ON A PROBLEM POSED BY STEVE SMALE

PETER BÜRGISSER AND FELIPE CUCKER

ABSTRACT. The 17th of the problems proposed by Steve Smale for the 21st century asks for the existence of a deterministic algorithm computing an approximate solution of a system of n complex polynomials in n unknowns in time polynomial, on the average, in the size N of the input system. A partial solution to this problem was given by Carlos Beltrán and Luis Miguel Pardo who exhibited a randomized algorithm doing so. In this paper we further extend this result in several directions. Firstly, we exhibit a linear homotopy algorithm that efficiently implements a non-constructive idea of Mike Shub. This algorithm is then used in a randomized algorithm, call it LV, à la Beltrán-Pardo. Secondly, we perform a smoothed analysis (in the sense of Spielman and Teng) of algorithm LV and prove that its smoothed complexity is polynomial in the input size and σ^{-1}, where σ controls the size of of the random perturbation of the input systems. Thirdly, we perform a condition-based analysis of LV. That is, we give a bound, for each system f, of the expected running time of LV with input f. In addition to its dependence on N this bound also depends on the condition of f. Fourthly, and to conclude, we return to Smale's 17th problem as originally formulated for deterministic algorithms. We exhibit such an algorithm and show that its average complexity is $N^{\mathcal{O}(\log\log N)}$. This is nearly a solution to Smale's 17th problem.

CONTENTS

Date: November 6, 2009.
2000 *Mathematics Subject Classification.* 65H20, 65Y20.
Key words and phrases. polynomial equation solving, homotopy methods, approximate zero, complexity, polynomial time, smoothed analysis.
Partially supported by DFG grant BU 1371/2-1 and Paderborn Institute for Scientific Computation (PaSCo).
Partially supported by GRF grant CityU 100808.

1. Introduction

In 2000, Steve Smale published a list of mathematical problems for the 21st century [28]. The 17th problem in the list reads as follows:

> *Can a zero of n complex polynomial equations in n unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?*

Smale pointed out that "it is reasonable" to homogenize the polynomial equations by adding a new variable and to work in projective space after which he made precise the different notions intervening in the question above. We provide these definitions in full detail in Section 2. Before doing so, in the remaining of this section, we briefly describe the recent history of Smale's 17th problem and the particular contribution of the present paper. The following summary of notations should suffice for this purpose.

We denote by $\mathcal{H}_{\mathbf{d}}$ the linear space of complex homogeneous polynomial systems in $n+1$ variables, with a fixed degree pattern $\mathbf{d} = (d_1, \ldots, d_n)$. We let $D = \max_i d_i$, $N = \dim_{\mathbb{C}} \mathcal{H}_{\mathbf{d}}$, and $\mathcal{D} = \prod_i d_i$. We endow this space with the unitarily invariant Bombieri-Weyl Hermitian product and consider the unit sphere $S(\mathcal{H}_{\mathbf{d}})$ with respect to the norm induced by this product. We then make this sphere a probability space by considering the uniform measure on it. The expression "on the average" refers to expectation on this probability space. Also, the expression "approximate zero" refers to a point for which Newton's method, starting at it, converges immediately, quadratically fast.

This is the setting underlying the series of papers [21, 22, 23, 24, 25] — commonly referred to as "the Bézout series"— written by Shub and Smale during the first half of the 1990s, a collection of ideas, methods, and results that pervade all the research done in Smale's 17th problem since this was proposed. The overall idea in the Bézout series is to use a linear homotopy. That is, one starts with a system g and a zero ζ of g and considers the segment $E_{f,g}$ with extremities f and g. Here f is the system whose zero we want to compute. Almost surely, when one moves from g to f, the zero ζ of g follows a curve in projective space to end in a zero of f. The homotopy method consists of dividing the segment $E_{f,g}$ in a number, say k, of subsegments E_i small enough to ensure that an approximate zero x_i of the system at the origin of E_i can be made into an approximate zero x_{i+1} of the system at its end (via one step of Newton's method). The difficulty of this overall idea lies in the following issues:

(1) How does one choose the initial pair (g, ζ)?
(2) How does one choose the subsegments E_i? In particular, how large k should be?

The state of the art at the end of the Bézout series, i.e., in [25], showed an incomplete picture. For (2), the rule consisted of taking a regular subdivision of $E_{f,g}$ for a given k, executing the path-following procedure, and repeating with k replaced by $2k$ if the final point could not be shown to be an approximate zero of f (Shub and Smale provided criteria for checking this). Concerning (1), Shub and Smale proved that good initial pairs (g, ζ) (in the sense that the average number of iterations for the rule above was polynomial in the size of f) existed for each degree pattern $\mathbf{d}$, but they could not exhibit a procedure to generate one such pair.

The next breakthrough took a decade to come. Beltrán and Pardo proposed in [4, 5] that the initial pair (g, ζ) should be randomly chosen. The consideration of randomized algorithms departs from the formulation of Smale's 17th problem[1] but it is widely accepted that, in practical terms, such algorithms are as good as their deterministic siblings. And in the case at hand this departure turned out to pay off. The average (over f) of the expected (over (g, ζ)) number of iterations of the algorithm proposed in [5] is $\mathcal{O}(n^5 N^2 D^3 \log \mathcal{D})$. One of the most notable features of the ideas introduced

[1]In his description of Problem 17 Smale writes "Time is measured by the number of arithmetic operations and comparisons, $\leq$, using real machines (as in Problem 3)" and in the latter he points that, "In [Blum-Shub-Smale,1989] a satisfactory definition [of these machines] is proposed." The paper [9] quoted by Smale deals exclusively with deterministic machines. Furthermore, Smale adds that "a probability measure must be put on the space of all such f, for each $\mathbf{d} = (d_1, \dots, d_n)$, and the time of an algorithm is averaged over the space of f." Hence, the expression 'average time' refers to expectation over the input data only.

by Beltrán and Pardo is the use of a measure on the space of pairs (g,ζ) which is friendly enough to perform a probabilistic analysis while, at the same time, does allow for an efficient sampling.

Shortly after the publication of [4, 5] Shub wrote a short paper of a great importance [20]. Complexity bounds in both the Bézout series and the Beltrán-Pardo results rely on condition numbers. Shub and Smale had introduced a measure of condition $\mu_{\rm norm}(f,\zeta)$ for $f\in\mathcal{H}_{\mathbf{d}}$ and $\zeta\in\mathbb{C}^{n+1}$ which, in case ζ is a zero of f, quantifies how much does ζ vary when f is slightly perturbed. Using this measure they defined the *condition number* of a system f by taking

$$\mu_{\max}(f) := \max_{\zeta\mid f(\zeta)=0}\mu_{\rm norm}(f,\zeta). \tag{1}$$

The bounds mentioned above make use of an estimate for the worst-conditioned system along the segment $E_{f,g}$, that is, of the quantity

$$\max_{q\in E_{f,g}}\mu_{\max}(q). \tag{2}$$

The main result in [20] shows that there exists a partition of $E_{f,g}$ which successfully computes an approximate zero of f whose number k of pieces satisfies

$$k\le CD^{3/2}\int_{q\in E_{f,g}}\mu_2^2(q)\,dq, \tag{3}$$

where C is a constant and μ_2 is the *mean square condition number* of q given by

$$\mu_2^2(q) := \frac{1}{\mathcal{D}}\sum_{\zeta\mid q(\zeta)=0}\mu^2_{\rm norm}(q,\zeta). \tag{4}$$

This partition is explicitly described in [20]. Unfortunately, however, this description does not appear to lead to a constructive procedure to compute the partition.

In an oversight of this non-constructibility, Beltrán and Pardo [6] provided a new version of their randomized algorithm[2] with an improved complexity of $\mathcal{O}(D^{3/2}nN)$.

A first goal of this paper is to validate Beltrán and Pardo's analysis in [6] by exhibiting an efficiently constructible partition of $E_{f,g}$ which satisfies a bound like (3). Our way of doing so owes much to the ideas in [20]. The path-following procedure ALH relying on this partition is described in detail

[2]The algorithm in [6] explicitly calls as a subroutine "the homotopy algorithm of [20]" without noticing that the partition in [20] is non-algorithmic. Actually, the word 'algorithm' is never used in [20]. The main goal of [20], as stated in the abstract, is to motivate "the study of short paths or geodesics in the condition metric" —the proof of (3) does not require the homotopy to be linear and one may wonder whether other paths in $\mathcal{H}_{\mathbf{d}}$ may substantially decrease the integral in the right-hand side. This goal has been addressed, but not attained, in [7]. As of today it remains a fascinating open problem.

in §3.1 together with a result, Theorem 3.1, bounding its complexity as in (3).

The second goal of this paper is to perform a smoothed analysis of a randomized algorithm (essentially Beltrán-Pardo randomization plus ALH) computing a zero of f, which we call LV. What smoothed analysis is, is succinctly explained in the citation of the Gödel prize 2008 awarded to its creators, Daniel Spielman and Teng Shang-Hua[3].

> Smoothed Analysis is a novel approach to the analysis of algorithms. It bridges the gap between worst-case and average case behavior by considering the performance of algorithms under a small perturbation of the input. As a result, it provides a new rigorous framework for explaining the practical success of algorithms and heuristics that could not be well understood through traditional algorithm analysis methods.

In a nutshell, smoothed analysis is a probabilistic analysis which replaces the 'evenly spread' measures underlying the usual average-case analysis (uniform measures, standard normals, ...) by a measure centered at the input data. That is, it replaces the 'average data input' (an unlikely input in actual computations) by a small random perturbation of a worst-case data and substitutes the typical quantity studied in the average-case context,

$$\mathop{\mathbb{E}}_{f\sim\mathcal{R}} \varphi(f),$$

by

$$\sup_{\overline{f}} \mathop{\mathbb{E}}_{f\sim\mathcal{C}(\overline{f},r)} \varphi(f).$$

Here $\varphi(f)$ is the function of f one is interested in (e.g., the complexity of an algorithm over input f), $\mathcal{R}$ is the 'evenly spread' measure mentioned above and $\mathcal{C}(\overline{f},r)$ is an isotropic measure centered at $\overline{f}$ with a dispersion (e.g., variance) given by a (small) parameter $r>0$.

An immediate advantage of smoothed analysis is its robustness with respect to the measure $\mathcal{C}$ (see §3.4 below). This is in contrast with the most common critique to average-case analysis: "A bound on the performance of an algorithm under one distribution says little about its performance under another distribution, and may say little about the inputs that occur in practice" [30].

The precise details of the smoothed analysis we perform for zero finding are in §3.4.

To describe the third goal of this paper we recall Smale's ideas of complexity analysis as exposed in [27]. In this program-setting paper Smale writes that he sees "much of the complexity theory [...] of numerical analysis conveniently represented by a two-part scheme." The first part amounts to

[3]See `http://www.fmi.uni-stuttgart.de/ti/personen/Diekert/citation08.pdf` for the whole citation

obtain, for the running time $\mathsf{time}(f)$ of an algorithm on input f, an estimate of the form

$$\mathsf{time}(f) \leq K(\mathrm{size}(f) + \mu(f))^c \tag{5}$$

where K, c are positive constants and $\mu(f)$ is a condition number for f. The second takes the form

$$\mathrm{Prob}\{\mu(f) \geq T\} \;\leq\; T^{-c} \tag{6}$$

"where a probability measure has been put on the space of inputs." The first part of this scheme provides understanding on the behavior of the algorithm for specific inputs f (in terms of their condition as measured by $\mu(f)$). The second, combined with the first, allows one to obtain probability bounds for $\mathsf{time}(f)$ in terms of $\mathrm{size}(f)$ only. But these bounds say little about $\mathsf{time}(f)$ for actual input data f.

Part one of Smale's program is missing in the work related with his 17th problem. All estimates on the running time of path-following procedures for a given f occurring in both the Bézout series and the work by Beltrán and Pardo are expressed in terms of the quantity in (2) or the integral in (3), not purely in terms of the condition of f. We fill this gap by showing for the expected running time of LV a bound like (5) with $\mu(f) = \mu_{\max}(f)$. The precise statement, Theorem 3.6, is in §3.5 below.

Last but not least, to close this introduction, we return to its opening theme: Smale's 17th problem. Even though randomized algorithms are efficient in theory and reliable in practice they do not offer an answer to the question of the existence of a deterministic algorithm computing approximate zeros of complex polynomial systems in average polynomial time. The situation is akin to the development of primality testing. It was precisely with this problem that randomized algorithms became a means to deal with apparently intractable problems [29, 16]. Yet, the eventual display of a deterministic polynomial-time algorithm [1] was justly welcomed as a major achievement. The fourth main result in this paper exhibits a deterministic algorithm computing approximate zeros in average time $N^{\mathcal{O}(\log\log N)}$. To do so we design and analyze a deterministic homotopy algorithm, call it MD, whose average complexity is polynomial in n and N and exponential in D. This already yields a polynomial-time algorithm when one restricts the degree D to be at most $n^{1-\varepsilon}$ for any fixed $\varepsilon > 0$ (and, in particular, when D is fixed as in a system of quadratic or cubic equations). Algorithm MD is fast when D is small. We complement it with an algorithm that uses a procedure proposed by Jim Renegar [17] and which computes approximate zeros similarly fast when D is large.

In order to prove the results described above we have relied on a number of ideas and techniques. Some of them —e.g., the use of the coarea formula or of the Bombieri-Weyl Hermitian inner product— are taken from the Bézout series and are pervasive in the literature on the subject. Some others — notably the use of the Gaussian distribution and its truncations in Euclidean space instead of the uniform distribution on a sphere or a projective space—are less common. The blending of these ideas has allowed us a development which unifies the treatment of the several situations we consider for zero finding in this paper.

Acknowledgments. We thank Carlos Beltrán, Jean-Pierre Dedieu and Mike Shub for helpful criticism and comments.

2. Preliminaries

2.1. **Setting and Notation.** For $d \in \mathbb{N}$ we denote by $\mathcal{H}_d$ the subspace of $\mathbb{C}[X_0, \dots, X_n]$ of homogeneous polynomials of degree d. For $f \in \mathcal{H}_d$ we write

$$f(x) = \sum_{\alpha} \binom{d}{\alpha}^{1/2} a_\alpha X^\alpha$$

where $\alpha = (\alpha_0, \dots, \alpha_n)$ is assumed to range over all multi-indices such that $|\alpha| = \sum_{k=0}^n \alpha_k = d$, $\binom{d}{\alpha}$ denotes the multinomial coefficient, and $X^\alpha := X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. That is, we take for basis of the linear space $\mathcal{H}_d$ the *Bombieri-Weyl* basis consisting of the monomials $\binom{d}{\alpha}^{1/2} X^\alpha$. A reason to do so is that the Hermitian inner product associated to this basis is unitarily invariant. That is, if $g \in \mathcal{H}_d$ is given by $g(x) = \sum_\alpha \binom{d}{\alpha}^{1/2} b_\alpha X^\alpha$, then the canonical Hermitian inner product

$$\langle f, g \rangle = \sum_{|\alpha|=d} a_\alpha \, \overline{b_\alpha}$$

satisfies, for all element ν in the unitary group $\mathcal{U}(n+1)$, that

$$\langle f, g \rangle = \langle f \circ \nu, g \circ \nu \rangle.$$

Fix $d_1, \dots, d_n \in \mathbb{N} \setminus \{0\}$ and let $\mathcal{H}_{\mathbf{d}} = \mathcal{H}_{d_1} \times \dots \times \mathcal{H}_{d_n}$ be the vector space of polynomial systems $f = (f_1, \dots, f_n)$ with $f_i \in \mathbb{C}[X_0, \dots, X_n]$ homogeneous of degree d_i. The space $\mathcal{H}_{\mathbf{d}}$ is naturally endowed with a Hermitian inner product $\langle f, g \rangle = \sum_{i=1}^n \langle f_i, g_i \rangle$. We denote by $\|f\|$ the corresponding norm of $f \in \mathcal{H}_{\mathbf{d}}$.

Recall that $N = \dim_{\mathbb{C}} \mathcal{H}_{\mathbf{d}}$ and $D = \max_i d_i$. Also, in the rest of this paper, we assume $D \geq 2$ (the case $D = 1$ being solvable with elementary linear algebra).

Let $\mathbb{P}^n := \mathbb{P}(\mathbb{C}^{n+1})$ denote the complex projective space associated to $\mathbb{C}^{n+1}$ and $S(\mathcal{H}_{\mathbf{d}})$ the unit sphere of $\mathcal{H}_{\mathbf{d}}$. These are smooth manifolds that naturally carry the structure of a Riemannian manifold (for $\mathbb{P}^n$ the metric is called Fubini-Study metric). We will denote by $d_{\mathbb{P}}$ and $d_{\mathbb{S}}$ their Riemannian distances which, in both cases, amount to the angle between the arguments. Specifically, for $x, y \in \mathbb{P}^n$ one has

$$\cos d_{\mathbb{P}}(x, y) = \frac{|\langle x, y \rangle|}{\|x\| \, \|y\|}. \tag{7}$$

Ocasionally, for $f, g \in \mathcal{H}_{\mathbf{d}} \setminus \{0\}$, we will abuse language and write $d_{\mathbb{S}}(f,g)$ to denote this angle, that is, the distance $d_{\mathbb{S}}\big(\frac{f}{\|f\|}, \frac{g}{\|g\|}\big)$.

We define the *solution variety* to be

$$V_{\mathbb{P}} := \{(f,\zeta) \in \mathcal{H}_{\mathbf{d}} \times \mathbb{P}^n \mid f \neq 0 \text{ and } f(\zeta) = 0\}.$$

This is a smooth submanifold of $\mathcal{H}_{\mathbf{d}} \times \mathbb{P}^n$ and hence also carries a Riemannian structure. We denote by $V_{\mathbb{P}}(f)$ the zero set of $f \in \mathcal{H}_{\mathbf{d}}$ in $\mathbb{P}^n$. By Bézout's Theorem, it contains $\mathcal{D}$ points for almost all f. Let $Df(\zeta)_{|T_\zeta}$ denote the restriction of the derivative of $f \colon \mathbb{C}^{n+1} \to \mathbb{C}^n$ at ζ to the tangent space $T_\zeta := \{v \in \mathbb{C}^{n+1} \mid \langle v, \zeta\rangle = 0\}$ of $\mathbb{P}^n$ at ζ. The *subvariety of ill-posed pairs* is defined as

$$\Sigma'_{\mathbb{P}} := \{(f,\zeta) \in V_{\mathbb{P}} \mid \mathsf{rank}\, Df(\zeta)_{|T_\zeta} < n\}.$$

Note that $(f,\zeta) \notin \Sigma'_{\mathbb{P}}$ means that ζ is a simple root of f. In this case, by the implicit function theorem, the projection $V_{\mathbb{P}} \to \mathcal{H}_{\mathbf{d}}, (g,x) \mapsto g$ can be locally inverted around (f,ζ). The image Σ of $\Sigma'_{\mathbb{P}}$ under the projection $V_{\mathbb{P}} \to \mathcal{H}_{\mathbf{d}}$ is called the *discriminant variety*.

2.2. **Newton's Method.** In [19], Mike Shub introduced the following projective version of Newton's method. We associate to $f \in \mathcal{H}_{\mathbf{d}}$ (with $Df(x)$ of rank n for some x) a map $N_f : \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{C}^{n+1} \setminus \{0\}$ defined (almost everywhere) by

$$N_f(x) = x - Df(x)^{-1}_{|T_x} f(x).$$

Note that $N_f(x)$ is homogeneous of degree 0 in f and of degree 1 in x so that N_f induces a rational map from $\mathbb{P}^n$ to $\mathbb{P}^n$ (which we will still denote by N_f) and this map is invariant under multiplication of f by constants.

We note that $N_f(x)$ can be computed from f and x very efficiently: since the Jacobian $Df(x)$ can be evaluated with $\mathcal{O}(N)$ arithmetic operations [3], one can do with a total of $\mathcal{O}(N + n^3)$ arithmetic operations.

It is well-known that when x is sufficiently close to a simple zero ζ of f, the sequence of Newton iterates beginning at x will converge quadratically fast to ζ. This property lead Steve Smale to define the following intrinsic notion of approximate zero.

Definition 2.1. By an *approximate zero* of $f \in \mathcal{H}_{\mathbf{d}}$ associated with a zero $\zeta \in \mathbb{P}^n$ of f we understand a point $x \in \mathbb{P}^n$ such that the sequence of Newton iterates (adapted to projective space)

$$x_{i+1} := N_f(x_i)$$

with initial point $x_0 := x$ converges immediately quadratically to ζ, i.e.,

$$d_{\mathbb{P}}(x_i,\zeta) \leq \left(\frac{1}{2}\right)^{2^i - 1} d_{\mathbb{P}}(x_0,\zeta)$$

for all $i \in \mathbb{N}$.

