Smoothed analysis of complex conic condition numbers

Peter Bürgisser[*], Felipe Cucker[†], and Martin Lotz[†]

Abstract. Smoothed analysis of complexity bounds and condition numbers has been done, so far, on a case by case basis. In this paper we consider a reasonably large class of condition numbers for problems over the complex numbers and we obtain smoothed analysis estimates for elements in this class depending only on geometric invariants of the corresponding sets of ill-posed inputs. These estimates are for a version of smoothed analysis proposed in this paper which, to the best of our knowledge, appears to be new. Several applications to linear and polynomial equation solving show that estimates obtained in this way are easy to derive and quite accurate.

1 Introduction

1.1 Conic condition numbers—Main results

A distinctive feature of the computations considered in numerical analysis is that they are affected by errors. A main character in the understanding of the effects of these errors is the *condition number* of the input at hand. This is a positive number which, roughly speaking, quantifies the effects just mentioned when computations are performed with infinite precision but the input has been modified by a small perturbation. It depends only on the data and the problem at hand. The best known condition number is that for matrix inversion and linear equation solving. For a square matrix A it takes the form $\kappa(A) = \|A\|\|A^{-1}\|$ and was independently introduced by Goldstine and von Neumann [39] and Turing [37].

Condition numbers occur in endless instances of round-off analysis. They also appear as a parameter in complexity bounds for a variety of iterative algorithms. Yet, condition numbers are not easily computable. It has even been conjectured [21] that computing the condition number $\mathscr{C}(a)$ for a certain data a is at least as difficult as solving the problem for which a is a data. A way out for this situation is to assume a probability measure on the set of data and to study the condition number of this data as a random variable.

[*]Dept. of Mathematics, University of Paderborn, Germany. Partially supported by DFG grant BU 1371.

[†]Dept. of Mathematics, City University of Hong Kong, Kowloon Tong, Hong Kong. Partially supported by CityU SRG grant 7001860.

The above ideas have been systematized in a number of places. Notably, Blum [3] suggested a complexity theory for numerical algorithms parameterized by a condition number $\mathscr{C}(a)$ of input data (in addition to input size). Then, Smale [30, §1] extended this suggestion by proposing to obtain estimates on the probability distribution of $\mathscr{C}(a)$. Combining both ideas, he argued, one can give probabilistic bounds on the complexity of numerical algorithms.

Classically, probabilistic analysis of condition numbers takes two forms: bounds on the tail of the distribution of $\mathscr{C}(a)$ —showing that it is unlikely that $\mathscr{C}(a)$ will be large— and bounds on the expected value of $\ln(\mathscr{C}(a))$ —estimating the average loss of precision and average running time—. Examples of such results abound for a variety of condition numbers [6, 9, 11, 14, 25, 36].

Recently D. Spielman and S.-H. Teng [31, §3] suggested a new approach to Smale's agenda above. The idea (e.g., for the distribution's tail) is to replace showing that

> "it is unlikely that $\mathscr{C}(a)$ will be large"

by showing that

> "for all a and all slight random perturbation Δa, it is unlikely that $\mathscr{C}(a+\Delta a)$ will be large."

A survey of this approach, called *smoothed analysis*, can be found in [31]. We briefly describe its main features in §1.2.

The goal of this paper is to give bounds for the smoothed analysis (both tail and expected value) for a large class of condition numbers for problems over the complex numbers. We assume our data space is $\mathbb{C}^{p+1}$, endowed with a Hermitian product $\langle\ ,\ \rangle$. We say that $\mathscr{C}$ is a *conic condition number* if there exists an algebraic cone $\Sigma \subset \mathbb{C}^{p+1}$ (the set of *ill-posed inputs*) such that, for all data a,

$$\mathscr{C}(a) = \frac{\|a\|}{\mathsf{dist}(a,\Sigma)},$$

where $\|\ \|$ and dist are the norm and distance induced by $\langle\ ,\ \rangle$, respectively.

As defined above, $\kappa(A)$ is not conic since the operator norm $\|\ \|$ is not induced by a Hermitian product. Replacing this norm by the Frobenius norm $\|\ \|_F$ yields the (commonly considered) version $\kappa_F(A) := \|A\|_F\|A^{-1}\|$ of $\kappa(A)$. The Condition Number Theorem of Eckart and Young [13] then states that $\kappa(A)_F$ is conic (with Σ the set of singular matrices). Other examples can be found in [7], where a certain property (related with the so called level-2 condition numbers) is proved for conic condition numbers. Furthermore, it is argued in [10] that for many problems, their condition number can be bounded by a conic one.

Note that, since Σ is a cone, for all $z \in \mathbb{C}\setminus\{0\}$, $\mathscr{C}(a) = \mathscr{C}(za)$. Hence, we may restrict to data $a \in \mathbb{P}^p := \mathbb{P}^p(\mathbb{C})$ for which the condition number takes the form

$$\mathscr{C}(a) = \frac{1}{d_{\mathbb{P}^p}(a,\Sigma)} \tag{1}$$

where, abusing notation, Σ is interpreted now as a subset of $\mathbb{P}^p$ and $d_{\mathbb{P}^p}$ denotes the projective distance in $\mathbb{P}^p$ (precise definitions follow in §2.1 below). We will denote by $B(a,\sigma)$ the open ball of radius σ around a in $\mathbb{P}^p$ with respect to projective distance.

In what follows we assume Σ is purely dimensional and we write $m = \dim(\Sigma)$. Recall that the degree $\deg(\Sigma)$ of Σ equals (cf. [23])

$$\deg(\Sigma) = \min\{\ell \mid \#(\Sigma \cap \mathbb{P}^{p-m}) \leq \ell \text{ for almost all } \mathbb{P}^{p-m} \subset \mathbb{P}^p\}.$$

Our main result is the following.

Theorem 1.1 *Let $\mathscr{C}$ be a conic condition number with set of ill-posed inputs $\Sigma \subset \mathbb{P}^p$, of pure dimension m, $0 < m < p$. Then, for all $a \in \mathbb{P}^p$, all $\sigma \in (0,1]$, and all $t \geq \frac{p\sqrt{2}}{p-m}$, we have*

$$\operatorname*{Prob}_{z \in B(a,\sigma)} \{\mathscr{C}(z) \geq t\} \leq K(p,m)\deg(\Sigma) \left(\frac{1}{t\sigma}\right)^{2(p-m)} \left(1 + \frac{p}{p-m}\frac{1}{t\sigma}\right)^{2m}$$

and

$$\operatorname*{\mathbf{E}}_{z \in B(a,\sigma)} (\ln \mathscr{C}(z)) \leq \frac{1}{2(p-m)} (\ln K(p,m) + \ln \deg(\Sigma) + 3) + \ln \frac{pm}{p-m} + 2 \ln \frac{1}{\sigma},$$

with the constant $K(p,m) := 2\frac{p^{3p}}{m^{3m}(p-m)^{3(p-m)}}$.

We will devote §3 to derive applications of Theorem 1.1 to some condition numbers which occur in the literature.

In most of our applications, the set of ill-posed inputs Σ is a hypersurface. That is, Σ is the zero set $\mathcal{Z}(f)$ of a nonzero homogeneous polynomial f and thus $\deg(\Sigma)$ is at most the degree of f. In this case, we have the following easy to apply corollary.

Corollary 1.2 *Let $\mathscr{C}$ be a conic condition number with set of ill-posed inputs $\Sigma \subseteq \mathbb{P}^p$. Assume $\Sigma \subseteq \mathcal{Z}(f)$ with $f \in \mathbb{C}[X_0, \ldots, X_p]$ homogeneous of degree d. Then, for all $a \in \mathbb{P}^p$, all $\sigma \in (0,1]$, and all $t \geq p\sqrt{2}$,*

$$\operatorname*{Prob}_{z \in B(a,\sigma)} \{\mathscr{C}(z) \geq t\} \leq 2p^3 e^3 d \left(\frac{1}{t\sigma}\right)^2 \left(1 + p\frac{1}{t\sigma}\right)^{2(p-1)}$$

and

$$\operatorname*{\mathbf{E}}_{z \in B(a,\sigma)} (\ln \mathscr{C}(z)) \leq \frac{7}{2} \ln p + \frac{1}{2} \ln d + 4 + 2 \ln \frac{1}{\sigma}.$$

The main idea towards the proof of Theorem 1.1 is to reformulate the probability distribution of a conic condition number as a geometric problem in a complex projective space. Indeed, for $V \subseteq \mathbb{P}^p$ we denote by $v(V)$ the volume of V, and by

V_ε the ε-tube around V in $\mathbb{P}^p$ (precise definitions follow in §2.1 below). With this notation,

$$\operatorname*{Prob}_{z\in B(a,\sigma)}\left\{\mathscr{C}(z)\geq\frac{1}{\varepsilon}\right\}=\operatorname*{Prob}_{z\in B(a,\sigma)}\{d_{\mathbb{P}^p}(z,\Sigma)\leq\varepsilon\}=\frac{v(\Sigma_\varepsilon\cap B(a,\sigma))}{v(B(a,\sigma))}.$$

The first claim in Theorem 1.1 will thus follow from the following purely geometric statement.

