Asymptotics Bounds on the Combinatorial Diameter of Random Polytopes

Gilles Bonnet[1*] Daniel Dadush[2†] Uri Grupel[3]
gilles.bonnet@rub.de dadush@cwi.nl uri.grupel@uibk.ac.at
Sophie Huiberts[2] Galyna Livshyts[4]
s.huiberts@cwi.nl glivshyts6@math.gatech.edu

[1]Faculty of Mathematics, Ruhr University Bochum, Germany
[2]Centrum Wiskunde & Informatica, Netherlands
[3]Faculty of Mathematics, University of Innsbruck, Austria
[4]Faculty of Mathematics, Georgia Institute of Technology, USA

September 15, 2021

Abstract

The combinatorial diameter $\operatorname{diam}(P)$ of a polytope P is the maximum shortest-path distance between any pair of vertices. In this paper, we provide upper and lower bounds on the combinatorial diameter of a random "spherical" polytope, which is tight to within one factor of dimension when the number of inequalities is large compared to the dimension. More precisely, for an n-dimensional polytope P defined by the intersection of m i.i.d. half-spaces whose normals are chosen uniformly from the sphere, we show that $\operatorname{diam}(P)$ is $\Omega(nm^{\frac{1}{n-1}})$ and $O(n^2 m^{\frac{1}{n-1}} + n^8 16^n)$ with high probability when $m \geq 2^{\Omega(n)}$.

For the upper bound, we first prove that the number of vertices in any fixed two dimensional projection sharply concentrates around its expectation when m is large, where we rely on the $\Theta(n^2 m^{\frac{1}{n-1}})$ bound on the expectation due to Borgwardt [Math. Oper. Res., 1999]. To obtain the diameter upper bound, we stitch these "shadows paths" together over a suitable net using worst-case diameter bounds to connect vertices to the nearest shadow. For the lower bound, we first reduce to lower bounding the diameter of the dual polytope P°, corresponding to a random convex hull, by showing the relation $\operatorname{diam}(P) \geq (n-1)(\operatorname{diam}(P^\circ) - 2)$. We then prove that the shortest-path between any "nearly" antipodal pair vertices of P° has length $\Omega(m^{\frac{1}{n-1}})$.

1 Introduction

When does a polyhedron have small (combinatorial) diameter? This question has fascinated mathematicians, operation researchers and computer scientists for more than half a century. In a letter to Dantzig in 1957, motivated by the study of the simplex method for linear programming, Hirsch

*Funded by the DFG Priority Program (SPP) 2265 Random Geometric Systems, project P23.
†Supported by the ERC Starting grant QIP–805241.

conjectured that any n-dimensional polytope with m facets has diameter at most $m - n$. While recently disproved by Santos [San12] (for unbounded polyhedra, counter-examples were already given by Klee and Walkup [KW+67]), the question of whether the diameter is bounded by a polynomial in n and m, known as the *polynomial Hirsch conjecture*, remains wide open. In fact, the current counter-examples violate the $m - n$ bound by at most 25 percent.

The best known general upper bounds on the combinatorial diameter of polyhedra are the $2^{n-3}m$ bound by Barnette and Larman [Bar69; Lar70; Bar74], which is exponential in n and linear in m, and the *quasi-polynomial* $m^{\log_2 n+1}$ bound by Kalai and Kleitman [KK92]. The Kalai-Kleitman bound was recently improved to $(m-n)^{\log_2 n}$ by Todd [Tod14] and $(m-n)^{\log_2 O(n/\log n)}$ by Sukegawa [Suk19]. Similar diameter bounds have been established for graphs induced by certain classes of simplicial complexes, which vastly generalize 1-skeleta of polyhedra. In particular, Eisenbrand et al [Eis+10] proved both Barnette-Larman and Kalai-Kleitman bounds for so-called connected-layer families (see Theorem 23), and Labbé et al [LMS17] extended the Barnette-Larman bound to pure, normal, pseudo-manifolds without boundary.

Moving beyond the worst-case bounds, one may ask for which families of polyhedra does the Hirsch conjecture hold, or more optimistically, are there families for which we can significantly beat the Hirsch conjecture? In the first line, many interesting classes induced by combinatorial optimization problems are known, including the class of polytopes with vertices in $\{0,1\}^n$ [Nad89], Leontief substitution systems [Gri71], transportation polyhedra and their duals [Bal84; BVS06; BDF18], as well as the fractional stable-set and perfect matching polytopes [MS14; San18].

Related to the second vein, there has been progress on obtaining diameter bounds for classes of "well-conditioned" polyhedra. If P is a polytope defined by an integral constraint matrix $A \in \mathbb{Z}^{m\times n}$ with all square submatrices having determinant of absolute value at most Δ, then diameter bounds polynomial in m, n and Δ have been obtained [DF94; Bon+14; DH16; NSS21]. The best current bound is $O(n^3\Delta^2 \log(\Delta))$, due to [DH16]. Extending on the result of Naddef [Nad89], strong diameter bounds have been proved for polytopes with vertices in $\{0, 1, \ldots, k\}^n$ [KO92; DM16; DP18]. In particular, [KO92] proved that the diameter is at most nk, which was improved to $nk - \lceil n/2\rceil$ for $k \geq 2$ [DM16] and to $nk - \lceil 2n/3\rceil - (k-2)$ for $k \geq 4$ [DP18].

Diameter of Random Polytopes. With a view of beating the Hirsch bound, the main focus on this paper will be to analyze the diameter of random polytopes, which one may think of as well-conditioned on "average". Coming both from the average case and smoothed analysis literature [Bor87; Bor99; ST04; Ver09; DH19], there is tantilizing evidence that important classes of random polytopes may have very small diameters.

In the average-case context, Borgwardt [Bor87; Bor99] proved that for $P := Ax \leq 1$, $A \in \mathbb{R}^{m\times n}$ where the rows of A are drawn from any rotational symmetric distribution (RSD), that the expected number of edges in any fixed 2 dimensional projection of P – the so-called *shadow bound* – is $O(n^2 m^{\frac{1}{n-1}})$. Borgwardt also showed that this bound is tight when the rows of A are drawn uniformly from the sphere, that is, the expected shadow size is $\Theta(n^2 m^{\frac{1}{n-1}})$. In the smoothed analysis context, A has the form $\bar{A} + \sigma G$, where $\bar{A}$ is a fixed matrix with rows of ℓ_2 norm at most 1 and G has i.i.d. $\mathcal{N}(0,1)$ entries and $\sigma > 0$. Bounds on the expected size of the shadow in this context were first studied by Spielman and Teng [ST04], later improved by [Ver09; DH19], where the best current bound is $O(n^2\sqrt{\log m}/\sigma^2)$ due to [DH19] when $\sigma \leq \frac{1}{\sqrt{n \log m}}$.

From the perspective of short paths, these results directly implies that if one samples objectives v, w uniformly from the sphere, then there is a path between the maximizers of v and w in P

of expected length $O(n^2 m^{\frac{1}{n-1}})$ in the RSD model, and expected length $O(n^2\sqrt{\log m}/\sigma^2)$ in the smoothed model. That is, "most pairs" of vertices (with respect to the distribution in the last sentence), are linked by short expected length path. Note that both of these bounds scale either sublinearly or logarithmically in m, which is far better than $m - n$. While these bounds provide evidence, they do not directly upper bound the diameter, since this would need to work for all pairs of vertices rather than most pairs.

A natural question is thus whether the shadow bound is close to the true diameter. In this paper, we show that this is indeed the case, in the setting where the rows of A are drawn uniformly from the sphere and when m is (exponentially) large compared to n. More formally, our main result is as follows:

Theorem 1. *Suppose that $n, m \in \mathbb{N}$ satisfy $n \geq 2$ and $m \geq 2^{\Omega(n)}$. Let $A^\mathsf{T} := (a_1, \dots, a_M) \in \mathbb{R}^{n\times M}$, where M is Poisson distributed with $\mathbb{E}[M] = m$, and $a_1, \dots, a_M$ are sampled independently and uniformly from $\mathbb{S}^{n-1}$. Then, letting $P(A) := \{x \in \mathbb{R}^n : Ax \leq 1\}$, with probability at least $1 - 4n^{-n}m^{-1}$, we have that*

$$\Omega(nm^{\frac{1}{n-1}}) \leq \operatorname{diam}(P(A)) \leq O(n^2 m^{\frac{1}{n-1}} + n^8 16^n).$$

In the above, we note that the number of constraints M is chosen according to a Poisson distribution with expectation m. This is only for technical convenience (it ensures useful independence properties), and with small modifications, our arguments also work in the case where $M := m$ deterministically. Also, since the constraints are chosen from the sphere, M is almost surely equal to the number of facets of $P(A)$ above (i.e., there are no redundant inequalities).

From the bounds, we see that $\operatorname{diam}(P(A)) \leq O(n^2 m^{\frac{1}{n-1}})$ as long as $m \geq 2^{\Omega(n^2)}$. This shows that the shadow bound indeed upper bounds the diameter when $m \to \infty$. Furthermore, the shadow bound is tight to within one factor of dimension in this regime. We note that in the upper bound is already non-trivial when $m \geq 2^{cn}$, for $c \geq 1$ sufficiently large, since then $O(n^2 m^{\frac{1}{n-1}}) + 2^{O(n)} = 2^{O(n)} \leq m - n$.

While our bounds are only interesting when m is exponential, the bounds are nearly tight asymptotically, and as far as we are aware, they represent the first non-trivial improvements over worst-case upper bounds for a natural class of polytopes defined by random halfspaces.

Our work naturally leaves two interesting open problems. The first is whether the shadow bound upper bounds the diameter when m is polynomial in n. The second is to close the factor n gap between upper and lower bound in the large m regime.

Prior work. Lower bounds on the diameter of $P(A)$, $A^\mathsf{T} = (a_1, \dots, a_m) \in \mathbb{R}^{n\times m}$, were studied by Borgwardt and Huhn [BH99]. They examined the case where each row is sampled from a RSD with radial distribution $\Pr_a[\|a\|_2 \leq r] = \frac{\int_0^r (1-t^2)^\beta t^{n-1} dt}{\int_0^1 (1-t^2)^\beta t^{n-1} dt}$, for $r \in [0, 1]$, $\beta \in (-1, \infty)$. Restricting their results to the case $\beta \to -1$, corresponding to the uniform distribution on the sphere (where the bound is easier to state), they proved a lower bound of $\Omega(m^{1/(n-1)(1-\delta(n))} n^{-\delta(n)})$, where $\delta(n) \to 0$ as $n \to \infty$. We improve their lower bound to $\Omega(nm^{1/(n-1)})$ when $m \geq 2^{\Omega(n)}$, noting that $m^{1/(n-1)} = O(1)$ for $m = 2^{O(n)}$.

In terms of upper bounds, the diameter of a *random convex hull of points*, instead of a random intersection of halfspaces, has been implicitly studied. Given $A^\mathsf{T} = (a_1, \dots, a_m) \in \mathbb{R}^{n\times m}$, let us define

$$Q(A) := \operatorname{conv}(\{a_1, \dots, a_m\}) \tag{1}$$

to be the convex hull of the rows of A. When the rows of A are sampled uniformly from $\mathbb{B}_2^n$, the question of when the diameter of $Q(A)$ is exactly 1 (i.e., every pair of distinct vertices is connected by an edge) was studied by Bárány and Füredi[BF88]. They proved that with probability $1-o(1)$, $\mathrm{diam}(Q(A)) = 1$ if $m \le 1.125^n$ and $\mathrm{diam}(Q(A)) > 1$ if $m \ge 1.4^n$.

In dimension 3, letting $a_1, \dots, a_M \in \mathbb{S}^2$ be chosen independently and uniformly from the 2-sphere, where M is Poisson distributed with $\mathbb{E}[M] = m$, Glisse, Lazard, Michel and Pouget [Gli+16] proved that with high probability the maximum number of edges in any 2-dimensional projection of $Q(A)$ is $\Omega(\sqrt{n})$. This in particular proves that the combinatorial diameter is at most $O(\sqrt{n})$ with high probability.

It is important to note that the geometry of $P(A)$ and $Q(A)$ are strongly related. Indeed, as long as $m = \Omega(n)$ and the rows of A are drawn from a symmetric distribution, $P(A)$ and $Q(A)$ are polars of each other. That is, $Q(A)^\circ = P(A)$ and $P(A)^\circ := \{x \in \mathbb{R}^n : \langle x, y\rangle \le 1, \forall y \in P(A)\} = Q(A)$[1].

