Foundations of Computational Mathematics
https://doi.org/10.1007/s10208-019-09414-2

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

The Real Polynomial Eigenvalue Problem is Well Conditioned on the Average

Carlos Beltrán[1] · Khazhgali Kozhasov[2,3,4]

Received: 20 February 2018 / Revised: 10 January 2019 / Accepted: 29 January 2019

Abstract
We study the average condition number for polynomial eigenvalues of collections of matrices drawn from some random matrix ensembles. In particular, we prove that polynomial eigenvalue problems defined by matrices with random Gaussian entries are very well conditioned on the average.

Keywords Condition number · Polynomial eigenvalue problem · Random matrices

Mathematics Subject Classification 14Q20 · 15A18 · 15A22 · 15B52 · 65F15

Introduction

Following the ideas in [3,7,19], we note that many different numerical problems can be described within the following simple general framework. We consider a space of *inputs* and a space of *outputs* denoted by $\mathcal{I}$ and $\mathcal{O}$, respectively, and some equation of

Communicated by Alan Edelman.

Carlos Beltrán was supported by the Spanish “Ministerio de Economía y Competitividad” under Projects MTM2017-83816-P and MTM2017-90682-REDT (Red ALAMA), as well as by the Banco Santander and Universidad de Cantabria under Project 21.SI01.64658.

✉ Khazhgali Kozhasov
kozhasov@mis.mpg.de

Carlos Beltrán
beltranc@unican.es

1 Universidad de Cantabria, Av. de los Castros, s/n 39005, Santander, Spain

2 SISSA, Via Bonomea 265, 34136 Trieste, Italy

3 Max-Planck-Institute for Mathematics in the Sciences, Inselstraße 22, 04103 Leipzig, Germany

4 Present Address: TU Braunschweig, Universitätsplatz 2, 38106 Braunschweig, Germany

Published online: 06 May 2019

the form $ev(i, o) = 0$ stating when an output is a solution for a given input. Both $\mathcal{I}$ and $\mathcal{O}$, and the *solution variety*

$$\mathcal{V} = \{(i, o) \in \mathcal{I} \times \mathcal{O} : o \text{ is an output to } i\} = \{(i, o) \in \mathcal{I} \times \mathcal{O} : ev(i, o) = 0\}$$

are frequently real algebraic or just semialgebraic sets. The numerical problem to be solved can then be written as "given $i \in \mathcal{I}$, find $o \in \mathcal{O}$ such that $(i, o) \in \mathcal{V}$," or "find all $o \in \mathcal{O}$ such that $(i, o) \in \mathcal{V}$." One can have in mind the following examples:

1. Polynomial Root Finding: $\mathcal{I}$ is the set of univariate real polynomials of degree d, $\mathcal{O} = \mathbb{R}$ and $\mathcal{V} = \{(f, \zeta) : f(\zeta) = 0\}$. If we look for, say, the largest real zero, then the solution variety $\mathcal{V} = \{(f, \zeta) : f(\zeta) = 0, \nexists \eta > \zeta : f(\eta) = 0\}$ is semialgebraic.
2. Polynomial System Solving, which we can see as the homogeneous multivariate version of Polynomial Root Finding: $\mathcal{I}$ is the projective space of (dense or structured) systems of n real homogeneous polynomials of degrees $d_1, \dots, d_n$ in variables $x_0, \dots, x_n$, $\mathcal{O} = \mathbb{R}\mathrm{P}^n$ is the real projective space of dimension n and $\mathcal{V} = \{(f, \zeta) : f(\zeta) = 0\}$.
3. EigenValue Problem: $\mathcal{I} = \mathbb{R}^{n \times n}$, $\mathcal{O} = \mathbb{R}$ and $\mathcal{V} = \{(A, \lambda) : \det(A - \lambda \,\mathrm{Id}) = 0\}$.
4. (Homogeneous) Polynomial EigenValue Problem (in the sequel called PEVP): $\mathcal{I}$ is the set of tuples of $d+1$ real $n \times n$ matrices $A = (A_0, \dots, A_d)$, $\mathcal{O} = \mathbb{R}\mathrm{P}^1$ and $\mathcal{V} = \{(A, [\alpha : \beta]) : P(A, \alpha, \beta) = \det(\alpha^0 \beta^d A_0 + \alpha^1 \beta^{d-1} A_1 + \cdots + \alpha^d \beta^0 A_d) = 0\}$. One can force some of the matrices to be symmetric and/or positive definite (which leads to a semialgebraic solution variety), a particularly important case in applications, or consider other structured problems, see [10,13,18,21]. In the cases $d = 1$ and $d = 2$ polynomial eigenvalues are often referred to as *generalized eigenvalues* and *quadratic eigenvalues*, respectively. If $n = 1$, we recover the homogeneous version of 1.

In this paper, we prove a general theorem computing exactly the expected value of the condition number in a wide collection of problems, including problem 4 above.

We start by recalling the general geometric definition of the condition number, which is usually thought of as "a measure of the sensitivity of the solution o under an infinitesimal perturbation of the input i." A *Finsler structure* on a differentiable manifold M is a smooth field of norms $\|\cdot\|_p : T_pM \to \mathbb{R}$, $p \in M$ on M (see [3, p. 223] for more details). In particular, a Riemannian structure $\langle \cdot, \cdot \rangle$ on M defines a Finsler structure on it by $\|\dot{p}\|_p = \sqrt{\langle \dot{p}, \dot{p} \rangle_p}$, $p \in M$, $\dot{p} \in T_pM$.

Definition 1 (*Condition number in the algebraic setting*) Let $\mathcal{I}$, $\mathcal{O}$ and $\mathcal{V} \subseteq \mathcal{I} \times \mathcal{O}$ be real algebraic varieties such that the smooth loci of $\mathcal{I}$, $\mathcal{O}$ are endowed with Finsler structures and let $(i, o) \in \mathcal{V}$ be a smooth point of $\mathcal{V}$ such that $i \in \mathcal{I}$, $o \in \mathcal{O}$ are smooth points of $\mathcal{I}$ and $\mathcal{O}$, respectively. Moreover, assume that $D_{(i,o)} p_1 : T_{(i,o)}\mathcal{V} \to T_i\mathcal{I}$ is invertible. Then, the *condition number* $\mu(i, o)$ of $(i, o) \in \mathcal{V}$ is defined as

$$\mu(i, o) = \left\| D_{(i,o)} p_2 \circ D_{(i,o)} p_1^{-1} \right\|_{\mathrm{op}},$$

where $p_1 : \mathcal{V} \to \mathcal{I},\ p_2 : \mathcal{V} \to \mathcal{O}$ are the projections and $\|\cdot\|_{\text{op}}$ is the operator norm. For points $(i, o) \in \mathcal{V}$ not satisfying the above assumptions, the condition number is set to ∞.

See [7, Sec. 14.1] for more on this geometric approach to the condition number.

Remark 1 Definition 1 is intrinsic in $\mathcal{I}$, i.e., changing $\mathcal{I}$ to some subvariety $\mathcal{I}' \subset \mathcal{I}$ leads (in general) to different, smaller, value of the condition number, since perturbations of the input are only allowed in the direction of the tangent space to the input set. Note also that the condition number depends on choices of Finsler structures on $\mathcal{I}$ and $\mathcal{O}$.

Example 1 The classical Turing's condition number $\mu(A) = \|A\|_{\text{op}}\|A^{-1}\|_{\text{op}}$ for matrix inversion corresponds to the following setting:

- $\mathcal{O} = \mathcal{I} = M(n, \mathbb{R})$ is the set of $n \times n$ real matrices endowed with the Finsler structure associated to relative errors in operator norm: $\|\dot{A}\|_A = \|\dot{A}\|_{\text{op}}/\|A\|_{\text{op}}$.
- $\mathcal{V} = \{(A, B) : AB = \text{Id}\} = \{(A, B) : B = A^{-1}\}$.