Theorem 1.3 *Let V be a projective variety in $\mathbb{P}^p$ of pure dimension $0<m<p$. Moreover, let $a\in\mathbb{P}^p$, $\sigma\in(0,1]$, and $0<\varepsilon\leq\frac{1}{\sqrt{2}}\frac{p-m}{p}$. Then we have*

$$\frac{v(V_\varepsilon\cap B(a,\sigma))}{v(B(a,\sigma))}\leq K(p,m)\deg(V)\left(\frac{\varepsilon}{\sigma}\right)^{2(p-m)}\left(1+\frac{p}{p-m}\frac{\varepsilon}{\sigma}\right)^{2m}.$$

One of the central tools in the derivation of Theorem 1.3 is integral geometry. An essential formula of integral geometry [22, §15.2] allows to relate the volume of certain geometric objects to the expected volume of their intersection when they are moved at random. A simple application is the equality $v(V)=\deg(V)v(\mathbb{P}^m)$ for the volume of an irreducible m-dimensional subvariety $V\subseteq\mathbb{P}^p$. In order to obtain a corresponding bound for $V_\varepsilon\cap B(a,\sigma)$, a more sophisticated use of this equality is needed (cf. Lemma 2.2).

1.2 Relation to previous work

Let $\mathbb{K}=\mathbb{R}$ or $\mathbb{C}$. In the study of the behaviour of a function $f\colon\mathbb{K}^n\to\mathbb{R}_+$ (e.g., a condition number, a complexity bound) two frameworks have been extensively used: worst-case and average-case. Recently, a third framework has been proposed which arguably blends the best of the former two. The worst-case framework studies the quantity

$$\sup_{a\in\mathbb{K}^n} f(a) \tag{2}$$

and the average-case the quantity

$$\mathop{\mathbf{E}}_{z\in\Psi} f(z)=\int_{z\in\mathbb{K}^n} f(z)\psi(z)dz \tag{3}$$

where $z\in\Psi$ means that the expected value is taken for a random z whose distribution Ψ has density function ψ. The *smoothed analysis* of f studies the behaviour of

$$\sup_{a\in\mathbb{K}^n}\mathop{\mathbf{E}}_{z\in N^n(0,\sigma^2)} f(a+z) \tag{4}$$

(possibly for sufficiently small σ) where $N^n(0,\sigma^2)$ denotes the n-dimensional Gaussian distribution over $\mathbb{K}$ with mean 0 and variance σ^2. Note that while (2) and

(3) usually yield functions on n, (4) yields a function on n and σ. It has been argued that smoothed analysis interpolates between worst and average cases since it amounts to the first for $\sigma = 0$ and it approaches the second for large σ. Instances of smoothed analysis can be found in [8, 12, 31, 32, 33, 42].

When f is homogeneous of degree 0 —e.g., a conic condition number— it makes sense to restrict f to the projective space $\mathbb{P}^{n-1}(\mathbb{K})$. In this case, it also makes sense to replace the distribution $a + N^n(0, \sigma^2)$ by the uniform distribution supported on the disk $B(a, \sigma) \subseteq \mathbb{P}^{n-1}$ and consider, instead of (4), the following quantity

$$\sup_{a \in \mathbb{P}^{n-1}} \mathop{\mathbf{E}}_{z \in B(a,\sigma)} f(z). \tag{5}$$

Note that in this case, the interpolation mentioned above is transparent. When $\sigma = 0$ the expected value amounts to $f(a)$ and we obtain worst-case analysis, while if $\sigma = 1$ (the diameter of $\mathbb{P}^{n-1}$) the expected value is independent of a and we obtain average-case analysis.

It is this version of smoothed analysis we deal with in this paper. To the best of our knowledge it appears here for the first time. Note that while, technically, this "uniform smoothed analysis" differs from the Gaussian one considered so far, both share the viewpoint described in §1.1 above.

We have already mentioned the references [8, 12, 31, 32, 33, 42] as instances of previous work in smoothed analysis. In all these cases, an *ad hoc* argument is used to obtain the desired bounds. This is in contrast with the goal of this paper which is to provide general estimates which can be applied to a large class of condition numbers. We believe the applications in §3 give substance to this goal.

The idea of reformulating probability distributions as quotients of volumes in projective spaces (or spheres) to estimate condition measures goes back at least to Smale [29] and Renegar [20]. In particular, [20] uses this idea to show bounds on the probability distribution of a random variable in the average-case setting. Central to his argument is the fact that this random variable can be bounded by a conic condition number. The set of ill-posed inputs in [20] is a hypersurface. An extension of these results to the case of codimension greater than one was done by Demmel [11] where, in addition, an average-case analysis of several conic condition numbers is performed. Our paper is an extension of these arguments to the smoothed-analysis framework.

In a recent paper, Beltrán and Pardo [1] obtained estimates similar to those proved by Demmel (always for the average-case setting) when the input data a is assumed to belong to a complex projective variety $V \subseteq \mathbb{P}^p$ and averages are taken for the uniform distribution on V. An extension of Theorem 1.1 in this direction is certainly doable, but we have not included it in this paper.

Probably the most important extension of the present paper would be to obtain a result akin to Theorem 1.1 (or Corollary 1.2) for problems defined over the real numbers. For the average-case setting Demmel [11] states such results. Unfortunately, his results directly rely on an unpublished report by Ocneanu dating from

1985, which apparently contains an upper bound on the volume of tubes around a real variety in terms of degrees (cf. Theorem 4.3 in [11]). We are currently working towards an extension to the real case.

2 Proof of Theorem 1.1

2.1 Distances and volumes in projective space

We refer to [4, Chapter 12] for a more detailed introduction to the concepts needed here. A general reference for complex analytic geometry is [16].

The complex projective space $\mathbb{P}^p := \mathbb{P}^p(\mathbb{C})$ is defined as the set of one dimensional complex subspaces of $\mathbb{C}^{p+1}$. The space $\mathbb{P}^p$ carries the structure of a compact $2p$-dimensional real manifold. A Hermitian inner product $\langle\ ,\ \rangle$ on $\mathbb{C}^{p+1}$ induces a Riemannian distance d_R on $\mathbb{P}^p$ (called Fubini-Study distance), which is defined as

$$d_R(x,y) = \arccos \frac{|\langle \overline{x}, \overline{y}\rangle|}{\|\overline{x}\|\,\|\overline{y}\|} \qquad \text{for } x, y \in \mathbb{P}^p,$$

where $\overline{x}, \overline{y}$ are representatives of x and y in $\mathbb{C}^{p+1}$, respectively, and $\|\ \|$ denotes the norm induced by $\langle\ ,\ \rangle$.

The natural projection $\mathbb{R}^{2p+2} \setminus \{0\} \cong \mathbb{C}^{p+1} \setminus \{0\} \to \mathbb{P}^p$ factors through a (everywhere regular) projection $\pi\colon S^{2p+1} \to \mathbb{P}^p$ with fiber S^1. It is easy to check that the restriction of the derivative $d\pi(x)$ to the orthogonal complement of its kernel is orthogonal with respect to the Riemannian metrics on S^{2p+1} and $\mathbb{P}^p$ induced by $\langle\ ,\ \rangle$. By means of the Co-Area formula [4, p. 241], this observation allows to reduce the computation of integrals on $\mathbb{P}^p$ to the computation of integrals on S^{2p+1}. More precisely, for any integrable function $f\colon \mathbb{P}^p \to \mathbb{R}$ and measurable $U \subseteq \mathbb{P}^p$ we have

$$\int_U f\, d\mathbb{P}^p = \frac{1}{2\pi} \int_{\pi^{-1}(U)} f \circ \pi \, dS^{2p+1}, \tag{6}$$

where $d\mathbb{P}^p$ and dS^{2p+1} denote the volume forms induced by $\langle\ ,\ \rangle$.

For an open subset $U \subseteq M$ of an m-dimensional Riemannian manifold, we write $v(U) := \int_U dM$ for the *m-dimensional volume* of U, where dM is the volume form on M induced by the Riemannian metric. In particular, using (6) we get for the complex projective space

$$v(\mathbb{P}^p) = \frac{1}{2\pi} v(S^{2p+1}) = \frac{\pi^p}{p!}. \tag{7}$$

Instead of the Riemannian metric d_R on $\mathbb{P}^p$, we will be working with the associated projective metric $d_{\mathbb{P}^p}$, which is defined as

$$d_{\mathbb{P}^p}(x,y) = \sin d_R(x,y).$$

Unless otherwise stated, this is the distance function we will be using throughout this paper. The use of this distance function is motivated by our applications. In fact, for a conic condition number with ill-posed set $\Sigma \subseteq \mathbb{C}^{p+1}$, $d_{\mathbb{P}^p}(a, \Sigma)$ (recall our abuse of notation in the introduction) just gives the normalized distance of a representative of a to Σ.