As we will see, our proof of Theorem 1 will in fact imply similarly tight diameter bounds for $\mathrm{diam}(Q(A))$ as for $\mathrm{diam}(P(A))$, yielding analogues and generalizations of the above results, when $A^\mathsf{T} = (a_1, \dots, a_M) \in \mathbb{R}^{n\times M}$ and M is Poisson with $\mathbb{E}[M] = m$. More precisely, we will show that for $m \ge 2^{\Omega(n)}$, with high probability

$$\Omega(m^{\frac{1}{n-1}}) \le \mathrm{diam}(Q(A)) \le O(nm^{\frac{1}{n-1}} + n^8 16^n).$$

In essence, for m large enough, our bounds for $\mathrm{diam}(Q(A))$ are a factor $\Theta(n)$ smaller than our bounds for $\mathrm{diam}(P(A))$. This relation will be explained in the next section.

Organization. In Section 2, we introduce some basic notation as well as background materials on Poisson processes, the measure of spherical caps, and concentration inequalities for independent random variables. In Section 3, we prove the upper bound. Halfway into that section, we also prove Theorem 12, a tail bound on the shadow size that is of independent interest. We prove the lower bound in Section 4.

2 Preliminaries

For notational simplicity in the sequel, it will be convenient to treat A as a subset of $\mathbb{S}^{n-1}$ instead of a matrix. For $A \subseteq \mathbb{S}^{n-1}$, we will slightly abuse notation and let $P(A) := \{x \in \mathbb{R}^n : \langle x, a\rangle \le 1, \forall a \in A\}$ and $Q(A) := \mathrm{conv}(A)$.

2.1 Cap Volumes

For a subset $C \subseteq \mathbb{S}^{n-1}$, we write $\sigma(C) := \sigma_{n-1}(C)$ to denote the measure of C with respect to the uniform measure on $\mathbb{S}^{n-1}$. In particular, $\sigma(\mathbb{S}^{n-1}) = 1$. For $v \in \mathbb{S}^{n-1}, \varepsilon \ge 0$, let $C(v, \varepsilon) := \{x \in \mathbb{S}^{n-1} : \|x - v\| \le \varepsilon\}$ denote the spherical cap of radius ε around v.

We will need relatively precise estimates on the measure of spherical caps. The following lemma gives a useful upper and lower bounds on the ratio of cap volumes.

[1]Precision: $P(A) = Q(A)^\circ$ always holds and $P(A)^\circ = Q(A)$ requires that $0 \in Q(A)$ which, as a direct consequence of Wendel's theorem [SW08, Theorem 8.2.1], happens with probability $1 - o(1)$ when $m \ge cn$ for some $c > 2$. In general $P(A)^\circ = \mathrm{conv}(A \cup \{0\})$ holds.

Lemma 2. *For any $s, \varepsilon > 0$ and $v \in \mathbb{S}^{n-1}$ we have*

$$\frac{\sigma(C(v,(1+s)\varepsilon))}{(1+s)^{n-1}} \leq \sigma(C(v,\varepsilon)) \leq \frac{\sigma(C(v,(1-s)\varepsilon))}{(1-s)^{n-1}},$$

assuming for the first inequality that $(1+s)\varepsilon \leq 2$ and for the second that $s < 1$ and $\varepsilon \leq 2$.

Proof. First we write the area of the cap as the following integral, for any $r \in [0,2]$

$$\sigma(C(v,r)) = c_{n-1} \int_0^{r^2/2} \sqrt{2t - t^2}^{\,n-3} \mathrm{dt},$$

where $c_{n-1} := \mathrm{vol}_{n-2}(\mathbb{S}^{n-2})/\mathrm{vol}_{n-1}(\mathbb{S}^{n-1})$. Note that $\sqrt{2t-t^2}$ is the radius of the slice $\mathbb{S}^{n-1} \cap \{x \in \mathbb{S}^{n-1} : \langle x, v \rangle = 1 - t\} = (1-t)v + \sqrt{2t-t^2}(S^{n-1} \cap v^\perp)$. The scaling of the volume of the central slice by $\sqrt{2t-t^2}^{\,n-3}$ instead of $\sqrt{2t-t^2}^{\,n-2}$ is to account for the curvature of the sphere. With this integral in our toolbox, we can prove our desired inequalities. We start with the first one, assuming that $(1+s)^2 r^2/2 \leq 2$ so that we only take square roots of positive numbers.

$$\begin{aligned}
\sigma(C(v,(1+s)\varepsilon)) &= c_{n-1} \int_0^{(1+s)^2 r^2/2} \sqrt{2t - t^2}^{\,n-3} \mathrm{dt} \\
&= c_{n-1}(1+s)^2 \int_0^{r^2/2} \sqrt{2(1+s)^2 u - (1+s)^4 u^2}^{\,n-3} \mathrm{du} \\
&\leq c_{n-1}(1+s)^2 \int_0^{r^2/2} \sqrt{2(1+s)^2 u - (1+s)^2 u^2}^{\,n-3} \mathrm{du} \\
&= (1+s)^{n-1} c_{n-1} \int_0^{r^2/2} \sqrt{2u - u^2}^{\,n-3} \mathrm{du} \\
&= (1+s)^{n-1} \sigma(C(v,\varepsilon)).
\end{aligned}$$

The second similarly, assuming that $1 - s \geq 0$:

$$\begin{aligned}
\sigma(C(v,(1-s)\varepsilon)) &= c_{n-1} \int_0^{(1-s)^2 r^2/2} \sqrt{2t - t^2}^{\,n-3} \mathrm{dt} \\
&= c_{n-1}(1-s)^2 \int_0^{r^2/2} \sqrt{2(1-s)^2 t - (1-s)^4 t^2}^{\,n-3} \mathrm{dt} \\
&\geq c_{n-1}(1-s)^2 \int_0^{r^2/2} \sqrt{2(1-s)^2 t - (1-s)^2 t^2}^{\,n-3} \mathrm{dt} \\
&= c_{n-1}(1-s)^{n-1} \int_0^{r^2/2} \sqrt{2t - t^2}^{\,n-3} \mathrm{dt} \\
&= c_{n-1}(1-s)^{n-1} \sigma(C(v,\varepsilon)).
\end{aligned}$$

□

We now give absolute estimates on cap volume measure due to [Bri+01]. We note that [Bri+01] parametrize spherical caps with respect to the distance of their defining halfspace to the origin.

The following lemma is derived using the fact that the cap $C(v,\varepsilon)$, $\varepsilon \in [0,\sqrt{2}]$, $v \in \mathbb{S}^{n-1}$, is induced by intersecting $\mathbb{S}^{n-1}$ with the halfspace $\langle v, x\rangle \geq 1-\varepsilon^2/2$, whose distance to the origin is exactly $1-\varepsilon^2/2$.

Lemma 3. *[Bri+01, Lemma 2.1] For $n \geq 2$, $\varepsilon \in [0,\sqrt{2}]$, $v \in \mathbb{S}^{n-1}$, the following estimates holds:*

- *If $\varepsilon \in [\sqrt{2(1-\frac{2}{\sqrt{n}})}, \sqrt{2}]$, then $\sigma(C(v,\varepsilon)) \in [1/12, 1/2]$.*
- *If $\varepsilon \in [0, \sqrt{2(1-\frac{2}{\sqrt{n}})}]$, then*

$$\frac{1}{6(1-\varepsilon^2/2)\sqrt{n}}(\varepsilon\sqrt{1-\varepsilon^2/4})^{n-1} \leq \sigma(C(v,\varepsilon)) \leq \frac{1}{2(1-\varepsilon^2/2)\sqrt{n}}(\varepsilon\sqrt{1-\varepsilon^2/4})^{n-1}.$$

2.2 Poisson Processes

The Poisson distribution $\mathrm{Pois}(\lambda)$ with parameter $\lambda \geq 0$ has probability mass function $f(x,\lambda) := e^{-\lambda}\frac{\lambda^x}{x!}$, $x \in \mathbb{Z}_+$. We note that $\mathrm{Pois}(0)$ is the random variable taking value 0 with probability 1. Recall that $\mathbb{E}[\mathrm{Pois}(\lambda)] = \lambda$. We will rely on the following standard tail-estimate (see [Can19, Theorem 1]):

Lemma 4. *Let $X \sim \mathrm{Pois}(\lambda)$. Then for $x \geq 0$, we have that*

$$\max\{\Pr[X \geq \lambda + x], \Pr[X \leq \lambda - x]\} \leq e^{-\frac{x^2}{2(\lambda+x)}}. \tag{2}$$

We define a random subset A to be distributed as $\mathrm{Pois}(\mathbb{S}^{n-1},\lambda)$, $\lambda \geq 0$, if $A = \{a_1,\dots,a_M\}$, where $|A| = M \sim \mathrm{Pois}(\lambda)$ and $a_1,\dots,a_M$ are uniformly and independently distributed on $\mathbb{S}^{n-1}$. Note that $\mathbb{E}[|A|] = \lambda$. In standard terminology, A is called a homogeneous Poisson point process on $\mathbb{S}^{n-1}$ with intensity $\lambda > 0$.

A basic fact about such a Poisson process is that the number of samples landing in disjoint subsets are independent Poisson random variables.

Proposition 5. *Let $A \sim \mathrm{Pois}(\mathbb{S}^{n-1},\lambda)$. Let $C_1,\dots,C_k \subseteq \mathbb{S}^{n-1}$ be pairwise disjoint measurable sets. Then, the random variables $|A \cap C_i|$, $i \in [k]$, are independent and $|A \cap C_i| \sim \mathrm{Pois}(\lambda\sigma(C_i))$, $i \in [k]$.*

2.3 Density Estimates

In this section, we give bounds on the fineness of the net induced by a Poisson distributed subset of $\mathbb{S}^{n-1}$. Roughly speaking, if A is $\mathrm{Pois}(\mathbb{S}^{n-1},m)$ distributed then A will be $\Theta((\log m/m)^{1/(n-1)})$-dense, see Definition 6. While this estimate is standard in the stochastic geometry, it is not so easy to find a reference giving quantitative probabilistic bounds, as more attention has been given to establishing exact asymptotics as $m \to \infty$ (see [RS16]). We provide a simple proof of this fact here, together with the probabilistic estimates that we will need.

Definition 6. *For $w \in \mathbb{S}^{n-1}$ and $r \geq 0$, we write $C(w,r) = \{x \in \mathbb{S}^{n-1} : \|w-x\| \leq r\}$.*

We say $A \subseteq \mathbb{S}^{n-1}$ is ε-dense in the sphere for $\varepsilon > 0$ if for every $w \in \mathbb{S}^{n-1}$ there exists $a \in A$ such that $a \in C(w,\varepsilon)$.

Lemma 7. *Let $m \geq n \geq 2$ be such that $p = 3e\log(n^n m)/m \leq 1/12$. Let $\varepsilon > 0$ be such that $\sigma(C(v,\varepsilon)) = p$ for any $v \in \mathbb{S}^{n-1}$. Then, for $A \sim \mathrm{Pois}(\mathbb{S}^{n-1}, m)$,*

$$\Pr[\exists v \in \mathbb{S}^{n-1} : \ C(v,\varepsilon) \cap A = \emptyset] \leq n^{-n} m^{-2},$$

and for every $t \geq 1$,

$$\Pr[\exists v \in \mathbb{S}^{n-1} : \ |C(v, t\varepsilon) \cap A| \geq 2epmt^{n-1}] \leq (n^n m^2)^{-t^{n-1}}.$$

Proof. Let $N \subseteq \mathbb{S}^{n-1}$ denote the centers of a maximal packing of spherical caps of radius $\varepsilon/(2n)$. By maximality, N is ε/n net. Comparing volumes, by Lemma 2, we see that

$$1 \geq |N|\sigma(C(v, \varepsilon/(2n)) \geq |N|(2n)^{-(n-1)}\sigma(C(v,\varepsilon)),$$

so $|N| \leq (2n)^{n-1} \cdot 1/p \leq (2n)^n m$. By way of a net argument, using that $|C(v,(1-1/n)\varepsilon) \cap A| \sim \mathrm{Pois}(m|C(v,(1-1/n)\varepsilon)$, $\forall v \in \mathbb{S}^{n-1}$, we analyze our first probability

$$\begin{aligned}
\Pr[\exists v \in \mathbb{S}^{n-1} : \ C(v,\varepsilon) \cap A = \emptyset] &\leq \Pr[\exists v \in N : \ C(v,(1-1/n)\varepsilon) \cap A = \emptyset] \\
&\leq |N| \max_{v \in N} \Pr[C(v,(1-1/n)\varepsilon) \cap A = \emptyset] \\
&= (2n)^n m e^{-m\sigma(C(v,(1-1/n)\varepsilon))} \\
&\leq (2n)^n m e^{-(1-1/n)^{n-1} m\sigma(C(v,\varepsilon))} \\
&\leq (2n)^n m e^{-pm/e} \leq n^{-n} m^{-2}.
\end{aligned}$$

We now prove the second estimate. For $t \geq 1$, let $\lambda := m\sigma(C(v,(1+1/n)t\varepsilon))$. By Lemma 2, we have that $\lambda \leq (1+1/n)^{n-1} t^{n-1} m\sigma(C(v,\varepsilon)) \leq et^{n-1}pm$. By a similar net argument as above, we see that

$$\begin{aligned}
\Pr[\exists v \in \mathbb{S}^{n-1} : \ |C(v,t\varepsilon) \cap A| \geq 2epmt^{n-1}] &\leq \Pr[\exists v \in N : \ |C(v,(1+1/n)t\varepsilon) \cap A| \geq 2epmt^{n-1}] \\
&\leq |N| \max_{v \in N} \Pr[|C(v,(1+1/n)t\varepsilon) \cap A| \geq 2epmt^{n-1}] \\
&\leq |N| \Pr_{X \sim \mathrm{Pois}(\lambda)}[X \geq 2epmt^{n-1}] \leq |N| e^{-\frac{(2epmt^{n-1}-\lambda)^2}{2(2epmt^{n-1})}} \\
&\quad (\text{ by the Poisson tailbound, Lemma 4 }) \\
&\leq |N| e^{-\frac{e}{4}pmt^{n-1}} \leq (2n)^n m (n^n m)^{-3t^{n-1}} \leq (n^n m^2)^{-t^{n-1}}.
\end{aligned}$$

□

We now give effective bounds on the density estimate ε above. Note that taking the $n-1^{th}$ root of the bounds for ε^{n-1} below yields $\varepsilon = \Theta((\log m/m)^{1/(n-1)})$ for $m = n^{\Omega(1)}$. The stated bounds follow directly from the cap measure estimates in Lemma 3.