In the PEVP, the input space $\mathcal{I}$ is endowed with the following Riemannian structure: $\langle \dot{A}, \dot{B}\rangle_A = ((\dot{A}_0, \dot{B}_0) + \cdots + (\dot{A}_d, \dot{B}_d))/((A_0, A_0) + \cdots + (A_d, A_d))$, where $(\cdot,\cdot)$ is the Frobenius inner product $(A, B) = \text{trace}(B^t A)$, $A = (A_0, \ldots, A_d)$ and $\dot{A} = (\dot{A}_0, \ldots, \dot{A}_d)$, $\dot{B} = (\dot{B}_0, \ldots, \dot{B}_d) \in T_A\mathcal{I}$. The output space $\mathcal{O} = \mathbb{R}\text{P}^1$ possesses the standard metric, and the solution variety $\mathcal{V} = \{(A, [\alpha : \beta]) : P(A, \alpha, \beta) = 0\}$ is endowed with the induced product Riemannian structure. An explicit formula for the condition number for the Homogeneous PEVP was derived in [10, Th. 4.2] (we write here the relative condition number version):

$$\mu(A, (\alpha, \beta)) = \left(\sum_{k=0}^{d} \alpha^{2k}\beta^{2d-2k}\right)^{1/2} \frac{\|r\|\|\ell\|}{|\ell^t v|}\,\|A\|, \tag{1}$$

where $A = (A_0, \ldots, A_d)$, $(\alpha, \beta) \in \mathbb{R}^2$ is a (representative of a) polynomial eigenvalue of A, r and ℓ are the corresponding right and left eigenvectors and

$$v = \beta \frac{\partial}{\partial\alpha} P(A, \alpha, \beta)r - \alpha\frac{\partial}{\partial\beta} P(A, \alpha, \beta)r.$$

A given tuple A can have up to nd real isolated polynomial eigenvalues. We define the condition number of A simply as the sum of the condition numbers over all these PEVs:

$$\mu(A) = \sum_{[\alpha:\beta]\in\mathbb{R}\text{P}^1 \text{is a PEV of } A} \mu(A, (\alpha, \beta)).$$

(If $A = (A_0, \ldots, A_d)$ has infinitely many polynomial eigenvalues, we have $\mu(A) = \infty$). The most important result in this paper is a very general theorem which is designed to provide exact formulas for the expected value of the condition number in the PEVP and other problems. A simple particular case of our general theorem is as follows. We say that a random matrix $A \in M(n, \mathbb{R})$ is $\mathcal{N}_{M(n,\mathbb{R})}$-distributed if the entries of A are i.i.d. standard Gaussian variables, i.e., the probability density function for each entry of A is $(2\pi)^{-1/2}e^{-x^2/2}$.

Theorem 1 (Gaussian Homogeneous PEVP is well conditioned on the average) *If* $A_0, \ldots, A_d \in M(n, \mathbb{R})$ *are independent* $\mathcal{N}_{M(n,\mathbb{R})}$*-distributed matrices, then*

$$\underset{A_0,\ldots,A_d \sim i.i.d. \mathcal{N}_{M(n,\mathbb{R})}}{\mathbb{E}} \mu(A) = \pi \frac{\Gamma\left(\frac{(d+1)n^2}{2}\right)}{\Gamma\left(\frac{(d+1)n^2-1}{2}\right)} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)}$$
$$= \frac{\pi}{2}\sqrt{(d+1)n^3}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right), \quad n \to +\infty \tag{2}$$

In Corollary 3, we provide an analogous formula in the case when $A_0, \ldots, A_d$ are independent GOE(n)-distributed matrices.

Remark 2 Recently in [1] Armentano and the first author of the current article investigated the expectation of the squared condition number for polynomial eigenvalues of complex Gaussian matrices. Theorem 1 establishes the "asymptotic square root law" for the considered problem, i.e., when $n \to +\infty$ (and up to the factor $\pi/2$) our answer in (2) equals the square root of the answer in [1]. See [2,5,8,15,20] for different contexts where a square root law has been established. For an example of a problem where a square root law fails to hold, see [6].

In Sect. 1, we state our main results, of which Theorem 1 is an easy consequence. Their proofs are given in Sect. 3 and in Sect. 4; some technical results are left for Appendix.

1 Main Results

In this section, we state our most general result, from which Theorem 1 will follow. First, let us fix a general framework which analyzes the input–output problems described above in a semialgebraic context. For the rest of this paper, the input and the output sets will be, respectively, the punctured real vector space $\mathcal{I} = \mathbb{R}^m \backslash \{0\}$ and the unit circle $S^1 \subset \mathbb{R}^2$ endowed with the standard Riemannian structures. The solution variety will be a semialgebraic set $\mathcal{S} \subset \mathbb{R}^m \times S^1 \subset \mathbb{R}^m \times \mathbb{R}^2$ (we change letter from $\mathcal{V}$ to $\mathcal{S}$ to remark the fact that it is semialgebraic). We denote by $\mathcal{S}_{\text{top}}$ the union of top-dimensional (smooth) strata of $\mathcal{S}$ (see Sect. 2 for details). Then, the smooth manifold $\mathcal{S}_{\text{top}} \subset \mathbb{R}^m \times S^1$ is endowed with the induced Riemannian product structure. The two projections defined on $\mathcal{S}$ are denoted by $p_1 : \mathcal{S} \to \mathbb{R}^m$, $p_2 : \mathcal{S} \to S^1$.

Definition 2 (*Condition number in the semialgebraic setting*) Let $\mathcal{S} \subseteq \mathbb{R}^m \times S^1$ be any m–dimensional semialgebraic set. Near a regular point $(a, x) \in \mathcal{S}_{\text{top}}$ the first projection $p_1 : \mathcal{S}_{\text{top}} \to \mathbb{R}^m$ is locally invertible, i.e., there exists a neighborhood $U \subset \mathbb{R}^m$ of $a \in U$ and a unique smooth map $p_1^{-1} : U \to \mathcal{S}_{\text{top}}$ such that $p_1^{-1}(a) = (a, x)$ and $p_1 \circ p_1^{-1} = \text{id}_U$. In this case, the *local relative condition number* $\mu(a, x)$ is defined as

$$\mu(a,x) := \|a\| \sup_{\dot{a}\in\mathbb{R}^m\backslash\{0\}} \frac{\|D_a(p_2\circ p_1^{-1})(\dot{a})\|}{\|\dot{a}\|}$$

For points $(a,x)\in\mathcal{S}_{\text{low}}=\mathcal{S}\backslash\mathcal{S}_{\text{top}}$ in the strata of lower dimension of $\mathcal{S}$ as well as for critical points $(a,x)\in\mathcal{S}_{\text{top}}$ of $p_1:\mathcal{S}_{\text{top}}\to\mathbb{R}^m$, we set $\mu(a,x):=\infty$.

The relative condition number $\mu(a)$ of $a\in\mathbb{R}^m$ is defined to be the sum of all local relative condition numbers $\mu(a,x)$:

$$\mu(a) := \sum_{x\in S^1:\,(a,x)\in\mathcal{S}} \mu(a,x)$$

Remark 3 Note that, by convention, if $p_1^{-1}(a)=\emptyset$, that is, if there is no output for $a\in\mathbb{R}^m\backslash\{0\}$, then $\mu(a)=0$. Note also that Definition 2 agrees with Definition 1 if $\mathcal{S}$ is algebraic and we endow the input space $\mathcal{I}=\mathbb{R}^m\backslash\{0\}$ with the Riemannian structure associated to relative errors, that is, $\langle\dot{a},\dot{b}\rangle_a=(\dot{b}^t\dot{a})/\|a\|^2,\ a\in\mathbb{R}^m\backslash\{0\}$.

To simplify terminology, throughout the rest of the paper, we omit the word "relative" when referring to (local) relative condition number.

We deal with a large class of semialgebraic subsets of $\mathbb{R}^m\times S^1$ that we define next.

Definition 3 We say that the semialgebraic set $\mathcal{S}\subset\mathbb{R}^m\times S^1$ is *non-degenerate* if the following conditions are satisfied:

1. for any $x\in S^1$, the fiber $p_2^{-1}(x)$ is of dimension $m-1$,
2. the semialgebraic set $\Sigma_1\subset\mathcal{S}_{\text{top}}$ of critical points of $p_1:\mathcal{S}_{\text{top}}\to\mathbb{R}^m$ is at most $(m-1)$-dimensional. In Proposition 1, we show that this condition is equivalent to the following one:

2′. there exists a semialgebraic subset $B\subset\mathbb{R}^m$ of dimension at most $m-2$ such that for any $a\notin B$ the fiber $p_1^{-1}(a)$ is finite.

The first condition in Definition 3 implies that $\mathcal{S}$ is m-dimensional (see Lemma 1). To perform our probabilistic study, we take the input variables $a=(a_1,\ldots,a_m)\in\mathbb{R}^m$ to be independent standard Gaussians: $a\sim N(0,1)$. In the following theorem, we establish a general formula for the expectation of the condition number $\mu(a)$ of a randomly chosen $a\in\mathbb{R}^m$:

Theorem 2 *If* $\mathcal{S}\subset\mathbb{R}^m\times S^1$ *is a non-degenerate semialgebraic set, then* $\dim(\mathcal{S})=m$ *and*

$$\mathbb{E}_{a\sim N(0,1)}\left(\sum_{x\in S^1:\,(a,x)\in\mathcal{S}}\mu(a,x)\right)=\frac{1}{\sqrt{2\pi}^{\,m}}\int_{x\in S^1}\int_{a\in p_2^{-1}(x)}\|a\|e^{-\frac{\|a\|^2}{2}}\,\mathrm{d}a\,\mathrm{d}x, \quad (3)$$

where μ *is given in Definition 2. If, moreover,* $\mathcal{S}$ *is scale-invariant with respect to the first m variables, i.e.,* $(a,x)\in\mathcal{S}$ *if and only if* $(ta,x)\in\mathcal{S}$ *for any* $t>0$*, then*

$$\mathbb{E}_{a\sim N(0,1)}\left(\sum_{x\in S^1:\,(a,x)\in\mathcal{S}}\mu(a,x)\right)=\frac{\Gamma\left(\frac{m}{2}\right)}{2\sqrt{\pi}^m}\int\limits_{x\in S^1}|p_2^{-1}(x)\cap S^{m-1}|\,\mathrm{d}x,$$

where $S^{m-1}\subseteq\mathbb{R}^m$ *is the unit sphere and* $|p_2^{-1}(x)\cap S^{m-1}|$ *denotes the volume of the* $(m-2)$*-dimensional semialgebraic spherical set* $p_2^{-1}(x)\cap S^{m-1}$.

