



HAL
open science

On the Number of Real Zeros of Random Sparse Polynomial Systems

Alperen A. Ergür, Máté L. Telek, Josué Tonelli-Cueto

► **To cite this version:**

Alperen A. Ergür, Máté L. Telek, Josué Tonelli-Cueto. On the Number of Real Zeros of Random Sparse Polynomial Systems. 2024. hal-04475973

HAL Id: hal-04475973

<https://hal.science/hal-04475973>

Preprint submitted on 24 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the Number of Real Zeros of Random Sparse Polynomial Systems

Alperen A. Ergür

University of Texas at San Antonio
Dept. of Mathematics
San Antonio, Texas, USA
alperen.ergur@utsa.edu

Máté L. Telek

University of Copenhagen
Dept. Math. Sciences
Copenhagen, DENMARK
mlt@math.ku.dk

Josué Tonelli-Cueto

University of Texas at San Antonio
Dept. of Mathematics
San Antonio, Texas, USA
josue.tonelli.cueto@bizkaia.eu

Abstract

Consider a random system $f_1(x) = 0, \dots, f_n(x) = 0$ of n random real polynomials in n variables, where each f_k has a prescribed set of exponent vectors in a set $A_k \subseteq \mathbb{Z}^n$ of size t_k . Assuming that the coefficients of the f_k are independent Gaussian of any variance, we prove that the expected number of zeros of the random system in the positive orthant is bounded from above by $4^{-n} \prod_{k=1}^n t_k(t_k - 1)$. This result is a probabilistic version of Kushnirenko's conjecture; it provides a bound that only depends on the number of terms and is independent of their degree.

1 Introduction

Instances of polynomial system solving arise in a variety of problems coming from kinematics [70], dynamical systems [32], mathematical modeling of chemical reaction networks [27], computer vision [48], and computer aided geometric design [24, 66]. The common thread among these plethora of applications is that the polynomial systems that occur are structured, and the solutions that are most useful are the real ones. In this setting, the basic question is: how many real zeros are there?

When we consider zeros over complex numbers, we have the power of intersection theory [30]. In particular, for sparse polynomial systems the number of complex solutions is given by the celebrated BKK bound [7, 50] (cf. [71, Chapter 3]). The story becomes more complicated and interesting for real zeros. Consider the following simple polynomial system:

$$\begin{aligned}a_1 + b_1X + \gamma_1Y + c_1XYZ^d &= 0 \\a_2 + b_2X + \gamma_2Y + c_2XYZ^d &= 0 \\a_3 + b_3X + \gamma_3Y + c_3XYZ^d &= 0.\end{aligned}$$

where $d \in \mathbb{N}$ and the a_k, b_k, c_k and d_k are real numbers. Although the system has, generically, d complex zeros, it has at most two real solutions. This example illustrates that the number of real zeros cannot be estimated using the number of complex solutions.

The above phenomenon is a general one. Khovanskiĭ, in his seminal book *Fewnomials* [44], showed that the maximum number of real zeros of a polynomial system can be bounded in terms of the description complexity of the system. The term *fewnomial* refers to a polynomial with few monomials, and so to a polynomial with a low description complexity. He showed that independent of the degree of its monomials, real fewnomial systems have few real zeros.

The work of Khovanskiĭ was an answer to several conjectures by Kushnirenko in 1977 [49]: A regular positive zero of a polynomial system $f = (f_1, f_2, \dots, f_n)$ is a point $x \in \mathbb{R}^n$ with positive coordinates ($x_i > 0$) such that the Jacobian matrix of the polynomial system f at x , $D_x f$, is full-rank. We denote the set of regular positive real zeros by $\mathcal{Z}_r(f, \mathbb{R}_+^n)$. Among the conjectures of Kushnirenko, the following one remains widely open:

Kushnirenko's Question: Let $A_1, \dots, A_n \subset \mathbb{N}^n$ be finite sets of sizes t_1, \dots, t_n and f the system of fewnomials given by

$$\begin{aligned} f_1 &= \sum_{\alpha \in A_1} f_{1,\alpha} X^\alpha \\ &\vdots \\ f_n &= \sum_{\alpha \in A_n} f_{n,\alpha} X^\alpha \end{aligned}$$

Is there a bound of the form

$$\#\mathcal{Z}_r(f, \mathbb{R}_+^n) \leq \text{poly}(t_1, \dots, t_n)^n?$$

It is fair to say that Kushnirenko's question is one of the most challenging problems in real algebraic geometry. However, its reach and importance goes far beyond. In complexity theory, variants of Kushnirenko's question (where the bound should be explicit in an algebraic complexity measure), such as the real τ -conjecture [45] or the adelic τ -conjecture [63], imply Valiant's algebraic variant of P vs NP (see [19] for details and relation to classical questions in complexity theory, and [17] for a probabilistic take on the problem).

Specific cases of Kushnirenko's question play an important role in studying chemical reaction networks. In that setting, the steady states of the network correspond to positive real zeros of a certain parameterized polynomial system [27]. Although there exist several methods to decide whether the system has at least two positive zeros [10, 60, 62, 35, 34], finding (tight) upper bounds is a hard and open problem. The polynomial system arising from a reaction network is usually sparse, and the maximum number of its positive zeros is much smaller compared to the number of complex zeros [39, 61]. Thus techniques from real algebraic geometry are required to have insight into the number of steady states [33, 37, 10].

Khovanskii [44, §3.14, Corollary 4] obtained a bound of the form

$$2^{\binom{t-1}{2}} (n+1)^{t-1}$$

where $t = \#(\cup_{k=1}^n A_k)$ is the number of types of monomials appearing in the system. Later, Bihan and Sottile [14, 13] would improve this bound to

$$\frac{e^2 + 3}{4} 2^{\binom{t-n-1}{2}} n^{t-n-1}$$

and, in a special mixed case in which $t = \sum_{k=1}^n t_k - n + 1$, further improved this bound to

$$\frac{e^2 + 3}{4} 2^{\binom{t-n-1}{2}} \binom{t-n-1}{t_1-2, \dots, t_n-2}.$$

After four decades of hard work, as of today, we are still far from answering Kushnirenko's question. We only have precise bounds for special cases [11, 46, 54], and even the bivariate case of Kushnirenko's question remains open [46]. We refer the reader to [71] for a comprehensive exposition, to [28] for a short survey and to [74, Appendix F, §1] for a historical survey.

Our current inability to answer Kushnirenko's question, and the pressing need for an answer in applications, motivates a probabilistic take on the problem. How many zeros of a random real fewnomial system are real? This question turns out to be harder than it sounds. There is a well-developed theory (either relying on the kinematic formula [5, 29] or convex bodies [15, 42, 58]) in random real algebraic geometry. This theory has produced strong results on the expected number of real zeros of random dense polynomials, that is, random polynomials supported on all monomials of a given degree [47, 69, 2, 52, 53, 3, 4]. However, in the case of random structured polynomials, applying the theory becomes more complicated [16, 43], and earlier available results are either for random polynomials supported on a product of simplices [65] or depend strongly on the degree of the monomials [57]¹. In summary, the aforementioned results in random real algebraic geometry do

¹Recently, Malajovich [56, 55] has provided a bound that bridges between the dense and the sparse cases. In a different direction, there are results on complex zeros of random sparse complex polynomials [6, 67, 68].

not address Kushnirenko's question. In [22], we obtained a bound for random fewnomial systems with fixed support ($A = A_1 = \dots = A_n$) and centered Gaussian random coefficients with the same variance structure. In our view, the importance of the bound in [22] relies on two facts:

- (1) The bound depends only in the number of distinct monomials.
- (2) The bound does not depend on the variance structure of the random coefficients.

This latter point should be stressed, since, for random dense polynomial systems all available results place strong assumptions on the variance structure.

Recently, Bürgisser [20] generalized the results of [22] to the mixed case (where A_1, A_2, \dots, A_n are not necessarily equal). However, the result in [20] only holds for centered Gaussian fewnomial systems in which all variances are equal to one. In this paper, we obtain estimates that hold for arbitrary support sets and arbitrary variances in the same spirit with Kushnirenko's question.

The simplest form of our result can be seen in the theorem below. In the remainder of the introduction we explain the consequences of our result in specific cases and state our main theorem in full technical detail. We also provide side results on the volume of random fewnomial varieties.

Theorem 1.1. *Let $A_1, \dots, A_n \subset \mathbb{R}^n$ be finite sets of sizes t_1, \dots, t_n , and \mathfrak{f} the system of n random fewnomials given by*

$$\begin{aligned} \mathfrak{f}_1 &= \sum_{\alpha \in A_1} \mathfrak{f}_{1,\alpha} X^\alpha \\ &\vdots \\ \mathfrak{f}_n &= \sum_{\alpha \in A_n} \mathfrak{f}_{n,\alpha} X^\alpha \end{aligned} \tag{1.1}$$

where the $\mathfrak{f}_{k,\alpha}$ are independent centered Gaussian random variables (with no restrictions placed on variances). Then we have

$$\mathbb{E}_{\mathfrak{f}} \# \mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) \leq \frac{1}{4^n} \prod_{k=1}^n t_k (t_k - 1) \tag{1.2}$$

where $\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n)$ is the zero set of \mathfrak{f} in \mathbb{R}_+^n .

Remark 1.2. Observe that if the affine span of $\sum_{k=1}^n A_k$ is not the whole \mathbb{R}^n (or, more generally, if A_1, \dots, A_n does not contain an independent transversal (see [76, Lemma 1] for the precise definition)), then $\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) = \emptyset$ with probability one.

1.1 Random Mixed Fewnomials with Restricted Variances

The following theorem shows that the bound of Theorem 1.1 can be improved when we impose restrictions on the variances on the random fewnomial system. This result improves the main theorem of Bürgisser [20, Theorem 1.1] by allowing more flexible assumptions on the variance structure and a better multiplying factor: 4^{-n} instead of $(2\pi)^{-n/2}$. We give the proof in Section 3.

Theorem 1.3. *Under the same notations and assumptions of Theorem 1.1, assume that the variance vectors*

$$\mathbf{v}_k = (\mathbf{v}_{k,\alpha})_{\alpha \in A_k}$$

of the \mathfrak{f}_k satisfy the following conditions:

(VM1) for all k and all $\alpha \in A_k$, $\mathbf{v}_{k,\alpha} \leq 1$.

(VM2) for all k and $\alpha \in A_k$ a vertex of the polytope $P_k := \text{conv}(A_k)$, $\mathbf{v}_{k,\alpha} = 1$.

Then

$$\mathbb{E}_{\mathfrak{f}} \# \mathcal{Z}_r(\mathfrak{f}, \mathbb{R}_+^n) \leq \frac{1}{4^n} V \left(\sum_{k=1}^n P_k \right) \prod_{k=1}^n (t_k - 1) \tag{1.3}$$

where $V(\sum_{k=1}^n P_k)$ is the number of vertices of the Minkowski sum $\sum_{k=1}^n P_k$.

Remark 1.4. Interestingly, in the univariate case ($n = 1$), the obtained upper bound, $(t_1 - 1)/2$, agrees with the average value of the bound given by Descartes' rule of signs [26]. However, optimal results in the univariate case, when all variances are equal to one, were already obtained in [41].

1.2 Random Unmixed Fewnomials with Restricted Variances

In the case where the system is unmixed and some restrictions are imposed on the variances we obtain better bounds. This result improves the main theorem of [22, Theorem 1.2] (see Remark 1.6 for details). We give the proof of this in Section 4.

Theorem 1.5. *Under the same notations and assumptions of Theorem 1.1, assume that*

$$A = A_1 = \cdots = A_n$$

for some $A \subset \mathbb{R}^n$ of size t , and assume that the variance vectors \mathbf{v}_k of the \mathfrak{f}_k satisfy either the assumptions (VM1) and (VM2) in Theorem 1.3 or

$$\mathbf{v}_1 = \cdots = \mathbf{v}_n. \quad (1.4)$$

Then

$$\mathbb{E}_{\mathfrak{f}} \# \mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) \leq \frac{n+1}{4^n} \binom{t}{n+1}. \quad (1.5)$$

Remark 1.6. Theorem 1.5 improves [22, Theorem 1.2] in the following sense: The main result of [22, Theorem 1.2] only holds under the assumption (1.4) on the variance vectors, whereas Theorem 1.5 has more flexible assumptions. Moreover, the upper bound in [22, Theorem 1.2] is of the form $\frac{1}{2^{n-1}} \binom{t}{n}$. Therefore, Theorem 1.5 gives a smaller bound if and only if $t - n \leq 2^{2n-n+1}$.

A specific case that attracted considerable attention is when $\#A = n + \ell$ and ℓ is a fixed constant [14], specially when $\ell = 2$ [8, 9, 64]. The following corollary (whose proof is at the end of Section 4) shows that if such systems are generated randomly then it is hard to find any positive zero at all.