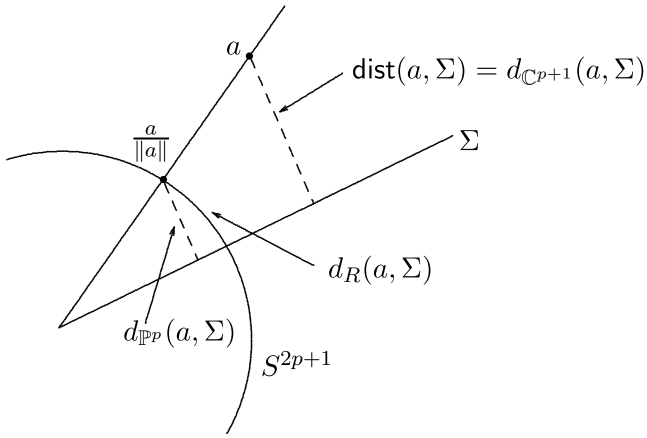

Fig. 1 Three distances

We denote by $B(x, \varepsilon) = B_{\mathbb{P}^p}(x, \varepsilon)$ the open ball of radius ε around x in $\mathbb{P}^p$ (with respect to $d_{\mathbb{P}^p}$), and by $S^p(x, \varepsilon)$ the sphere of radius ε around x. For a subset $V \subseteq \mathbb{P}^p$ we define the *ε-tube* around V in $\mathbb{P}^p$ to be the open set

$$V_\varepsilon := \{x \in \mathbb{P}^p \mid d_{\mathbb{P}^p}(x, V) < \varepsilon\}.$$

We will also use the notation $v_\varepsilon(V) := v(V_\varepsilon)$ for the volume of an ε-tube in $\mathbb{P}^p$ around a subset $V \subseteq \mathbb{P}^p$. If we wish to stress the ambient space in which the tube is considered, we will write $v_\varepsilon^{\mathbb{P}^p}(V)$ instead. We will similarly do so if the ambient space is a sphere.

For a purely m-dimensional subvariety $V \subseteq \mathbb{P}^p$, the set $V \backslash \mathrm{Sing}(V)$ (where $\mathrm{Sing}(V)$ denotes the singular locus of V) is a real $2m$-dimensional Riemannian manifold (with the metric induced from $\mathbb{P}^p$), and we define the volume of V as $v(V) := v(V \backslash \mathrm{Sing}(V))$. This coincides with any other reasonable notion of volume.

Lemma 2.1 *Let $\mathbb{P}^{p-m} \subseteq \mathbb{P}^p$ and let $0 < \varepsilon \leq 1$. Then*

$$v_\varepsilon^{\mathbb{P}^p}(\mathbb{P}^{p-m}) \leq v(\mathbb{P}^{p-m}) v(\mathbb{P}^m) \varepsilon^{2m},$$

with equality if and only if $p - m = 0$. In particular, for the volume of a ball of radius ε around $x \in \mathbb{P}^p$ we have

$$v\left(B_{\mathbb{P}^p}(x, \varepsilon)\right) = v(\mathbb{P}^p) \varepsilon^{2p}.$$

Proof. A ball of radius ε in $\mathbb{P}^p$ with respect to $d_{\mathbb{P}^p}$ corresponds to a ball in $\mathbb{P}^p$ of radius $\delta = \arccos(\varepsilon)$ with respect to d_R. From Equation (6) we get the identity

$$v_\varepsilon^{\mathbb{P}^p}\left(\mathbb{P}^{p-m}\right) = \frac{v_\delta^{S^{2p+1}}\left(S^{2(p-m)+1}\right)}{2\pi}. \tag{8}$$

Recall that on the sphere we use the usual Riemannian metric induced from the ambient space. We have thus reduced our problem to that of computing the volume of a tube around a subsphere of a sphere. Expressions for this volume are straightforward to calculate: for a sphere $S^m \subseteq S^p$ we have

$$v_\delta^{S^p}(S^m) = v(S^m)v(S^{p-m-1})\int_0^\delta \cos(t)^m \sin(t)^{p-m-1}dt.$$

Plugging this into Equation (8) we get

$$\begin{aligned} v_\varepsilon^{\mathbb{P}^p}\left(\mathbb{P}^{p-m}\right) &= \frac{v\left(S^{2(p-m)+1}\right)v\left(S^{2m-1}\right)}{2\pi}\int_0^\delta \cos(t)^{2(p-m)+1}\sin(t)^{2m-1}dt \\ &\stackrel{(7)}{=} 2\pi\, v(\mathbb{P}^{p-m})v(\mathbb{P}^{m-1})\int_0^\delta \cos(t)^{2(p-m)+1}\sin(t)^{2m-1}dt \\ &= 2\pi\, v(\mathbb{P}^{p-m})v(\mathbb{P}^{m-1})\int_0^\varepsilon (1-u^2)^{p-m}u^{2m-1}du, \end{aligned}$$

where in the last step we used the substitution $u = \sin(t)$. For $0 < u \leq 1$ we have $(1-u^2)^{p-m} \leq 1$, with equality if and only if $p - m = 0$. Substituting this bound in the above equation and evaluating the integral, we get

$$v_\varepsilon^{\mathbb{P}^p}\left(\mathbb{P}^{p-m}\right) \leq \frac{2\pi\, v(\mathbb{P}^{p-m})v(\mathbb{P}^{m-1})}{2m}\varepsilon^{2m} = v(\mathbb{P}^{p-m})v(\mathbb{P}^m)\varepsilon^{2m},$$

where we used the fact that $v(\mathbb{P}^m) = v(\mathbb{P}^{m-1})\pi/m$ for the last equality. □

2.2 A fact from integral geometry

We will repeatedly use a variation of a classical formula from integral geometry. Let $M, N \subseteq \mathbb{P}^p$ be submanifolds of (real) dimension $2m$ and $2n$, respectively. The unitary group $G := U(p+1)$ acts transitively on $\mathbb{P}^p$ in a straightforward way. A key result in integral geometry states that the expected volume of the intersection of M with a random translate gN of N satisfies

$$\frac{\mathbf{E}_{g\in G}(v(M \cap gN))}{v(\mathbb{P}^{m+n-p})} = \frac{v(M)v(N)}{v(\mathbb{P}^m)v(\mathbb{P}^n)}. \tag{9}$$

Hereby the expectation is taken with respect to the normalized Haar measure on G. The above equality also holds if M and N are (possibly singular) subvarieties of $\mathbb{P}^p$. Equation (9) is easily derived, using (6), from the corresponding statement in [22, §15.2] for spheres.

2.3 Estimating the volume of patches of projective varieties

The following lemma allows to estimate the volume of the intersection of a projective variety V with a ball in terms of the degree of V and the radius of the ball.

Lemma 2.2 *Let $V \subset \mathbb{P}^p$ be an irreducible m-dimensional projective variety, $a \in \mathbb{P}^p$, $0 < \varepsilon \leq 1$ and $V' = V \cap B_{\mathbb{P}^p}(a, \varepsilon)$. Then*

$$\frac{v(V')}{v(\mathbb{P}^m)} \leq \deg(V) \binom{p}{m} \varepsilon^{2m}.$$

PROOF. Taking $M = \mathbb{P}^{p-m}$ and $N = V'$ in (9) we obtain

$$\frac{v(V')}{v(\mathbb{P}^m)} = \mathbf{E}(|gV' \cap \mathbb{P}^{p-m}|)$$

where the expectation is over all g in the unitary group U_{p+1} taken w.r.t. the normalized Haar measure (so that U_{p+1} has volume 1). Since $|gV' \cap \mathbb{P}^{p-m}| \leq |gV \cap \mathbb{P}^{p-m}| \leq \deg(V)$ for almost all $g \in U_{p+1}$ we obtain

$$\mathbf{E}(|gV' \cap \mathbb{P}^{p-m}|) \leq \deg(V) \operatorname*{Prob}_{g \in U_{p+1}} \{gV' \cap \mathbb{P}^{p-m} \neq \emptyset\}.$$

Since $V' \subseteq B(a, \varepsilon)$ we have

$$\operatorname*{Prob}_{g \in U_{p+1}} \{gV' \cap \mathbb{P}^{p-m} \neq \emptyset\} \leq \operatorname*{Prob}_{g \in U_{p+1}} \{gB(a, \varepsilon) \cap \mathbb{P}^{p-m} \neq \emptyset\} = \frac{v_\varepsilon^{\mathbb{P}^p}(\mathbb{P}^{p-m})}{v(\mathbb{P}^p)}.$$

The statement now follows from Lemma 2.1 using that $v(\mathbb{P}^p) = \frac{\pi^p}{p!}$. □

The following crucial lemma is the only step in our chain of argumentation that fails to be true over $\mathbb{R}$.

Lemma 2.3 [1, Theorem 22] *Let $V \subset \mathbb{P}^p$ be an irreducible projective variety of dimension $m \geq 1$, $y \in V$ and $0 < \varepsilon \leq 1/\sqrt{2}$. Then we have*

$$v(V \cap B_{\mathbb{P}^p}(y, \varepsilon)) \geq \frac{1}{2} v(\mathbb{P}^m) \varepsilon^{2m}.$$ □

2.4 Bounding the expectation

The next result gives a convenient way to bound the expectation of a nonnegative random variable whose tail probabilities can be estimated by some power law.

Proposition 2.4 *Let X be a nonnegative, absolutely continuous, random variable and α, t_0, K be positive constants satisfying* $\text{Prob}\{X \geq t\} \leq Kt^{-\alpha}$ *for all $t \geq t_0$. Then we have*

$$\mathbf{E}(\ln X) \leq \ln t_0 + \frac{1}{\alpha}(\ln K + 1).$$

Moreover, if $t_0 \leq K^{\frac{1}{\alpha}}$ then $\mathbf{E}(\ln X) \leq \frac{1}{\alpha}(\ln K + 1)$.