Corollary 8. *Let $\varepsilon > 0$ be as in Lemma 7, i.e., satisfying $\sigma(C(v,\varepsilon)) = 3e\log(n^n m)/m \leq 1/12$. Then $\varepsilon \in [0, \sqrt{2(1-\frac{2}{\sqrt{n}})}]$,*

$$\varepsilon^{n-1} \geq 12e\log(n^n m)/m$$

and

$$\left(\varepsilon/\sqrt{2}\right)^{n-1} \leq \left(\varepsilon\sqrt{1-\varepsilon^2/4}\right)^{n-1} \leq 18e\sqrt{n}\log(n^n m)/m.$$

Proof. The claim $\varepsilon \in [0, \sqrt{2(1-\frac{2}{\sqrt{n}})}]$ follows by Lemma 3 part 1 and our assumption that $|C(v,\varepsilon)| \leq 1/12$. The lower bound on ε^{n-1} follows from the upper bound from Lemma 3 part 2

$$3e\log(n^n m)/m = |C(v,\varepsilon)| \leq \frac{1}{2(1-\varepsilon^2/2)\sqrt{n}}(\varepsilon\sqrt{1-\varepsilon^2/4})^{n-1} \leq \frac{\varepsilon^{n-1}}{4},$$

where the last inequality follows since $\varepsilon \in [0, \sqrt{2(1-\frac{2}{\sqrt{n}})}]$. For the upper bound on ε, we relying on the corresponding estimate in Lemma 3 part 2:

$$3e\log(n^n m)/m = |C(v,\varepsilon)| \geq \frac{(\varepsilon\sqrt{1-\varepsilon^2/4})^{n-1}}{6(1-\varepsilon^2/2)\sqrt{n}} \geq \frac{(\varepsilon\sqrt{1-\varepsilon^2/4})^{n-1}}{6\sqrt{n}} \geq \frac{(\varepsilon/\sqrt{2})^{n-1}}{6\sqrt{n}},$$

where the last inequality follows from $\varepsilon \in [0, \sqrt{2}]$. The desired inequalities now follow by rearranging. ☐

2.4 Concentration for Independent Random Variables

For a random variable $X \in \mathbb{R}$, let $\mathrm{Var}[X] := \mathbb{E}[X^2] - \mathbb{E}[X]^2$ denote its variance.

We will require Hoeffding's inequality, see e.g. [BW07].

Lemma 9. *Let $X_1, \ldots, X_n$ be independent random variables taking values in the intervals $[a_i, b_i]$. Denote their sum by $S = X_1 + \cdots + X_n$. Then, for any $t \geq 0$, the following inequality holds*

$$\max\{\Pr[S \geq \mathbb{E}[S] + t], \Pr[S \leq \mathbb{E}[S] - t]\} \leq \exp\left(\frac{-2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

3 Shadow size and upper bounding the diameter

In the first part of this section, we prove a concentration result on the number of *shadow vertices* of $P(A)$. This addresses an open problem from [Bor87]. In the second part, we use the resulting tools to prove Theorem 13, our high-probability upper bound on the diameter of $P(A)$.

Definition 10. *Let $P \subseteq \mathbb{R}^n$ be a polyhedron and $W \subseteq \mathbb{R}^n$ be a two-dimensional plane. We denote by $\mathcal{S}(P, W)$ the set of* shadow vertices*: the vertices of P that maximize a non-zero objective function $\langle w, \cdot\rangle$ with $w \in W$.*

The set of shadow vertices is connected induces a connected subgraph in the graph consisting of vertices and edges of P, and so any two shadow vertices are connected by a path of length at most $|\mathcal{S}(P, W)|$. As such, for nonzero $w_1, w_2 \in W$, we might speak of a *shadow path* from w_1 to w_2 to denote a path from a maximizer of $\langle w_1, \cdot\rangle$ to a maximizer of $\langle w_2, \cdot\rangle$ that stays inside $\mathcal{S}(P, W)$ and is monotonous with respect to $\langle w_2, \cdot\rangle$. The shadow path was studied by Borgwardt:

Theorem 11 ([Bor87; Bor99])**.** *Let $m \geq n$ and fix a two-dimensional plane $W \subseteq \mathbb{R}^n$. Pick any probability distribution on $\mathbb{R}^n$ that is invariant under rotations and let the entries of $A \subseteq \mathbb{R}^n, |A| = m$, be independently sampled from this distribution. Then, almost surely, for any linearly independent $w_1, w_2 \in W$ there is a unique shadow path from w_1 to w_2 and the vertices in $\mathcal{S}(P(A), W)$*

are in one-to-one correspondence to the vertices of $\pi_W(P(A))$, the orthogonal projection of $P(A)$ onto W. Moreover, we have the upper bound

$$\mathbb{E}[|\mathcal{S}(P(A),W)|] = O(n^2 m^{\frac{1}{n-1}}).$$

This upper bound is tight up to constant factors for the uniform distribution on $\mathbb{S}^{n-1}$.

We prove a tail bound for the shadow size when $A \sim \mathrm{Pois}(\mathbb{S}^{n-1}, m)$. This result answers a question of Borgwardt [*The Simplex Method: A Probabilistic Analysis*, 1987] in the asymptotic regime, regarding whether bounds on higher moments of the shadow size can be given. To obtain such concentration, we show that the shadow decomposes into a sum of nearly independent "local shadows", using that A will be ε-dense per Lemma 7, allowing us to apply standard concentration results on independent sums.

Theorem 12 (Diameter Upper Bound)**.** *Let $t = n\sqrt{304\varepsilon^{-1}\log(n^n m^2)} \cdot \left(6e^4 \log(n^n m)2^n\right)^n$, where $\varepsilon > 0$ is as in Lemma 7. Then for $A \sim \mathrm{Pois}(\mathbb{S}^{n-1}, m)$, the shadow size satisfies*

$$\Pr[|\mathcal{S}(P(A),W)| \geq \mathbb{E}[|\mathcal{S}(P(A),W)|] + t] \leq 304 n^{-n+1} m^{-2}.$$

In the second part of this section, we extend on this line of argument for our main upper bound result.

Theorem 13 (Diameter Upper Bound)**.** *Let $A = \{a_1, \ldots, a_M\} \in \mathbb{S}^{n-1}$, where M is Poisson with $\mathbb{E}[M] = m$, and $a_1, \ldots, a_M$ are uniformly and independently distributed in $\mathbb{S}^{n-1}$. Then, we have that*

$$\Pr[\mathrm{diam}(P(A)) > O(n^2 m^{\frac{1}{n-1}} + n^8 16^n)] < O(1/m).$$

3.1 Only 'nearby' constraints are relevant

We will start by showing that, with very high probability, constraints that are 'far away' from a given point on the sphere will not have any impact on the paths nearby. That will result in a limited degree of independence between different parts of the sphere, which will be essential in getting concentration bounds on key quantities.

Lemma 14. *If $A \subseteq \mathbb{S}^{n-1}$ is ε-dense for $\varepsilon \leq \sqrt{2}$ then $\mathbb{B}_2^n \subseteq P(A) \subseteq \left(1 - \frac{\varepsilon^2}{2}\right)^{-1} \mathbb{B}_2^n$.*

Proof. The first inclusion follows immediately from the construction of $P(A)$.

Recall that $P(A)$ is the polar of $Q(A)$ and therefore the second inclusion is equivalent to $(1 - \varepsilon^2/2)^{-1}\mathbb{B}_2^n \subseteq Q(A)$. This inclusion is equivalent to the statements that $0 \in Q(A)$ and that, for any facet of $Q(A)$, its supporting hyperplane is at distance at least $(1 - \varepsilon^2/2)$ from the origin. The first statement follows from the fact that every half-sphere $\{x \in \mathbb{S}^{n-1} : \langle x, w\rangle \geq 0\}$, $w \in \mathbb{S}^{n-1}$, contains at least one point of A because this point set is at least $\sqrt{2}$-dense. For the second statement, consider a hyperplane H supporting a facet and write it as $H = \{x \in \mathbb{R}^n : \langle x, w\rangle = h\}$ where $w \in \mathbb{S}^{n-1}$ is the outer unit normal vector of the facet and h the distance between the origin and the hyperplane. Observe that for any point $u \in \mathbb{S}^{n-1}$ with $\langle u, w\rangle \leq h$ one has

$$\|w - u\|^2 = \|w\|^2 + \|u\|^2 - 2\langle u, w\rangle \geq 1 + 1 - 2h = 2(1-h),$$

and thus

$$\left(\widehat{C}\left(w, \sqrt{2(1-h)}\right)\right) \cap A \subseteq \{x \in \mathbb{S}^{n-1} : \langle x, w\rangle > h\} \cap A = \emptyset,$$

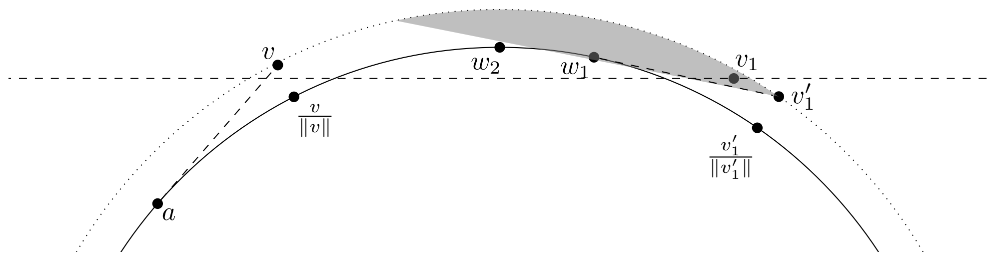

Figure 1: Illustration of the proof of Lemma 16. The inner (resp. outer dotted) curve represents part of the sphere $\mathbb{S}^{n-1}$ (resp. $(1-\varepsilon^2/2)^{-1}\mathbb{S}^{n-1}$). The horizontal dashed line represents the hyperplane $\{x \in \mathbb{R}^d : \langle x, w_2\rangle = \langle v_1, w_2\rangle\}$. The two oblique dashed line segments represent parts of the hyperplanes tangent to the unit sphere at the points a and w_1. The grey area represents the set B.

where $\widehat{C}(y,r) = \{x \in \mathbb{S}^{n-1} : \|y-x\| < r\}$ denotes the open spherical cap of radius r centered at y, $y \in \mathbb{S}^{n-1}$, $r > 0$. The equality in the last displayed equation follows from the fact that H supports a facet of $Q(A)$. Since A is ε-dense it implies $\sqrt{2(1-h)} \le \varepsilon$, equivalently $h \ge 1-\varepsilon^2/2$, which is precisely the second statement. $\square$

Lemma 15. *If $w \in \mathbb{S}^{n-1}$, $\alpha < 1$, $\|v\| \le (1-\alpha)^{-1}$ and $\langle v, w\rangle \ge 1$ then $\|v/\|v\| - w\|^2 \le 2\alpha$.*

Proof. We have $1 \le \langle v, w\rangle = \|v\| \cdot \langle v/\|v\|, w\rangle \le (1-\alpha)^{-1}\langle v/\|v\|, w\rangle$. Hence $1 - \|v/\|v\| - w\|^2/2 = \langle v/\|v\|, w\rangle \ge 1-\alpha$, which exactly implies that $\|v/\|v\| - w\|^2 \le 2\alpha$ as required. $\square$

Now we have arrived at our main technical estimate of this subsection.