Corollary 1.7. *Under the same the same notations and assumption of Theorem 1.5, assume that for some constant $\ell \in \mathbb{N}$,*

$$\#A = n + \ell$$

Then

$$\mathbb{P}_{\mathfrak{f}} (\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) \neq \emptyset) \leq \frac{\ell(n+1)^\ell}{4^n}. \quad (1.6)$$

Moreover, since ℓ is a fixed constant, we have that $\lim_{n \rightarrow \infty} \mathbb{P}_{\mathfrak{f}} (\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) \neq \emptyset) = 0$.

Remark 1.8. If we substitute the constant ℓ by logpolynomial function $\ell(n) = \mathcal{O}(\log^a(n))$ with $a > 0$ a constant, the limit probability would still be zero.

1.3 Main Result in Full Technical Detail

Recall that given a finite set $A \subset \mathbb{R}^n$ and a map

$$\pi : A \rightarrow \mathbb{R},$$

the *upper envelope of A with respect π* is the convex polyhedron given by

$$\mathcal{L}(A, \pi) := \text{conv} \left\{ \begin{pmatrix} \pi(\alpha) - s \\ \alpha \end{pmatrix} \mid \alpha \in A, s \geq 0 \right\}. \quad (1.7)$$

Intuitively, this set arises when we lift A according to π and we look at the convex hull of these lifted points,

$$P^\pi := \text{conv} \left\{ \begin{pmatrix} \pi(\alpha) \\ \alpha \end{pmatrix} \mid \alpha \in A \right\},$$

from above. We can now state our main theorem, from which Theorems 1.1 and 1.3 will also follow.

Theorem 1.9. Let $A_1, \dots, A_n \subset \mathbb{R}^n$ be finite sets of sizes t_1, \dots, t_n , and \mathfrak{f} the system of n random fewnomials given by

$$\begin{aligned} \mathfrak{f}_1 &= \sum_{\alpha \in A_1} \mathfrak{f}_{1,\alpha} X^\alpha \\ &\vdots \\ \mathfrak{f}_n &= \sum_{\alpha \in A_n} \mathfrak{f}_{n,\alpha} X^\alpha \end{aligned}$$

where the $\mathfrak{f}_{k,\alpha}$ are independent centered Gaussian random variables. Consider, for each \mathfrak{f}_k , its variance vector

$$\mathbf{v}_k = (\mathfrak{v}_{k,\alpha})_{\alpha \in A_k}$$

and construct the lifting functions $\mathfrak{u}_k : A_k \rightarrow \mathbb{R}$ given by

$$\mathfrak{u}_k : \alpha \mapsto \frac{1}{2} \ln \mathfrak{v}_{k,\alpha}. \quad (1.8)$$

Then we have

$$\mathbb{E}_{\mathfrak{f}} \# \mathcal{Z}_r(\mathfrak{f}, \mathbb{R}_+^n) \leq \frac{1}{4^n} V \left(\sum_{k=1}^n \mathcal{L}(A_k, \mathfrak{u}_k) \right) \prod_{k=1}^n (t_k - 1) \quad (1.9)$$

where $V(\sum_{k=1}^n \mathcal{L}(A_k, \mathfrak{u}_k))$ is the number of vertices of the Minkowski sum $\sum_{k=1}^n \mathcal{L}(A_k, \mathfrak{u}_k)$.

We note that one can interpret the expression

$$V \left(\sum_{k=1}^n \mathcal{L}(A_k, \mathfrak{u}_k) \right)$$

as the number of elements of $\sum_{k=1}^n A_k$ that are used in the regular mixed subdivision induced by the lifting functions $\mathfrak{u}_1, \dots, \mathfrak{u}_n$ which are defined by the logarithm of the variances. Indeed, we find the theory of regular (mixed) subdivisions [25] at the core of our development. Subdivisions have been used earlier in the work of Bihan, Santos, and Spaenlehauer [12] and Sturmfels [73] for constructing fewnomial systems with many zeros, in the work of Sturmfels on the Newton polytope of A -resultants [72, Sect. 2], in the seminal work by Gelfand, Kapranov and Zelevinsky [36], and implicitly in Viro's patchworking method [75] (see [31, Section 2.2] for an exposition). We don't have any good explanation for why mixed regular subdivisions appear in random fewnomial theory, but there seems to be a deep connection to be uncovered.

1.4 Bounds on Volume of Random Projective Fewnomial Varieties

In complex algebraic geometry, the (normalized) volume of a complex algebraic variety is just the degree [21, Corollary 20.10]. In real algebraic geometry, we can only talk about the average volume of a random variety— (normalized) volume is also referred to as “average degree” [23]. Shub and Smale [69] showed that for a random KSS homogeneous polynomial system \mathfrak{f} of degrees d_1, \dots, d_q in the $n+1$ variables X_0, X_1, \dots, X_n , we have that

$$\mathbb{E}_{\mathfrak{f}} \text{vol}_{n-q} \mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) = \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \sqrt{\prod_{k=1}^q d_k}, \quad (1.10)$$

where $\text{vol}_k \mathbb{P}_{\mathbb{R}}^k$ is the volume under the usual Riemannian structure. Moreover, we even have a central limit theorem in the case that all degrees are equal [4]. The following result shows that, for random projective varieties given by random fewnomials, the average volume can be bounded independently of the degree. We give the proof in Section 5.

Theorem 1.10. Let $q \leq n$, $d_1, \dots, d_q \in \mathbb{N}$ and $A_1, \dots, A_q \subset \mathbb{N}^{n+1}$ be finite subsets of sizes t_1, \dots, t_q such that for all k ,

$$\{d_k e_0, \dots, d_k e_n\} \subseteq A_k \subseteq d_k \Delta_n$$

where $\{e_0, \dots, e_n\}$ is the standard basis of \mathbb{R}^{n+1} and $\Delta_n := \text{conv}(e_0, \dots, e_n)$ the n -simplex. Consider the random homogeneous fewnomial system \mathfrak{f} given by

$$\begin{aligned} \mathfrak{f}_1 &= \sum_{\alpha \in A_1} \mathfrak{f}_{1,\alpha} X^\alpha \\ &\vdots \\ \mathfrak{f}_q &= \sum_{\alpha \in A_q} \mathfrak{f}_{q,\alpha} X^\alpha \end{aligned}$$

where the $\mathfrak{f}_{k,\alpha}$ are independent centered Gaussian random variables (with no restrictions placed on the variances). Then, with probability one, $\mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n)$ is of dimension at most $n - q$ and

$$\mathbb{E}_{\mathfrak{f}} \text{vol}_{n-q} \mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) \leq \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \frac{(n(n+1))^{n-q}}{2^n} \prod_{k=1}^q t_k(t_k - 1) \quad (1.11)$$

Remark 1.11. In Theorem 1.10, we are imposing $\text{conv}(A_k) = d_k \Delta_n$ to guarantee that $\mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n)$ does not contain a coordinate hyperplane with probability one. Although this can be achieved under more general conditions, we prioritize a simple statement.

Remark 1.12. By our assumption, we have $t_k \geq n + 1$. Hence, when degree is large, for example, when

$$t_k \leq \frac{2^{n/q}}{(n(n+1))^{n/q-1}} \sqrt{d_k},$$

(1.11) gives a better bound than (1.10). In particular, the random projective fewnomial hypersurface given by

$$\sum_{i=0}^n \mathfrak{f}_i X_i^d$$

has an average volume bounded by

$$\frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \left(\frac{n(n+1)}{2} \right)^n,$$

which does not depend on the degree.

1.5 Overview and Outline of the Proof

Our proof follows a similar path to the proof in [22]. We first prove an integral-probabilistic formula for the number of zeros which depends on the determinant of a random matrix. To bound this complicated integral, we use the Cauchy-Binet formula² and express the determinant as a summation of many determinants of $n \times n$ matrices. In turn, this splits the integral formula into a sum of integrals over determinants of $n \times n$ matrices. We bound these summands by interpreting them as expected number of real zeros of a specific system of random polynomials and bounding these expectations simply by the maximum number of zeros of these special systems.

Expanding the above, we prove the integral-probabilistic formula (2.2) in Section 2 using kinematic formulas [23, 40] and a measure theoretic result of Appendix A. After this, in Section 3, we use the Cauchy-Binet formula [18, Theorem 4.15] to split the integral into several summands. However, the proof complicates and we need to do a polyhedral subdivision—induced by the normal fan of $\sum_{k=1}^n \mathcal{L}(A_k, \mathfrak{A}_k)$ in the statement of Theorem 1.9—to perform the reduction of the random general case to the deterministic case—a binomial system—analyzed in Proposition 3.2.

Although the above reduction from the general random case to special deterministic cases plays a central role in our proof, a direct analytical proof is possible. We provide a fully analytical proof of the Proposition 3.2 to show this fact.

²Curiously enough, this formula appears in the proof of many upper bounds in fewnomial theory [14, 20, 22].

Organization

In Section 2 we obtain a Rice formula for the expected number of real zeros. Section 3 proves our main result. Section 4 deals with unmixed systems, and Section 5 contains the proof of volume estimate for random fewnomial varieties.

Acknowledgements

We thank Alicia Dickenstein for always making time to share her knowledge whenever we asked a question. We thank Maurice Rojas for inspiration and his enthusiasm for fewnomials. We are thankful to Peter Bürgisser and Elias Tsigaridas for helpful discussions.

A.E. and J.T.-C. thanks Paul Breiding, Sonja Petrovic and Gregory G. Smith for organizing the *BIRS Workshop “Random Algebraic Geometry” (23w5070)* at the Banff International Research Station, in Canada, from April 16 to April 21, 2023, which served as inspiration for this paper.

A.E. is supported by NSF CCF 2110075.

J.T.-C. thanks Evgeniya Lagoda for her constant support and Jazz G. Suchen for his insightful suggestion regarding equation (2.3). J.T.-C. also thanks Alperen A. Ergür, Eduardo Dueñez, José Iovino, José Morales, Nikos Salingaros, Chris La Valle, Chris Duffer and the UTSA Problem Solving Club (specially Thamara, Rachell, Adam, Taylor, Lila and Alyssa) for making him feel welcome at UTSA during his postdoctoral stay; Jeaheang Bang and Huan Xu for the nice atmosphere at the postdocs’ office; and Alejandra Vincencio for making the official paperwork much easier during this stay.

M.T. is funded by the European Union under the Grant Agreement no. 101044561, POSALG. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or European Research Council (ERC). Neither the European Union nor ERC can be held responsible for them.

2 A Rice Formula for the Expected Number of Zeros

At the center of [20], we find an integral-probabilistic formula for the number of expected zeros of a random system. This formula is only implicitly stated in a special case (the case where ψ is injective). We make this formula explicit and prove it in its full generality. We do this by combining the kinematic formulas [23, 40] used in [20] with standard arguments of measure theory, such as Dynkin’s lemma [1, p. 4.11]. We note that the formula below is a special case of Rice formula [5, Theorem 6.2]. We provide a proof using the kinematic formula for completeness and because this proof is interesting in its own right.

Recall that for $f : U \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^n$ with $U \subseteq \mathbb{R}^n$ open,

$$\mathcal{Z}_r(f, U) := \{\zeta \in U \mid f(\zeta) = 0, \det D_\zeta f(\zeta) \neq 0\}$$

is the set of regular zeros of f in U . The following theorem gives the promised integral-probabilistic formula for the number of zeros of a random system where each equation is generated independently.

Theorem 2.1 (Rice formula). *Let $\Omega \subseteq \mathbb{R}^n$ be an open set and let*

$$\varphi_k : \Omega \rightarrow \mathbb{R}^{m_k+1}$$

be smooth maps such that the map $\psi : \Omega \rightarrow \prod_{k=1}^n \mathbb{S}^{m_k}$ given by

$$\psi : x \mapsto \begin{pmatrix} \psi_1(x) \\ \vdots \\ \psi_n(x) \end{pmatrix} := \begin{pmatrix} \varphi_1(x)/\|\varphi_1(x)\| \\ \vdots \\ \varphi_n(x)/\|\varphi_n(x)\| \end{pmatrix} \quad (2.1)$$

is well-defined. Consider a random system of equations $f_1(x) = 0, \dots, f_n(x) = 0$ given by

$$f_k := \sum_{i=0}^{m_k+1} c_{k,i} \varphi_{k,i}$$

where the $\mathbf{c}_{k,i}$ are i.i.d. standard Gaussian random variables. Then, for every Borel measurable set $\tilde{\Omega} \subseteq \Omega$,

$$\mathbb{E}_{\mathbf{c}} \# \mathcal{Z}_r(\mathbf{f}, \tilde{\Omega}) = (2\pi)^{-n/2} \int_{\tilde{\Omega}} \mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| dx \quad (2.2)$$

where the \mathbf{a}_k are independent standard Gaussian vectors in $\psi_k(x)^\perp \subset \mathbb{R}^{m_k+1}$, i.e., the subspace orthogonal to $\psi_k(x)$.