2.3. **Condition Numbers.** How close need x to be from ζ to be an approximate zero? This depends on how well conditioned the zero ζ is.

For $f \in \mathcal{H}_{\mathbf{d}}$ and $x \in \mathbb{C}^{n+1} \setminus \{0\}$ we define the *(normalized) condition number* $\mu_{\mathrm{norm}}(f,x)$ by

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

where the right-hand side norm denotes the spectral norm and $\mathsf{diag}(a_i)$ denotes the diagonal matrix with entries a_i. Note that $\mu_{\mathrm{norm}}(f,x)$ is homogeneous of degree 0 in both arguments, hence it is well defined for $(f,x) \in \mathcal{H}_{\mathbf{d}} \times \mathbb{P}^n$.

The following result (essentially, a γ-Theorem in Smale's theory of estimates for Newton's method [26]) quantifies our claim above.

Theorem 2.2. *Assume $f(\zeta) = 0$ and $d_{\mathbb{P}}(x,\zeta) \le \frac{u_0}{D^{3/2}\mu_{\mathrm{norm}}(f,\zeta)}$ where $u_0 := 3 - \sqrt{7} \approx 0.3542$. Then x is an approximate zero of f associated with ζ.*

Proof. This is an immediate consequence of the projective γ-Theorem in [8, p.263, Thm. 1] combined with the higher derivative estimate [8, p.267, Thm. 2]. □

3. Statement of Main Results

3.1. **The Homotopy Continuation Routine** ALH. Suppose that we are given an input system $f \in \mathcal{H}_{\mathbf{d}}$ and an initial pair (g,ζ) in the solution variety $V_{\mathbb{P}}$ such that f and g are $\mathbb{R}$-linearly independent. Let $\alpha = d_{\mathbb{S}}(f,g)$. Consider the line segment $E_{f,g}$ in $\mathcal{H}_{\mathbf{d}}$ with endpoints f and g. We parameterize this segment by writing

$$E_{f,g} = \{q_\tau \in \mathcal{H}_{\mathbf{d}} \mid \tau \in [0,1]\}$$

with q_τ being the only point in $E_{f,g}$ such that $d_{\mathbb{S}}(g,q_\tau) = \tau\alpha$ (see Figure 1). Explicitly, we have $q_\tau = tf + (1-t)g$, where $t = t(\tau)$ is given by Equation (12). If $E_{f,g}$ does not intersect the discriminant variety Σ, there is a unique continuous map $[0,1] \to V_{\mathbb{P}}, \tau \mapsto (q_\tau,\zeta_\tau)$ such that $(q_0,\zeta_0) = (g,\zeta)$, called the *lifting* of $E_{f,g}$ with origin (g,ζ). In order to find an approximation of the zero ζ_1 of $f = q_1$ we may start with the zero $\zeta = \zeta_0$ of $g = q_0$ and numerically follow the path (q_τ,ζ_τ) by subdividing $[0,1]$ into points $0 = \tau_0 < \tau_1 < \cdots < \tau_k = 1$ and by successively computing approximations x_i of ζ_{τ_i} by Newton's method.

More precisely, we consider the following algorithm ALH (Adaptive Linear Homotopy) with the stepsize parameter $\lambda = 7.53 \cdot 10^{-3}$.

Algorithm ALH

input $f, g \in \mathcal{H}_{\mathbf{d}}$ and $\zeta \in \mathbb{P}^n$ such that $g(\zeta) = 0$

$\alpha := d_{\mathbb{S}}(f, g)$, $r := \|f\|$, $s := \|g\|$

$\tau := 0$, $q := g$, $x := \zeta$

`repeat`

$\Delta\tau := \frac{\lambda}{\alpha D^{3/2} \mu_{\rm norm}^2(q,x)}$

$\tau := \min\{1, \tau + \Delta\tau\}$

$t := \frac{s}{r \sin\alpha \cot(\tau\alpha) - r\cos\alpha + s}$

$q := tf + (1-t)g$

$x := N_q(x)$

`until` $\tau = 1$

`RETURN` x

Our main result for this algorithm, which we will prove in Section 4, is the following.

Theorem 3.1. *The algorithm* ALH *stops after at most* k *steps with*

$$k \le 217\, D^{3/2}\, d_{\mathbb{S}}(f, g) \int_0^1 \mu_{\rm norm}^2(q_\tau, \zeta_\tau)\, d\tau.$$

The returned point x *is an approximate zero of* f *with associated zero* ζ_1.

Remark 3.2. **1.** The bound in Theorem 3.1 is optimal up to a constant factor. This easily follows by an inspection of its proof given in §4.

2. Algorithm ALH requires the computation of $\mu_{\rm norm}$ which, in turn, requires the computation of the operator norm of a matrix. This cannot be done exactly with rational operations and square roots only. We can do, however, with a sufficiently good approximation of $\mu_{\rm norm}^2(q, x)$ and there exist several numerical methods efficiently computing such an approximation. We will therefore neglect this issue pointing, however, for the sceptical reader that another course of action is possible. Indeed, one may replace the operator by the Frobenius norm in the definition of $\mu_{\rm norm}$ and use the bounds $\|M\| \le \|M\|_F \le \sqrt{\mathsf{rank}(M)}\|M\|$ to show that this change preserves the correctness of ALH and adds a multiplicative factor n in the right-hand side of Theorem 3.1. A similar comment applies to the computation of α and $\cot(\tau\alpha)$ in algorithm ALH which cannot be done exactly with rational operations.

3.2. **Randomization and Complexity: the Algorithm LV.** ALH will serve as the basic routine for a number of algorithms computing zeros of polynomial systems in different contexts. In these contexts both the input system f and the origin (g, ζ) of the homotopy may be randomly chosen: in the case of (g, ζ) as a computational technique and in the case of f in order to perform a probabilistic analysis of the algorithm's running time.

In both cases, a probability measure is needed: one for f and one for the pair (g,ζ). The measure for f will depend on the kind of probabilistic analysis (standard average-case or smoothed analysis) we perform. In contrast, we will consider only one measure on $V_{\mathbb{P}}$—which we denote by $\rho_{\mathbf{st}}$— for the initial pair (g,ζ). It consists of drawing g from $\mathcal{H}_{\mathbf{d}}$ from the standard Gaussian distribution (defined via the isomorphism $\mathcal{H}_{\mathbf{d}} \simeq \mathbb{R}^{2N}$ given by the Bombieri-Weyl basis) and then choosing one of the (almost surely) $\mathcal{D}$ zeros of g from the uniform distribution on $\{1,\dots,\mathcal{D}\}$. The formula for the density of $\rho_{\mathbf{st}}$ will be derived later, see Lemma 6.6(5). The above procedure is clearly non-constructive as computing a zero of a system is the problem we wanted to solve in the first place. One of the major contributions in [4] was to show that this drawback can be repaired. The following result (a detailed version of the effective sampling in [6]) will be proved in Section 7 as a special case of more general results we will need in our development.

Proposition 3.3. *We can compute a random pair $(g,\zeta)\in V_{\mathbb{P}}$ according to the density $\rho_{\mathbf{st}}$ with $\mathcal{O}(N)$ choices of random real numbers from the standard Gaussian distribution and $\mathcal{O}(DnN+n^3)$ arithmetic operations (including square roots of positive numbers).*

Algorithms using randomly drawn data are called probabilistic (or randomized). Those that always return a correct output are said to be of type *Las Vegas*. The following algorithm (which uses Proposition 3.3) belongs to this class.

Algorithm LV
input $f\in\mathcal{H}_{\mathbf{d}}$
  `draw` $(g,\zeta)\in V_{\mathbb{P}}$ `from` $\rho_{\mathbf{st}}$
  `run` ALH `on input` (f,g,ζ)

For an input $f\in\mathcal{H}_{\mathbf{d}}$ algorithm LV either outputs an approximate zero x of f or loops forever. By the *running time* $t(f,g,\zeta)$ we will understand the number of elementary operations (i.e., arithmetic operations, elementary functions, and comparisons) performed by LV on input f with initial pair (g,ζ). For fixed f, this is a random variable and its expectation $t(f) := \mathbb{E}_{(g,\zeta)\sim\rho_{\mathbf{st}}}(t(f,g,\zeta))$ is said to be the *expected running time* of LV on input f.

For all f,g,ζ_0, the running time $t(f,g,\zeta)$ is given by the *number of iterations* $K(f,g,\zeta)$ of ALH with input this triple times the cost of an iteration, the latter being dominated by that of computing one Newton iterate (which is $\mathcal{O}(N+n^3)$ independently of the triple (f,g,ζ), see §2.2). It therefore follows that analyzing the expected running times of LV amounts to do so for the expected value —over $(g,\zeta)\in V_{\mathbb{P}}$ drawn from $\rho_{\mathbf{st}}$— of $K(f,g,\zeta)$. We denote this expectation by

$$K(f) := \mathop{\mathbb{E}}_{(g,\zeta)\sim\rho_{\mathbf{st}}}(K(f,g,\zeta)).$$

3.3. **Average Analysis of** LV**.** To talk about average complexity of LV requires specifying a measure for the set of inputs. The most natural choice is the standard Gaussian distribution on $\mathcal{H}_{\mathbf{d}}$. Since $K(f)$ is invariant under scaling, we may equivalently assume that f is chosen in the unit sphere $S(\mathcal{H}_{\mathbf{d}})$ from the uniform distribution. With this choice, we say a Las Vegas algorithm is *average polynomial time* when the average —over $f \in S(\mathcal{H}_{\mathbf{d}})$— of its expected running time is polynomially bounded in the size N of f. The following result shows that LV is average polynomial time. It is essentially the main result in [6] (modulo the existence of ALH and with specific constants).

Theorem 3.4. *The average of the expected number of iterations of Algorithm* LV *is bounded as ($n \geq 4$)*

$$\mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} K(f) \leq 3707\, D^{3/2} N(n+1).$$

3.4. **Smoothed Analysis of** LV**.** A smoothed analysis of an algorithm consists of bounding, for all possible input data $\overline{f}$, the average of its running time (its expected running time if it is a Las Vegas algorithm) over small perturbations of $\overline{f}$. To perform such an analysis, a family of measures (parameterized by a parameter r controlling the size of the perturbation) is considered with the following characteristics:

(1) the density of an element f depends only on the distance $\|f - \overline{f}\|$.
(2) the value of r is closely related to the variance of $\|f - \overline{f}\|$.

Then, the average above is estimated as a function of the data size N and the parameter r, and a satisfying result, which is described by the expression *smoothed polynomial time*, demands that this function is polynomially bounded in r^{-1} and N. Possible choices for the measures' family are the Gaussians $N(\overline{f}, \sigma^2\mathrm{I})$ (used, for instance, in [13, 18, 31, 32]) and the uniform measure on disks $B(\overline{f}, r)$ (used in [2, 10, 11]). Other families may also be used and an emerging impression is that smoothed analysis is robust in the sense that its dependence on the chosen family of measures is low. This tenet was argued for in [14] where a uniform measure is replaced by an adversarial measure (one having a pole at $\overline{f}$) without a significant loss in the estimated averages.

In this paper, for reasons of technical simplicity and consistency with the rest of the exposition, we will work with truncated Gaussians defined as follows. For $\overline{f} \in \mathcal{H}_{\mathbf{d}}$ and $\sigma > 0$ we shall denote by $N(\overline{f}, \sigma^2\mathrm{I})$ the Gaussian distribution on $\mathcal{H}_{\mathbf{d}}$ with mean $\overline{f}$ and covariance matrix $\sigma^2\mathrm{I}$ (defined with respect to the Bombieri-Weyl basis). Further, for $A > 0$ let $P_{A,\sigma} := \mathrm{Prob}\{\|f\| \leq A \mid f \sim N(0, \sigma^2\mathrm{I})\}$. We define the *truncated Gaussian* $N_A(\overline{f}, \sigma^2\mathrm{I})$ with center $\overline{f} \in \mathcal{H}_{\mathbf{d}}$ as the probability measure on $\mathcal{H}_{\mathbf{d}}$ with density

$$\rho(f) = \begin{cases} \frac{\rho_{\overline{f},\sigma}(f)}{P_{A,\sigma}} & \text{if } \|f - \overline{f}\| \leq A \\ 0 & \text{otherwise,} \end{cases} \tag{8}$$

where $\rho_{\overline{f},\sigma}$ denotes the density of $N(\overline{f},\sigma^2\mathrm{I})$. Note that $N_A(\overline{f},\sigma^2\mathrm{I})$ is isotropic around its mean $\overline{f}$.

For our smoothed analysis we will take $A=\sqrt{2N}$. In this case, we have $P_{A,\sigma}\geq\frac{1}{2}$ for all $\sigma\leq 1$ (Lemma 8.2). Note also that $\mathsf{Var}(\|f-\overline{f}\|)\leq\sigma^2$, so that any upper bound polynomial in σ^{-2} is also an upper bound polynomial in $\mathsf{Var}(\|f-\overline{f}\|)^{-1}$.

We can now state our smoothed analysis result for LV.

Theorem 3.5. *For any $0<\sigma\leq 1$, Algorithm LV satisfies*

$$\sup_{\overline{f}\in S(\mathcal{H}_{\mathbf{d}})}\ \mathop{\mathbb{E}}_{f\sim N_A(\overline{f},\sigma^2\mathrm{I})} K(f)\leq 3707\,D^{3/2}\big(N+2^{-1/2}\sqrt{N}\big)(n+1)\,\frac{1}{\sigma}.$$

3.5. **Condition-based Analysis of LV.** We are here interested in estimating $K(f)$ for a fixed input system $f\in S(\mathcal{H}_{\mathbf{d}})$. Such an estimate will have to depend on, besides N, n, and D, the condition of f. We measure the latter using Shub and Smale's [21] $\mu_{\max}(f)$ defined in (1). Our condition-based analysis of LV is summarized in the following statement.

Theorem 3.6. *The expected number of iterations of Algorithm LV with input $f\in S(\mathcal{H}_{\mathbf{d}})\setminus\Sigma$ is bounded as*

$$K(f)\leq 157109\,D^3N(n+1)\mu^2_{\max}(f).$$

3.6. **A Near Solution of Smale's 17th Problem.** We finally want to consider *deterministic* algorithms finding zeros of polynomial systems. Our goal is to exhibit one such algorithm working in nearly-polynomial average time, more precisely in average time $N^{\mathcal{O}(\log\log N)}$. A first ingredient to do so is a deterministic homotopy algorithm which is fast when D is small. This consists of algorithm ALH plus the initial pair $(\overline{U},\boldsymbol{z}_1)$, where $\overline{U}=(\overline{U}_1,\ldots,\overline{U}_n)\in S(\mathcal{H}_{\mathbf{d}})$ with $\overline{U}_i=\frac{1}{\sqrt{2n}}(X_0^{d_i}-X_i^{d_i})$ and $\boldsymbol{z}_1=(1:1:\ldots:1)$.

We consider the following algorithm MD (Moderate Degree):

Algorithm MD
input $f\in\mathcal{H}_{\mathbf{d}}$
  `run` ALH `on input` $(f,\overline{U},\boldsymbol{z}_1)$

We write $K_{\overline{U}}(f):=K(f,\overline{U},\boldsymbol{z}_1)$ for the number of iterations of algorithm MD with input f. We are interested in computing the average over f of $K_{\overline{U}}(f)$ for f randomly chosen in $S(\mathcal{H}_{\mathbf{d}})$ from the uniform distribution.

The complexity of MD is bounded as follows.

Theorem 3.7. *The average number of iterations of Algorithm MD is bounded as*

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} K_{\overline{U}}(f)\leq 314217\,D^3\,N(n+1)^{D+1}.$$

Algorithm MD is efficient when D is small, say, when $D\leq n$. For $D>n$ we use another approach, namely, a real number algorithm designed by Jim Renegar [17] which in this case has a performance similar to that of MD

when $D \le n$. Putting both pieces together we will reach our last main result.

Theorem 3.8. *There is a* deterministic *real number algorithm that on input $f \in \mathcal{H}_{\mathbf{d}}$ computes an approximate zero of f in average time $N^{\mathcal{O}(\log\log N)}$, where $N = \dim \mathcal{H}_{\mathbf{d}}$ measures the size of the input f. Moreover, if we restrict data to polynomials satisfying*

$$D \le n^{\frac{1}{1+\varepsilon}} \quad \text{or} \quad D \ge n^{1+\varepsilon},$$

for some fixed $\varepsilon > 0$, then the average time of the algorithm is polynomial in the input size N.

4. Complexity Analysis of ALH

The goal of this section is to prove Theorem 3.1. An essential component in this proof is an estimate of how much does $\mu_{\mathrm{norm}}(f,\zeta)$ change when f or ζ (or both) are slightly perturbed. The following result gives upper and lower bounds on this variation. It is a precise version, with explicit constants, of Theorem 1 of [20].

Proposition 4.1. *Assume $D \ge 2$. Let $0 < \varepsilon \le 0.13$ be arbitrary and $C \le \frac{\varepsilon}{5.2}$. For all $f, g \in S(\mathcal{H}_{\mathbf{d}})$ and all $x, \zeta \in \mathbb{P}^n$, if $d(f,g) \le \frac{C}{D^{1/2}\mu_{\mathrm{norm}}(f,\zeta)}$ and $d(\zeta,x) \le \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(g,\zeta)}$, then*

$$\frac{1}{1+\varepsilon}\,\mu_{\mathrm{norm}}(g,x) \le \mu_{\mathrm{norm}}(f,\zeta) \le (1+\varepsilon)\mu_{\mathrm{norm}}(g,x). \qquad \square$$

In what follows, we will fix the constants as $\varepsilon = 0.13$ and $C = \frac{\varepsilon}{5.2} = 0.025$.

Remark 4.2. The constants C and ε implicitly occur in the statement of Theorem 3.1 since the 217 therein is a function of these numbers. But their role is not limited to this since they also occur in the algorithm ALH in the parameter $\lambda = \frac{C(1-\varepsilon)}{2(1+\varepsilon)^3}$ controlling the update $\tau + \Delta\tau$ of τ. We note that for the former we could do without precise values by using the big Oh notation. In contrast, we cannot talk of a constructive procedure unless all of its steps are precisely given.

Proof of Theorem 3.1. Let $0 = \tau_0 < \tau_1 < \ldots < \tau_k = 1$ and $\zeta_0 = x_0, x_1, \ldots, x_k$ be the sequences of τ-values and points in $\mathbb{P}^n$ generated by the algorithm ALH. To simplify notation we write q_i instead of q_{τ_i} and ζ_i instead of ζ_{τ_i}.

We claim that, for $i = 0, \ldots, k-1$, the following inequalities are true:

(a) $\quad d_{\mathbb{P}}(x_i,\zeta_i) \le \dfrac{C}{D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)}$

(b) $\quad \dfrac{\mu_{\mathrm{norm}}(q_i,x_i)}{(1+\varepsilon)} \le \mu_{\mathrm{norm}}(q_i,\zeta_i) \le (1+\varepsilon)\mu_{\mathrm{norm}}(q_i,x_i)$

(c) $\quad d_{\mathbb{S}}(q_i,q_{i+1}) \le \dfrac{C}{D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)}$

(d) $d_{\mathbb{P}}(\zeta_i,\zeta_{i+1}) \le \dfrac{C}{D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}\,\dfrac{(1-\varepsilon)}{(1+\varepsilon)}$

(e) $d_{\mathbb{P}}(x_i,\zeta_{i+1}) \le \dfrac{2C}{(1+\varepsilon)D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}$

We proceed by induction showing that

$$(\mathbf{a},i) \Rightarrow (\mathbf{b},i) \Rightarrow ((\mathbf{c},i) \text{ and } (\mathbf{d},i)) \Rightarrow (\mathbf{e},i) \Rightarrow (\mathbf{a},i+1).$$

Inequality (a) for $i=0$ is trivial.

