \frac{(s-\gamma+1)(s-\gamma)\ldots(s-\gamma-\rho+2)}{s(s-1)\ldots(s-\rho+1)}$$
$$= \frac{(s-\rho)!(s-\gamma+1)!}{s!(s-\gamma-\rho+1)!}$$

Using a symmetric argument for T_- and applying a union bound, we get

$$1 - f(\gamma,\rho) \leq 2\,\frac{(s-\rho)!(s-\gamma+1)!}{s!(s-\gamma-\rho+1)!}.$$

Since $\log(N!) \leq N\log(N)$ and for $\gamma = \left\lceil\frac{\mathbb{E}[B]}{2}\right\rceil$ and $\rho = \left\lceil\frac{\mathbb{E}[B']}{2}\right\rceil$, both γ and ρ are $\Theta(n) = o(s)$,

$$\begin{aligned}\log(1-f(\gamma,\rho)) \leq & s\log\frac{(s-\rho)(s-\gamma+1)}{s(s-\gamma-\rho+1)} - \rho\log\frac{s-\rho}{s-\gamma-\rho+1} \\ & - \gamma\log\frac{s-\gamma+1}{s-\gamma-\rho+1} + \log\frac{s-\gamma+1}{s-\gamma-\rho+1} + \log 2 \\ = & s\log\left(1+\frac{\rho(\gamma-1)}{s(s-\gamma-\rho+1)}\right) - \rho\log\left(1+\frac{\gamma-1}{s-\gamma-\rho+1}\right) \\ & - \gamma\log\left(1+\frac{\rho}{s-\gamma-\rho+1}\right) + O\left(\log s\right).\end{aligned}$$

Now in the regime we are looking at, we have $\gamma = c_1 n/2 - O\left(\log^\nu n\right)$, $\rho = c_2 n/2 - O\left(\log^\nu n\right)$, and $s = \frac{n^2}{\log^\nu n}$. Taking first order Taylor expansions, our bound rewrites as

$$\log(1-f(\gamma,\rho)) \leq -\frac{\rho\gamma}{s-\gamma-\rho+1} + O(\log s) = -\frac{c_1 c_2}{4}\log^\nu n + O\left(\log n\right)$$

provided we have $\nu > 1$. Hence, $f(\gamma,\rho) \geq 1 - \exp(\Theta(\log^\nu n))$. Since $f(\gamma,\rho)$ is increasing, the bound apply to any $\gamma \geq \left\lceil \frac{\mathbb{E}[B]}{2} \right\rceil$ and $\rho \geq \left\lceil \frac{\mathbb{E}[B']}{2} \right\rceil$, and we get that $\mathbb{P}\left(\mathcal{O}|\mathcal{G}\right)$ is exponentially close to 1. Since $\mathbb{P}\left(\mathcal{G}\right)$ is also exponentially close to 1, we finally get that our event $\mathcal{O}$ holds with probability exponentially close to 1. With Corollary 22, this proves Lemma 20.

References

[1] Dominique Attali, Jean-Daniel Boissonnat, and André Lieutier. Complexity of the Delaunay triangulation of points on surfaces the smooth case. In *Proceedings of the nineteenth annual symposium on Computational Geometry*, pages 201–210, 2003. doi:10.1145/777792.777823.

[2] I. Bárány and D. G. Larman. Convex bodies, economic cap coverings, random polytopes. *Mathematika*, 35(2):274–291, 1988. doi:10.1112/S0025579300015266.

[3] Imre Bárány and William Steiger. On the expected number of k-sets. *Discrete & Computational Geometry*, 11:243–263, 1994. doi:10.1007/BF02574008.

[4] Marshall Bern, David Eppstein, and Frances Yao. The expected extremes in a Delaunay triangulation. *International Journal of Computational Geometry & Applications*, 1(01):79–91, 1991. doi:10.1142/S0218195991000074.

[5] L. E. Blumenson. Classroom notes: A derivation of n-dimensional Spherical Coordinates. *Amer. Math. Monthly*, 67(1):63–66, 1960. doi:10.2307/2308932.