The following form of Theorem 2 for sets in $\mathbb{R}^m\times\mathbb{R}\mathrm{P}^1$ better fits our purposes.

Corollary 1 *Let* $\mathcal{S}\subset\mathbb{R}^m\times S^1$ *be a non-degenerate semialgebraic set that is scale-invariant with respect to the first m variables and suppose that* $\mathcal{S}$ *is invariant under the map* $(a,x)\mapsto(a,-x)$, $(a,x)\in\mathbb{R}^m\times S^1$. *Then* $\mu(a,x)=\mu(a,-x)$, $(a,x)\in\mathcal{S}$, *the fibers* $p_2^{-1}(x)$, $p_2^{-1}(-x)$ *are isometric and*

$$\mathbb{E}_{a\sim N(0,1)}\left(\sum_{[x]\in\mathbb{R}P^1:\,(a,x)\in\mathcal{S}}\mu(a,x)\right)=\frac{\Gamma\left(\frac{m}{2}\right)}{2\sqrt{\pi}^m}\int\limits_{[x]\in\mathbb{R}P^1}|p_2^{-1}(x)\cap S^{m-1}|\,d[x],$$

Note that Corollary 1 is just a "projective" version of the second part of Theorem 2.

As pointed out in the introduction, we are specifically interested in the *polynomial eigenvalue problem*. Given $d+1$ matrices $A_0,\ldots,A_d\in M(n,\mathbb{R})$ a point $[x]=[\alpha:\beta]\in\mathbb{R}\mathrm{P}^1$ is a (real) *polynomial eigenvalue* (PEV) of $A=(A_0,\ldots,A_d)$ if

$$\det(\alpha^0\beta^dA_0+\cdots+\alpha^d\beta^0A_d)=0.$$

The space $M(n,\mathbb{R})$ of $n\times n$ real matrices is endowed with the Frobenius inner product and the associated norm:

$$(A,B)=\mathrm{tr}(A^tB),\quad\|A\|^2=(A,A),\quad A,B\in M(n,\mathbb{R}).\tag{4}$$

Then, a k-dimensional vector subspace $V\subset M(n,\mathbb{R})$ is endowed with the standard normal probability distribution $\mathcal{N}_V$:

$$\mathbb{P}_{\mathcal{N}_V}(U)=\frac{1}{\sqrt{2\pi}^k}\int\limits_U e^{-\frac{\|v\|^2}{2}}\mathrm{d}v,$$

where $\mathrm{d}v$ is the Lebesgue measure on $(V,(\cdot,\cdot))$ and $U\subset V$ is a measurable subset. Denote by $\Sigma_V=\{A\in V:\det A=0\}\subset V$ the variety of singular matrices in V.

The condition number for polynomial eigenvalues of $A=(A_0,\ldots,A_d)\in V^{d+1}$ is defined via

$$\mu(A):=\sum_{[x]\in\mathbb{R}\mathrm{P}^1\text{is a PEV of }A}\mu(A,x),$$

where $\mu(A,x)$ is as in Definition 2 with $\mathbb{R}^m=(V,(\cdot,\cdot))^{d+1}$ so that $m=(d+1)k$ and

$$\mathcal{S} = \{(A, x) = ((A_0, \ldots, A_d), (\alpha, \beta)) \in V^{d+1} \times S^1 : \\ \det(\alpha^0\beta^d A_0 + \cdots + \alpha^d\beta^0 A_d) = 0\}.$$

As proved in [10], in the case $V = M(n, \mathbb{R})$ this definition for $\mu(A, x)$ is equivalent to (1). In the following theorem, we investigate the expected condition number for polynomial eigenvalues of independent $\mathcal{N}_V$-distributed matrices $A_0, \ldots, A_d \in V$.

Theorem 3 *If $\Sigma_V \subset V$ is of codimension one, then*

$$\underset{A_0,\ldots,A_d \sim i.i.d. \mathcal{N}_V}{\mathbb{E}} \mu(A) = \sqrt{\pi} \frac{\Gamma\left(\frac{(d+1)k}{2}\right)}{\Gamma\left(\frac{(d+1)k-1}{2}\right)} \frac{|\Sigma_V \cap S^{k-1}|}{|S^{k-2}|}. \tag{5}$$

Poincaré's formula [14, (3–5)] allows to derive the following universal upper bound.

Corollary 2 *If $\Sigma_V \subset V$ is of codimension one, then*

$$\underset{A_0,\ldots,A_d \sim i.i.d. \mathcal{N}_V}{\mathbb{E}} \mu(A) \le \sqrt{\pi} n \frac{\Gamma\left(\frac{(d+1)k}{2}\right)}{\Gamma\left(\frac{(d+1)k-1}{2}\right)} \tag{6}$$

In the case $V = M(n, \mathbb{R})$ of all square matrices, we provide an explicit formula for the expected condition number, that is the claim of our Theorem 1 above.

We give an explicit answer also in the case $V = Sym(n, \mathbb{R})$ of symmetric matrices. In this case, the probability space $(Sym(n, \mathbb{R}), \mathcal{N}_{Sym(n,\mathbb{R})})$ is usually referred to as *Gaussian Orthogonal Ensemble* (GOE).

Corollary 3 *If $A_0, \ldots, A_d \in Sym(n, \mathbb{R})$ are independent* GOE(n)*-matrices and n is even, then*

$$\underset{A_0,\ldots,A_d \sim i.i.d. \,\mathrm{GOE}(n)}{\mathbb{E}} \mu(A) = \sqrt{2} n \frac{\Gamma\left(\frac{(d+1)n(n+1)}{4}\right)}{\Gamma\left(\frac{(d+1)n(n+1)-2}{4}\right)} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n+2}{2}\right)} \\ = \sqrt{(d+1)n^3}\left(1 + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right), \; n \to +\infty. \tag{7}$$

If n is odd, the explicit formula is more complicated and is given in the proof of the corollary. However, the above asymptotic formula is valid for both even and odd n.

2 Preliminaries

Below, we state few classical results in semialgebraic geometry that we will use; the proofs can be found in [4,9].

Given a semialgebraic set $S \subset \mathbb{R}^N$ of dimension $k \le N$, we fix a *semialgebraic stratification* of S, i.e., a partition of S into finitely many semialgebraic subsets (called *strata*) such that each stratum is a smooth submanifold of $\mathbb{R}^N$ and the boundary of any stratum of dimension $i \leq N$ is a union of some strata of dimension less than i. We denote by S_{top} the union of all k-dimensional strata of S and by $S_{\text{low}} = S \setminus S_{\text{top}}$ the union of the strata of dimension less than k. The sets $S_{\text{top}}, S_{\text{low}} \subset \mathbb{R}^N$ are semialgebraic, and S_{top} is a smooth k-dimensional submanifold of $\mathbb{R}^N$.

One of the central results about semialgebraic mappings is Hardt's theorem.

Theorem 4 (Hardt's semialgebraic triviality) *Let $S \subset \mathbb{R}^N$ be a semialgebraic set and let $f : S \to \mathbb{R}^M$ be a continuous semialgebraic mapping. Then, there exists a finite partition of $\mathbb{R}^M$ into semialgebraic sets $C_1, \ldots, C_r \subset \mathbb{R}^M$ such that f is semialgebraically trivial over each C_i, i.e., there are a semialgebraic set F_i and a semialgebraic homeomorphism $h_i : f^{-1}(C_i) \to C_i \times F_i$ such that the composition of h_i with the projection $C_i \times F_i \to C_i$ equals $f|_{f^{-1}(C_i)}$.*

The following two corollaries of Hardt's theorem are frequently used to estimate dimension of semialgebraic sets.

Corollary 4 *Let $f : S \to \mathbb{R}^M$ be as above. The set $A_d = \{x \in \mathbb{R}^M : \dim(f^{-1}(x)) = d\}$ is semialgebraic and has dimension not greater than* $\dim(S) - d$.

