Coverage processes on spheres and condition numbers for linear programming

Burgisser, Peter and Cucker, Felipe and Lotz, Martin

2010

MIMS EPrint: **2012.106**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

The Annals of Probability
2010, Vol. 38, No. 2, 570–604
DOI: 10.1214/09-AOP489

COVERAGE PROCESSES ON SPHERES AND CONDITION NUMBERS FOR LINEAR PROGRAMMING

By Peter Bürgisser[1], Felipe Cucker[2] and Martin Lotz

University of Paderborn, City University of Hong Kong and Oxford University

This paper has two agendas. Firstly, we exhibit new results for coverage processes. Let $p(n,m,\alpha)$ be the probability that n spherical caps of angular radius α in S^m do not cover the whole sphere S^m. We give an exact formula for $p(n,m,\alpha)$ in the case $\alpha \in [\pi/2,\pi]$ and an upper bound for $p(n,m,\alpha)$ in the case $\alpha \in [0,\pi/2]$ which tends to $p(n,m,\pi/2)$ when $\alpha \to \pi/2$. In the case $\alpha \in [0,\pi/2]$ this yields upper bounds for the expected number of spherical caps of radius α that are needed to cover S^m.

Secondly, we study the condition number $\mathscr{C}(A)$ of the linear programming feasibility problem $\exists x \in \mathbb{R}^{m+1} Ax \leq 0, x \neq 0$ where $A \in \mathbb{R}^{n\times(m+1)}$ is randomly chosen according to the standard normal distribution. We exactly determine the distribution of $\mathscr{C}(A)$ conditioned to A being feasible and provide an upper bound on the distribution function in the infeasible case. Using these results, we show that $\mathbf{E}(\ln \mathscr{C}(A)) \leq 2\ln(m+1) + 3.31$ for all $n > m$, the sharpest bound for this expectancy as of today. Both agendas are related through a result which translates between coverage and condition.

1. Introduction.

1.1. *Coverage processes on spheres.*

One of the oldest problems in the theory of coverage processes is that of calculating the chance that a given region is completely covered by a sequence of random sets. Unfortunately there is only a small number of useful circumstances where this probability may be calculated explicitly. (Hall [13], Section 1.11.)

Received April 2008; revised March 2009.
[1]Supported in part by DFG Grant BU 1371/2-1.
[2]Supported in part by CityU GRF Grant CityU 100808.
AMS 2000 subject classifications. 60D05, 52A22, 90C05.
Key words and phrases. Condition numbers, covering processes, geometric probability, integral geometry, linear programming.

In 1897 Whitworth [30] considered the following problem. Assume we place n arcs of angular radius α in the unit circle S^1, whose centers are independently and randomly chosen from the uniform distribution in S^1. What is the probability that these arcs do not cover S^1?

Whitworth's problem is arguably at the origin of the theory of coverage processes. It was not until 1939 that an answer to the problem was given when Stevens [28] showed that the probability in question is

$$\sum_{j=1}^{k}(-1)^{j+1}\binom{n}{j}\left(1-\frac{j\alpha}{\pi}\right)^{n-1}, \tag{1}$$

where $k=\lfloor\frac{\pi}{\alpha}\rfloor$. Extensions of this result to other quantities related with random arcs in S^1 are given in [25]. Extensions to random arcs with different lengths are given in [9, 16] and in [26] where an exact formula for the probability above is given for randomly placed arcs having random independent size.

The extension of the original problem in S^1 to the two-dimensional unit sphere S^2 was considered by Moran and Fazekas de St. Groth [20]. Let $p(n,\alpha)$ denote the probability that n spherical caps of angular radius α, and centers randomly and independently chosen from the uniform distribution on S^2 do not cover S^2. Moran and Fazekas de St. Groth exhibited an approximation of $p(n,\alpha)$, and numerically estimated this quantity for $\alpha=53^\circ 26'$ (a value arising in a biological problem motivating their research). Shortly thereafter, Gilbert [10] showed the bounds

$$(1-\lambda)^n \le p(n,\alpha) \le \tfrac{4}{3}n(n-1)\lambda(1-\lambda)^{n-1}, \tag{2}$$

where $\lambda=(\sin\frac{\alpha}{2})^2=\frac{1}{2}(1-\cos\alpha)$ is the fraction of the surface of the sphere covered by each cap. In addition, Gilbert conjectured that, for $n\to\infty$, $p(n,\alpha)$ satisfies the asymptotic equivalence

$$p(n,\alpha)\approx n(n-1)\lambda^2(1-\lambda^2)^{n-1}.$$

This conjecture was proven by Miles [18] who also found an explicit expression (cf. [17]) for $p(n,\alpha)$ if $\alpha\in[\pi/2,\pi]$, namely

$$\begin{aligned} p(n,\alpha) &= \binom{n}{2}\int_0^{\pi-\alpha}\sin^{2(n-2)}(\theta/2)\sin(2\theta)\,d\theta \\ &\quad+\frac{3}{4}\binom{n}{3}\int_0^{\pi-\alpha}\sin^{2(n-3)}(\theta/2)\sin^3\theta\,d\theta. \end{aligned} \tag{3}$$

More on the coverage problem for S^1 and S^2 can be found in [27]. Extensions of these results to the unit sphere S^m in $\mathbb{R}^{m+1}$ for $m>2$ are scarce. Let $p(n,m,\alpha)$ be the probability that n spherical caps of angular radius α in

S^m do not cover S^m. That is, for $\alpha \in [0,\pi]$, and $a_1,\dots,a_n$ randomly and independently chosen points in S^m from the uniform distribution, define

$$p(n,m,\alpha) := \mathsf{Prob}\left\{ S^m \neq \bigcup_{i=1}^{n} \mathsf{cap}(a_i,\alpha) \right\},$$

where $\mathsf{cap}(a,\alpha)$ denotes the spherical cap of angular radius α around a. It can easily be seen that for $n \leq m+1$ and $\alpha \leq \pi/2$ we have $p(n,m,\alpha) = 1$. Moreover, Wendel [29] has shown that

$$p(n,m,\pi/2) = 2^{1-n} \sum_{k=0}^{m} \binom{n-1}{k}. \tag{4}$$

Furthermore, a result by Janson [15] gives an asymptotic estimate of $p(n,m,\alpha)$ for $\alpha \to 0$. Actually, Janson's article covers a situation much more general than fixed radius caps on a sphere and it was preceded by a paper by Hall [12] where bounds for the coverage probability were shown for the case of random spheres on a torus.

A goal of this paper is to extend some of the known results for S^1 and S^2 to higher dimensions. To describe our results we first introduce some notation. We denote by

$$\mathcal{O}_m := \mathsf{vol}_m(S^m) = \frac{2\pi^{(m+1)/2}}{\Gamma((m+1)/2)}$$

the m-dimensional volume of the sphere S^m. Also, for $t \in [0,1]$, denote the relative volume of a cap of radius $\arccos t \in [0,\pi/2]$ in S^m by $\lambda_m(t)$. It is well known that

$$\lambda_m(t) = \frac{\mathcal{O}_{m-1}}{\mathcal{O}_m} \int_0^{\arccos t} (\sin\theta)^{m-1}\, d\theta. \tag{5}$$

Our results are formulated in terms of a family of numbers $C(m,k)$ defined for $1 \leq k \leq m$. These numbers are defined in Section 4.1 and studied in Section 5 where we give bounds on $C(m,k)$ and derive a closed form for $k \in \{1, m-1, m\}$. Furthermore, we will show that, for each m, the $C(m,k)$ can be obtained as the solution of a system of linear equations which easily allows us to produce a table for their values (cf. Table 1).

A main result in this paper is the following.

THEOREM 1.1. *Let $n > m \geq 1$, $\alpha \in [0,\pi]$, and $\varepsilon = \cos(\pi - \alpha)$. For $\alpha \in [\frac{\pi}{2}, \pi]$*

$$p(n,m,\alpha) = \sum_{k=1}^{m} \binom{n}{k+1} C(m,k) \int_{\varepsilon}^{1} t^{m-k}(1-t^2)^{km/2-1} \lambda_m^{n-k-1}(t)\, dt$$

TABLE 1
A few values for $C(m,k)$

$k \setminus m$	1	2	3	4	5	6
1	$\frac{2}{\pi}$	2	5.0930	12	27.1639	60
2		3/4	3.9317	477/32	49.5841	78795/512
3			0.6366	39/8	25.1644	897345/8192
4				15/32	4.8525	132225/4096
5					0.3183	4335/1024
6						105/512

and for $\alpha \in [0, \frac{\pi}{2})$ we have

$$p(n,m,\alpha) \leq \frac{\sum_{k=0}^{m} \binom{n-1}{k}}{2^{n-1}} + \binom{n}{m+1} C(m,m) \int_0^{|\varepsilon|} (1-t^2)^{(m^2-2)/2} (1-\lambda_m(t))^{n-m-1}\, dt.$$

We remark that this formula, for $\alpha \in [\pi/2, \pi]$ and $m = 2$, is identical to the one given by Miles (3). Also, for $\alpha \in [0, \pi/2]$ and $m = 1$, our upper bound for $p(n,1,\alpha)$ coincides with the first term in Steven's formula (1) (cf. Remark 4.9 below).

We may use Theorem 1.1, together with the bound on the $C(m,k)$, to derive bounds for the expected value of $N(m,\alpha)$, the number of random caps of radius α needed to cover S^m. The asymptotic behavior of $N(m,\alpha)$ for $\alpha \to 0$ has been studied by Janson [15]. Otherwise, we have not found any bound for $\mathbf{E}(N(m,\alpha))$ in the literature.

THEOREM 1.2. *For $\alpha \in (0, \frac{\pi}{2}]$ we have*

$$\mathbf{E}(N(m,\alpha)) \leq 3m + 2 + \sqrt{m}(m+1)\cos(\alpha)\lambda_m(\cos(\alpha))^{-2}\left(\frac{1}{2\lambda_m(\cos(\alpha))}\right)^m.$$

1.2. *Polyhedral conic systems and their condition.* Among the number of interrelated problems collectively known as linear programming, we consider the following two.

Feasibility of polyhedral conic systems (FPCS). Given a matrix $A \in \mathbb{R}^{n\times(m+1)}$, decide whether there exists a nonzero $x \in \mathbb{R}^{m+1}$ such that $Ax \leq 0$ (componentwise).

Computation of points in polyhedral cones (CPPC). Given a matrix $A \in \mathbb{R}^{n\times(m+1)}$ such that $\mathscr{S} = \{x \in \mathbb{R}^{m+1} \mid Ax < 0\} \neq \varnothing$, find $x \in \mathscr{S}$.

By scaling we may assume without loss of generality that the rows $a_1, \ldots, a_n$ of A have Euclidean norm one and interpret the matrix A as a point in $(S^m)^n$. We say that the elements of the set

$$\mathcal{F}_{n,m} := \{A \in (S^m)^n \mid \exists x \in S^m \langle a_1, x\rangle \leq 0, \ldots, \langle a_n, x\rangle \leq 0\}, \tag{6}$$

are *feasible*. Similarly, we say that the elements in

$$\mathcal{F}^\circ_{n,m} := \{A \in (S^m)^n \mid \exists x \in S^m \langle a_1, x\rangle < 0, \ldots, \langle a_n, x\rangle < 0\} \tag{7}$$

are *strictly feasible*. Elements in $(S^m)^n \setminus \mathcal{F}_{n,m}$ are called *infeasible*. Finally, we call *ill-posed* the elements in $\Sigma_{n,m} := \mathcal{F}_{n,m} \setminus \mathcal{F}^\circ_{n,m}$.

For several iterative algorithms solving the two problems above, it has been observed that the number of iterations required by an instance A increases with the quantity

$$\mathscr{C}(A) = \frac{1}{\mathsf{dist}(A, \Sigma_{n,m})},$$

(here dist is the distance with respect to an appropriate metric; for the precise definition we refer to Section 2.1). This quantity, known as the *GCC-condition number* of A [3, 11], occurs together with the dimensions n and m in the theoretical analysis (for both complexity and accuracy) of the algorithms mentioned above. For example, a primal-dual interior-point method is used in [6] to solve (FPCS) within

$$\mathcal{O}(\sqrt{m+n}(\ln(m+n) + \ln \mathscr{C}(A))) \tag{8}$$

iterations. The Agmon–Motzkin–Schönberg relaxation method[1] [1, 21] or the perceptron method [23] solve (CPPC) in a number of iterations of order $\mathcal{O}(\mathscr{C}(A)^2)$ (see Appendix B of [5] for a brief description of this).

The complexity bounds above, however, are of limited use since, unlike n and m, $\mathscr{C}(A)$ cannot be directly read from A. A way to remove $\mathscr{C}(A)$ from these bounds consists in trading worst-case by average-case analysis. To this end, one endows the space $(S^m)^n$ of matrices A with a probability measure and studies $\mathscr{C}(A)$ as a random variable with the induced distribution. In most of these works, this measure is the unform one in $(S^m)^n$ (i.e., matrices A are assumed to have its n rows independently drawn from the uniform distribution in S^m).

Once a measure has been set on the space of matrices [and in what follows we will assume the uniform measure in $(S^m)^n$], an estimate on $\mathbf{E}(\ln \mathscr{C}(A))$

[1]This method gives also the context in which $\mathscr{C}(A)$ was first studied, although in the feasible case only [11].

yields bounds on the average complexity for (FPCS) directly from (8). For (CPPC) the situation is different since it is known [5], Corollary 9.4, that $\mathbf{E}(\mathscr{C}(A)^2)=\infty$. Yet, an estimate for $\varepsilon>0$ on

$$\mathsf{Prob}\{\mathscr{C}(A)\geq 1/\varepsilon \mid A\in\mathcal{F}_{n,m}\}$$

yields bounds on the probability that the relaxation or perceptron algorithms will need more than a given number of iterations. Efforts have therefore been devoted to compute the expected value (or the distribution function) of $\mathscr{C}(A)$ for random matrices A.