[6] Karl Heinz Borgwardt. Average-case analysis of the double description method and the beneath-beyond algorithm. *Discrete & Computational Geometry*, 37:175–204, 2007. doi:10.1007/s00454-006-1257-8.

[7] Prosenjit Bose and Luc Devroye. On the stabbing number of a random Delaunay triangulation. *Computational Geometry*, 36(2):89–105, 2007. doi:10.1016/j.comgeo.2006.05.005.

[8] Nicolas Broutin, Olivier Devillers, and Ross Hemsley. Efficiently navigating a random Delaunay triangulation. *Random Structures & Algorithms*, 49(1):95–136, 2016. doi:10.1002/rsa.20630.

[9] Kevin Buchin, Maarten Löffler, Pat Morin, and Wolfgang Mulzer. Preprocessing imprecise points for Delaunay triangulation: Simplified and extended. *Algorithmica*, 61(3):674–693, 2011. doi:10.1007/s00453-010-9430-0.

[10] Jean Cardinal, Ruy Fabila-Monroy, and Carlos Hidalgo-Toscano. Chirotopes of random points in space are realizable on a small integer grid, 2020. doi:10.48550/arXiv.2001.08062.

[11] Nicolas Chenavier and Olivier Devillers. Stretch factor in a planar Poisson-Delaunay triangulation with a large intensity. *Advances in Applied Probability*, 50(1):1–30, 2018. doi:10.1017/apr.2018.3.

[12] Olivier Devillers. Delaunay triangulation of imprecise points, preprocess and actually get a fast query time. *Journal of Computational Geometry*, 2(1):30–45, 2011. doi:10.20382/jocg.v2i1a3.

[13] Devdatt Dubhashi and Desh Ranjan. Balls and bins: A study in negative dependence. *Random Structures and Algorithms*, 13(2):99–124, 1998. doi:10.1002/(SICI)1098-2418(199809)13:2\%3C99::AID-RSA1\%3E3.0.CO;2-M.

[14] Ruy Fabila-Monroy and Clemens Huemer. Order types of random point sets can be realized with small integer coordinates. In *XVII Spanish Meeting on Computational Geometry: book of abstracts, Alicante, June 26-28*, pages 73–76, 2017. URL: https://upcommons.upc.edu/handle/2117/113414.

[15] Xavier Goaoc and Emo Welzl. Convex hulls of random order types. *Journal of the ACM*, 70(1):1–47, 2023. doi:10.1145/3570636.

[16] Jacob E Goodman and Richard Pollack. Upper bounds for configurations and polytopes in $\mathbb{R}^d$. *Discrete & Computational Geometry*, 1(3):219–227, 1986. doi:10.1007/BF02187696.

[17] Jacob E Goodman, Richard Pollack, and Bernd Sturmfels. The intrinsic spread of a configuration in $\mathbb{R}^d$. *Journal of the American Mathematical Society*, pages 639–651, 1990. doi:10.1090/S0894-0347-1990-1046181-2.

[18] Leonidas Guibas, David Salesin, and Jorge Stolfi. Constructing strongly convex approximate hulls with inaccurate primitives. *Algorithmica*, 9:534–560, 1993. doi:10.1007/BF01190154.

[19] Jie Han, Yoshiharu Kohayakawa, Marcelo Tadeu Sales, and Henrique Stagni. On some extremal results for order types. *Acta Mathematica Universitatis Comenianae*, 88(3):779–785, 2019. URL: http://www.iam.fmph.uniba.sk/amuc/ojs/index.php/amuc/article/view/1305.

[20] Ida Kantor, Jiří Matoušek, and Robert Šámal. *Mathematics++: Selected Topics Beyond the Basic Courses*, volume 75. American Mathematical Society, 2015.

[21] Jan Kratochvíl and Jirí Matousek. Intersection graphs of segments. *Journal of Combinatorial Theory, Series B*, 62(2):289–315, 1994. doi:10.1006/jctb.1994.1071.