PROOF. Define the monotonically decreasing function $g : (0, 1) \to \mathbb{R}$ by

$$g(y) = \begin{cases} -\frac{1}{\alpha}\ln\left(\frac{y}{K}\right) & \text{if } y \leq Kt_0^{-\alpha} \\ \ln t_0 & \text{otherwise.} \end{cases}$$

We claim that $\text{Prob}\{\ln X \geq g(y)\} \leq y$ for all $y \in (0, 1)$. Indeed, if $y \leq Kt_0^{-\alpha}$ then there exists $t \geq t_0$ such that $y = Kt^{-\alpha}$. Therefore,

$$g(y) = -\frac{1}{\alpha}\ln\left(\frac{y}{K}\right) = \ln t$$

and

$$\text{Prob}\{\ln X \geq g(y)\} = \text{Prob}\{\ln X \geq \ln t\} = \text{Prob}\{X \geq t\} \leq Kt^{-\alpha} = y.$$

If, instead, $y > Kt_0^{-\alpha}$ then

$$\text{Prob}\{\ln X \geq g(y)\} = \text{Prob}\{\ln X \geq \ln t_0\} = \text{Prob}\{X \geq t_0\} \leq Kt_0^{-\alpha} < y.$$

Using [4, Prop. 2, Ch. 11] it follows that

$$\begin{aligned}
\mathbf{E}(\ln X) &\leq \int_0^1 g(y)dy \\
&= -\int_0^{Kt_0^{-\alpha}} \frac{1}{\alpha}\ln(y/K)dy + \int_{Kt_0^{-\alpha}}^1 \ln t_0 \, dy \\
&\leq -\int_0^1 \frac{1}{\alpha}\ln(y/K)\, dy + \int_0^1 \ln t_0 \, dy \\
&= \frac{1}{\alpha}y(\ln y - 1)\Big|_1^0 + \frac{1}{\alpha}\ln K + \ln t_0 \\
&= \frac{1}{\alpha}(1 + \ln K) + \ln t_0.
\end{aligned}$$

If $t_0 \leq K^{\frac{1}{\alpha}}$ then $Kt_0^{-\alpha} \geq 1$ and the integral above has only its first term. □

2.5 Proof of main results

Proof of Theorem 1.3. It is sufficient to prove the assertion for an irreducible V. In order to see this recall that $\deg(V) = \deg(V_1) + \cdots + \deg(V_q)$, where $V_1, \ldots, V_q$ are the irreducible components of V which we assume to be all of the same dimension.

So we assume that V is irreducible. We follow the arguments in [1, Proof of Theorem 16]. Fix $\varepsilon_1 \in (0, 1]$ such that $0 < \varepsilon_1 - \varepsilon \leq \frac{1}{\sqrt{2}}$ (we will specify ε_1 later). For each $z \in V_\varepsilon$ there exists $y \in V$ such that $d_{\mathbb{P}^p}(z, y) \leq \varepsilon$ and hence $B(y, \varepsilon_1 - \varepsilon) \subseteq B(z, \varepsilon_1)$.

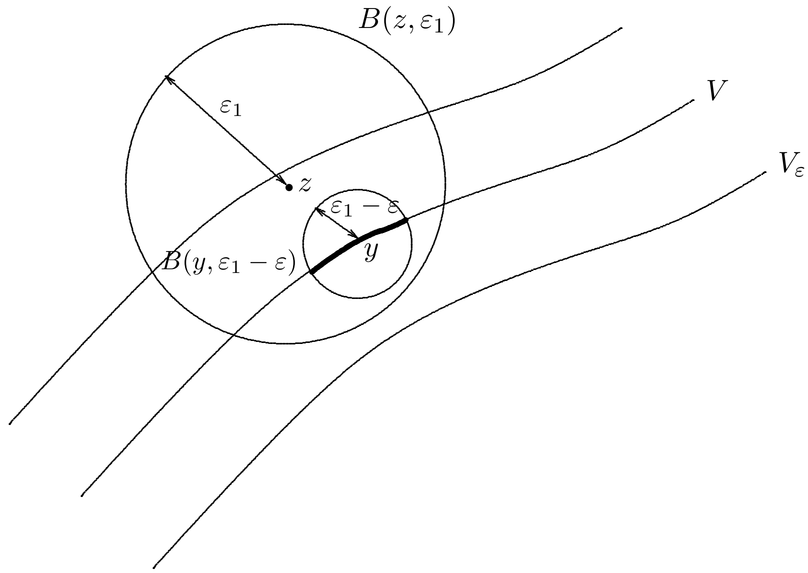

Fig. 2 The thick curve segment is $V \cap B(y, \varepsilon_1 - \varepsilon)$

Since $\varepsilon_1 - \varepsilon \leq \frac{1}{\sqrt{2}}$ we may use Lemma 2.3 to obtain

$$v(V \cap B(z, \varepsilon_1)) \geq v(V \cap B(y, \varepsilon_1 - \varepsilon)) \geq \frac{1}{2} v(\mathbb{P}^m)(\varepsilon_1 - \varepsilon)^{2m}. \tag{10}$$

In order to estimate $v(V_\varepsilon \cap B(a, \sigma))$ we put $V' := V \cap B(a, \sigma + \varepsilon_1)$ and note that $V \cap B(z, \varepsilon_1) \subseteq V'$ for all $z \in V_\varepsilon \cap B(a, \sigma)$.

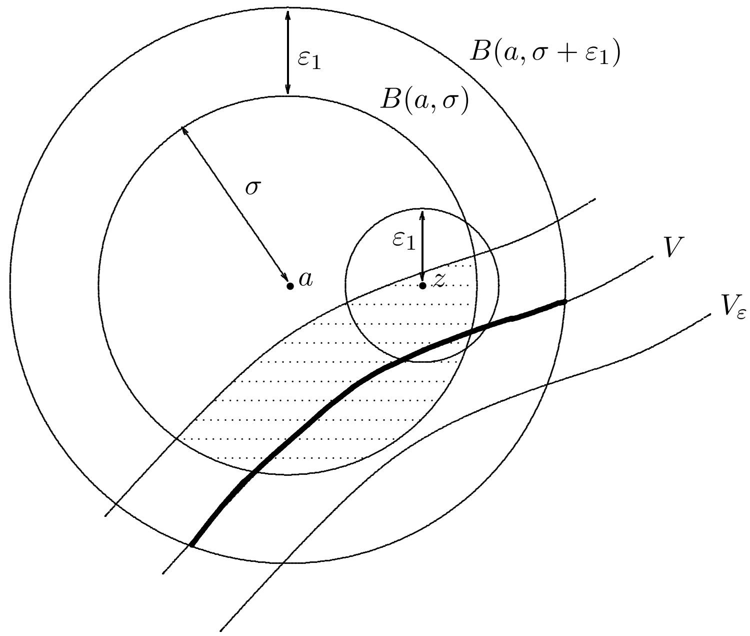

Fig. 3 The thick curve segment is $V' = V \cap B(a, \sigma + \varepsilon_1)$ and the shaded region is $V_\varepsilon \cap B(a, \sigma)$

Using (10) we have

$$\begin{aligned}\frac{v(V_\varepsilon \cap B(a,\sigma))}{v(\mathbb{P}^p)} &= \frac{1}{v(\mathbb{P}^p)} \int_{z \in V_\varepsilon \cap B(a,\sigma)} 1\, dz \\ &\leq \frac{1}{v(\mathbb{P}^p)} \int_{z \in V_\varepsilon \cap B(a,\sigma)} \frac{2\, v(V \cap B(z,\varepsilon_1))}{v(\mathbb{P}^m)(\varepsilon_1 - \varepsilon)^{2m}} dz \\ &\leq \frac{2}{v(\mathbb{P}^m)(\varepsilon_1 - \varepsilon)^{2m}} \frac{1}{v(\mathbb{P}^p)} \int_{z \in \mathbb{P}^p} v(V' \cap B(z,\varepsilon_1)) dz.\end{aligned}$$

In addition,

$$\begin{aligned}\frac{1}{v(\mathbb{P}^p)} \int_{z \in \mathbb{P}^p} v(V' \cap B(z,\varepsilon_1)) dz &= \int_{g \in U_{p+1}} v(V' \cap B(gz_0, \varepsilon_1)) dg \\ &\overset{(9)}{=} v(\mathbb{P}^m) \frac{v(V')}{v(\mathbb{P}^m)} \frac{v(B(z_0,\varepsilon_1))}{v(\mathbb{P}^p)},\end{aligned}$$

where z_0 is any point in $\mathbb{P}^p$ and the second equality follows from (9). Using Lemma 2.1 we conclude that

$$\frac{1}{v(\mathbb{P}^p)} \int_{z \in \mathbb{P}^p} v(V' \cap B(z,\varepsilon_1)) dz = v(V') \varepsilon_1^{2p}.$$