Existing results for these efforts are easily summarized. A bound for $\mathbf{E}(\ln\mathscr{C}(A))$ of the form $\mathcal{O}(\min\{n, m\ln n\})$ was shown in [4]. This bound was improved [7] to $\max\{\ln m, \ln\ln n\}+\mathcal{O}(1)$ assuming that n is moderately larger than m. Still, in [5], the asymptotic behavior of both $\mathscr{C}(A)$ and $\ln\mathscr{C}(A)$ was exhaustively studied, and these results were extended in [14] to matrices $A\in(S^m)^n$ drawn from distributions more general than the uniform. Independently of this stream of results, in [8], a smoothed analysis for a related condition number is performed from which it follows that $\mathbf{E}(\ln\mathscr{C}(A))=\mathcal{O}(\ln n)$.

Our second set of results adds to the line of research above. First, we provide the exact distribution of $\mathscr{C}(A)$ conditioned to A being feasible and a bound on this distribution for the infeasible case.

THEOREM 1.3. *Let $A\in(S^m)^n$ be randomly chosen from the uniform distribution in $(S^m)^n$, $n>m$. Then, for $\varepsilon\in(0,1]$, we have*

$$\begin{aligned}
&\mathsf{Prob}\{\mathscr{C}(A)\geq 1/\varepsilon \mid A\in\mathcal{F}_{n,m}\}\\
&\quad=\frac{2^{n-1}}{\sum_{k=0}^{m}\binom{n-1}{k}}\sum_{k=1}^{m}\binom{n}{k+1}C(m,k)\\
&\qquad\qquad\times\int_0^{\varepsilon}t^{m-k}(1-t^2)^{km/2-1}\lambda_m(t)^{n-k-1}\,dt,\\
&\mathsf{Prob}\{\mathscr{C}(A)\geq 1/\varepsilon \mid A\notin\mathcal{F}_{n,m}\}\\
&\quad\leq\frac{2^{n-1}}{\sum_{k=m+1}^{n-1}\binom{n-1}{k}}\binom{n}{m+1}C(m,m)\\
&\qquad\times\int_0^{\varepsilon}(1-t^2)^{(m^2-2)/2}(1-\lambda_m(t))^{n-m-1}\,dt.
\end{aligned}$$

Second, we prove an upper bound on $\mathbf{E}(\ln\mathscr{C}(A))$ that depends only on m, in sharp contrast with all the previous bounds for this expected value.

THEOREM 1.4. *For matrices A randomly chosen from the uniform distribution in $(S^m)^n$ with $n>m$, we have $\mathbf{E}(\ln\mathscr{C}(A))\leq 2\ln(m+1)+3.31$.*

Note that the best previously established upper bound for $\mathbf{E}(\ln \mathscr{C}(A))$ (for arbitrary values of n and m) was $\mathcal{O}(\ln n)$. The bound $2\ln(m+1)+3.31$ is not only sharper (in that it is independent of n) but also more precise (in that it does not rely on the $\mathcal{O}$ notation).[2]

1.3. *Coverage processes versus condition numbers.* Theorems 1.1 and 1.3 are not unrelated. Our next result, which will be the first one we will prove, shows a precise link between coverage processes and condition for polyhedral conic systems.

PROPOSITION 1.5. *Let $a_1, \dots, a_n$ be randomly chosen from the uniform distribution in S^m. Denote by A the matrix with rows $a_1, \dots, a_n$. Then, setting $\varepsilon := |\cos(\alpha)|$ for $\alpha \in [0, \pi]$, we have*

$$p(n,m,\alpha) = \begin{cases} \mathsf{Prob}\left\{A \in \mathcal{F}_{n,m} \text{ and } \mathscr{C}(A) \le \dfrac{1}{\varepsilon}\right\}, & \text{if } \alpha \in [\pi/2, \pi], \\ \dfrac{\sum_{k=0}^{m} \binom{n-1}{k}}{2^{n-1}} & \\ \qquad + \mathsf{Prob}\left\{A \notin \mathcal{F}_{n,m} \text{ and } \mathscr{C}(A) \ge \dfrac{1}{\varepsilon}\right\}, & \text{if } \alpha \in [0, \pi/2]. \end{cases}$$

In particular, $p(n,m,\pi/2) = \mathsf{Prob}\{A \in \mathcal{F}_{n,m}\} = 2^{1-n} \sum_{k=0}^{m} \binom{n-1}{k}$.

While Proposition 1.5 provides a dictionary between the coverage problem in the sphere and the condition of polyhedral conic systems, it should be noted that, traditionally, these problems have not been dealt with together. Interest on the second focused on the case of $\mathscr{C}(A)$ being large or, equivalently, on α being close to $\pi/2$. In contrast, research on the first mostly focused on asymptotics for either small α or large n (an exception being [29]).

2. Main ideas. In this section we describe in broad strokes how the results presented in the Introduction are arrived at. In a first step in Section 2.1, we give a characterization of the GCC condition number which establishes a link to covering problems thus leading to a proof of Proposition 1.5. We then proceed by explaining the main ideas behind the proof of Theorem 1.3.

In all that follows, we will write $[n] = \{1, \dots, n\}$ for $n \in \mathbb{N}$.

[2]Recently a different derivation of a $\mathcal{O}(\ln m)$ bound for $\mathbf{E}(\ln \mathscr{C}(A))$ was given in [2]. However, this derivation does not provide explicit estimates for the constant in the $\mathcal{O}$ notation.

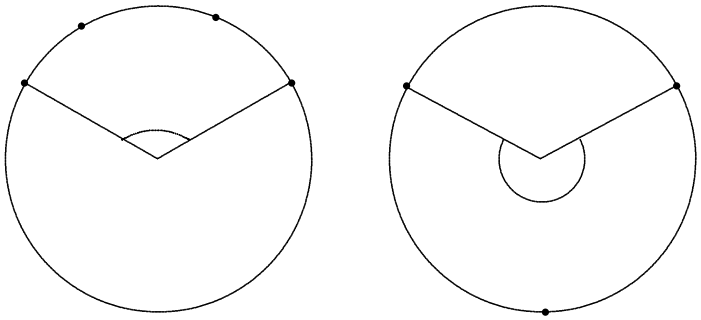

FIG. 1. *A SIC with $\alpha \in (0, \pi/2)$ (left) and with $\alpha \in (\pi/2, \pi)$ (right).*

2.1. *The GCC condition number and spherical caps.* A key ingredient in what follows is a way of characterizing the GCC condition number in terms of spherical caps. For $p \in S^m$ and $\alpha \in [0, \pi]$, recall that

$$\mathsf{cap}(p, \alpha) := \{x \in S^m \mid \langle p, x \rangle \geq \cos \alpha\}.$$

A *smallest including cap* (SIC) for $A = (a_1, \ldots, a_n) \in (S^m)^n$ is a spherical cap of minimal radius containing the points $a_1, \ldots, a_n$. If p denotes its center, then its *blocking set* is defined as $\{i \in [n] \mid \langle p, a_i \rangle = \cos \alpha\}$ which can be seen as a set of "active" rows (cf. Figure 1).

A *largest excluding cap* (LEC) for A is the complement of a smallest including cap for A. Note that (by a compactness argument) a SIC always exists, and while there may be several SIC for A, its radius is uniquely determined. For the rest of this article, we denote this radius by $\rho(A)$ and set $t(A) := \cos \rho(A)$. The following is one of many equivalent ways [3, 5] of defining the GCC condition number.

DEFINITION 2.1. The GCC condition number of $A \in (S^m)^n$ is defined as $\mathscr{C}(A) := 1/|\cos \rho(A)| \in (1, \infty]$.

In order to understand the relation of this condition number to distance to ill-posedness, we review a few known facts (for more information, see [3] and [5]). Recall the definition of $\mathcal{F}_{n,m}$ and $\mathcal{F}^\circ_{n,m}$ given in equations (6) and (7). It is easy to see that $\mathcal{F}_{n,m}$ is a compact semialgebraic set with nonempty interior $\mathcal{F}^\circ_{n,m}$. The set $\Sigma_{n,m} := \mathcal{F}_{n,m} \setminus \mathcal{F}^\circ_{n,m}$ is the topological boundary of $\mathcal{F}_{n,m}$. It consists of the feasible instances that are not strictly feasible. Note that if $n > m + 1$, then $\Sigma_{n,m}$ is also the boundary of the set of infeasible instances $\mathcal{I}_{n,m} := (S^m)^n \setminus \mathcal{F}_{n,m}$. Hence in this case $\Sigma_{n,m}$ consists of those instances that can be made both feasible and infeasible by arbitrarily small perturbations.

The next lemma summarizes results from [3], Theorem 1, and [5], Proposition 4.1. It is enough to prove Proposition 1.5.

LEMMA 2.2. *We have $\rho(A) < \pi/2$ if and only if $A \in \mathcal{F}^\circ_{n,m}$. Moreover, $\rho(A) = \pi/2$ if and only if $A \in \Sigma_{n,m}$.*

PROOF OF PROPOSITION 1.5. We claim that

$$p(n,m,\alpha) = \mathsf{Prob}\{\rho(A) \le \pi - \alpha\}. \tag{9}$$

Indeed, $\bigcup_{i=1}^n \mathsf{cap}(a_i,\alpha) \neq S^m$ iff there exists $y \in S^m$ such that $y \notin \mathsf{cap}(a_i,\alpha)$ for all i. This is equivalent to $\exists y\ \forall i\ a_i \notin \mathsf{cap}(y,\alpha)$ which means that an LEC for A has angular radius at least α. This in turn is equivalent to $\rho(A) \le \pi - \alpha$ thus proving the claim.

Equation (9) for $\alpha = \pi/2$ combined with Lemma 2.2 and Wendel's result [29] stated in equation (4) yields

$$2^{1-n} \sum_{k=0}^{m} \binom{n-1}{k} = p(n,m,\pi/2) = \mathsf{Prob}\{\rho(A) \le \pi/2\} = \mathsf{Prob}\{A \in \mathcal{F}_{n,m}\}.$$

Suppose now $\alpha \in [\pi/2, \pi]$. Then

$$\rho(A) \le \pi - \alpha \quad \iff \quad \rho(A) \le \pi/2 \quad \text{and} \quad \mathscr{C}(A) \le \frac{1}{\varepsilon},$$

showing the first assertion of Proposition 1.5. Furthermore, for $\alpha \in [0, \frac{\pi}{2}]$

$$\rho(A) \le \pi - \alpha$$

iff

$$\rho(A) \le \pi/2 \quad \text{or} \quad (\rho(A) > \pi/2 \text{ and } |\cos\rho(A)| \le |\cos(\pi - \alpha)|),$$

showing the second assertion of Proposition 1.5. □

2.2. *Toward the proof of Theorem 1.3.* To prove the feasible case in Theorem 1.3 we note that

$$\mathsf{Prob}\left\{ \mathscr{C}(A) \ge \frac{1}{\varepsilon} \;\middle|\; A \in \mathcal{F}_{n,m} \right\} = \frac{1}{\mathsf{vol}\,\mathcal{F}_{n,m}} \mathsf{vol}\,\mathcal{F}_{n,m}(\varepsilon),$$

where $\mathcal{F}_{n,m}(\varepsilon) = \{A \in \mathcal{F}^\circ_{n,m} \mid t(A) < \varepsilon\}$. But $\mathsf{vol}\,\mathcal{F}_{n,m}$ is known by Proposition 1.5. Therefore, our task is reduced to computing $\mathsf{vol}\,\mathcal{F}_{n,m}(\varepsilon)$. As we will see in Section 3.1, the smallest including cap $\mathrm{SIC}(A)$ is uniquely determined for all $A \in \mathcal{F}^\circ_{n,m}$. Furthermore, for such A, $t(A)$ depends only on the blocking set of A. Restricting to a suitable open dense subset $\mathcal{R}_{n,m}(\varepsilon) \subseteq \mathcal{F}_{n,m}(\varepsilon)$ of "regular" instances, these blocking sets are of cardinality at most $m+1$. This induces a partition

$$\mathcal{R}_{n,m}(\varepsilon) = \bigcup_I \mathcal{R}^I_{n,m}(\varepsilon),$$

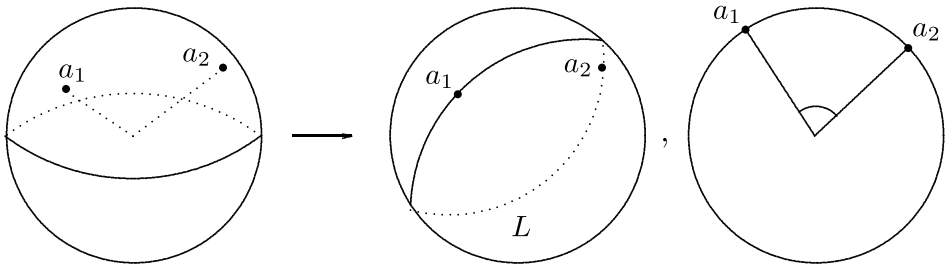

FIG. 2. *Determining* $(a_1, a_2) \in (S^2)^2$ *by first giving its span* $L \in \mathrm{G}_2(\mathbb{R}^3)$ *and then* $a_i \in S^2 \cap L$.

where the union is over all subsets $I \subseteq [n]$ of cardinality at most $m+1$, and $\mathcal{R}^I_{n,m}(\varepsilon)$ denotes the set of matrices in $\mathcal{R}_{n,m}(\varepsilon)$ with blocking set indexed by I. By symmetry, $\mathsf{vol}\,\mathcal{R}^I_{n,m}(\varepsilon)$ only depends on the cardinality of I; hence it is enough to focus on computing $\mathsf{vol}\,\mathcal{R}^{[k+1]}_{n,m}(\varepsilon)$ for $k = 1, \ldots, m$. The orthogonal invariance and the particular structure of the $\mathcal{R}^{[k+1]}_{n,m}(\varepsilon)$ (involving certain convexity conditions) makes possible a change of coordinates that allows one to split the occurring integral into an integral over t and a quantity $C(m,k)$ that depends only on m and k:

$$\mathsf{vol}\,\mathcal{R}^{[k+1]}_{n,m}(\varepsilon) = C(m,k) \int_0^\varepsilon g(t,n,m,k)\, dt.$$

More precisely, we proceed as follows:

(1) By Fubini, we split the integral over $\mathcal{R}^{[k+1]}_{n,m}(\varepsilon)$ into an integral over the first $k+1$ vectors $a_1, \ldots, a_{k+1}$ (determining the blocking set $[k+1]$) and an integral over $a_{k+2}, \ldots, a_n$ taken from $\mathrm{SIC}(A)$:

$$\begin{aligned} \mathsf{vol}\,\mathcal{R}^{[k+1]}_{n,m}(\varepsilon) &= \int_{A \in \mathcal{R}^{[k+1]}_{k+1,m}(\varepsilon)} \left(\int_{\mathsf{cap}(p(A),\rho(A))^{n-k-1}} d(S^m)^{n-k-1} \right) d\mathcal{R}^{[k+1]}_{k+1,m} \\ &= \int_{A \in \mathcal{R}^{[k+1]}_{k+1,m}(\varepsilon)} G(A)\, d\mathcal{R}^{[k+1]}_{k+1,m}. \end{aligned} \tag{10}$$

This is an integral of the function $G(A) := \mathsf{vol}(\mathsf{cap}(p(A), \rho(A)))^{n-k-1}$ which is a certain power of the volume of the spherical cap $\mathrm{SIC}(A)$.