[22] Maarten Löffler and Jack Snoeyink. Delaunay triangulations of imprecise points in linear time after preprocessing. In *Proceedings of the twenty-fourth annual symposium on Computational geometry*, pages 298–304, 2008. doi:10.1145/1377676.1377727.

[23] Maarten Löffler and Marc van Kreveld. Largest and smallest convex hulls for imprecise points. *Algorithmica*, 56(2):235–269, 2010. doi:10.1007/s00453-008-9174-2.

[24] Jiri Matousek. *Lectures on discrete geometry*, volume 212. Springer Science & Business Media, 2013.

[25] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[26] Wolfgang Mulzer. Five proofs of Chernoff's bound with applications. In *Bulletin of the EATCS (BEATCS)*, 2018. doi:10.48550/arXiv.1801.03365.

[27] Takayuki Nagai, Seigo Yasutome, and Nobuki Tokura. Convex hull problem with imprecise input. In *Discrete and Computational Geometry: Japanese Conference, JCDCG'98 Tokyo, Japan, December 9-12, 1998. Revised Papers*, pages 207–219. Springer, 2000. doi:10.1007/978-3-540-46515-7_18.

[28] M. Reitzner. Random polytopes. In Wilfrid S. Kendall and Ilya Molchanov, editors, *New Perspectives in Stochastic Geometry*, chapter 2, pages 45–75. Oxford University Press, 2009.

[29] David Salesin, Jorge Stolfi, and Leonidas Guibas. Epsilon geometry: building robust algorithms from imprecise computations. In *Proceedings of the fifth annual symposium on Computational geometry*, pages 208–217, 1989. doi:10.1145/73833.73857.

[30] Manfred Scheucher. Many order types on integer grids of polynomial size. *Computational Geometry*, 109:101924, 2023. doi:10.1016/j.comgeo.2022.101924.

[31] Carsten Schütt and Elisabeth Werner. Homothetic floating bodies. *Geom. Dedicata*, 49(3):335–348, 1994. doi:10.1007/BF01264033.

[32] Ivor van der Hoog, Tillmann Miltzow, and Martijn van Schaik. Smoothed analysis of order types, 2019. doi:10.48550/arXiv.1907.04645.

The following section does not rely on negative association and is thus given in appendix, we provide it because it is necessary to prove that the lower bound of Theorem 2 matches the upper bound.

A Upper bound for order types

Theorem 2 proposes a lower bound of roughly $4n \log_2 n$ on the number of bits that must be read to determine the order type.

We propose below (Theorem 24) an algorithm that matches this lower bound and read a different number of bits for each point. We also recall the result of Fabila-Monroy and Huemer [14, Thm 1] (Theorem 23) that says that if we want to read the same number of bits for each point, then you must read roughly $6 \log_2 n$ bits per point.

Let G_m the subdivision of the unit square $[0,1] \times [0,1]$ in a grid whose cells are

$$\left[(i-1)\frac{1}{m}, i\frac{1}{m}\right] \times \left[(j-1)\frac{1}{m}, j\frac{1}{m}\right] \text{ for} i, j \in [n].$$

For a point $p \in [0.1]^2$ reading k bits of each coordinates of p means identifying the grid cell in G_{2^k} containing it.

Theorem 23 ([14]). *Let $\epsilon > 0$, let P_n be a set of random cells i.i.d. in G_{2^k} $k = (3+\epsilon)\log_2 n$. Then, there is no line that stabs three cells in P_n with probability that tends to 1 as n tends to infinity.*

The presentation in Fabila-Monroy and Huemer is different, but the proof of their Theorem 1, can be easily modified to prove the statement above.