On the other hand, by Lemma 2.2, we have

$$\frac{v(V')}{v(\mathbb{P}^m)} \leq \deg(V) \binom{p}{m} (\sigma + \varepsilon_1)^{2m}$$

since $V' = V \cap B(a, \sigma + \varepsilon_1)$. Combining all the above we get the estimate

$$\frac{v(V_\varepsilon \cap B(a,\sigma))}{v(\mathbb{P}^p)} \leq \frac{2}{(\varepsilon_1 - \varepsilon)^{2m}} \frac{v(V')}{v(\mathbb{P}^m)} \varepsilon_1^{2p} \leq \frac{2\varepsilon_1^{2p}}{(\varepsilon_1 - \varepsilon)^{2m}} \deg(V) \binom{p}{m} (\sigma + \varepsilon_1)^{2m}.$$

Using again $v(B(a,\sigma)) = v(\mathbb{P}^p)\sigma^{2p}$ it follows that

$$\frac{v(V_\varepsilon \cap B(a,\sigma))}{v(B(a,\sigma))} \leq \frac{2}{(\varepsilon_1 - \varepsilon)^{2m}} \left(\frac{\varepsilon_1}{\sigma}\right)^{2p} \deg(V) \binom{p}{m} (\sigma + \varepsilon_1)^{2m}.$$

We finally choose $\varepsilon_1 := \frac{p}{p-m}\varepsilon$. Note that then

$$\varepsilon_1 - \varepsilon = \frac{m}{p-m}\varepsilon \leq \frac{1}{\sqrt{2}}$$

as we needed, the inequality since $\varepsilon \leq \frac{1}{\sqrt{2}}\frac{p-m}{m}$. We obtain

$$\frac{v(V_\varepsilon \cap B(a,\sigma))}{v(B(a,\sigma))} \leq \frac{2p^{2p}}{m^{2m}(p-m)^{2(p-m)}} \binom{p}{m} \deg(V) \left(\frac{\varepsilon}{\sigma}\right)^{2(p-m)} \left(1 + \frac{p}{p-m}\frac{\varepsilon}{\sigma}\right)^{2m}.$$

Taking into account the estimate $\binom{p}{m} \leq \frac{p^p}{m^m(p-m)^{p-m}}$ (which readily follows from the binomial expansion of $p^p = (m + (p-m))^p$) we finish the proof. □

Proof of Theorem 1.1. The inequality for the tail follows directly from Theorem 1.3. For the expectation estimate, let $\varepsilon_0 := \frac{p-m}{pm}\sigma$ and $t_0 := \varepsilon_0^{-1}$. Note that, for $\varepsilon \leq \varepsilon_0$,

$$\left(1 + \frac{p}{p-m}\frac{\varepsilon}{\sigma}\right)^{2m} \leq \left(1 + \frac{1}{m}\right)^{2m} \leq e^2$$

and thus

$$\frac{v(V_\varepsilon \cap B(a,\sigma))}{v(B(a,\sigma))} \leq K(p,m)\deg(\Sigma) \left(\frac{\varepsilon}{\sigma}\right)^{2(p-m)} e^2.$$

Therefore, for all $t \geq t_0$, writing $\varepsilon = 1/t$,

$$\begin{aligned}
\operatorname*{Prob}_{z \in B(a,\sigma)} \{\mathscr{C}(z) \geq t\} &= \operatorname*{Prob}_{z \in B(a,\sigma)} \{d(z, \Sigma) \leq \varepsilon\} \\
&= \frac{v(V_\varepsilon \cap B(a,\sigma))}{v(B(a,\sigma))} \\
&\leq K(p,m)\deg(\Sigma) \left(\frac{1}{\sigma}\right)^{2(p-m)} e^2 t^{-2(p-m)}.
\end{aligned}$$

A straightforward application of Proposition 2.4 yields

$$\operatorname*{\mathbf{E}}_{z \in B(a,\sigma)} (\ln \mathscr{C}(z)) \leq \frac{1}{2(p-m)} (\ln K(p,m) + \ln\deg(\Sigma) + 3) + \ln\frac{pm}{p-m} + 2\ln\frac{1}{\sigma}.$$

□

Proof of Corollary 1.2. Put $\Sigma' = \mathcal{Z}(f)$ and note that $\mathscr{C}(a) = \frac{1}{d_{\mathbb{P}^p}(a,\Sigma)} \leq \frac{1}{d_{\mathbb{P}^p}(a,\Sigma')}$. The assertion follows from Theorem 1.1 applied to Σ' and the inequality

$$K(p,p-1) = 2\frac{p^{3p}}{(p-1)^{3p-3}}p = 2\left[\left(1+\frac{1}{p-1}\right)^{p-1}\right]^3 p^3 \leq 2e^3p^3. \qquad \square$$

3 Some Applications

In this section we obtain smooth analysis estimates for the condition numbers of four problems: linear equation solving, Moore-Penrose inversion, eigenvalue computations, and polynomial equation solving. For the first two, instances of such analysis already exist and we therefore compare our results with those in the literature. The following differences, however, should be noted. Firstly, these analyses were done for problems over the reals. Secondly, they hold within the Gaussian framework for smoothed analysis described in §1.2. The first feature is not important since a cursory look at the refered proofs shows that similar results hold for complex matrices. One should though keep in mind the second.

3.1 Linear equation solving

The first natural application of our result is for the classical condition number $\kappa(A)$. In [42], M. Wschebor showed (solving a conjecture posed in [31]) that, for all $n \times n$ real matrices M with $\|M\| \leq 1$, all $0 < \sigma \leq 1$ and all $t > 0$

$$\operatorname*{Prob}_{E \in N^{n^2}(0,\sigma^2)} (\kappa(M+E) \geq t) \leq \frac{Kn}{\sigma t}$$

with K a universal constant. Note that, by Proposition 2.4, this implies

$$\operatorname*{\mathbf{E}}_{E \in N^{n^2}(0,\sigma^2)} (\ln \kappa(M+E)) \leq \ln n + \ln\frac{1}{\sigma} + \ln K + 1.$$

We next compare Wschebor's result with what can be obtained from Corollary 1.2. To do so, we first note that, for $A \in \mathbb{C}^{n \times n}$,

$$\kappa(A) = \|A\|\|A^{-1}\| \leq \|A\|_F\|A^{-1}\| =: \kappa_F(A)$$

and that, by the Condition Number Theorem of Eckart and Young [13] (see also [4, Theorem 1, Chapter 11]), $\|A^{-1}\| = d_F(A,\Sigma)^{-1}$. Here $\| \,\|_F$ and d_F are the Frobenius norm and distance in $\mathbb{C}^{n\times n}$ which are induced by the Hermitian product $(A,B) \mapsto \mathsf{trace}(AB^*)$. It follows that $\kappa_F(A)$ is conic. We can thus give upper bounds for $\kappa_F(A)$ and they will hold as well for $\kappa(A)$.

Proposition 3.1 *For all $n \geq 1$, $0 < \sigma \leq 1$, and $M \in \mathbb{C}^{n\times n}$ we have*

$$\mathop{\mathbf{E}}_{A\in B(M,\sigma)}(\ln \kappa_F(A)) \leq \frac{15}{2}\ln n + 2\ln\left(\frac{1}{\sigma}\right) + 4,$$

where the expectation is over all A uniformly distributed in the disk of radius σ centered at M in projective space $\mathbb{P}^{n^2-1}$ (recall that we always use the projective and not the Riemannian distance).

PROOF. The variety Σ of singular matrices is a hypersurface in $\mathbb{P}^{n^2-1}$ of degree n. We now apply Corollary 1.2. □

Note, the bound in Proposition 3.1 is of the same order of magnitude than Wschebor's, worse by just a constant factor. On the other hand, its derivation from Corollary 1.2 is rather immediate. We next extend this bound to rectangular matrices.

3.2 Moore-Penrose inversion

Let $\ell \geq n$ and consider the space $\mathbb{C}^{\ell\times n}$ of $\ell \times n$ rectangular matrices. Denote by $\Sigma \subset \mathbb{C}^{\ell\times n}$ the subset of rank-deficient matrices. Let $A \notin \Sigma$ and let $A^\dagger$ denote its Moore-Penrose inverse (see, e.g., [2, 5]). The condition number of A (for the computation of $A^\dagger$) is defined as

$$\mathsf{cond}^\dagger(A) = \lim_{\varepsilon\to 0}\sup_{\|\Delta A\|_2\leq\varepsilon}\frac{\|(A+\Delta A)^\dagger - A^\dagger\|_2\|A\|_2}{\|A^\dagger\|_2\|\Delta A\|_2}.$$

This is not a conic condition number but it happens to be close to one. One defines $\kappa^\dagger(A) = \|A\|_2\|A^\dagger\|_2$ and, since $\|A^\dagger\|_2 = \mathsf{dist}(A,\Sigma)^{-1}$ [15], we obtain

$$\kappa^\dagger(A) = \frac{\|A\|_2}{\mathsf{dist}(A,\Sigma)}.$$

In addition (see [34, §III.3]),

$$\kappa^\dagger(A) \leq \mathsf{cond}^\dagger(A) \leq \frac{1+\sqrt{5}}{2}\kappa^\dagger(A).$$

Thus, $\ln(\mathsf{cond}^\dagger(A))$ differs from $\ln(\kappa^\dagger(A))$ just by a small additive constant. As for square matrices, $\kappa^\dagger(A)$ is not conic since the operator norm is not induced by a Hermitian product in $\mathbb{C}^{\ell\times n}$. But, again, we can bound $\kappa^\dagger(A)$ by the conic condition number $\kappa^\dagger_F(A) := \|A\|_F\|A^\dagger\|$.