Lemma 16. *Let $\varepsilon \in (0,1]$ and consider an ε-dense finite subset of the unit sphere $A \subseteq \mathbb{S}^{n-1}$. Let $w_1, w_2 \in \mathbb{S}^{n-1}$ satisfy $\|w_1 - w_2\| \le 2\varepsilon/n$. Let $v_1 \in P(A)$ satisfy $\langle w_1, v_1\rangle \ge 1$. Let $v \in P(A)$ satisfy $\langle w_2, v\rangle \ge \langle w_2, v_1\rangle$ and let $a \in \mathbb{S}^{n-1}$ satisfy $\langle a, v\rangle \ge 1$. Then we have $\|w_2 - a\| \le (2+2/n)\varepsilon$.*

Proof. First we explain that we only need to prove that there exists a vector v_1' such that the three following inequalities hold.

$$\left\|\frac{v}{\|v\|} - a\right\| \le \varepsilon, \qquad \left\|\frac{v_1'}{\|v_1'\|} - w_1\right\| \le \varepsilon, \qquad \left\|\frac{v}{\|v\|} - w_2\right\| \le \left\|\frac{v_1'}{\|v_1'\|} - w_2\right\|. \tag{3}$$

Indeed, assuming this is the case, a combination of the triangular inequality (applied twice) and the third inequality above provides

$$\begin{aligned}
\|w_2 - a\| &\le \left\|w_2 - \frac{v}{\|v\|}\right\| + \left\|\frac{v}{\|v\|} - a\right\| \\
&\le \left\|w_2 - \frac{v_1'}{\|v_1'\|}\right\| + \left\|\frac{v}{\|v\|} - a\right\| \\
&\le \|w_2 - w_1\| + \left\|w_1 - \frac{v_1'}{\|v_1'\|}\right\| + \left\|\frac{v}{\|v\|} - a\right\|,
\end{aligned}$$

and with the assumption on $\|w_2 - w_1\|$ and the first and second inequalities of (3) we get

$$\|w_2 - a\| \leq \frac{2\varepsilon}{n} + \varepsilon + \varepsilon,$$

which is the claim of the lemma.

We have $\|v_1\|, \|v\| \leq (1 - \varepsilon^2/2)^{-1}$ by Lemma 14. The first inequalty of (3) now follows from Lemma 15 with $\alpha = \varepsilon^2$, since we assumed that $\|v\| \leq (1 - \varepsilon^2/2)^{-1}$ and $\|a\| = 1$.

Before we move on to proving the two other inequalities of (3), we need to define v_1'. By definition, v_1 belongs to the set

$$B = B(w_1, \varepsilon) = \left\{ x \in \mathbb{R}^d : \langle w_1, x\rangle \geq 1,\ \|x\| \leq \left(1 - \frac{\varepsilon^2}{2}\right)^{-1} \right\}.$$

Now we set $v_1' \in B$ such that $\langle w_2, \cdot\rangle$ is minimal. Note that the minimum is achieved at the boundary of B because $\langle w_2, \cdot\rangle$ is a linear function and B is a compact set. Since w_1, w_2 are linearly independent, v_1' cannot be only tight at the constraint $\langle w_1, x\rangle \geq 1$. This implies that $\|v_1'\| = (1 - \varepsilon^2/2)^{-1}$.

From Lemma 15 we learn that any point $x \in B$ satisfies $\|x/\|x\| - w_1\| \leq \varepsilon$, and in particular this is true for v_1', making the second inequality of (3) hold. It remains to show the third inequality of (3). For this, we note that

$$\langle w_2, v\rangle \geq \langle w_2, v_1'\rangle, \qquad \qquad \|v\| \leq \left(1 - \frac{\varepsilon^2}{2}\right)^{-1} = \|v_1'\|.$$

The first inequality is a direct consequence of the assumption $\langle w_2, v\rangle \geq \langle w_2, v_1\rangle$ and the construction of v_1'. The second was proven above. Hence we have

$$\langle w_2, \frac{v}{\|v\|}\rangle \geq \langle w_2, \frac{v_1'}{\|v_1'\|}\rangle.$$

The third inequality of (3) now follows from the fact that $u \in \mathbb{S}^{n-1} \mapsto \|u - w_2\|$ is a decreasing function of $\langle u, w_2\rangle$, and thus the proof is complete. □

To round out this subsection, we derive a *local* version of Lemma 16.

Definition 17. *Given sets $A, C \subseteq \mathbb{S}^{n-1}$ and $0 < \varepsilon < 1$, we say that A is ε-dense for C if for every $c \in C$ there exists $a \in A$ such that $\|a - c\| \leq \varepsilon$.*

Lemma 18. *For $w_1, w_2 \in \mathbb{S}^{n-1}$ and $v_1, v \in \mathbb{R}^n$, suppose $\langle w_1, v_1\rangle \geq 1$ and $\langle w_2, v\rangle \geq \langle w_2, v_1\rangle$. Futhermore assume that $\|w_1 - w_2\| \leq 2\varepsilon/n$. Assume $A \subseteq \mathbb{S}^{n-1}$ is finite and ε-dense for $C(w_2, 4\varepsilon)$, and $v_1, v \in P(A)$.*

Now let $a \in \mathbb{S}^{n-1}$ satisfy $\langle a, v\rangle \geq 1$. Then we have $\|w_2 - a\| \leq (2 + 2/n)\varepsilon$.

Proof. Let $A \subseteq A' \subseteq \mathbb{S}^{n-1}$ be finite, ε-dense, and such that $A' \cap C(w_2, (2+2/n)\varepsilon) \subseteq A$. One valid choice is to take any finite ε-net $N \subseteq \mathbb{S}^{n-1}$ and set $A' = A \cup (N \setminus C(w_2, 3\varepsilon))$. Then any $x \in C(w_2, 4\varepsilon)$ has an $a \in A \subseteq A'$ with $\|a - x\| \leq \varepsilon$ and any $y \notin C(w_2, 4\varepsilon)$ has some $b \in N$ with $\|y - b\| \leq b$ and $b \notin C(w_2, 3\varepsilon)$. Moreover we have $(N \setminus C(w_2, 3\varepsilon)) \cap C(w_2, (2+2/n)\varepsilon) = \emptyset$ so this choice of A' satisfies our requirements.

If $v, v_1 \in P(A')$ then we can apply Lemma 16 to the set A' and vectors w_1, w_2, v, v_1 and a to conclude $\|w_2 - a\| \leq (2+2/n)\varepsilon$ as required.

For the remaining cases, observe that given w_1, w_2 and A, the set of pairs (v_1, v) that satisfy the conditions of Lemma 16 is a convex set and contains (w_1, w_1).

If $v_1 \notin P(A')$, let (x, y) be the convex combination of (v_1, v_1) and (w_1, w_1) such that $x = y \in P(A')$ and there exists $a' \in A' \setminus A$ such that $\langle a', x\rangle = 1$. Such a' will exist because A' is finite.

Otherwise we have $v \notin P(A')$ and let (x, y) be a convex combination of (v_1, v) and (w_1, w_1) such that $x, y \in P(A')$ and there exists $a' \in A' \setminus A$ such that $\langle a', x\rangle = 1$. Such a' will exist because A' is finite.

Either way, apply Lemma 16 to A', w_1, w_2, x, y and a' to find that $\|w_2 - a'\| \leq (2+2/n)\varepsilon$. This contradicts the earlier claim that $a' \in A' \setminus A$. From this contradiction we conclude that $v, v_1 \in P(A')$, which finishes the proof. □

Note also the contrapositive of the above statement: for w_1, w_2, v_1, v, A satisfying the conditions above, we have for $a \in \mathbb{S}^{n-1}$ that $\|w_2 - a\| > (2+2/n)\varepsilon$ implies $\langle a, v\rangle < 1$.

3.2 Locality, independence, and concentration

With an eye to Lemma 18, this subsection is concerned with proving concentration for sums of random variables that behave nicely when A is dense in given neighbourhoods. The specific random variables that we will use this for are the paths between the maximizers of $w_1, w_2 \in \mathbb{S}^{n-1}$ with $|w_1 - w_2| \leq 2\varepsilon/n$.

Definition 19. *Let $\varepsilon > 0$ be as in Lemma 7 and $A \subseteq \mathbb{R}^n$ be random. For $x, y \in \mathbb{S}^{n-1}$ define the event $E_{x,y}$ as:*

- *A is ε-dense for $C(x, \|x-y\| + 4\varepsilon)$, and*
- *for every $z \in [x, y]$ we have*

$$\left| A \cap C\left(\frac{z}{\|z\|}, (2+2/n)\varepsilon\right) \right| \leq 6e^4 \log(n^n m) 2^n$$

We call K a (x, y)-local random variable if $E_{x,y}$ implies that K is a function of $A \cap C(x, 5\varepsilon + \|x-y\|)$.

Many paths on $P(A)$ turn out to be such local random variables. One example are the shadow paths from Theorem 11.

Lemma 20. *Let $w_1, w_2 \in \mathbb{S}^{n-1}$ satisfy $\|w_1 - w_2\| \leq 2\varepsilon/n$. Then the length of the shadow path from w_1 to w_2 is a (w_1, w_2)-local random variable and E_{w_1,w_2} implies that this path has length at most $(6e^4 \log(n^n m) 2^n)^n$.*

Proof. By Lemma 18, assuming E_{w_1,w_2}, every vertex on the shadow path from w_1 to w_2 is induced by constraints in $A \cap C(w_2, (2+2/n)\varepsilon)$. Because of this, if E_{w_1,w_2} then one only needs to inspect $A \cap C(w_2, (2+2/n)\varepsilon)$ to deduce whether a point $x \in \mathbb{R}^n$ is a vertex on the shadow path. Moreover, the upper bound follows because every vertex on the shadow path is visited at most once and, assuming E_{w_1,w_2}, almost surely every vertex on the shadow path is induced by n constraints out of $A \cap C(w_2, (2+2/n)\varepsilon)$. □

Lemma 21. *Let $x_1, \dots, x_k \in \mathbb{S}^{n-1}$ and $y_1, \dots, y_k \in \mathbb{S}^{n-1}$. Then $\Pr[\bigcap_{i\in[k]} E_{x_i,y_i}] \geq 1 - 2n^{-n}m^{-2}$.*

Proof. Consider the F event that for every $z \in \mathbb{S}^{n-1}$ there exists $a \in A$ with $\|a - z\| \leq \varepsilon$ and $|C(z, (2+2/n)\varepsilon) \cap A| \leq 6e^4 \log(n^n m)2^n$. Note that F implies $E_{x,y}$ for every $x, y \in \mathbb{S}^{n-1}$. By Lemma 7 we get $\Pr[F] \geq 1 - 2n^{-n}m^{-2}$, proving the lemma. □

Lemma 22. *Let $0 < \varepsilon < 1/76n$ be as in Lemma 7 and let $k \geq 2\pi n/\varepsilon$ be the smallest number divisible by $76n$. Let $W \subseteq \mathbb{R}^n$ be a fixed 2D plane and let $w_1, \dots, w_k, w_{k+1} \in W \cap \mathbb{S}^{n-1}$ be equally spaced around the circle. Assume for every $i \in [k]$ that $K_i \geq 0$ is a (w_i, w_{i+1})-local random variable which satisfies $K_i \leq U$ when $E_{w_i,w_{i+1}}$. Then*

$$\Pr\Big[\sum_{i\in[k]} K_i \geq \mathbb{E}\big[\sum_{i\in[k]} K_i\big] + t\Big] \leq 304n^{-n+1}m^{-2}$$

for $t \geq Un\sqrt{304\varepsilon^{-1}\log(n^n m^2)}$.

Proof. We partition $[k]$ into parts. For $j \in [76n]$ define $I_j = \{i \in [k] \mid i \equiv j \mod 76n\}$.

First, observe that $w_1, \dots, w_k$ are placed on a unit circle and every $[w_i, w_{i+1}]$ is an edge of $\mathrm{conv}(w_1, \dots, w_k)$. As such we know that $\sum_{i\in[k]} \|w_i - w_{i+1}\| \leq 2\pi$. Since $k \geq 2\pi n/\varepsilon$ that gives us $\|w_i - w_{i+1}\| \leq \varepsilon/n$ for every $i \in [k]$. Next, from $\varepsilon \leq 1/76n$ we know that $k \leq 2\pi n/\varepsilon + 76n \leq 8n/\varepsilon$. Since $k \geq 4$ we have $\sum_{i\in[k]} \|w_i - w_{i+1}\| \geq 4$ and hence $\|w_i - w_{i+1}\| \geq 4/k \geq \varepsilon/2n$ for every $i \in [k]$. Last, we use that $\|w_i - w_{i+76n}\| \leq 76n \cdot \varepsilon/n \leq 1$ to deduce

$$\|w_i - w_{i+76n}\| \geq \frac{1}{\pi} \sum_{k=i}^{i+75n} \|w_k - w_{k+1}\| \geq \frac{76n}{\pi} \cdot \varepsilon/2n > 12\varepsilon.$$

This lets us conclude that if $i, i' \in I_j$ are distinct then $\|w_i - w_{i'}\| > 12\varepsilon$.