Theorem 24. *Let P_n be a set of random points i.i.d. in $[0,1]^2$. The algorithm below determines the order type of P_n by reading on average $4n\log_2 n + O(n)$ coordinate bits.*

Greedy algorithm. Given a point set P. The algorithm that we propose refines greedily the coordinates of a point involved in a triangle with undetermined orientation, until the chirotope can be determined. We start with no bit read, so we only know that all points are in the unit square. At every step, we select one point and read one more bit for both of its coordinates. So, at every step of the algorithm, we divide by two the size of the cell known to contain a point. The selection is done greedily as follows:

> *Find three pairwise distinct indices a, b, c such that the cells known to contain p_a, p_b, p_c can be intersected by a line, and select one among these points whose cell as the greater size.*

We break ties arbitrarily, so this is perhaps a method rather than an algorithm. By definition, when the algorithm stops, the chirotope of P can be determined from the precision at which every point is known. The algorithm does *not* stop if P contains three aligned points.

The end of this section is devoted to the proof of Theorem 24.

Let $P = \{p_1, p_2, \dots p_n\}$. For $i \in [n]$, we define $U(i)$ as the smallest k such that for any $a, b \in [n] \setminus \{i\}$, there does not exist a line that intersects the cells in G_{2^k} that contain p_a, p_b, and p_i. If p_i is aligned with some two other points of P, we let $U(i) = \infty$. The following implies that our greedy algorithm terminates if P has no aligned triple.

Lemma 25. *In the greedy algorithm above, independently of how ties are resolved, for every $i \in [n]$, at most $U(i)$ bits are read from each coordinate of p_i.*

Proof. Assume that at some point in the algorithm, we read the k^{th} bit of both coordinates of point p_i. To read these bits, our selection method requires that there exist $a, b \in [n] \setminus \{i\}$ such that (1) in $\{p_a, p_b, p_i\}$, p_i is one of the points known at coarsest resolution, and (2) there exists a line intersecting the cells known to contain p_a, p_b, and p_i. Condition (1) ensures that for each of $\{p_a, p_b, p_i\}$, the cell known to contain the point is contained in a cell of $G_{2^{k-1}}$. Condition (2) ensures that these cells in $G_{2^{k-1}}$ can be intersected by a line. Thus, $k - 1 < U(i)$. □

Butterflies

Given two points $p, q \in [0,1]^2$, we first let B be the union of all lines intersecting the cells of G_m containing p and q; we then define $B_m(p,q)$ as the intersection of
$[0,1]^2$ with the Minkowski sum of B with a disk of radius $\frac{\sqrt{2}}{m}$. We call $B_m(p,q)$ the *butterfly* of p and q (at resolution m, see Figure 6-left). Note that the butterfly $B_m(p,q)$ contains all the cells intersecting B. Hence, if there exists a line intersecting the cells of p, q and r, then $r \in B_m(p,q)$. The following lemma bounds the area of $B_m(p,q)$ by $O(\frac{1}{m\delta(p,q)})$.

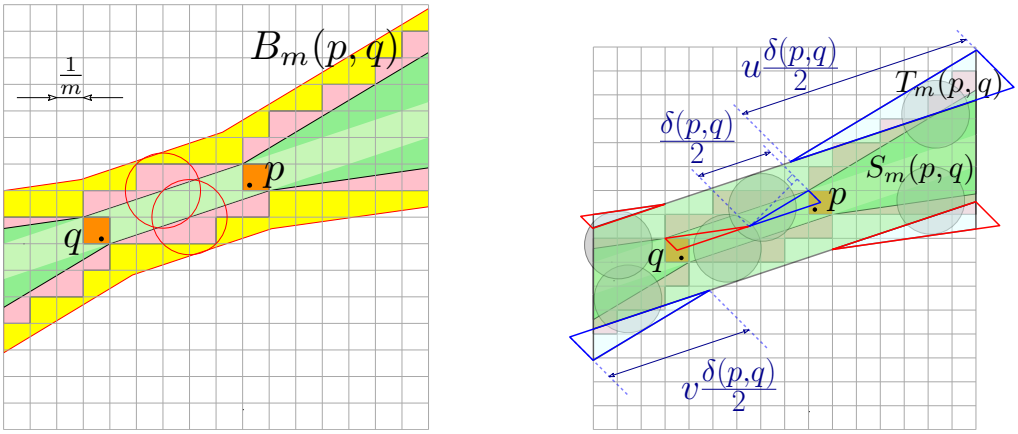

Figure 6: Buterfly, Definition and decomposition.
Right: The grid cells containing two of the points (in orange), the union of lines through them (in green), and the cells intersecting such a line (in red).
Left: Decomposition in a strip and four triangles.

