Lectures on Random Algebraic Geometry

Paul Breiding and Antonio Lerario

Contents

1 How many zeros of a polynomial are real?

How many zeros has a polynomial? The answer to this question is taught in a basic algebra course: it is equal to the degree of the polynomial. This is known as the fundamental theorem of algebra.

However, this assumes that the question was stated as *How many complex zeros does a polynomial have?*. Yet, if the person, who asked that question, had in mind a real polynomial and real zeros, the answer is less clear. For instance, the polynomial $x^2 + ax + b$ has two real zeros, if $a^2 - 4b > 0$, it has one real zero, if $a^2 - 4b = 0$, and in the case $a^2 - 4b < 0$ it has no real zeros. The situation is depicted in Figure 1.1. This simple yet important example shows already that we can not give an answer to the above question in terms of the degree of the polynomial. Instead, we have to use a list of algebraic equalities and inequalities. While for polynomials of degree 2 this was simple enough for us to understand, more complicated counting problems pose uncomparably harder challenges. Think of the number of eigenvalues of an $n \times n$ matrix. The number of complex eigenvalues is always n (counted with multiplicity). But the algebraic constraints for the number of real solutions are already so complicated, that it is very difficult just to compute this number without computing all eigenvalues in the first place.

In this book we want to lay out an alternative perspective on counting problems like the ones above. Instead of computing a deterministic real picture, we want to understand its *statistical properties*. This thinking is not new: already in the 1930s and 1940s Littlewood, Offord [9] and Kac [6, 7] considered real zeros of random polynomials. Later, in 1973, Montgomery [10] introduced randomness to number therory. In the 1950s, Wigner [12], Dyson [2] and others proposed using probability for understanding models in theoretical physics. Ginibre [5] summarizes their motivation as follows.

> *"In the absence of any precise knowledge [...], one assumes a reasonable probability distribution [...], from which one deduces statistical properties [...]. Apart from the intrinsic interest of the problem, one may hope that the methods and results will provide further insight in the cases of physical interest or suggest as yet lacking applications."*

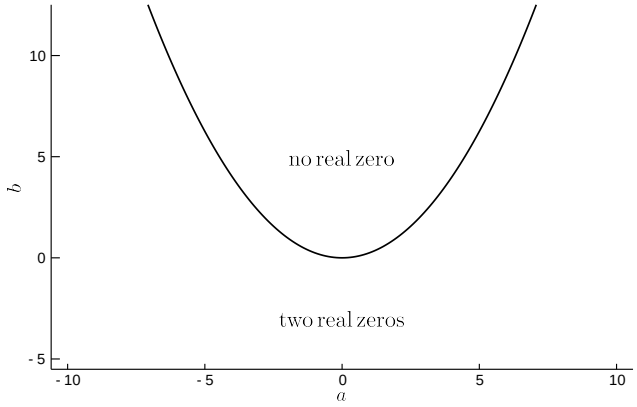

Figure 1.1: The configuration space for real zeros of the polynomial $f = x^2 + ax + b$. The blue curve $a^2 - 4b = 0$ is called the discriminant. If (a, b) is below the discriminant, then f has two real zeros. If it is above, it has no real zero. Polynomials on the discriminant have one real zero.

Although written in the context of statistical physics, Ginibre's words perfectly outline the ideas we wish to present with this book: we want to use tools from probability theory to understand the nature of algebraic–geometric objects.

Edelman and Kostlan [3] condense the probabilistic approach in the title of their seminal paper "How many zeros of a random polynomial are real?" (the answer is in Example 3 below). We chose the title of this introductory section as a homage of their work. Starting from their results, we explore in this book algebraic geometry from a probabilistic point of view. Our name for this new field of research is *Random Algebraic Geometry*.

Here is an illustrative example of what we have in mind: consider the degree 8 polynomial $f_\epsilon(x) = 1 + \epsilon_1 x + \epsilon_2 x^2 + \epsilon_3 x^3 + \epsilon_4 x^4 + \epsilon_5 x^5 + \epsilon_6 x^6 + \epsilon_7 x^7 + \epsilon_8 x^8$, where $\epsilon = (\epsilon_1, \ldots, \epsilon_8) \in \{-1, 1\}^8$. This polynomial can have $0, 2, 4, 6$ or 8 zeros, because complex zeros come in conjugate pairs. Instead of attempting to understand the equations separating the regions with a certain number of real solutions, we endow the coefficients of f_ϵ with a probability distribution. We assume that $\epsilon_1, \ldots, \epsilon_8$ are independent random variables with $\mathbb{P}\{\epsilon_i = 1\} = \frac{1}{2}$ for $1 \leq i \leq 8$, and we denote by $n(\epsilon)$ the random variable "number of real zeros of f_ϵ". Booth [1] showed that

$$\mathbb{P}\{n(\epsilon) = 0\} = \frac{58}{2^8}, \quad \mathbb{P}\{n(\epsilon) = 2\} = \frac{190}{2^8}, \quad \mathbb{P}\{n(\epsilon) = 4\} = \frac{8}{2^8}, \quad \text{and}$$
$$\mathbb{P}\{n(\epsilon) = 6\} = \mathbb{P}\{n(\epsilon) = 8\} = 0,$$

which shows that f_ϵ has at most 4 zeros, and having more than 2 zeros is unlikely.