(2) The next idea is to specify $A = (a_1, \ldots, a_{k+1})$ in $\mathcal{R}^{[k+1]}_{k+1,m}(\varepsilon)$ by first specifying the subspace L spanned by these vectors and then the position of the a_i on the sphere $S^m \cap L \cong S^k$ (cf. Figure 2).

Let $\mathrm{G}_{k+1}(\mathbb{R}^{m+1})$ denote the Grassmann manifold of $(k+1)$-dimensional subspaces in $\mathbb{R}^{m+1}$ and consider the map

$$\mathcal{R}^{[k+1]}_{k+1,m}(\varepsilon) \to \mathrm{G}_{k+1}(\mathbb{R}^{m+1}),$$

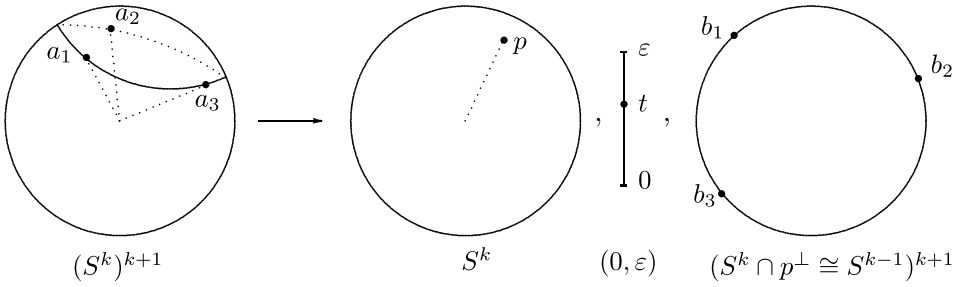

FIG. 3. *Determining* $(a_1, a_2, a_3) \in (S^2)^3$ *by specifying the direction* p*, the height* t*, and the* a_i *on the subsphere* $\{a \in S^2 \mid \langle a, p\rangle = t\}$ *by* b_i*.*

(11)
$$(a_1, \dots, a_{k+1}) \mapsto L = \mathsf{span}\{a_1, \dots, a_{k+1}\}.$$

Clearly, a vector $a \in S^m$ lies in the special subspace $L_0 := \mathbb{R}^{k+1} \times 0$ iff it lies in the subsphere S^k. Hence the fibre over L_0 consists of all "regular" tuples $A = (a_1, \dots, a_{k+1}) \in (S^k)^{k+1}$ such that $t(A) < \varepsilon$, and hence the fibre can be identified with $\mathcal{R}^{[k+1]}_{k+1,k}(\varepsilon)$. Using the orthogonal invariance and the coarea formula (also called Fubini's theorem for Riemannian manifolds) we can reduce the computation of the integral (10) to an integral over the special fibre $\mathcal{R}^{[k+1]}_{k+1,k}(\varepsilon)$. This leads to

$$\int_{\mathcal{R}^{[k+1]}_{k+1,m}(\varepsilon)} G(A)\, d\mathcal{R}^{[k+1]}_{k+1,m} = \mathsf{vol}\, \mathrm{G}_{k+1}(\mathbb{R}^{m+1}) \int_{\mathcal{R}^{[k+1]}_{k+1,k}(\varepsilon)} G(A) J(A)\, d\mathcal{R}^{[k+1]}_{k+1,k},$$

where $J(A)$ is the normal Jacobian of the transformation (11).

(3) To specify a regular $A = (a_1, \dots, a_{k+1}) \in (S^k)^{k+1}$, we first specify the direction $p = p(A) \in S^k$ and the height $t = t(A) \in (0, \varepsilon)$ and then the position of the a_i on the subsphere $\{a \in S^k \mid \langle a, p\rangle = t\} \simeq S^{k-1}$ (cf. Figure 3).

More precisely, we consider the map

(12)
$$\mathcal{R}^{[k+1]}_{k+1,k}(\varepsilon) \to S^k \times (0, \varepsilon), \qquad A \mapsto (p(A), t(A)).$$

The fibre over (p_0, t), where $p_0 = (0, \dots, 0, 1)$ is the "north pole," consists of tuples $(a_1, \dots, a_{k+1})$ lying on the "parallel" subsphere $\{a \in S^k \mid \langle a, p\rangle = t\}$. The vectors a_i can be described by points $b_i \in S^{k-1}$, which are obtained by projecting a_i orthogonally onto $\mathbb{R}^k \times 0$ and scaling the resulting vector to length one.

The orthogonal invariance and the coarea formula allow us to reduce the computation of the integral over $\mathcal{R}^{[k+1]}_{k+1,k}(\varepsilon)$ to the integration over $t \in [0, \varepsilon]$ of an integral over the special fibres over (p_0, t). The latter integral is captured by the coefficient $C(m, k)$ which can be interpreted as a higher moment of

the volume of the simplex Δ spanned by random points $b_1, \dots, b_{k+1}$ on the sphere S^{k-1}. However, we have to respect the convexity condition that the origin is contained in the simplex Δ spanned by the b_i, which complicates matters. Altogether, we are lead to a formula for $\mathsf{vol}\,\mathcal{R}_{n,m}^{[k+1]}(\varepsilon)$ of the shape,

$$\mathsf{vol}\,\mathrm{G}_{k+1}(\mathbb{R}^{m+1}) \int_{\mathcal{R}_{k+1,k}^{[k+1]}(\varepsilon)} G(A)J(A)\,d\mathcal{R}_{k+1,k}^{[k+1]}$$
$$= C(m,k) \int_0^{\varepsilon} g(t,n,m,k)\,dt,$$

where $g(t,n,m,k)$ is obtained by isolating the part of the resulting integrand that depends on t.

In order to implement this plan, we have to isolate the appropriate regularity conditions, that is, to identify the sets $\mathcal{R}_{n,m}^{I}(\varepsilon)$, and to compute the normal Jacobians of the maps (11) and (12). For the latter task, we prefer to use the language of differential forms as is common in integral geometry [24].

Unfortunately, the above argument does not carry over to the infeasible case. Nevertheless, the ideas described above are sufficient to obtain the upper bound in Theorem 1.3.

The rest of the paper proceeds as follows. In Section 3 we describe the basic facts on smallest including caps and integration on manifolds that will be needed to make formal the ideas expressed above. Then, in Section 4, we prove Theorem 1.3. Theorem 1.1 immediately follows via Proposition 1.5. Finally, in Section 5, we give bounds for all, explicit expressions for some, and a way to compute the coefficients $C(m,k)$. From these bounds we derive Theorems 1.2 and 1.4.

3. Preliminaries.

3.1. *Properties of smallest including caps.* Recall from Section 2.1 the definition of smallest including caps (SICs) for a given $A = (a_1, \dots, a_n) \in (S^m)^n$. A crucial feature of our proofs is the fact that a strictly feasible A has a uniquely determined SIC. This is a consequence of the following crucial lemma which provides an explicit criterion for a spherical cap being a smallest including cap of A. This lemma is a generalization of Lemma 4.5 in [5].

LEMMA 3.1. (a) *For a strictly feasible $A \in \mathcal{F}_{n,m}^{\circ}$ there exists exactly one smallest including cap.*

(b) *Let $(p,t) \in S^m \times (0,1]$ and $1 \le k < n$. Suppose that $\langle a_i, p\rangle = t$ for all $i \in [k+1]$ and $\langle a_i, p\rangle > t$ for all $i \in [n] \setminus [k+1]$. Then $\mathsf{cap}(p, \arccos t)$ is the smallest including cap of A if and only if*

$$tp \in \mathsf{conv}\{a_1, \dots, a_{k+1}\}.$$

PROOF. We first show that assertion (b) implies assertion (a). Suppose $\mathsf{cap}(p_1,\rho)$ and $\mathsf{cap}(p_2,\rho)$ are SICs for A, and put $t := \cos\rho$. Note that $t > 0$. Assertion (b) implies that tp_1 is contained in the convex hull of $a_1,\dots,a_n$; hence there exist $\lambda_i \geq 0$ such that $\sum_i \lambda_i = 1$ and $tp_1 = \sum_i \lambda_i a_i$. Therefore, $\langle tp_1, p_2\rangle = \sum_i \lambda_i \langle a_i, p_2\rangle \geq t$, as $\langle a_i, p_2\rangle \geq t$ for all i. This implies $\langle p_1, p_2\rangle \geq 1$ and hence $p_1 = p_2$.

The proof of assertion (b) goes along the lines of Lemma 4.5 in [5]. Suppose first that $\mathsf{cap}(p,\alpha)$ is a SIC for A where $\alpha := \arccos t$. It is sufficient to show that $p \in \mathsf{cone}\{a_1,\dots,a_{k+1}\}$. Indeed, if $p = \sum \lambda_i a_i$ with $\lambda_i \geq 0$, then $tp = \sum (t\lambda_i) a_i$. Furthermore, $\sum(t\lambda_i) = \sum \lambda_i \langle a_i, p\rangle = \langle \sum \lambda_i a_i, p\rangle = \|p\|^2 = 1$. Hence $tp \in \mathsf{conv}\{a_1,\dots,a_{k+1}\}$.

We now argue by contradiction: if p is not contained in $\mathsf{cone}\{a_1,\dots,a_{k+1}\}$, then there exists a vector $v \in S^m$ such that $\langle p, v\rangle < 0$ and $\langle a_i, v\rangle > 0$ for all $i \in \{1,\dots,k+1\}$. For $\delta > 0$ we set

$$p_\delta := \frac{p+\delta v}{\|p+\delta v\|} = \frac{p+\delta v}{\sqrt{1+2\delta\langle p,v\rangle+\delta^2}}. \tag{13}$$

Then for $1 \leq i \leq k+1$ and sufficiently small δ we have

$$\langle a_i, p_\delta\rangle = \frac{t+\delta\langle a_i, v\rangle}{\sqrt{1+2\delta\langle p,v\rangle+\delta^2}} > t,$$

where we used that $\langle a_i, p\rangle = t$, $\langle a_i, v\rangle > 0$ and $\langle p, v\rangle < 0$.

For $k+2 \leq i \leq n$ the function $\delta \to \langle a_i, p_\delta\rangle$ is continuous at $\delta = 0$. Since, by hypothesis, $\langle a_i, p\rangle = \langle a_i, p_0\rangle > t$, it follows that $\langle a_i, p_\delta\rangle > t$ for δ sufficiently small. From this we conclude that for sufficiently small δ there exists $t_\delta > t$ such that $\langle a_i, p_\delta\rangle > t_\delta$ for all $i \in [n]$. Setting $\alpha_\delta = \arccos t_\delta$ we obtain that $\alpha_\delta < \alpha$ and $a_i \in \mathsf{cap}(p_\delta, \alpha_\delta)$ for all $i \in [n]$, contradicting the assumption that $\mathsf{cap}(p,\alpha)$ is a smallest including cap.

To prove the other direction, we suppose $tp \in \mathsf{conv}\{a_1,\dots,a_{k+1}\}$. For $q \in S^m$ let $\alpha(q)$ we denote the angular radius of the smallest spherical cap with center q containing $a_1,\dots,a_n$. If we assume that $\mathsf{cap}(p,\alpha)$ is not a SIC for A, then there exists a vector $v \in S^m$ and $\delta_0 > 0$, such that $\langle v, p\rangle = 0$ and, for all $0 < \delta \leq \delta_0$, $\alpha(p_\delta) < \alpha(p)$ where $p_\delta = \frac{p+\delta v}{\sqrt{1+\delta^2}}$ (i.e., we have a direction v along which we can move to obtain a smaller cap). This means that

$$\min_{1\leq i\leq n} \langle a_i, p_\delta\rangle > \min_{1\leq i\leq n} \langle a_i, p\rangle = t.$$

Therefore, for all $i \in [k+1]$ we have

$$\langle a_i, p_\delta\rangle = \frac{\langle a_i, p\rangle + \delta\langle a_i, v\rangle}{\sqrt{1+\delta^2}} > t = \langle a_i, p\rangle$$

for sufficiently small δ which implies that $\langle a_i, v\rangle > 0$. Let $\mu \in \mathbb{R}^{k+1}_{\geq 0}$ be such that $tp = \sum_{1\leq i\leq k+1} \mu_i a_i$ and $\sum_{1\leq i\leq k+1} \mu_i = 1$. Then we have

$$t\langle p, v\rangle = \sum_{1\leq i\leq k+1} \mu_i \langle a_i, v\rangle > 0,$$

contradicting the assumption that $\langle p, v\rangle = 0$. Thus $\mathsf{cap}(p, \alpha)$ is indeed a smallest including cap. □

For a strictly feasible A, we denote the center of its uniquely determined SIC by $p(A)$ and its radius by $\rho(A)$. The blocking set $\mathrm{BS}(A)$ of A is defined as the blocking set of the SIC of A. It is not hard to see that $\mathrm{BS}(A)$ can have any cardinality greater than one.

However, we note that in the infeasible case, there may be more than one smallest including cap. Consider for instance three equilateral points on the circle (right-hand side in Figure 1). It is known [5], Proposition 4.2, that in this case, the blocking set of a SIC has at least $m+1$ elements. In the infeasible case, one direction of the characterization of smallest including caps of Lemma 3.1 still holds. The proof is similar as for Lemma 3.1.

LEMMA 3.2. *Let* $\mathsf{cap}(p, \arccos t)$ *be a* SIC *for* $A \in (S^m)^n$ *with* $p \in S^m$ *and* $t \in (-1, 0)$. *Suppose* $\langle a_i, p\rangle = t$ *for* $i \in [m+1]$ *and* $\langle a_i, p\rangle > t$ *for* $i = m+2, \ldots, n$. *Then* $tp \in \mathsf{conv}\{a_1, \ldots, a_{m+1}\}$.