Next we write $F_j = \bigcap_{i\in I_j} E_i$ for all $j \in [76n]$. With this notation in place we can start calculating:

$$\begin{aligned}\Pr\big[\sum_{i\in[k]} K_i > \mathbb{E}[\sum_{i\in[k]} K_i] + t\big] &\leq \sum_{j\in[76n]} \Pr\big[\sum_{i\in I_j} K_i > \mathbb{E}[\sum_{i\in I_j} K_i] + t/76n\big] \\ &\leq \sum_{j\in[76n]} \left(\Pr[\neg F_j] + \Pr[\sum_{i\in I_j} K_i > \mathbb{E}[\sum_{i\in I_j} K_i] + t/76n \wedge F_j]\right).\end{aligned}$$

We know that $\Pr[\neg F_j] \leq 2n^{-n}m^{-2}$ by Lemma 21, so for the rest of the proof we can focus on the remaining summand $\Pr[\sum_{i\in I_j} K_i > \mathbb{E}[\sum_{i\in I_j} K_i] + t/76n \wedge F_j]$.

Write $1[E_i]$ for the indicator function of E_i, i.e., let $1[E_i] = 1$ if E_i and $1[E_i] = 0$ otherwise. Recall that F_j implies that $1[E_i] = 1$ for every $i \in I_j$. We immediately get by inclusion that

$$\Pr[\sum_{i\in I_j} K_i > \mathbb{E}[\sum_{i\in I_j} K_i] + t/76n \wedge F_j] \leq \Pr[\sum_{i\in I_j} K_i 1[E_i] > \mathbb{E}[\sum_{i\in I_j} K_i 1[E_i]] + t/76n].$$

Recall $\|w_i - w_{i+1}\| \leq \varepsilon/n$ and observe that $K_i 1[E_i]$ is a function of $C(w_i, (5+1/n)\varepsilon) \cap A$. From the fact that $\|w_i - w_{i'}\| > 12\varepsilon$ for every distinct $i, i' \in I_j$, we conclude that the random variables $K_i 1[E_i]$ for $i \in I_j$ are mutually independent. Moreover, $K_i 1[E_i] \leq U$ always holds. We can now apply Lemma 9:

$$\Pr\big[\sum_{i\in I_j} K_i 1[E_i] > \mathbb{E}[\sum_{i\in I_j} K_i 1[E_i]] + t/76n\big] \leq 2\exp\left(-\frac{2(t/76n)^2}{|I_j|\cdot U^2}\right).$$

We know that $|I_j| = k/76n$ and $k \leq 8n/\varepsilon$, so taking everything together we get

$$\Pr\big[\sum_{i\in[k]} K_i > \mathbb{E}[\sum_{i\in[k]} K_i] + t\big] \leq 76n \cdot \left(2n^{-n}m^{-2} + 2\exp\left(-\frac{t^2}{304\frac{n^2}{\varepsilon}\cdot U^2}\right).\right).$$

The result is obtained by filling in t. $\square$

3.3 Upper Tailbounds for the Shadow Size

To illustrate the use of the above technical results, we show in this subsection that $|\mathcal{S}(P(A), W)|$ is concentrated around its mean. By Theorem 11 we have $\mathbb{E}[|\mathcal{S}(P(A), W)|] = \Theta(n^2 m^{\frac{1}{n-1}})$.

Theorem 12 (Diameter Upper Bound)**.** *Let $t = n\sqrt{304\varepsilon^{-1}\log(n^n m^2)} \cdot \big(6e^4 \log(n^n m)2^n\big)^n$, where $\varepsilon > 0$ is as in Lemma 7. Then for $A \sim \mathrm{Pois}(\mathbb{S}^{n-1}, m)$, the shadow size satisfies*

$$\Pr[|\mathcal{S}(P(A), W)| \geq \mathbb{E}[|\mathcal{S}(P(A), W)|] + t] \leq 304n^{-n+1}m^{-2}.$$

Proof. Let $w_1, \ldots, w_k$ be as in Lemma 22 and let K_i denote the number of edges on the shadow path from w_i to w_{i+1}. By Lemma 20, each K_i is a (w_i, w_{i+1})-local random variable which satisfies $K_i \leq (6e^4 \log(n^n m)2^n)^n$ when $E_{w_i, w_{i+1}}$.

By Theorem 11 we have $\sum_{i\in[k]} K_i = |\mathcal{S}(P(A), W)|$ almost surely. We apply Lemma 22 to $\sum_{i\in[k]} K_i$:

$$\Pr\big[|\mathcal{S}(P(A), W)| - \mathbb{E}[|\mathcal{S}(P(A), W)|] > t\big] = \Pr\big[\sum_{i\in[k]} K_i - \mathbb{E}[\sum_{i\in[k]} K_i] > t\big] \leq 304n^{-n+1}m^{-2}.$$

$\square$

This theorem is most interesting when $m > 2^{\Omega(n^2)}$, since Theorem 11 and Theorem 12 then together imply that $|\mathcal{S}(P(A), W)| = O(n^2 m^{\frac{1}{n-1}})$ with probability at least $1 - 304n^{-n+1}m^{-2}$.

3.4 Upper bound on the diameter

We could upper bound the diameter using Theorem 12, but that would give a larger error term. Instead, we will first upper bound the maximum distance between any two shadow vertices. This will allow bounding the diameter with a smaller error term. For this purpose, we require the following abstract diameter bound from [Eis+10]. We will only need the Barnette–Larman style bound.

Theorem 23. *Let $G = (V, E)$ be a connected graph, where the vertices V of G are subsets of $\{1, \dots, k\}$ of cardinality n and the edges E of G are such that for each $u, v \in V$ there exists a path connecting u and v whose intermediate vertices all contain $u \cap v$.*

Then the following upper bounds on the diameter of G hold:

$$2^{n-1} \cdot k - 1 \text{ (Barnette–Larman)}, \qquad k^{1+\log n} - 1 \text{ (Kalai–Kleitman)}.$$

To confirm that the above theorem indeed gives variants of the Barnette–Larman and Kalai–Kleitman bounds, let $A = \{a_1, ..., a_m\} \subseteq \mathbb{S}^{n-1}$ be in general position. For a vertex $x \in P(A)$, we denote $A_x = \{a \in A : \langle a, x\rangle = 1\}$. Consider the following sets

$$V = \{A_x : x \text{ is a vertex of } P(A)\},$$
$$E = \{\{A_x, A_y\} : [x, y] \text{ is an edge of } P(A)\}.$$

One can check that $G = (V, E)$ satisfies almost surely the assumptions of Theorem 9 which therefore shows that the combinatorial diameter of $P(A)$ is less than $\min(2^{n-1} \cdot m - 1, m^{1+\log n} - 1)$. Up to a constant factor difference, these bounds correspond to the same bounds described in the introduction.

Now we use the Barnette–Larman style bound to bound the lenght of the local paths.

Lemma 24. *Let $w_1, w_2 \in \mathbb{S}^{n-1}$ satisfy $\|w_1 - w_2\| \leq 2\varepsilon/n$. Furthermore, let K denote the maximum over all $w \in [w_1, w_2]$ of the length of the shortest path from a maximizer $v_w \in P(A)$ of $\langle w, \cdot\rangle$ to the maximizer of $\langle w_2, \cdot\rangle$ of which every vertex $v \in P(A)$ on the path satisfies $\langle w_2, v\rangle \geq \langle w_2, v_w\rangle$. Then K is a (w_1, w_2)-local random variable and E_{w_1,w_2} implies that it is at most $6e^4 \log(n^n m)4^n$.*

Proof. Let $w \in [w_1, w_2]$ and let $v_w \in P(A)$ be a vertex maximizing $\langle w, \cdot\rangle$. By Lemma 18, assuming E_{w_1,w_2}, for every vertex $v \in P(A)$ satisfying $\langle w_2, v\rangle \geq \langle w_2, v_w\rangle$ and every $a \in A$ such that $\langle a, v\rangle \geq 1$ we have $a \in A \cap C(w_2, (2 + 2/n)\varepsilon)$.

First, this implies that if E_{w_1,w_2} and if $v \in \mathbb{R}^n$ is satisfies $\langle w_2, v\rangle \geq \langle w_2, v_w\rangle$ then we need only inspect $A \cap C(w_2, (2 + 2/n)\varepsilon)$ to decide if v is a vertex of $P(A)$. From this we conclude that if E_{w_1,w_2} then the shortest path described in the lemma statement can be computed knowing only $A \cap C(w_2, (2 + 2/n)\varepsilon)$. This implies that the path length is a (w_1, w_2)-local random variable.

Second, assuming E_{w_1,w_2} we consider the sets

$$\widehat{V} = \{v \in P(A) : v \text{ is a vertex and } \langle w_2, v\rangle \geq \langle w_2, v_1\rangle\},$$
$$\widehat{A} = \{a \in A : \text{ there exist a vertex } v \in \widehat{V} \text{ such that } \langle a, v\rangle = 1\} \subseteq A \cap C\left(w_2, \left(2 + \frac{2}{n}\right)\varepsilon\right).$$

The last inclusion follows directly from Lemma 18.

Recall the notation $A_v = \{a \in A : \langle a, v\rangle = 1\}$ for vertices $v \in P(A)$. We will apply Theorem 23 to the graph

$$V = \{A_v : v \in \widehat{V}\} \simeq \widehat{V},$$
$$E = \{\{A_{v_1}, A_{v_2}\} : v_1, v_2 \in \widehat{V},\ [v_1, v_2] \text{ is an edge of } P(A)\}.$$

We need to check that the assumptions of Theorem 23 are met. First we note that almost surely $P(A)$ is a simple polytope and thus the vertices of the graph (V, E) are subsets of A of cardinality n. Consider two vertices $A_v = \{a_{i_1}, \ldots, a_{i_n}\}, A_{v'} = \{a_{i'_1}, \ldots, a_{i'_n}\} \in V$. Observe that the set

$$F = \{x \in P(A) : \langle x, a\rangle = 1\ \forall a \in A_v \cap A_{v'}\}$$

is the minimum face of $P(A)$ containing both v and v'. We build paths $v_0 = v, v_1, \ldots, v_k$ and $v'_0 = v', v'_1, \ldots, v'_{k'}$ satisfying the following monotonicity properties

$$\langle w_2, v\rangle = \langle w_2, v_0\rangle \le \langle w_2, v_1\rangle \le \cdots \le \langle w_2, v_k\rangle = \operatorname{argmax}\{\langle w_2, x\rangle : x \in F\},$$
$$\langle w_2, v'\rangle = \langle w_2, v'_0\rangle \le \langle w_2, v'_1\rangle \le \cdots \le \langle w_2, v'_{k'}\rangle = \operatorname{argmax}\{\langle w_2, x\rangle : x \in F\}.$$

Moreover one can assume that $v_k = v'_{k'}$ by potentially completing the paths moving along the edges of $\operatorname{argmax}\{\langle w_2, x\rangle : x \in F\}$ (in the case this face contains more than one vertex). By construction all vertices v_i and v'_i belong to $\widehat{V}$. Stitching the two paths and adopting the dual point of view we found a path $A_v = A_{v_0}, \ldots, A_{v_k} = A_{v'_{k'}}, \ldots A_{v'_0} = A_{v'}$ whose vertices contain the intersection $A_v \cap A_{v'}$.

We can thus apply Theorem 23 and conclude that there is a path in the graph (V, E) from A_{v_1} to A_{v_2} of length at most $2^{n-1} \cdot |A \cap C(w_2, (2 + 2/n)\varepsilon)|$. It follows that $K \le 2^{n-1} \cdot |A \cap C(w_2, (2 + 2/n)\varepsilon)|$. □

Theorem 25. *Let $t = n\sqrt{304\varepsilon^{-1}\log(n^n m^2)} \cdot 6e^4 \log(n^n m) 4^n$, where $\varepsilon > 0$ is as in Lemma 7. For $W \subseteq \mathbb{R}^n$ a fixed 2D plane and $A \sim \mathrm{Pois}(\mathbb{S}^{n-1}, m)$, the largest distance T between any two shadow vertices satisfies*

$$\Pr[T \ge O(n^2 m^{\frac{1}{n-1}}) + t] \le 304 n^{-n+1} m^{-2}.$$

Proof. Let $w_1, \ldots, w_k$ be as in Lemma 22 and let K_i denote the maximum over all $w \in [w_i, w_{i+1}]$ of the length of the shortest path from a shadow vertex v_w maximizing $\langle w, \cdot\rangle$ to a vertex maximizing $\langle w_{i+1}, \cdot\rangle$ such that every vertex v on this path satisfies $\langle w_{i+1}, v\rangle \ge \langle w_{i+1}, v_w\rangle$.