In Booth's example we have access to the full probability law. However, during this book we will encounter many situations in which computing the probability law is too ambitious. Instead, it is often feasible to compute or estimate the expected value of a random geometric property. For instance, in Booth's example the expected value of the number of roots is $\mathbb{E}\, n(\epsilon) = 1.609375$. Just based on this information we can conclude that having a large number of zeros is unlikely.

Interestingly, many of the expected values we will meet later in this book obey what is called the "square-root law": the expected number of real solutions is roughly the square-root of the number of complex solutions. If this law holds, it immediately implies that instances, for which the number of real solutions equal the number of complex solutions, are *rarae aves*. This phenomenon, which is specific of a particular, but natural, probability distribution that we will work with, has several manifestation: from geometry (expectation of volumes of real algebraic sets) to topology (expectation of Betti numbers).

1.1 Discriminants

Let us have a closer look at the picture in Figure 1.1. We can see that the *discriminant* $\Sigma_{\mathbb{R}} := \{(a,b) \in \mathbb{R}^2 \mid a^2 - 4b = 0\}$ divides the real (a,b)-plane into two components – one, where the number of real zeros is two, and one, where there are no real zeros. This is because the discriminant is a curve of *real* codimension 1. The complex picture is different: here, the complex curve $\Sigma_{\mathbb{C}} = \{(a,b) \in \mathbb{C}^2 \mid a^2 - 4b = 0\}$ is of *complex* codimension one. In particular, it is of real codimesion two, and $\mathbb{C}^2 \backslash \Sigma_{\mathbb{C}}$ is path-connected! We show this in Lemma 1.4, but it can also be seen in Figure 1.2. This is the reason for why each polynomial of degree 2 outside $\Sigma_{\mathbb{C}}$ has two complex zeros: a function which is locally constant on a connected space is constant. We say that having two complex zeros is a *generic property*. We will give a more precise definition of this later in Definition 1.3.

In algebraic geometry, it is more appropriate to work with zeros of polynomials in *projective space* rather than with zeros in $\mathbb{C}^n$. The definition of projective space comes next.

Definition 1.1 (Complex projective Space)**.** The complex projective space $\mathbb{C}\mathrm{P}^n$ of dimension n is defined to be the set of lines through the origin in $\mathbb{C}^{n+1}$. That is, $\mathbb{C}\mathrm{P}^n := (\mathbb{C}^{n+1} \backslash \{0\}) / \sim$, where $y \sim z$, if and only of there exists some $\lambda \in \mathbb{C} \backslash \{0\}$ with $y = \lambda z$. For a point $(z_0, z_1, \ldots, z_n) \in \mathbb{C}^{n+1}$ we denote by $[z_0, z_1, \ldots, z_n]$ its equivalence class in $\mathbb{C}\mathrm{P}^n$.

For completing the terminology, and distinguishing it from projective space, we say that $\mathbb{C}^n$ is an n-dimensional *affine complex space*.

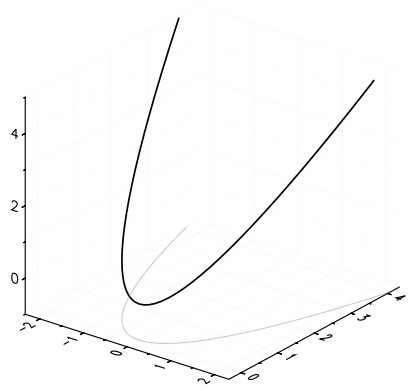

Figure 1.2: The picture shows the part of the complex discriminant $(a_1 + ia_2)^2 - 4(b_1 + ib_2) = 0$, where $a_1 = 2a_2$ As can be seen from the picture, the discriminant is of real codimension two. Because one can "go around" the discriminant without crossing it, a generic complex polynomial of degree 2 has two complex zeros.

The map

$$P : \mathbb{C}^{n+1}\backslash\{0\} \to \mathbb{C}\mathrm{P}^n \, , (z_0, z_1, \ldots, z_n) \mapsto [z_0 : \ldots : z_n]$$

projects $(n+1)$-dimensional affine space onto n-dimensional projective space. On the other hand, the map $\psi : \mathbb{C}^n \to \mathbb{C}\mathrm{P}^n$, $(z_1, \ldots, z_n) \mapsto [1, z_1 : \ldots : z_n]$ embeds n-dimensional affine space into n-dimensional projective space. Using this embedding we can define the zero sets in Example 1 to be in $\mathbb{C}\mathrm{P}^n$.