Corollary 2.2. *Under the same assumptions and notations of Theorem 2.1, for every Borel measurable set $\tilde{\Omega} \subseteq \Omega$,*

$$\mathbb{E}_{\mathbf{c}} \# \mathcal{Z}_r(\mathbf{f}, \tilde{\Omega}) = (2\pi)^{-n/2} \int_{\tilde{\Omega}} \frac{1}{\prod_{k=1}^n \|\varphi_k(x)\|} \mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} \right| dx \quad (2.3)$$

where the \mathbf{a}_k are independent standard Gaussian vectors in the subspace $\varphi_k(x)^\perp$.

Corollary 2.3. *Under the same assumptions and notations of Theorem 2.1, if*

$$m_1 = m_2 = \cdots = m_n = 1$$

and, for some $\xi : \Omega \rightarrow \mathbb{R}^n$,

$$\varphi_1 = \begin{pmatrix} 1 \\ \xi_1(x) \end{pmatrix}, \dots, \varphi_n = \begin{pmatrix} 1 \\ \xi_n(x) \end{pmatrix}$$

then, for every Borel measurable set $\tilde{\Omega} \subseteq \Omega$,

$$\mathbb{E}_{\mathbf{c}} \# \mathcal{Z}_r(\mathbf{f}, \tilde{\Omega}) = \frac{1}{\pi^n} \int_{\tilde{\Omega}} \frac{|\det D_x \xi|}{\prod_{k=1}^n (1 + \xi_k(x)^2)} dx \quad (2.4)$$

Proof of Theorem 2.1. We will show later that without loss of generality we can assume that $\psi : \Omega \rightarrow \prod_{k=1}^n \mathbb{S}^{m_k}$ is an *embedding*, i.e., it satisfies:

(I1) ψ is an *immersion*, i.e., for all $x \in \Omega$, $\text{rank } D_x \psi = n$.

(I2) ψ is injective.

Moreover, we can further assume that

(O) $\tilde{\Omega} = \Omega$.

Under these assumptions, $\psi(\Omega)$ is an open embedded submanifold of $\prod_{k=1}^n \mathbb{S}^{m_k}$. Now, consider the random hyperplanes

$$\mathfrak{H}_k := \left\{ x \in \mathbb{R}^{m_k+1} \mid \sum_{i=0}^{m_k} \mathbf{c}_{k,i} x_{k,i} = 0 \right\}$$

which are uniformly distributed in the corresponding Grassmannian (because the $\mathbf{c}_{k,i}$ are i.i.d. standard Gaussians). Observe that

$$\# \mathcal{Z}(\mathbf{f}, \Omega) = \# \psi(\Omega) \cap (\mathfrak{H}_1 \times \cdots \times \mathfrak{H}_n), \quad (2.5)$$

since $\psi(x) \in \mathfrak{H}_1 \times \cdots \times \mathfrak{H}_n$ if and only if $x \in \mathcal{Z}(\mathbf{f}, \Omega)$. Moreover, by Sard's Theorem [59, §2] (cf. [21, Proposition A.18]), the intersection

$$\psi(\Omega) \cap (\mathfrak{H}_1 \times \cdots \times \mathfrak{H}_n)$$

is transversal with probability one, and hence it is zero-dimensional almost surely. Hence, with probability one,

$$\# \mathcal{Z}_r(\mathbf{f}, \Omega) = \# \mathcal{Z}(\mathbf{f}, \Omega) = \# \psi(\Omega) \cap (\mathfrak{H}_1 \times \cdots \times \mathfrak{H}_n),$$

and so

$$\mathbb{E}_c \# \mathcal{Z}_r(\mathbf{f}, \Omega) = \mathbb{E}_{\mathfrak{H}_1, \dots, \mathfrak{H}_n} \# \psi(\Omega) \cap (\mathfrak{H}_1 \times \dots \times \mathfrak{H}_n).$$

Now, by the kinematic formula stated in [20, Theorem 3.2] (cf. [23, 40]) and [20, Lemma 3.4.], the equation (2.2) holds for $\tilde{\Omega} = \Omega$.

We now show that we can assume (I1), (I2) and (O) without loss of generality. If (I1) does not hold, then the set

$$V := \{x \in \Omega \mid \text{rank } D_x \psi < n\}$$

is non-empty. Now for a given $x \in V$, note that

$$D_x \psi_k = \frac{1}{\|\varphi_k(x)\|} (\mathbb{I} - \psi_k(x) \psi_k(x)^T) D_x \varphi_k. \quad (2.6)$$

So, to have $D_x \psi < n$ we have to have a $v_x \in \mathbb{R}^n \setminus 0$ in the kernel of $D_x \psi$ for which we have that for all k

$$D_x \varphi_k(v_x) \in \mathbb{R} \varphi_k(x).$$

That is there exist $v_x \in \mathbb{R}^n \setminus 0$ and $t_1, \dots, t_n \in \mathbb{R}$ such that for all k ,

$$D_x \varphi_k(v_x) = t_k \varphi_k(x).$$

Translating this into $D_x \mathbf{f}$ we conclude that there are $t_k \in \mathbb{R}$ that satisfies

$$D_x \mathbf{f}(v_x) = \begin{pmatrix} \mathbf{c}_1^T D_x \varphi_1(v_x) \\ \vdots \\ \mathbf{c}_n^T D_x \varphi_n(v_x) \end{pmatrix} = \begin{pmatrix} t_1 \mathbf{c}_1^T \varphi_1(x) \\ \vdots \\ t_n \mathbf{c}_n^T \varphi_n(x) \end{pmatrix} = \begin{pmatrix} t_1 \mathbf{f}_1(x) \\ \vdots \\ t_n \mathbf{f}_n(x) \end{pmatrix}.$$

This means \mathbf{f} cannot have regular zeros at x for any $x \in V$. Hence,

$$\# \mathcal{Z}_r(\mathbf{f}, V) = 0 \text{ and } \# \mathcal{Z}_r(\mathbf{f}, \tilde{\Omega}) = \# \mathcal{Z}_r(\mathbf{f}, \tilde{\Omega} \setminus V).$$

Moreover, since for all $x \in V$, $\text{rank } D_x \psi < n$, we have that for all $a_1 \in \mathbb{R}^{m_1+1}, \dots, a_n \in \mathbb{R}^{m_n+1}$,

$$\det \begin{pmatrix} a_1^T D_x \psi_1 \\ \vdots \\ a_n^T D_x \psi_n \end{pmatrix} = 0$$

and so

$$\int_{\tilde{\Omega}} \mathbb{E}_a \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| dx = \int_{\tilde{\Omega} \setminus V} \mathbb{E}_a \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| dx.$$

Hence, taking $\Omega \setminus V$ instead of Ω , we can assume, without loss of generality, that (I1) holds.

Assume now that (I1) holds. We will show how we can assume (I2) and (O) without loss of generality. We will make use of Theorem A.4, which relies on standard arguments in measure theory and which we prove in Appendix A. By (I1), the map $\psi : \Omega \rightarrow \mathbb{S}^n$ is an immersion and so, by [51, Proposition 5.22], it is a *local embedding*, i.e., for each $x \in \Omega$, there is $r_x > 0$ such that $\psi : B(x, r_x) \subseteq \Omega \rightarrow \prod_{k=1}^n \mathbb{S}^{m_k}$ is injective. Therefore the collection of open sets

$$\mathcal{U} := \{U \subseteq \Omega \mid U \text{ open, } \bar{U} \subseteq \Omega, \bar{U} \text{ compact and } \psi|_U \text{ injective}\}. \quad (2.7)$$

satisfies that for all $x \in \Omega$, there is $r_x > 0$ such that for all $r < r_x$, $B(x, r) \in \mathcal{U}$. Hence \mathcal{U} is a base for the topology of Ω —assumption (U0) of Theorem A.4. Moreover, \mathcal{U} is closed under containment of open sets—assumption (U1) of Theorem A.4.

Consider the following two Borel measures:

$$\mu : B \mapsto \mathbb{E}_c \# \mathcal{Z}_r(\mathbf{f}, B)$$

and

$$\nu : B \mapsto (2\pi)^{-n/2} \int_B \mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| dx.$$

We only need to show that $\mu = \nu$. Once this is done, (2.2) holds in the desired generality.

For each $U \in \mathcal{U}$, (I2) holds. Thus we have that (2.2) holds with $\tilde{\Omega} = U$, and so

$$\mu(U) = \nu(U)$$

—assumption (U4) of Theorem A.4. Moreover, this quantity is finite—assumption (U3) of Theorem A.4. To see this, note that

$$\mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| \leq \sqrt{\mathbb{E}_{\mathbf{a}} \prod_{k=1}^n \|\mathbf{a}_k\|^2} \sqrt{\mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \hat{\mathbf{a}}_1^T D_x \psi_1 \\ \vdots \\ \hat{\mathbf{a}}_n^T D_x \psi_n \end{pmatrix} \right|^2}$$

where $\hat{\mathbf{a}}_k := \mathbf{a}_k / \|\mathbf{a}_k\|$ is uniformly distributed in $\mathbb{S}^{m_k} \cap \psi_k(x)^\perp$, and so, by compactness, for $x \in U$,

$$\mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| \leq \sqrt{\mathbb{E}_{\mathbf{a}} \prod_{k=1}^n \|\mathbf{a}_k\|^2} \max_{\substack{\hat{\mathbf{a}}_k \in \mathbb{S}^{m_k} \\ x \in \bar{U}}} \left| \det \begin{pmatrix} \hat{\mathbf{a}}_1^T D_x \psi_1 \\ \vdots \\ \hat{\mathbf{a}}_n^T D_x \psi_n \end{pmatrix} \right| < \infty.$$

Thus the integral of the left-hand side over $U \subset \bar{U}$, and so $\nu(U)$, must be finite.

Now, Ω is σ -compact, because it is an open subset of \mathbb{R}^n and all hypothesis of Theorem A.4 ((U0), (U1), (U2) and (U3)) are satisfied, so $\mu = \nu$ as we wanted to show. \square

Remark 2.4. The above proof can be applied to extend [22] to functions that are not semialgebraic and this immediately extends the result in [22] to arbitrary real exponents.

Proof of Corollary 2.2. This follows from Theorem 2.1 using (2.6), the properties of the determinant and that $\mathbf{a}_k(\mathbb{I} - \psi_k(x)\psi_k(x)^T) = \mathbf{a}_k$ due to $\mathbf{a}_k \in \psi_k(x)^\perp = \varphi_k(x)^\perp$. \square

Proof of Corollary 2.3. We just have to apply Corollary 2.2. Fix $x \in \Omega$, we only have to show that

$$(2\pi)^{-\frac{n}{2}} \mathbb{E}_{\mathbf{a}} \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} \right| = \frac{1}{\pi^n} \frac{|\det D_x \xi|}{\prod_{k=1}^n \sqrt{1 + \xi_k(x)^2}}$$

where the $\mathbf{a}_k \in \psi_k(x)^\perp$ are independent standard Gaussian random vectors.

Since we are in \mathbb{R}^2 , we have that

$$\varphi_k(x)^\perp = \text{span} \left(\frac{1}{\sqrt{1 + \xi_k(x)}} \begin{pmatrix} -\xi_k(x) \\ 1 \end{pmatrix} \right)$$

and so we can write

$$\mathbf{a}_k = \frac{\mathfrak{z}_k}{\sqrt{1 + \xi_k(x)}} \begin{pmatrix} -\xi_k(x) \\ 1 \end{pmatrix}$$

with the $\mathfrak{z}_k \in \mathbb{R}$ i.i.d. standard Gaussians. Moreover, because of this, $\mathbf{a}_k D_x \varphi_k = \frac{\mathfrak{z}_k}{\sqrt{1 + \xi_k(x)^2}} D_x \xi_k$, and so

$$\left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \psi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \psi_n \end{pmatrix} \right| = \prod_{k=1}^n |\mathfrak{z}_k| \frac{|\det D_x \xi|}{\prod_{k=1}^n (1 + \xi_k(x)^2)}.$$

Now, an easy computation shows that $\mathbb{E}_{\mathfrak{z}} \prod_{k=1}^n |\mathfrak{z}_k| = (2/\pi)^{n/2}$, and the claim follows. \square

We finish this section with the following two propositions which will allow us to drop the regularity assumption from our theorems.

Proposition 2.5. *Under the same assumptions and notations of Theorem 2.1, if for all $x \in \Omega$,*

$$\text{rank } D_x \psi = n,$$

then, for every Borel measurable set $\tilde{\Omega} \subseteq \Omega$,

$$\mathcal{Z}(\mathfrak{f}, \tilde{\Omega}) = \mathcal{Z}_r(\mathfrak{f}, \tilde{\Omega})$$

with probability one.