Proof With the notations of Hardt's theorem, let us write

$$D_i = C_i \cap A_d = \{x \in C_i : \dim(h_i^{-1}(\{x\} \times F_i)) = d\}.$$

Now, since h_i is a semialgebraic homeomorphism we have $\dim(h_i^{-1}(\{x\} \times F_i)) = \dim(F_i)$ independently of $x \in C_i$. In other words, $D_i = C_i$ if $\dim(F_i) = d$ and $D_i = \emptyset$ otherwise. We thus have $A_d = \cup_{i \in I} C_i$ for some finite index set I, and we conclude that A_d is a semialgebraic set. Moreover, for $i \in I$ we have that $f^{-1}(C_i) \equiv C_i \times F_i$ has dimension $\dim(C_i) + \dim(F_i) = \dim(C_i) + d$. In other words,

$$\dim(C_i) + d \leq \dim(S),$$

and the second claim of the corollary follows. □

Corollary 5 *Let $f : S \to \mathbb{R}^M$ be as above and let $Z \subseteq \mathbb{R}^M$. Then, for some $z \in Z$ we have* $\dim(f^{-1}(Z)) \leq \dim(Z) + \dim(f^{-1}(z))$.

Proof Again using the notation of Hardt's theorem for the restriction $g : f^{-1}(Z) \to Z$ of f to $f^{-1}(Z)$, we have $Z = \cup_{i \in I} C_i$ for some finite index set I and $f^{-1}(Z) \equiv \cup_{i \in I} C_i \times F_i$. Without loss of generality, we assume that $\dim(f^{-1}(Z)) = \dim(C_1 \times F_1)$ that for $z \in C_1$ equals

$$\dim(f^{-1}(Z)) = \dim(C_1) + \dim(f^{-1}(z)) \leq \dim(Z) + \dim(f^{-1}(z)). \qquad \square$$

3 Proof of Main Results

In this section, we prove our main results, Theorems 2 and 3. Let us first fix some notations that are used in the rest of the paper: For a non-degenerate subset $\mathcal{S} \subset$

$\mathbb{R}^m \times S^1$ by $\Sigma_1, \Sigma_2 \subset \mathcal{S}_{\text{top}}$, we denote the semialgebraic sets of critical points of $p_1 : \mathcal{S}_{\text{top}} \to \mathbb{R}^m$ and $p_2 : \mathcal{S}_{\text{top}} \to S^1$, respectively, the corresponding semialgebraic sets of critical values are denoted by $\sigma_1 = p_1(\Sigma_1) \subset \mathbb{R}^m$ and $\sigma_2 = p_2(\Sigma_2) \subset S^1$.

3.1 Proof of Theorem 2

In this subsection, $\mathcal{S}$ denotes a non-degenerate semialgebraic subset of $\mathbb{R}^m \times S^1$. For the proof of Theorem 2, we need few technical lemmas which we state and prove below.

Lemma 1 *The semialgebraic sets $\mathcal{S} \subset \mathbb{R}^m \times S^1$ and $p_1(\mathcal{S}) \subset \mathbb{R}^m$ are of dimension m.*

Proof Since $\mathcal{S}$ is non-degenerate, for every $x \in S^1$ the fiber $p_2^{-1}(x)$ is $(m-1)$-dimensional. From Theorem 4, it follows that for some $x \in S^1$ we have $\dim(\mathcal{S}) = \dim(p_2^{-1}(x)) + \dim(S^1) = (m-1) + 1 = m$.

The map $p_1 : \mathcal{S}_{\text{top}} \to \mathbb{R}^m$ has a regular point $(a, x) \in \mathcal{S}_{\text{top}} \backslash \Sigma_1$ since $\mathcal{S}$ is m-dimensional and the set Σ_1 of critical points of p_1 is at most $(m-1)$-dimensional. The image $p_1(U)$ of a small open neighborhood $U \subset \mathcal{S}_{\text{top}} \backslash \Sigma_1$ of $(a, x) \in U$ is open in $\mathbb{R}^m$, and hence, $\dim(p_1(\mathcal{S})) = m$. □

Lemma 2 *There exists an open semialgebraic subset $M \subset \mathcal{S}_{\text{top}}$ such that $p_1(M)$ is open in $\mathbb{R}^m$, $M = p_1^{-1}(p_1(M))$, the restriction $p_1 : M \to p_1(M)$ is a submersion and* $\dim(\mathcal{S} \backslash M) \leq m - 1$.

Proof Define $M := p_1^{-1}(\mathbb{R}^m \backslash N) = \mathcal{S}_{\text{top}} \backslash p_1^{-1}(N)$, where $N := \overline{p_1(\mathcal{S}_{\text{low}} \cup \Sigma_1)}$ and the bar stands for the Euclidean closure of a set. Note that M is an open subset of $\mathcal{S}_{\text{top}}$ and $M = p_1^{-1}(p_1(M))$. Moreover, M consists of regular points of the projection $p_1 : \mathcal{S}_{\text{top}} \to \mathbb{R}^m$, which implies that $p_1(M)$ is an open subset of $\mathbb{R}^m$ and $p_1 : M \to p_1(M)$ is a submersion of smooth manifolds. Indeed, for $a \in p_1(M)$ and $(a, x) \in M$ the image $p_1(U)$ of a small open neighborhood $U \subset M$ of $(a, x) \in U$ is open in $\mathbb{R}^m$ and $a \in p_1(U)$.

We now prove that $\mathcal{S} \backslash M = p_1^{-1}(N)$ is at most $(m-1)$-dimensional. Since $\mathcal{S}$ is non-degenerate, there exists a semialgebraic set $B \subset \mathbb{R}^m$ with $\dim(B) \leq m - 2$ such that $p_1^{-1}(a)$ is finite for $a \notin B$. We decompose the semialgebraic set $N = (N \cap B) \cup (N \backslash B)$. From Corollary 5, it follows that there exists some $a \in N \cap B$ such that $\dim(p_1^{-1}(N \cap B)) \leq \dim(p_1^{-1}(a)) + \dim(N \cap B) \leq 1 + (m-2) = m - 1$. For $a \in N \backslash B$, the fiber $p_1^{-1}(a)$ is discrete, which together with the non-degeneracy of $\mathcal{S}$ and Corollary 5 implies $\dim(p_1^{-1}(N \backslash B)) \leq \dim(p_1^{-1}(a)) + \dim(N \backslash B) \leq \dim(\mathcal{S}_{\text{low}} \cup \Sigma_1) \leq m - 1$. Thus, $\dim(\mathcal{S} \backslash M) = \dim(p_1^{-1}(N)) = \dim(p_1^{-1}(N \cap B) \cup p_1^{-1}(N \backslash B)) \leq m - 1$. □

Lemma 3 *There exists an open semialgebraic subset $R \subset \mathcal{S}_{\text{top}}$ such that $S^1 \backslash p_2(R)$ is finite, $p_2 : R \to p_2(R)$ is a submersion, $\dim(\mathcal{S} \backslash R) \leq m - 1$ and* $\dim(p_2^{-1}(x) \backslash R) \leq$ *$m - 2$ for $x \in p_2(R)$.*

Proof Since $\mathcal{S}$ is non-degenerate, every fiber $p_2^{-1}(x)$, $x \in S^1$ is $(m-1)$-dimensional.

Note that the set $S^1\backslash p_2(\mathcal{S}_{\text{top}})$ is semialgebraic and zero-dimensional, thus finite. Indeed, if it was one-dimensional Theorem 4 together with $\dim(p_2^{-1}(x)) = m-1$, $x \in S^1$ would imply that $p_2^{-1}(S^1\backslash p_2(\mathcal{S}_{\text{top}})) \subset \mathcal{S}\backslash\mathcal{S}_{\text{top}}$ is m-dimensional which would contradict to $\dim(\mathcal{S}\backslash\mathcal{S}_{\text{top}}) \leq m-1$.

The semialgebraic set $\sigma_2 = p_2(\Sigma_2) \subset S^1$ of critical values of $p_2 : \mathcal{S}_{\text{top}} \to S^1$ has measure zero by Sard's theorem (see [12, p. 39]). Hence, $\sigma_2 \subset S^1$ consists of a finite number of points.

Applying Corollary 4 to $p_2 : \mathcal{S}_{\text{low}} \to S^1$, we have that $C := \{x \in S^1 : \dim(p_2^{-1}(x) \cap \mathcal{S}_{\text{low}}) = m-1\}$ is a semialgebraic subset of S^1 and $\dim(C) \leq \dim(\mathcal{S}_{\text{low}}) - (m-1) \leq 0$. Thus, C is a (possibly empty) finite set.