From Lemma 24 we know that K_i is a (w_i, w_{i+1})-local random variable and $K_i \le 6e^4 \log(n^n m) 4^n$ whenever $E_{w_i, w_{i+1}}$.

Now recall Theorem 11. Observe that $T \le \sum_{i \in [k]} K_i$ almost surely by concatenating the above-mentioned paths, and note that that $\sum_{i \in [k]} K_i \le \mathcal{S}(P(A), W)$ holds almost surely, which implies $\mathbb{E}[\sum_{i \in [k]} K_i] = O(n^2 m^{\frac{1}{n-1}})$. We apply Lemma 22 to $\sum_{i \in [k]} K_i$ and get the desired result. □

Theorem 13 (Diameter Upper Bound)**.** *Let $A = \{a_1, \ldots, a_M\} \in \mathbb{S}^{n-1}$, where M is Poisson with $\mathbb{E}[M] = m$, and $a_1, \ldots, a_M$ are uniformly and independently distributed in $\mathbb{S}^{n-1}$. Then, we have that*

$$\Pr[\operatorname{diam}(P(A)) > O(n^2 m^{\frac{1}{n-1}} + n^8 16^n)] < O(1/m).$$

Proof. Let $\varepsilon > 0$ be as in Lemma 7 and let $N \subseteq \mathbb{S}^{n-1}$ be a fixed minimal ε-net. Consider the following statements:

- For every $n \in N$, any two vertices in $\mathcal{S}(P(A), \operatorname{span}(e_1, n))$ are connected by a path of length at most $O(n^2 m^{\frac{1}{n-1}}) + t$, where t is defined in Theorem 25.
- A is ε-dense.
- For any $x \in \mathbb{S}^{n-1}$ we have $|A \cap C(x, (2+2/n)\varepsilon)| \leq 6e^4 2^n \log(n^n m)$

By the union bound these statements all hold with probability at least $1 - O(m^{-1})$. We will show that the above conditions imply that $P(A)$ has combinatorial diameter at most $C_3 n^2 m^{\frac{1}{n-1}}$.

First, observe that we only need to show an upper bound for all $w \in \mathbb{S}^{n-1}$ on the length of a path connecting any vertex maximizing $\langle w, \cdot\rangle$ to a vertex maximizing $\langle e_1, \cdot\rangle$. The combinatorial diameter is at most twice that upper bound.

Let $w \in \mathbb{S}^{n-1}$ and pick $n \in N$ such that $\|w - n\| \leq \varepsilon$. By the first statement, there is a path from the vertex maximizing $\langle n, \cdot\rangle$ to the vertex maximizing $\langle e_1, \cdot\rangle$ of length $O(n^2 m^{\frac{1}{n-1}}) + t$.

By the second two statements, E_{w_1,w_2} is satisfied for every $w_1, w_2 \in \mathbb{S}^{n-1}$. Concatenating at most $O(n)$ paths together, we conclude from Lemma 24 that there is a path from any vertex maximizing $\langle w, \cdot\rangle$ to the vertex maximizing $\langle n, \cdot\rangle$ of length $O(n4^n \log(n^n m))$.

Therefore, when all three statements hold the combinatorial diameter of $P(A)$ is at most

$$O(n^2 m^{\frac{1}{n-1}}) + t + O(n4^n \log(n^n m)).$$

Now we fill in t as defined in Theorem 25 and ε as in Lemma 7, obtaining an upper bound of

$$O\left(n^2 m^{\frac{1}{n-1}} + n4^n \log(n^n m)\sqrt{\log(n^n m)^{1-\frac{1}{n-1}} m^{\frac{1}{n-1}}}\right) \leq O(n^2 m^{\frac{1}{n-1}} + n^3 4^n \log(m)^2 m^{\frac{1/2}{n-1}}).$$

This latter quantity we upper bound by $O(n^2 m^{\frac{1}{n-1}} + n^8 16^n)$. $\square$

4 Lower Bounding the Diameter of $P(A)$

To begin, we first reduce to lower bounding the diameter of the polar polytope P°, corresponding to a convex hull of m uniform points on $\mathbb{S}^{n-1}$, via the following simple lemma.

Lemma 26 (Diameter Relation)**.** *For $n \geq 2$, let $P \subseteq \mathbb{R}^n$ be a simple bounded polytope containing the origin in its interior and let $Q = P^\circ := \{x \in \mathbb{R}^n : \langle x, y\rangle \leq 1, \forall y \in P\}$ denote the polar of P. Then,* $\operatorname{diam}(P) \geq (n-1)(\operatorname{diam}(Q) - 2)$.

We then associate any "antipodal" path to a continuous curve on the sphere corresponding to objectives maximized by vertices along the path. From here, we decompose any such curve into $\Omega(m^{\frac{1}{n-1}})$ segments whose endpoints are at distance $\Theta(m^{-1/(n-1)})$ on the sphere. Finally, we apply a suitable union bound, to show that for any such curve, an $\Omega(1)$ fraction of the segments induce at least 1 edge on the corresponding path.

Theorem 27 (Lower Bound for Q(A))**.** *There exist positive constants $c_2 < 1$ and $c_3 > 1$ independent of $n \geq 3$ and m such that the following holds. Let $A = \{a_1, \ldots, a_M\} \in \mathbb{S}^{n-1}$, where M is Poisson with $\mathbb{E}[M] = m$, and $a_1, \ldots, a_M$ are uniformly and independently distributed in $\mathbb{S}^{n-1}$. Then, with probability at least $1 - e^{-c_3^{n-1} m^{1/(n-1)}}$, the combinatorial diameter of $Q(A)$ is at least $c_2 m^{1/(n-1)}$.*

4.1 Relating the diameter of $Q(A)$ and $P(A)$

Lemma 26 (Diameter Relation)**.** *For $n \geq 2$, let $P \subseteq \mathbb{R}^n$ be a simple bounded polytope containing the origin in its interior and let $Q = P^\circ := \{x \in \mathbb{R}^n : \langle x, y\rangle \leq 1, \forall y \in P\}$ denote the polar of P. Then,* $\mathrm{diam}(P) \geq (n-1)(\mathrm{diam}(Q) - 2)$.

Proof of Lemma 26. If $\mathrm{diam}(Q) \leq 1$, the statement is trivial, so we may assume that $\mathrm{diam}(Q) \geq 2$. Let $a_1, a_2 \in Q$ be vertices of Q at distance $\mathrm{diam}(Q) \geq 2$. Since P is bounded, note that 0 is in the interior of Q and hence $a_1, a_2 \neq 0$. We must show that there exists a path from a_1 to a_2 of length $L \geq 2$ such $\mathrm{diam}(P) \geq (n-1)(L-2)$.

Let $F_i := \{x \in P : \langle a_i, x\rangle = 1\}$, $i \in [2]$, the corresponding facets of P. Pick the two vertices $v_1 \in F_1$, $v_2 \in F_2$ whose distance in P is minimized. Let $v_1 := w_0, \dots, w_D := v_2$ be a shortest path from v_1 to v_2 in P. Here $w_0, \dots, w_D$ are all vertices of P, and $[w_i, w_{i+1}]$, $0 \leq i \leq D-1$, are edges of P. By definition, $D \leq \mathrm{diam}(P)$.

To complete the proof, we will extract a "long walk" from a_1 to a_2 in Q from the path $w_0, \dots, w_D$. For this purpose, let $Q_i := Q \cap \{x \in \mathbb{R}^n : \langle x, w_i\rangle = 1\}$, $0 \leq i \leq D$, denote the facet of Q induced by w_i. By our assumption that P is simple, each Q_i, $i \in [D]$, is a $n-1$-dimensional simplex, and hence there exists $S_i \subseteq \mathrm{vertices}(Q)$, $|S_i| = n$, such that $Q_i := \mathrm{conv}(a : a \in S_i)$. In particular, the combinatorial diameter of each Q_i, $0 \leq i \leq D$, is 1. That is, every distinct pair of vertices of Q_i induces an edge of Q_i, and hence an edge of Q.

By the above discussion, note that if $a_1, a_2 \in S_0$, then a_1, a_2 are adjacent in Q. Since we assume that the distance between a_1, a_2 is at least 2, we conclude that $a_1, a_2 \notin S_0$, and hence that $D \geq 1$. Furthermore, since we assume that v_1, v_2 are at minimum distance in P subject to $v_1 \in F_1, v_2 \in F_2$, we conclude that $a_1 \in S_0 \setminus \cup_{j=1}^{D} S_j$ and $a_2 \in S_L \setminus \cup_{j=0}^{D-1} S_j$, since otherwise we could shortcut the path.

We now define a walk $a_1 = u_0, \dots, u_L = a_2$, for some $L \geq 2$, from a_1 to a_2 in Q as follows. Letting $l_0 = 0$ and $S_{D+1} := \emptyset$, for $i \geq 1$ inductively define $l_i := \max\{j \geq l_{i-1} : \cap_{r=l_{i-1}}^{j} S_r \neq \emptyset\}$ and let $L = \min\{i \geq 1 : l_i = D\} + 1$. For $1 \leq i \leq L-1$, choose u_i from $\cap_{r=l_{i-1}}^{l_i} S_r$ arbitrarily. To relate the length of the walk to D, we will need the following claim.

Claim 28. *For any interval $I \subseteq \{0, \dots, D\}$, $|\cap_{i \in I} S_i| \geq n - |I| + 1$.*

Proof. First note that $|S_j \cap S_{j+1}| = n - 1 = |S_j| - 1$, $0 \leq j \leq D-1$, since P is simple and $S_j \cap S_{j+1}$ indexes the tight constraints of an edge of P. In particular, $|S_j \setminus S_{j+1}| = 1$, $0 \leq j \leq D-1$. Thus, for an interval $I = \{c, c+1, \dots, d\} \subseteq \{0, \dots, D\}$, we see that $|\cap_{i=c}^{d} S_i| \geq |\cap_{i=c}^{d-1} S_i| - |S_{d-1} \setminus S_d| = |\cap_{i=c}^{d-1} S_i| - 1 \geq |S_c| - (d-c) = n + 1 - |I|$. ☐

Applying the claim to the interval $I = \{l_{i-1}, \dots, l_i + 1\}$, $1 \leq i \leq L-1$, we see that $\cap_{r=l_{i-1}}^{l_i+1} S_r = \emptyset$ implies that either $l_i = D$ or that $|I| \geq n+1 \Leftrightarrow l_i - l_{i-1} \geq n-1$. In particular, $l_i - l_{i-1} \geq n-1$ for $0 \leq i \leq L-2$ and $l_{L-1} - l_{L-2} \geq 1$ (since $l_{L-1} = D$ and $l_{L-2} < D$).

Let us now verify that $a_1 = u_0, u_1, \dots, u_L = a_2$ induces a walk in Q. Here, we must check that $[u_i, u_{i+1}]$, $0 \leq i \leq L-1$, is an edge of Q. By construction u_i, u_{i+1} are both vertices of the simplex Q_{l_i}. Furthermore, $u_i \neq u_{i+1}$, since either $u_i = a_1 \neq u_{i+1}$ or $u_{i+1} = a_2 \neq u_i$ or $u_{i+1} \in S_{l_i+1}$ and $u_i \notin S_{l_i+1}$. Thus, $[u_i, u_{i+1}]$ is indeed an edge of Q_i and thus of Q, as explained previously. Note by our assumption that a_1 and a_2, we indeed have $2 \leq \mathrm{diam}(Q) \leq L$.

We can now compare the diameters of P and Q as follows:

$$\operatorname{diam}(P) \geq D = l_{L-1} - l_0 = \sum_{i=1}^{L-1}(l_i - l_{i-1}) \geq \sum_{i=1}^{L-2}(n-1) = (n-1)(L-2) \geq (n-1)(\operatorname{diam}(Q) - 2),$$

as needed. $\square$

4.2 Lower Bounding the Diameter of $Q(A)$

For a discrete set $N \subseteq S^{n-1}$, a point $x_0 \in N$ and a positive number $\varepsilon > 0$ we denote by

$$X_k := X_k(N, x_0, \varepsilon) = \{\mathbf{x} \in N^k : x_i \neq x_j \text{ and } 6\varepsilon \leq \|x_i - x_{i+1}\| \leq 8\varepsilon \text{ for any } 0 \leq i < j \leq k\}$$

the set of all sequences of k distinct points in N with jumps of length between 6ε and 8ε (including an extra initial jump between x_0 and x_1).