Proposition 2.6. *Under the same analogous notations of Theorem 2.1, assume that the map the map $\psi : \Omega \rightarrow \prod_{k=1}^q \mathbb{S}^{m_k}$, with $q > n$, given by*

$$\psi : x \mapsto \begin{pmatrix} \psi_1(x) \\ \vdots \\ \psi_n(x) \end{pmatrix} := \begin{pmatrix} \varphi_1(x) / \|\varphi_1(x)\| \\ \vdots \\ \varphi_q(x) / \|\varphi_q(x)\| \end{pmatrix} \quad (2.8)$$

is well-defined and that for all $x \in \Omega$,

$$\text{rank } D_x \psi = n.$$

Consider the random overdetermined system $\mathfrak{f}_1(x) = 0, \dots, \mathfrak{f}_q(x) = 0$ given by

$$\mathfrak{f}_k := \sum_{i=0}^{m_k+1} \mathfrak{c}_{k,i} \varphi_{k,i}$$

where the $\mathfrak{c}_{k,i}$ are i.i.d. standard Gaussian random variables. Then

$$\mathcal{Z}(\mathfrak{f}, \Omega) = \emptyset$$

with probability one.

Proof of Proposition 2.5. The proof is as the proof of Theorem 2.1, but now we don't need to remove any subset from Ω so that that (I1) holds. Hence, arguing as before using (2.5) with the cover \mathcal{U} , we have, by Sard's Theorem [59, §2] (cf. [21, Proposition A.18]), that for all $U \in \mathcal{U}$,

$$\mathcal{Z}(\mathfrak{f}, U) = \mathcal{Z}_r(\mathfrak{f}, U)$$

with probability one. Since this holds for all open sets in an open cover of Ω , it holds for Ω too. \square

Proof of Proposition 2.6. The proof is analogous to that of Proposition 2.5. However, when writing down the analogous of (2.5), we have that we are intersecting $q > n$ hyperplanes with an n -dimensional submanifold in $\prod_{k=1}^q \mathbb{S}^{m_k}$. By Sard's Theorem [59, §2] (cf. [21, Proposition A.18]), this intersection is almost surely transversal which implies that this intersection is empty as desired. \square

3 Proof of the Main Theorem

We now prove Theorem 1.9 which yields Theorems 1.1 and 1.3 as direct corollaries. We also prove Proposition 3.1, which allows us to remove the regularity from our statements for random fewnomial systems; and the key Proposition 3.2 that plays a central role in the proof of the main theorem.

Proposition 3.1. *Under the notations and assumptions of Theorem 1.9,*

$$\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) = \mathcal{Z}_r(\mathfrak{f}, \mathbb{R}_+^n)$$

with probability one.

Proposition 3.2. Let $\gamma_1, \dots, \gamma_n \in \mathbb{R}^n$, $s_1, \dots, s_n \in \mathbb{R}$ and consider the following the random binomial system \mathfrak{h} given by the equations

$$\begin{aligned} \mathfrak{h}_1 &= \mathfrak{a}_1 \exp(\gamma_1^T X + s_1) + \mathfrak{b}_1 \\ &\vdots \\ \mathfrak{h}_n &= \mathfrak{a}_n \exp(\gamma_n^T X + s_n) + \mathfrak{b}_n \end{aligned} \tag{3.1}$$

where the \mathfrak{a}_k and \mathfrak{b}_k are i.i.d. standard Gaussian random variables, and the following Borel-measurable set

$$B := \{x \in \mathbb{R}^n \mid \text{for all } k, \gamma_k^T x + s_k \leq 0\}.$$

Then

$$\frac{1}{\pi^n} \int_B \frac{\prod_{k=1}^n \exp(\gamma_k^T x + s_k)}{\prod_{k=1}^n (1 + \exp(2\gamma_k^T x + 2s_k))} |\det(\gamma_1 \cdots \gamma_n)| dx = \mathbb{E}_{\mathfrak{h}} \# \mathcal{Z}_r(\mathfrak{h}, B) \leq \frac{1}{4^n}.$$

Remark 3.3. If the γ_k are linearly independent, then the inequality in Proposition 3.2 is an equality.

Proof of Theorem 1.9. By Proposition 3.1, we can just bound the number of expected regular zeros. Instead of a system of fewnomials, we consider the equivalent system of exponential sums $\mathfrak{g} = (\mathfrak{g}_1, \dots, \mathfrak{g}_n)$ defined as

$$\begin{aligned} \mathfrak{g}_1 &= \sum_{\alpha \in A_1} \mathfrak{c}_{1,\alpha} \exp(\alpha^T X + \mathfrak{h}_1(\alpha)) \\ &\vdots \\ \mathfrak{g}_n &= \sum_{\alpha \in A_n} \mathfrak{c}_{n,\alpha} \exp(\alpha^T X + \mathfrak{h}_n(\alpha)) \end{aligned} \tag{3.2}$$

where the $\mathfrak{c}_{k,\alpha}$ are i.i.d. standard Gaussian variables. Observe that

$$\mathbb{E}_{\mathfrak{c}} \# \mathcal{Z}_r(\mathfrak{g}, \mathbb{R}^n) = \mathbb{E}_{\mathfrak{f}} \# \mathcal{Z}_r(\mathfrak{f}, \mathbb{R}_+^n).$$

So we will need to bound the expected number zeros of \mathfrak{g} on \mathbb{R}^n . We do this by decomposing \mathbb{R}^n into a collection of polyhedral cells, and bounding the number the number zeros on each of these polyhedral cells.

To define the polyhedral cell, for $\alpha_1 \in A_1, \dots, \alpha_n \in A_n$, consider

$$M(\alpha_1, \dots, \alpha_n) := \{x \in \mathbb{R}^n \mid \text{for all } k \text{ and for all } \alpha \in A_k, \alpha^T x + \mathfrak{h}_k(\alpha) \leq \alpha_k^T x + \mathfrak{h}_k(\alpha_k)\}. \tag{3.3}$$

Observe that $z \in M(\alpha_1, \dots, \alpha_n)$ if and only if the map

$$\begin{pmatrix} s \\ x \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ z \end{pmatrix}^T \begin{pmatrix} s \\ x \end{pmatrix} = s + z^T x$$

attains, for each k , its maximum value inside $\mathcal{L}(A_k, \mathfrak{h}_k)$ at

$$\begin{pmatrix} \mathfrak{h}_k(\alpha_k) \\ \alpha_k \end{pmatrix},$$

i.e.,

$$\text{if } \begin{pmatrix} 1 \\ z \end{pmatrix} \text{ is, for each } k, \text{ in the normal cone of } \mathcal{L}_k(A_k, \mathfrak{h}_k) \text{ at } \begin{pmatrix} \mathfrak{h}_k(\alpha_k) \\ \alpha_k \end{pmatrix}.$$

This shows that $M(\alpha_1, \dots, \alpha_n)$ is a full-dimensional polyhedral cell if and only if

$$\sum_{k=1}^n \begin{pmatrix} \mathfrak{h}_k(\alpha_k) \\ \alpha_k \end{pmatrix}$$

is a vertex of the Minkowski sum $\sum_{k=1}^n \mathcal{L}(A_k, \mathfrak{h}_k)$. Moreover, since $M(\alpha_1, \dots, \alpha_n)$ is obtained by maximizing the value of linear functional over a finite collection of points, we have

$$\mathbb{R}^n = \bigcup \{M(\alpha_1, \dots, \alpha_n) \mid \alpha_1 \in A_1, \dots, \alpha_n \in A_n\}. \tag{3.4}$$

So, by subadditivity of the zero counting function, we only need to prove that for all $\alpha_1 \in A_1, \dots, \alpha_n \in A_n$ the following bound holds

$$\mathbb{E}_c \# \mathcal{Z}_r(\mathbf{g}, M(\alpha_1, \dots, \alpha_n)) \leq \frac{1}{4^n} \prod_{k=1}^n (t_k - 1). \quad (3.5)$$

Observe that the solutions of \mathbf{g} in any region do not change if we multiply each equation by $\exp(-\alpha_k^T x - \mathfrak{I}_k(\alpha_k))$. Thus, without loss of generality, we can assume that $\alpha_1 = \dots = \alpha_n = 0$ and that $\mathfrak{I}_k(\alpha_k) = 0$. Thus by considering $M := M(0, \dots, 0)$, $\varphi_k(x) = (\exp(\alpha^T x + \mathfrak{I}_i(\alpha)))_{\alpha \in A_k}$, and applying Corollary 2.2, we get

$$\mathbb{E}_c \# \mathcal{Z}_r(\mathbf{g}, M) = (2\pi)^{-\frac{n}{2}} \int_M \frac{1}{\prod_{k=1}^n \|\varphi_k(x)\|} \mathbb{E}_a \left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} \right| dx \quad (3.6)$$

where the $\mathbf{a}_k \in \varphi_k(x)^\perp$ are independent standard Gaussian random vectors. Observe that $D_x \varphi_{k,0} = 0$ since $\varphi_{k,0} = 1$. Thus, by the Cauchy-Binet formula [18, Theorem 4.15] applied to

$$\begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} = \begin{pmatrix} \mathbf{a}_1^T & & \\ & \ddots & \\ & & \mathbf{a}_n^T \end{pmatrix} D_x \varphi,$$

we obtain

$$\det \begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} = \sum_{\beta_1 \in A_1 \setminus \{0\}, \dots, \beta_n \in A_n \setminus \{0\}} \prod_{k=1}^n \mathbf{a}_{k, \beta_k} \det \begin{pmatrix} D_x \varphi_{1, \beta_1} \\ \vdots \\ D_x \varphi_{n, \beta_n} \end{pmatrix},$$

since, to get a full-rank minor of $\text{diag}(\mathbf{a}_k^T)$, we need to pick a column corresponding to each \mathbf{a}_k^T . So, by the triangle inequality we have

$$\left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} \right| \leq \sum_{\beta_1 \in A_1 \setminus \{0\}, \dots, \beta_n \in A_n \setminus \{0\}} \prod_{k=1}^n |\mathbf{a}_{k, \beta_k}| \left| \det \begin{pmatrix} D_x \varphi_{1, \beta_1} \\ \vdots \\ D_x \varphi_{n, \beta_n} \end{pmatrix} \right|. \quad (3.7)$$

Now we use following observation: The coordinate projection

$$\begin{aligned} \mathbb{R}^{A_k} &\rightarrow \mathbb{R} \\ x &\mapsto x_{\beta_k} \end{aligned}$$

induces a linear functional $\lambda_k : \varphi_k(x)^\perp \rightarrow \mathbb{R}$ which has the norm

$$\|\lambda_k\| = \sqrt{1 - \frac{\varphi_{k, \beta_k}(x)^2}{\|\varphi_k(x)\|^2}} = \frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k, \beta_k}(x)^2}}{\|\varphi_k(x)\|}.$$

Thus $\mathbf{a}_{k, \beta_k} = \lambda_{\beta_k}(\mathbf{a}_k)$ is a centered Gaussian random variable with variance $\|\lambda_k\|^2$, because it is the result of projecting the standard Gaussian random vector $\mathbf{a}_k \in \varphi_k(x)^\perp$ with the linear functional λ_k of norm $\|\lambda_k\|$. Therefore

$$\mathbb{E}_a |\mathbf{a}_{k, \beta_k}| = \frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k, \beta_k}(x)^2}}{\|\varphi_k(x)\|} \sqrt{\frac{2}{\pi}}. \quad (3.8)$$

Substituting (3.8) and $D_x \varphi_{k, \beta_k} = \exp(\beta_k^T x + \mathfrak{I}_k(\beta_k)) \beta_k^T$ back in (3.6) combined with (3.7), we get

$$\begin{aligned} &\mathbb{E}_c \# \mathcal{Z}_r(\mathbf{g}, M) \\ &\leq \sum_{\beta_k \in A_k \setminus \{0\}} \frac{1}{\pi^n} \int_M \prod_{k=1}^n \frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k, \beta_k}(x)^2} \exp(\beta_k^T x + \mathfrak{I}_k(\beta_k))}{\|\varphi_k(x)\|^2} |\det(\beta_1 \cdots \beta_n)| dx. \end{aligned}$$

If we bound each of the summands in the right-hand side by $1/4^n$, we are done, since there are at most $\prod_{k=1}^n (t_k - 1)$ many summands.