A smoothed analysis for $\kappa^\dagger(A)$ was performed in [8]. Computer experiments reported in that paper, however, suggest that the exhibited bounds, while sharp when ℓ is close to n, are not so for more elongated matrices. Actually, an empirical average $\mathbf{Avr}(\ln\kappa^\dagger(A))$ was computed for several pairs (n,ℓ) and matrices of the form $A = M + \Delta$ with M a fixed ill-posed matrix and Δ a small perturbation. It was then mentioned [8, §7] that "one sees that when one fixes n and lets ℓ increase the quantity $\mathbf{Avr}(\ln\kappa^\dagger(A))$ decreases. This is in contrast with the behaviour of [our bound]. It appears that our methods are not sharp enough to capture the behaviour of $\mathbf{E}(\ln\kappa^\dagger(A))$." As we next see, the bounds following from Theorem 1.1 capture this behaviour much better.

The bound shown in [8] is of the form

$$\sup_{A\in\mathbb{R}^{\ell\times n}} \mathop{\mathbf{E}}_{E\in N^{\ell n}(0,\sigma)} (\ln\kappa^\dagger(A+E)) \le \mathcal{O}\left(\ln\ell + \ln\frac{1}{\sigma}\right). \tag{11}$$

It depends on ℓ and tends to ∞ when ℓ does so. Our next result shows that for large ℓ, the expected value above (now with respect to uniform perturbations) is bounded by an expression depending only on n and σ.

Proposition 3.2 *For all $n \ge 1$ and $0 < \sigma \le 1$ we have*

$$\limsup_{\ell\to\infty} \sup_{M\in\mathbb{P}^{\ell n-1}} \mathop{\mathbf{E}}_{A\in B(M,\sigma)} (\ln\kappa_F^\dagger(A)) \le \left(n+\frac{3}{2}\right)\ln(n) + n\ln 2 + 2 + (n+1)\ln\frac{1}{\sigma}.$$

PROOF. It is well known that (the image in $\mathbb{P}^{n\ell-1}(\mathbb{C})$ of) Σ is a projective variety of codimension $\ell-n+1$ and degree $\binom{\ell}{n-1}$ (see [17, Examples 12.1 and 19.10]). By Theorem 1.1, for all $M\in\mathbb{P}^p$ and $t\ge t_0=1$

$$\begin{aligned}\mathop{\mathrm{Prob}}_{A\in B(M,\sigma)}\{\kappa_F^\dagger(A)\ge t\} &\le K(p,m)\deg(\Sigma)\left(\frac{1}{t\sigma}\right)^{2(p-m)}\left(1+\frac{p}{p-m}\frac{1}{t\sigma}\right)^{2m}\\ &\le K(p,m)\deg(\Sigma)\left(\frac{1}{t\sigma}\right)^{2(p-m)}\left(\frac{2p}{\sigma(p-m)}\right)^{2m}\end{aligned}$$

with

$$p=\ell n-1,\qquad m=\ell n-\ell+n-2,\qquad \text{and}\qquad \deg(\Sigma)=\binom{\ell}{n-1}.$$

Therefore, by Proposition 2.4,

$$\mathop{\mathbf{E}}_{A\in B(M,\sigma)}(\ln\kappa_F^\dagger(A)) \le \frac{1}{2(p-m)}\ln\left(K(p,m)\deg(\Sigma)\left(\frac{2p}{\sigma(p-m)}\right)^{2m}+1\right)+\ln\frac{1}{\sigma}.$$

We next bound the logarithms of the expressions inside the parenthesis.

To bound the binomial coefficients we use the following estimates (see [38, (1.4.5)])

$$\ln\binom{p}{m} \le \ln\frac{p^p}{m^m(p-m)^{(p-m)}} \le p\,\mathrm{H}\left(\frac{m}{p}\right),$$

where H denotes the binomial entropy function defined by $\mathrm{H}(z) = -z\ln z - (1-z)\ln(1-z)$ for $z \in (0,1)$. Note that H is monotonically increasing on $(0, \frac{1}{2})$ and $\mathrm{H}(z) = \mathrm{H}(1-z)$ for $z \in (0,1)$.

It will be convenient to use the asymptotic notations $f(n,\ell) \sim g(n,\ell)$ and $f(n,\ell) \lesssim g(n,\ell)$ to express that $\lim_{\ell\to\infty} \frac{f(n,\ell)}{g(n,\ell)} = 1$ and $\limsup_{\ell\to\infty} \frac{f(n,\ell)}{g(n,\ell)} \le 1$, respectively.

We obtain

$$p\,\mathrm{H}\Big(\frac{m}{p}\Big) = p\,\mathrm{H}\Big(\frac{p-m}{p}\Big) \le p\,\mathrm{H}\Big(\frac{\ell-n+1}{\ell n-1}\Big) \sim \ell n\,\mathrm{H}\Big(\frac{1}{n}\Big) \le \ell(1+\ln n)$$

using

$$\mathrm{H}\Big(\frac{1}{n}\Big) = \frac{1}{n}\ln n + \frac{n-1}{n}\ln\frac{n}{n-1} \le \frac{1}{n}(1+\ln n).$$

Hence $\ln K(p,m) \simeq 3\ell(1+\ln n)$. Similarly,

$$\ln\deg(\Sigma) = \ln\binom{\ell}{n-1} \le \ell\, H\Big(\frac{n}{\ell}\Big) \lesssim n\ln\frac{\ell}{n}.$$

Finally,

$$2m\ln\left(\frac{2p}{\sigma(p-m)}\right) \simeq 2\ell n(\ln n + \ln\frac{2}{\sigma}).$$

Therefore,

$$\begin{aligned}
&\sup_{M\in\mathbb{P}^{\ell n-1}} \mathop{\mathbf{E}}_{A\in B(M,\sigma)} (\ln \kappa_F^{\dagger}(A)) \\
&\qquad\lesssim \frac{1}{2\ell}\left(3\ell(1+\ln n) + n\ln\left(\frac{\ell}{n}\right) + 2\ell n\left(\ln n + \ln\frac{2}{\sigma}\right)\right) + \ln\frac{1}{\sigma} \\
&\qquad\le \left(n+\frac{3}{2}\right)\ln n + (n+1)\ln\frac{1}{\sigma} + n\ln 2 + 2,
\end{aligned}$$

which shows the claim. □

Remark 3.3 The bound in Proposition 3.2 is independent of ℓ. Yet, its dependance on n is linear and the term on $\ln\frac{1}{\sigma}$ is multiplied by a factor n. This is too large a bound. We now note that bounds such as (11) also follow from our results. For a very short derivation, note that if a matrix A is rank deficient then, $\det(\overline{A}) = 0$ where $\overline{A}$ is the $n\times n$ matrix obtained by removing all rows of A with index greater than n. Therefore $\Sigma \subseteq \overline{\Sigma} = \{A \in \mathbb{C}^{\ell\times n} \mid \det(\overline{A}) = 0\}$. This implies that, if $\|A\|_F = 1$

$$\kappa_F^{\dagger}(A) \le \frac{1}{d_{\mathbb{P}^{\ell n-1}}(A,\overline{\Sigma})}.$$

Since $\overline{\Sigma}$ is a hypersurface of degree n, an immediate application of Corollary 1.2 yields

$$\sup_{M\in\mathbb{P}^{\ell n-1}} \mathop{\mathbf{E}}_{A\in B(M,\sigma)} (\ln \kappa^{\dagger}(A)) \le \frac{7}{2}\ln\ell + 4\ln n + 4 + 2\ln\left(\frac{1}{\sigma}\right).$$

For small ℓ (say, polynomially bounded in n) this last bound is better than that in Proposition 3.2. We conjecture that an asymptotic bound of the form $\mathcal{O}(\ln(n) + \ln(1/\sigma))$ holds.

3.3 Eigenvalue computations

Let $A \in \mathbb{C}^{n\times n}$ and $\lambda \in \mathbb{C}$ be a simple eigenvalue of $\mathbb{C}$. For any sufficiently small perturbation ΔA there exists a unique eigenvalue $\widetilde{\lambda}$ of $A + \Delta A$ close to λ. It is known [18] that

$$|\lambda - \widetilde{\lambda}| \leq \|P\|\|\Delta A\| + \mathcal{O}(\|\Delta A\|^2) \tag{12}$$

where $P \in \mathbb{C}^{n\times n}$ is the *projection matrix* given by

$$P = (y^H x)^{-1} x y^H.$$

Here x and y are right and left eigenvectors associated to λ, respectively, (i.e., satisfying $Ax = \lambda x$ and $y^H A = \lambda y^H$) and y^H is the transpose conjugate of y. Note that $y^H x$ is a scalar. Furthermore, inequality (12) is sharp in the sense that the factor $\|P\|$ can not be decreased. We can then define

$$\kappa(A, \lambda) := \begin{cases} \|P\| & \text{if } \lambda \text{ is simple} \\ \infty & \text{otherwise} \end{cases}$$

and the (absolute) condition number of A for eigenvalue computations

$$\kappa_{\mathsf{eigen}}(A) := \max_{\lambda} \kappa(A, \lambda),$$

where the maximum is over all the eigenvalues λ of A. Note that $\kappa_{\mathsf{eigen}}(A)$ is homogeneous of degree 0 in A. Also, the set Σ where κ_{eigen} is infinite is the set of matrices having multiple eigenvalues. Finally, Wilkinson [41] proved that

$$\kappa_{\mathsf{eigen}}(A) \leq \frac{\sqrt{2}\|A\|_F}{\mathsf{dist}(A, \Sigma)}. \tag{13}$$

In [11], Demmel used the fact that the right-hand side of (13) is conic to obtain bounds on the tail of $\kappa_{\mathsf{eigen}}(A)$ for random A. We next use it to obtain smoothed analysis estimates.