Assume now that (a) holds for some $i \le k-1$. Then, Proposition 4.1 (with $f=g=q_i$) implies

$$\frac{\mu_{\rm norm}(q_i,x_i)}{(1+\varepsilon)} \le \mu_{\rm norm}(q_i,\zeta_i) \le (1+\varepsilon)\mu_{\rm norm}(q_i,x_i)$$

and thus (b). We now show (c) and (d). To do so, let $\tau_* > \tau_i$ be such that $\int_{\tau_i}^{\tau_*}(\|\dot q_\tau\|+\|\dot\zeta_\tau\|)d\tau = \frac{C}{D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}\frac{(1-\varepsilon)}{(1+\varepsilon)}$ or $\tau_*=1$, whichever the smallest. Then, for all $t\in[\tau_i,\tau_*]$,

$$\begin{aligned} d_{\mathbb{P}}(\zeta_i,\zeta_t) &= \int_{\tau_i}^{t}\|\dot\zeta_\tau\|\,d\tau \le \int_{\tau_i}^{\tau_*}(\|\dot q_\tau\|+\|\dot\zeta_\tau\|)d\tau \\ &\le \frac{C}{D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}\,\frac{(1-\varepsilon)}{(1+\varepsilon)} \end{aligned}$$

and, similarly,

$$d_{\mathbb{S}}(q_i,q_t) \le \frac{C}{D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}\,\frac{(1-\varepsilon)}{(1+\varepsilon)} \le \frac{C}{D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}.$$

It is therefore enough to show that $\tau_{i+1}\le\tau_*$. This is trivial if $\tau_*=1$. We therefore assume $\tau_*<1$. The two bounds above allow us to apply Proposition 4.1 and to deduce, for all $\tau\in[\tau_i,\tau_*]$,

$$\mu_{\rm norm}(q_\tau,\zeta_\tau) \le (1+\varepsilon)\mu_{\rm norm}(q_i,\zeta_i).$$

From $\|\dot\zeta_\tau\| \le \mu_{\rm norm}(q_\tau,\zeta_\tau)\,\|\dot q_\tau\|$ (cf. [8, §12.3-12.4]) it follows that

$$\begin{aligned} \frac{C}{D^{3/2}\mu_{\rm norm}(q_i,\zeta_i)}\,\frac{(1-\varepsilon)}{(1+\varepsilon)} &= \int_{\tau_i}^{\tau_*}(\|\dot q_\tau\|+\|\dot\zeta_\tau\|)d\tau \le \int_{\tau_i}^{\tau_*}2\mu_{\rm norm}(q_\tau,\zeta_\tau)\|\dot q_\tau\|d\tau \\ &\le\ 2(1+\varepsilon)\mu_{\rm norm}(q_i,\zeta_i)\int_{\tau_i}^{\tau_*}\|\dot q_\tau\|d\tau\ \le\ 2d_{\mathbb{S}}(q_i,q_{\tau_*})(1+\varepsilon)\mu_{\rm norm}(q_i,\zeta_i). \end{aligned}$$

Consequently, using (b), we obtain

$$d_{\mathbb{S}}(q_i,q_{\tau_*}) \ge \frac{C(1-\varepsilon)}{2(1+\varepsilon)^2D^{3/2}\mu^2_{\rm norm}(q_i,\zeta_i)} \ge \frac{C(1-\varepsilon)}{2(1+\varepsilon)^3D^{3/2}\mu^2_{\rm norm}(q_i,x_i)}.$$

The parameter λ in ALH is chosen as $\frac{C(1-\varepsilon)}{2(1+\varepsilon)^3}$ (or slightly less). By the definition of $\tau_{i+1}-\tau_i$ in ALH we have $\alpha(\tau_{i+1}-\tau_i) = \frac{\lambda}{D^{3/2}\mu^2_{\rm norm}(q_i,x_i)}$. So we obtain

$$d_{\mathbb{S}}(q_i,q_{\tau_*}) \ge \alpha(\tau_{i+1}-\tau_i)\ =\ d_{\mathbb{S}}(q_i,q_{i+1}).$$

This implies $\tau_{i+1} \le \tau_*$ as claimed and hence, inequalities (c) and (d). With them, we may apply Proposition 4.1 to deduce, for all $\tau \in [\tau_i, \tau_{i+1}]$,

$$\frac{\mu_{\mathrm{norm}}(q_i,\zeta_i)}{1+\varepsilon} \le \mu_{\mathrm{norm}}(q_\tau,\zeta_\tau) \le (1+\varepsilon)\mu_{\mathrm{norm}}(q_i,\zeta_i). \tag{9}$$

Next we use the triangle inequality, (a), and (d), to obtain

$$\begin{aligned} d_{\mathbb{P}}(x_i,\zeta_{i+1}) &\le d_{\mathbb{P}}(x_i,\zeta_i) + d_{\mathbb{P}}(\zeta_i,\zeta_{i+1}) \\ &\le \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)} + \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)}\frac{(1-\varepsilon)}{(1+\varepsilon)} \\ &= \frac{2C}{(1+\varepsilon)D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)}, \end{aligned}$$

which proves (e). Theorem 2.2 yields that x_i is an approximate zero of q_{i+1} associated with its zero ζ_{i+1}. Indeed, by our choice of C and ε, we have $2C \le u_0(1+\varepsilon)$ and hence $d_{\mathbb{P}}(x_i,\zeta_{i+1}) \le \frac{u_0}{D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)}$. Therefore, $x_{i+1} = N_{q_{i+1}}(x_i)$ satisfies

$$d_{\mathbb{P}}(x_{i+1},\zeta_{i+1}) \le \frac{1}{2}\, d_{\mathbb{P}}(x_i,\zeta_{i+1}).$$

Using (e) and the right-hand inequality in (9) with $t = t_{i+1}$, we obtain

$$d_{\mathbb{P}}(x_{i+1},\zeta_{i+1}) \le \frac{C}{(1+\varepsilon)D^{3/2}\mu_{\mathrm{norm}}(q_i,\zeta_i)} \le \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(q_{i+1},\zeta_{i+1})},$$

which proves (a) for $i+1$. The claim is thus proved.

The estimate $d_{\mathbb{P}}(x_k,\zeta_k) \le \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(q_k,\zeta_k)}$ just shown for $i = k-1$ implies by Theorem 2.2 that the returned point x_k is an approximate zero of $q_k = f$ with associated zero ζ_1.

Consider now any $i \in \{0,\dots,k-1\}$. Using (9) and (b) we obtain

$$\begin{aligned} \int_{\tau_i}^{\tau_{i+1}} \mu^2_{\mathrm{norm}}(q_\tau,\zeta_\tau)d\tau &\ge \int_{\tau_i}^{\tau_{i+1}} \frac{\mu^2_{\mathrm{norm}}(q_i,\zeta_i)}{(1+\varepsilon)^2}d\tau = \frac{\mu^2_{\mathrm{norm}}(q_i,\zeta_i)}{(1+\varepsilon)^2}(\tau_{i+1}-\tau_i) \\ &\ge \frac{\mu^2_{\mathrm{norm}}(q_i,x_i)}{(1+\varepsilon)^4}(\tau_{i+1}-\tau_i) \\ &= \frac{\mu^2_{\mathrm{norm}}(q_i,x_i)}{(1+\varepsilon)^4}\frac{\lambda}{\alpha D^{3/2}\mu^2_{\mathrm{norm}}(q_i,x_i)} \\ &= \frac{\lambda}{(1+\varepsilon)^4\alpha D^{3/2}} \ \ge\ \frac{1}{217}\frac{1}{\alpha D^{3/2}}. \end{aligned}$$

This implies

$$\int_0^1 \mu^2_{\mathrm{norm}}(q_\tau,\zeta_\tau)d\tau \ge \frac{k}{217}\frac{1}{\alpha D^{3/2}},$$

which proves the stated bound on k. □

5. A Useful Change of Variables

The remaining of this article is devoted to prove Theorems 3.4–3.8. All of them involve expectations —over random f and/or g— of the integral

$$\int_0^1 \mu_2^2(q_\tau)d\tau$$

where, we recall, $\mu_2^2(q_\tau) := \frac{1}{\mathcal{D}}\sum_{\zeta\in V_{\mathbb{P}}(q_\tau)} \mu^2_{\rm norm}(q_\tau,\zeta)$. In all cases, we will eventually deal with such an expectation with f and g Gaussian. Since a linear combination (with fixed coefficients) of two such Gaussian systems is Gaussian as well, it is convenient to parameterize the interval $E_{f,g}$ by a parameter $t\in[0,1]$ representing a ratio of Euclidean distances (instead of a ratio of angles as τ does). Thus we write, abusing notation, $q_t = tf+(1-t)g$. For fixed t, as noted before, q_t follows a Gaussian law. For this new parametrization we have the following result.

Proposition 5.1. *Let $f,g\in\mathcal{H}_{\mathbf{d}}$ be $\mathbb{R}$-linearly independent and $\tau_0\in[0,1]$. Then*

$$d_{\mathbb{S}}(f,g)\int_{\tau_0}^1 \mu_2^2(q_\tau)d\tau \le \int_{t_0}^1 \|f\|\,\|g\|\,\frac{\mu_2^2(q_t)}{\|q_t\|^2}\,dt,$$

where

$$t_0 = \frac{\|g\|}{\|g\|+\|f\|(\sin\alpha\cot(\tau_0\alpha)-\cos\alpha)}$$

is the fraction of the Euclidean distance $\|f-g\|$ corresponding to the fraction τ_0 of the angle $\alpha = d_{\mathbb{S}}(f,g)$.

Proof. For $t\in[0,1]$, abusing notation, we let $q_t = tf+(1-t)g$ and $\tau(t)\in[0,1]$ be such that $\tau(t)\alpha$ is the angle between g and q_t. This defines a bijective map $[t_0,1]\to[\tau_0,1], t\mapsto\tau(t)$. We denote its inverse by $\tau\mapsto t(\tau)$. We claim that

$$\frac{d\tau}{dt} = \frac{\sin\alpha}{\alpha}\,\frac{\|f\|\cdot\|g\|}{\|q_t\|^2}. \tag{10}$$

Note that the stated inequality easily follows from this claim by the transformation formula for integrals together with the bound $\sin\alpha\le 1$.

To prove Claim (10), denote $r=\|f\|$ and $s=\|g\|$. We will explicitly compute $t(\tau)$ by some elementary geometry. For this, we introduce cartesian coordinates in the plane spanned by f and g and assume that g has the coordinates $(s,0)$ and f has the coordinates $(r\cos\alpha, r\sin\alpha)$, see Figure 1.

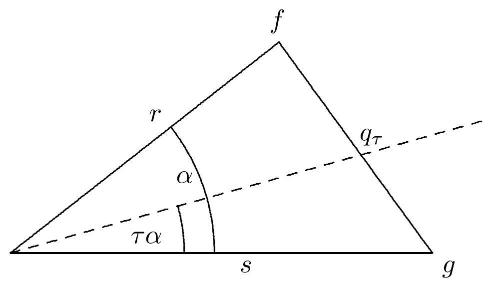

FIGURE 1. Computing $t(\tau)$.

Then, the lines determining q_τ have the equations

$$x = y\,\frac{\cos(\tau\alpha)}{\sin(\tau\alpha)} \qquad \text{and} \qquad x = y\,\frac{r\cos\alpha - s}{r\sin\alpha} + s$$

from where it follows that the coordinate y of q_τ is

$$y = \frac{rs\sin\alpha\sin(\tau\alpha)}{r\sin\alpha\cos(\tau\alpha) - r\cos\alpha\sin(\tau\alpha) + s\sin(\tau\alpha)}. \tag{11}$$

Since $t(\tau) = \frac{y}{r\sin\alpha}$ it follows that

$$t(\tau) = \frac{s}{r\sin\alpha\cot(\tau\alpha) - r\cos\alpha + s}. \tag{12}$$

This implies the stated formula for $t_0 = t(\tau_0)$. Derivating with respect to τ, using (11) and $\sin(\tau\alpha) = \frac{y}{\|q_\tau\|}$, we obtain from (12)

$$\begin{aligned}\frac{dt}{d\tau} &= \frac{\alpha rs\sin\alpha}{(r\sin\alpha\cos(\tau\alpha) - r\cos\alpha\sin(\tau\alpha) + s\sin(\tau\alpha))^2}\\ &= \frac{\alpha y^2}{rs\sin^2(\tau\alpha)\sin\alpha} = \frac{\alpha\|q_{t(\tau)}\|^2}{rs\sin\alpha}.\end{aligned}$$

This finishes the proof of Claim (10). □

In all the cases we will deal with, the factor $\|f\|\,\|g\|$ will be easily bounded and factored out the expectation. We will ultimately face the problem of estimating expectations of the form

$$\mathop{\mathbb{E}}_{q_t\sim N(\overline{q}_t,\sigma_t^2\mathrm{I})}\left(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\right)$$

for different choices of $\overline{q}_t$ and σ_t. In the next section we perform such analysis.

6. Smoothed Analysis of the Mean Square Condition Number

6.1. **Outline.** The goal of this section is to prove the following result.

Theorem 6.1. *Let $\overline{q} \in \mathcal{H}_{\mathbf{d}}$ and $\sigma > 0$. For $q \in \mathcal{H}_{\mathbf{d}}$ drawn from $N(\overline{q}, \sigma^2\mathrm{I})$ we have*

$$\mathop{\mathbb{E}}_{\mathcal{H}_{\mathbf{d}}}\Big(\frac{\mu_2^2(q)}{\|q\|^2}\Big) \;\le\; \frac{e(n+1)}{2\sigma^2}.$$

Note that the assumption does not require a bound on the norm of $\overline{q}$. Indeed, using $\mu_2(\lambda q) = \mu_2(q)$, it is easy to see that the assertion for $\overline{q}, \sigma$ implies the assertion for $\lambda\overline{q}, \lambda\sigma$, for any $\lambda > 0$.

Before going into the details, we give a brief outline of the proof of Theorem 6.1. From now on we will distinguish points $[\zeta] \in \mathbb{P}^n$ from their representatives ζ in the sphere $\mathbb{S}^n := \{\zeta \in \mathbb{C}^{n+1} \mid \|\zeta\| = 1\}$. Note that $[\zeta] \cap \mathbb{S}^n$ is a circle with radius one. It will therefore be necessary to work with the "lifting"

$$V := \{(q,\zeta) \in \mathcal{H}_{\mathbf{d}} \times \mathbb{S}^n \mid q(\zeta) = 0\}$$

of the solution variety $V_{\mathbb{P}}$. Think of choosing (q,ζ) at random from V by first choosing $q \in \mathcal{H}_{\mathbf{d}}$ from $N(\overline{q}, \sigma^2\mathrm{I})$, then choosing one of its $\mathcal{D}$ zeros $[\zeta] \in \mathbb{P}^n$ at random from the uniform distribution on $\{1, \dots, \mathcal{D}\}$, and finally choosing a representative ζ in the unit circle $[\zeta] \cap \mathbb{S}^n$ uniformly at random (we will derive in §6.3 an explicit expression of the corresponding probability density ρ_V on V, see (23)). Then we have (cf. Lemma 6.6)

$$\mathop{\mathbb{E}}_{\mathcal{H}_{\mathbf{d}}}\Big(\frac{\mu_2^2(q)}{\|q\|^2}\Big) \;=\; \mathop{\mathbb{E}}_{V}\Big(\frac{\mu_{\mathrm{norm}}^2(q,\zeta)}{\|q\|^2}\Big), \tag{13}$$

where $\mathbb{E}_{\mathcal{H}_{\mathbf{d}}}$ and $\mathbb{E}_V$ refer to the expectations with respect to the distribution $N(\overline{q}, \sigma^2\mathrm{I})$ on $\mathcal{H}_{\mathbf{d}}$ and the probability density ρ_V on V, respectively.

To estimate the right-hand side in (13) we reduce the problem to one in a space of matrices. This is how. Let $\mathscr{M}$ denote the space $\mathbb{C}^{n\times(n+1)}$ of matrices. In the special case, where all the degrees d_i are one, the solution manifold V specializes to the manifold

$$W := \big\{(M,\zeta) \in \mathscr{M} \times \mathbb{S}^n \mid M\zeta = 0\big\}.$$

Consider the following map of differentiable vector bundles over $\mathbb{S}^n$:

$$\Psi\colon V \to W, (q,\zeta) \mapsto (M,\zeta),\ \text{where } M = \mathsf{diag}(d_i^{-1/2})Dq(\zeta). \tag{14}$$

By the definition of μ_{norm} we have, for $(q,\zeta) \in V$,

$$\mu_{\mathrm{norm}}(q,\zeta) = \|q\| \cdot \|M^\dagger\|,$$

where $M^\dagger = M^*(MM^*)^{-1}$ denotes the Moore-Penrose inverse of M and $\|M^\dagger\|$ its spectral norm. Therefore,

$$\mathop{\mathbb{E}}_{V}\Big(\frac{\mu_{\mathrm{norm}}^2(q,\zeta)}{\|q\|^2}\Big) \;=\; \mathop{\mathbb{E}}_{W}\Big(\|M^\dagger\|^2\Big), \tag{15}$$

where $\mathbb{E}_W$ denotes the expectation with respect to the pushforward density ρ_W of the density ρ_V via the map Ψ.

We have thus reduced our problem to the probability analysis of $\|M^\dagger\|$, which is a quantity closely related to the matrix condition number $\kappa(M) = \|M\|\|M^\dagger\|$. In order to proceed, we need to get some understanding of the probability density ρ_W. For this, it will be useful to consider the projection $p_2 \colon W \to \mathbb{S}^n, (M,\zeta) \mapsto \zeta$ with fibers

$$\mathscr{M}_\zeta := \{M \in \mathscr{M} \mid M\zeta = 0\} \simeq p_2^{-1}(\zeta).$$

The probability density ρ_W defines a pushforward density $\rho_{\mathbb{S}^n}$ on $\mathbb{S}^n$, as well as conditional probability densities $\widetilde{\rho}_{\mathscr{M}_\zeta}$ on the fibers $\mathscr{M}_\zeta$ (see §6.2 for the formal definition) and we have (cf. (20)),

$$\mathop{\mathbb{E}}_{W}\left(\|M^\dagger\|^2\right) \;=\; \mathop{\mathbb{E}}_{\zeta\sim\rho_{\mathbb{S}^n}}\Big(\mathop{\mathbb{E}}_{M\sim\widetilde{\rho}_{\mathscr{M}_\zeta}}\left(\|M^\dagger\|^2\right)\Big), \tag{16}$$

where $\widetilde{\rho}_{\mathscr{M}_\zeta}$ is the density of the conditional distribution of M on $\mathscr{M}_\zeta$. For the proof of Theorem 6.1 it is therefore enough to show that for all $\zeta \in \mathbb{S}^n$

$$\mathop{\mathbb{E}}_{M\sim\widetilde{\rho}_{\mathscr{M}_\zeta}}\left(\|M^\dagger\|^2\right) \;\le\; \frac{e(n+1)}{2\sigma^2}. \tag{17}$$

We will provide the proof of this bound in §6.5. The analysis of the situation reveals that the density $\widetilde{\rho}_{\mathscr{M}_\zeta}$ is closely related to a Gaussian, namely it has the form (c denoting a normalization factor)

$$\widetilde{\rho}_{\mathscr{M}_\zeta}(M) = c \cdot \det(MM^*)\,\rho_{\mathscr{M}_\zeta}(M),$$

where $\rho_{\mathscr{M}_\zeta}$ is a noncentered Gaussian density on $\mathscr{M}_\zeta$. This fact allows one to prove tail bounds similarly as it was done in Sankar et al. [18, §3].

We begin now by recalling the fundamental coarea formula and then proceed in the following subsections by a careful analysis of the geometry of the bundle map $\Psi \colon V \to W$, which allows to compute the resulting probability densities.

6.2. **Coarea Formula.** Suppose that X, Y are Riemannian manifolds of dimensions m, n, respectively such that $m \ge n$. Let $\varphi \colon X \to Y$ be differentiable. By definition, the derivative $d_x\varphi \colon T_xX \to T_{\varphi(x)}Y$ at a regular point $x \in X$ is surjective. Hence the restriction of $d_x\varphi$ to the orthogonal complement of its kernel yields a linear isomorphism. The absolute value of its determinant is called the *normal Jacobian* of φ at x and denoted $\mathrm{NJ}\varphi(x)$. We set $\mathrm{NJ}\varphi(x) := 0$ if x is not a regular point. We note that the fiber $F_y := \varphi^{-1}(y)$ is a Riemannian submanifold of X of dimension $m-n$ if y is a regular value of φ. Sard's lemma states that almost all $y \in Y$ are regular values.

We recall the fundamental coarea formula, sometimes also called Fubini's Theorem for Riemannian manifolds. A proof can be found e.g., in [15, Appendix].

Proposition 6.2. *Suppose that X, Y are Riemannian manifolds of dimensions m, n, respectively, and let $\varphi\colon X \to Y$ be a surjective differentiable map. Put $F_y = \varphi^{-1}(y)$. Then we have for any function $\chi\colon X \to \mathbb{R}$ that is integrable with respect to the volume measure of X that*

$$\int_X \chi\, dX = \int_{y\in Y} \left(\int_{F_y} \frac{\chi}{\mathrm{NJ}\varphi}\, dF_y \right) dY. \qquad \square$$

Now suppose that we are in the situation described in the statement of Proposition 6.2 and we have a probability measure on X with density ρ_X. For a regular value $y \in Y$ we set

$$\rho_Y(y) = \int_{F_y} \frac{\rho_X}{\mathrm{NJ}\varphi}\, dF_y. \tag{18}$$

The coarea formula implies that for all measurable sets $B \subseteq Y$ we have

$$\int_{\varphi^{-1}(B)} \rho_X\, dX = \int_B \rho_Y\, dY.$$

Hence ρ_Y is a probability density on Y. We call it the *pushforward* of ρ_X with respect to φ.