Projective zero sets are defined by *homogeneous polynomials*. It is common to use the notation $f = \sum_{|\alpha|=d} f_\alpha \, z^\alpha$ for complex homogeneous polynomials of degree d in $n+1$ variables, where $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{N}^{n+1}$, $z^\alpha = \prod_{i=0}^n z_i^{\alpha_i}$ and $|\alpha| = \alpha_0 + \cdots + \alpha_n$. The space of homogeneous polynomials of degree d in $n+1$ many variables is

$$\mathbb{C}[x_0, \ldots, x_n]_{(d)} := \left\{ \sum_{|\alpha|=d} f_\alpha \, z^\alpha \;\middle|\; (f_\alpha) \in \mathbb{C}^N \right\}, \text{ where } N = \binom{n+d}{d},$$

and the projective space of polynomials is thus $\mathbb{C}\mathrm{P}^{N-1}$. The complex projective zero set of k polynomials $f = (f_1, \ldots, f_k)$, where the i-th polynomial is $f_i \in \mathbb{C}[z_0, \ldots, z_n]_{(d_i)}$, is

$$Z_{\mathbb{C}}(f) = \{[z] \in \mathbb{C}\mathrm{P}^n : f_1(z) = 0, \ldots, f_k(z) = 0\}.$$

For a simplified notation we also denote by $Z_{\mathbb{C}}(f)$ the zero set of f in $\mathbb{C}^{n+1}$.

Remark 1.2. A polynomial $f \in \mathbb{C}[z_0, \dots, z_n]_{(d)}$ is not a function on the complex projective space $\mathbb{C}\mathrm{P}^n$, but its zero set is still well defined.

Example 1. Here are a few more examples of generic properties. The first generalizes our introductory example to higher degrees.

1. A generic homogeneous polynomial $f \in \mathbb{C}[z_0, z_1]_{(d)}$ of degree d has d distinct zeros in $\mathbb{C}\mathrm{P}^1$ unless $\mathrm{Res}(f, f') = 0$ (i.e. the resultant of f and f' is zero). We define the polynomial map $\mathrm{disc}(f) := \mathrm{Res}(f, f')$ that associates to a polynomial f the resultant $\mathrm{Res}(f, f')$. Then, the zero set $\Sigma = Z_{\mathbb{C}}(\mathrm{disc})$ of this polynomial is a proper algebraic set in $\mathbb{C}[z_0, z_1]_d$, which we again call the discriminant. By Lemma 1.4 below, $\mathbb{C}[z_0, z_1]_d \setminus \Sigma$ is path-connected. This causes polynomials in $\mathbb{C}[z_0, z_1]_d \setminus \Sigma$ to admit the generic behavior of having d distinct zeros in $\mathbb{C}\mathrm{P}^1$, because we continuously deform the zero set of any $f_1 \notin \Sigma$ to the zero set of any other $f_2 \notin \Sigma$.
2. The zero set $Z_{\mathbb{C}}(f) \subset \mathbb{C}\mathrm{P}^2$ of a generic $f \in \mathbb{C}[z_0, z_1, z_2]_{(d)}$ of degree d is homeomorphic to a surface of genus $g = \frac{(d-1)(d-2)}{2}$. In this case what happens is that there exists a polynomial $\mathrm{disc} : \mathbb{C}[z_0, z_1, z_2]_{(d)} \to \mathbb{C}$, which vanishes exactly at polynomials whose corresponding zero set in the projective plane is singular. Again, we call $\Sigma = Z_{\mathbb{C}}(\mathrm{disc})$ the discriminant. Outside of the discriminant the topology of $Z(f)$ all look the same: the reason is again that $\mathbb{C}[z_0, z_1, z_2]_{(d)} \setminus \Sigma$ is path-connected by Lemma 1.4.
3. Let $\mathbb{C}[z_0, z_1]_{(3)}$ be the space of homogeneous complex polynomials of degree 3. Inside this space there is the cone $X^{\mathbb{C}}$ of polynomials which are powers of linear forms: $X^{\mathbb{C}} = \{f \in \mathbb{C}[z_0, z_1]_{(3)} \mid \exists \ell \in \mathbb{C}[z_0, z_1]_{(1)} : f = \ell^3\}$. The linear span of $X^{\mathbb{C}}$ is the whole $\mathbb{C}[z_0, z_1]_{(3)}$, therefore for every $f \in \mathbb{C}[z_0, z_1]_{(3)}$ there exist $\ell_1, \dots, \ell_s \in \mathbb{C}[z_0, z_1]_{(1)}$ and $\alpha_1, \dots, \alpha_s \in \mathbb{C}$ such that $f = \sum_{i=1}^{s} \alpha_i \ell_i^3$. For the generic $f \in \mathbb{C}[z_0, z_1]_{(3)}$ the minimal s for having this is $s = 2$. This means that there is a discriminant $\Sigma \subsetneq \mathbb{C}[z_0, z_1]_{(3)}$, which is a proper algebraic subset, such that this property holds outside Σ.
4. The zero set $Z_{\mathbb{C}}(f) \subset \mathbb{C}\mathrm{P}^3$ of a generic cubic $f \in \mathbb{C}[z_0, z_1, z_2, z_3]_{(3)}$ contains 27 complex lines. We will discuss in details this type of problems later, but still let us now try to see what is happening, at least in an informal way. The set of lines in $\mathbb{C}\mathrm{P}^3$ is itself a manifold, which is called the Grassmanian of (projective) lines and denoted by $\mathbb{G}(1, 3)$ (1-dimensional projective subspaces of 3-dimensional projective space). There is a rank-4 complex vector bundle $E \to \mathbb{G}(1, 3)$ whose fiber over a line $\ell \in \mathbb{C}\mathrm{P}^3$ consists of homogeneous polynomials of degree 3 over this line. Every polynomial $f \in \mathbb{C}[z_0, z_1, z_2, z_3]_{(3)}$ defines naturally a section $\sigma_f : \mathbb{G}(1, 3) \to E$ by $\sigma_f(\ell) = f|_\ell$ and a line ℓ is contained in $Z_{\mathbb{C}}(f)$ if and only if $\sigma_f(\ell) = 0$. The discriminant $\Sigma \subset \mathbb{C}[z_0, z_1, z_2, z_3]_{(3)}$ consists of those polynomials whose section σ_f is not transversal to the zero section