Set now $R := \mathcal{S}_{\text{top}}\backslash p_2^{-1}(\sigma_2 \cup C)$. Note that R is an open semialgebraic subset of $\mathcal{S}_{\text{top}}$ and $S^1\backslash p_2(R) = \sigma_2 \cup C \cup (S^1\backslash p_2(\mathcal{S}_{\text{top}}))$ is finite by the above arguments. Since R consists of regular points of $p_2 : \mathcal{S}_{\text{top}} \to S^1$, the map $p_2 : R \to p_2(R)$ is a submersion. Since $\dim(\mathcal{S}_{\text{low}}) \leq m-1$ and $p_2^{-1}(\sigma_2 \cup C)$ is a finite collection of $(m-1)$-dimensional fibers, we have that $\dim(\mathcal{S}\backslash R) = \dim(\mathcal{S}_{\text{low}} \cup p_2^{-1}(\sigma_2 \cup C)) \leq m-1$. Finally, $\dim(p_2^{-1}(x)\backslash R) = \dim(p_2^{-1}(x) \cap \mathcal{S}_{\text{low}}) \leq m-2$ for $x \in p_2(R)$ because $p_2(R) \cap C = \varnothing$. □

Lemma 4 *For any measurable function $f : \mathcal{S} \to [0, +\infty)$, we have*

$$\int\limits_{a\in\mathbb{R}^m} \sum_{x\in S^1:\,(a,x)\in\mathcal{S}} f(a,x)\,\mathrm{d}a = \int\limits_{x\in S^1} \int\limits_{a\in p_2^{-1}(x)} \frac{NJ_{(a,x)}p_1}{NJ_{(a,x)}p_2} f(a,x)\,\mathrm{d}a\,\mathrm{d}x.$$

Here, NJ stands for the normal Jacobian of a smooth map, that is, the absolute value of the determinant of the differential restricted to the orthogonal complement to its kernel.

Proof Let $M \subset \mathcal{S}_{\text{top}}$ be as in Lemma 2. The smooth coarea formula [14, (A-2)] applied to the measurable function $f : M \to [0, +\infty)$ and to the submersion $p_1 : M \to p_1(M)$ reads

$$\int\limits_{(a,x)\in M} NJ_{(a,x)}p_1\, f(a,x)\,\mathrm{d}(a,x) = \int\limits_{a\in p_1(M)} \sum_{x\in S^1:\,(a,x)\in\mathcal{S}} f(a,x)\,\mathrm{d}a, \tag{8}$$

where we used that $M = p_1^{-1}(p_1(M))$ (Lemma 2) to be able to sum over the whole fiber $p_1^{-1}(a) = \{(a,x) \in \mathcal{S}\}$, $a \in p_1(M)$. By Lemma 2, we have $\dim(\mathcal{S}\backslash M) \leq m-1$, and hence, $\dim(p_1(\mathcal{S})\backslash p_1(M)) = \dim(p_1(\mathcal{S}\backslash M)) \leq \dim(\mathcal{S}\backslash M) \leq m-1$. Thus, we extend the integrations in (8) over $\mathcal{S}$ and $p_1(\mathcal{S})$, respectively, without changing the result. Moreover, the integration over $p_1(\mathcal{S})$ can be further extended to the whole space $\mathbb{R}^m$ since for a point $a \in \mathbb{R}^m\backslash p_1(\mathcal{S})$ the summation $\sum_{x\in S^1:(a,x)\in\mathcal{S}} f(a,x)$ is performed over the empty set $p_1^{-1}(a)$ and the sum is conventionally set to 0. All together, the above arguments imply

$$\int_{(a,x)\in\mathcal{S}} NJ_{(a,x)}p_1\, f(a,x)\,\mathrm{d}(a,x) = \int_{a\in\mathbb{R}^m} \sum_{x\in S^1:\,(a,x)\in\mathcal{S}} f(a,x)\,\mathrm{d}a. \tag{9}$$

Let $R \subset \mathcal{S}_{\mathrm{top}}$ be as in Lemma 3. Applying the smooth coarea formula [14, (A-2)] to the measurable function $\frac{NJp_1}{NJp_2} f : R \to [0,+\infty)$ and to the submersion $p_2 : R \to p_2(R)$, we obtain

$$\int_{(a,x)\in R} NJ_{(a,x)}p_1\, f(a,x)\,\mathrm{d}(a,x) = \int_{x\in p_2(R)} \int_{a\in p_2^{-1}(x)\cap R} \frac{NJ_{(a,x)}p_1}{NJ_{(a,x)}p_2} f(a,x)\,\mathrm{d}a\,\mathrm{d}x. \tag{10}$$

By Lemma 3 $\dim(\mathcal{S}\backslash R) \le m-1$, $S^1\backslash p_2(R)$ is finite, and $\dim(p_2^{-1}(x)\backslash R) \le m-2$ for $x \in p_2(R)$. Thus, the integrations in (10) can be extended over $\mathcal{S}$, S^1 and $p_2^{-1}(x)$, respectively, leading to

$$\int_{(a,x)\in\mathcal{S}} NJ_{(a,x)}p_1\, f(a,x)\,\mathrm{d}(a,x) = \int_{x\in S^1} \int_{a\in p_2^{-1}(x)} \frac{NJ_{(a,x)}p_1}{NJ_{(a,x)}p_2} f(a,x)\,\mathrm{d}a\,\mathrm{d}x. \tag{11}$$

Combining (11) with (9), we finish the proof. □

Now comes the proof of Theorem 2.

Proof of Theorem 2 The following identity is the key point of the proof:

$$\mu(a,x) = \|a\| \frac{NJ_{(a,x)}p_2}{NJ_{(a,x)}p_1}, \quad (a,x) \in M \cap R \subset \mathcal{S}_{\mathrm{top}} \tag{12}$$

where $M \subset \mathcal{S}_{\mathrm{top}}$ and $R \subset \mathcal{S}_{\mathrm{top}}$ are as in Lemmas 2 and 3, respectively, and $\mu(a,x)$, the local condition number of $(a,x) \in \mathcal{S}$, is defined in Definition 2. The proof of the identity comes after we derive the statement of Theorem 2.

Applying Lemma 4 to the measurable function $f(a,x) = \mu(a,x)e^{-\|a\|^2/2}/\sqrt{2\pi}^m$, $(a,x) \in \mathcal{S}$, and using (12), we obtain:

$$\begin{aligned}\mathbb{E}_{a\sim N(0,1)}\left(\sum_{x\in S^1:\,(a,x)\in\mathcal{S}} \mu(a,x)\right) &= \frac{1}{\sqrt{2\pi}^m} \int_{a\in\mathbb{R}^m} \left(\sum_{x\in S^1:\,(a,x)\in\mathcal{S}} \mu(a,x)\right) e^{-\frac{\|a\|^2}{2}}\,\mathrm{d}a \\ &= \frac{1}{\sqrt{2\pi}^m} \int_{x\in S^1} \int_{a\in p_2^{-1}(x)} \|a\| e^{-\frac{\|a\|^2}{2}}\,\mathrm{d}a\,\mathrm{d}x = (*),\end{aligned}$$

which gives the claimed formula (3). If $\mathcal{S}$ is scale-invariant with respect to $a \in \mathbb{R}^m$ by Lemma 5, we have

$$(*) = \frac{\Gamma\left(\frac{m}{2}\right)}{2\sqrt{\pi}^m} \int\limits_{x \in S^1} |p_2^{-1}(x) \cap S^{m-1}| \, \mathrm{d}x.$$

Now, we turn to the proof of (12).

For $(a, x) \in M \cap R \subset \mathcal{S}_{\text{top}}$ let $(\dot{a}_0, \dot{x}_0), (\dot{a}_1, 0), \ldots, (\dot{a}_{m-1}, 0)$ be an orthonormal basis of $T_{(a,x)}R$ with $(\dot{a}_j, 0) \in \ker D_{(a,x)}p_2$, $j = 1, \ldots, m-1$. Note that $\dot{a}_0 \in \mathbb{R}^m$, $\dot{x}_0 \in T_x S^1$ are nonzero since $p_1 : M \to p_1(M)$, $p_2 : R \to p_2(R)$ are submersions and $\dot{a}_0 \in \mathbb{R}^m$ is orthogonal to $\dot{a}_j \in \mathbb{R}^m$, $j = 1, \ldots, m-1$. We compute the normal Jacobians $NJ_{(a,x)}p_1$ and $NJ_{(a,x)}p_2$ using the following orthonormal bases:

$$\{(\dot{a}_0, \dot{x}_0), (\dot{a}_1, 0), \ldots, (\dot{a}_{m-1}, 0)\} \subset T_{(a,x)}\mathcal{S}_{\text{top}}$$
$$\left\{\frac{\dot{a}_0}{\|\dot{a}_0\|}, \dot{a}_1, \ldots, \dot{a}_{m-1}\right\} \subset T_a\mathbb{R}^m$$
$$\left\{\frac{\dot{x}_0}{\|\dot{x}_0\|}\right\} \subset T_x S^1$$

It is straightforward to see that $NJ_{(a,x)}p_1 = \|\dot{a}_0\|$ and $NJ_{(a,x)}p_2 = \|\dot{x}_0\|$ and hence

$$\frac{NJ_{(a,x)}p_2}{NJ_{(a,x)}p_1} = \frac{\|\dot{x}_0\|}{\|\dot{a}_0\|} \tag{13}$$