For a regular value $y \in Y$ and $x \in F_y$ we define

$$\rho_{F_y}(x) = \frac{1}{\rho_Y(y)} \frac{\rho_X(x)}{\mathrm{NJ}\varphi(x)}. \tag{19}$$

Clearly, this defines a probability density on F_y. The coarea formula implies that for all measurable functions $\chi\colon X \to \mathbb{R}$

$$\int_X \chi\, \rho_X\, dX = \int_{y\in Y} \left(\int_{F_y} \chi\, \rho_{F_y}\, dF_y \right) \rho_Y(y)\, dY,$$

provided the left-hand integral exists. Therefore, we can interpret ρ_{F_y} as the *density of the conditional distribution* of x in the fiber F_y and briefly express the formula above as

$$\mathop{\mathbb{E}}_{x\sim\rho_X} (\chi(x)) = \mathop{\mathbb{E}}_{y\sim\rho_Y} \big(\mathop{\mathbb{E}}_{x\sim\rho_{F_y}} (\chi(x)) \big). \tag{20}$$

6.3. **The Geometric Situation.** The Bombieri-Weyl Hermitian inner product on $\mathcal{H}_{\mathbf{d}}$ and the standard metric on the sphere $\mathbb{S}^n$ define a Riemannian metric on $\mathcal{H}_{\mathbf{d}} \times \mathbb{S}^n$ on which the unitary group $\mathcal{U}(n+1)$ operates isometrically. The solution variety V is easily seen to be a $\mathcal{U}(n+1)$-invariant Riemannian submanifold of $\mathcal{H}_{\mathbf{d}} \times \mathbb{S}^n$. Note that the fiber $V(q)$ of the projection $\pi_1\colon V \to \mathcal{H}_{\mathbf{d}}, (q,\zeta) \mapsto q$ at $q \in \mathcal{H}_{\mathbf{d}}$ is a disjoint union of $\mathcal{D} = d_1 \cdots d_n$ circles if q does not lie in the discriminant variety Σ. Moreover, the projection $\pi_2\colon V \to \mathbb{S}^n, (q,\zeta) \mapsto \zeta$ defines a vector bundle. In the special case where all the degrees are one, π_2 specializes to the vector bundle $p_2\colon W \to \mathbb{S}^n, (M,\zeta) \mapsto \zeta$ with fibers $\mathscr{M}_\zeta$. The various maps we are considering are summarized in the following commutative diagram

$$\begin{tikzcd}
& \mathbb{S}^n & \\
V \arrow[ur, "\pi_2"] \arrow[rr, "\Psi"] \arrow[d, "\pi_1"'] & & W \arrow[ul, "p_2"'] \arrow[d, "p_1"] \\
\mathcal{H}_{\mathbf{d}} & & \mathscr{M}
\end{tikzcd}$$

FIGURE 2. The geometric situation.

In order to understand the fibers of π_2, we are going to decompose the vector bundle $\pi_2\colon V \to \mathbb{S}^n$ as an orthogonal sum of three subbundles: $V = C \oplus L \oplus R$. The fibers of these subbundles over $\zeta \in \mathbb{S}^n$ are defined as the following linear subspaces of $\mathcal{H}_{\mathbf{d}}$:

$$C_\zeta := \{(c_1\langle X,\zeta\rangle^{d_1},\dots,c_n\langle X,\zeta\rangle^{d_n}) \mid c_1,\dots,c_n \in \mathbb{C}\}$$
$$L_\zeta := \left\{\left(\sqrt{d_1}\langle X,\zeta\rangle^{d_1-1}m_1X,\dots,\sqrt{d_n}\langle X,\zeta\rangle^{d_n-1}m_nX\right) \mid M \in \mathscr{M}_\zeta\right\}$$
$$R_\zeta := \{h \in \mathcal{H}_{\mathbf{d}} \mid h(\zeta)=0, Dh(\zeta)=0\}$$

where m_i denotes the ith row of M. Moreover, given $\zeta \in \mathbb{S}^n$ and $M \in \mathscr{M}_\zeta$, we define $g_{M,\zeta} \in L_\zeta$ by

$$g_{M,\zeta} := \mathsf{diag}\big(\sqrt{d_i}\langle X,\zeta\rangle^{d_i-1}\big)MX.$$

For each ζ this defines a map

$$\mathscr{M}_\zeta \to L_\zeta,\ M \mapsto g_{M,\zeta}. \tag{21}$$

Example 6.3. In case $\zeta = e_0 = (1,0,\dots,0)$ we have

$$\mathscr{M}_{e_0} = \left\{ \left[\begin{array}{c|c} 0 & \\ \vdots & A \\ 0 & \end{array}\right] : A \in \mathbb{C}^{n\times n} \right\}.$$

Note that $\|M^\dagger\| = \|A^{-1}\|$ for $M \in \mathscr{M}_{e_0}$. Also, writing $\overline{X} = (X_1,\dots,X_n)$, we obtain

$$C_{e_0} := \{(c_1X_0^{d_1},\dots,c_nX_0^{d_n}) \mid c_1,\dots,c_n \in \mathbb{C}\}$$
$$L_{e_0} := \left\{\left(\sqrt{d_1}X_0^{d_1-1}A_1\overline{X},\dots,\sqrt{d_n}X_0^{d_n-1}A_n\overline{X}\right) \mid A \in \mathbb{C}^{n\times n}\right\}$$
$$R_{e_0} := \left\{h \in \mathcal{H}_{\mathbf{d}} \mid h_i = \sum_{k=2}^{d_i} X_0^k q_{ik} \text{ with } q_{ik} \in \mathbb{C}[\overline{X}] \text{ homog. of degree } d_i - k\right\}.$$

The next lemma summarizes the properties of the decomposition $V = C \oplus L \oplus R$.

Lemma 6.4. *For all $\zeta \in \mathbb{S}^n$,*

(1) $\mathcal{H}_{\mathbf{d}} = C_\zeta \oplus L_\zeta \oplus R_\zeta$ *is an orthogonal decomposition.*

(2) *The map in* (21) *is a linear isometry (w.r.t. the restriction to $\mathscr{M}_\zeta$ of the standard Hermitian inner product in $\mathscr{M}$).*

(3) $Dg_{M,\zeta}(\zeta) = \mathsf{diag}\big(\sqrt{d_i}\big)M$. *In particular,* $\Psi(g_{M,\zeta},\zeta) = (M,\zeta)$.

(4) *For given $q \in \mathcal{H}_{\mathbf{d}}$, the orthogonal decomposition $q = k + g_{M,\zeta} + h$ with $k \in C_\zeta$, $M = [m_{ij}] \in \mathscr{M}$, and $h \in R_\zeta$ can be computed as*

$$\begin{aligned} k_i &= q_i(\zeta)\langle X,\zeta\rangle^{d_i} \\ m_{ij} &= d_i^{-1/2}\big(\partial_{X_j} q_i(\zeta) - q_i(\zeta)\overline{\zeta_j}\big) \\ h &= q - k - g_{M,\zeta}. \end{aligned}$$

Proof. Since the truth of the first three assertions is preserved under the action of $\mathcal{U}(n+1)$ we may assume that $\zeta = e_0 = (1,0,\ldots,0)$. The validity of part (1) and (2) is now apparent in Example 6.3.

Part (3) is a straightforward calculation.

For Part (4), it is easy to see that $Dk(\zeta)v = \langle v,\zeta\rangle q(\zeta)$ for $v \in \mathbb{C}^{n+1}$. This gives k. Also, $q = k + g_{M,\zeta} + h$ implies, using Part (3),

$$M = \mathsf{diag}(d_i^{-1/2})Dg_{M,\zeta}(\zeta) = \mathsf{diag}(d_i^{-1/2})\big(Dq(\zeta) - Dk(\zeta)\big).$$

The expression for h is trivial. □

Let $(q,\zeta) \in V$. Lemma 6.4 implies that there are uniquely determined $M \in \mathscr{M}_\zeta$ and $h \in R_\zeta$ such that $q = g_{M,\zeta} + h$. Moreover, we have

$$\|q\|^2 = \|g_{M,\zeta}\|^2 + \|h\|^2 = \|M\|_F^2 + \|h\|^2$$

with $\|M\|_F = (\mathrm{tr}(MM^*))^{1/2}$ denoting the Frobenius norm, as well as

$$Dq(\zeta) = Dg_{M,\zeta}(\zeta) = \mathsf{diag}\big(\sqrt{d_i}\big)M.$$

In particular, we get $(M,\zeta) = \Psi(q,\zeta)$ for $(q,\zeta) \in V$, where Ψ is the bundle map from (14). We conclude that for $(M,\zeta) \in W$

$$R_\zeta \to \Psi^{-1}(M,\zeta), h \mapsto (g_{M,\zeta} + h, \zeta) \tag{22}$$

is a bijective map (actually an isometry of Riemannian manifolds).

To apply the coarea formula it is essential to compute the normal Jacobians of the projections π_i, p_i and of the map Ψ. In the next lemma, let $\Sigma' := \pi_1^{-1}(\Sigma) \subseteq V$ denote the inverse image of the discriminant variety Σ.

Proposition 6.5. *Consider the map $\Phi\colon V \to W, (q,\zeta) \mapsto (N,\zeta)$, where $N = Dq(\zeta)$. For $(q,\zeta) \in V \setminus \Sigma'$ we have*

(1) $\mathrm{NJ}\Phi(q,\zeta) = \mathcal{D}^n$.
(2) $\mathrm{NJ}\pi_1(q,\zeta) = \mathrm{NJ}p_1(N,\zeta) = \det(I_n + (N^\dagger)^* N^\dagger)^{-1}$.
(3) $\frac{\mathrm{NJ}p_1(M,\zeta)}{\mathrm{NJ}p_2(M,\zeta)} = \det(MM^*)$.
(4) $\mathrm{NJ}\Psi(q,\zeta) = \frac{1}{\mathcal{D}} \cdot \frac{\mathrm{NJ}p_1(N,\zeta)}{\mathrm{NJ}p_1(M,\zeta)}$.

Proof. (1). This is shown in [6, Lemma 1].

(2) and (3). These are shown in [22] (see also [8, Section 13.2, Lemmas 2-3]) for the projections of the solution varieties lying in $\mathbb{P}^n(\mathcal{H}_{\mathbf{d}}) \times \mathbb{P}^n$. It is straightforward to see that one gets the same normal Jacobian determinants for solutions varieties in $\mathcal{H}_{\mathbf{d}} \times \mathbb{S}^n$.

(4). The scalar multiplication $\mathbb{C} \to \mathbb{C}, z \mapsto \lambda z$ with $\lambda \in \mathbb{C}$ has the Jacobian determinant $|\lambda|^2$. This implies that the map

$$\mathrm{sc}\colon \mathscr{M} \to \mathscr{M}, N \mapsto M = \mathsf{diag}(d_i^{-1/2})N$$

has the Jacobian determinant $\mathcal{D}^{-n-1}$. The assertion follows now from (1) using $\Psi = p_1^{-1} \circ \mathrm{sc} \circ p_1 \circ \Phi$. □

6.4. **Induced Probability Measures.** Fix $\overline{q} \in \mathcal{H}_{\mathbf{d}}$ and $\sigma > 0$ and suppose that a random $q \in \mathcal{H}_{\mathbf{d}}$ is chosen according to the Gaussian distribution $N(\overline{q}, \sigma^2\mathrm{I})$ with mean $\overline{q}$ and isotropic covariance matrix $\sigma^2\mathrm{I}$. The corresponding density shall be denoted by $\rho_{\mathcal{H}_{\mathbf{d}}}$ and $\mathbb{E}_{\mathcal{H}_{\mathbf{d}}}$ stands for expectation taken with respect to that density. We now associate with $\rho_{\mathcal{H}_{\mathbf{d}}}$ the function $\rho_V : V \to \mathbb{R}$ defined by

$$\rho_V(q,\zeta) := \frac{1}{2\pi\mathcal{D}}\, \rho_{\mathcal{H}_{\mathbf{d}}}(q)\, \mathrm{NJ}\pi_1(q,\zeta). \tag{23}$$

The next result shows that ρ_V is the probability density function of the distribution on V we described in §6.1.

Lemma 6.6. (1) *The function ρ_V is a probability density on V.*

(2) *The expectation of any function $\varphi\colon V \to \mathbb{R}$ that is integrable with respect to ρ_V can be expressed as $\mathbb{E}_V(\varphi) = \mathbb{E}_{\mathcal{H}_{\mathbf{d}}}(\varphi_{av})$, where*

$$\varphi_{\mathrm{av}}(q) := \frac{1}{2\pi\mathcal{D}} \int_{V(q)} \varphi\, dV(q)$$

with $V(q) = \{\zeta \in \mathbb{S}^n \mid q(\zeta) = 0\}$.

(3) *The pushforward of ρ_V with respect to π_1 equals $\rho_{\mathcal{H}_{\mathbf{d}}}$.*

(4) *For $q \notin \Sigma$, the conditional density on the fiber $V(q)$ is the density of the uniform distribution on $V(q)$ (which is a disjoint union of $\mathcal{D}$ unit circles).*

(5) *The probability density $\rho_{\mathbf{st}}$ on $V_{\mathbb{P}}$ introduced in §3.2 is obtained from the density ρ_V in the case $\overline{q} = 0$, $\sigma = 1$ as the pushforward under the canonical map $V \to V_{\mathbb{P}}, (f,\zeta) \mapsto (f,[\zeta])$. Explicitly, we have*

$$\rho_{\mathbf{st}}(q,[\zeta]) = \frac{1}{\mathcal{D}}\frac{1}{(2\pi)^N}\, e^{-\frac{1}{2}\|q\|^2}\mathrm{NJ}\pi_1(q,\zeta).$$

Proof. The coarea formula (Proposition 6.2) applied to $\pi_1\colon V \to \mathcal{H}_{\mathbf{d}}$ implies

$$\begin{aligned}
\int_V \varphi\, \rho_V\, dV &= \int_{q\in\mathcal{H}_{\mathbf{d}}} \int_{\zeta\in V(q)} \varphi(q,\zeta) \frac{\rho_V(q,\zeta)}{\mathrm{NJ}\pi_1(q,\zeta)}\, dV(q)\, d\mathcal{H}_{\mathbf{d}} \\
&= \int_{q\in\mathcal{H}_{\mathbf{d}}} \varphi_{\mathrm{av}}(q)\, \rho_{\mathcal{H}_{\mathbf{d}}}(q)\, d\mathcal{H}_{\mathbf{d}}.
\end{aligned}$$

Taking $\varphi = 1$ reveals that ρ_V is a density, proving the first assertion. The above formula also shows the second assertion.

By Equation (18) the pushforward density ρ with respect to π_1 satisfies

$$\rho(q) = \int_{\zeta \in V(q)} \frac{\rho_V(q,\zeta)}{\mathrm{NJ}\pi_1(q,\zeta)}\, dV(q) = \rho_{\mathcal{H}_{\mathbf{d}}}(q).$$

This shows the third assertion. By (19) the conditional density satisfies

$$\rho_{V(q)}(q) = \frac{1}{\rho_{\mathcal{H}_{\mathbf{d}}}(q)}\, \frac{\rho_V(q,\zeta)}{\mathrm{NJ}\pi/x_1(q,\zeta)} = \frac{1}{2\pi\mathcal{D}},$$

which shows the forth assertion. The fifth assertion is trivial. $\square$

We are now going to compute the pushforward density ρ_W of ρ_V with respect to the map $\Psi\colon V \to W$. We will also compute the pushforward density of ρ_W and the conditional density on the fiber $\mathscr{M}_\zeta$ with respect to the projection $p_2\colon W \to \mathbb{S}^n$.

For this purpose, fix $\zeta \in \mathbb{S}^n$ and decompose

$$\overline{q} = \overline{k}_\zeta + \overline{g}_\zeta + \overline{h}_\zeta \tag{24}$$

according to the orthogonal decomposition $\mathcal{H}_{\mathbf{d}} = C_\zeta \oplus L_\zeta \oplus R_\zeta$. Let $\overline{M}_\zeta$ denote the image of $\overline{g}_\zeta$ under the isometry $\gamma_\zeta\colon L_\zeta \to \mathscr{M}_\zeta$. We denote by $\rho_{C_\zeta}, \rho_{\mathscr{M}_\zeta}, \rho_{R_\zeta}$ the densities of the Gaussians in the spaces $C_\zeta, \mathscr{M}_\zeta, R_\zeta$ with covariance matrices $\sigma^2\mathrm{I}$ and means $\overline{k}_\zeta, \overline{M}_\zeta, \overline{h}_\zeta$, respectively. Then, due to the isotropy of the covariance matrices, the density $\rho_{\mathcal{H}_{\mathbf{d}}}$ factors as

$$\rho_{\mathcal{H}_{\mathbf{d}}}(k + g_{M,\zeta} + h) = \rho_{C_\zeta}(k) \cdot \rho_{\mathscr{M}_\zeta}(M) \cdot \rho_{R_\zeta}(h). \tag{25}$$

For instance we have for $k \in C_\zeta$

$$\rho_{C_\zeta}(k) = (\sigma\sqrt{2\pi})^{-2n} \exp\Big(-\frac{1}{2\sigma^2}\|k - \overline{k}_\zeta\|^2 \Big).$$

As $\overline{k}_\zeta$ lies in C_ζ it is of the form $\overline{k}_\zeta = (c_1\langle X,\zeta\rangle^{d_1}, \dots, c_n\langle X,\zeta\rangle^{d_n})$, hence $\overline{q}(\zeta) = \overline{k}_\zeta(\zeta) = (c_1,\dots,c_n)$. This yields $\|\overline{q}(\zeta)\|^2 = \sum_i |c_i|^2 = \|\overline{k}_\zeta\|^2$. Therefore

$$a(\zeta) := \rho_{C_\zeta}(0) = (\sigma\sqrt{2\pi})^{-2n} \exp\Big(-\frac{1}{2\sigma^2}\|\overline{q}(\zeta)\|^2 \Big). \tag{26}$$

Lemma 6.7. (1) *The pushforward density ρ_W of ρ_V with respect to Ψ equals*

$$\rho_W(M,\zeta) = \frac{1}{2\pi}\, a(\zeta) \cdot \rho_{\mathscr{M}_\zeta}(M) \cdot \mathrm{NJ}p_1(M,\zeta).$$

(2) *The conditional density on the fiber $\Psi^{-1}(M,\zeta)$ is induced from the density ρ_{R_ζ} via the isometry $R_\zeta \xrightarrow{\sim} \Psi^{-1}(M,\zeta)$ of (22).*

(3) *The pushforward density $\rho_{\mathbb{S}^n}$ of ρ_W with respect to $p_2\colon W \to \mathbb{S}^n$ equals*

$$\rho_{\mathbb{S}^n}(\zeta) = \frac{1}{2\pi}\, a(\zeta) \cdot \mathop{\mathbb{E}}_{\mathscr{M}_\zeta}(\det(MM^*)),$$

where the expectation refers to the Gaussian density $\rho_{\mathscr{M}_\zeta}$.