We will use Proposition 3.2 with $\gamma_k = \beta_k$ and $s_k = \pi_k(\beta_k)$ to bound each summand by $1/4^n$. To do this, we only need to show that

$$\prod_{k=1}^n \frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k,\beta_k}(x)^2}}{\|\varphi_k(x)\|^2} \leq \frac{1}{\prod_{k=1}^n (1 + \exp(2\beta_k^T x + 2\pi_k(\beta_k)))}. \quad (3.9)$$

So, it suffices to show that for each k we have

$$\frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k,\beta_k}(x)^2}}{\|\varphi_k(x)\|^2} \leq \frac{1}{(1 + \exp(2\beta_k^T x + 2\pi_k(\beta_k)))}. \quad (3.10)$$

We define

$$u_k(x) := \varphi_{k,\beta_k}(x) = \exp(\beta_k^T x + \pi_k(\beta_k))$$

and

$$v_k(x) = \sqrt{\|\varphi_k(x)\|^2 - \varphi_{k,\beta_k}(x)^2} = \sqrt{\sum_{\alpha \in A_k \setminus \{0, \beta_k\}} \exp(2\alpha^T x + 2\pi_k(\alpha))}.$$

We only need to show then that

$$\frac{\sqrt{1 + v_k(x)^2}}{1 + u_k(x)^2 + v_k(x)^2} \leq \frac{1}{1 + u_k(x)^2},$$

which is equivalent to

$$\left(\sqrt{1 + v_k(x)^2}\right)^2 - (1 + u_k(x)^2)\sqrt{1 + v_k(x)^2} + u_k(x)^2 \geq 0.$$

Observe that the polynomial $T^2 - (1 + u_k(x)^2)T + u_k(x)^2$ has two roots: 1 and $u_k(x)^2$. Since $\sqrt{1 + v_k(x)^2} \geq 1$, the above inequality is valid independently of $v_k(x)$ as long as $u_k(x) \leq 1$, which is precisely what happens for $x \in M$ since

$$M = M(0, \dots, 0) = \{x \in \mathbb{R}^n \mid \text{for all } k, \text{ for any } \beta_k \in A_k, \beta_k^T x + \pi_k(\beta_k) \leq 0\}.$$

Hence, (3.9) holds in M , and by Proposition 3.2,

$$\frac{1}{\pi^n} \int_M \prod_{k=1}^n \frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k,\beta_k}(x)^2} \exp(\beta_k^T x + \pi_k(\beta_k))}{\|\varphi_k(x)\|^2} |\det(\beta_1 \cdots \beta_n)| dx \leq \frac{1}{4^n}.$$

which completes the proof. \square

Proof of Proposition 3.1. Assume that the affine span of $\sum_{k=1}^n A_k$ is the whole of \mathbb{R}^n . By Propositions 2.5, we only need to show that for the map

$$\psi = (\varphi_1/\|\varphi_1\|, \dots, \varphi_n/\|\varphi_n\|)$$

where

$$\varphi_k(x) = (\exp(\alpha^T x + \pi_k(\alpha)))_{\alpha \in A_k},$$

satisfies that for all $x \in \mathbb{R}^n$, $\text{rank } D_x \psi = n$. Note that working with this exponential formulation is enough as it does not affect the regularity of the zeros of a fewnomial system.

Now, by (2.6), we have that $\text{rank } D_x \psi < n$ if and only if there is $v_x \in \mathbb{R}^n \setminus \{0\}$ such that for all k , $D_x \varphi(v_x) \in \mathbb{R} \varphi_k(x)$. Thus $\text{rank } D_x \psi < n$ if and only if there is $v_x \in \mathbb{R}^n \setminus \{0\}$ and $t_1, \dots, t_n \in \mathbb{R}^n$ such that for all k , $D_x \varphi(v_x) = t_k \varphi_k(x)$. For all k and $\alpha_k \in A_k$,

$$D_x \varphi_{k,\alpha_k} = \varphi_{k,\alpha_k} \alpha_k^T.$$

Hence $\text{rank } D_x \psi < n$ if and only if there is $v_x \in \mathbb{R}^n \setminus \{0\}$ and $t_1, \dots, t_n \in \mathbb{R}^n$ such that for all k and all $\alpha_k \in A_k$, $\alpha_k^T v_x = t_k$. In other words, $\text{rank } D_x \psi < n$ if and only if the A_k are contained in parallel (affine) hyperplanes. If the affine span of $\sum_{k=1}^n A_k$ is \mathbb{R}^n , as we are assuming, then the latter is not possible and so $D_x \psi$ is injective, as desired.

Now, assume that the affine span of $\sum_{k=1}^n A_k$ is not the entire \mathbb{R}^n . After a change of variables of the form $x \mapsto \exp(A \log(x) + b)$, we can assume, without loss of generality, that the affine span of $\sum_{k=1}^n A_k$ is

$$\mathbb{R}^m \times 0 \subset \mathbb{R}^n$$

with $m < n$. In this case we have that \mathfrak{f} is a random overdetermined system in the variables X_1, \dots, X_m . Moreover, arguing as before, we have that for all $x \in \mathbb{R}^m$, $\text{rank } D_x \psi = m$. Hence, by Proposition 2.6, we have

$$\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^m \times \{\mathbf{1}\}) = \emptyset$$

with probability one. This implies that if the affine span of $\sum_{k=1}^n A_k$ is not the entire \mathbb{R}^n we have $\emptyset = \mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n)$ with probability one, and so $\mathcal{Z}(\mathfrak{f}, \mathbb{R}_+^n) = \mathcal{Z}_r(\mathfrak{f}, \mathbb{R}_+^n)$ with probability one. \square

Geometric Proof of Proposition 3.2. Without loss of generality, assume that the γ_k are linearly independent. Otherwise the proposition is immediate, with both the integral and the expectation being zero.

Note that the the left-hand side equality follows from Corollary 2.3, after taking $\xi_k(x) = \exp(\gamma_k^T x + s_k)$ and observing that $D_x \xi_k = \exp(\gamma_k^T x + s_k) \gamma_k^T$. Hence we only need to bound the expectation of the number of real zeros.

Observe that the system (3.1) have a solution if and only if for all k , \mathbf{a}_k and \mathbf{b}_k have opposite signs. Moreover, in that case, the system is equivalent to the following linear system

$$\begin{aligned} \gamma_1^t X &= -s_1 + \ln(-\mathbf{b}_1/\mathbf{a}_1) \\ &\vdots \\ \gamma_n^t X &= -s_n + \ln(-\mathbf{b}_n/\mathbf{a}_n) \end{aligned} \tag{3.11}$$

which has exactly one regular real solution. This system has this unique solution inside B if and only if the $\ln(-\mathbf{b}_k/\mathbf{a}_k)$ are non-positive, which happens with probability $1/4^n$. Hence

$$\mathbb{E}_{\mathfrak{h}} \# \mathcal{Z}_r(\mathfrak{h}, B) = \mathbb{P}(\# \mathcal{Z}_r(\mathfrak{h}, B) \neq 0) = \frac{1}{4^n},$$

as we wanted to show. \square

Analytical Proof of Proposition 3.2. The analytical proof is like the geometric one, but we compute directly now the left-hand side integral. Under the change of variables $y_k = -(\gamma_k^T x_k + s_k)$, the left-hand side integral becomes

$$\frac{1}{\pi^n} \int_{\mathbb{R}_+^n} \frac{\prod_{k=1}^n \exp(-y_k)}{\prod_{k=1}^n (1 + \exp(-2y_k))} dy.$$

Under the further change of variables $z_k = \exp(-y_k)$, this integral becomes

$$\frac{1}{\pi^n} \int_{[0,1]^n} \frac{1}{\prod_{k=1}^n (1 + z_k^2)} dz.$$

Now, separating variables, this integral equals

$$\left(\frac{1}{\pi} \int_0^1 \frac{1}{1+t^2} dt \right)^n = \frac{1}{4^n},$$

where the last equality follows from $\arctan'(t) = 1/(1+t^2)$. \square

4 Zeros of Random Unmixed Fewnomials

We now prove Theorem 1.5. We will actually prove a more general result, and then show that Theorem 1.5 is obtained as a corollary.

Theorem 4.1. *Under the same notations and assumptions of Theorem 1.9, assume that*

$$A = A_1 = \cdots = A_n$$

and that the Minkowski sum $\sum_{k=1}^n \mathcal{L}(A, \pi_k)$ satisfies

$$(MV) \text{ for some } \pi : A \rightarrow \mathbb{R}, \sum_{k=1}^n \mathcal{L}(A, \pi_k) = n\mathcal{L}(A, \pi).$$

Then

$$\mathbb{E}_{\mathfrak{f}} \#\mathcal{Z}_r(\mathfrak{f}, \mathbb{R}_+^n) \leq \frac{n+1}{4^n} \binom{V(\mathcal{L}(A, \pi))}{n+1} \quad (4.1)$$

where $V(\mathcal{L}(A, \pi)) \leq \#A$ is the number of vertices of $\mathcal{L}(A, \pi)$.

Proof of Theorem 4.1. The proof is the same as that of Theorem 1.9, but it differs in the combinatorics at two points:

1st point: When we write the decomposition (3.4), we only care about those $\alpha_1, \dots, \alpha_n$ such that

$$\sum_{k=1}^n \binom{\pi_k(\alpha_k)}{\alpha_k}$$

is a vertex of $\sum_{k=1}^n \mathcal{L}(A, \pi_k)$. However, due to the assumption (MV), we necessarily have that $\alpha_1 = \cdots = \alpha_n$, since those are the vertices of $\mathcal{L}(A, \pi)$. Hence we only need to look at polyhedral cells of the form $M(\alpha, \dots, \alpha)$ where $\alpha \in A$ is a vertex of $\mathcal{L}(A, \pi)$ —and so $n\alpha$ a vertex of $n\mathcal{L}(A, \pi)$. Moreover, as we did in the proof of Theorem 1.9, we can assume, without loss of generality, that $\alpha = 0$ and that for all k , $\pi_k(\alpha) = 0$.

2nd point: When we apply the Cauchy-Binet formula to obtain our decomposition. Since we use the same functions but different variances, we can write for each k ,

$$\varphi_k = \Sigma_k \tilde{\varphi}$$

where $\tilde{\varphi}(x) = (x^\alpha)_{\alpha \in A}$ and Σ_k is a diagonal positive matrix with entries given by $\exp(\pi_k(\alpha))$.

It is important to note that the claim “we use the same function but different variances” really requires the extra assumption $\alpha = \alpha_1 = \cdots = \alpha_n$. Otherwise, when doing the translation to put $\alpha_1, \dots, \alpha_n$ at the origin, we will end up with $\varphi_1, \dots, \varphi_n$ being different not only up to multiplication by a diagonal positive matrix. However, we do not need the $\pi_k(\alpha)$ being independent of k , since turning them into zero only requires multiplying the φ_k by positive diagonal matrices. Now,

$$\begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} = \begin{pmatrix} \mathbf{a}_1^T & & \\ & \ddots & \\ & & \mathbf{a}_n^T \end{pmatrix} \begin{pmatrix} \Sigma_1 \\ \vdots \\ \Sigma_n \end{pmatrix} D_x \tilde{\varphi} = \begin{pmatrix} (\Sigma_1 \mathbf{a}_1)^T \\ \vdots \\ (\Sigma_n \mathbf{a}_n)^T \end{pmatrix} D_x \tilde{\varphi},$$

and so, by the Cauchy-Binet formula [18, Theorem 4.15] and the triangle inequality,

$$\left| \det \begin{pmatrix} \mathbf{a}_1^T D_x \varphi_1 \\ \vdots \\ \mathbf{a}_n^T D_x \varphi_n \end{pmatrix} \right| \leq \sum_{\{\beta_1, \dots, \beta_n\} \subset A \setminus \{0\}} \prod_{k=1}^n \exp(\pi_k(\beta_k)) |\mathbf{a}_{k, \beta_k}| \left| \det \begin{pmatrix} D_x \tilde{\varphi}_{\beta_1} \\ \vdots \\ D_x \tilde{\varphi}_{\beta_n} \end{pmatrix} \right|,$$

where the sum runs over subsets of size n . Hence we get

$$\binom{t-1}{n}$$

summands at most, instead of $(t-1)^n$. Now, for each summand, the same computation as before gives us that each summand becomes

$$\frac{1}{\pi^n} \int_M \prod_{k=1}^n \frac{\sqrt{\|\varphi_k(x)\|^2 - \varphi_{k,\beta_k}(x)^2} \exp(\beta_k^T x + \mathfrak{I}_k(\beta_k))}{\|\varphi_k(x)\|^2} |\det(\beta_1 \cdots \beta_n)| dx$$

and so the proof ends as it did in the proof of Theorem 1.9. \square

The following lemma shows that Theorem 1.5 is a corollary of Theorem 4.1.

Lemma 4.2. *Under the same notations and assumptions of Theorem 1.9, assume that $A = A_1 = \cdots = A_n$. Then the following holds:*

- (1) *If $\mathfrak{I} = \mathfrak{I}_1 = \cdots = \mathfrak{I}_n$ then $\mathcal{L}(A, \mathfrak{I}_1) = \cdots = \mathcal{L}(A, \mathfrak{I}_n)$ and $\sum_{k=1}^n \mathcal{L}(A, \mathfrak{I}_k) = n\mathcal{L}(A, \mathfrak{I})$*
- (2) *If for all k and all $\alpha \in A$ we have $\mathfrak{I}_k(\alpha) \leq 0$ with equality whenever α is a vertex of $P := \text{conv}(A)$, then, for all k ,*

$$\mathcal{L}(A, \mathfrak{I}_k) = (-\infty, 0] \times P$$

$$\text{and so } \sum_{k=1}^n \mathcal{L}(A, \mathfrak{I}_k) = (-\infty, 0] \times (n \text{ conv}(A)) = n\mathcal{L}(A, 0).$$

Proof of Lemma 4.2. (1) For a convex set $K \subseteq \mathbb{R}^n$ and $\alpha_1, \alpha_2, \dots, \alpha_n \in K$

$$\alpha_1 + \cdots + \alpha_n = \frac{1}{n}(n\alpha_1 + \cdots + n\alpha_n) \in nK,$$

and so taking Minkowski sums of K with itself is the same as taking integer dilations of K . This is essentially the first claim.