Since $D_a(p_2 \circ p_1^{-1})(\dot{a}_j) = D_{(a,x)}p_2 \circ D_a p_1^{-1}(\dot{a}_j) = 0$ for $j = 1, \ldots, m-1$ and since $D_a(p_2 \circ p_1^{-1})(\dot{a}_0) = D_{(a,x)}p_2 \circ D_a p_1^{-1}(\dot{a}_0) = \dot{x}_0$, we obtain

$$\mu(a, x) = \|a\| \sup_{\dot{a} \in \mathbb{R}^m \setminus \{0\}} \frac{\|D_a(p_2 \circ p_1^{-1})(\dot{a})\|}{\|\dot{a}\|} = \|a\| \frac{\|\dot{x}_0\|}{\|\dot{a}_0\|}$$

This together with (13) implies the claimed identity (12). □

3.2 Proof of Theorem 3

For a k-dimensional vector subspace $V \subset M(n, \mathbb{R})$ and for a basis $f = (f_0(\alpha, \beta), \ldots, f_d(\alpha, \beta))$ of the space $P_{d,2}$ of binary forms of degree $d \geq 1$, let us define the algebraic variety

$$\mathcal{S}(V, f) := \{(A, x) \in V^{d+1} \times S^1 : \det(A_0 f_0(\alpha, \beta) + \cdots + A_d f_d(\alpha, \beta)) = 0\}$$

Theorem 3 follows from the following more general result that we state for any choice of basis (not necessarily the monomial basis) since for some problems it may be useful to consider other bases such as the one coming from harmonic forms [16].

Theorem 5 *If $\Sigma_V \subset V$ is of codimension one and f is any basis of $P_{d,2}$, then $\mathcal{S}(V, f)$ is non-degenerate and*

$$\mathop{\mathbb{E}}_{A_0,\dots,A_d \sim i.i.d.\mathcal{N}_V} \left(\sum_{[x]\in\mathbb{R}P^1:\,(A,x)\in\mathcal{S}(V,f)} \mu(A,x) \right) = \sqrt{\pi}\,\frac{\Gamma\left(\frac{(d+1)k}{2}\right)}{\Gamma\left(\frac{(d+1)k-1}{2}\right)}\frac{|\Sigma_V \cap S^{k-1}|}{|S^{k-2}|},$$

Proof Observe first that for any $x = (\alpha, \beta) \in S^1$, the vector $f(x) = (f_0(\alpha, \beta), \dots, f_d(\alpha, \beta))$ is nonzero. For any such x, let $g = (g_{ij}) \in O(d+1)$ be an orthogonal matrix that sends $f(x)$ to $(c, 0, \dots, 0) \in \mathbb{R}^{d+1}\setminus\{0\}$, where $c \neq 0$ is a constant, i.e.,

$$\sum_{j=0}^{d} g_{ij} f_j(\alpha, \beta) = \begin{cases} c, i = 0, \\ 0, i = 1, \dots, d \end{cases}$$

It is easy to verify that the linear change of coordinates $A_j = \sum_{i=0}^{d} g_{ij}\tilde{A}_i,\ j = 0, \dots, d$ is an isometry of the product space $(V, (\cdot,\cdot))^{d+1}$ (where the inner product $(\cdot,\cdot)$ on V is defined in (4)) and

$$\sum_{j=0}^{d} f_j(\alpha,\beta)A_j = \sum_{j=0}^{d} f_j(\alpha,\beta)\left(\sum_{i=0}^{d} g_{ij}\tilde{A}_i\right) = \sum_{i=0}^{d}\left(\sum_{j=0}^{d} g_{ij} f_j(\alpha,\beta)\right)\tilde{A}_i = c\tilde{A}_0$$

Therefore, for $x = (\alpha, \beta) \in S^1$ there is a global isometry $\mathcal{I}_x : (V, (\cdot,\cdot))^{d+1} \to (V, (\cdot,\cdot))^{d+1}$ that sends the fiber $p_2^{-1}(x) = \{A \in V^{d+1} : \det(A_0 f_0(\alpha,\beta) + \dots + A_d f_d(\alpha,\beta)) = 0\}$ to $\{\tilde{A} \in V^{d+1} : \det(\tilde{A}_0) = 0\} = \Sigma_V \times V^d$. In particular, under the assumption $\dim(\Sigma_V) = k - 1$ we have that $p_2^{-1}(x)$ is of codimension one in V^{d+1}, and hence, condition (1) in Definition 3 is satisfied.

Since both $f_0(\alpha,\beta), \dots, f_d(\alpha,\beta)$ and $\alpha^0\beta^d, \dots, \alpha^d\beta^0$ are bases of $P_{d,2}$, for some matrix $h = (h_{ij}) \in GL(d+1)$, we have $\alpha^i\beta^{d-i} = \sum_{j=0}^{d} h_{ij} f_j(\alpha,\beta),\ i = 0, \dots, d$. Let us define $B = \{A \in V^{d+1} : A_j = \sum_{i=0}^{d} h_{ij}\tilde{A}_i,\ j = 0, \dots, d,\ \det(\tilde{A}_0) = \det(\tilde{A}_d) = 0\}$. Since $\dim(\Sigma_V) = k - 1$ and since h is a non-degenerate transformation, the algebraic subset $B \subset V^{d+1}$ has codimension 2. For $A \notin B$, the matrix

$$\begin{aligned}\sum_{j=0}^{d} f_j(\alpha,\beta)A_j &= \sum_{j=0}^{d} f_j(\alpha,\beta)\left(\sum_{i=0}^{d} h_{ij}\tilde{A}_i\right)\\ &= \sum_{i=0}^{d}\left(\sum_{j=0}^{d} h_{ij} f_j(\alpha,\beta)\right)\tilde{A}_i = \sum_{i=0}^{d}\alpha^i\beta^{d-i}\tilde{A}_i\end{aligned}$$

is non-degenerate at $(\alpha, \beta) = (0, 1)$ (at $(\alpha, \beta) = (1, 0)$) if $\det(\tilde{A}_0) \neq 0$ ($\det(\tilde{A}_d) \neq 0$, respectively) and hence after the choice of some representatives the binary form $\det(A_0 f_0(\alpha, \beta) + \cdots + A_d f_d(\alpha, \beta))$ is nonzero. Consequently, the fiber

$$p_1^{-1}(A) \equiv \{(\alpha, \beta) \in S^1 : \det(A_0 f_0(\alpha, \beta) + \cdots + A_d f_d(\alpha, \beta)) = 0\}$$

is finite for any $A \notin B$ and condition (2′) in Definition 3 is satisfied. Applying Theorem 2 to $\mathcal{S}(V, f) \subset \mathbb{R}^{(d+1)k} \times S^1$, $\mathbb{R}^{(d+1)k} \simeq V^{d+1}$ and noting that the solutions lie naturally in $\mathbb{R}\mathrm{P}^1$, we obtain

$$\begin{aligned} &\mathop{\mathbb{E}}_{A_0,\ldots,A_d \sim i.i.d. \mathcal{N}_V} \left(\sum_{[x] \in \mathbb{R}\mathrm{P}^1 :\, (A,x) \in \mathcal{S}(V,f)} \mu(A, x) \right) \\ &= \frac{1}{2\sqrt{2\pi}^{(d+1)k}} \int\limits_{x \in S^1} \int\limits_{A \in p_2^{-1}(x)} \|A\| e^{-\frac{\|A\|^2}{2}} \mathrm{d}A \, \mathrm{d}x, \end{aligned}$$

where $\|A\|^2 = \|A_0\|^2 + \cdots + \|A_d\|^2$. Since each fiber $p_2^{-1}(x)$, $x \in S^1$, is an algebraic subset of $\mathbb{R}^{(d+1)k}$ of codimension one we have by Lemma 5

$$\int\limits_{A \in p_2^{-1}(x)} \|A\| e^{-\frac{\|A\|^2}{2}} \mathrm{d}A = \sqrt{2} \frac{\Gamma\left(\frac{(d+1)k}{2}\right)}{\Gamma\left(\frac{(d+1)k-1}{2}\right)} \int\limits_{A \in p_2^{-1}(x)} e^{-\frac{\|A\|^2}{2}} \mathrm{d}A.$$