In most cases the properties we will be interested in are described by a list of numbers associated to elements of some parameter space S. Let us re-interpret the statement from Example 1 using this language. If $S = P(\mathbb{C}[z_0, z_1]_{(d)} = \mathbb{CP}^d$ is the projective space of complex polynomials of degree d, we might be interested in the number of zeroes of these polynomials. We can interpret this number as a map $\beta : \mathbb{CP}^d \to \mathbb{C}$ given by

$$\beta : f \mapsto \#Z(f).$$

This β is a constant map outside $\Sigma = \{f \mid \mathrm{Res}(f, f') = 0\}$.

The next definition gives a rigorous definition for genericity in our setting.

Definition 1.3 (Generic Properties)**.** Let S be a semialgebraic set[1]. We say that a property β is *generic* for the elements of S if there exists a semialgebraic set $\Sigma \subset S$ of codimension at least one in S such that the property β is true for all elements in $S\backslash\Sigma$. We call the largest (by inclusion) such Σ the *discriminant* of the property β.

When working over the complex numbers most properties are generic in the sense that the discriminant is a proper *complex* algebraic set. Since proper complex algebraic sets in $\mathbb{CP}^N$ do not disconnect the whole space, these properties are constant on an open dense set. This is a simple observation that we record in the next lemma.

Lemma 1.4. *Let $\Sigma \subsetneq \mathbb{CP}^N$ be a proper algebraic subset. Then, $\mathbb{CP}^N\backslash\Sigma$ is path-connected.*

Proof. Let $z_1, z_2 \in \mathbb{CP}^N\backslash\Sigma$. Choose a complex linear space $L \subset \mathbb{CP}^N$ of dimension one, such that $z_1, z_2 \in L$. Then, $L \cap \Sigma$ is a subvariety of L. Since L is irreducible, if $\dim(L \cap \Sigma) = 1$, we must have $L \subset \Sigma$, but this contradicts $z_1, z_2 \notin \Sigma$. Thus, we have $\dim(L \cap \Sigma) = 0$, which means that L intersects Σ in finitely many points. Since L is of complex dimension one, it is of real dimenson two, and thus $L\backslash\Sigma$ is path-connected. We find a real path from z_1 to z_2 that does not intersect Σ. □

Very often the properties that we will be interested in are values of some semialgebraic functions $\beta : S \to \mathbb{C}^n$, as in the second point from Example 1. To see this, let $S = P(\mathbb{C}[z_0, \ldots, z_n]_{(d)})$ be the projective space of polynomials and consider the "property" $\beta : S \to \mathbb{C}^{2n+1}$ given by $\beta(f) = (b_0(Z_{\mathbb{C}}(f)), \ldots, b_{2n}(Z_{\mathbb{C}}(f)))$ (i.e. $\beta(f)$ is the list of the Betti numbers of the zero set of f in $\mathbb{CP}^n$; this number does not depend on the representative of f that we pick, as a nonzero multiple of a polynomial has the same zero set as the original polynomial). The property β

[1] A semialgebraic set $S \subset \mathbb{R}^n$ is a finite union and intersections of sets of the form $\{f \leq 0\}$ or $\{f < 0\}$, with $f \in \mathbb{R}[x_0, \ldots, x_n]$.

in this case takes a constant value on the complement of a complex discriminant $\Sigma \subset S$. In other words, there exists $\beta_0 \in \mathbb{C}^{2n+1}$ such that for all $f \in S \backslash \Sigma$ we have $\beta(Z_{\mathbb{C}}(f)) = \beta_0$. In the case $n = 2$, because the genus is $\frac{(d-1)(d-2)}{2}$, we have that $\beta_0 = (1, (d-1)(d-2), 1)$. A similar argument can be done for the third point in Example 1: the property "number of lines on the zero set of f" is constant outside a complex discriminant $\Sigma \subset \mathbb{C}[z_0, \ldots, z_3]_{(3)}$.

As already briefly discussed in the beginning of this section, the topological reason for the existence of such strong generic properties over the complex numbers ultimately is Lemma 1.4. The additional technical ingredient that one needs to deduce that topological properties are stable under nondegenerate deformations goes under the name of *Thom's Isotopy Lemma* and we will prove it and discuss its implications later.

1.2 Real discriminants

Moving to the real world, let us copy the notation from the preceding section to the real numbers.

Definition 1.5 (Real projective Space)**.** The real projective space $\mathbb{R}\mathrm{P}^n$ of dimension n is defined to be the set of lines through the origin in $\mathbb{R}^{n+1}$. That is, $\mathbb{R}\mathrm{P}^n := (\mathbb{R}^{n+1} \backslash \{0\}) / \sim$, where $y \sim z$, if and only of there exists some $\lambda \in \mathbb{R} \backslash \{0\}$ with $y = \lambda z$. For a point $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ we denote by $[x_0 : x_1 : \ldots : x_n]$ its equivalence class in $\mathbb{R}\mathrm{P}^n$.