(4) *The conditional density $\widetilde{\rho}_{\mathscr{M}_\zeta}$ on the fiber $\mathscr{M}_\zeta$ of $p_2\colon W \to \mathbb{S}^n$ equals*

$$\widetilde{\rho}_{\mathscr{M}_\zeta}(\zeta) = \frac{\det(MM^*)\, \rho_{\mathscr{M}_\zeta}(M)}{\mathbb{E}_{\mathscr{M}_\zeta}(\det(MM^*))}.$$

Proof. Fix $(M,\zeta) \in W$. Equation (18) applied to Ψ yields

$$\rho_W(M,\zeta) = \int_{(q,\zeta)\in\Psi^{-1}(M,\zeta)} \frac{1}{\mathrm{NJ}\Psi(q,\zeta)}\, \rho_V(q,\zeta)\, d\Psi^{-1}(M,\zeta)$$

Recall the isometry $R_\zeta \to \Psi^{-1}(M,\zeta), h \mapsto (g_{M,\zeta}+h,\zeta)$ from (22). The density $\rho_{\mathcal{H}_{\mathbf{d}}}$, according to (25), factors as

$$\rho_{\mathcal{H}_{\mathbf{d}}}(g_{M,\zeta}+h) = \rho_{C_\zeta}(0)\cdot \rho_{\mathscr{M}_\zeta}(M)\cdot \rho_{R_\zeta}(h).$$

In (26) we have set $a(\zeta) = \rho_{C_\zeta}(0)$. Using Proposition 6.5(2), the density ρ_V can be thus written as

$$\rho_V(g_{M,\zeta}+h,\zeta) = \frac{1}{2\pi\mathcal{D}}\, \rho_{\mathcal{H}_{\mathbf{d}}}(g_{M,\zeta}+h)\, \mathrm{NJ}p_1(N,\zeta),$$

where $N = \mathsf{diag}(\sqrt{d_i})M$. Combining these observations with Proposition 6.5(4) and the definition (23) of ρ_V we obtain

$$\begin{aligned}\rho_W(M,\zeta) &= \int_{h\in R_\zeta} \mathcal{D}\,\frac{\mathrm{NJ}p_1(M,\zeta)}{\mathrm{NJ}p_1(N,\zeta)}\,\frac{1}{2\pi\mathcal{D}}\, a(\zeta)\, \rho_{\mathscr{M}_\zeta}(M)\, \rho_{R_\zeta}(h)\, \mathrm{NJ}p_1(N,\zeta)\, dh\\ &= \frac{1}{2\pi}\, a(\zeta)\, \rho_{\mathscr{M}_\zeta}(M)\, \mathrm{NJ}p_1(M,\zeta) \int_{h\in R_\zeta} \rho_{R_\zeta}(h)\, dh\\ &= \frac{1}{2\pi}\, a(\zeta)\, \rho_{\mathscr{M}_\zeta}(M)\, \mathrm{NJ}p_1(M,\zeta),\end{aligned}$$

which proves the first assertion.

By Equation (19), the conditional density in $\Psi^{-1}(M,\zeta)$ is given by

$$\rho_{\Psi^{-1}(M,\zeta)}(q,\zeta) = \frac{1}{\rho_W(M,\zeta)}\, \frac{\rho_V(q,\zeta)}{\mathrm{NJ}\Psi(q,\zeta)}.$$

Plugging in here the definition of ρ_V, the formula for ρ_W from the first assertion, and the expressions for the normal Jacobians of Proposition 6.5, we get, after a short calculation, that $\rho_{\Psi^{-1}(M,\zeta)}(q,\zeta) = \rho_{R_\zeta}(q)$. This proves the second assertion.

Equation (18) applied to p_2 yields, for $\zeta\in\mathbb{S}^n$,

$$\rho_{\mathbb{S}^n}(\zeta) = \int_{M\in\mathscr{M}_\zeta} \frac{1}{\mathrm{NJ}p_2(M,\zeta)}\, \rho_W(M,\zeta)\, dM.$$

Using Proposition 6.5(3) this implies

$$\begin{aligned}\rho_{\mathbb{S}^n}(\zeta) &= \frac{1}{2\pi}\, a(\zeta) \int_{M\in\mathscr{M}_\zeta} \det(MM^*)\rho_{\mathscr{M}_\zeta}(M)\, dM\\ &= \frac{1}{2\pi}\, a(\zeta) \mathop{\mathbb{E}}_{\mathscr{M}_\zeta}(\det(MM^*))\end{aligned}$$

showing the third assertion.

The fourth assertion immediately follows from the first, the third and the definition (19) of the conditional density. □

6.5. **Proof of Theorem 6.1.** In the following we fix $\overline{A} \in \mathbb{C}^{n\times n}$, $\sigma > 0$ and denote by $\rho(A)$ the density of $A \in \mathbb{C}^{n\times n}$ chosen from $N(\overline{A}, \sigma^2\mathrm{I})$. Moreover, we consider the density

$$\widetilde{\rho}(A) = c^{-1}\,|\det A|^2\,\rho(A) \quad \text{where } c := \mathop{\mathbb{E}}_{A\sim\rho}(|\det A|^2).$$

We note that $\widetilde{\rho}$ corresponds to the conditional density $\widetilde{\rho}_{\mathscr{M}_{\zeta_0}}$ in the fiber $\mathscr{M}_{\zeta_0} \simeq \mathbb{C}^{n\times n}$, see Example 6.3 and Lemma 6.7(4).

We shall denote by $S(\mathbb{C}^n)$ the sphere of vectors $v \in \mathbb{C}^n$ with $\|v\| = 1$.

Lemma 6.8. *For any $v \in S(\mathbb{C}^n)$ and any $t > 0$ we have*

$$\mathop{\mathrm{Prob}}_{A\sim\widetilde{\rho}}\Big\{\|A^{-1}v\| \geq t\Big\} \;\leq\; \frac{1}{4\sigma^4 t^4}.$$

Proof. We first claim that, because of unitary invariance, we may assume that $v = e_n := (0,\dots,0,1)$. To see this, take $S \in U(n)$ such that $v = Se_n$. Consider the isometric map $A \mapsto B = S^{-1}A$ which transforms the density $\widetilde{\rho}(A)$ to a density of the same form, namely

$$\widetilde{\rho}'(B) = \widetilde{\rho}(A) = c^{-1}|\det A|^2\rho(A) = c^{-1}|\det B|^2\rho'(B),$$

where $\rho'(B)$ denotes the density of $N(S^{-1}\overline{A}, \sigma^2\mathrm{I})$ and $c = \mathbb{E}_\rho(|\det A|^2) = \mathbb{E}_{\rho'}(|\det B|^2)$. Thus the assertion for e_n and random B (chosen from any isotropic Gaussian distribution) implies the assertion for v and A, noting that $A^{-1}v = B^{-1}e_n$. This proves the claim.

Let a_i denote the ith row of A. Almost surely, the rows $a_1,\dots,a_{n-1}$ are linearly independent. We are going to characterize $\|A^{-1}e_n\|$ in a geometric way. Let $S_n := \mathsf{span}\{a_1,\dots,a_{n-1}\}$ and denote by $a_n^\perp$ the orthogonal projection of a_n onto $S_n^\perp$. Consider $w := A^{-1}e_n$, which is the nth column of A^{-1}. Since $AA^{-1} = \mathrm{I}$ we have $\langle w, a_i\rangle = 0$ for $i = 1,\dots,n-1$ and hence $w \in S_n^\perp$. Moreover, $\langle w, a_n\rangle = 1$, so $\|w\|\,\|a_n^\perp\| = 1$ and we arrive at

$$\|A^{-1}e_n\| = \frac{1}{\|a_n^\perp\|}. \tag{27}$$

Let $A_n \in \mathbb{C}^{(n-1)\times n}$ denote the matrix obtained from A by omitting a_n. We shall write $\mathsf{vol}(A_n) = \det(AA^*)^{1/2}$ for the $(n-1)$-dimensional volume of the parallelepiped spanned by the rows of A_n. Similarly, $|\det A|$ can be interpreted as the n-dimensional volume of the parallelepiped spanned by the rows of A.

Now we write $\rho(A) = \rho_1(A_n)\rho_2(a_n)$ where ρ_1 and ρ_2 are the density functions of $N(\overline{A}_n, \sigma^2\mathrm{I})$ and $N(\overline{a}_n, \sigma^2\mathrm{I})$, respectively (the meaning of $\overline{A}_n$ and $\overline{a}_n$ being clear). Moreover, note that

$$\mathsf{vol}(A)^2 = \mathsf{vol}(A_n)^2\,\|a_n^\perp\|^2.$$

Fubini's Theorem combined with (27) yields for $t > 0$

$$\int_{\|A^{-1}e_n\|\geq t} \mathsf{vol}(A)^2 \rho(A)\, dA \;=\; \int_{A_n\in\mathbb{C}^{(n-1)\times n}} \mathsf{vol}(A_n)^2\, \rho_1(A_n) \cdot \left(\int_{\|a_n^\perp\|\leq 1/t} \|a_n^\perp\|^2 \rho_2(a_n)\, da_n\right) dA_n. \tag{28}$$

We next show that for fixed, linearly independent $a_1,\ldots,a_{n-1}$ and $\lambda > 0$ we have

$$\int_{\|a_n^\perp\|\leq\lambda} \|a_n^\perp\|^2 \rho_2(a_n)\, da_n \leq \frac{\lambda^4}{2\sigma^2}. \tag{29}$$

For this, note that $a_n^\perp \sim N(\overline{a}_n^\perp, \sigma^2\mathrm{I})$ in $S_n^\perp \simeq \mathbb{C}$ where $\overline{a}_n^\perp$ is the orthogonal projection of $\overline{a}_n$ onto $S_n^\perp$. Thus, proving (29) amounts to showing

$$\int_{|z|\leq\lambda} |z|^2 \rho_{\overline{z}}(z) dz \leq \frac{\lambda^4}{2\sigma^2}$$

for the Gaussian density $\rho_{\overline{z}}(z) = \frac{1}{2\pi\sigma^2} e^{-\frac{1}{2\sigma^2}|z-\overline{z}|^2}$ of $z \in \mathbb{C}$, where $\overline{z} \in \mathbb{C}$. Clearly, it is enough to show that

$$\int_{|z|\leq\lambda} \rho_{\overline{z}}(z) dz \leq \frac{\lambda^2}{2\sigma^2}. \tag{30}$$

Without loss of generality we may assume that $\overline{z} = 0$, since the integral in the left-hand side is maximized at this value of $\overline{z}$. Then, writing $z = \sigma w$, we have

$$\begin{aligned}\int_{|z|\leq\lambda} \rho_0(z) dz &= \int_{|w|\leq\frac{\lambda}{\sigma}} \frac{1}{2\pi} e^{-\frac{1}{2}|w|^2}\, dw = \int_0^{\frac{\lambda}{\sigma}} \frac{1}{2\pi} e^{-\frac{1}{2}r^2} 2\pi r\, dr \\ &= -e^{-\frac{1}{2}r^2}\Big|_0^{\frac{\lambda}{\sigma}} = 1 - e^{-\frac{\lambda^2}{2\sigma^2}} \leq \frac{\lambda^2}{2\sigma^2},\end{aligned}$$

which proves inequality (29).

Plugging (29) with $\lambda = \frac{1}{t}$ into (28) we obtain

$$\int_{\|A^{-1}e_n\|\geq t} \mathsf{vol}(A)^2 \rho(A)\, dA \;\leq\; \frac{1}{2\sigma^2 t^4} \mathop{\mathbb{E}}_{\rho_1} \big(\mathsf{vol}(A_n)^2\big).$$

Lemma 6.11, stated in §6.6 below, tells us that

$$\mathop{\mathbb{E}}_{\rho_1} \big(\mathsf{vol}(A_n)^2\big) \leq \frac{1}{2\sigma^2} \mathop{\mathbb{E}}_{\rho} \big(\mathsf{vol}(A)^2\big).$$

Therefore,

$$\int_{\|A^{-1}e_n\|\geq t} \mathsf{vol}(A)^2 \rho(A)\, dA \;\leq\; \frac{1}{4\sigma^4 t^4} \mathop{\mathbb{E}}_{\rho} \big(\mathsf{vol}(A)^2\big).$$

By the definition of the density $\widetilde{\rho}$, this means that

$$\operatorname*{Prob}_{A\sim\widetilde{\rho}} \{\|A^{-1}e_n\| \geq t\} \;\leq\; \frac{1}{4\sigma^4 t^4},$$

which was to be shown. $\square$

Lemma 6.9. *For fixed $u \in S(\mathbb{C}^n)$, $0 \leq s \leq 1$, and random v uniformly chosen in $S(\mathbb{C}^n)$ we have*

$$\operatorname*{Prob}_{v} \Big\{ |u^{\mathrm{T}} v| \geq s \Big\} = (1-s^2)^{n-1}.$$

Proof. Recall the Riemannian distance $d_{\mathbb{P}}$ in $\mathbb{P}^{n-1} := \mathbb{P}(\mathbb{C}^n)$ from (7). Accordingly, for $0 \leq \theta \leq \pi/2$, we have

$$\operatorname*{Prob}_{v} \Big\{ |u^{\mathrm{T}} v| \geq \cos\theta \Big\} = \frac{\mathsf{vol}\big\{[v] \in \mathbb{P}^{n-1} \mid d_{\mathbb{P}}([u],[v]) \leq \theta\big\}}{\mathsf{vol}\,\mathbb{P}^{n-1}} = (\sin\theta)^{2(n-1)},$$

where the last equality is due to [10, Lemma 2.1]. $\square$

The goal is to prove the bound (17) on the conditional expectation in the fibers $\mathscr{M}_\zeta$. For this, we first provide an upper bound on the probability tail. We may assume without loss of generality that $\zeta = e_0$.

Lemma 6.10. *For any $t > 0$ we have*

$$\operatorname*{Prob}_{A\sim\widetilde{\rho}} \Big\{ \|A^{-1}\| \geq t \Big\} \;\leq\; \frac{e^2(n+1)^2}{16\sigma^4}\,\frac{1}{t^4}.$$

Proof. We use an idea in Sankar et al. [18, §3]. For any invertible $A \in \mathbb{C}^{n\times n}$ there exists $u \in S(\mathbb{C}^n)$ such that $\|A^{-1}u\| = \|A^{-1}\|$. For almost all A, the vector u is uniquely determined up to a scaling factor θ of modulus 1. We shall denote by u_A a representative of such u.

The following is an easy consequence of the singular value decomposition of $\|A^{-1}\|$: for any $v \in S(\mathbb{C}^n)$ we have

$$\|A^{-1}v\| \;\geq\; \|A^{-1}\| \cdot |u_A^{\mathrm{T}} v|. \tag{31}$$

We choose now a random pair (A, v) with A following the law $\widetilde{\rho}$ and, independently, $v \in S(\mathbb{C}^n)$ from the uniform distribution. Lemma 6.8 implies that

$$\operatorname*{Prob}_{A,v} \left\{ \|A^{-1}v\| \geq t\sqrt{\frac{2}{n+1}} \right\} \;\leq\; \frac{(n+1)^2}{16\sigma^4 t^4}.$$

On the other hand, we have by (31)

$$\begin{aligned}
&\operatorname*{Prob}_{A,v} \Big\{ \|A^{-1}v\| \geq t\sqrt{2/(n+1)} \Big\} \\
&\quad\geq\; \operatorname*{Prob}_{A,v} \Big\{ \|A^{-1}\| \geq t \;\text{ and }\; |u_A^{\mathrm{T}} v| \geq \sqrt{2/(n+1)} \Big\} \\
&\quad\geq\; \operatorname*{Prob}_{A} \Big\{ \|A^{-1}\| \geq t \Big\} \; \operatorname*{Prob}_{A,v} \Big\{ |u_A^{\mathrm{T}} v| \geq \sqrt{2/(n+1)} \;\Big|\; \|A^{-1}\| \geq t \Big\}.
\end{aligned}$$

Lemma 6.9 tells us that for any fixed $u \in S(\mathbb{C}^n)$ we have

$$\operatorname*{Prob}_v \left\{ |u^{\mathrm{T}}\, v| \geq \sqrt{2/(n+1)} \right\} = (1 - 2/(n+1))^{n-1} \geq e^{-2},$$

the last inequality as $(\frac{n+1}{n-1})^{n-1} = (1 + \frac{2}{n-1})^{n-1} \leq e^2$. We thus obtain

$$\operatorname*{Prob}_A \left\{ \|A^{-1}\| \geq t \right\} \leq e^2 \operatorname*{Prob}_{A,v} \left\{ \|A^{-1}v\| \geq t\sqrt{\frac{2}{n+1}} \right\} \leq \frac{e^2(n+1)^2}{16\sigma^4 t^4},$$

as claimed. □

We can now finally provide the proof of Theorem 6.1.

Proof of Theorem 6.1. Fix $\zeta \in \mathbb{S}^n$ and let $\mathbb{E}$ and Prob refer to the conditional distribution in the fiber $\mathscr{M}_\zeta$ with density $\widetilde{\rho}_{\mathscr{M}_\zeta}$. Lemma 6.10 implies that

$$\operatorname{Prob} \left\{ \|M^\dagger\| \geq T \right\} \;\leq\; \frac{e^2(n+1)^2}{16\sigma^4} \, \frac{1}{T^2}$$

for any $T > 0$. Hence we obtain, for any $T_0 > 0$,

$$\begin{aligned} \mathbb{E}\left(\|M^\dagger\|^2\right) &= \int_0^\infty \operatorname{Prob}\left\{\|M^\dagger\|^2 \geq T\right\} dT \\ &\leq\; T_0 + \textstyle\int_{T_0}^\infty \operatorname{Prob}\left\{\|M^\dagger\|^2 \geq T\right\} dT \;\leq\; T_0 + \frac{e^2(n+1)^2}{16\sigma^4} \, \frac{1}{T_0}, \end{aligned}$$

using $\int_{T_0}^\infty T^{-2}\, dT = T_0^{-1}$. Choosing $T_0 = \frac{e(n+1)}{4\sigma^2}$ yields $\mathbb{E}\left(\|M^\dagger\|^2\right) \leq \frac{e(n+1)}{2\sigma^2}$. This proves the estimate (17) for any $\zeta \in \mathbb{S}^n$. As outlined in §6.1, this completes the proof of Theorem 6.1. □

6.6. **Expected Volume of Parallelepipeds.** Here we complete the proof of Theorem 6.1 by providing the proof of the following result.

Lemma 6.11. *Suppose that $\overline{A} \in \mathbb{C}^{n\times n}$, $\sigma > 0$, and A is chosen from $N(\overline{A}, \sigma^2\mathrm{I})$. Then for any $i \in [n]$ we have*

$$\mathbb{E}\left(\mathsf{vol}(A_i)^2\right) \leq \; \frac{1}{2\sigma^2}\, \mathbb{E}\left(\mathsf{vol}(A)^2\right).$$

In the following we assume $1 \leq m \leq n$. Let us recall a few notations: If $B \in \mathbb{C}^{m\times n}$ then we write $\mathsf{vol}(B) = \mathsf{vol}(b_1, \ldots, b_m) = \det(BB^*)^{1/2}$ for the m-dimensional volume of the parallelepiped spanned by the rows b_i of B. If $i \in [m]$ we denote by B_i the matrix obtained from B by omitting the ith row.

Lemma 6.12. *Suppose $B \in \mathbb{C}^{m\times n}$ is chosen from $N(0, \mathrm{I})$. Then we have* $\mathbb{E}\left(\mathsf{vol}(B)^2\right) = 2^m\, n!/(n-m)!$.

Proof. We denote by b_i the ith row of B. Denote by S the span of fixed linearly independent $b_1, \ldots, b_{m-1}$. We decompose $b_m = b_m^{\|} + b_m^{\perp}$, with $b_m^{\|} \in S$ and $b_m^{\perp} \in S^\perp$. Conditional on $B_m = \{b_1, \ldots, b_{m-1}\}$, the vector $b_m^{\|}$ has the distribution of $N(0, \sigma^2\mathrm{I})$ in $S \simeq \mathbb{C}^{m-1}$ and $b_m^{\perp}$ has the distribution of

$N(0,\sigma^2\mathrm{I})$ in $S^\perp \simeq \mathbb{C}^{n-m+1}$. Moreover, $b_m^{\|}$ and $b_m^\perp$ are independent. Hence $\mathbb{E}(\|b_m^\perp\|^2) = 2(n-m+1)$.

From $\mathsf{vol}(B) = \mathsf{vol}(B_m)\cdot\|b_m^\perp\|$ we get

$$\begin{aligned}\mathbb{E}\left(\mathsf{vol}(B)^2\right) &= \mathbb{E}\left(\mathbb{E}(\|b_m^\perp\|^2 \mid B_m)\,\mathsf{vol}(B_m)\right)\\ &= 2(n-m+1)\,\mathbb{E}\left(\mathsf{vol}(B_m)\right).\end{aligned}$$

The assertion follows by induction. □

We extend the previous result to the case of noncentered Gaussian distributions. Write $[m] := \{1,2,\dots,m\}$.

Lemma 6.13. *Let $\overline{A} \in \mathbb{C}^{m\times n}$ have rows $\overline{a}_i$ and suppose $\sigma > 0$. For a subset $I \subseteq [m]$ of cardinality $0 < k \le m$ we put*

$$\mathsf{rvol}_I^2 := \frac{1}{k!\,(2\sigma^2)^k}\,\mathsf{vol}(\overline{a}_i \mid i \in I)^2.$$

We further set $\mathsf{rvol}_\emptyset^2 := 1$. Suppose $A \in \mathbb{C}^{m\times n}$ is chosen from $N(\overline{A},\sigma^2\mathrm{I})$. Then we have

$$\frac{1}{m!\,(2\sigma^2)^m}\,\mathbb{E}\left(\mathsf{vol}(A)^2\right) = \sum_{k=0}^m \binom{n-k}{m-k}\frac{1}{\binom{m}{k}}\sum_{\substack{I\subseteq[m]\\|I|=k}}\mathsf{rvol}_I^2.$$

Proof. Consider the mth alternating power $\bigwedge^m \mathbb{C}^m$ together with the standard Hermitian inner product. Let a_i denote the ith row of A. Then $\|a_1\wedge\ldots\wedge a_m\| = \mathsf{vol}(a_1,\dots,a_m)$.