Lemma 29. *Let $\varepsilon > 0$. If $N \subseteq S^{n-1}$ is a minimal ε-net, then*

$$|X_k| \leq (17^{n-1})^k$$

Proof. For any $x \in N$ we find an upper bound for the number of points $y \in N$ such that $6\varepsilon \leq \|x - y\| \leq 8\varepsilon$. Recall that $C(x, r)$ denotes the closed spherical cap centered at x with radius $r > 0$. By the triangle inequality, the minimality of N implies that for any different points $y_1, y_2 \in N$ we have

$$\operatorname{int}(C(y_1, \varepsilon/2)) \cap C(y_2, \varepsilon/2) = \emptyset.$$

Taking a union of spherical caps centered at all points inside the annulus, we obtain a subset of the inflated annulus

$$C(x, 17\varepsilon/2) \setminus \operatorname{int}(C(x, 11\varepsilon/2)).$$

Since the caps $C(y, \varepsilon/2)$, $y \in N$, have pairwise disjoint interiors, the volume of their union is the sum of the volumes. Hence, the maximal number of points in the annulus is bounded by

$$\frac{|C(x, 17\varepsilon/2)| - |C(x, 11\varepsilon/2)|}{|C(x, \varepsilon/2)|} \leq \frac{|C(x, 17\varepsilon/2)|}{|C(x, \varepsilon/2)|}.$$

Using Lemma 2 we have

$$|\{y \in N : \ 6\varepsilon \leq \|x - y\| \leq 8\varepsilon\}| \leq \frac{(17/2)^{n-1}}{(1/2)^{n-1}} = 17^{n-1}.$$

Thus, the overall number of paths in X_k is bounded by

$$|X_k| \leq 17^{k(n-1)}.$$

$\square$

Lemma 30. *Let $f\colon [0,1] \to S^{n-1}$ be a continuous function. Let $\varepsilon > 0$ and $N \subseteq S^{n-1}$ be a minimal ε-net, such that $f(0) \in N$. There exist $k \in \mathbb{N}_0$, $0 \leq t_0 < t_1 < \cdots < t_k \leq 1$ and $x_0, \ldots, x_k \in N$ such that*

1. $\|f(t_i) - x_i\| \leq \varepsilon$ *for any* $i \in \{0, \ldots, k\}$,

2. $\|f(t) - x_i\| \geq \varepsilon$ *for any* $i \in \{0, \ldots, k\}$ *and* $t > t_i$,

3. $(x_1, \ldots, x_k) \in X_k(N, x_0, \varepsilon)$,

4. $\|x_k - f(1)\| < 7\varepsilon$.

Proof. We build the desired couple of sequences (x_i) and (t_i) by induction. We start by taking $x_0 = f(0)$ and
$$t_0 = \sup\{t \geq 0 : \|f(t) - x_0\| \leq \varepsilon\}.$$
Note that with these choices, we have a couple of (very short) sequences for which 1-3 are fulfilled.

Assume that $x_0, \ldots, x_\ell$ and $0 \leq t_0 < \ldots < t_\ell \leq 1$ are sequences for which 1-3 hold true.

If $\|x_\ell - f(1)\| < 7\varepsilon$ then we may take $k = \ell$, and we are done.

Assume otherwise, and define
$$t' = \min\{t \in [t_\ell, 1] : \exists x_{\ell+1} \in N \text{ with } \|f(t) - x_{\ell+1}\| \leq \varepsilon \text{ and } \|x_{\ell+1} - x_\ell\| \geq 6\varepsilon\},$$
Since 4 is not fulfilled, the set in non-empty (it contains 1) and t' is well defined. We take $x_{\ell+1}$ as it appears in the definition of t'. Set
$$t_{\ell+1} = \sup\{t \in [0, 1] : \|f(t) - x_{\ell+1}\| \leq \varepsilon\}.$$
By 2 for any $i \leq \ell$
$$\|f(t_{\ell+1}) - x_i\| > \varepsilon,$$
hence $x_i \neq x_{\ell+1}$. Combining this with the definition of $t_{\ell+1}$ and $x_{\ell+1}$ we only need to show that $\|x_\ell - x_{\ell+1}\| \leq 8\varepsilon$ in order to get that $0 \leq t_0 < \ldots < t_\ell < t_{\ell+1} \leq 1$ and $x_0, \ldots, x_{\ell+1}$ fulfill 1-3.

By the minimality of t', for any $s \in (t_\ell, t')$ we have $\|x_\ell - f(s)\| \leq 7\varepsilon$, otherwise there would be $x' \in N$ such that $\|x' - f(s)\| \leq \varepsilon$ but $\|x_\ell - x'\| \geq 6\varepsilon$, hence $t' \leq s$ in contradiction to the definition of s. Hence
$$\|x_\ell - x_{\ell+1}\| \leq \|x_\ell - f(s)\| + \|f(s) - f(t')\| + \|f(t') - x_{\ell+1}\| \leq 7\varepsilon + \|f(s) - f(t')\| + \varepsilon.$$

This holds for all $s \in (t_\ell, t')$. By continuity of f we may take $s \nearrow t'$ and have $\|f(s) - f(t')\| \to 0$. Thus $\|x_\ell - x_{\ell+1}\| \leq 8\varepsilon$.

Since N is finite and the points $x_0, \ldots, x_\ell$ are distinct the process must end at most after $|N|$ steps. □

Lemma 31. *Let $A \subseteq S^{n-1}$ be a finite subset of the sphere. Let $[a_0, a_1]$, $[a_1, a_2]$, $\ldots$, $[a_{\ell-1}, a_\ell]$ be a path along the edges of $Q(A)$. There exists a continuous function $f\colon [0, 1] \to S^{n-1}$ and $0 = s_0 < s_1 < \cdots < s_{\ell+1} = 1$ such that $f(0) = a_0$, $f(1) = a_\ell$, and for any $i \in \{0, 1, \ldots, \ell\}$ and any $t \in [s_i, s_{i+1}]$,*
$$a_i \in \operatorname{argmin}_{a \in A}(\|f(t) - a\|).$$

Proof. First we consider the case where the path consist of a single edge, i.e. $\ell = 1$. Consider a point $x \in S^{n-1}$ and a real $r > 0$ such that the cap $C(x, r)$ contains a_0 and a_1 on its boundary and no point of A in its interior. A possible choice is given by the circumscribed cap of any facet of

$Q(A)$ which contains $[a_0, a_1]$ as an edge. Now we set f such that it interpolates a_0, x and a_1 by two geodesic segments,

$$f(t) = \frac{\tilde{f}(t)}{\|\tilde{f}(t)\|}, \qquad \tilde{f}(t) = \begin{cases} (1-2t)a_0 + 2tx, & t \in [0, \frac{1}{2}], \\ (2-2t)x + (2t-1)a_1, & t \in [\frac{1}{2}, 1]. \end{cases}$$

By construction we get that for any $t \in [0, \frac{1}{2}]$ (resp. $t \in [\frac{1}{2}, 1]$), the cap $C(f(t), \|f(t) - a_0\|)$ (resp. $C(f(t), \|f(t) - a_1\|)$) is a subset of $C(x, r)$. Thus it contains a_0 (resp. a_1) on its boundary and no point of A in its interior. This implies that $f(0) = a_0$, $f(1) = a_1$, and

$$a_0 \in \operatorname{argmin}_{a \in A}(\|f(t) - a\|), \quad t \in [0, \frac{1}{2}],$$
$$a_1 \in \operatorname{argmin}_{a \in A}(\|f(t) - a\|), \quad t \in [\frac{1}{2}, 1].$$

This yields the proof in the case $\ell = 1$ (with $s_0 = 0 < s_1 = \frac{1}{2} < s_{1+1} = 1$). The general case follows by concatenating and renormalizing the functions corresponding to each edge. $\square$

Lemma 32. *Let $A \subseteq \mathbb{S}^{n-1}$ be a finite subset of the sphere, containing two points $a_+, a_- \in A$ such that $\|a_+ - a_-\| \geq 1$. Let $\varepsilon > 0$ and N be a minimal ε-net, such that $a_+ \in N$. Set $x_0 = a_+$ and $k_0 = \lceil 1/8\varepsilon \rceil - 1$. It holds that*

$$\operatorname{diam}(Q(A)) \geq \min_{k \geq k_0} \min_{\mathbf{x} \in X_k(N, x_0, \varepsilon)} \sum_{0 \leq i \leq k-1} \mathbf{1}(C(x_i, \varepsilon/2) \cap A \neq \emptyset) \mathbf{1}(C(x_{i+1}, \varepsilon/2) \cap A \neq \emptyset).$$

Proof. The diameter of $Q(A)$ is at least the combinatorial distance between a_+ and a_-, i.e., the minimal number of edges required to form a path between these two vertices. Note that this minimum is realized for a path without loops. Let $[a_0, a_1]$, $[a_1, a_2]$, $\ldots$, $[a_{\ell-1}, a_\ell]$ be such a path. Here we denote $a_0 = a_+ = x_0$ and $a_\ell = a_-$.

Consider a function f and a sequence $0 = s_0 < s_1 < \cdots < s_{\ell+1} = 1$ as in Lemma 31, and consider $k \in \mathbb{N}_0$, $0 \leq t_0 < t_1 < \cdots < t_k \leq 1$ and $x_0, \ldots, x_k \in N$ as in Lemma 30. We set $j(0) \leq j(1) \leq \cdots \leq j(k)$ such that $t_i \in [s_{j(i)}, s_{j(i)+1}]$. In particular, with this notation set up we have

$$\|x_i - x_{i+1}\| \geq 6\varepsilon, \qquad i \in \{0, \ldots, k-1\}, \tag{4}$$

$$\|a_{j(i)} - f(t_i)\| = \min_{a \in A} \|a - f(t_i)\|, \qquad i \in \{0, \ldots, k\}, \tag{5}$$

and

$$\|x_i - f(t_i)\| \leq \varepsilon, \qquad i \in \{0, \ldots, k\}. \tag{6}$$

From (6) we get $C(f(t_i), 3\varepsilon/2) \supset C(x_i, \varepsilon/2)$. Hence, if $C(x_i, \varepsilon/2) \cap A \neq \emptyset$, we have that $\|a_{j(i)} - f(t_i)\| \leq 3\varepsilon/2$ because of (5). Therefore if, for some $i \in \{0, \ldots, k-1\}$, both caps $C(x_i, \varepsilon/2)$ and $C(x_{i+1}, \varepsilon/2)$ contain points of A, then

$$\begin{aligned} \|a_{j(i)} - a_{j(i+1)}\| &\geq \|x_i - x_{i+1}\| - \|x_i - f(t_i)\| - \|f(t_i) - a_{j(i)}\| - \|a_{j(i+1)} - f(t_{i+1})\| - \|f(t_{i+1}) - x_{i+1}\| \\ &\geq 6\varepsilon - \varepsilon - 3\varepsilon/2 - 3\varepsilon/2 - \varepsilon = \varepsilon > 0 \end{aligned}$$

and we get $a_{j(i+1)} \neq a_{j(i)}$ which implies that $j(i) < j(i')$ for any $i' > i$. This shows that if

$$i, i' \in I = \{i : C(x_i, \varepsilon/2) \cap A \neq 0 \text{ and } C(x_{i+1}, \varepsilon/2) \cap A \neq 0\} \subseteq \{0, 1, \dots, k-1\},$$

with $i \neq i'$, then $a_{j(i)}$ and $a_{j(i')}$ are distinct vertices of the path. Therefore

$$\ell \geq |I| = \sum_{0 \leq i \leq k-1} \mathbf{1}(C(x_i, \varepsilon/2) \cap A \neq \emptyset)\mathbf{1}(C(x_{i+1}, \varepsilon/2) \cap A \neq \emptyset).$$

Also, we note that from

$$\begin{aligned}\|a_+ - a_-\| &\leq \|a_+ - x_0\| + \sum_{1 \leq i \leq k} \|x_i - x_{i-1}\| + \|x_k - a_-\| \\ &< \varepsilon + k \times 8\varepsilon + 7\varepsilon = 8(k+1)\varepsilon\end{aligned}$$

we have $k \geq k_0$, and therefore

$$(x_0, \dots, x_k) \in \cup_{k \geq k_0} X_k(N, x_0, \varepsilon).$$

□

Theorem 27 (Lower Bound for Q(A))**.** *There exist positive constants $c_2 < 1$ and $c_3 > 1$ independent of $n \geq 3$ and m such that the following holds. Let $A = \{a_1, \dots, a_M\} \in \mathbb{S}^{n-1}$, where M is Poisson with $\mathbb{E}[M] = m$, and $a_1, \dots, a_M$ are uniformly and independently distributed in $\mathbb{S}^{n-1}$. Then, with probability at least $1 - e^{-c_3^{n-1} m^{1/(n-1)}}$, the combinatorial diameter of $Q(A)$ is at least $c_2 m^{1/(n-1)}$.*

Proof. Without loss of generality $m \geq (1/c_2)^{n-1}$ since otherwise the statement of the theorem is trivial.

In this proof the constants $1 < c_3 < c_4 < c_5 < c_6 < c_2^{-1}$ are large enough constants, independent from n and m.