Similar to before, we define the projection

$$P : \mathbb{R}^{n+1} \backslash \{0\} \to \mathbb{R}\mathrm{P}^n,\ (x_0, x_1, \ldots, x_n) \mapsto [x_0 : x_1 : \ldots : x_n]. \tag{1.1}$$

The space of real homogeneous polynomials is

$$\mathbb{R}[x_0, \ldots, x_n]_{(d)} := \left\{ \sum_{|\alpha|=d} f_\alpha \, x^\alpha \;\middle|\; (f_\alpha) \in \mathbb{R}^N \right\},\ \text{where } N = \binom{n+d}{d}.$$

The projective space of real polynomials is $P(\mathbb{R}[x_0, \ldots, x_n]_{(d)})$. The real projective zero set of k polynomials $f = (f_1, \ldots, f_k)$ is

$$Z(f) = \{[x] \in \mathbb{R}\mathrm{P}^n : f_1(x) = 0, \ldots, f_k(x) = 0\}.$$

Over the Reals we do not have in general an analogue of Lemma 1.4: a proper real algebraic set can in general disconnect the ambient space. To see this, let us look again at the problems discussed in example 1, but from the real point of view.

Example 2. Let us start by noticing that the complex properties studied in Example 1 are still generic over the reals, in the sense that for the generic *real* polynomial the structure of the *complex* zero set has a constant generic behavior; the structure of the *real* zero set is instead highly dependent on the coefficients of f and there is no "generic" behaviour.

1. A generic univariate polynomial $f \in \mathbb{R}[x]_d$ of degree d has at most d distinct zeros in $\mathbb{R}$, but this number can range anywhere between $\frac{1+(-1)^{d+1}}{2}$ and d. In particular there is no generic number of real zeroes.

   A property which is generic is having real *distinct* zeroes. In this case, however, the real discriminant is not algebraic, but rather just semialgebraic. Unless $d = 2$ it not coincide with the real part of $\{\mathrm{Res}(f, f') = 0\}$: the equation $\mathrm{Res}(f, f') = 0$, which is real for real f, tells us whether f has a double root, but this root can also be complex. The subset of the real part of $\{\mathrm{Res}(f, f') = 0\}$ which corresponds to polynomials with a double real root is only a piece of this discriminant and this piece is selected by imposing some extra inequalities on the coefficients of the polynomial.

2. The zero set $Z(f) \subset \mathbb{R}\mathrm{P}^2$ of a generic $f \in \mathbb{R}[x_0, x_1, x_2]_{(d)}$ is a smooth curve (being smooth is a generic property) but the topology of this curve depends on the coefficients of the polynomial – Harnack's inequality tells that

$$b_0(Z(f)) \leq \frac{(d-1)(d-2)}{2} + 1. \tag{1.2}$$

   For instance $\{x_0^2 + x_1^2 + x_2^2 = 0\} \subset \mathbb{R}\mathrm{P}^2$ is empty and $\{x_0^2 - x_1^2 - x_2^2 = 0\} \subset \mathbb{R}\mathrm{P}^2$ is homeomorphic to a circle (they are both smooth).

3. Let $\mathbb{R}[x_0, x_1]_{(3)}$ be the space of homogeneous real polynomials of degree 3. Inside this space there is the cone X of polynomials which are powers of real linear forms: $X = \{f \in \mathbb{R}[x_0, x_1]_{(3)} \mid \exists \ell \in \mathbb{R}[x_0, x_1]_{(1)} : f = \ell^3\}$. The linear span of X is the whole $\mathbb{R}[z_0, z_1]_{(3)}$, as in the complex case. Therefore, for every polynomial $f \in \mathbb{R}[z_0, z_1]_{(3)}$ there exist $\ell_1, \ldots, \ell_s \in \mathbb{R}[x_0, x_1]_{(1)}$ and $\alpha_1, \ldots, \alpha_s \in \mathbb{R}$ such that $f = \sum_{i=1}^{s} \alpha_i \ell_i^3$. However now, differently than from the complex case, there is no generic minimal value that the number s can take. In fact, denoting by $\mathrm{rk}_{\mathbb{R}}(f)$ the minimum such s we have that $\mathrm{rk}_{\mathbb{R}}(f) = 2$ whenever a polynomial has one real zero and $\mathrm{rk}_{\mathbb{R}}(f) = 3$ whenever it has 3 real zeroes.

4. The zero set $Z \subset \mathbb{R}\mathrm{P}^3$ of a generic cubic $f \in \mathbb{R}[x_0, x_1, x_2, x_3]_{(3)}$ is smooth and it can contain either $27, 15, 7$ or 3 real lines.
   Remark. There exists a *generic* way of counting the lines on $Z(f)$: it is possible to canonically associate a sign $s(\ell)$ to each line $\ell \subset Z(f)$ and the number $\sum_{\ell \subset Z(f)} s(\ell)$ (a signed count) is generically equal to 3.