Write $a_i = \overline{a}_i + \sigma b_i$ where $b_i \in \mathbb{C}^n$, $b_i \in N(0,\mathrm{I})$, for $i = 1,\dots,m$. The multilinearity of the wedge product then implies that

$$a_1\wedge\ldots\wedge a_m = \sum_{k=0}^m \sigma^{m-k}\sum_{\substack{I\subseteq[m]\\|I|=k}}\bigwedge_{i\in I}\overline{a}_i \wedge \bigwedge_{i\notin I} b_i.$$

This implies

$$\|a_1\wedge\ldots\wedge a_m\|^2 = \sum_{k=0}^m (\sigma^2)^{m-k}\sum_{\substack{I\subseteq[m]\\|I|=k}}\left\|\bigwedge_{i\in I}\overline{a}_i\wedge\bigwedge_{i\notin I} b_i\right\|^2 + \text{ mixed terms.} \tag{32}$$

The expectations of the mixed terms vanish due to the invariance with respect to the transformations $b_i \mapsto \pm b_i$. Therefore,

$$\mathbb{E}\left(\|a_1\wedge\ldots\wedge a_m\|^2\right) = \sum_{k=0}^m (\sigma^2)^{m-k}\sum_{\substack{I\subseteq[m]\\|I|=k}}\mathbb{E}\left(\left\|\bigwedge_{i\in I}\overline{a}_i\wedge\bigwedge_{i\notin I} b_i\right\|^2\right). \tag{33}$$

Let $I = \{1,2,\dots,k\}$ and denote by $b_{k+1}^\perp,\dots,b_m^\perp$ the orthogonal projections of $b_{k+1},\dots,b_m$ onto $\mathsf{span}\{\overline{a}_1,\dots,\overline{a}_k\}^\perp$, respectively. Assume this span has complex dimension k. Then

$$\Big\| \bigwedge_{i\in I} \overline{a}_i \wedge \bigwedge_{i\notin I} b_i \Big\|^2 = \mathsf{vol}(\overline{a}_1,\ldots,\overline{a}_k)^2\, \mathsf{vol}(b_{k+1}^{\perp},\ldots,b_m^{\perp})^2. \tag{34}$$

If $\mathsf{span}\{\overline{a}_1,\ldots,\overline{a}_k\}$ has complex dimension less than k, this equality still holds since both left- and right-hand sides are zero. Note that $(b_{k+1}^{\perp},\ldots,b_m^{\perp})$ is standard normally distributed in $\mathsf{span}\{\overline{a}_1,\ldots,\overline{a}_k\}^{\perp} \simeq \mathbb{C}^{n-k}$. Hence, by Lemma 6.12,

$$\mathbb{E}\left(\mathsf{vol}(b_{k+1}^{\perp},\ldots,b_m^{\perp})^2\right) = 2^{m-k}\,\frac{(n-k)!}{(n-m)!}.$$

We conclude with (33) that

$$\mathbb{E}\left(\|a_1\wedge\ldots\wedge a_m\|^2\right) = \sum_{k=0}^{m} (2\sigma^2)^{m-k}\frac{(n-k)!}{(n-m)!} \sum_{\substack{I\subseteq[m]\\ |I|=k}} \mathsf{vol}(\overline{a}_i \mid i\in I)^2.$$

The assertion follows dividing both sides by $m!\,(2\sigma^2)^m$. □

Proof of Lemma 6.11 . Without loss of generality, take $i=n$. Lemma 6.13 applied to $A_n \in \mathbb{C}^{(n-1)\times n}$ (with $m=n-1$) yields

$$\begin{aligned}\frac{1}{(n-1)!\,(2\sigma^2)^{n-1}}\ \mathbb{E}\left(\mathsf{vol}(A_n)^2\right) &= \sum_{k=0}^{n-1} \frac{n-k}{\binom{n-1}{k}} \sum_{\substack{I\subseteq[n-1]\\ |I|=k}} \mathsf{rvol}_I^2 \\ &= n\sum_{k=0}^{n-1}\frac{1}{\binom{n}{k}} \sum_{\substack{I\subseteq[n-1]\\ |I|=k}} \mathsf{rvol}_I^2 \le n\sum_{k=0}^{n}\frac{1}{\binom{n}{k}} \sum_{\substack{I\subseteq[n]\\ |I|=k}} \mathsf{rvol}_I^2.\end{aligned}$$

By Lemma 6.13 applied to A, the latter equals

$$n\,\frac{1}{n!\,(2\sigma^2)^n}\ \mathbb{E}\left(\mathsf{vol}(A)^2\right),$$

which shows the assertion. □

7. Effective Sampling in the Solution Variety

We turn now to the question of effective sampling in the solution variety endowed with the measure $\rho_{\mathbf{st}}$. More precisely, we provide the proof of Proposition 3.3 stated in Section 3.2.

We specialize the discussion in §6.4 to the case $\overline{q}=0, \sigma=1$ using the notation introduced there. Recall, drawing $(q,[\zeta])\in V_{\mathbb{P}}$ from $\rho_{\mathbf{st}}$ amounts to choosing a system $q\in\mathcal{H}_{\mathbf{d}}$ from the standard Gaussian distribution and then choosing one of the $\mathcal{D}$ projective zeros of q at random from the uniform distribution. This procedure is clearly non-effective, as computing a zero of q is the problem we wanted to solve in the first place. However, the following description of $\rho_{\mathbf{st}}$ suggests that we may proceed differently.

Proposition 7.1. *In the setting of §6.4 suppose $\overline{q} = 0, \sigma = 1$. Then the pushforward density $\rho_{\mathscr{M}}$ of ρ_W with respect to $p_1 \colon W \to \mathscr{M}$ equals the standard Gaussian distribution in $\mathscr{M}$. The conditional distributions in the fibers of p_1 are uniform distributions on unit circles. Moreover, the pushforward density $\rho_{\mathbb{S}^n}$ of ρ_W with respect to $p_2 \colon W \to \mathbb{S}^n$ equals the uniform density on $\mathbb{S}^n$. Finally, the conditional distribution in the fibers of Ψ is induced from the standard Gaussian in R_ζ via the isometry (22).*

Proof. Let $M \in \mathscr{M}$ be of full rank and $\zeta \in \mathbb{S}^n$ such that $M\zeta = 0$. Note that $\rho_W(M, \lambda\zeta) = \rho_W(M, \zeta)$ for $\lambda \in \mathbb{C}$ of absolute value 1. Therefore, Equation (18) yields $\rho_{\mathscr{M}}(M) = 2\pi\rho_W(M, \zeta)/\mathrm{NJ}p_1(M, \zeta)$. Lemma 6.7 implies that $\rho_{\mathscr{M}}(M) = a(\zeta) \cdot \rho_{\mathscr{M}_\zeta}(M)$. In the case $\overline{q} = 0, \sigma = 1$ we have (see (26))

$$a(\zeta) = (2\pi)^{-n}, \quad \rho_{\mathscr{M}_\zeta}(M) = (2\pi)^{-n^2} \exp\Big(-\frac{1}{2}\|M\|_F^2\Big).$$

Hence $\rho_{\mathscr{M}}(M) = a(\zeta)\rho_{\mathscr{M}_\zeta}(M)$ equals the density of the standard Gaussian distribution on $\mathscr{M}$. Equation (19) implies now that the conditional density in the fiber of M equals $1/(2\pi)$, as claimed.

Lemma 6.7(3) shows that $\rho_{\mathbb{S}^n}$ is independent of ζ and hence equals the uniform density on $\mathbb{S}^n$. The last assertion is immediate from Lemma 6.7(2). □

Proof of Proposition 3.3. The procedure for drawing pairs $(g, [\zeta])$ from $\rho_{\mathbf{st}}$ is the following:

(1) choose $M \in \mathscr{M}$ from the standard Gaussian distribution (almost surely M has rank n),
(2) compute the unique $[\zeta] \in \mathbb{P}^n$ such that $M\zeta = 0$,
(3) choose a representative ζ uniformly at random in $[\zeta] \cap \mathbb{S}^n$,
(4) compute $g_{M,\zeta}$,
(5) choose $h \in R_\zeta$ from the standard Gaussian distribution,
(6) compute $q = g_{M,\zeta} + h$ and return $(q, [\zeta])$.

An elegant way of choosing h in step 5 is to draw $q \in \mathcal{H}_{\mathbf{d}}$ from $N(0, \mathrm{I})$ and then to compute the image h of q under the orthogonal projection $\mathcal{H}_\zeta \to R_\zeta$. Since the orthogonal projection of a standard Gaussian is a standard Gaussian, this amounts to draw h from a standard Gaussian in R_ζ. The projection is easily computed using Lemma 6.4(4).

It is easy to check that $\mathcal{O}(N)$ samples from the standard Gaussian distribution on $\mathbb{R}$ are sufficient for implementing this procedure. As for the operation count: step (4) turns out to be the most expensive one and can be done, e.g., as follows. Suppose that all the coefficients of $\langle X, \zeta\rangle^{k-1}$ have already been computed. Then each coefficient of $\langle X, \zeta\rangle^k = (X_0\overline{\zeta}_0 + \cdots + X_n\overline{\zeta}_n)\langle X, \zeta\rangle^{k-1}$ can be obtained by $\mathcal{O}(n)$ arithmetic operations, hence all the coefficients of $\langle X, \zeta\rangle^k$ are obtained with $\mathcal{O}\big(n\binom{n+k}{n}\big)$ operations. It follows that $\langle X, \zeta\rangle^{d_i}$ can be computed with $\mathcal{O}(d_i n N_i)$ operations, hence $\mathcal{O}(DnN)$ operations suffice for the computation of $g_{M,\zeta}$. It is clear that this is also an upper bound on the cost of computing (q, ζ). □

8. Average-case Analysis of LV (proof)

We first draw a conclusion of Theorem 3.1, that we will need several times.

Proposition 8.1. *The expected number of iterations of* ALH *on input* $f \in \mathcal{H}_{\mathbf{d}} \setminus \Sigma$ *is bounded as*

$$K(f) \leq 217\, D^{3/2} \mathop{\mathbb{E}}_{g \in S(\mathcal{H}_{\mathbf{d}})} \left(d_{\mathbb{S}}(f,g) \int_0^1 \mu_2^2(q_\tau) d\tau \right).$$

Proof. Fix $g \in \mathcal{H}_{\mathbf{d}}$ such that the segment $E_{f,g}$ does not intersect the discriminant variety Σ (which is the case for almost all g, as $f \notin \Sigma$). To each of the zeros $\zeta^{(i)}$ of g there corresponds a lifting $[0,1] \to V, \tau \mapsto (q_\tau, \zeta_\tau^{(i)})$ of $E_{f,g}$ such that $\zeta_0^{(i)} = \zeta^{(i)}$. Theorem 3.1 states that

$$K(f,g,\zeta^{(i)}) \leq 217\, D^{3/2}\, d_{\mathbb{S}}(f,g) \int_0^1 \mu_{\mathrm{norm}}^2(q_\tau, \zeta_\tau^{(i)})\, d\tau.$$

Since $\zeta_\tau^{(1)}, \ldots, \zeta_\tau^{(\mathcal{D})}$ are the zeros of q_τ, we have by the definition (4) of the mean square condition number

$$\frac{1}{\mathcal{D}} \sum_{i=1}^{\mathcal{D}} K(f,g,\zeta^{(i)}) \leq 217\, D^{3/2}\, d_{\mathbb{S}}(f,g) \int_0^1 \mu_2^2(q_\tau)\, d\tau. \tag{35}$$

The assertion follows now from (compare Lemma 6.6)

$$K(f) = \mathop{\mathbb{E}}_{(g,\zeta) \sim \rho_{\mathbf{st}}} (K(f,g,\zeta)) = \mathop{\mathbb{E}}_{g \in S(\mathcal{H}_{\mathbf{d}})} \left(\frac{1}{\mathcal{D}} \sum_{i=1}^{\mathcal{D}} K(f,g,\zeta^{(i)}) \right). \qquad \square$$

Theorem 3.1, Proposition 5.1, and Theorem 6.1 now allow us a quick derivation of our remaining main results, Theorems 3.5–3.7. To warm up, we first prove Theorem 3.4. This illustrates the blending of these previous results in a simpler setting.

In the following we set $A := \sqrt{2N}$ and write $P_{A,\sigma} = \mathrm{Prob}\{\|f\| \leq A \mid f \sim N(0, \sigma^2 \mathrm{I})\}$ for $\sigma > 0$.

Lemma 8.2. *We have* $P_{A,\sigma} \geq \frac{1}{2}$ *for all* $0 < \sigma \leq 1$.

Proof. Clearly it suffices to assume $\sigma = 1$. The random variable $\|f\|^2$ is chi-square distributed with $2N$ degrees of freedom. Its mean equals $2N$. In [12, Corollary 6] is is shown that the median of a chi-square distribution is always less than its mean. $\square$

Proof of Theorem 3.4. We use Proposition 8.1 to obtain

$$\begin{aligned}
\mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} K(f) &\leq 217\, D^{3/2} \mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} \mathop{\mathbb{E}}_{g \in S(\mathcal{H}_{\mathbf{d}})} \left(d_{\mathbb{S}}(f,g) \int_0^1 \mu_2^2(q_\tau) d\tau \right) \\
&= 217\, D^{3/2} \mathop{\mathbb{E}}_{f \sim N_A(0,\mathrm{I})} \mathop{\mathbb{E}}_{g \sim N_A(0,\mathrm{I})} \left(d_{\mathbb{S}}(f,g) \int_0^1 \mu_2^2(q_\tau) d\tau \right).
\end{aligned}$$

The equality follows from the fact that, since both $d_{\mathbb{S}}(f,g)$ and $\mu_2^2(q_\tau)$ are homogeneous of degree 0 in both f and g, we may replace the uniform distribution on $S(\mathcal{H}_{\mathbf{d}})$ by any rotationally invariant distribution on $\mathcal{H}_{\mathbf{d}}$, in particular by the centered truncated Gaussian $N_A(0,\mathrm{I})$ defined in (8). Now we use Proposition 5.1 (with $\tau_0 = 0$) to get

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} K(f) \;\le\; 217 D^{3/2} A^2 \mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})} \mathop{\mathbb{E}}_{g\sim N_A(0,\mathrm{I})} \left(\int_0^1 \frac{\mu_2^2(q_t)}{\|q_t\|^2}\, dt\right). \tag{36}$$

Denoting by $\rho_{0,1}$ the density of $N(0,\mathrm{I})$, the right-hand side of (36) equals

$$\begin{aligned}
&217\, D^{3/2} \frac{A^2}{P_{A,1}^2} \int_{\|f\|\le A} \int_{\|g\|\le A} \left(\int_0^1 \frac{\mu_2^2(q_t)}{\|q_t\|^2}\, dt\right) \rho_{0,1}(g)\, \rho_{0,1}(f)\, dg\, df \\
&\le\; 217\, D^{3/2} \frac{A^2}{P_{A,1}^2} \mathop{\mathbb{E}}_{f\sim N(0,\mathrm{I})} \mathop{\mathbb{E}}_{g\sim N(0,\mathrm{I})} \left(\int_0^1 \frac{\mu_2^2(q_t)}{\|q_t\|^2}\, dt\right) \\
&=\; 217\, D^{3/2} \frac{A^2}{P_{A,1}^2} \int_0^1 \mathop{\mathbb{E}}_{q_t\sim N(0,(t^2+(1-t)^2)\mathrm{I})} \left(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\right) dt,
\end{aligned}$$

where the last equality follows from the fact that, for fixed t, the random polynomial system $q_t = tf + (1-t)g$ has a Gaussian distribution with law $N(0, \sigma_t^2\mathrm{I})$, where $\sigma_t^2 := t^2 + (1-t)^2$. Note that we deal with nonnegative integrands, so the interchange of integrals is justified by Tonelli's theorem. By Lemma 8.2 we have $\frac{A^2}{P_{A,1}^2} \le 8N$.

We now apply Theorem 6.1 to deduce that

$$\int_0^1 \mathop{\mathbb{E}}_{q_t\sim N(0,\sigma_t^2\mathrm{I})} \left(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\right) dt \le \frac{e(n+1)}{2} \int_0^1 \frac{dt}{t^2+(1-t)^2} = \frac{e\pi(n+1)}{4}.$$

Consequently,

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} K(f) \le 217\, D^{3/2} \cdot 8N \cdot \frac{e\pi(n+1)}{4} \le 3707\, D^{3/2} N(n+1). \qquad \square$$

Remark 8.3. The proof (modulo the existence of ALH) for the average complexity of LV given by Beltrán and Pardo in [6] differs from the one above. It relies on the fact (elegantly shown by using integral geometry arguments) that, for all $\tau \in [0,1]$, when f and g are uniformly drawn from the sphere, so is $q_\tau/|q_\tau\|$. The extension of this argument to more general situations appears to be considerably more involved. In contrast, as we shall shortly see, the argument based on Gaussians in the proof above carries over, *mutatis mutandis*, to the smoothed analysis context.

9. Smoothed Analysis of LV (proof)

The smoothed analysis of LV is shown similarly to its average-case analysis.

Proof of Theorem 3.5. Fix $\overline{f} \in S(\mathcal{H}_{\mathbf{d}})$. Reasoning as in the proof of Theorem 3.4 and using $\|f\| \le \|\overline{f}\| + \|f - \overline{f}\| \le 1 + A$, we show that

$$\begin{aligned} \mathop{\mathbb{E}}_{f\sim N_A(\overline{f},\sigma^2\mathrm{I})} K(f) &\le 217 D^{3/2} \frac{(A+1)A}{P_{A,\sigma}P_{A,1}} \mathop{\mathbb{E}}_{f\sim N(\overline{f},\sigma^2\mathrm{I})} \mathop{\mathbb{E}}_{g\sim N(0,\mathrm{I})} \left(\int_0^1 \frac{\mu_2^2(q_t)}{\|q_t\|}\, dt \right) \\ &= 217 D^{3/2} \frac{(A+1)A}{P_{A,\sigma}P_{A,1}} \int_0^1 \mathop{\mathbb{E}}_{q_t\sim N(\overline{q}_t,\sigma_t^2\mathrm{I})} \left(\frac{\mu_2^2(q_t)}{\|q_t\|} \right) dt \end{aligned}$$

with $\overline{q}_t = t\overline{f}$ and $\sigma_t^2 = (1-t)^2 + \sigma^2 t^2$. We now apply Theorem 6.1 to deduce

$$\int_0^1 \mathop{\mathbb{E}}_{q_t\sim N(\overline{q}_t,\sigma_t^2\mathrm{I})} \left(\frac{\mu_2^2(q_t)}{\|q_t\|^2} \right) dt \;\le\; \frac{e(n+1)}{2} \int_0^1 \frac{dt}{(1-t)^2 + \sigma^2 t^2} = \frac{e\pi(n+1)}{4\sigma}.$$

Consequently, using Lemma 8.2, we get

$$\mathop{\mathbb{E}}_{f\sim N_A(\overline{f},\sigma^2\mathrm{I})} K(f) \le 217\, D^{3/2} \cdot 4 \cdot (2N + \sqrt{2N})\, \frac{e\pi(n+1)}{4\sigma}$$

which proves the assertion. □

10. Homotopies with a Fixed Extremity

The next two cases we wish to analyze (the condition-based analysis of LV and a solution for Smale's 17th problem with moderate degrees) share the feature that one endpoint of the homotopy segment is fixed, not randomized. This sharing actually allows one to derive both corresponding results (Theorems 3.6 and 3.7, respectively) as a consequence of the following statement.

Theorem 10.1. *For $g \in S(\mathcal{H}_{\mathbf{d}}) \setminus \Sigma$ we have*

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} \left(d_{\mathbb{S}}(f,g) \int_0^1 \mu_2^2(q_\tau) d\tau \right) \le 724\, D^{3/2} N(n+1) \mu_{\max}^2(g) + 0.01.$$

The idea to prove Theorem 10.1 is simple. For small values of τ the system q_τ is close to g and therefore, the value of $\mu_2^2(q_\tau)$ can be bounded by a small multiple of $\mu_{\max}^2(g)$. For the remaining values of τ, the corresponding $t = t(\tau)$ is bounded away from 0 and therefore so is the variance σ_t^2 in the distribution $N(\overline{q}_t, \sigma_t^2\mathrm{I})$ for q_t. This allows one to control the denominator in the right-hand side of Theorem 6.1 when using this result. Here are the precise details.