PROOF. Suppose $tp \notin \mathsf{conv}\{a_1, \ldots, a_{m+1}\}$. Then $-p \notin \mathsf{cone}\{a_1, \ldots, a_{m+1}\}$ and hence there exists a vector $v \in S^m$ such that $\langle -p, v\rangle < 0$ and $\langle a_i, v\rangle > 0$ for all i. For $\delta > 0$ we define p_δ as in (13). Take δ sufficiently small so that $t < t + \delta\langle a_i, v\rangle < 0$ for all $i \in [m+1]$. Then, for $i \in [m+1]$ and δ sufficiently small, we have

$$\langle a_i, p_\delta\rangle = \frac{t + \delta\langle a_i, v\rangle}{\sqrt{1 + 2\delta\langle p, v\rangle + \delta^2}} > t,$$

where we used that $\langle a_i, p\rangle = t$, $\langle a_i, v\rangle > 0$, and $\langle p, v\rangle > 0$. This shows that $\mathsf{cap}(p, \arccos t)$ is not a smallest including cap. □

We present a few more auxiliary results that are needed for the proof of our main result.

LEMMA 3.3. *For given linearly independent* $a_1, \ldots, a_{k+1} \in S^m$, $1 \leq k \leq m$, *there exist unique* $p \in S^m$ *and* $t \in (0, 1)$ *such that*

$$p \in \mathsf{span}\{a_1, \ldots, a_{k+1}\}$$

and

$$\langle a_i, p\rangle = t \qquad \text{for all } i \in [k+1].$$

Moreover, the map $(a_1, \ldots, a_{k+1}) \mapsto (p, t)$ *is differentiable.*

PROOF. Let $\mathcal{A}$ denote the affine span of $a_1, \dots, a_{k+1}$, L the underlying linear space and $\mathcal{L}$ the linear span of $\mathcal{A}$. Since the a_i are linearly independent, we have $\mathcal{A} \neq L$ and thus $\dim \mathcal{A} = \dim L = k$, $\dim \mathcal{L} = k+1$. Hence the intersection of $\mathcal{L}$ with the orthogonal complement $L^\perp$ is one-dimensional and contains exactly two elements of length one. Take the one such that the common value $t = \langle a_i, p\rangle$ is positive. This shows existence and at the same time the uniqueness of p, t.

Suppose now $k = m$, and let A denote the square matrix with the rows $a_1, \dots, a_{m+1}$. The conditions $\langle a_i, p\rangle = t$ can be written in matrix form as $Ap = te$ where $e := (1, \dots, 1)^\top$. By solving this equation we obtain the following explicit formulas:

$$p(A) = \frac{1}{\|A^{-1}e\|} A^{-1}e, \qquad t(A) = \frac{1}{\|A^{-1}e\|}. \tag{14}$$

This shows the differentiability of the map $A \mapsto (p, t)$ in the case $k = m$. We leave the proof in the general case to the reader. □

The next result, though very elementary, will be useful for clarification.

Let $p \in S^k$ and $t \neq 0$ and consider elements $a_1, \dots, a_{k+1} \in S^k$ satisfying $\langle a_i, p\rangle = t$ for all i. Let $b_i \in S^{k-1}$ be the scaled-to-one orthogonal projection of a_i onto the orthogonal complement of $\mathbb{R}p$. That is, $a_i = rb_i + tp$ where $r = (1 - t^2)^{1/2}$.

LEMMA 3.4. *The following conditions are equivalent:*

1. *The affine hull $\mathcal{A}$ of $a_1, \dots, a_{k+1}$ has dimension k.*
2. *The span of $b_1, \dots, b_{k+1}$ has dimension k.*
3. *$a_1, \dots, a_{k+1}$ are linearly independent.*

PROOF. The equivalence of the first two conditions is obvious. The equivalence of the first and third condition follows from $\dim \mathsf{span}(\mathcal{A}) = \dim \mathcal{A} + 1$ (here we use $t \neq 0$). □

3.2. *Volume forms on Grassmann manifolds.* Integration on Grassmann manifolds will play a crucial role in our proofs. We recall some facts about the relevant techniques from integral geometry and refer to Santaló's book [24], II.9–12, and the article [19] for more information. We recall that volume elements are always unsigned forms.

Let M be a Riemannian manifold of dimension m, $p \in M$, and let $y = (y_1, \dots, y_m)^\top : U \mapsto \mathbb{R}^m$ be local coordinates in a neighborhood U of p such that $\partial/\partial y_1, \dots, \partial/\partial y_m$ are an orthonormal basis of T_pM. The natural volume form on M at p associated to its Riemannian metric is then given by $dM = dy_1 \wedge \cdots \wedge dy_m$ where dy_i is the differential of the coordinate function y_i at p.

In the case of a sphere, we get such local coordinates around a point $p \in S^m$ by projecting onto the orthogonal complement of p. More precisely, let $\langle e_1, \dots, e_{m+1}\rangle$ be an orthonormal basis of $\mathbb{R}^{m+1}$ satisfying $e_1 = p$ (so that $e_2, \dots, e_{m+1}$ span the tangent space T_pS^m). For a point $x = (x_1, \dots, x_{m+1})^\top \in S^m$ in a neighbourhood of p set $y_i = \langle x, e_i\rangle$. Then $(y_2, \dots, y_{m+1})$ are local coordinates of S^m around p such that $\partial/\partial y_i$ are pairwise orthogonal at p. Hence the volume element of S^m at p is given by

$$dS^m = \omega_2 \wedge \cdots \wedge \omega_{m+1},$$

where $\omega_i := dy_i = \langle dx, e_i\rangle$ and $dx = (dx_1, \dots, dx_{m+1})^\top$. Hence, if we denote by E the $(m+1) \times (m+1)$-matrix having the e_i as rows, we obtain the volume form by wedging the nonzero entries of $E\,dx$.

In a similar fashion we define volume forms on Stiefel manifolds (for details and further justification we refer to [24]). A *k-frame* is a set of k linearly independent vectors. For $1 \le k \le m+1$, the *Stiefel manifold* $V_k(\mathbb{R}^{m+1})$ is defined as the set of orthonormal k-frames in $\mathbb{R}^{m+1}$. It is a compact Riemannian submanifold of $(S^m)^k$. Let $Q = (q_1, \dots, q_k) \in V_k(\mathbb{R}^{m+1})$ and $\langle e_1, \dots, e_{m+1}\rangle$ an orthonormal basis of $\mathbb{R}^{m+1}$ such that $e_1 = q_1, \dots, e_k = q_k$. Then the volume element of $V_k(\mathbb{R}^{m+1})$ at Q is given by

$$dV_k(\mathbb{R}^{m+1}) = \bigwedge_{1 \le i \le k} (\omega_{i,i+1} \wedge \cdots \wedge \omega_{i,m+1}),$$

where $\omega_{i,j} = \langle dq_i, e_j\rangle$ for $1 \le i \le k$ and $1 \le j \le m+1$. [In terms of the $(m+1) \times k$ matrix $E\,dQ$, this corresponds to wedging the entries below the main diagonal.] With this volume element we have $\mathsf{vol}\, V_k(\mathbb{R}^{m+1}) = \mathcal{O}_m \cdots \mathcal{O}_{m+1-k}$.

We denote by $\mathrm{G}_k(\mathbb{R}^{m+1})$ the *Grassmann manifold* of k-dimensional subspaces of $\mathbb{R}^{m+1}$. One way of characterizing it is as a quotient of a Stiefel manifold, by identifying frames that span the same subspace. Let $L \in \mathrm{G}_k(\mathbb{R}^{m+1})$ and choose a frame $Q \in V_k(\mathbb{R}^{m+1})$ spanning L. If $V_k(L)$ denotes the Stiefel manifold of orthonormal k-frames in L and $dV_k(L)$ its volume element at Q, then it is known that the volume element $d\mathrm{G}_k(\mathbb{R}^{m+1})$ of the Grassmann manifold at L satisfies (see [19], equation (10))

$$dV_k(\mathbb{R}^{m+1}) = d\mathrm{G}_k(\mathbb{R}^{m+1}) \wedge dV_k(L). \tag{15}$$

From this equality it follows that

$$d\mathrm{G}_k(\mathbb{R}^{m+1}) = \bigwedge_{1 \le i \le k} (\omega_{i,k+1} \wedge \cdots \wedge \omega_{i,m+1})$$

with the $\omega_{i,j}$ as defined in the case of the Stiefel manifold. (In terms of the matrix $E dQ$, this corresponds to wedging the elements in the lower $(m+1-k) \times k$ rectangle.) As a consequence of (15), the volume of the Grassmannian is given by

$$\mathcal{G}_{k,m+1} := \mathsf{vol}\, \mathrm{G}_k(\mathbb{R}^{m+1}) = \frac{\mathcal{O}_{m+1-k} \cdots \mathcal{O}_m}{\mathcal{O}_0 \cdots \mathcal{O}_{k-1}}.$$

Equation (15) has a generalization to frames that are not orthogonal, that is, to points in a product of spheres $(S^m)^k$. Let $L \in \mathrm{G}_k(\mathbb{R}^{m+1})$ and set $S(L) := L \cap S^m$, so that $S(L) \cong S^{k-1}$. Choose a basis $a_1, \dots, a_k$ of L consisting of unit length vectors, that is, a point $A = (a_1, \dots, a_k)$ in $S(L)^k$. We denote by $\mathsf{vol}(A)$ the volume of the parallelepiped spanned by the a_i. Then the volume form of $(S^m)^k$ at A can be expressed as

$$d(S^m)^k = \mathsf{vol}(A)^{m-k+1}\, d\mathrm{G}_k(\mathbb{R}^{m+1}) \wedge dS(L)^k. \tag{16}$$

This equation can be derived as in [19] (see also [24], II.12.3). It also follows as a special case of a general formula of Blaschke–Petkantschin-type derived by Zähle [31] (see also the discussion in [22]).

A beautiful application of equation (16) is that it allows an easy computation of the moments of the absolute values of random determinants. The following lemma is an immediate consequence of (16) (see also [19]).

LEMMA 3.5. *Let $B \in (S^k)^{k+1}$ be a matrix with rows $b_1, \dots, b_k$ independently and uniformly distributed in S^k. Then*

$$\mathbf{E}(|\det(B)|^{m-k+1}) = \left(\frac{\mathcal{O}_m}{\mathcal{O}_{k-1}}\right)^k \frac{1}{\mathcal{G}_{k,m+1}}.$$

4. The probability distribution of $\mathscr{C}(A)$. This section is devoted to the proof of Theorem 1.3.

4.1. *The feasible case.* Recall that, for $A \in \mathcal{F}^\circ_{n,m}$, we denote the center and the angular radius of the unique smallest including cap of A by $p(A)$ and $\rho(A)$, respectively, and we write $t(A) = \cos\rho(A)$.

Our goal here is to prove the first part of Theorem 1.3, for which, as we noted in Section 2.2, we just need to compute the volume of the following sets:

$$\mathcal{F}_{n,m}(\varepsilon) := \{A \in \mathcal{F}^\circ_{n,m} \mid t(A) < \varepsilon\}.$$

For this purpose it will be convenient to decompose $\mathcal{F}_{n,m}(\varepsilon)$ according to the size of the blocking sets. Recall that the *blocking set* of $A \in \mathcal{F}^\circ_{n,m}$ is defined as

$$\mathrm{BS}(A) = \{i \in [n] \mid \langle p(A), a_i\rangle = t(A)\}. \tag{17}$$

For $I \subseteq [n]$ with $|I| \le n$ and $\varepsilon \in (0,1]$ we define $\mathcal{F}^I_{n,m}(\varepsilon)$ to be the set of all $A \in \mathcal{F}_{n,m}(\varepsilon)$ such that $\mathrm{BS}(A) = I$.

For technical reasons we have to require some regularity conditions for the elements of $\mathcal{F}^I_{n,m}(\varepsilon)$.

DEFINITION 4.1. We call a family $(a_1, \dots, a_{k+1})$ of elements of a vector space *centered with respect to a vector* c in the affine hull $\mathcal{A}$ of the a_i if $\dim \mathcal{A} = k$, and c lies in the relative interior of the convex hull of the a_i. We call the family *centered* if it is centered with respect to the origin. We now define, for $I \subseteq [n]$,

$$\mathcal{R}^I_{n,m}(\varepsilon) := \{A \in \mathcal{F}^I_{n,m}(\varepsilon) \mid (a_i)_{i\in I} \text{ is centered with respect to } t(A)p(A)\}.$$

Note that, by definition, the a_i are affinely independent if $|I| \le m+1$.

LEMMA 4.2. 1. *$\mathcal{F}^I_{n,m}(\varepsilon)$ is of measure zero if $|I| > m+1$.*
2. *If $|I| \le m+1$, then $\mathcal{R}^I_{n,m}(\varepsilon)$ is open in $(S^m)^n$, and $\mathcal{F}^I_{n,m}(\varepsilon)$ is contained in the closure of $\mathcal{R}^I_{n,m}(\varepsilon)$.*
3. *$\mathcal{F}^I_{n,m}(\varepsilon) \setminus \mathcal{R}^I_{n,m}(\varepsilon)$ has measure zero.*

PROOF. 1. If $A \in \mathcal{F}^I_{n,m}(\varepsilon)$, then $\{a_i \mid i \in I\}$ is contained in the boundary of the SIC of A, and hence its affine hull has dimension at most m. On the other hand, the affine hull of $(a_i)_{i\in I}$ is almost surely $\mathbb{R}^{m+1}$ if $|I| > m+1$.

2. The fact that $\mathcal{R}^I_{n,m}(\varepsilon)$ is open in $(S^m)^n$ easily follows from the continuity of the map $A \mapsto (p(A), t(A))$ established in Lemma 3.3.

Suppose now $A \in \mathcal{F}^I_{n,m}(\varepsilon)$. By Lemma 3.1 we have $t(A)p(A) \in \mathsf{conv}\{a_i \mid i \in I\}$ for $A \in \mathcal{F}^I_{n,m}(\varepsilon)$. It is now easy to see that there are elements A' arbitrarily close to A such that A' is centered with respect to $t(A')p(A')$. This shows the second assertion.