We set $\varepsilon = c_6 m^{-1/(n-1)}$, and want to apply Lemma 32. Let N be an ε-minimal net such that it contains a point a_+ from the set A. For independence properties needed later we take a_+ randomly and uniformly from the set A. With probability $1 - e^{-m/2}$ we have that A intersects the halfsphere $\{u \in \mathbb{S}^{n-1} : \langle a_+, u \rangle \leq 0\}$. In which case there exists a point $a_- \in A$ such that $\|a_+ - a_-\| \geq \sqrt{2} \geq 1$. Therefore we can apply Lemma 32 with $x_0 = a_+$. Combined with the union bound, we get

$$\Pr\left(\operatorname{diam} Q(A) \leq c_2 m^{1/(n-1)}\right) \leq e^{-m/2} + \sum_{k \geq k_0} \sum_{\mathbf{x} \in X_k(N, x_0, \varepsilon)} \Pr\left(\sum_{0 \leq i \leq k-1} B_i \leq c_2 m^{1/(n-1)}\right),$$

where

$$k_0 = \lceil 1/8\varepsilon \rceil + 1 \geq 1/8\varepsilon = m^{1/(n-1)}/8c_6,$$

and the summands in the probability are Bernouilli random variables

$$B_i = \mathbf{1}(C(x_i, \varepsilon/2) \cap A \neq \emptyset)\mathbf{1}(C(x_{i+1}, \varepsilon/2) \cap A \neq \emptyset).$$

For $1 \leq i \leq k-1$, they are identically distributed, with failure probability

$$\begin{aligned}\Pr(B_i = 0) &\leq 2\Pr(C(x_i,\varepsilon/2) \cap A = 0) = 2\exp\left(-m\sigma(C(x_i,\varepsilon/2))\right) \\ &\leq 2\exp\left(-m\left(\varepsilon/4\right)^{n-1}\right) = 2\exp\left(-\left(\frac{c_6}{4}\right)^{n-1}\right) =: 1-p.\end{aligned}$$

Note that we used Lemma 2 to lower bound the volume of the cap $\sigma(C(x_i,\varepsilon/2)) \geq (\varepsilon/4)^{n-1}\sigma(C(x_i,2))$. Since N forms an ε-net and the x_i are distinct, the caps $C(x_i,\varepsilon/2)$ are disjoint and therefore the random variables $B_1, B_3, B_5, \ldots$ are independent. Next we exploit this independence. Let $k \geq k_0$, and set $K = \lfloor k/2 \rfloor$. Note that $K \geq 1/16\varepsilon = m^{1/(n-1)}/16c_6$. Assuming that $c_2 \leq 1/32c_6$, we have

$$\Pr\left(\sum_{0\leq i\leq k-1} B_i \leq c_2 m^{1/(n-1)}\right) \leq \Pr\left(\sum_{1\leq i\leq K} B_{2i-1} \leq \frac{K}{2}\right) = \sum_{1\leq i\leq \lfloor K/2\rfloor} \binom{K}{i} p^i (1-p)^{K-i}.$$

Now we bound p by 1, $(1-p)^{K-i}$ by $(1-p)^{K/2}$ and $\sum\binom{K}{i}$ by 2^K, which provides us the bound

$$\Pr\left(\sum_{0\leq i\leq k-1} B_i \leq c_2 m^{-1/(n-1)}\right) \leq (2(1-p)^{1/2})^K = \left(e^{\left(-\frac{1}{2}\left(\frac{c_6}{4}\right)^{n-1}+\frac{3}{2}\ln 2\right)}\right)^K \leq \left(e^{\left(-c_5^{n-1}\right)}\right)^K.$$

Thus, with the bound $|X_k| \leq (17^{n-1})^k$ from lemma 29, and the fact that $K \geq k/2$, we get

$$\begin{aligned}\Pr\left(\operatorname{diam} Q(A) \leq c_2 m^{-1/(n-1)}\right) &\leq e^{-m/2} + \sum_{k\geq k_0}\left(e^{\left(-\frac{1}{2}(c_5)^{n-1}+(n-1)\ln 17\right)}\right)^k \\ &\leq e^{-m/2} + \sum_{k\geq k_0}\left(e^{-(c_4)^{n-1}}\right)^k \\ &= e^{-m/2} + \frac{e^{-k_0 c_4^{n-1}}}{1-e^{-(c_4)^{n-1}}} \\ &\leq e^{-m/2} + \frac{e^{-\frac{m^{1/(n-1)}}{8c_6}c_4^{n-1}}}{1-e^{-c_4^{n-1}}} \\ &\leq e^{-c_3^{n-1}m^{1/(n-1)}}.\end{aligned}$$

□

Acknowledgements. This work was done in part while the authors were participating in the Probability, Geometry and Computation in High Dimensions semester at the Simons Institute for the Theory of Computing and in the Interplay between High-Dimensional Geometry and Probability trimester at the Hausdorff Research Institute for Mathematics.

References

[1] Francisco Santos. "A counterexample to the Hirsch Conjecture". In: *Annals of Mathematics* 176.1 (July 2012), pp. 383–412. ISSN: 0003-486X. DOI: 10.4007/annals.2012.176.1.7.

[2] Victor Klee, David W Walkup, et al. "The d-step conjecture for polyhedra of dimension $d < 6$". In: *Acta Mathematica* 117 (1967), pp. 53–78.

[3] David Barnette. "Wv paths on 3-polytopes". In: *Journal of Combinatorial Theory* 7.1 (July 1969), pp. 62–70. ISSN: 0021-9800. DOI: 10.1016/s0021-9800(69)80007-4.

[4] D.G. Larman. "Paths on Polytopes". In: *Proc. London Math. Soc. (3)* s3-20.1 (Jan. 1970), pp. 161–178. ISSN: 0024-6115. DOI: 10.1112/plms/s3-20.1.161.

[5] David Barnette. "An upper bound for the diameter of a polytope". In: *Discrete Mathematics* 10.1 (1974), pp. 9–13. ISSN: 0012-365X. DOI: 10.1016/0012-365x(74)90016-8.

[6] Gil Kalai and Daniel J. Kleitman. "A quasi-polynomial bound for the diameter of graphs of polyhedra". In: *Bull. Amer. Math. Soc.* 26.2 (July 1992), pp. 315–317. ISSN: 0273-0979. DOI: 10.1090/s0273-0979-1992-00285-9.

[7] Michael J Todd. "An improved Kalai–Kleitman bound for the diameter of a polyhedron". In: *SIAM Journal on Discrete Mathematics* 28.4 (2014), pp. 1944–1947.

[8] Noriyoshi Sukegawa. "An asymptotically improved upper bound on the diameter of polyhedra". In: *Discrete & Computational Geometry* 62.3 (2019), pp. 690–699.

[9] Friedrich Eisenbrand, Nicolai Hähnle, Alexander Razborov, and Thomas Rothvoss. "Diameter of Polyhedra: Limits of Abstraction". In: *Mathematics of Operations Research* 35.4 (2010), pp. 786–794.

[10] Jean-Philippe Labbé, Thibault Manneville, and Francisco Santos. "Hirsch polytopes with exponentially long combinatorial segments". In: *Mathematical Programming* 165.2 (2017), pp. 663–688.

[11] Denis Naddef. "The Hirsch conjecture is true for (0, 1)-polytopes". In: *Mathematical Programming: Series A and B* 45.1-3 (1989), pp. 109–110.

[12] Richard C Grinold. "The Hirsch conjecture in Leontief substitution systems". In: *SIAM Journal on Applied Mathematics* 21.3 (1971), pp. 483–485.

[13] Michel L Balinski. "The Hirsch conjecture for dual transportation polyhedra". In: *Mathematics of Operations Research* 9.4 (1984), pp. 629–633.

[14] Graham Brightwell, Jan Van den Heuvel, and Leen Stougie. "A linear bound on the diameter of the transportation polytope". In: *Combinatorica* 26.2 (2006), pp. 133–139.

[15] Steffen Borgwardt, Jesús A De Loera, and Elisabeth Finhold. "The diameters of network-flow polytopes satisfy the Hirsch conjecture". In: *Mathematical Programming* 171.1 (2018), pp. 283–309.

[16] Carla Michini and Antonio Sassano. "The Hirsch Conjecture for the fractional stable set polytope". In: *Mathematical Programming* 147.1 (2014), pp. 309–330.

[17] Laura Sanità. "The diameter of the fractional matching polytope and its hardness implications". In: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2018, pp. 910–921.

[18] Martin Dyer and Alan Frieze. "Random walks, totally unimodular matrices, and a randomised dual simplex algorithm". In: *Mathematical Programming* 64.1 (1994), pp. 1–16.

[19] Nicolas Bonifas, Marco Di Summa, Friedrich Eisenbrand, Nicolai Hähnle, and Martin Niemeier. "On sub-determinants and the diameter of polyhedra". In: *Discrete & Computational Geometry* 52.1 (2014), pp. 102–115.

[20] Daniel Dadush and Nicolai Hähnle. "On the Shadow Simplex Method for Curved Polyhedra". In: *Discrete Computational Geometry* 56.4 (June 2016), pp. 882–909. DOI: 10.1007/s00454-016-9793-3.

[21] Hariharan Narayanan, Rikhav Shah, and Nikhil Srivastava. *A Spectral Approach to Polytope Diameter*. 2021. arXiv: 2101.12198 [math.CO].

[22] Peter Kleinschmidt and Shmuel Onn. "On the diameter of convex polytopes". In: *Discrete mathematics* 102.1 (1992), pp. 75–77.

[23] Alberto Del Pia and Carla Michini. "On the diameter of lattice polytopes". In: *Discrete & Computational Geometry* 55.3 (2016), pp. 681–687.

[24] Antoine Deza and Lionel Pournin. "Improved bounds on the diameter of lattice polytopes". In: *Acta Mathematica Hungarica* 154.2 (2018), pp. 457–469.

[25] Karl Heinz Borgwardt. *The simplex method: a probabilistic analysis.* Vol. 1. Algorithms and Combinatorics: Study and Research Texts. Berlin: Springer-Verlag, 1987, pp. xii+268. ISBN: 3-540-17096-0. DOI: 10.1007/978-3-642-61578-8.

[26] Karl Heinz Borgwardt. "Erratum: A Sharp Upper Bound for the Expected Number of Shadow Vertices in LP-Polyhedra under Orthogonal Projection on Two-Dimensional Planes". In: *Mathematics of Operations Research* 24.4 (1999), pp. 925–984. URL: http://www.jstor.org/stable/3690611.

[27] Daniel A Spielman and Shang-Hua Teng. "Smoothed analysis of algorithms: Why the simplex algorithm usually takes polynomial time". In: *Journal of the ACM (JACM)* 51.3 (2004), pp. 385–463.

[28] Roman Vershynin. "Beyond Hirsch conjecture: walks on random polytopes and smoothed complexity of the simplex method". In: *SIAM J. Comput.* 39.2 (2009). Preliminary version in FOCS '06, pp. 646–678. ISSN: 0097-5397. DOI: 10.1137/070683386. URL: http://dx.doi.org/10.1137/070683386.

[29] Daniel Dadush and Sophie Huiberts. "A friendly smoothed analysis of the simplex method". In: *SIAM Journal on Computing* 49.5 (2019), STOC18–449.

[30] Karl Heinz Borgwardt and Petra Huhn. "A lower bound on the average number of Pivot-steps for solving linear programs Valid for all variants of the Simplex-Algorithm". In: *Mathematical Methods of Operations Research* 49.2 (Apr. 1999), pp. 175–210. DOI: 10.1007/s186-1999-8373-5.

[31] Imre Bárány and Zoltán Füredi. "On the shape of the convex hull of random points". In: *Probability Theory and Related Fields* 77.2 (Feb. 1988), pp. 231–240. ISSN: 0178-8051, 1432-2064. DOI: 10.1007/bf00334039.

[32] Marc Glisse, Sylvain Lazard, Julien Michel, and Marc Pouget. "Silhouette of a random polytope". In: *Journal of Computational Geometry* 7.1 (2016), p. 14.

[33] Rolf Schneider and Wolfgang Weil. *Stochastic and integral geometry.* Probability and its Applications (New York). Springer-Verlag, Berlin, 2008, pp. xii+693. ISBN: 978-3-540-78858-4. DOI: 10.1007/978-3-540-78859-1. URL: https://doi.org/10.1007/978-3-540-78859-1.

[34] Andreas Brieden, Peter Gritzmann, Ravindran Kannan, Victor Klee, László Lovász, and Miklós Simonovits. "Deterministic and randomized polynomial-time approximation of radii". In: *Mathematika* 48.1-2 (2001), pp. 63–105.

[35] Clément Canonne. *A short note on Poisson tail-bounds*. Github repository link: https://github.com/ccanonne/probabilitydistributiontoolbox/blob/master/poissonconcentration.pdf. 2019.

[36] A Reznikov and EB Saff. "The covering radius of randomly distributed points on a manifold". In: *International Mathematics Research Notices* 2016.19 (2016), pp. 6065–6094.

[37] Rabindra Nath Bhattacharya and Edward C Waymire. *A basic course in probability theory*. Vol. 69. Springer, 2007.