In the following fix $g \in S(\mathcal{H}_{\mathbf{d}}) \setminus \Sigma$. First note that we may again replace the uniform distribution of f on $S(\mathcal{H}_{\mathbf{d}})$ by the truncated Gaussian $N_A(0,\mathrm{I})$. We therefore need to bound the quantity

$$Q_g := \mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})} \left(d_{\mathbb{S}}(f,g) \int_0^1 \mu_2^2(q_\tau) d\tau \right).$$

To simplify notation, we set as before $\varepsilon = 0.13$, $C = 0.025$, $\lambda = 7.53 \cdot 10^{-3}$, and define

$$\delta_0 := \frac{\lambda}{D^{3/2}\mu_{\max}^2(g)}, \quad t_A := \frac{1}{1 + A + 1.00001\,\frac{A}{\delta_0}}.$$

Proposition 10.2. *We have*

$$Q_g \le (1+\varepsilon)^2\delta_0\,\mu^2_{\max}(g) + \frac{A}{P_{A,1}}\int_{t_A}^1 \mathop{\mathbb{E}}_{q_t\sim N(\overline{q}_t,t^2\mathrm{I})}\left(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\right)dt,$$

where $\overline{q}_t = (1-t)g$.

Proof. Let $\zeta^{(1)},\dots,\zeta^{(\mathcal{D})}$ be the zeros of g and denote by $(q_\tau,\zeta_\tau^{(j)})_{\tau\in[0,1]}$ the lifting of $E_{f,g}$ in V corresponding to the initial pair $(g,\zeta^{(j)})$ and final system $f\in\mathcal{H}_{\mathbf{d}}\setminus\Sigma$.

Equation (9) for $i=0$ in the proof of Theorem 3.1 shows the following: for all j and all $\tau \le \frac{\lambda}{d_{\mathbb{S}}(f,g)D^{3/2}\mu^2_{\mathrm{norm}}(g,\zeta^{(j)})}$ we have

$$\mu_{\mathrm{norm}}(q_\tau,\zeta_\tau^{(j)}) \le (1+\varepsilon)\mu_{\mathrm{norm}}(g,\zeta^{(j)}) \le (1+\varepsilon)\mu_{\max}(g).$$

In particular, this inequality holds for all j and all $\tau\le\frac{\delta_0}{d_{\mathbb{S}}(f,g)}$ and hence, for all such τ, we have

$$\mu_2(q_\tau) \le (1+\varepsilon)\mu_{\max}(g). \tag{37}$$

Splitting the integral in Q_g at $\tau_0(f) := \min\big\{1,\frac{\delta_0}{d_{\mathbb{S}}(f,g)}\big\}$ we obtain

$$Q_g = \mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})}\Big(d_{\mathbb{S}}(f,g)\int_0^{\tau_0(f)}\mu_2^2(q_\tau)\,d\tau\Big) + \mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})}\Big(d_{\mathbb{S}}(f,g)\int_{\tau_0(f)}^1\mu_2^2(q_\tau)\,d\tau\Big).$$

Using (37) we bound the first term in the right-hand side as follows,

$$\mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})}\Big(d_{\mathbb{S}}(f,g)\int_0^{\tau_0(f)}\mu_2^2(q_\tau)\,d\tau\Big) \le (1+\varepsilon)^2\,\delta_0\mu_{\max}(g)^2.$$

To bound the second term, we w.lo.g. assume that $\tau_0(f)\le 1$. We apply Proposition 5.1 to obtain, for a fixed f,

$$d_{\mathbb{S}}(f,g)\int_{\tau_0(f)}^1 \mu_2^2(q_\tau)\,d\tau \le \int_{t_0(f)}^1 \|f\|\frac{\mu_2^2(q_t)}{\|q_t\|^2}\,dt,$$

where $t_0(f)$ is given by

$$t_0(f) = \frac{1}{1+\|f\|(\sin\alpha\cot\delta_0 - \cos\alpha)},\quad \alpha := d_{\mathbb{S}}(f,g).$$

Now note that $\|f\|\le A$ since we draw f from $N_A(0,\mathrm{I})$. This will allow us to bound $t_0(f)$ from below by a quantity independent of f. For $\|f\|\le A$ we have

$$0\le \sin\alpha\cot\delta_0-\cos\alpha \le \frac{1}{\sin\delta_0}-\cos\alpha \le \frac{1}{\sin\delta_0}+1$$

and moreover, $\sin\delta_0 \ge 0.99999\,\delta_0$ since $\delta_0\le 2^{-3/2}\lambda\le 0.00267$. We can therefore bound $t_0(f)$ as

$$t_0(f) \ge \frac{1}{1+A+\frac{A}{\sin(\delta_0)}} \ge \frac{1}{1+A+1.00001\,\frac{A}{\delta_0}} = t_A.$$

We can now bound the second term in Q_g as follows

$$\begin{aligned}
\mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})}\Big(d_{\mathbb{S}}(f,g)\int_{\tau_0(f)}^1 \mu_2^2(q_\tau)\,d\tau\Big) &\le \mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})}\Big(A\int_{t_A}^1 \frac{\mu_2^2(q_t)}{\|q_t\|^2}\,dt\Big)\\
= A\int_{t_A}^1 \mathop{\mathbb{E}}_{f\sim N_A(0,\mathrm{I})}\Big(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\Big)\,dt &\le \frac{A}{P_{A,1}}\int_{t_A}^1 \mathop{\mathbb{E}}_{f\sim N(0,\mathrm{I})}\Big(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\Big)\,dt.
\end{aligned}$$

To conclude, note that, for fixed t and when f is distributed following $N(0,\mathrm{I})$, the variable $q_t = (1-t)g + tf$ follows the Gaussian $N(\overline{q}_t, t^2\mathrm{I})$, where $\overline{g}_t = (1-t)g$. □

Proof of Theorem 10.1. By homogeneity we can replace the uniform distribution on $S(\mathcal{H}_{\mathbf{d}})$ by $N_A(0,\mathrm{I})$, so that we only need to estimate Q_g by the right-hand side of Proposition 10.2. In order to bound the first term there we note that

$$(1+\varepsilon)^2\delta_0\,\mu_{\max}^2(g) = (1+\varepsilon)^2\lambda D^{-3/2} \le (1+\varepsilon)^2\lambda \le 0.01.$$

For bounding the second term we apply Theorem 6.1 to deduce that

$$\begin{aligned}
\int_{t_A}^1 \mathop{\mathbb{E}}_{q_t\sim N(\overline{q}_t,t^2\mathrm{I})}\Big(\frac{\mu_2^2(q_t)}{\|q_t\|^2}\Big)\,dt &\le \int_{t_A}^1 \frac{e(n+1)}{2t^2}\,dt = \frac{e(n+1)}{2}\Big(\frac{1}{t_A}-1\Big)\\
&= \frac{e(n+1)A}{2}\Big(1+\frac{1.00001}{\delta_0}\Big).
\end{aligned}$$

Replacing this bound in Proposition 10.2 we obtain

$$\begin{aligned}
Q_g &\le \frac{eA^2(n+1)}{2P_{A,1}}\Big(1+\frac{1.00001}{\lambda}D^{3/2}\mu_{\max}^2(g)\Big)+0.01\\
&\le 2eN(n+1)D^{3/2}\mu_{\max}^2(g)\Big(\frac{1}{D^{3/2}}+\frac{1.00001}{\lambda}\Big)+0.01\\
&\le 724\,N(n+1)D^{3/2}\mu_{\max}^2(g)+0.01,
\end{aligned}$$

where we used $D\ge 2$ for the last inequality. □

10.1. **Condition-based Analysis of LV (proof).**

Proof of Theorem 3.6. The result follows immediately by combining Proposition 8.1 with Theorem 10.1, with the roles of f and g swapped. □

10.2. **The Complexity of a Deterministic Homotopy Continuation.**

We next prove Theorem 3.7, beginning with some general considerations. The unitary group $\mathcal{U}(n+1)$ naturally acts on $\mathbb{P}^n$ as well as on $\mathcal{H}_{\mathbf{d}}$ via $(\nu, f)\mapsto f\circ\nu^{-1}$. The following lemma results from the unitary invariance of our setting. The proof is immediate.

Lemma 10.3. *Let $g\in\mathcal{H}_{\mathbf{d}}$, $\zeta\in\mathbb{P}^n$ be a zero of g, and $\nu\in\mathcal{U}(n+1)$. Then $\mu_{\mathrm{norm}}(g,\zeta)=\mu_{\mathrm{norm}}(g\circ\nu^{-1},\nu\zeta)$. Moreover, for $f\in\mathcal{H}_{\mathbf{d}}$, we have $K(f,g,\zeta)=K(f\circ\nu^{-1},g\circ\nu^{-1},\nu\zeta)$.* □

Recall $\overline{U}_i = \frac{1}{\sqrt{2n}}(X_0^{d_i} - X_i^{d_i})$ and denote by $z_{(i)}$ a d_ith primitive root of unity. The $\mathcal{D}$ zeros of $\overline{U} = (\overline{U}_1, \ldots, \overline{U}_n)$ are the points $\boldsymbol{z}_j = \big(1 : z_{(1)}^{j_1} : \ldots : z_{(n)}^{j_n}\big) \in \mathbb{P}^n$ for all the possible tuples $j = (j_1, \ldots, j_n)$ with $j_i \in \{0, \ldots, d_i - 1\}$. Clearly, each $\boldsymbol{z}_j$ can be obtained from $\boldsymbol{z}_1 := (1 : 1 : \ldots : 1)$ by a unitary transformation ν_j, which leaves $\overline{U}$ invariant, that is,

$$\nu_j \boldsymbol{z}_1 = \boldsymbol{z}_j, \quad \overline{U} \circ \nu_j^{-1} = \overline{U}.$$

Hence Lemma 10.3 implies $\mu_{\mathrm{norm}}(\overline{U}, \boldsymbol{z}_j) = \mu_{\mathrm{norm}}(\overline{U}, \boldsymbol{z}_1)$ for all j. In particular, $\mu_{\max}(\overline{U}) = \mu_{\mathrm{norm}}(\overline{U}, \boldsymbol{z}_1)$.

Proposition 10.4. $K_{\overline{U}}(f) = K(f, \overline{U}, \boldsymbol{z}_1)$ *satisfies*

$$\mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} K_{\overline{U}}(f) = \mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} \frac{1}{\mathcal{D}} \sum_{j=1}^{\mathcal{D}} K(f, \overline{U}, \boldsymbol{z}_j).$$

Proof. Lemma 10.3 implies for all j

$$K(f, \overline{U}, \boldsymbol{z}_1) = K(f \circ \nu_j^{-1}, \overline{U} \circ \nu_j^{-1}, \nu_j \boldsymbol{z}_1) = K(f \circ \nu_j^{-1}, \overline{U}, \boldsymbol{z}_j).$$

It follows that

$$K_{\overline{U}}(f) = K(f, \overline{U}, \boldsymbol{z}_1) = \frac{1}{\mathcal{D}} \sum_{j=1}^{\mathcal{D}} K(f \circ \nu_j^{-1}, \overline{U}, \boldsymbol{z}_j).$$

The assertion follows now since, for all measurable functions $\varphi\colon S(\mathcal{H}_{\mathbf{d}}) \to \mathbb{R}$ and all $\nu \in \mathcal{U}(n+1)$, we have

$$\mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} \varphi(f) = \mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} \varphi(f \circ \nu),$$

due to the isotropy of the uniform measure on $S(\mathcal{H}_{\mathbf{d}})$, $\square$

Lemma 10.5. *We have*

$$\mu_{\max}^2(\overline{U}) \le 2n \max_i \frac{1}{d_i}(n+1)^{d_i - 1} \le 2\,(n+1)^D.$$

Proof. Recall $\mu_{\max}(\overline{U}) = \mu_{\mathrm{norm}}(\overline{U}, \boldsymbol{z}_1)$, so it suffices to bound $\mu_{\mathrm{norm}}(\overline{U}, \boldsymbol{z}_1)$. Consider $M := \mathsf{diag}(d_i^{-\frac{1}{2}} \|\boldsymbol{z}_1\|^{1-d_i})\, D\overline{U}(\boldsymbol{z}_1) \in \mathbb{R}^{n \times (n+1)}$. By definition we have (cf. §2.3)

$$\mu_{\mathrm{norm}}(\overline{U}, \boldsymbol{z}_1) = \|\overline{U}\|\, \|M^{\dagger}\| = \|M^{\dagger}\| = \frac{1}{\sigma_{\min}(M)},$$

where $\sigma_{\min}(M)$ denotes the smallest singular value of M. It can be characterized as a constrained minimization problem as follows:

$$\sigma_{\min}^2(M) = \min_u \|Mu\|^2 \quad \text{subject to } u \in (\ker M)^{\perp},\ \|u\|^2 = 1.$$

In our situation, $\ker M = \mathbb{R}(1,\dots,1)$ and $D\overline{U}(\boldsymbol{z}_1)$ is given by the following matrix, shown here for $n=3$:

$$D\overline{U}(\boldsymbol{z}_1) = \frac{1}{\sqrt{2n}}\begin{bmatrix} -d_1 & d_1 & 0 & 0 \\ -d_2 & 0 & d_2 & 0 \\ -d_3 & 0 & 0 & d_3 \end{bmatrix}.$$

Hence for $u=(u_0,\dots,u_n)\in\mathbb{R}^{n+1}$,

$$\|Mu\|^2 = \frac{1}{2n}\sum_{i=1}^n \frac{d_i}{(n+1)^{d_i-1}}(u_i-u_0)^2 \geq \frac{1}{2n}\min_i \frac{d_i}{(n+1)^{d_i-1}}\cdot\sum_{i=1}^n (u_i-u_0)^2.$$

A straightforward calculation shows that

$$\sum_{i=1}^n (u_i-u_0)^2 \geq 1 \quad \text{if} \quad \sum_{i=0}^n u_i = 0,\ \sum_{i=0}^n u_i^2 = 1.$$

The assertion follows by combining these observations. □

Proof of Theorem 3.7. Equation (35) in the proof of Proposition 8.1 implies for $g=\overline{U}$ that

$$\frac{1}{\mathcal{D}}\sum_{i=1}^{\mathcal{D}} K(f,\overline{U},\boldsymbol{z}_i) \leq 217\,D^{3/2}\,d_{\mathbb{S}}(f,\overline{U})\int_0^1 \mu_2^2(q_\tau)\,d\tau.$$

Using Proposition 10.4 we get

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} K_{\overline{U}}(f) \leq 217\,D^{3/2} \mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})}\Big(d_{\mathbb{S}}(f,\overline{U})\int_0^1 \mu_2^2(q_\tau)\,d\tau\Big).$$

Applying Theorem 10.1 with $g=\overline{U}$ we obtain

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} K_{\overline{U}}(f) \leq 217\,D^{3/2}\big(724\,D^{3/2}N(n+1)\,\mu_{\max}^2(\overline{U})+0.01\big).$$

We now plug in the bound $\mu_{\max}(\overline{U})^2\leq 2(n+1)^D$ of Lemma 10.5 to obtain

$$\mathop{\mathbb{E}}_{f\in S(\mathcal{H}_{\mathbf{d}})} K_{\overline{U}}(f) \leq 314216\,D^3\,N(n+1)^{D+1} + 2.17\,D^{3/2}.$$

This is bounded from above by $314217\,D^3\,N(n+1)^{D+1}$, which completes the proof. □

11. A near solution to Smale's 17th problem

We finally proceed with the proof of Theorem 3.8. The algorithm we will exhibit uses different routines for $D\leq n$ and $D>n$. Our exposition reflects this structure.

11.1. **The case $D \leq n$.** Theorem 3.7 bounds the number of iterations of Algorithm MD as

$$\mathop{\mathbb{E}}_{f \in S(\mathcal{H}_{\mathbf{d}})} K_{\overline{U}}(f) = \mathcal{O}(D^3 N n^{D+1}).$$

For comparing the order of magnitude of this upper bound to the input size $N = \sum_{i=1}^n \binom{n+d_i}{n}$ we need the following technical lemma (which will be useful for the case $D > n$ as well).

Lemma 11.1. (1) *For $D \leq n$, $n \geq 4$, we have*

$$n^D \leq \binom{n+D}{D}^{\ln n}.$$

(2) *For $D^2 \geq n \geq 1$ we have*

$$\ln n \leq 2 \ln \ln \binom{n+D}{n} + 4.$$

(3) *For $0 < c < 1$ there exists K such that for all n, D*

$$D \leq n^{1-c} \Longrightarrow n^D \leq \binom{n+D}{n}^K.$$

(4) *For $D \leq n$ we have*

$$n^D \leq N^{2 \ln \ln N + \mathcal{O}(1)}.$$

(5) *For $n \leq D$ we have*

$$D^n \leq N^{2 \ln \ln N + \mathcal{O}(1)}.$$

Proof. Stirling's formula states $n! = \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n} e^{\frac{\Theta_n}{12n}}$ with $0 < \Theta_n < 1$. Let $H(x) = x \ln \frac{1}{x} + (1-x) \ln \frac{1}{1-x}$ denote the binary entropy function, defined for $0 < x < 1$. By a straightforward calculation we get from Stirling's formula the following asymptotics for the binomial coefficient: for any $0 < m < n$ we have

$$\ln \binom{n}{m} = nH\Big(\frac{m}{n}\Big) + \frac{1}{2} \ln \frac{n}{m(n-m)} - 1 + \varepsilon_{n,m}, \tag{38}$$

where $-0.1 < \varepsilon_{n,m} < 0.2$.

(1) The first claim is equivalent to $e^D \leq \binom{n+D}{D}$. The latter is easily checked for $D \in \{1, 2, 3\}$ and $n \geq 4$. So assume $n \geq D \geq 4$. By monotonicity it suffices to show that $e^D \leq \binom{2D}{D}$ for $D \geq 4$. Equation (38) implies

$$\ln \binom{2D}{D} > 2D \ln 2 + \frac{1}{2} \ln \frac{2}{D} - 1.1$$

and the right-hand side is easily checked to be at least D, for $D \geq 4$.

(2) If $D \geq m := \sqrt{n}$ then $\binom{n+D}{n} \geq \binom{n+\lceil \sqrt{n} \rceil}{n}$. Equation (38) implies

$$\ln \binom{n + \lceil \sqrt{n} \rceil}{n} \geq (n+m) H\Big(\frac{m}{n+m}\Big) + \frac{1}{2} \ln \frac{1}{m} - 1.1.$$

The entropy function can be bounded as

$$H\Big(\frac{m}{n+m}\Big) \geq \frac{m}{n+m}\ln\Big(1+\frac{n}{m}\Big) \geq \frac{m}{n+m}\,\ln m.$$

It follows that

$$\ln\binom{n+\lceil\sqrt{n}\rceil}{n} \geq \frac{1}{2}\sqrt{n}\,\ln n - \frac{1}{4}\ln n - 1.1 \geq \frac{1}{4}\sqrt{n}\,\ln n$$

the right-hand inequality holding for $n \geq 10$. Hence

$$\ln\ln\binom{n+\lceil\sqrt{n}\rceil}{n} \geq \frac{1}{2}\ln n + \ln\ln n - \ln 4 \geq \frac{1}{2}\ln n - 2,$$

the right-hand inequality holding for $n \geq 2$. This shows the second claim for $n \geq 10$. The cases $n \leq 9$ are easily directly checked.

(3) Writing $D = n\delta$ we obtain from Equation (38)

$$\ln\binom{n+D}{n} = (n+D)H\Big(\frac{\delta}{1+\delta}\Big) - \frac{1}{2}\ln D + \mathcal{O}(1).$$

Estimating the entropy function yields

$$H\Big(\frac{\delta}{1+\delta}\Big) \geq \frac{\delta}{1+\delta}\ln\Big(1+\frac{1}{\delta}\Big) \geq \frac{\delta}{2}\,\ln\frac{1}{\delta} = \frac{\delta\varepsilon}{2}\,\ln n,$$

where ε is defined by $\delta = n^{-\varepsilon}$. By assumption, $\varepsilon \geq c$. From the last two lines we get

$$\frac{1}{D\ln n}\ln\binom{n+D}{n} \;\geq\; \frac{c}{2} - \frac{1-c}{2D} + \mathcal{O}\Big(\frac{1}{\ln n}\Big).$$

In the case $c \leq \frac{3}{4}$ we have $D \geq n^{1/4}$ and we bound the above by

$$\frac{c}{2} - \frac{1}{2n^{1/4}} + \mathcal{O}\Big(\frac{1}{\ln n}\Big),$$

which is greater than $c/4$ for sufficiently large n. In the case $c \geq \frac{3}{4}$ we bound as follows

$$\frac{1}{D\ln n}\ln\binom{n+D}{n} \;\geq\; \frac{c}{2} - \frac{1-c}{2} + \mathcal{O}\Big(\frac{1}{\ln n}\Big) = c - \frac{1}{2} + \mathcal{O}\Big(\frac{1}{\ln n}\Big) \geq \frac{1}{5}$$

for sufficiently large n.