Performing the isometric change of coordinates $\mathcal{I}_x : (V, (\cdot, \cdot))^{d+1} \to (V, (\cdot, \cdot))^{d+1}$ that was constructed above, we write the last integral as follows:

$$\begin{aligned} \int\limits_{A \in p_2^{-1}(x)} e^{-\frac{\|A\|^2}{2}} \mathrm{d}A &= \int\limits_{\{\tilde{A} \in V^{d+1} :\, \det(\tilde{A}_0) = 0\}} e^{-\frac{\|\tilde{A}_0\|^2}{2}} e^{-\frac{\|\tilde{A}_1\|^2}{2}} \ldots e^{-\frac{\|\tilde{A}_d\|^2}{2}} \mathrm{d}\tilde{A}_0 \mathrm{d}\tilde{A}_1 \ldots \mathrm{d}\tilde{A}_d \\ &= \sqrt{2\pi}^{dk} \int\limits_{\tilde{A}_0 \in \Sigma_V} e^{-\frac{\|\tilde{A}_0\|^2}{2}} \mathrm{d}\tilde{A}_0 \\ &= \sqrt{2\pi}^{dk} \sqrt{2}^{k-3} \Gamma\left(\frac{k-1}{2}\right) |\Sigma_V \cap S^{k-1}|, \end{aligned}$$

where in the last step Lemma 5 has been used. Note that this quantity is independent of $x \in S^1$. Collecting everything together, we write

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{A_0,\ldots,A_d\sim i.i.d.\mathcal{N}_V}\left(\sum_{[x]\in\mathbb{R}\mathrm{P}^1:\,(A,x)\in\mathcal{S}(V,f)}\mu(A,x)\right)\\
&=\sqrt{\pi}\,\frac{\Gamma\left(\frac{(d+1)k}{2}\right)}{\Gamma\left(\frac{(d+1)k-1}{2}\right)}\,\frac{\Gamma\left(\frac{k-1}{2}\right)}{2\sqrt{\pi}^{k-1}}|\Sigma_V\cap S^{k-1}|\\
&=\sqrt{\pi}\,\frac{\Gamma\left(\frac{(d+1)k}{2}\right)}{\Gamma\left(\frac{(d+1)k-1}{2}\right)}\,\frac{|\Sigma_V\cap S^{k-1}|}{|S^{k-2}|},
\end{aligned}
$$

since $|S^{k-2}|=2\sqrt{\pi}^{k-1}/\Gamma\left(\frac{k-1}{2}\right)$. This completes the proof. □

Proof of Theorem 3 Taking $f_i(\alpha,\beta)=\alpha^i\beta^{d-i}$, $i=0,\ldots,d$, in Theorem 5, we obtain the claim of Theorem 3. □

4 Applications of Main Results

In this section, we derive Theorem 1 and Corollaries 2, 3.

Proof of Corollary 2 Recall Poincaré's formula [14, (3–5)] (see also [7, Th. A.55]): if M, N are two algebraic subvarieties of S^d of respective dimensions m, n with $m+n\ge d$, then for the invariant Haar probability measure on the group of orthogonal matrices $O(d+1)$ we have

$$
\mathbb{E}_{g\in O(d+1)}|M\cap gN|=|S^{m+n-d}|\frac{|M|\,|N|}{|S^m|\,|S^n|}.
$$

Applying this result to the $(k-2)$–dimensional subvariety $M=\Sigma_V\cap S^{k-1}=\{A\in V:\|A\|=1,\det(A)=0\}\subset S^{k-1}$ and any one–dimensional great circle $N\equiv S^1\subseteq S^{k-1}$, we get

$$
2\frac{|\Sigma_V\cap S^{k-1}|}{|S^{k-2}|}=\mathbb{E}_{g\in O(k)}\#\{A\in gN:\det(A)=0\}.
$$

Now, for almost all $g\in O(k)$ there are at most $2n$ isolated singular matrices in gN that correspond to the real projective roots $[\alpha:\beta]\in\mathbb{R}\mathrm{P}^1$ of $\det(\alpha A+\beta B)=0$, where A, B are two different matrices in the circle gN. We conclude that

$$
\frac{|\Sigma_V\cap S^{k-1}|}{|S^{k-2}|}\le n,
$$

which together with (5) implies the claimed bound (6). □

In case of any particular space $V \subset M(n, \mathbb{R})$ satisfying $\dim(\Sigma_V) = k - 1 = \dim(V) - 1$ by Theorem 3 explicit computation of the expected condition number for polynomial eigenvalues amounts to computing the volume of the hypersurface $\Sigma_V \cap S^{k-1}$. In cases $V = M(n, \mathbb{R})$ and $V = Sym(n, \mathbb{R})$ formulas for the volume of $\Sigma_V \cap S^{k-1}$ were found in [11] and [17], respectively. It is easy to see that in both of these cases, the variety Σ_V of singular matrices is of codimension one, and hence, the hypothesis of Theorem 3 is satisfied.

Proof of Theorem 1 The formula from [11] reads

$$\frac{|\Sigma_{M(n,\mathbb{R})} \cap S^{n^2-1}|}{|S^{n^2-2}|} = \sqrt{\pi}\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)}$$

Plugging it in (5) for $V = M(n, \mathbb{R})$, $k = \dim(V) = n^2$ leads to

$$\mathop{\mathbb{E}}_{A_0,\ldots,A_d \sim i.i.d.\mathcal{N}_{M(n,\mathbb{R})}} \mu(A) = \pi \frac{\Gamma\left(\frac{(d+1)n^2}{2}\right)}{\Gamma\left(\frac{(d+1)n^2-1}{2}\right)} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)}$$

$$= \frac{\pi}{2}\sqrt{(d+1)n^3}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right), \; n \to +\infty,$$

where the asymptotic is obtained using formula (1) from [22]. □

Proof of Corollary 3 In [17] it was proved that

$$\frac{|\Sigma_{Sym(n,\mathbb{R})} \cap S^{\frac{n(n+1)}{2}-1}|}{|S^{\frac{n(n+1)}{2}-2}|} = \sqrt{\frac{2}{\pi}} n \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n+2}{2}\right)} \tag{14}$$

for even n and

$$\frac{|\Sigma_{Sym(n,\mathbb{R})} \cap S^{\frac{n(n+1)}{2}-1}|}{|S^{\frac{n(n+1)}{2}-2}|} = \frac{(-1)^m\sqrt{\pi}n!}{2^n m!\Gamma\left(\frac{n+2}{2}\right)}\left(1 - \frac{4\sqrt{2}}{\sqrt{\pi}}\sum_{i=0}^{m-1}(-1)^i \frac{\Gamma\left(\frac{2i+3}{2}\right)}{i!}\right) \tag{15}$$

for odd $n = 2m + 1$. Plugging (14) and (15) in (5) for $V = Sym(n, \mathbb{R})$, $k = \frac{n(n+1)}{2}$ leads to explicit formulas for the expected condition number (see (7) in case of even n). In [17, Remark 3] it was shown that

$$\frac{|\Sigma_{Sym(n,\mathbb{R})} \cap S^{\frac{n(n+1)}{2}-1}|}{|S^{\frac{n(n+1)}{2}-2}|} = \frac{2\sqrt{n}}{\sqrt{\pi}}\left(1 + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right), \; n \to +\infty$$

regardless parity of n. This leads to the asymptotic

$$\mathop{\mathbb{E}}_{A_0,\ldots,A_d\sim i.i.d.\,\mathrm{GOE}(n)} \mu(A) = \sqrt{\pi}\frac{\Gamma\left(\frac{(d+1)n(n+1)}{4}\right)}{\Gamma\left(\frac{(d+1)n(n+1)-2}{4}\right)} \frac{|\Sigma_{Sym(n,\mathbb{R})}\cap S^{\frac{n(n+1)}{2}-1}|}{|S^{\frac{n(n+1)}{2}-2}|}$$
$$= \sqrt{(d+1)n^3}\left(1+\mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right),\ n\to+\infty,$$

where we again used formula (1) from [22] for the asymptotic of the ratio of two Gamma functions. ◻

Acknowledgements Open access funding provided by Max Planck Society. The authors want to thank two anonymous referees for helpful comments.

Appendix

In the following proposition, we show that the conditions (2) and (2′) in Definition 3 of a non-degenerate semialgebraic set $\mathcal{S}\subset\mathbb{R}^m\times S^1$ are equivalent.

Proposition 1 *Let $\mathcal{S}\subset\mathbb{R}^m\times S^1$ be a semialgebraic subset of dimension m. Then,*

(2) *the semialgebraic set $\Sigma_1\subset\mathcal{S}_{\mathrm{top}}$ of critical points of the first projection $p_1:\mathcal{S}_{\mathrm{top}}\to\mathbb{R}^m$ is at most $(m-1)$-dimensional if and only if*

(2′) *there exists a semialgebraic subset $B\subset\mathbb{R}^m$ of dimension at most $m-2$ such that for any $a\notin B$ the fiber $p_1^{-1}(a)$ is finite.*

Proof (2) ⇒ (2′) By Sard's theorem, the semialgebraic set $\sigma_1=p_1(\Sigma_1)\subset\mathbb{R}^m$ of critical values of $p_1:\mathcal{S}_{\mathrm{top}}\to\mathbb{R}^m$ is of dimension $\le m-1$. The set $p_1^{-1}(\sigma_1)\subset\mathcal{S}$ of critical fibers is also of dimension $\le m-1$. Indeed, if it was m-dimensional there would exist a nonempty open set $U\subset p_1^{-1}(\sigma_1)\backslash(\Sigma_1\cup\mathcal{S}_{\mathrm{low}})$ of regular points of p_1. The image $p_1(U)\subset\sigma_1$ of U is open in $\mathbb{R}^m$ which contradicts to $\dim(\sigma_1)\le m-1$.