3. By part two we have $\mathcal{R}^I_{n,m}(\varepsilon) \subseteq \mathcal{F}^I_{n,m}(\varepsilon) \subseteq \overline{\mathcal{R}^I_{n,m}(\varepsilon)}$. Since we are dealing with semialgebraic sets, the boundary of $\mathcal{R}^I_{n,m}(\varepsilon)$ is of measure zero. □

It is clear that the $\mathcal{F}^I_{n,m}$ with I of the same cardinality just differ by a permutation of the vectors. Using Lemma 4.2 we obtain

$$\mathsf{vol}\, \mathcal{F}_{n,m}(\varepsilon) = \sum_{|I|\le m+1} \mathsf{vol}\, \mathcal{F}^I_{n,m}(\varepsilon) = \sum_{k=1}^{m} \binom{n}{k+1} \mathsf{vol}\, \mathcal{R}^k_{n,m}(\varepsilon), \tag{18}$$

where we have put $\mathcal{R}^k_{n,m}(\varepsilon) := \mathcal{R}^{[k+1]}_{n,m}(\varepsilon)$ to ease notation.

Hence it is sufficient to compute the volume of $\mathcal{R}^k_{n,m}(\varepsilon)$. For this purpose we introduce now the coefficients $C(m,k)$.

DEFINITION 4.3. We define for $1 \le k \le m$

$$C(m,k) = \frac{(k!)^{m-k+1}}{\mathcal{O}^k_m} \mathcal{G}_{k,m} \int_{M_k} (\mathsf{vol}_k \Delta)^{m-k+1}\, d(S^{k-1})^{k+1},$$

where M_k is the following open subset of S^{k-1}:

$$M_k := \{(b_1, \dots, b_{k+1}) \in (S^{k-1})^{k+1} \mid (b_1, \dots, b_{k+1}) \text{ is centered}\}$$

and $\Delta : M_k \to \mathbb{R}$ maps $B = (b_1, \dots, b_{k+1})$ to the convex hull of the b_i.

EXAMPLE 4.4. We compute $C(m,1)$. Note that $M_{1,1} = \{(-1,1),(1,-1)\}$ and $\mathcal{G}_{1,m} = \frac{1}{2}\mathcal{O}_{m-1}$. Hence

$$C(m,1) = \frac{1}{\mathcal{O}_m}\frac{1}{2}\mathcal{O}_{m-1}\int_{M_{1,1}} (\mathsf{vol}_1 \Delta)^m \, dM_{1,1} = \frac{\mathcal{O}_{m-1}}{\mathcal{O}_m} 2^m.$$

The assertion in Theorem 1.3 about the feasible case follows immediately from Proposition 1.5, equation (18) and the following result.

PROPOSITION 4.5. *Let $\varepsilon \in (0,1]$. The relative volume of $\mathcal{F}^k_{n,m}(\varepsilon)$ is given by*

$$\frac{\mathsf{vol}\,\mathcal{R}^k_{n,m}(\varepsilon)}{\mathcal{O}^n_m} = C(m,k)\int_0^\varepsilon t^{m-k}(1-t^2)^{km/2-1}\lambda_m(t)^{n-k-1}\,dt.$$

PROOF. Consider the projection

$$\mathcal{R}^k_{n,m}(\varepsilon) \to \mathcal{R}^k_{k+1,m}(\varepsilon), \qquad (a_1, \dots, a_n) \mapsto A = (a_1, \dots, a_{k+1}).$$

By Lemma 3.1, this map is surjective and its fiber over A consists of all $(A, a_{k+2}, \dots, a_n)$ such that a_i lies in the interior of the cap $\mathsf{cap}(p(A), \rho(A))$ for all $i > k+1$. By Fubini, and using (5), we conclude that

$$\frac{\mathsf{vol}\,\mathcal{R}^k_{n,m}(\varepsilon)}{\mathcal{O}^{n-k-1}_m} = \int_{A \in \mathcal{R}^k_{k+1,m}(\varepsilon)} \lambda_m(t(A))^{n-k-1}\, d(S^m)^{k+1}. \tag{19}$$

We consider now the following map (which is well defined [cf. Lemma 3.4]):

$$\mathcal{R}^k_{k+1,m}(\varepsilon) \to \mathrm{G}_{k+1}(\mathbb{R}^{m+1}), \qquad (a_1, \dots, a_{k+1}) \mapsto L = \mathsf{span}\{a_1, \dots, a_{k+1}\}.$$

We can thus integrate over $\mathcal{R}^k_{k+1,m}(\varepsilon)$ by first integrating over $L \in \mathrm{G}_{k+1}(\mathbb{R}^{m+1})$ and then over the fiber of L. By equation (16), the volume form of $(S^m)^{k+1}$ at A can be written as

$$d(S^m)^{k+1} = \mathsf{vol}(A)^{m-k}\, d\mathrm{G}_{k+1}(\mathbb{R}^{m+1})(L) \wedge dS(L)^{k+1},$$

where $S(L)^{k+1}$ denotes $(k+1)$-fold product of the unit sphere of L. By invariance under orthogonal transformations, the integral over the fiber does not depend on L. We may therefore assume that $L = \mathbb{R}^{k+1}$, in which case

the fiber over L can be identified with $\mathcal{R}^k_{k+1,k}(\varepsilon)$. Thus we conclude from equation (19) that

$$\frac{\operatorname{vol}\mathcal{R}^k_{n,m}(\varepsilon)}{\mathcal{O}_m^{n-k-1}} = \mathcal{G}_{k+1,m+1}\int_{A\in\mathcal{R}^k_{k+1,k}(\varepsilon)} \operatorname{vol}(A)^{m-k}\lambda_m(t(A))^{n-k-1}\,d(S^k)^{k+1}. \tag{20}$$

In a next step, we will perform a change of variables in order to express the integral on the right-hand side of equation (20) as an integral over t involving the coefficients $C(m,k)$.

Note that by Lemma 3.3, $p(A)\in S^k$ and $t(A)\in(0,1)$ are defined for any $A\in \mathrm{GL}(k+1,\mathbb{R})$ and depend smoothly on A. A moment's thought (together with Lemmas 3.1 and 3.4) shows that we have the following complete characterization of $\mathcal{R}^k_{k+1,k}(\varepsilon)$:

$$\begin{aligned}\mathcal{R}^k_{k+1,k}(\varepsilon) = \{A\in(S^k)^{k+1} \mid A \text{ is centered with respect to } t(A)p(A),\\ 0<t(A)<\varepsilon, \forall i\ \langle a_i, p(A)\rangle = t(A)\}.\end{aligned}$$

For $A\in\mathcal{R}^k_{k+1,k}(\varepsilon)$ set $p:=p(A)$, $t:=t(A)$, and $r:=r(t):=(1-t^2)^{1/2}$. For $i\in[k+1]$ we define b_i as the scaled-to-one orthogonal projection of a_i onto the orthogonal complement of $\mathbb{R}p$, briefly $a_i = rb_i + tp$. The matrix $B=B(A)$ with the rows $b_1,\dots,b_{k+1}$ can be written as $B=\frac{1}{r}(A-tep^\top)$. Clearly, B is centered.

We define now

$$W_k = \{(B,p)\in(S^k)^{k+1}\times S^k \mid Bp=0 \text{ and } B \text{ is centered}\}.$$

This is a Riemannian submanifold of $(S^k)^{k+2}$ of dimension $k(k+1)-1$. We thus have a map,

$$\varphi_k : \mathcal{R}^k_{k+1,k}(\varepsilon)\to W_k\times(0,\varepsilon), \qquad A\mapsto (B(a),p(A),t(A)).$$

The inverse of this map is given by $(B,p,t)\mapsto A = rB+tep^\top$. It is well defined since, by Lemma 3.4, A is invertible when B is centered. The Jacobian $J(A)$ of the diffeomorphism φ_k is stated in the next lemma, whose proof will be momentarily postponed. We remark that this lemma can also be derived from [22], Lemma 1 (a special case of Zähle's theorem [31]) with K being the unit ball.

LEMMA 4.6. *The volume form of $(S^k)^{k+1}$ at A can be expressed in terms of the volume form of $W_k\times(0,\varepsilon)$ as follows:*

$$d(S^k)^{k+1} = J(A)\,dW_k\wedge dt = \frac{r^{(k-2)(k+1)}\operatorname{vol}(A)}{t}\,dW_k\wedge dt.$$

We now express the Jacobian $J(A)$ in terms of (B,p,t). The volume $\mathsf{vol}(A)$ of the parallelepiped spanned by the a_i equals $(k+1)!$ times the volume of the pyramid with apex 0 and base $\Delta(a_1,\dots,a_{k+1})$, the latter denoting the simplex with vertices $a_1,\dots,a_{k+1}$. Moreover, this pyramid has height t and it is well known that the volume of a $(k+1)$-dimensional pyramid with height t and base B is $\frac{t}{k+1}$ times the (k-dimensional) volume of B. This implies

$$\mathsf{vol}(A) = (k+1)!\frac{t}{k+1}\,\mathsf{vol}_{k-1}\,\Delta(rb_1,\dots,rb_{k+1}) = k!r^k t\,\mathsf{vol}_k\,\Delta(B).$$

From this expression, together with (20), we conclude that

$$\begin{aligned}\frac{\mathsf{vol}\,\mathcal{R}^k_{n,m}(\varepsilon)}{\mathcal{O}^n_m} &= \frac{\mathcal{G}_{k+1,m+1}}{\mathcal{O}^{k+1}_m}\int_{W_k\times(0,\varepsilon)} \mathsf{vol}(A)^{m-k+1}\frac{r(t)^{(k-2)(k+1)}}{t}\\ &\qquad\qquad \times \lambda_m(t)^{n-k-1}\,d(S^k)^{k+1}\\ &= \frac{\mathcal{G}_{k+1,m+1}(k!)^{m-k+1}}{\mathcal{O}^{k+1}_m}\int_{W_k}\mathsf{vol}_k\,\Delta(B)^{m-k+1}\,dW_k\\ &\quad\times\int_0^\varepsilon t^{m-k}r(t)^{km-2}\lambda_m(t)^{n-k-1}\,dt.\end{aligned}$$

Consider the projection $\mathrm{pr}\colon W_k\to S^k, (B,p)\mapsto p$. We note that its fiber over p can be identified with the set M_k (cf. Definition 4.3). By the invariance of $\mathsf{vol}_k\,\Delta(B)$ under rotation of $p\in S^k$, we get

$$\int_{W_k}\mathsf{vol}_k\,\Delta(B)^{m-k+1}\,dW_k = \mathcal{O}_k\int_{M_k}\mathsf{vol}_k\,\Delta(B)^{m-k+1}\,d(S^{k-1})^{k+1}.$$

Note that, up to a scaling factor, the right-hand side above is the coefficient $C(m,k)$ introduced in Definition 4.3. Using $(\mathcal{O}_k/\mathcal{O}_m)\mathcal{G}_{k+1,m+1}=\mathcal{G}_{k,m}$ we obtain

$$\frac{\mathsf{vol}\,\mathcal{R}^k_{n,m}(\varepsilon)}{\mathcal{O}^n_m} = C(m,k)\int_0^\varepsilon t^{m-k}r(t)^{km-2}\lambda_m(t)^{n-k-1}\,dt. \tag{21}$$

This completes the proof. □

Proof of Lemma 4.6. For given $p\in S^k$, let $S(p^\perp)$ denote the $(k-1)$-subsphere of S^k perpendicular to p. At a point $(B,p)\in W_k$ we have $dW_k = dS(p^\perp)^{k+1}\wedge dS^k$, and we have $dS(p^\perp)^{k+1} = dS(p^\perp)\wedge\cdots\wedge dS(p^\perp)$ at the point $B=(b_1,\dots,b_{k+1})$. The Jacobian $J(A)$ we are looking for is hence determined by

$$d(S^k)^{k+1}(A) = J(A)\,dS(p^\perp)^{k+1}(B)\wedge dS^k(p)\wedge dt.$$

Choose an orthonormal moving frame $e_1, \dots, e_k, e_{k+1}$ with $p(A) = e_{k+1}$. For $1 \le i \le k$ define the one-forms $\mu_i := -\langle e_i, dp\rangle$ (compare Section 3.2). Then the volume form of S^k at p is given by $dS^k(p) = \mu_1 \wedge \cdots \wedge \mu_k$.

Differentiating $te = Ap$ we get $e\,dt = dAp + A\,dp$. By multiplying both sides with A^{-1} and using formula (14) we obtain

$$p(dt/t) - dp = A^{-1}\,dAp.$$

Let Q denote the $(k+1)\times(k+1)$ matrix having the e_i as rows. With respect to this basis, the above equation takes the form

$$(\mu_1, \dots, \mu_k, dt/t)^\top = Q(p(dt/t) - dp) = QA^{-1}\,dAp. \tag{22}$$

Wedging the entries on both sides yields

$$dS^k(p) \wedge dt = t\,\mathsf{vol}(A)^{-1}\langle p, da_1\rangle \wedge \cdots \wedge \langle p, da_{k+1}\rangle. \tag{23}$$

The volume form of $S(p^\perp)$ at b_i is given by

$$dS(p^\perp) = \langle e_1, db_i\rangle \wedge \cdots \wedge \langle e_{k-1}, db_i\rangle.$$

In order to compare $dS(p^\perp)^{k+1} \wedge dS^k \wedge dt$ with $d(S^k)^{k+1}$ we use a different moving frame. Fix an i, $1 \le i \le k+1$, and choose the moving frame as above and additionally with $e_k = b_i$. Consider the modified frame $\tilde e_1, \dots, \tilde e_{k+1}$ that arises after rotating b_i to a_i and leaving the orthogonal complement of $\operatorname{span}\langle a_i, p\rangle$ fixed, that is, $\tilde e_j = e_j$ for $1 \le j \le k-1$, $\tilde e_k := a_i$, and $\tilde e_{k+1} = -tb_i + rp$ (cf. Figure 4).