Lemma 26. *The area of $B_m(p,q)$ is at most $\frac{6}{m} + \frac{4}{m\delta(p,q)}$ where $\delta(p,q)$ is the distance between the centers of the cells of p and q.*

Proof. This lemma is similar to Lemma 3 in Fabila-Monroy and Huemer paper [14], although their analogous of butterfly have different definition. Note that the bound holds trivially if p and q are in the same cell ($\delta(p,q) = 0$) or in adjacent cells ($\delta(p,q) = 1/m$). Otherwise, the butterfly $B_m(p,q)$ consists of two parts: a strip $S_m(p,q)$ and the union $T_m(p,q)$ of four triangles (shaded in, respectively, green and blue in Figure 6-right). We have

$$\text{Area}\,(S_m(p,q)) \leq \left(3\frac{\sqrt{2}}{m}\right) \cdot \sqrt{2} = \frac{6}{m}.$$

The four triangles come in two pairs of homothetic triangles, intersected with $[0,1]^2$. Each homothetic pair consists of images under scaling of a triangle whose basis is the half diagonal of a cell of length $\frac{\sqrt{2}}{2m}$ and whose height h is at least $\frac{\delta(p,q)}{2\sqrt{2}}$ (the two kinds of triangles have blue and red boundaries in the Figure 6-right). Letting u and v denote the scaling factors, the areas of the two homothetic triangles sum to $\frac{1}{2}(u^2+v^2)h\frac{\sqrt{2}}{2m}$. Since the scalings turn the height of the reference triangles to two lengths that sum to[2] at most $\sqrt{2}$, we have $(u+v)h \leq \sqrt{2}$. This implies that $u^2+v^2 \leq \left(\frac{\sqrt{2}}{h}\right)^2$ and one pair of homothetic triangles contributes at most $\frac{1}{2}\frac{2}{h^2}h\frac{\sqrt{2}}{2m} = \frac{\sqrt{2}}{2hm} \leq \frac{2}{m\delta(p,q)}$. Altogether, $\text{Area}\,(T_m(p,q)) \leq \frac{4}{m\delta(p,q)}$. Finally $\text{Area}\,(B_m(p,q)) \leq \frac{6}{m} + \frac{4}{m\delta(p,q)}$. □

Distribution of $U(1)$

We now analyze the distribution function of the random variable $U(1)$. Recall that the randomness here refers to the choice of the random points $p_1, p_2, \ldots p_n$, which are taken independently and uniformly in $[0,1]^2$.

[2]The heights are smaller than the sides and the sides are inside the square $[0,1]^2$ and have disjoint projection on the line (pq).

Lemma 27. $\mathbb{P}\left(U(1) > k\right) \leq 57n^2 2^{-k}$.

Proof. This lemma is similar to Lemma 4 in Fabila-Monroy and Huemer paper [14]. In our setting, we have:

$$\begin{aligned}\mathbb{P}\left(U(1) > k\right) &\leq \mathbb{P}\left(\exists i,j \in \binom{[n]\setminus\{1\}}{2} : p_j \in B_{2^k}(p_1,p_i)\right)\\ &\leq (n-1)\mathbb{P}\left(\exists j \in [n]\setminus\{1,2\} : p_j \in B_{2^k}(p_1,p_2)\right)\\ &\leq (n-1)\mathbb{E}\left[1-(1-\text{Area}\left(B_{2^k}(p_1,p_2)\right))^{n-2}\right].\end{aligned}$$