For the map $p_1:p_1^{-1}(\sigma_1)\to\sigma_1$ define $B_1:=\{a\in\sigma_1:\dim(p_1^{-1}(a))=1\}$, the semialgebraic set of points in σ_1 for which the fiber $p_1^{-1}(a)$ is infinite. Since $\dim(p_1^{-1}(\sigma_1))\le m-1$ Corollary 4 implies that $\dim(B_1)\le m-2$.

Similarly, for the map $p_1:\mathcal{S}_{\mathrm{low}}\to p_1(\mathcal{S}_{\mathrm{low}})$ let us define $B_2:=\{a\in p_1(\mathcal{S}_{\mathrm{low}}):\dim(p_1^{-1}(a)\cap\mathcal{S}_{\mathrm{low}})=1\}$, the semialgebraic set of points in $p_1(\mathcal{S}_{\mathrm{low}})$ for which the fiber $p_1^{-1}(a)\cap\mathcal{S}_{\mathrm{low}}$ is infinite. Since $\dim(\mathcal{S}_{\mathrm{low}})\le m-1$ Corollary 4 gives $\dim(B_2)\le m-2$.

Take now any $a\notin B_1\cup B_2$. If $a\in\sigma_1$ the fiber $p_1^{-1}(a)$ is finite since $a\notin B_1$. If $a\notin\sigma_1$, it is a regular point of the map $p_1:\mathcal{S}_{\mathrm{top}}\to\mathbb{R}^m$ between two m-dimensional manifolds. Therefore, the semialgebraic set $p_1^{-1}(a)\cap\mathcal{S}_{\mathrm{top}}$ is zero-dimensional manifold, and hence, it is finite. The set $p_1^{-1}(a)\cap\mathcal{S}_{\mathrm{low}}$ is finite because $a\notin B_2$. Consequently, the fiber $p_1^{-1}(a)=(p_1^{-1}(a)\cap\mathcal{S}_{\mathrm{top}})\cup(p_1^{-1}(a)\cap\mathcal{S}_{\mathrm{low}})$ is finite for any point $a\notin B$ out of the at most $(m-2)$-dimensional semialgebraic subset $B:=B_1\cup B_2\subset\mathbb{R}^m$.

(2) $\Leftarrow$ (2′) Recall that $\dim(\sigma_1) \leq m-1$ and let us consider the map $p_1 : \Sigma_1 \to \sigma_1$. If Σ_1 was m-dimensional, the semialgebraic set $B := \{a \in \sigma_1 : \dim(p_1^{-1}(a) \cap \Sigma_1) = 1\}$, by Corollary 4, would be $(m-1)$-dimensional, which would contradict to (2′).

□

The following elementary lemma is frequently used throughout Sect. 3.

Lemma 5 *If $X \subset (\mathbb{R}^m, \|\cdot\|)$ is a scale-invariant semialgebraic variety of dimension $p \leq m$ and $q > 0$, then*

$$\int_{a\in X} \|a\|^q \, e^{-\frac{\|a\|^2}{2}} \mathrm{d}a = \sqrt{2}^{\,p+q-2}\,\Gamma\left(\frac{p+q}{2}\right) |X \cap S^{m-1}| = \sqrt{2}^{\,q} \frac{\Gamma\left(\frac{p+q}{2}\right)}{\Gamma\left(\frac{p}{2}\right)} \int_{a\in X} e^{-\frac{\|a\|^2}{2}} \mathrm{d}a, \quad (16)$$

where $|X \cap S^{m-1}|$ denotes the volume of the $(p-1)$-dimensional semialgebraic spherical set $X \cap S^{m-1}$.

Proof By the smooth coarea formula [14, (A-2)] applied to the submersion $\pi : X_{\text{top}} \to X_{\text{top}} \cap S^{m-1}$, $\pi(a) = a/\|a\|$ whose Normal Jacobian is $1/\|a\|^{p-1}$, we have:

$$\begin{aligned} \int_{a\in X} \|a\|^q \, e^{-\frac{\|a\|^2}{2}} \mathrm{d}a &= \int_0^{+\infty} r^{p+q-1} e^{-\frac{r^2}{2}} dr \; |X \cap S^{m-1}| \\ &= \sqrt{2}^{\,p+q-2}\,\Gamma\left(\frac{p+q}{2}\right) |X \cap S^{m-1}| \end{aligned}$$

Combining this with the same formula for $q = 0$, we obtain the second claim in (16).

□

References

1. Armentano, D., Beltrán, C.: The polynomial eigenvalue problem is well conditioned for random inputs. arXiv:1706.06025 (2017)
2. Basu, S., Lerario, A., Lundberg, E., Peterson, C.: Random fields and the enumerative geometry of lines on real and complex hypersurfaces. arXiv:1610.01205 (2016)
3. Blum, L., Cucker, F., Shub, M., Smale, S.: Complexity and real computation. Springer-Verlag, New York (1998). With a foreword by Richard M. Karp
4. Bochnak, J., Coste, M., Roy, M.F.: Real algebraic geometry, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, vol. 36. Springer-Verlag, Berlin (1998)
5. Breiding, P.: The expected number of Z-eigenvalues of a real gaussian tensor. SIAM Journal on Applied Algebra and Geometry **1**(1), 254–271 (2017)
6. Breiding, P., Kozhasov, Kh., Lerario, A.: On the geometry of the set of symmetric matrices with repeated eigenvalues. Arnold Mathematical Journal (2019). https://doi.org/10.1007/s40598-018-0095-0
7. Bürgisser, P., Cucker, F.: Condition: The geometry of numerical algorithms, *Grundlehren der Mathematischen Wissenschaften*, vol. 349. Springer, Heidelberg (2013)
8. Bürgisser, P., Lerario, A.: Probabilistic Schubert calculus. Journal für die reine und angewandte Mathematik (Crelles Journal) (2018). 10.1515/crelle-2018-0009
9. Coste, M.: An introduction to semialgebraic geometry. RAAG network school **145**, 30 (2002)
10. Dedieu, J.P., Tisseur, F.: Perturbation theory for homogeneous polynomial eigenvalue problems. Linear Algebra Appl. **358**, 71–94 (2003). Special issue on accurate solution of eigenvalue problems (Hagen, 2000)

11. Edelman, A., Kostlan, E., Shub, M.: How many eigenvalues of a random matrix are real? Journal of the American Mathematical Society **7**(1), 247–267 (1994)
12. Guillemin, V., Pollack, A.: Differential topology. Prentice-Hall, Inc., Englewood Cliffs, N.J. (1974)
13. Hammarling, S., Munro, C.J., Tisseur, F.: An algorithm for the complete solution of quadratic eigenvalue problems. ACM Trans. Math. Software **39**(3), Art. 18, 19 (2013)
14. Howard, R.: The kinematic formula in Riemannian homogeneous spaces. Mem. Amer. Math. Soc. **106**(509), vi+69 (1993)
15. Kostlan, E.: On the distribution of roots of random polynomials. In: From Topology to Computation: Proceedings of the Smalefest (Berkeley, CA, 1990), pp. 419–431. Springer, New York (1993)
16. Kozhasov, Kh.: On fully real eigenconfigurations of tensors. SIAM Journal on Applied Algebra and Geometry **2**(2), 339–347 (2018)
17. Lerario, A., Lundberg, E.: Gap probabilities and Betti numbers of a random intersection of quadrics. Discrete Comput. Geom. **55**(2), 462–496 (2016)
18. Mehrmann, V., Voss, H.: Nonlinear eigenvalue problems: a challenge for modern eigenvalue methods. GAMM Mitt. Ges. Angew. Math. Mech. **27**(2), 121–152 (2005) (2004)
19. Shub, M., Smale, S.: Complexity of Bézout's theorem. I. Geometric aspects. J. Amer. Math. Soc. **6**(2), 459–501 (1993)
20. Shub, M., Smale, S.: Complexity of Bézout's theorem II: volumes and probabilities. In: F. Eyssette, A. Galligo (eds.) Computational Algebraic Geometry, *Progress in Mathematics*, vol. 109, pp. 267–285. Birkhäuser (1993)
21. Tisseur, F., Meerbergen, K.: The quadratic eigenvalue problem. SIAM Rev. **43**(2), 235–286 (2001)
22. Tricomi, F.G., Erdélyi, A.: The asymptotic expansion of a ratio of gamma functions. Pacific J. Math. **1**(1), 133–142 (1951)