(2) For second claim, we have that, for all k , $\mathfrak{I}_k \leq 0$ and equality happens at the vertices of P . Thus, for all k , $\mathcal{L}(A, \mathfrak{I}_k) = (-\infty, 0] \times P$. The rest follows as in (1). \square

We finish with a proof of Corollary 1.7.

Proof of Corollary 1.7. By Markov's inequality [21, Corollary 2.9] and Theorem 1.5,

$$\mathbb{P}_f(\mathcal{Z}(f, \mathbb{R}_+^n) \neq \emptyset) = \mathbb{P}_f(\#\mathcal{Z}(f, \mathbb{R}_+^n) \geq 1) \leq \mathbb{E}_f \#\mathcal{Z}(f, \mathbb{R}_+^n) \leq \frac{n+1}{4^n} \binom{n+\ell}{n+1},$$

since $\#\mathcal{Z}(f, \mathbb{R}_+^n)$ is a random variable with integer values. Now,

$$(n+1) \binom{n+\ell}{n+1} = \ell \binom{n+\ell}{\ell} = \ell \prod_{k=1}^{\ell} \left(\frac{n}{k} + 1 \right) \leq \ell(n+\ell)^\ell.$$

Hence the claim follows. \square

5 Volume of Random Projective Fewnomial Varieties

We prove Theorem 1.10, we will need the following proposition.

Proposition 5.1. *Let $d_1, \dots, d_{n+1} \in \mathbb{N}$ and $A_1, \dots, A_{n+1} \subset \mathbb{N}^{n+1}$ be finite subsets such that for all k ,*

$$\{d_k e_0, \dots, d_k e_n\} \subseteq A_k \subseteq d_k \Delta_n$$

where $\{e_0, \dots, e_n\}$ is the standard basis of \mathbb{R}^{n+1} and $\Delta_n := \text{conv}(e_0, \dots, e_n)$ the n -simplex. Consider the random overdetermined homogeneous fewnomial system \mathfrak{g} given by

$$\begin{aligned} \mathfrak{g}_1 &= \sum_{\alpha \in A_1} \mathfrak{g}_{1,\alpha} X^\alpha \\ &\vdots \\ \mathfrak{g}_{n+1} &= \sum_{\alpha \in A_{n+1}} \mathfrak{g}_{n+1,\alpha} X^\alpha \end{aligned}$$

where the $\mathbf{g}_{k,\alpha}$ are independent continuous random variables. Then

$$\mathcal{Z}(\mathbf{g}, \mathbb{P}_{\mathbb{R}}^n) = \emptyset$$

with probability one.

Proof of Theorem 1.10. Consider an homogeneous fewnomial system f given by

$$\begin{aligned} f_1 &= \sum_{\alpha \in A_1} f_{1,\alpha} X^\alpha \\ &\vdots \\ f_q &= \sum_{\alpha \in A_q} f_{q,\alpha} X^\alpha \end{aligned}$$

Then, by [38, (2.7)], $\mathcal{Z}(f, \mathbb{P}_{\mathbb{R}}^n)$ admits a finite Whitney stratification. Thus, we can consider a partition of $\mathcal{Z}(f, \mathbb{P}_{\mathbb{R}}^n)$ into disjoint subsets

$$\mathcal{Z}_0(f, \mathbb{P}_{\mathbb{R}}^n), \dots, \mathcal{Z}_n(f, \mathbb{P}_{\mathbb{R}}^n) \subset \mathbb{P}_{\mathbb{R}}^n$$

such that that $\mathcal{Z}_\ell(f, \mathbb{P}_{\mathbb{R}}^n)$ is an ℓ -dimensional smooth submanifold of $\mathcal{Z}(f, \mathbb{P}_{\mathbb{R}}^n)$ or empty.

Let $\mathfrak{H}_1, \dots, \mathfrak{H}_{n-q}$ be random hyperplanes of $\mathbb{P}_{\mathbb{R}}^n$ given by

$$\mathfrak{l}_k = \sum_{i=0}^n \mathbf{a}_{k,i} X_i$$

with the $\mathbf{a}_{k,i}$ i.i.d. standard Gaussians—one can easily see that this is equivalent to moving by a random $\mathbf{g} \in O(n+1)$ (with respect the Haar probability measure) a fixed $(n-q)$ -plane L in $\mathbb{P}_{\mathbb{R}}^n$. By [21, Proposition A.18], all the intersections

$$\mathcal{Z}_\ell(f, \mathbb{P}_{\mathbb{R}}^n) \cap \mathfrak{H}_1 \cap \dots \cap \mathfrak{H}_{n-q} \quad (5.1)$$

are transversal with probability one. Hence, for $\ell < n-q$, (5.1) is empty with probability one; and for $\ell \geq n-q$, (5.1) is, with probability one, either empty or a smooth submanifold of dimension $\ell - (n-q)$. By Poincaré's kinematic formula [21, Theorem A.55], we have that

$$\text{vol}_{n-q} \mathcal{Z}_{n-q}(f, \mathbb{P}_{\mathbb{R}}^n) = \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \mathbb{E}_{\mathfrak{H}_1, \dots, \mathfrak{H}_{n-q}} \#(\mathcal{Z}_{n-q}(f, \mathbb{P}_{\mathbb{R}}^n) \cap \mathfrak{H}_1 \cap \dots \cap \mathfrak{H}_{n-q}).$$

Now, set the convention that $\text{vol}_{n-q}(\mathcal{Z}(f, \mathbb{P}_{\mathbb{R}}^n)) = \infty$, if for some $\ell > n-q$, $\mathcal{Z}_\ell(f, \mathbb{P}_{\mathbb{R}}^n) \neq \emptyset$; and $\mathcal{Z}_{n-q}(f, \mathbb{P}_{\mathbb{R}}^n) = 0$, if for all $\ell \geq n-q$, $\mathcal{Z}_\ell(f, \mathbb{P}_{\mathbb{R}}^n) = \emptyset$. Then, we have that

$$\text{vol}_{n-q} \mathcal{Z}(f, \mathbb{P}_{\mathbb{R}}^n) = \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \mathbb{E}_{\mathfrak{H}_1, \dots, \mathfrak{H}_{n-q}} \#(\mathcal{Z}(f, \mathbb{P}_{\mathbb{R}}^n) \cap \mathfrak{H}_1 \cap \dots \cap \mathfrak{H}_{n-q}),$$

since if some for some $\ell > n-q$, $\mathcal{Z}_\ell(f, \mathbb{P}_{\mathbb{R}}^n)$ is non-empty, then the right-hand side will be infinite—(5.1) will be a non-empty positive dimensional smooth submanifold with probability one—and if for all $\ell \geq n-q$, $\mathcal{Z}_\ell(f, \mathbb{P}_{\mathbb{R}}^n)$ is empty, then the right-hand side will be zero—(5.1) will be empty with probability one.

By the above discussion, we have that

$$\mathbb{E}_{\mathfrak{f}} \text{vol}_{n-q} \mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) = \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \mathbb{E}_{\mathfrak{f}} \mathbb{E}_{\mathfrak{H}_1, \dots, \mathfrak{H}_{n-q}} \#(\mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) \cap \mathfrak{H}_1 \cap \dots \cap \mathfrak{H}_{n-q}),$$

and so, by Tonelli's theorem,

$$\mathbb{E}_{\mathfrak{f}} \text{vol}_{n-q} \mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) = \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \mathbb{E}_{(\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q})} \# \mathcal{Z}((\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}), \mathbb{P}_{\mathbb{R}}^n). \quad (5.2)$$

Assume (we prove this at the end) that, for all i ,

$$\# \mathcal{Z}((\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}), H_i) = 0,$$

where $H_i := \mathcal{Z}(X_i, \mathbb{P}_{\mathbb{R}}^n)$ is the i th coordinate hyperplane in $\mathbb{P}_{\mathbb{R}}^n$, with probability one. Then

$$\mathcal{Z}((\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}), \mathbb{P}_{\mathbb{R}}^n) = \bigcup \{ \mathcal{Z}((\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}), S\mathbb{P}_{\mathbb{R}}^n) \mid S = \text{diag}(\pm 1, \dots, \pm 1) \},$$

where $\mathbb{P}_{\mathbb{R}}^n := \{x \in \mathbb{P}^n \mid x_0 > 0, \dots, x_n > 0\}$, with probability one; and therefore, by symmetry,

$$\mathbb{E}_{\mathfrak{f}} \text{vol}_{n-q} \mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) = 2^n \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} \mathbb{E}_{\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}} \# \mathcal{Z}((\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}), \mathbb{P}_{\mathbb{R}}^n). \quad (5.3)$$

Now, by Theorem 1.1,

$$\mathbb{E}_{\mathfrak{f}} \text{vol}_{n-q} \mathcal{Z}(\mathfrak{f}, \mathbb{P}_{\mathbb{R}}^n) \leq \frac{1}{4^n} \frac{\text{vol}_{n-q} \mathbb{P}_{\mathbb{R}}^{n-q}}{\text{vol}_n \mathbb{P}_{\mathbb{R}}^n} (n(n+1))^{n-q} \prod_{k=1}^q t_k(t_k - 1),$$

since the \mathfrak{l}_k have support of size $n+1$, and we obtain the desired upper bound.

We now prove our claim regarding coordinate hyperplanes. Without loss of generality assume that $i = n$. To show that

$$\mathcal{Z}((\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q}), H_n)$$

is empty, it is enough to show that the random overdetermined system

$$\mathfrak{g} := (\mathfrak{f}, \mathfrak{l}_1, \dots, \mathfrak{l}_{n-q})(X_0, \dots, X_{n-1}, 0),$$

obtained by setting X_n equal to 0, has no zeros in $\mathbb{P}_{\mathbb{R}}^{n-1}$. But this is precisely what Proposition 5.1 states. \square

Proof of Proposition 5.1. We will prove this by induction on n . The statement is obvious for $n = 0$. Consider the system

$$\mathfrak{g}_1(X_0, \dots, X_{n-1}, 0), \dots, \mathfrak{g}_n(X_0, \dots, X_{n-1}, 0),$$

then, by the induction hypothesis, this system does not have any zero in $\mathbb{P}_{\mathbb{R}}^{n-1}$ with probability one. In other words, as adding equations can only reduce the number of zeros,

$$\mathcal{Z}(\mathfrak{g}, \mathbb{P}_{\mathbb{R}}^n) \cap \mathcal{Z}(X_n, \mathbb{P}_{\mathbb{R}}^n) = \emptyset$$

with probability one. Now, the same argument works, if instead of X_n we consider X_i . Therefore, for all i ,

$$\mathcal{Z}(\mathfrak{g}, \mathbb{P}_{\mathbb{R}}^n) \cap \mathcal{Z}(X_i, \mathbb{P}_{\mathbb{R}}^n) = \emptyset$$

with probability one. Now, we only need to show that

$$\bigcup \{ \mathcal{Z}(\mathfrak{g}, S\mathbb{P}_{\mathbb{R}}^n) \mid S = \text{diag}(\pm 1, \dots, \pm 1) \} = \emptyset,$$

with probability one, where $\mathbb{P}_{\mathbb{R}}^n := \{x \in \mathbb{P}^n \mid x_0 > 0, \dots, x_n > 0\}$. Now, by symmetry, it is enough to show that, with probability one,

$$\mathcal{Z}(\mathfrak{g}, \mathbb{P}_{\mathbb{R}}^n) = \emptyset.$$

However, the latter follows from the fact that a generic overdetermined system of Laurent polynomials does not have zeros in $(\mathbb{C}^*)^n$ [76, Lemma 1]. This is not explicitly stated in [76, Lemma 1], but it can be easily seen by considering the overdetermined system of $q > n$ equations in n variables as a system in q variables after adding $q - n$ dummy variables—then, by [76, Lemma 1], the corresponding ideal is not proper for generic polynomials and, by evaluating to 1 the dummy variables, so it was not the original ideal. \square