1.3 Reasonable probability distributions

In the quote of Ginibre it says "one assumes a reasonable probability distribution". He was probably thinking of physically meaningful distributions. But for us this means the following: suppose that $\mathcal{F}$ is a space of geometric objects endowed with a probability distribution, and that $X : \mathcal{F} \to \mathbb{R}^m$ is a random variable on $\mathcal{F}$. If X has symmetries, by which we mean that there is a group G acting on $\mathcal{F}$, such that $X(g \cdot f) = X(f)$ for all g, then the probability distribution is reasonable, if it is invariant under G; that is $g \cdot f \sim f$. This interpretation follows the *Erlangen program* by Felix Klein. In "A comparative review of recent researches in geometry" [8] Klein lays out a perspective on geometry based on a group of symmetries:

> *"Geometric properties are characterized by their remaining invariant under the transformations of the principal group."*

He writes that geometry should be seen as the following comprehensive problem.

> *"Given a manifoldness and a group of transformations of the same; to investigate the configurations belonging to the manifoldness with regard to such properties as are not altered by the transformations of the group."*

Therefore, reasonable probability distributions are distributions which respect geometry in Klein's sense. A reasonable probability distribution should not prefer one instance over another if they share the same geometry.

To illustrate this line of thought, we recall Booth's example from the beginning of this section. The space of geometric objects $\mathcal{F}$ is the space of univariate polynomials of degree 8 with coefficients in $\{-1, 1\}$. The random variable $X(f)$ is the number of real zeros of the polynomial $f \in \mathcal{F}$. The group $G = \{-1, 1\}$ acts on $\mathcal{F}$ as $g.f(x) = 1 + \epsilon'_1 x + \epsilon'_2 x^2 + \epsilon'_3 x^3 + \epsilon'_4 x^4 + \epsilon'_5 x^5 + \epsilon'_6 x^6 + \epsilon'_7 x^7 + \epsilon'_8 x^8$, where $\epsilon'_i = \epsilon_i g^i$. Since for all i we have $\epsilon_i g^i \in \{-\epsilon_i, \epsilon_i\}$ and since $\epsilon_i \sim -\epsilon_i$, we see that $gf \sim f$. In this sense, the distribution proposed by Booth is reasonable. In many cases the space $\mathcal{F}$ comes with the structure of a smooth manifold (e.g. a vector space, a Lie group or a homogeneous space) and in this case a "reasonable" probability distribution should be absolutely continuous with respect to Lebesgue measure (notice that the notion of sets of measure zero is well defined on a smooth manifold and independent of the possible choice of an actual measure).

In these lectures, when $\mathcal{F}$ is a linear space (e.g. the space of polynomials) we will mostly consider a special class of distributions called *gaussian*. The reason for this is that the set of gaussian distributions is rich enough to describe interesting phenomena and simple enough to be able to put our hands on it.

Definition 1.6 (Nondegenerate gaussian distribution)**.** A probability distribution on $\mathbb{R}^N$ is said to be *nondegenerate gaussian* if there exist a positive definite symmetric matrix $Q \in \mathrm{Sym}(N, \mathbb{R})$ and a vector $\mu \in \mathbb{R}^N$ such that for all $U \subseteq \mathbb{R}^N$ measurable subset we have:

$$\mathbb{P}(U) = \frac{1}{((2\pi)^N \det(Q))^{1/2}} \int_U e^{-\frac{(y-\mu)^T Q^{-1}(y-\mu)}{2}} dy. \tag{1.3}$$

Whenever $\mu = 0$ the distribution is called *centered*. The *standard gaussian distribution* corresponds to the choice $Q = \mathbf{1}$ and $\mu = 0$. For a random variables ξ on the real line distributed as a standard gaussian we will write $\xi \sim N(0, 1)$ and sometimes also call it a *standard normal*. More generally, if $X \in \mathbb{R}^N$ has probability density (1.3), we will say that X is a multivariate nondegenerate gaussian variable with mean μ and covariance matrix $\Sigma = Q^{-1}$, and we will write $X \sim N(\mu, \Sigma)$.

From now on we will always assume that Gaussian distributions are nondegenerate and centered.

Remark 1.7. Let us discuss one important property of gaussian distributions. The matrix $Q > 0$ in (1.4) is positive definite and it therefore defines a scalar product on $\mathbb{R}^N$ by the rule $\langle y_1, y_2 \rangle_Q := y_1^T Q y_2$. If we choose an orthonormal basis $\mathcal{B}_Q = \{e_j\}_{j=1,\dots,N}$ for the scalar product $\langle \cdot, \cdot, \rangle_Q$, then a random element X from the gaussian distribution (1.4) can be written as: $X = \sum_{j=1}^N \xi_j \cdot e_j$ (i.e. X is a linear combination of the basis elements with independent standard gaussian coefficients). This observation will play a crucial practical role later in the book, when dealing with space of random gaussian functions, for which we will need the presentation as a gaussian combination of some basis elements.

We want to introduce now a reasonable probability distribution on the space $\mathbb{R}[x_0, \dots, x_n]_{(d)}$ and, in line with the previous discussion, we require that such distribution satisfies some invariance suggested by the geometry of the objects we are considering.