The geometry of $B_{2^k}(p_1,p_2)$ depends on the distance between the centers of the cells that contain p_1 and p_2. We therefore condition on the cell containing p_1, then sum the contributions of the cell containing p_2 by distance to the cell containing p_1. Accounting for boundary effects, for any $1 \leq t \leq 2^k$ there are at most $8t$ cells whose center lies at a distance between $t2^{-k}$ and $(t+1)2^{-k}$ from a given cell. We thus have (using Lemma 26)

$$\begin{aligned}&\mathbb{E}\left[1-(1-\text{Area}\big(B_{2^k}(p_1,p_2)\big)^{n-2}\right]\\ &= \sum_{c\in \text{ cells of } G_{2^k}} \mathbb{P}\left(p_2 \in c\right)\cdot \mathbb{E}\left[1-(1-\text{Area}\big(B_{2^k}(p_1,p_2)\big)^{n-2} \mid p_2 \in c\right]\\ &\leq \frac{1}{(2^k)^2}\sum_{t=1}^{2^k} 8t\left(1-\left(1-\left(\frac{6}{2^k}+\frac{4}{2^k\cdot(t2^{-k})}\right)\right)^{n-2}\right).\end{aligned}$$

Using $(1-x)^{n-2} \geq 1-(n-2)x$ we get

$$\begin{aligned}\mathbb{E}\left[1-(1-\text{Area}\big(B_{2^k}(p_1,p_2)\big)^{n-2}\right] &\leq (n-2)2^{-2k}\sum_{t=1}^{2^k} 8t\left(6\cdot 2^{-k}+\frac{4}{t}\right)\\ &\leq n2^{-2k}\left(\sum_{t=1}^{2^k} 48t2^{-k}\right)+n2^{-2k}2^k 32\\ &\leq 24n2^{-k}(1+2^{-k})+32n2^{-k}.\end{aligned}$$

The statement trivially bounds a probability by something greater than 1 for $k \leq 5$. For $k \geq 6$, the final term is at most $57n2^{-k}$. □

Lemma 28. $\mathbb{E}\left[U(1)\right] \leq 2\log_2 n + 8$

Proof. By definition we have

$$\mathbb{E}\left[U(1)\right] = \sum_{k=1}^{\infty} k\mathbb{P}\left(U(1)=k\right) = \sum_{k=0}^{\infty}\mathbb{P}\left(U(1)>k\right).$$

For the first $2\log_2 n + 6$ terms, we use the trivial upper bound of 1 and for the remaining terms we use the upper bound of Lemma 27:

$$\mathbb{E}\left[U(1)\right] \leq (2\log_2 n+6) + 57n^2 \sum_{k\geq 6+2\log_2 n}^{\infty} 2^{-k} = (2\log_2 n+6) + 57n^2\cdot 2^{-5-2\log_2 n}.$$

Altogether it comes that $\mathbb{E}\left[U(1)\right] \leq 2\log_2 n + 8$. □

We can now prove that our greedy algorithm for deciding the chirotope of P reads on average at most $4n \log_2 n + O(n)$ coordinate bits.

Proof of Theorem 24. By Lemma 25, our greedy algorithm reads at most $U(a)$ bits from each coordinate of point p_a. Thus, using Lemma 28, the average number of bits used by our algorithm is at most:

$$2\mathbb{E}\left[\sum_{i=1}^{n} U(i)\right] = 2\sum_{i=1}^{n} \mathbb{E}\left[U(i)\right] = 2n\mathbb{E}\left[U(1)\right] \leq 4n \log_2 n + 16n. \qquad \square$$

We can also prove Theorem 23:

Proof of Theorem 23. By Lemma 27, $\mathbb{P}\left(U(1)\,(3+\epsilon)\log_2 n\right) \leq 57n^2 n^{-3-\epsilon} \leq n^{-1-\epsilon}$. Thus by union bound, the probability that one point needs to read more than $(3+\epsilon)\log_2 n$ is

$$\mathbb{P}\left(\exists i \in [n] : U(i)\,(3+\epsilon)\log_2 n\right) \leq 57n^{-\epsilon}. \qquad \square$$