Proposition 3.4 *For all $n \geq 1$ and $M \in \mathbb{C}^{n\times n}$,*

$$\mathop{\mathbf{E}}_{A\in B(M,\sigma)} (\ln \kappa_{\mathsf{eigen}}(A)) \leq 8 \ln n + 2 \ln \frac{1}{\sigma} + 5.$$

PROOF. Let χ_A be the characteristic polynomial of A. This is a monic polynomial of degree n whose coefficient of degree i is a homogeneous polynomial of degree $n - i$ in the entries of A. Clearly, A has multiple eigenvalues if and only if χ_A

has multiple roots. This happens if and only if the discriminant $\mathsf{disc}(\chi_A)$ of A is zero. The discriminant $\mathsf{disc}(\chi_A)$ is a polynomial in the entries of A, which can be expressed in terms of the eigenvalues $\lambda_1, \ldots, \lambda_n$ of A as follows

$$\mathsf{disc}(\chi_A) = \prod_{i<j} (\lambda_i - \lambda_j)^2.$$

Note that $\alpha\lambda_1, \ldots, \alpha\lambda_n$ are the eigenvalues of αA, for $\alpha \in \mathbb{C}$. Hence

$$\mathsf{disc}(\chi_{\alpha A}) = \prod_{i<j} (\alpha\lambda_i - \alpha\lambda_j)^2 = \alpha^{n^2-n} \prod_{i<j} (\lambda_i - \lambda_j)^2.$$

We conclude that $\mathsf{disc}(\chi_A)$ is homogeneous of degree $n^2 - n$ in the entries of A.

We now apply Corollary 1.2 with $p = n^2 - 1$ and $d = n^2 - n$ to get (use (13))

$$\mathop{\mathbf{E}}_{A \in B(M,\sigma)} (\ln \kappa_{\mathsf{eigen}}(A)) \leq 8 \ln n + 2 \ln \frac{1}{\sigma} + 4 + \frac{1}{2} \ln 2. \qquad \square$$

3.4 Complex polynomial systems

Let $d_1, \ldots, d_n \in \mathbb{N} \setminus \{0\}$. We denote by $\mathcal{H}_{\mathbf{d}}$ the vector space of polynomial systems $f = (f_1, \ldots, f_n)$ with $f_i \in \mathbb{C}[X_0, \ldots, X_n]$ homogeneous of degree d_i, $i = 1, \ldots, n$. For $f, g \in \mathcal{H}_{\mathbf{d}}$ we write

$$f_i(x) = \sum_{\alpha} a^i_\alpha X^\alpha, \quad g_i(x) = \sum_{\alpha} b^i_\alpha X^\alpha,$$

where $\alpha = (\alpha_0, \ldots, \alpha_n)$ is assumed to range over all multi-indices such that $|\alpha| = \sum_{k=0}^n \alpha_k = d_i$ and $X^\alpha := X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$.

The space $\mathcal{H}_{\mathbf{d}}$ is endowed with a Hermitian inner product $\langle f, g \rangle = \sum_{i=1}^n \langle f_i, g_i \rangle$, where

$$\langle f_i, g_i \rangle = \sum_{|\alpha| = d_i} a^i_\alpha \, \overline{b^i_\alpha} \binom{d_i}{\alpha}^{-1}.$$

Here, the bar denotes complex conjugate and the multinomial coefficients are defined by:

$$\binom{d}{\alpha} = \frac{d!}{\alpha_0! \alpha_1! \cdots \alpha_n!}.$$

Note that choosing this Hermitian product amounts to choosing the monomials $\sqrt{\binom{d_i}{\alpha}} X^\alpha$ as orthonormal basis of $\mathcal{H}_{\mathbf{d}}$.

In the case of one variable, this product was introduced by H. Weyl [40]. Its use in computational mathematics goes back at least to Kostlan [19]. Throughout this section, let $\|f\|$ denote the corresponding norm of f. As described in §2.1, the Weyl product defines a Riemannian structure on the corresponding space $\mathbb{P}(\mathcal{H}_{\mathbf{d}})$, with its associated projective distance $d_{\mathbb{P}(\mathcal{H}_{\mathbf{d}})}$.

In a seminal series of papers, M. Shub and S. Smale [24, 25, 26, 28, 27] studied the problem of, given $f \in \mathcal{H}_{\mathbf{d}}$, compute (an approximation of) a zero of f. They proposed an algorithm and studied its complexity in terms of, among other parameters, a condition number $\mu_{\mathrm{norm}}(f)$ for f. We recall its definition (see [4, Chapter 12] for details). For a simple zero $\zeta \in \mathbb{P}^n$ of $f \in \mathcal{H}_{\mathbf{d}}$ one defines

$$\mu_{\mathrm{norm}}(f,\zeta) := \|f\| \left\| (Df(\zeta)_{|T_\zeta})^{-1} \mathsf{diag}(\sqrt{d_1}\|\zeta\|^{d_1-1}, \ldots, \sqrt{d_n}\|\zeta\|^{d_n-1}) \right\|,$$

where $Df(\zeta)_{|T_\zeta}$ denotes restriction of the derivative of $f\colon \mathbb{C}^{n+1} \to \mathbb{C}^n$ at ζ to the tangent space $T_\zeta\mathbb{P}^n = \{v \in \mathbb{C}^{n+1} \mid \langle v, \zeta\rangle = 0\}$ of $\mathbb{P}^n$ at ζ. Note that $\mu_{\mathrm{norm}}(f,\zeta)$ is homogeneous of degree 0 in f and ζ. If f has only simple zeros $\zeta_1, \ldots, \zeta_q$ we define

$$\mu_{\mathrm{norm}}(f) := \max_{i \le q} \mu_{\mathrm{norm}}(f, \zeta_i);$$

otherwise we set $\mu_{\mathrm{norm}}(f) = \infty$. The study of $\mu_{\mathrm{norm}}(f)$ plays a central role in the series of papers above. A main result is the following [25] (see also [4, Theorem 1, Chapter 13]).

Theorem 3.5 *Let $n > 1$. The probability that $\mu_{\mathrm{norm}}(f) > 1/\varepsilon$ for $f \in \mathbb{P}(\mathcal{H}_{\mathbf{d}})$ and $\varepsilon > 0$ is less than or equal to*

$$\varepsilon^4 n^3 (n+1) N(N-1)\mathcal{D}$$

where $\dim \mathcal{H}_{\mathbf{d}} = N + 1$ and $\mathcal{D} = \prod_{i=1}^{n} d_i$ is the Bézout number.

We want to extend Theorem 3.5 to a smoothed analysis of $\mu_{\mathrm{norm}}(f)$. To do so, we first bound $\mu_{\mathrm{norm}}(f)$ by a conic condition number. Let $\Sigma \subset \mathbb{P}(\mathcal{H}_{\mathbf{d}})$ be the discriminant variety, which consists of the systems $f \in \mathbb{P}(\mathcal{H}_{\mathbf{d}})$ having multiple zeros. The Condition Number Theorem [4, §12.4] states that, for a zero $\zeta \in \mathbb{P}^n(\mathbb{C})$ of f,

$$\mu_{\mathrm{norm}}(f,\zeta) = \frac{1}{d_{\mathbb{P}(\mathcal{H}_{\mathbf{d}})}(f, \Sigma \cap V_\zeta)},$$

where $V_\zeta := \{f \in \mathbb{P}(\mathcal{H}_{\mathbf{d}}) \mid f(\zeta) = 0\}$. Therefore,

$$\mu_{\mathrm{norm}}(f) = \max_{i \le q} \mu_{\mathrm{norm}}(f,\zeta_i) = \frac{1}{\min_{i \le q} d_{\mathbb{P}(\mathcal{H}_{\mathbf{d}})}(f, \Sigma \cap V_{\zeta_i})} \le \frac{1}{d_{\mathbb{P}(\mathcal{H}_{\mathbf{d}})}(f, \Sigma)}.$$

We can now proceed with the desired extension.

We identify the f_i with their coefficient vectors in $\mathbb{C}^{N_i}$, where $N_i = \binom{n+d_i}{d_i}$. Set $N = \sum_i N_i - 1$ so that $\Sigma \subset \mathbb{P}^N$. Our next result bounds the degree of Σ. Similar bounds were given in [20, Proposition 6.1].