References

- [1] C. D. Aliprantis and K. C. Border. *Infinite dimensional analysis: A hitchhiker's guide*. Third Edition. Springer, Berlin, 2006. DOI: 10.1007/3-540-29587-9.
- [2] D. Armentano, J.-M. Azaïs, F. Dalmao, and J. R. León. “Asymptotic variance of the number of real roots of random polynomial systems”. In: *Proc. Amer. Math. Soc.* 146.12 (2018), pp. 5437–5449. DOI: 10.1090/proc/14215.
- [3] D. Armentano, J.-M. Azaïs, F. Dalmao, and J. R. León. “Central limit theorem for the number of real roots of Kostlan Shub Smale random polynomial systems”. In: *Amer. J. Math.* 143.4 (2021), pp. 1011–1042. DOI: 10.1353/ajm.2021.0026.
- [4] D. Armentano, J.-M. Azaïs, F. Dalmao, and J. R. León. “Central limit theorem for the volume of the zero set of Kostlan-Shub-Smale random polynomial systems”. In: *J. Complexity* 72 (2022), Paper No. 101668, 22. DOI: 10.1016/j.jco.2022.101668.
- [5] J.-M. Azaïs and M. Wschebor. *Level sets and extrema of random processes and fields*. John Wiley & Sons, Inc., Hoboken, NJ, 2009. DOI: 10.1002/9780470434642.
- [6] T. Bayraktar and A. U. Ö. Kışisel. *Expected Multivolumes of Random Amoebas*. 2023. DOI: 10.48550/arXiv.2304.01530.
- [7] D. N. Bernshtein. “The number of roots of a system of equations”. In: *Functional Analysis and Its Applications* 9.3 (1975), pp. 183–185. DOI: 10.1007/BF01075595.
- [8] F. Bihan. “Polynomial systems supported on circuits and dessins d’enfants”. In: *J. Lond. Math. Soc. (2)* 75.1 (2007), pp. 116–132. DOI: 10.1112/jlms/jdl013.
- [9] F. Bihan and A. Dickenstein. “Descartes’ rule of signs for polynomial systems supported on circuits”. In: *Int. Math. Res. Not. IMRN* 22 (2017), pp. 6867–6893. DOI: 10.1093/imrn/rnw199.
- [10] F. Bihan, A. Dickenstein, and M. Giaroli. “Lower bounds for positive roots and regions of multistationarity in chemical reaction networks”. In: *J. Algebra* 542 (2020), pp. 367–411. DOI: <https://doi.org/10.1016/j.jalgebra.2019.10.002>.
- [11] F. Bihan and B. El Hilany. “A sharp bound on the number of real intersection points of a sparse plane curve with a line”. In: *J. Symbolic Comput.* 81 (2017), pp. 88–96. DOI: 10.1016/j.jsc.2016.12.003.
- [12] F. Bihan, F. Santos, and P.-J. Spaenlehauer. “A polyhedral method for sparse systems with many positive solutions”. In: *SIAM J. Appl. Algebra Geom.* 2.4 (2018), pp. 620–645. DOI: 10.1137/18M1181912.
- [13] F. Bihan and F. Sottile. “Fewnomial bounds for completely mixed polynomial systems”. In: *Adv. Geom.* 11.3 (2011), pp. 541–556. DOI: 10.1515/ADVGEOM.2011.019.
- [14] F. Bihan and F. Sottile. “New fewnomial upper bounds from Gale dual polynomial systems”. In: *Mosc. Math. J.* 7.3 (2007), pp. 387–407, 573. DOI: 10.17323/1609-4514-2007-7-3-387-407.
- [15] P. Breiding, P. Bürgisser, A. Lerario, and L. Mathis. “The zonoid algebra, generalized mixed volumes, and random determinants”. In: *Adv. Math.* 402 (2022), Paper No. 108361, 57. DOI: 10.1016/j.aim.2022.108361.
- [16] P. Breiding, S. Fairchild, P. Santarsiero, and E. Shehu. *Average degree of the essential variety*. 2022. DOI: 10.48550/arXiv.2212.01596.
- [17] I. Briquel and P. Bürgisser. “The real tau-conjecture is true on average”. In: *Random Structures Algorithms* 57.2 (2020), pp. 279–303. DOI: 10.1002/rsa.20926.
- [18] J. G. Broida and S. G. Williamson. *A comprehensive introduction to linear algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.
- [19] P. Bürgisser. *Completeness and reduction in algebraic complexity theory*. Vol. 7. Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 2000. DOI: 10.1007/978-3-662-04179-6.

- [20] P. Bürgisser. “Real Zeros of Mixed Random Fewnomial Systems”. In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*. ISSAC '23. Tromsø, Norway: Association for Computing Machinery, 2023, pp. 107–115. DOI: 10.1145/3597066.3597105.
- [21] P. Bürgisser and F. Cucker. *Condition: The Geometry of Numerical Algorithms*. Vol. 349. Grundlehren der mathematischen Wissenschaften. Springer, 2013. DOI: 10.1007/978-3-642-38896-5.
- [22] P. Bürgisser, A. A. Ergür, and J. Tonelli-Cueto. “On the number of real zeros of random fewnomials”. In: *SIAM J. Appl. Algebra Geom.* 3.4 (2019), pp. 721–732. DOI: 10.1137/18M1228682.
- [23] P. Bürgisser and A. Lerario. “Probabilistic Schubert calculus”. In: *J. Reine Angew. Math.* 760 (2020), pp. 1–58. DOI: 10.1515/crelle-2018-0009.
- [24] D. A. Cox. *Applications of Polynomial Systems*. Vol. 134. CBMS Regional Conference Series in Mathematics. American Mathematical Society, 2020. With contributions by C. D’Andrea, A. Dickenstein, J. Hauenstein, H. Schenck and J. Sidman.
- [25] J. A. De Loera, J. Rambau, and F. Santos. *Triangulations: Structures for algorithms and applications*. Vol. 25. Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 2010. DOI: 10.1007/978-3-642-12971-1.
- [26] R. Descartes. *La Géométrie*. Digital reproduction of 2008 by Project Gutenberg (Ebook number: 26400). Librairie Scientifique A. Hermann, 1886. URL: <http://www.gutenberg.org/ebooks/26400>.
- [27] A. Dickenstein. “Algebraic geometry tools in systems biology”. In: *Notices Amer. Math. Soc.* 67.11 (2020), pp. 1706–1715. DOI: 10.1090/noti.
- [28] A. Dickenstein. “Positive solutions of sparse polynomial systems”. In: *ISSAC’20—Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 2020, pp. 5–7. DOI: 10.1145/3373207.3403978.
- [29] A. Edelman and E. Kostlan. “How many zeros of a random polynomial are real?” In: *Bull. Amer. Math. Soc. (N.S.)* 32.1 (1995), pp. 1–37. DOI: 10.1090/S0273-0979-1995-00571-9.
- [30] D. Eisenbud and J. Harris. *3264 and all that—a second course in algebraic geometry*. Cambridge University Press, Cambridge, 2016. DOI: 10.1017/CB09781139062046.
- [31] A. A. Ergür and T. de Wolff. “A polyhedral homotopy algorithm for real zeros”. In: *Arnold Mathematical Journal* (2022). DOI: 10.1007/s40598-022-00219-w.
- [32] G. Fantuzzi, D. Goluskin, D. Huang, and S. I. Chernyshenko. “Bounds for deterministic and stochastic dynamical systems using sum-of-squares optimization”. In: *SIAM J. Appl. Dyn. Syst.* 15.4 (2016), pp. 1962–1988. DOI: 10.1137/15M1053347.
- [33] E. Feliu and M. Helmer. “Multistationarity and bistability for Fewnomial chemical reaction networks”. In: *Bull. Math. Biol.* 81.4 (2019), pp. 1089–1121. DOI: 10.1007/s11538-018-00555-z.
- [34] E. Feliu and A. Sadeghimanesh. “Kac-Rice formulas and the number of solutions of parametrized systems of polynomial equations”. In: *Math. Comp.* 91.338 (2022), pp. 2739–2769. DOI: 10.1090/mcom/3760.
- [35] E. Feliu and C. Wiuf. “A computational method to preclude multistationarity in networks of interacting species”. In: *Bioinformatics* 29.18 (July 2013), pp. 2327–2334. DOI: 10.1093/bioinformatics/btt400.
- [36] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2008. DOI: 10.1007/978-0-8176-4771-1. Reprint of the 1994 edition.
- [37] M. Giaroli, R. Rischter, M. P. Millán, and A. Dickenstein. “Parameter regions that give rise to $2\lfloor\frac{n}{2}\rfloor + 1$ positive steady states in the n -site phosphorylation system”. In: *Math. Biosci. Eng.* 16.6 (2019), pp. 7589–7615. DOI: 10.3934/mbe.2019381.
- [38] C. G. Gibson, K. Wirthmüller, A. A. du Plessis, and E. J. N. Looijenga. *Topological stability of smooth mappings*. Lecture Notes in Mathematics, Vol. 552. Springer-Verlag, Berlin-New York, 1976. DOI: 10.1007/BFb0095244.
- [39] E. Gross, H. A. Harrington, Z. Rosen, and B. Sturmfels. “Algebraic systems biology: a case study for the Wnt pathway”. In: *Bull. Math. Biol.* 78.1 (2016), pp. 21–51. DOI: 10.1007/s11538-015-0125-1.

- [40] R. Howard. “The kinematic formula in Riemannian homogeneous spaces”. In: *Mem. Amer. Math. Soc.* 106.509 (1993), pp. vi+69. DOI: 10.1090/memo/0509.
- [41] G. Jindal, A. Pandey, H. Shukla, and C. Zisopoulos. “How many zeros of a random sparse polynomial are real?” In: *ISSAC’20—Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 2020, pp. 273–280. DOI: 10.1145/3373207.3404031.
- [42] B. Ya. Kazarnovskii. “Average Number of Roots of Systems of Equations”. In: *Functional Analysis and Its Applications* 54.2 (2020), pp. 100–109. DOI: 10.1134/S0016266320020033.
- [43] B. Ya. Kazarnovskii. “How many roots of a system of random Laurent polynomials are real?” In: *Sbornik: Mathematics* 213.4 (Apr. 2022), p. 466. DOI: 10.1070/SM9559.
- [44] A. G. Khovanskii. *Fewnomials*. Vol. 88. Translations of Mathematical Monographs. Providence, RI: American Mathematical Society, 1991.
- [45] P. Koiran. “Shallow Circuits with High-Powered Inputs”. In: *Logical Approaches to Barriers in Computing and Complexity*. Ed. by A. Beckmann, C. Gaßner, and B. Löwe. Alfried Krupp Wissenschaftskolleg Greifswald. Greifswald, Germany, Feb. 2010, pp. 55–57.
- [46] P. Koiran, N. Portier, and S. Tavenas. “On the intersection of a sparse curve and a low-degree curve: a polynomial version of the lost theorem”. In: *Discrete Comput. Geom.* 53.1 (2015), pp. 48–63. DOI: 10.1007/s00454-014-9642-1.
- [47] E. Kostlan. “On the distribution of roots of random polynomials”. In: *From Topology to Computation: Proceedings of the Smalefest (Berkeley, CA, 1990)*. Springer, New York, 1993, pp. 419–431. DOI: 10.1007/978-1-4612-2740-3_38.
- [48] Z. Kukulova, M. Bujnak, and T. Pajdla. “Automatic generator of minimal problem solvers”. In: *Computer Vision—ECCV 2008: 10th European Conference on Computer Vision, Marseille, France, October 12–18, 2008, Proceedings, Part III 10*. Springer. 2008, pp. 302–315. DOI: 10.1007/978-3-540-88690-7_23.
- [49] A. G. Kushnirenko. *Letter to Professor Sottile (February 26, 2008)*. Available at: [https://www.math.tamu.edu/~\[31/05/2019\]](https://www.math.tamu.edu/~[31/05/2019]).
- [50] A. G. Kushnirenko. “Polyèdres de Newton et nombres de Milnor [French]”. In: *Invent. Math.* 32.1 (1976), pp. 1–31. DOI: 10.1007/BF01389769.
- [51] J. M. Lee. *Introduction to smooth manifolds*. Second Edition. Vol. 218. Graduate Texts in Mathematics. Springer, New York, 2013. DOI: 10.1007/978-1-4419-9982-5.
- [52] T. Letendre. “Variance of the volume of random real algebraic submanifolds”. In: *Trans. Amer. Math. Soc.* 371.6 (2019), pp. 4129–4192. DOI: 10.1090/tran/7478.
- [53] T. Letendre and M. Puchol. “Variance of the volume of random real algebraic submanifolds II”. In: *Indiana Univ. Math. J.* 68.6 (2019), pp. 1649–1720. DOI: 10.1512/iumj.2019.68.7830.
- [54] T.-Y. Li, J. M. Rojas, and X. Wang. “Counting real connected components of trinomial curve intersections and m -nomial hypersurfaces”. In: *Discrete Comput. Geom.* 30.3 (2003), pp. 379–414. DOI: 10.1007/s00454-003-2834-8.
- [55] G. Malajovich. “On the expected number of real roots of polynomials and exponential sums”. In: *J. Complexity* 76 (2023), Paper No. 101720, 11. DOI: 10.1016/j.jco.2022.101720.
- [56] G. Malajovich. “On the expected number of zeros of nonlinear equations”. In: *Found. Comput. Math.* 13.6 (2013), pp. 867–884. DOI: 10.1007/s10208-013-9171-y.
- [57] G. Malajovich and J. M. Rojas. “Polynomial systems and the momentum map”. In: *Foundations of computational mathematics (Hong Kong, 2000)*. World Sci. Publ., River Edge, NJ, 2002, pp. 251–266. DOI: 10.1142/9789812778031_0010.
- [58] L. Mathis and M. Stecconi. *Expectation of a random submanifold: the zonoid section*. 2022. DOI: 10.48550/arXiv.2210.11214.
- [59] John W. Milnor. *Topology from the differentiable viewpoint*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1997. Based on notes by D. W. Weaver. Revised reprint of the 1965 original.