This implies $\langle \tilde e_{k+1}, da_i\rangle = r\langle p, da_i\rangle - t\langle b_i, da_i\rangle = (1/r)\langle p, da_i\rangle$ where we have used that $b_i = (a_i - tp)/r$ for the last equality. Hence the volume form of S^k at a_i equals

$$dS^k(a_i) = (1/r)\langle e_1, da_i\rangle \wedge \cdots \wedge \langle e_{k-1}, da_i\rangle \wedge \langle p, da_i\rangle.$$

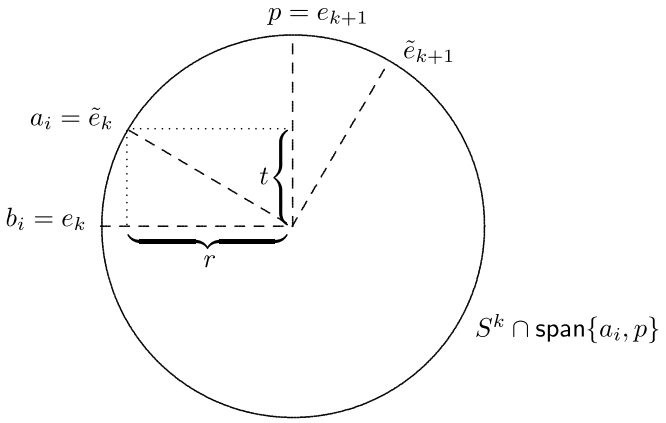

FIG. 4. *The frame (e_i) and its modification $(\tilde e_i)$.*

If we wedge the $\langle e_1, da_i\rangle \wedge \cdots \wedge \langle e_{k-1}, da_i\rangle$ to both sides of equation (23), we obtain, on the right-hand side,

$$\frac{t}{\mathsf{vol}(A)} \bigwedge_{i=1}^{k+1} \langle e_1, da_i\rangle \wedge \cdots \wedge \langle e_{k-1}, da_i\rangle \wedge \langle p, da_i\rangle = \frac{t}{\mathsf{vol}(A)} r^{k+1}\, d(S^k)^{k+1}(A).$$

On the left-hand side we obtain, using $\langle e_j, da_i\rangle = r\langle e_j, db_i\rangle + t\langle e_j, dp\rangle$ and taking into account that $\langle e_j, dp\rangle \wedge dS^k(p) = 0$ since $dS^k(p) = \bigwedge_{j=1}^{k}\langle e_j, dp\rangle$,

$$\begin{aligned}\bigwedge_{i=1}^{k+1}\bigwedge_{j=1}^{k-1} \langle e_j, da_i\rangle \wedge dS^k \wedge dt &= r^{(k-1)(k+1)} \bigwedge_{i=1}^{k+1}\bigwedge_{j=1}^{k-1} \langle e_j, db_i\rangle \wedge dS^k \wedge dt \\ &= r^{(k-1)(k+1)} dS(p^\perp)^{k+1} \wedge dS^k \wedge dt.\end{aligned}$$

This implies that $J(A) = t^{-1} r^{(k-2)(k+1)}\, \mathsf{vol}(A)$ as claimed. □

4.2. *The infeasible case.* Recall that $\mathcal{I}_{n,m} = (S^m)^n \setminus \mathcal{F}_{n,m}$ denotes the set of infeasible instances. We define, for $I \subseteq [n]$,

$$\mathcal{I}^I_{n,m}(\varepsilon) := \{A \in \mathcal{I}_{n,m} \mid \mathscr{C}(A) > \varepsilon^{-1} \text{ and } A \text{ has a SIC with blocking set } I\}.$$

We note that by symmetry, the volume of $\mathcal{I}^I_{n,m}(\varepsilon)$ only depends on the cardinality of I.

LEMMA 4.7. *$\mathcal{I}^I_{n,m}(\varepsilon)$ has measure zero if $|I| > m+1$.*

PROOF. If $A \in \mathcal{I}^I_{n,m}(\varepsilon)$, then $\{a_i \mid i \in I\}$ is contained in the boundary of a SIC of A with blocking set I. Hence the affine hull of $(a_i)_{i\in I}$ has dimension less than m. However, if $|I| > m+1$, the latter dimension is almost surely $m+1$. □

It is known [5], Proposition 4.2, that in the infeasible case, blocking sets have at least $m+1$ elements. This fact, together with Lemma 4.7, implies that

$$\mathsf{vol}\,\mathcal{I}_{n,m}(\varepsilon) \le \binom{n}{m+1} \mathsf{vol}\,\mathcal{I}^{[m+1]}_{n,m}(\varepsilon). \tag{24}$$

As with $\mathcal{F}_{n,m}$, for ease of notation, we write $\mathcal{I}^m_{n,m}(\varepsilon) := \mathcal{I}^{[m+1]}_{n,m}(\varepsilon)$.

The inequality in Theorem 1.3 for the infeasible case follows immediately from (24) and the following proposition.

PROPOSITION 4.8. *We have for $\varepsilon \in (0,1]$,*

$$\frac{\mathsf{vol}\,\mathcal{I}^m_{n,m}(\varepsilon)}{\mathcal{O}^n_m} \le C(m,m) \int_0^\varepsilon (1-t^2)^{(m^2-2)/2} (1-\lambda_m(t))^{n-m-1}\, dt.$$

PROOF. Consider the projection

$$\psi : \mathcal{I}^m_{n,m}(\varepsilon) \to (S^m)^{m+1}, \qquad A' = (a_1, \dots, a_n) \mapsto A = (a_1, \dots, a_{m+1}).$$

To investigate the image and the fibers of ψ assume $A' \in \mathcal{I}^m_{n,m}(\varepsilon)$. Then there exists $p \in S^m$ and $\alpha \in (\pi/2, \pi]$ such that $\mathsf{cap}(p, \alpha)$ is a SIC of $A' \in \mathcal{I}^m_{n,m}(\varepsilon)$ with blocking set $[m+1]$. Then we have that $\langle a_i, p\rangle = t$ for all $i \in [m+1]$ and $\langle a_i, p\rangle > t$ for all $i \in [n] \setminus [m+1]$ where $t := \cos\alpha \in [-1, 0)$. Lemma 3.2 implies that $tp \in \mathsf{conv}\{a_1, \dots, a_{m+1}\}$. In turn, Lemma 3.1 implies that $\mathsf{cap}(-p, \pi - \alpha)$ is a SIC of A with blocking set $[m+1]$, and we obtain that $A \in \mathcal{F}^m_{m+1,m}(\varepsilon)$. These reasonings show that the image of ψ is contained in $\mathcal{F}^m_{m+1,m}(\varepsilon)$.

Suppose now that $a_1, \dots, a_{m+1}$ are linearly independent. Then it follows from Lemma 3.3 that the vector p is uniquely determined by A. This implies that the fiber of A under ψ is contained in $\{A\} \times \mathsf{cap}(p, \alpha)^{n-m-1}$. We conclude that for almost all $A \in \mathcal{F}^m_{m+1,m}$

$$\frac{\mathsf{vol}\, \psi^{-1}(A)}{\mathcal{O}_m^{n-m-1}} \le (1 - \lambda_m(t))^{n-m-1}.$$

From these observations we obtain, by Fubini,

$$\frac{\mathsf{vol}\, \mathcal{I}^m_{n,m}(\varepsilon)}{\mathcal{O}_m^{n-m-1}} \le \int_{A \in \mathcal{F}^m_{m+1,m}(\varepsilon)} (1 - \lambda_m(t(A)))^{n-m-1}\, d(S^m)^{m+1}.$$

In the proof of Proposition 4.5 we derived, from the integral representation (19) for $\frac{\mathsf{vol}\, \mathcal{F}^k_{n,m}(\varepsilon)}{\mathcal{O}_m^{n-k-1}}$, formula (21). In exactly the same way we can show that

$$\frac{\mathsf{vol}\, \mathcal{I}^m_{n,m}(\varepsilon)}{\mathcal{O}_m^{n}} \le C(m,m) \int_0^\varepsilon (1 - t^2)^{(m^2-2)/2} (1 - \lambda_m(t))^{n-m-1}\, dt,$$

which proves the assertion. □

REMARK 4.9. (i) It may be of interest to compare, in the case $m = 1$, the upper bound for $p(n, 1, \alpha)$ which follows from our results with the exact expression (1) for this quantity shown by Stevens. Recall that the latter is

$$p(n,1,\alpha) = n\left(1 - \frac{\alpha}{\pi}\right)^{n-1} - \binom{n}{2}\left(1 - \frac{2\alpha}{\pi}\right)^{n-1} + \cdots + (-1)^{k+1}\binom{n}{k}\left(1 - \frac{k\alpha}{\pi}\right)^{n-1},$$

where $k = \lfloor \frac{\pi}{\alpha} \rfloor$. For $\alpha \in [0, \pi/2]$, Propositions 1.5 and 4.8 yield

$$\begin{aligned} p(n,1,\alpha) &= \mathsf{Prob}\{A \in \mathcal{F}_{n,1}\} + \mathsf{Prob}\left\{A \notin \mathcal{F}_{n,1} \text{ and } \mathscr{C}(A) \ge \frac{1}{\cos(\alpha)}\right\} \\ &\le \frac{n}{2^{n-1}} + \binom{n}{2} C(1,1) \int_0^{\cos\alpha} (1 - t^2)^{-1/2} (1 - \lambda_1(t))^{n-2}\, dt. \end{aligned}$$

We use now that $C(1,1)=\frac{2}{\pi}$, as shown in Example 4.4. Then

$$\begin{aligned} p(n,1,\alpha) &= \frac{n}{2^{n-1}} + \frac{n(n-1)}{\pi}\int_0^{\cos\alpha}(1-t^2)^{-1/2}\left(1-\frac{\arccos t}{\pi}\right)^{n-2}dt \\ &\le \frac{n}{2^{n-1}} + n(n-1)\int_{\alpha/\pi}^{1/2}(1-x)^{n-2}\,dx \\ &= n\left(1-\frac{\alpha}{\pi}\right)^{n-1}. \end{aligned}$$

That is, we get Stevens's first term.

(ii) It may also be of interest to compare, for the case $m=2$, our upper bound for $p(n,2,\alpha)$ with the upper bound in (2) obtained by Gilbert [10]. Recall that the latter gives

$$p(n,2,\alpha) \le \tfrac{4}{3}n(n-1)\lambda(1-\lambda)^{n-1},$$

where λ denotes the fraction of the surface of the sphere covered by the cap of radius α. It is easy to see that our bound implies

$$p(n,2,\alpha) \le \frac{1}{2^n}(n^2-n+2) + \frac{1}{2}n(n-2)(1-\lambda)^{n-1}.$$

The first term in this sum is negligible for large n. The second term compares with Gilbert's for moderately large caps but it becomes considerably worse for small caps.

5. On the values of the coefficients $C(m,k)$. In this section we provide estimates for the numbers $C(m,k)$. In Section 5.1 we derive upper and lower bounds for them which are elementary functions in m and k. In the case $m=k$ the upper bound is actually an equality, yielding an exact expression for $C(m,m)$. Then in Section 5.2 we use these bounds to prove Theorems 1.2 and 1.4. Finally, in Section 5.3 we briefly describe how to derive an exact expression for $C(m,m-1)$ and how, for any given m, one may obtain the values of the $C(m,k)$, $k=1,\dots,m$, by solving an $m\times m$ linear system.

5.1. *Bounding the coefficients $C(m,k)$.* Our first result provides bounds for $C(m,k)$ in terms of volumes of spheres.

LEMMA 5.1. *We have for $1\le k\le m$,*

$$\frac{k+1}{2^k}\frac{\mathcal{O}_{k-1}\mathcal{O}_{m-k}}{\mathcal{O}_m} \le C(m,k) \le \frac{(k+1)^{m-k+1}}{2^k}\frac{\mathcal{O}_{k-1}\mathcal{O}_{m-k}}{\mathcal{O}_m}$$

with equalities if $k=m$. In particular, $C(m,m)=\frac{m+1}{2^{m-1}}\frac{\mathcal{O}_{m-1}}{\mathcal{O}_m}$.

PROOF. Recall Definition 4.3 of the $C(m,k)$,

$$C(m,k) = \frac{(k!)^{m-k+1}}{\mathcal{O}_m^k}\mathcal{G}_{k,m}\int_{M_k}(\mathsf{vol}\,\Delta)^{m-k+1}\,dS.$$

We set $S := (S^{k-1})^{k+1}$ and denote by U the open dense subset of S consisting of all $B = (b_1,\dots,b_{k+1})$ such that every k of these vectors are linearly independent. By Definition 4.1, M_k is contained in U.

Set $\Delta(B) = \mathsf{conv}\{b_1,\dots,b_{k+1}\}$ and $\Delta_i(B) = \mathsf{conv}(0,b_1,\dots,\hat{b}_i,\dots,b_{k+1})$ (where $\hat{b}_i$ means that b_i is omitted). We define, for $B \in U$,

$$\mathsf{mvol}(B) := \sum_{i=1}^{k+1}\mathsf{vol}\,\Delta_i(B).$$

For $B \in M_k$ we clearly have $\mathsf{mvol}(B) = \mathsf{vol}\,\Delta(B)$, but in general this is not the case.

The essential observation is now the following:

$$\int_{M_k}(\mathsf{vol}\,\Delta)^{m-k+1}\,dS = \frac{1}{2^k}\int_U \mathsf{mvol}^{m-k+1}\,dS. \tag{25}$$

In order to show this, note that for $B \in U$ there exists a unique $\mu \in \mathbb{R}^{k+1}$ with $\mu_{k+1} = 1$, $\mu_1\cdots\mu_k \neq 0$, and such that $\sum_{i=1}^{k+1}\mu_i b_i = 0$. This allows to define the map $\phi : U \to \{-1,1\}^k, B \mapsto (\mathsf{sgn}(\mu_1),\dots,\mathsf{sgn}(\mu_k))$. Note that $M_k = \phi^{-1}(1,\dots,1)$. Moreover, each $\sigma \in \{-1,1\}^k$ defines an isometry,

$$M_k \to \phi^{-1}(\sigma), \qquad B \mapsto \sigma B := (\sigma_1 b_1,\dots,\sigma_k b_k, b_{k+1}).$$

It follows that $\mathsf{mvol}(B) = \mathsf{mvol}(\sigma B)$ since changing the signs of rows does not alter the absolute values of determinants. This implies

$$\begin{aligned}\int_U \mathsf{mvol}^{m-k+1}\,dS &= \sum_{\sigma\in\{-1,1\}^k}\int_{\phi^{-1}(\sigma)}\mathsf{mvol}^{m-k+1}\,dS\\ &= 2^k\int_{M_k}\mathsf{mvol}^{m-k+1}\,dS,\end{aligned}$$

which proves the claimed equation (25).