Lemma 3.6 *The discriminant variety $\Sigma \subset \mathbb{P}^N$ is a hypersurface, defined by a multihomogeneous polynomial of total degree*

$$\left(1 + \left(1 - n + \sum_{i=1}^{n} d_i\right) \sum_{i=1}^{n} \frac{1}{d_i}\right) \mathcal{D} \leq 2n\mathcal{D}^2$$

in the coefficients of $f_1, \ldots, f_n$.

PROOF. Given $n+1$ homogeneous polynomials $f_0, \ldots, f_n$ in $\mathbb{C}[X_0, X_1, \ldots, X_n]$ of degrees d_i, it is known (see [35, §4.2]) that there exists an irreducible polynomial $\mathsf{res}(f_0, \ldots, f_n)$ in the coefficients of the f_i (unique up to a scalar) such that $\mathsf{res}(f_0, \ldots, f_n) = 0$ if and only if the system $f_0 = \cdots f_n = 0$ has a projective solution. (The polynomial res is called the *multivariate resultant.*) Moreover, res is multihomogeneous of degree $\prod_{j \neq i} d_j$ in the coefficients of each f_i.

Now define

$$\delta(f_1, \ldots, f_n) := \mathsf{res}(g, f_1, \ldots, f_n),$$

where $g := \det(df_1, \ldots, df_n, \sum_i X_i dX_i)$. A solution ζ to the system $f = 0$ is degenerate if and only if the $df_i(\zeta)$ are linearly dependent, which is the case if and only if $g(\zeta) = 0$ (here we used Euler's identity, stating that for homogeneous f_i and all $x \in \mathbb{C}^{n+1}$, $df_i(x)$ is orthogonal to x). It follows that $\delta(f_1, \ldots, f_n)$ defines the discriminant variety Σ.

For the degree calculations, note first that $\deg g = 1 + \sum_{i=1}^{n}(d_i - 1) = 1 - n + \sum_{i=1}^{n} d_i$. We thus obtain

$$\deg \delta(f_1, \ldots, f_n) = \mathcal{D} + \deg g \sum_{i=1}^{n} \frac{\mathcal{D}}{d_i} = \mathcal{D}\left(1 + \deg g \sum_{i=1}^{n} d_i\right)$$

as claimed. This degree can be (rather crudely) estimated by $2n\mathcal{D}^2$. □

Theorem 3.7 *For all $f \in \mathbb{P}(\mathcal{H}_{\mathbf{d}})$, all $\sigma \in (0, 1]$, and all $t \geq N\sqrt{2}$ we have*

$$\operatorname*{Prob}_{g \in B(f,\sigma} \{\mu_{\text{norm}}(g) \geq t\} \leq 4N^3 e^3 n \mathcal{D}^2 \left(\frac{1}{t\sigma}\right)^2 \left(1 + N\frac{1}{t\sigma}\right)^{2(N-1)}$$

and

$$\operatorname*{\mathbf{E}}_{g \in B(f,\sigma} (\ln \mu_{\text{norm}}(g)) \leq \frac{7}{2} \ln N + \ln \mathcal{D} + \frac{1}{2} \ln n + 5 + 2 \ln \left(\frac{1}{\sigma}\right).$$

PROOF. It follows from Corollary 1.2 and Lemma 3.6. □

References

[1] C. Beltrán and L.M. Pardo. Upper bounds on the distribution of the condition number of singular matrices. To appear at *Found. Comput. Math.*

[2] A. Ben-Israel and T.N.E. Greville. *Generalized Inverses: Theory and Applications*. Springer-Verlag, 2nd edition, 2003.

[3] L. Blum. Lectures on a theory of computation and complexity over the reals (or an arbitrary ring). In E. Jen, editor, *Lectures in the Sciences of Complexity II*, pages 1–47. Addison-Wesley, 1990.

[4] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer, 1998.

[5] S.L. Campbell and C.D. Meyer. *Generalized Inverse of Linear Transformations*. Pitman, 1979.

[6] D. Cheung and F. Cucker. Probabilistic analysis of condition numbers for linear programming. *Journal of Optimization Theory and Applications*, 114:55–67, 2002.

[7] D. Cheung and F. Cucker. A note on level-2 condition numbers. *J. of Complexity*, 21:314–319, 2005.

[8] F. Cucker, H. Diao, and Y. Wei. Smoothed analysis of some condition numbers. *Numer. Lin. Alg. Appl.*, 13:71–84, 2005.

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

[10] J. Demmel. On condition numbers and the distance to the nearest ill-posed problem. *Numer. Math.*, 51:251–289, 1987.

[11] J. Demmel. The probability that a numerical analysis problem is difficult. *Math. Comp.*, 50:449–480, 1988.

[12] J. Dunagan, D.A. Spielman, and S.-H. Teng. Smoothed analysis of Renegar's condition number for linear programming. Preprint available at `http://theory.lcs.mit.edu/ spielman`, 2003.

[13] C. Eckart and G. Young. The approximation of one matrix by another of lower rank. *Psychometrika*, 1:211–218, 1936.

[14] A. Edelman. Eigenvalues and condition numbers of random matrices. *SIAM J. of Matrix Anal. and Applic.*, 9:543–556, 1988.

[15] G. Golub and C. Van Loan. *Matrix Computations*. John Hopkins Univ. Press, 1989.

[16] P. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley-Interscience [John Wiley & Sons], New York, 1978.

[17] J. Harris. *Algebraic Geometry. A First Course*. Springer-Verlag, 1992.

[18] T. Kato. *Perturbation Theory for Linear Operators*. Springer-Verlag, 1966.

[19] E. Kostlan. On the distribution of the roots of random polynomials. In M. Hirsch, J.E. Marsden, and M. Shub, editors, *From Topology to Computation: Proceedings of the Smalefest*, pages 419–431. Springer-Verlag, 1993.

[20] J. Renegar. On the efficiency of Newton's method in approximating all zeros of systems of complex polynomials. *Math. of Oper. Research*, 12:121–148, 1987.

[21] J. Renegar. Is it possible to know a problem instance is ill-posed? *J. of Complexity*, 10:1–56, 1994.

[22] L. A. Santaló. *Integral geometry and geometric probability.* Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976.

[23] I. R. Shafarevich. *Basic algebraic geometry.* Springer-Verlag, New York, 1974. Translated from the Russian by K. A. Hirsch, Die Grundlehren der mathematischen Wissenschaften, Band 213.

[24] M. Shub and S. Smale. Complexity of Bézout's theorem I: geometric aspects. *J. of the Amer. Math. Soc.*, 6:459–501, 1993.

[25] M. Shub and S. Smale. Complexity of Bézout's theorem II: volumes and probabilities. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 267–285. Birkhäuser, 1993.

[26] M. Shub and S. Smale. Complexity of Bézout's theorem III: condition number and packing. *Journal of Complexity*, 9:4–14, 1993.

[27] M. Shub and S. Smale. Complexity of Bézout's theorem V: polynomial time. *Theor. Comp. Science*, 133:141–164, 1994.

[28] M. Shub and S. Smale. Complexity of Bézout's theorem IV: probability of success; extensions. *SIAM J. of Numer. Anal.*, 33:128–148, 1996.

[29] S. Smale. The fundamental theorem of algebra and complexity theory. *Bull. Amer. Math. Soc.*, 4:1–36, 1981.

[30] S. Smale. Complexity theory and numerical analysis. In A. Iserles, editor, *Acta Numerica*, pages 523–551. Cambridge University Press, 1997.

[31] D.A. Spielman and S.-H. Teng. Smoothed analysis of algorithms. In *Proceedings of the International Congress of Mathematicians*, volume I, pages 597–606, 2002.

[32] D.A. Spielman and S.-H. Teng. Smoothed analysis of termination of linear programming algorithms. *Math. Programm. Series B*, 97:375–404, 2003.

[33] D.A. Spielman and S.-H. Teng. Smoothed analysis: Why the simplex algorithm usually takes polynomial time. *Journal of the ACM*, 51(3):385–463, 2004.

[34] G.W. Stewart and J. Sun. *Matrix Perturbation Theory.* Academic Press, 1990.

[35] B. Sturmfels. *Solving systems of polynomial equations*, volume 97 of *CBMS Regional Conference Series in Mathematics.* Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2002.

[36] M.J. Todd, L. Tunçel, and Y. Ye. Characterizations, bounds and probabilistic analysis of two complexity measures for linear programming problems. *Math. Programm.*, 90:59–69, 2001.

[37] A.M. Turing. Rounding-off errors in matrix processes. *Quart. J. Mech. Appl. Math.*, 1:287–308, 1948.

[38] J.H. van Lint. *Introduction to Coding Theory.* Springer-Verlag, 1999.

[39] J. von Neumann and H.H. Goldstine. Numerical inverting matrices of high order. *Bull. Amer. Math. Soc.*, 53:1021–1099, 1947.

[40] H. Weyl. *The Theory of Groups and Quantum Mechanics.* Dover, New York, 1950.

[41] J. Wilkinson. Note on matrices with a very ill-conditioned eigenproblem. *Numer. Math.*, 19:176–178, 1972.

[42] M. Wschebor. Smoothed analysis of $\kappa(a)$. *J. of Complexity*, 20:97–107, 2004.