- [60] S. Müller, E. Feliu, G. Regensburger, C. Conradi, A. Shiu, and A. Dickenstein. “Sign Conditions for Injectivity of Generalized Polynomial Maps with Applications to Chemical Reaction Networks and Real Algebraic Geometry”. In: *Found. Comput. Math.* 16 (2013), pp. 69–97. DOI: 10.1007/s10208-014-9239-3.
- [61] N. K. Obatake, A. Shiu, X. Tang, and A. Torres. “Oscillations and bistability in a model of ERK regulation”. In: *J. Math. Biol.* 79.4 (2019), pp. 1515–1549. DOI: 10.1007/s00285-019-01402-y.
- [62] M. Perez Millan, A. Dickenstein, A. Shiu, and C. Conradi. “Chemical Reaction Systems with Toric Steady States”. In: *Bull. Math. Biol.* 74 (Oct. 2011), pp. 1027–65. DOI: 10.1007/s11538-011-9685-x.
- [63] K. Phillipson and J. M. Rojas. “Fewnomial systems with many roots, and an adelic tau conjecture”. In: *Tropical and non-Archimedean geometry*. Vol. 605. Contemp. Math. Amer. Math. Soc., 2013, pp. 45–71. DOI: 10.1090/conm/605/12111.
- [64] J. M. Rojas. “Counting Real Roots in Polynomial-Time via Diophantine Approximation”. In: *Foundations of Computational Mathematics* (2022). DOI: 10.1007/s10208-022-09599-z.
- [65] J. M. Rojas. “On the average number of real roots of certain random sparse polynomial systems”. In: *The mathematics of numerical analysis (Park City, UT, 1995)*. Vol. 32. Lectures in Appl. Math. Amer. Math. Soc., 1996, pp. 689–699.
- [66] T. W. Sederberg and R. N. Goldman. “Algebraic geometry for computer-aided geometric design”. In: *IEEE Computer Graphics and Applications* 6.6 (1986), pp. 52–59. DOI: 10.1109/MCG.1986.276742.
- [67] B. Shiffman and S. Zelditch. “Random polynomials with prescribed Newton polytope”. In: *J. Amer. Math. Soc.* 17.1 (2004), pp. 49–108. DOI: 10.1090/S0894-0347-03-00437-5.
- [68] Bernard Shiffman and Steve Zelditch. “Random complex fewnomials, I”. In: *Notions of positivity and the geometry of polynomials*. Trends Math. Birkhäuser/Springer Basel AG, Basel, 2011, pp. 375–400. DOI: 10.1007/978-3-0348-0142-3_20.
- [69] M. Shub and S. Smale. “Complexity of Bezout’s theorem. II. Volumes and probabilities”. In: *Computational algebraic geometry (Nice, 1992)*. Vol. 109. Progr. Math. Birkhäuser Boston, Boston, MA, 1993, pp. 267–285. DOI: 10.1007/978-1-4612-2752-6_19.
- [70] A. J. Sommese and C. W. Wampler. *The Numerical solution of systems of polynomials arising in engineering and science*. World Scientific, 2005. DOI: 10.1142/5763.
- [71] F. Sottile. *Real solutions to equations from geometry*. Vol. 57. University Lecture Series. American Mathematical Society, Providence, RI, 2011. DOI: 10.1090/ulect/057.
- [72] B. Sturmfels. “On the Newton polytope of the resultant”. In: *J. Algebraic Combin.* 3.2 (1994), pp. 207–236. DOI: 10.1023/A:1022497624378.
- [73] B. Sturmfels. “On the number of real roots of a sparse polynomial system”. In: *Hamiltonian and gradient flows, algorithms and control*. Vol. 3. Fields Inst. Commun. Amer. Math. Soc., 1994, pp. 137–143. DOI: 10.1007/978-1-4939-7486-3_1.
- [74] J. Tonelli-Cueto. “Condition and Homology in Semialgebraic Geometry”. Doctoral thesis. Technische Universität Berlin, Dec. 2019. DOI: 10.14279/depositonce-9453.
- [75] O. Viro. “From the sixteenth Hilbert problem to tropical geometry”. In: *Jpn. J. Math.* 3.2 (2008), pp. 185–214. DOI: 10.1007/s11537-008-0832-6.
- [76] J. Yu. “Do most polynomials generate a prime ideal?” In: *J. Algebra* 459 (2016), pp. 468–474. DOI: 10.1016/j.jalgebra.2016.03.050.

A Borel measures and Dynkin’s lemma

The point of this appendix is to make clearer, for readers unfamiliar with measure theory, the measure-theoretic arguments underlying the proof of Theorem 2.1.

Recall the following definitions for families of sets.

Definition A.1. Let X be a set and $\mathcal{S} \subset \mathcal{P}(X)$ a non-empty collection of subsets of X . We say that:

- (σ) [1, 4.1 Definition] \mathcal{S} is a σ -algebra if \mathcal{S} contains the empty set and it is closed under complements and countable pairwise disjoint unions, i.e.,
- $\emptyset \in \mathcal{S}$.
 - for all $A \in \mathcal{S}$, $X \setminus A \in \mathcal{S}$.
 - for every pairwise disjoint numerable subfamily $\{A_n\}_{n \in \mathbb{N}}$ of \mathcal{S} , $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{S}$.
- (λ) [1, 4.9 Definition] \mathcal{S} is a λ -system if \mathcal{S} contains X , relative complements and monotone numerable unions, i.e.,
- $X \in \mathcal{S}$.
 - for all $A, B \in \mathcal{S}$ such that $B \subseteq A$, $A \setminus B \in \mathcal{S}$.
 - for every numerable subfamily $\{A_n\}_{n \in \mathbb{N}}$ of \mathcal{S} that is increasing (for all n , $A_n \subseteq A_{n+1}$), $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{S}$.
- (π) [1, 4.9 Definition] \mathcal{S} is a π -system if \mathcal{S} is closed under finite intersections, i.e., for every $A, B \in \mathcal{S}$, $A \cap B \in \mathcal{S}$.

Given any collection of sets, we can consider the σ -algebra, λ -system and π -system that it generates, by considering the smallest σ -algebra, λ -system or π -system that contains it. For a topological space, the following σ -algebra is essential.

Definition A.2. [1, 4.14 Definition] Let X be a topological space, its *Borel σ -algebra*, $\mathcal{B}(X)$, is the σ -algebra generated by the collection of its open subsets.

The Dynkin's lemma allows us to extend statements from π -systems to the σ -algebra they generate by checking that they are satisfied at a λ -system.

Theorem A.3 (Dynkin's lemma). [1, 4.11 Dynkin's Lemma] Let X be a set and \mathcal{S} collection of subsets of X . If \mathcal{S} is a π -system, then the λ -system it generates is a σ -algebra.

Recall that a topological space X is σ -compact if we can write X as a countable monotone union of compact sets and that a *Borel measure* of X is a measure of the form

$$\mu : \mathcal{B}(X) \rightarrow [0, \infty].$$

The following theorem lies at the core of the proof of Theorem 2.1.

Theorem A.4. Let X be a σ -compact topological space and μ and ν Borel measures on X . Assume that there is a collection of open subsets \mathcal{U} such that:

- (U0) \mathcal{U} is a base for the topology of X , i.e., every open set in X is an union of open sets in \mathcal{U} .
- (U1) \mathcal{U} is closed under containment, i.e., if U and V are open sets, $V \subseteq U$ and $U \in \mathcal{U}$, then $V \in \mathcal{U}$.
- (U2) for all $U \in \mathcal{U}$, $\mu(U)$ and $\nu(U)$ are finite.
- (U3) μ and ν agree on \mathcal{U} , i.e., for all $U \in \mathcal{U}$, $\mu(U) = \nu(U)$.

Then

$$\mu = \nu.$$

Proof. By assumption, there is an increasing sequence of compact subsets $\{X_n\}_{n \in \mathbb{N}}$ such that $X = \bigcup_{n \in \mathbb{N}} X_n$. Assume without loss of generality that $X_0 = \emptyset$. For each $n \in \mathbb{N}$, let

$$\mu_n := \mu|_{\mathcal{B}(X_n)} \quad \text{and} \quad \nu_n := \nu|_{\mathcal{B}(X_n)}$$

be the restriction of the Borel-measures μ and ν to X_n . If for all $n \in \mathbb{N}$, $\mu_n = \nu_n$, then $\mu = \nu$. To see this, take $B \in \mathcal{B}(X)$ and observe that

$$\mu(B) = \sum_{k=0}^{\infty} \mu(B \cap (X_{k+1} \setminus X_k)) = \sum_{k=0}^{\infty} \mu_n(B \cap (X_{k+1} \setminus X_k))$$

and

$$\nu(B) = \sum_{k=0}^{\infty} \nu(B \cap (X_{k+1} \setminus X_k)) = \sum_{k=0}^{\infty} \nu_n(B \cap (X_{k+1} \setminus X_k)).$$

Fix arbitrary $n \in \mathbb{N}$. We consider

$$\mathcal{U}_n := \{U \cap X_n \mid U \in \mathcal{U}\},$$

which is a collection of open subsets of X_n , and

$$\Lambda_n := \{B \in \mathcal{B}(X_n) \mid \mu_n(B) = \nu_n(B)\}.$$

If we show that \mathcal{U}_n satisfies (U0), (U1), (U3) and (U4) for μ_n and ν_n , then \mathcal{U}_n is a π -system contained in Λ_n whose generated σ -algebra is $\mathcal{B}(X_n)$. If we show, moreover, that Λ_n is a λ -system, then, by Dynkin's lemma (Theorem A.3),

$$\Lambda_n = \mathcal{B}(X_n)$$

and we are done, since then $\mu_n = \nu_n$.

We show now that \mathcal{U}_n satisfies (U0), (U1), (U3) and (U4) for μ_n and ν_n :

- \mathcal{U}_n satisfies (U0) and (U1), by the definition of the subspace topology and the construction of \mathcal{U}_n .
- For checking (U2) and (U3) for \mathcal{U}_n , we only need to write for $U \in \mathcal{U}$,

$$\mu(U \cap X_n) = \mu(U) - \mu(U \setminus X_n) = \nu(U) - \nu(U \setminus X_n) = \mu(U \cap X_n).$$

This is possible, because $U \setminus X_n \in \mathcal{U}$, by (U1); $\mu(U)$, $\nu(U)$, $\mu(U \setminus X_n)$ and $\nu(U \setminus X_n)$ are finite, by (U2); and $\mu(U) = \nu(U)$ and $\mu(U \setminus X_n) = \nu(U \setminus X_n)$, by (U3).

We show now that Λ_n is a λ -system:

- Since X_n is compact and \mathcal{U}_n is an open cover, we have that there are $U_1, \dots, U_\ell \in \mathcal{U}_n$ such that

$$X_n = U_1 \cup \dots \cup U_\ell.$$

But then, by the inclusion-exclusion principle, (U2) and (U3), $\mu_n(X_n) = \nu_n(X_n)$. Hence $X_n \in \Lambda_n$.

Moreover, this argument shows that $\mu_n(X_n) = \nu_n(X_n)$ is finite, and so $\mu_n(A)$ and $\nu_n(A)$ are finite for all $A \in \mathcal{B}(X_n)$.

- If $A, B \in \Lambda_n$ and $B \subseteq A$, then

$$\mu_n(A \setminus B) = \mu_n(A) - \mu_n(B) = \nu_n(A) - \nu_n(B) = \nu_n(A \setminus B),$$

where the middle equality follows from $A, B \in \Lambda_n$, since $\mu_n(A)$, $\mu_n(B)$, $\nu_n(A)$ and $\nu_n(B)$ are finite. Hence $A \setminus B \in \Lambda_n$.

- Let $\{A_k\}_{k \in \mathbb{N}} \subset \Lambda_n$ is an increasing family of subsets. Without loss of generality, assume that $A_0 = \emptyset$. Then

$$\mu_n \left(\bigcup_{k \in \mathbb{N}} A_k \right) = \sum_{k \in \mathbb{N}} \mu_n(A_{k+1} \setminus A_k)$$

and

$$\nu_n \left(\bigcup_{k \in \mathbb{N}} A_k \right) = \sum_{k \in \mathbb{N}} \nu_n(A_{k+1} \setminus A_k).$$

By the previous paragraph and the assumption $\{A_k\} \subset \Lambda_n$, the right-hand sides are equal. Therefore the left-hand sides are so, and $\bigcup_{k \in \mathbb{N}} A_k \in \Lambda_n$.

Now, the proof is complete. □