Recall now the norm inequalities

$$\begin{aligned}(x_1^\ell + \cdots + x_p^\ell) &\le (x_1 + \cdots + x_p)^\ell\\ &\le p^{\ell-1}(x_1^\ell + \cdots + x_p^\ell) \qquad \text{for } x_i \ge 0, \ell \ge 1,\end{aligned} \tag{26}$$

where the last follows from the convexity of the function $\mathbb{R} \to \mathbb{R}, y \mapsto y^\ell$. For the upper bound in the statement we now estimate the right-hand side

of equation (25) using the last inequality above (with $p = k+1$ and $\ell = m-k+1$). We obtain

$$\begin{aligned}\int_S \mathsf{mvol}^{m-k+1}\,dS &\le (k+1)^{m-k}\sum_{i=1}^{k+1}\int_S (\mathsf{vol}\,\Delta_i)^{m-k+1}\,dS\\ &= (k+1)^{m-k+1}\int_S (\mathsf{vol}\,\Delta_{k+1})^{m-k+1}\,dS\\ &= \frac{(k+1)^{m-k+1}}{k!^{m-k+1}}\int_S |\det \tilde{B}|^{m-k+1}\,dS,\end{aligned}$$

where $\tilde{B}\in\mathbb{R}^{k\times k}$ denotes the matrix with rows $b_1,\dots,b_k$. Since the integrand on the right does not depend on b_{k+1}, we can integrate over $\tilde{B}\in(S^{k-1})^k$ and pull out a factor $\mathcal{O}_{k-1}$ obtaining

$$\begin{aligned}\int_S \mathsf{mvol}^{m-k+1}\,dS &\le \frac{(k+1)^{m-k+1}}{k!^{m-k+1}}\mathcal{O}_{k-1}\int_{(S^{k-1})^k} |\det \tilde{B}|^{m-k+1}\,d(S^{k-1})^k\\ &= \frac{(k+1)^{m-k+1}}{k!^{m-k+1}}\mathcal{O}_{k-1}^{k+1}\mathbf{E}(|\det \tilde{B}|^{m-k+1}).\end{aligned}$$

We plug in here the formula of the moments from Lemma 3.5. Putting everything together, and using $\mathcal{G}_{k,m} = (\mathcal{O}_{m-k}/\mathcal{O}_m)\mathcal{G}_{k,m+1}$, the claimed upper bound on $C(m,k)$ follows. The lower bound is obtained by doing the same reasoning but now using the left-hand side inequality in (26).

In the case $k=m$ upper and lower bounds coincide and we get equalities for $C(m,m)$. □

REMARK 5.2. In the case $k=1$ the upper bound in Lemma 5.1 coincides with the value for $C(m,1)$ shown in Example 4.4.

For the proofs of Theorems 1.2 and 1.4 we need a more explicit expression for the bounds on the $C(m,k)$. We devote the rest of this section to deriving such expressions.

LEMMA 5.3. *For $1\le k\le m$ we have*

$$\frac{\mathcal{O}_{k-1}\mathcal{O}_{m-k}}{\mathcal{O}_m} \le \sqrt{\frac{\pi}{2}}k^{3/4}\sqrt{\binom{m}{k}}.$$

In the cases $k=1$ or $k=m$ one has the sharper bound $\frac{2\mathcal{O}_{m-1}}{\mathcal{O}_m}\le\sqrt{m}$.

The proof uses bounds on Gamma functions, which we derive next.

LEMMA 5.4. *For all $r \geq 1$,*

$$r^{1/4}2^{-(r-1)/2}\sqrt{(r-1)!} \leq \Gamma\left(\frac{r+1}{2}\right) \leq \sqrt{\frac{\pi}{2}}r^{1/4}2^{-(r-1)/2}\sqrt{(r-1)!}.$$

PROOF. The double factorials $k!!$ are defined as follows. For k even, $k!! := k(k-2)(k-4)\cdots 2$, and for k odd, $k!! := k(k-2)(k-4)\cdots 3\cdot 1$. Also, by convention, $0!! = 1$. By the functional equation $\Gamma(x+1) = x\Gamma(x)$ of the Gamma function, it easily follows that for $r \in \mathbb{N}$, $r \geq 1$,

$$\Gamma\left(\frac{r+1}{2}\right) = \begin{cases} \sqrt{\frac{\pi}{2}}(r-1)!!2^{-(r-1)/2}, & \text{if } r \text{ is even,} \\ (r-1)!!2^{-(r-1)/2}, & \text{if } r \text{ is odd.} \end{cases} \tag{27}$$

We estimate now double factorials in terms of factorials. If $r \geq 2$ is even,

$$\begin{aligned}(r!!)^2 &= rr(r-2)(r-2)\cdots 4\cdot 4\cdot 2\cdot 2 \\ &= r(r-1)\frac{r}{r-1}(r-2)(r-3)\frac{r-2}{r-3}\cdots 4\cdot 3\frac{4}{3}2\cdot 2 \\ &= r!\frac{r}{r-1}\frac{r-2}{r-3}\cdots\frac{4}{3}2 \\ &= r!\sqrt{\frac{r}{r-1}\frac{r}{r-1}\frac{r-2}{r-3}\frac{r-2}{r-3}\cdots\frac{4}{3}\frac{4}{3}2\cdot 2}.\end{aligned}$$

We use that $\frac{\ell+1}{\ell} \leq \frac{\ell}{\ell-1}$ for $\ell \geq 2$ to deduce from this

$$r!\sqrt{r+1} \leq (r!!)^2 \leq r!\sqrt{2r} \qquad \text{for } r \geq 2 \text{ even.} \tag{28}$$

Similarly, for $r \geq 1$ odd, one shows that

$$(r!!)^2 = r!\sqrt{\frac{r}{r-1}\frac{r}{r-1}\frac{r-2}{r-3}\frac{r-2}{r-3}\cdots\frac{5}{4}\frac{5}{4}\frac{3}{2}\frac{3}{2}},$$

which implies

$$r!\sqrt{\frac{r+1}{2}} \leq (r!!)^2 \leq r!\sqrt{r} \qquad \text{for } r \geq 1 \text{ odd.} \tag{29}$$

By applying the bounds (28) and (29) to (27) and noting that $2^{1/4} \leq \sqrt{\frac{\pi}{2}}$, the claim follows. □

PROOF OF LEMMA 5.3. Assume that $2 \leq k < m$. Then, using Lemma 5.4, we deduce that

$$\frac{\mathcal{O}_{k-1}\mathcal{O}_{m-k}}{\mathcal{O}_m} = 2\frac{\Gamma((m+1)/2)}{\Gamma(k/2)\Gamma((m-k+1)/2)}$$

$$\le \sqrt{\frac{\pi}{2}}\sqrt{\frac{(m-1)!}{(k-2)!(m-k-1)!}}\left(\frac{m}{(k-1)(m-k)}\right)^{1/4}$$
$$= \sqrt{\frac{\pi}{2}}\sqrt{\binom{m}{k}}\sqrt{\frac{(m-k)k(k-1)}{m}}\left(\frac{m}{(k-1)(m-k)}\right)^{1/4}$$
$$\le \sqrt{\frac{\pi}{2}}\sqrt{\binom{m}{k}}k^{3/4}.$$

The cases $k=1$ and $k=m$ follow similarly from Lemma 5.4. □

An immediate consequence of Lemmas 5.3 and 5.4 are the following bounds on the coefficients $C(m,k)$.

PROPOSITION 5.5. *For $1 \le k < m$,*

$$C(m,k) \le \sqrt{\frac{\pi}{2}}\frac{(k+1)^{m-k+1}}{2^k}k^{3/4}\sqrt{\binom{m}{k}}.$$

In addition, for all $m \ge 1$,

$$C(m,m) \le \frac{(m+1)\sqrt{m}}{2^m}.$$

REMARK 5.6. Using Lemmas 5.1 and 5.4 it is easy to obtain lower bounds for the $C(m,k)$ similar to the upper bounds in Proposition 5.5.

5.2. *Proof of Theorems 1.2 and 1.4.* The following identity is repeatedly used in the proof.

LEMMA 5.7. *We have $\sum_{n=k}^{\infty}\binom{n}{k}z^{n-k} = (1-z)^{-k-1}$ for $k \in \mathbb{N}$ and $z \in (0,1)$.*

PROOF. Take the kth derivative on both sides of $\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$. □

PROOF OF THEOREM 1.2. By definition, we have $N(m,\alpha) > n$ iff $\mathsf{cap}(a_1,\alpha) \cup \cdots \cup \mathsf{cap}(a_n,\alpha) \ne S^n$. Hence

$$\mathbf{E}(N(m,\alpha)) = \sum_{n=0}^{\infty}\mathsf{Prob}(N(m,\alpha) > n) = \sum_{n=0}^{\infty}p(n,m,\alpha).$$

We assume that $\alpha \le \pi/2$. Since $p(n,m,\alpha) = 1$ for $n \le m+1$, we conclude

$$\mathbf{E}(N(m,\alpha)) = m+1+\sum_{n=m+1}^{\infty}p(n,m,\alpha). \tag{30}$$

Proposition 1.5 states that, for $\alpha \in (0, \frac{\pi}{2}]$, and $\varepsilon = \cos(\alpha)$

$$p(n, m, \alpha) = 2^{1-n} \sum_{k=0}^{m} \binom{n-1}{k} + P_{n,m}(\varepsilon),$$

where we have put

$$P_{n,m}(\varepsilon) := \mathsf{Prob}\{A \in \mathcal{I}_{n,m} \text{ and } \mathscr{C}(A) \geq \varepsilon^{-1}\}.$$

We first estimate

$$T := \sum_{n=m+1}^{\infty} 2^{1-n} \sum_{k=0}^{m} \binom{n-1}{k}$$

as follows (take $r = n-1$)

$$T = \sum_{k=0}^{m} \sum_{r=m}^{\infty} \binom{r}{k} \left(\frac{1}{2}\right)^r \leq \sum_{k=0}^{m} \left(\frac{1}{2}\right)^k \sum_{r=k}^{\infty} \binom{r}{k} \left(\frac{1}{2}\right)^{r-k} - \sum_{k=0}^{m-1} \frac{1}{2^k}.$$

Applying Lemma 5.7 to the last expression we obtain

$$T \leq \sum_{k=0}^{m} \left(\frac{1}{2}\right)^k 2^{k+1} - 2 + \frac{1}{2^{m-1}} \leq 2m + 1.$$

We now estimate $T^* := \sum_{n=m+1}^{\infty} P_{n,m}(\varepsilon)$ using Theorem 1.3 which tells us that

$$P_{n,m}(\varepsilon) \leq \binom{n}{m+1} C(m,m) \int_0^{\varepsilon} (1-t^2)^{(m^2-2)/2} (1-\lambda_m(t))^{n-m-1}\, dt.$$

Hence, using Lemma 5.7 again,

$$\begin{aligned} T^* &= C(m,m) \sum_{n=m+1}^{\infty} \binom{n}{m+1} \int_0^{\varepsilon} (1-t^2)^{(m^2-2)/2} (1-\lambda_m(t))^{n-m-1}\, dt \\ &\leq C(m,m) \int_0^{\varepsilon} \sum_{n=m+1}^{\infty} \binom{n}{m+1} (1-\lambda_m(t))^{n-m-1}\, dt \\ &= C(m,m) \int_0^{\varepsilon} \lambda_m(t)^{-m-2}\, dt \leq C(m,m) \frac{\varepsilon}{\lambda(\varepsilon)^{m+2}}. \end{aligned}$$

Plugging in the estimate for $C(m,m)$ from Proposition 5.5, we obtain the claimed bound for $\mathbf{E}(N(m,\alpha)) \leq m + 1 + T + T^*$. □

We now turn to Theorem 1.4 on the expected value of $\ln \mathscr{C}(A)$. In Theorem 1.3 we derived tail estimates on the probability distribution of the GCC condition number. For the sake of clarity, we include the following simple observation showing how to use these tail estimates to bound the expected value of the logarithm of the condition number.

PROPOSITION 5.8. *Let Z be a random variable, almost surely greater or equal than 1, satisfying, for some $K, t_0 > 0$, that $\mathsf{Prob}\{Z \geq t\} \leq Kt^{-1}$ for all $t \geq t_0$. Then $\mathbf{E}(\ln Z) \leq \ln t_0 + \frac{K}{t_0}$.*

PROOF. We have $\mathsf{Prob}\{\ln Z \geq s\} \leq Ke^{-s}$ for all $s > \ln t_0$. Therefore,

$$\mathbf{E}(\ln Z) = \int_0^\infty \mathsf{Prob}\{\ln Z \geq s\}\, ds \leq \ln t_0 + \int_{\ln t_0}^\infty Ke^{-s}\, dt = \ln t_0 + \frac{K}{t_0}$$

as claimed. □

We next proceed to prove Theorem 1.4. To simplify notation we put

$$P_{n,m}(\varepsilon) := \mathsf{Prob}\{A \in \mathcal{I}_{n,m} \text{ and } \mathscr{C}(A) \geq \varepsilon^{-1}\},$$
$$Q_{n,m}(\varepsilon) := \mathsf{Prob}\{A \in \mathcal{F}_{n,m} \text{ and } \mathscr{C}(A) \geq \varepsilon^{-1}\}.$$

LEMMA 5.9. *For any $n > m \geq 1$ and $\varepsilon \in (0, 1]$ we have:*

(i) *If $\varepsilon^{-1} \geq 13(m+1)^{3/2}$ then $P_{n,m}(\varepsilon) \leq 2e(m+1)^{3/2}\varepsilon$.*
(ii) *If $\varepsilon^{-1} \geq (m+1)^2$ then $Q_{n,m}(\varepsilon) \leq \sqrt{2\pi e}(m+1)^{7/4}\varepsilon$.*

PROOF. (i) Theorem 1.3 tells us that

$$P_{n,m}(\varepsilon) \leq \binom{n}{m+1} C(m,m) \int_0^\varepsilon (1-t^2)^{(m^2-2)/2}(1-\lambda_m(t))^{n-m-1}\, dt.$$

Recall formula (5) for the relative volume $\lambda_m(t)$ of a cap of radius $\arccos(t)$ on S^m. Recall also from Lemma 5.3 that $\alpha_m := \frac{2\mathcal{O}_{m-1}}{\mathcal{O}_m} \leq \sqrt{m}$. The first order derivative of $\lambda_m(t)$

$$\frac{d\lambda_m(t)}{dt} = -\frac{1}{2}\alpha_m(1-t^2)^{(m-2)/2}$$

is increasing; hence λ_m is a convex function. Moreover, $\lambda_m(0) = 1/2$. This implies $2\lambda_m(t) \geq 1 - \alpha_m t$ for all $t \in [0,1]$; hence $1 - \lambda_m(t) \leq \frac{1}{2}(1 + \alpha_m t)$.