We have shown that for $0 < c < 1$ there exists n_c such that for $n \geq n_c$, $D \leq n^{1-c}$, we have

$$n^D \leq \binom{n+D}{n}^{K_c},$$

where $K_c := \max\{4/c, 5\}$. By increasing K_c we can achieve that the above inquality holds for all n, D with $D \leq n^{1-c}$.

(4) Clearly, $N \geq \binom{n+D}{n}$. If $D \leq \sqrt{n}$ then, by part (3), there exists K such that

$$n^D \leq \binom{n+D}{n}^{K} \leq N^K.$$

Otherwise $D \in [\sqrt{n}, n]$ and the desired inequality is an immediate consequence of parts (1) and (2).

(5) Use $\binom{n+D}{n} = \binom{n+D}{D}$ and swap the roles of n and D in part (4) above. $\square$

Theorem 3.7 combined with Lemma 11.1(4) implies that

$$\mathop{\mathbb{E}}_{f} K_{\overline{U}}(f) = N^{2\ln\ln N + \mathcal{O}(1)} \quad \text{if } D \le n. \tag{39}$$

Note that this bound is nearly polynomial in N. Moreover, if $D \le n^{1-c}$ for some fixed $0 < c < 1$, then Lemma 11.1(3) implies

$$\mathop{\mathbb{E}}_{f} K_{\overline{U}}(f) = N^{\mathcal{O}(1)}. \tag{40}$$

In this case, the expected running time is polynomially bounded in the input size N.

11.2. **The case $D > n$.** The homotopy continuation algorithm MD is not efficient for large degrees—the main problem being that we do not know how to deterministically compute a starting system g with small $\mu_{\max}(g)$. However, it turns out that an algorithm due to Jim Renegar [17], based on the factorization of the u-resultant, computes approximate zeros and is fast for large degrees.

Before giving the specification of Renegar's algorithm, we need to fix some notation. We identify $\mathbb{P}^n_0 := \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid x_0 \neq 0\}$ with $\mathbb{C}^n$ via the bijection $(x_0 : \cdots : x_n) \mapsto (x_1/x_0, \ldots, x_n/x_0)$. By $\|x\|_{\text{aff}}$ we denote the Euclidean norm of $x \in \mathbb{P}^n_0$, i.e.,

$$\|x\|_{\text{aff}} = \Big(\sum_{i=1}^{n} \Big|\frac{x_i}{x_0}\Big|^2\Big)^{\frac{1}{2}}$$

and we put $\|x\|_{\text{aff}} = \infty$ if $x \in \mathbb{P}^n \setminus \mathbb{P}^n_0$. By a *$\delta$-approximation* of a zero $\zeta \in \mathbb{C}^n$ of $f \in \mathcal{H}_{\mathbf{d}}$ we understand an $x \in \mathbb{C}^n$ such that $\|x - \zeta\|_{\text{aff}} \le \delta$.

We want to relate δ-approximations with approximate zeros in the sense of Definition 2.1. More precisely, we want a criterium allowing us to guarantee that a δ-approximation is an approximate zero. To do so we use Theorem 2.2 together with the following result.

Lemma 11.2. *For $x, y \in \mathbb{C}^n$ we have $d_{\mathbb{P}}(x, y) \le \|x - y\|_{\text{aff}}$.*

Proof. Let $x, y \in \mathbb{C}^n$ and put $e := (1, 0) \in \mathbb{C}^{n+1}$. By our identification of $\mathbb{C}^n$ with $\mathbb{P}^n_0$, the distance $\theta := d_{\mathbb{P}}(x, y)$ in $\mathbb{P}^n$ is defined by (cf. (7)),

$$\cos\theta = \frac{|\langle e + x, e + y\rangle|}{\|e + x\| \cdot \|e + y\|}.$$

We have

$$\|x-y\|^2 \ge \|(e+x)-(e+y)\|^2 = 1+\|x\|^2+1+\|y\|^2-2\|e+x\|\cdot\|e+y\| \cos\theta.$$

Writing $r := \|x\|$, $s := \|y\|$, $a := \frac{1}{2}\|x-y\|$, we obtain

$$\cos\theta \geq \frac{r^2+s^2+2-4a^2}{2\sqrt{1+r^2}\sqrt{1+s^2}}.$$

Using $2\sqrt{(1+r^2)(1+s^2)} \leq r^2+s^2+2$ this can be bounded below as

$$\cos\theta \geq 1 - \frac{4a^2}{r^2+s^2+2}.$$

By the triangle inequality we have $2a \leq r+s$, hence $r^2+s^2 \geq 2a^2$. Therefore,

$$\cos\theta \geq 1 - \frac{4a^2}{2a^2+2} = \frac{1-a^2}{1+a^2}.$$

Hence $\theta \leq \theta_0$, where θ_0 is defined by $\cos\theta_0 = \frac{1-a^2}{1+a^2}$. We have

$$\cos^2\frac{\theta_0}{2} = \frac{1+\cos\theta_0}{2} = \frac{1}{1+a^2},$$

hence $\tan\frac{\theta_0}{2} = a$. It follows that

$$\tan\frac{\theta}{2} \leq \tan\frac{\theta_0}{2} = a.$$

Summarizing, we have shown that

$$d_{\mathbb{P}}(x,y) \leq 2\tan\frac{d_{\mathbb{P}}(x,y)}{2} \leq \|x-y\|_{\mathrm{aff}}. \qquad \square$$

Corollary 11.3. *Let x be a δ-approximation of a zero ζ of f. Recall $C = 0.025$. If $D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta \leq C$, then x is an approximate zero of f.*

Proof. By Lemma 11.2 we have $d_{\mathbb{P}}(x,\zeta) \leq \|x-\zeta\|_{\mathrm{aff}} \leq \delta$. Suppose that $D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta \leq C$. Then, by Proposition 4.1 with $g = f$, we have $\mu_{\mathrm{norm}}(f,\zeta) \leq (1+\varepsilon)\mu_{\mathrm{norm}}(f,x)$ with $\varepsilon = 0.13$. Hence

$$D^{3/2}\mu_{\mathrm{norm}}(f,\zeta)d_{\mathbb{P}}(x,\zeta) \leq (1+\varepsilon)D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta \leq (1+\varepsilon)C.$$

We have $(1+\varepsilon)C \leq u_0 = 3-\sqrt{7}$. Now use Theorem 2.2. $\square$

Consider now $R \geq \delta > 0$. *Renegar's Algorithm* $\mathsf{Ren}(R,\delta)$ from [17] takes as input $f \in \mathcal{H}_{\mathbf{d}}$, decides whether its zero set $V(f) \subseteq \mathbb{P}^n$ is finite, and if so, computes δ-approximations x to at least all zeros ζ of f satisfying $\|\zeta\|_{\mathrm{aff}} \leq R$. (The algorithm even finds the multiplicities of those zeros ζ, see [17] for the precise statement.)

Renegar's Algorithm can be formulated in the BSS-model over $\mathbb{R}$. Its running time on input f (the number of arithmetic operations and inequality tests) is bounded by

$$\mathcal{O}\bigg(n\mathcal{D}^4(\log\mathcal{D})\Big(\log\log\frac{R}{\delta}\Big) + n^2\mathcal{D}^4\Big(\frac{1+\sum_i d_i}{n}\Big)^4\bigg). \tag{41}$$

To find an approximate zero of f we may use $\mathsf{Ren}(R,\delta)$ together with Corollary 11.3 and iterate with $R = 4^k$ and $\delta = 2^{-k}$ for $k = 1,2,\ldots$ until we are successful. More precisely, we consider the following algorithm:

Algorithm ItRen
input $f \in \mathcal{H}_{\mathbf{d}}$
`for` $k = 1, 2, \ldots$ `do`
  `run` $\mathsf{Re}(4^k, 2^{-k})$ `on input` f
  `for all` δ-approximations x found
    `if` $D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta \le C$ `stop and RETURN` x

Let $\Sigma_0 := \Sigma \cup \{f \in \mathcal{H}_{\mathbf{d}} \mid V(f) \cap \mathbb{P}^n_0 = \emptyset\}$. It is obvious that ItRen stops on inputs $f \notin \Sigma_0$. In particular, ItRen stops almost surely.

The next result bounds the probability Probfail that the main loop of ItRen, with parameters R and δ, fails to output an approximate zero for a standard Gaussian input $f \in \mathcal{H}_{\mathbf{d}}$ (and given R, δ). We postpone its proof to §11.3.

Lemma 11.4. *We have* $\mathrm{Probfail} = \mathcal{O}(n^3 N^2 D^6 \mathcal{D} \delta^4 + nR^{-2})$.

Let $T(f)$ denote the running time of algorithm ItRen on input f.

Proposition 11.5. *We have for standard Gaussian* $f \in \mathcal{H}_{\mathbf{d}}$

$$\mathop{\mathbb{E}}_{f} T(f) = (nN\mathcal{D})^{\mathcal{O}(1)}.$$

Proof. The probability that ItRen stops in the $(k+1)$th loop is bounded above by the probability p_k that $\mathsf{Re}(4^k, 2^{-k})$ fails to produce an approximate zero. Lemma 11.4 tells us that

$$p_k = \mathcal{O}\big(n^3 N^2 D^6 \mathcal{D}\, 16^{-k}\big).$$

If A_k denotes the running time of the $(k+1)$th loop we conclude

$$\mathop{\mathbb{E}}_{f} T(f) \le \sum_{k=0}^{\infty} A_k p_k.$$

According to (41), A_k is bounded by

$$\mathcal{O}\left(n\mathcal{D}^4 (\log \mathcal{D})(\log k) + n^2 \mathcal{D}^4 \left(\frac{1 + \sum_i d_i}{n}\right)^4 + (N + n^3)\mathcal{D}\right),$$

where the last term accounts for the cost of the tests. The assertion now follows by distributing the products $A_k p_k$ and using that the series $\sum_{k\ge 1} 16^{-k}$, and $\sum_{k \ge 1} 16^{-k} \log k$ have finite sums. $\square$

Proof of Theorem 3.8. We use Algorithm MD if $D \le n$ and Algorithm ItRen if $D > n$. We have already shown (see (39), (40)) that the assertion holds if $D \le n$. For the case $D > n$ we use Proposition 11.5 together with the inequality $\mathcal{D}^{\mathcal{O}(1)} \le D^{\mathcal{O}(n)} \le N^{\mathcal{O}(\log\log N)}$ which follows from Lemma 11.1(5). Moreover, in the case $D \ge n^{1+\varepsilon}$, Lemma 11.1(3) implies $\mathcal{D} \le D^n \le N^{\mathcal{O}(1)}$. $\square$

11.3. **Proof of Lemma 11.4.** Let $\mathcal{E}$ denote the set of $f \in \mathcal{H}_{\mathbf{d}}$ such that there is an x on the output list of $\mathsf{Ren}(R,\delta)$ on input f that satisfies $C < D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta$. Then

$$\mathrm{Probfail} \le \operatorname*{Prob}_{f\in\mathcal{H}_{\mathbf{d}}}\Big\{\min_{\zeta\in V(f)}\|\zeta\|_{\mathrm{aff}} \ge R\Big\} + \operatorname{Prob}\mathcal{E}.$$

Lemma 11.4 follows immediately from the following two results.

Lemma 11.6. *For $R>0$ and standard Gaussian $f\in\mathcal{H}_{\mathbf{d}}$ we have*

$$\operatorname*{Prob}_{f\in\mathcal{H}_{\mathbf{d}}}\big\{\min_{\zeta\in V(f)}\|\zeta\|_{\mathrm{aff}} \ge R\big\} \le \frac{n}{R^2}.$$

Proof. Choose $f\in\mathcal{H}_{\mathbf{d}}$ standard Gaussian and pick one of the $\mathcal{D}$ zeros $\zeta_f^{(1)},\ldots,\zeta_f^{(\mathcal{D})}$ of f uniformly at random, call it ζ. By Proposition 7.1, $\zeta\in\mathbb{P}^n$ is uniformly distributed. Therefore,

$$\operatorname*{Prob}_{f\in\mathcal{H}_{\mathbf{d}}}\big\{\min_i\|\zeta_f^{(i)}\|_{\mathrm{aff}} \ge R\big\} \le \operatorname*{Prob}_{\zeta\in\mathbb{P}^n}\big\{\|\zeta\|_{\mathrm{aff}}\ge R\big\}.$$

To estimate the right-hand side probability we observe that

$$\|\zeta\|_{\mathrm{aff}} \ge R \Longleftrightarrow d_{\mathbb{P}}(\zeta,\mathbb{P}^{n-1}) \le \frac{\pi}{2}-\theta,$$

where θ is defined by $R=\tan\theta$ and $\mathbb{P}^{n-1} := \{x\in\mathbb{P}^n \mid x_0=0\}$. Therefore,

$$\operatorname*{Prob}_{\zeta\in\mathbb{P}^n}\big\{\|\zeta\|_{\mathrm{aff}}\ge R\big\} = \frac{\mathsf{vol}\big\{x\in\mathbb{P}^n \mid d_{\mathbb{P}}(x,\mathbb{P}^{n-1})\le\frac{\pi}{2}-\theta\big\}}{\mathsf{vol}(\mathbb{P}^n)}.$$

Due to [10, Lemma 2.1] and using $\mathsf{vol}(\mathbb{P}^n)=\pi^n/n!$, this can be bounded by

$$\frac{\mathsf{vol}(\mathbb{P}^{n-1})\mathsf{vol}(\mathbb{P}^1)}{\mathsf{vol}(\mathbb{P}^n)}\sin^2\left(\frac{\pi}{2}-\theta\right) = n\cos^2\theta = \frac{n}{1+R^2} \le \frac{n}{R^2}. \qquad \square$$

Lemma 11.7. *We have* $\operatorname{Prob}\mathcal{E} = \mathcal{O}(n^3N^2D^6\mathcal{D}\delta^4)$.

Proof. Assume that $f\in\mathcal{E}$. Then, there exist $\zeta,x\in\mathbb{P}^n_0$ such that $f(\zeta)=0$, $\|\zeta\|_{\mathrm{aff}}\le R$, $\|\zeta-x\|_{\mathrm{aff}}\le\delta$, Ren returns x, and $D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta > C$.

We proceed by cases. Suppose first that $\delta \le \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(f,\zeta)}$. Then, by Proposition 4.1,

$$(1+\varepsilon)^{-1}C < (1+\varepsilon)^{-1}D^{3/2}\mu_{\mathrm{norm}}(f,x)\delta \le D^{3/2}\mu_{\mathrm{norm}}(f,\zeta)\delta,$$

hence

$$\mu_{\max}(f) \ge \mu_{\mathrm{norm}}(f,\zeta) \ge (1+\varepsilon)^{-1}CD^{-3/2}\delta^{-1}.$$

If, on the other hand, $\delta > \frac{C}{D^{3/2}\mu_{\mathrm{norm}}(f,\zeta)}$, then we have

$$\mu_{\max}(f) \ge \mu_{\mathrm{norm}}(f,\zeta) \ge CD^{-3/2}\delta^{-1}.$$

Therefore, for any $f\in\mathcal{E}$,

$$\mu_{\max}(f) \ge (1+\varepsilon)^{-1}CD^{-3/2}\delta^{-1} =: A_0D^{-3/2}\delta^{-1}.$$

Theorem C of [22] states that $\mathrm{Prob}_f\{\mu_{\max}(f) \geq \rho^{-1}\} = \mathcal{O}(n^3 N^2 \mathcal{D} \rho^4)$ for all $\rho > 0$. Therefore, we get

$$\mathrm{Prob}\,\mathcal{E} \leq \operatorname*{Prob}_{f \in \mathcal{H}_{\mathbf{d}}} \left\{ \mu_{\max}(f) \geq A_0 D^{-3/2} \delta^{-1} \right\} = \mathcal{O}(n^3 N^2 \mathcal{D} D^6 \delta^4)$$

as claimed. □

References

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[2] D. Amelunxen and P. Bürgisser. Robust smoothed analysis of a condition number of linear programming. Available at `arXiv:0803.0925`, 2008.

[3] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22(3):317–330, 1983.

[4] C. Beltrán and L. M. Pardo. On Smale's 17th problem: a probabilistic positive solution. *Found. Comput. Math.*, 8(1):1–43, 2008.

[5] C. Beltrán and L.M. Pardo. Smale's 17th problem: average polynomial time to compute affine and projective solutions. *J. Amer. Math. Soc.*, 22(2):363–385, 2009.

[6] C. Beltrán and L. M. Pardo. Fast linear homotopy to find approximate zeros of polynomial systems. Manuscript 2008.

[7] C. Beltrán and M. Shub. Complexity of Bézout's theorem VII: Distance estimates in the condition metric. *Found. Comput. Math.*, 9(2):179–195, 2009.

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

[9] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21(1):1–46, 1989.

[10] P. Bürgisser, F. Cucker, and M. Lotz. Smoothed analysis of complex conic condition numbers. *J. Math. Pures et Appl.*, 86:293–309, 2006.

[11] P. Bürgisser, F. Cucker, and M. Lotz. The probability that a slightly perturbed numerical analysis problem is difficult. *Math. Comp.*, 77(263):1559–1583, 2008.

[12] K. P. Choi. On the medians of gamma distributions and an equation of Ramanujan. *Proc. Amer. Math. Soc.*, 121(1):245–251, 1994.

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

[14] F. Cucker, R. Hauser, and M. Lotz. Adversarial smoothed analysis. Available at `arXiv:0903.3499v1`, 2009.

[15] R. Howard. The kinematic formula in Riemannian homogeneous spaces. *Mem. Amer. Math. Soc.*, 106(509):vi+69, 1993.

[16] M.O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12(1):128–138, 1980.

[17] J. Renegar. On the worst-case arithmetic complexity of approximating zeros of systems of polynomials. *SIAM J. Comput.*, 18:350–370, 1989.

[18] A. Sankar, D. A. Spielman, and S.-H. Teng. Smoothed analysis of the condition numbers and growth factors of matrices. *SIAM J. Matrix Anal. Appl.*, 28(2):446–476 (electronic), 2006.

[19] M. Shub. Some remarks on Bezout's theorem and complexity theory. In *From Topology to Computation: Proceedings of the Smalefest (Berkeley, CA, 1990)*, pages 443–455. Springer, New York, 1993.

[20] M. Shub. Complexity of Bézout's theorem VI: Geodesics in the condition (number) metric. *Found. Comput. Math.*, 9(2):171–178, 2009.

[21] M. Shub and S. Smale. Complexity of Bézout's theorem. I. Geometric aspects. *J. Amer. Math. Soc.*, 6(2):459–501, 1993.
[22] 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.
[23] M. Shub and S. Smale. Complexity of Bézout's theorem III: condition number and packing. *Journal of Complexity*, 9:4–14, 1993.
[24] M. Shub and S. Smale. Complexity of Bézout's theorem IV: probability of success; extensions. *SIAM J. of Numer. Anal.*, 33:128–148, 1996.
[25] M. Shub and S. Smale. Complexity of Bézout's theorem V: polynomial time. *Theoretical Computer Science*, 133:141–164, 1994.
[26] S. Smale. Newton's method estimates from data at one point. In *The merging of disciplines: new directions in pure, applied, and computational mathematics (Laramie, Wyo., 1985)*, pages 185–196. Springer, New York, 1986.
[27] S. Smale. Complexity theory and numerical analysis. In A. Iserles, editor, *Acta Numerica*, pages 523–551. Cambridge University Press, 1997.
[28] S. Smale. Mathematical problems for the next century. In *Mathematics: frontiers and perspectives*, pages 271–294. Amer. Math. Soc., Providence, RI, 2000.
[29] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 6(1):84–85, 1977.
[30] 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.
[31] 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.
[32] M. Wschebor. Smoothed analysis of $\kappa(a)$. *J. of Complexity*, 20:97–107, 2004.

Institute of Mathematics, University of Paderborn, D-33098 Paderborn, Germany
E-mail address: pbuerg@upb.de

Dept. of Mathematics, City University of Hong Kong, Kowloon Tong, Hong Kong
E-mail address: macucker@cityu.edu.hk