1. We want it to be "simple", and that is why we require it to be Gaussian, in the following sense. The space of real polynomials $\mathbb{R}[x_0, \dots, x_n]_{(d)}$ is a real vector space of dimension $N = \binom{n+d}{d}$ and therefore it is isomorphic to $\mathbb{R}^N$. We fix a linear isomorphism
$$\varphi : \mathbb{R}^N \to \mathbb{R}[x_0, \dots, x_n]_{(d)}$$
between these two spaces (for example the isomorphism could be given by the coefficients list of the polynomial in some basis). Then, we fix on $\mathbb{R}^N$ a nondegenerate Gaussian distribution $N(Q, \mu)$ in the sense of Definition 1.6. Then, a

Gaussian distribution on $\mathbb{R}[x_0, \ldots, x_n]_{(d)}$ is defined as follows:

$$\mathbb{P}(f \in A) = \frac{1}{((2\pi)^N \det(Q))^{1/2}} \int_{\varphi^{-1}(A)} e^{-\frac{(y-\mu)^T Q^{-1}(y-\mu)}{2}} dy. \tag{1.4}$$

2. A second requirement reflects the fact that the zero set of f and $-f$ are the same. Thinking in terms of group actions, the group $\mathbb{Z}_2 = \{\pm 1\}$ acts on the space of polynomials by $f \mapsto -f$ and we want our distribution to be invariant under this action. This forces $\mu = 0$ in (1.4).
3. Third – maybe the most important requirement, is that we want to get a model of randomness for which there are no preferred points or directions in the projective space $\mathbb{R}\mathrm{P}^n$. Using the language of group invariance, there is a representation $\rho : O(n+1) \to \mathrm{GL}(\mathbb{R}[x_0, \ldots, x_n]_{(d)})$ given by change of variables and we require our distribution to satisfy the property of being invariant under all elements of $\rho(O(n+1))$.

It turns out that the three conditions above do not identify uniquely a probability distribution, and in fact, as we will see later in these lectures, there is a whole family of such distributions. We will call them *invariant distributions*.

1.3.1 The Kostlan distribution

The Kostlan distribution is a special case of an invariant distribution which has some additional special features that make it good for comparisons with complex algebraic geometry. In order to define it, it is helpful to use the following notation:

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

Choose the linear isomorphism $\varphi_{\mathrm{Kostlan}} : \mathbb{R}^N \to \mathbb{R}[x_0, \ldots, x_n]_{(d)}$ defined by

$$\varphi_{\mathrm{Kostlan}}((f_\alpha)_\alpha) = \sum_{|\alpha|=d} f_\alpha \cdot \sqrt{\binom{d}{\alpha}} x_0^{\alpha_0} \cdots x_n^{\alpha_n}. \tag{1.5}$$

Then, for a measurable $A \subseteq \mathbb{R}[x_0, \ldots, x_n]_{(d)}$ its probability with respect to the Kostlan distribution is defined to be:

$$\mathbb{P}(f \in A) = \frac{1}{((2\pi)^N)^{\frac{N}{2}}} \int_{\varphi^{-1}_{\mathrm{Kostlan}}(A)} e^{-\frac{\|y\|^2}{2}} dy. \tag{1.6}$$

Kostlan polynomials are invariant as recorded in the next lemma.

Lemma 1.8. *The Kostlan distribution is an invariant distribution.*

We postpone the proof of this Lemma until we give a thorough discussion of probability distributions which are invariant under group actions.

Following Remark 1.7, let us note that a simple way to write down a Kostlan polynomial is by taking a combination of standard gaussians as follows:

$$f(x) = \sum_{|\alpha|=d} \xi_\alpha \cdot \sqrt{\binom{d}{\alpha}} x_0^{\alpha_0} \cdots x_n^{\alpha_n},$$

where $\{\xi_\alpha\}_{|\alpha|=d}$ is a family of standard, independent gaussian variables on $\mathbb{R}$. The Kostlan distribution, among the invariant ones, is the unique (up to multiples) for which a random polynomial can be written as a combination of independent gaussians in front of the standard monomial basis.

Proposition 1.9. *Among the invariant distributions, the Kostlan one is the unique (up to multiples) such that a random polynomial can be written as a linear combination of the standard monomial basis with coefficients independent gaussians.*

1.4 Expected properties

As we have seen, if the discriminant is a complex algebraic set, we have strong genericity over the complex numbers: the reason for this is Lemma 1.4, which says that the complex discriminant does not disconnect $\mathbb{C}\mathrm{P}^N$. However, if the discriminant is a real hypersurface, in general it might disconnect $\mathbb{R}\mathrm{P}^N$, this is why in Figure 1.1 there are two regions with different properties. Therefore, over the real numbers we might not have a notion of strong genericity, and we adopt a random point of view. The next definition is the probabilistic analogue of Definition 1.3.

Definition 1.10 (Expected Properties)**.** Let S be a semialgebraic set. A measurable property is a measurable function $\beta : S \to \mathbb{C}^m$. If we have a (reasonable) probability distribution on S, we call $\mathbb{E}_{s\in S}\, \beta(s)$ the expected property.

In fact, Definition 1.3 is a special case of Definition 1.10. We will discuss this in Subsection 1.4.1 below. First, let us revisit Example 1 from a probabilistic point of view.