Bounding $C(m,m)$ as in Proposition 5.5 we arrive at the estimate

$$P_{n,m}(\varepsilon) \leq 2(m+1)\sqrt{m}\frac{1}{2^n}\binom{n}{m+1}(1+\sqrt{m}\varepsilon)^{n-m-1}\varepsilon. \tag{31}$$

We now proceed dividing by cases. Suppose that $\varepsilon^{-1} \geq 13(m+1)^{3/2}$.

CASE 1 [$n \leq 13(m+1)$]. In this case $\varepsilon^{-1} \geq n\sqrt{m}$ and hence, using (31),

$$P_{n,m}(\varepsilon) \leq 2(m+1)\sqrt{m}(1+1/n)^{n-m-1}\varepsilon \leq 2e(m+1)\sqrt{m}\varepsilon.$$

CASE 2 $[n > 13(m+1)]$. This implies $\ln(e\frac{n}{m+1}) \le \frac{n}{m+1}\ln(\frac{4}{3})$, and it follows that

$$\binom{n}{m+1} \le \frac{1}{(m+1)!}n^{m+1} \le \left(\frac{en}{m+1}\right)^{m+1} \le \left(\frac{4}{3}\right)^n. \tag{32}$$

Since, in addition, $\varepsilon^{-1} \ge 13(m+1)\sqrt{m} \ge 2\sqrt{m}$ we get from (31)

$$P_{n,m}(\varepsilon) \le 2(m+1)\sqrt{m}\frac{1}{2^n}\binom{n}{m+1}\left(\frac{3}{2}\right)^n \varepsilon \le 2(m+1)\sqrt{m}\varepsilon.$$

(ii) Theorem 1.3 implies that

$$\begin{aligned} Q_{n,m}(\varepsilon) &= \sum_{k=1}^{m}\binom{n}{k+1}C(m,k)\int_0^\varepsilon t^{m-k}(1-t^2)^{km/2-1}\lambda_m(t)^{n-k-1}\,dt \\ &\le \sum_{k=1}^{m}\binom{n}{k+1}C(m,k)\varepsilon^{m-k+1}2^{-(n-k-1)} \\ &\le \sum_{k=1}^{m}C(m,k)\varepsilon^{m-k+1}2^{k+1}, \end{aligned}$$

the second line since $\lambda_m(t) \le \frac{1}{2}$. Using Proposition 5.5 we obtain

$$\begin{aligned} Q_{n,m}(\varepsilon) &\le \varepsilon\sqrt{2\pi}(m+1)^{7/4}\sum_{k=1}^{m}\sqrt{\binom{m}{k}}((m+1)\varepsilon)^{m-k} \\ &\le \varepsilon\sqrt{2\pi}(m+1)^{7/4}\sum_{k=1}^{m}\binom{m}{k}((m+1)\varepsilon)^{m-k} \\ &\le \varepsilon\sqrt{2\pi}(m+1)^{7/4}(1+(m+1)\varepsilon)^m. \end{aligned}$$

Under the assumption $\varepsilon^{-1} \ge (m+1)^2$ we have $(m+1)\varepsilon \le \frac{1}{(m+1)}$, and hence

$$Q_{n,m}(\varepsilon) \le \varepsilon\sqrt{2\pi}(m+1)^{7/4}\sqrt{e}. \qquad \square$$

PROOF OF THEOREM 1.4. For $\varepsilon^{-1} \ge 13(m+1)^2$ we have, by Lemma 5.9,

$$\begin{aligned} \mathsf{Prob}\{\mathscr{C}(A) \ge \varepsilon^{-1}\} &= P_{n,m}(\varepsilon) + Q_{n,m}(\varepsilon) \\ &\le (2e(m+1)^{3/2} + \sqrt{2\pi e}(m+1)^{7/4})\varepsilon \\ &\le 9.6(m+1)^2\varepsilon. \end{aligned}$$

An application of Proposition 5.8 with $K = 9.6(m+1)^2$ and $t_0 = 13(m+1)^2$ shows that

$$\mathbf{E}(\ln\mathscr{C}(A)) \le 2\ln(m+1) + \ln 13 + 9.6/13 \le 2\ln(m+1) + 3.31. \qquad \square$$

5.3. *On calculating the* $C(m,k)$. We describe a method for calculating the $C(m,k)$. For $1 \le k \le m < n$ we define the following integrals:

$$I(n,m,k) := 2^{n-1}\binom{n}{k+1}\int_0^1 t^{m-k}(1-t^2)^{km/2-1}\lambda_m(t)^{n-k-1}\,dt.$$

By setting $\varepsilon = 1$ in the first part of Theorem 1.3 we get from (4) that, for all $n > m$,

$$\sum_{k=1}^{m} I(n,m,k)C(m,k) = \sum_{k=0}^{m-1}\binom{n-1}{k}. \tag{33}$$

By taking m different values of n (e.g., $n = m+1,\dots,2m$) one obtains a (square) system of linear equations in the $C(m,k)$. Solving this system with Maple (symbolically for even m and numerically for odd m) we obtained Table 1.

We can further use (33) to obtain expressions for $C(m,k)$ for values of k other than 1 and m. We do so for $k = m-1$.

PROPOSITION 5.10. *For all* $m \ge 2$,

$$C(m,m-1) = \frac{m(m-1)}{2^{m-1}}(1+\alpha_m^2) \qquad \text{where } \alpha_m = \frac{2\mathcal{O}_{m-1}}{\mathcal{O}_m}.$$

SKETCH OF PROOF. Put $J(n,m,k) := \int_0^1 t^{m-k}(1-t^2)^{km/2-1}\lambda_m(t)^{n-k-1}\,dt$ so that $I(n,m,k) = 2^{n-1}\binom{n}{k+1}J(n,m,k)$. In the following we write $N = n-m$. One can prove that for fixed m the following asymptotic expansion holds for $N \to \infty$:

$$2^{n-m-1}J(n,m,m) = \frac{1}{\alpha_m}\frac{1}{N} - \frac{m(m-1)}{\alpha_m^3}\frac{1}{N^3} + \mathcal{O}\left(\frac{1}{N^5}\right),$$

$$2^{n-m}J(n,m,m-1) = \frac{1}{\alpha_m^2}\frac{1}{(N+1)(N+2)} + \mathcal{O}\left(\frac{1}{N^4}\right).$$

It follows after a short calculation that the left-hand side of (33) has the following expansion:

$$C(m,m)\frac{2^m}{(m+1)!}\left(\frac{1}{\alpha_m}N^m + \frac{a_1(m)}{\alpha_m}N^{m-1} + \left(\frac{a_2(m)}{\alpha_m} - \frac{m(m-1)}{\alpha_m^3}\right)N^{m-2}\right)$$
$$+ C(m,m-1)\frac{2^{m-1}}{m!}\frac{1}{\alpha_m^2}N^{m-2} + \mathcal{O}(N^{m-3}),$$

where

$$a_1(m) := \sum_{0\le j\le m} j = \frac{1}{2}m(m+1),$$

$$a_2(m) := \sum_{0\le i<j\le m} ij = \frac{1}{24}(m+1)m(m-1)(m-2)(3m+2).$$

Now we expand the right-hand side of (33) to obtain

$$\begin{aligned}\frac{1}{m!}N^m &+ \left(\frac{a_1(m-1)}{m!} + \frac{1}{(m-1)!}\right)N^{m-1}\\ &+ \left(\frac{a_2(m-1)}{m!} + \frac{a_1(m-1)}{(m-1)!} + \frac{1}{(m-2)!}\right)N^{m-2}\\ &+ \mathcal{O}(N^{m-3}).\end{aligned}$$

By comparing the coefficients of N^m (or those of N^{m-1}) we obtain

$$C(m,m) = \frac{m+1}{2^m}\alpha_m.$$

By comparing the coefficients of N^{m-2} we get, after a short calculation,

$$\begin{aligned}C(m,m-1) = \frac{\mathcal{O}^2_{m-1}}{\mathcal{O}^2_m 2^{m-3}}\Bigg(&a_2(m-1) - a_2(m) + ma_1(m-1)\\ &+ m(m-1) + \frac{m(m-1)\mathcal{O}^2_m}{4\mathcal{O}^2_{m-1}}\Bigg),\end{aligned}$$

and simplifying this expression, the claimed result follows. □

Finding a closed form for all coefficients $C(m,k)$ remains a challenging task.

Acknowledgment. We thank Dennis Amelunxen for pointing out an error in a previous version in the paper.

REFERENCES

[1] Agmon, S. (1954). The relaxation method for linear inequalities. *Canad. J. Math.* **6** 382–392. MR0062786

[2] Bürgisser, P. and Amelunxen, D. (2008). Uniform smoothed analysis of a condition number for linear programming. Accepted for *Math. Program. A.* Available at arXiv:0803.0925.

[3] Cheung, D. and Cucker, F. (2001). A new condition number for linear programming. *Math. Program.* **91** 163–174. MR1865268

[4] Cheung, D. and Cucker, F. (2002). Probabilistic analysis of condition numbers for linear programming. *J. Optim. Theory Appl.* **114** 55–67. MR1910854

[5] Cheung, D., Cucker, F. and Hauser, R. (2005). Tail decay and moment estimates of a condition number for random linear conic systems. *SIAM J. Optim.* **15** 1237–1261. MR2178497

[6] Cucker, F. and Peña, J. (2002). A primal-dual algorithm for solving polyhedral conic systems with a finite-precision machine. *SIAM J. Optim.* **12** 522–554. MR1885574

[7] Cucker, F. and Wschebor, M. (2002). On the expected condition number of linear programming problems. *Numer. Math.* **94** 419–478. MR1981163

[8] Dunagan, J., Spielman, D. A. and Teng, S.-H. (2009). Smoothed analysis of condition numbers and complexity implications for linear programming. *Math. Programming*. To appear. Available at http://arxiv.org/abs/cs/0302011v2.

[9] Dvoretzky, A. (1956). On covering a circle by randomly placed arcs. *Proc. Natl. Acad. Sci. USA* **42** 199–203. MR0079365

[10] Gilbert, E. N. (1965). The probability of covering a sphere with N circular caps. *Biometrika* **52** 323–330. MR0207005

[11] Goffin, J.-L. (1980). The relaxation method for solving systems of linear inequalities. *Math. Oper. Res.* **5** 388–414. MR594854

[12] Hall, P. (1985). On the coverage of k-dimensional space by k-dimensional spheres. *Ann. Probab.* **13** 991–1002. MR799434

[13] Hall, P. (1988). *Introduction to the Theory of Coverage Processes*. Wiley, New York. MR973404

[14] Hauser, R. and Müller, T. (2009). Conditioning of random conic systems under a general family of input distributions. *Found. Comput. Math.* **9** 335–358. MR2496555

[15] Janson, S. (1986). Random coverings in several dimensions. *Acta Math.* **156** 83–118. MR822331

[16] Kahane, J.-P. (1959). Sur le recouvrement d'un cercle par des arcs disposés au hasard. *C. R. Math. Acad. Sci. Paris* **248** 184–186. MR0103533

[17] Miles, R. E. (1968). Random caps on a sphere. *Ann. Math. Statist.* **39** 1371.

[18] Miles, R. E. (1969). The asymptotic values of certain coverage probabilities. *Biometrika* **56** 661–680. MR0254953

[19] Miles, R. E. (1971). Isotropic random simplices. *Adv. in Appl. Probab.* **3** 353–382. MR0309164

[20] Moran, P. A. P. and Fazekas de St. Groth, S. (1962). Random circles on a sphere. *Biometrika* **49** 389–396. MR0156434

[21] Motzkin, T. S. and Schoenberg, I. J. (1954). The relaxation method for linear inequalities. *Canad. J. Math.* **6** 393–404. MR0062787

[22] Reitzner, M. (2002). Random points on the boundary of smooth convex bodies. *Trans. Amer. Math. Soc.* **354** 2243–2278. MR1885651

[23] Rosenblatt, F. (1962). *Principles of Neurodynamics. Perceptrons and the Theory of Brain Mechanisms*. Spartan Books, Washington, DC. MR0135635

[24] Santaló, L. A. (1976). *Integral Geometry and Geometric Probability*. Addison-Wesley, Reading, MA. MR0433364

[25] Siegel, A. F. (1979). Asymptotic coverage distributions on the circle. *Ann. Probab.* **7** 651–661. MR537212

[26] Siegel, A. F. and Holst, L. (1982). Covering the circle with random arcs of random sizes. *J. Appl. Probab.* **19** 373–381. MR649974

[27] Solomon, H. (1978). *Geometric Probability*. SIAM, Philadelphia, PA. MR0488215

[28] Stevens, W. L. (1939). Solution to a geometrical problem in probability. *Ann. Eugenics* **9** 315–320. MR0001479

[29] Wendel, J. G. (1962). A problem in geometric probability. *Math. Scand.* **11** 109–111. MR0146858

[30] Whitworth, W. A. (1965). *DCC Exercises in Choice and Chance*. Dover, New York.

[31] Zähle, M. (1990). A kinematic formula and moment measures of random sets. *Math. Nachr.* **149** 325–340. MR1124814

P. Bürgisser
Institute of Mathematics
University of Paderborn
33098 Paderborn
Germany
E-mail: pbuerg@upb.de

F. Cucker
Department of Mathematics
City University of Hong Kong
Kowloon Tong
Hong Kong
E-mail: macucker@cityu.edu.hk

M. Lotz
Mathematical Institute
University of Oxford
24-29 St. Giles'
Oxford OX1 3LB
England
E-mail: lotz@maths.ox.ac.uk