Example 3. Let us endow the space of real polynomials with the Kostlan distribution. Then we can ask for the expectation of the real version of the properties that we have discussed in Example 1.

1. Let $f \in \mathbb{R}[x_0, x_1]_{(d)}$ be a Kostlan polynomial of degree d in 2 variables. Then, for the generic element $f \in \mathbb{R}[x_0, x_1]_{(d)}$ the number of complex zeroes is d, but the expected number of real zeros of f is $\sqrt{d}$.
2. Let $f \in \mathbb{R}[x_0, x_1, x_2]_{(d)}$ be a Kostlan polynomial of degree d in 3 variables. There exist constants $c, C > 0$ such that the expected value of the zero-th Betti number $b_0(f)$ of $Z(f)$ satisfies $cd \leq \mathbb{E}\, b_0(f) \leq Cd$.
3. Let $f \in \mathbb{R}[x_0, x_1]_{(3)}$ be a Kostlan polynomial, then the expectation of its real rank $\mathrm{rk}_{\mathbb{R}}(f)$ is $\frac{9-\sqrt{3}}{2}$.
4. Let $f \in \mathbb{R}[x_0, x_1, x_2, x_3]_{(3)}$ be a Kostlan polynomial of degree 3 in 3 variables. Then, the expected number of real lines on $Z(f)$ is $6\sqrt{2} - 3$.

The first example was proven in [3], the second in [4], and the third is actually a consequence of the first example, but we will also prove them in the remainder of these lectures. The fourth example was proved in [11]. We want to emphasize that the first two of those examples obey a square-root law – the expected value of the real property has the order of the square root of the generic value of the complex property.

1.4.1 Generic properties are expected properties

In closing of this introductory lecture we want to explain why generic properties are, in fact, random properties in disguise. The essence of this is a simple observation: suppose $z \in \mathbb{C}\mathrm{P}^N$ is a random variable that is supported on some full-dimensional subset of $\mathbb{C}\mathrm{P}^N$. In particular, this implies that, if β is a property with discriminant Σ, and if $\Sigma \subsetneq \mathbb{C}\mathrm{P}^N$ is an algebraic variety, then $\mathbb{P}\{z \in \Sigma\} = 0$, and so $\mathbb{P}\{\beta(z) \text{ has the generic value}\} = 1$. Therefore

$$\mathbb{E}\, \beta(z) = \text{ generic value of } \beta(z).$$

It is interesting to approach the problem of computing generic properties from a probablistic point of view. For instance, below we give a proof of a probabilistic Fundamental Theorem of Algebra.

This strategy becomes more effective as the counting problem over the complex numbers becomes more complicated. Consider in fact the random polynomial $f = \sum_{i=0}^{d} c_i x_0^i x_1^{d-i} \in \mathbb{C}[x_0, x_i]_{(d)}$, where the real and imaginary parts of the c_i are independent Gaussian random variables such that $\Re(c_i) \sim N(0, \frac{1}{2}\binom{d}{i})$ and $\Im(c_i) \sim N(0, \frac{1}{2}\binom{d}{i})$ (the factor $\frac{1}{2}$ is for normalizing the variance to $\mathbb{E}\,|c_i|^2 = 1$). Such a polynomial is called a *complex Kostlan polynomial*. The distribution we have put on the coefficients is absolutely continuous with respect to Lebesgue measure on

the space of coefficients, and in fact the distribution of $P(f)$ is supported on the whole $\mathbb{C}\mathrm{P}^d$. Therefore, we know that with probability one we have that $\#Z_{\mathbb{C}}(f)$ equals some constant (we know this constant is d, but let's pretend for a second that we did not know this). Then, if we can find a way (and there is such a way) to compute by elementary means the expectation of $\#Z_{\mathbb{C}}(f)$, we have found its generic value. This observation will be discussed in Section **??**, where we give a probabilistic proof of Bézout's theorem.

Bibliography

[1] Kathleen Booth. An investigation into the real roots of certain polynomials. *Math. Tables and Aids to Computation*, 8:47 pp., 1954.

[2] Freeman Dyson. Statistical Theory of the Energy Levels of Complex Systems. *J. Math. Phys.*, 3(1):140–156, 1962.

[3] Alan Edelman and Eric Kostlan. How many zeros of a random polynomial are real? *Math. Soc. Mathematical Reviews*, 32:1–37, 05 1995.

[4] Damien Gayet and Jean-Yves Welschinger. Lower estimates for the expected Betti numbers of random real hypersurfaces. *J. Lond. Math. Soc. (2)*, 90(1):105–120, 2014.

[5] Jean Ginibre. Statistical ensembles of complex, quaternion, and real matrices. *J. Math. Phys.*, 6:440–449, 1965.

[6] Mark Kac. On the average number of real roots of a random algebraic equation. *Bull. Amer. Math. Soc.*, 49:314–320, 1943.

[7] Mark Kac. On the average number of real roots of a random algebraic equation II. *Proc. London Math. Soc.*, 50:390–408, 1949.

[8] Felix Klein. A comparative review of recent researches in geometry. *Bull. Amer. Math. Soc.*, 2(10):215–249, 1893.

[9] John Littlewood and Albert Offord. On the number of real roots of a random algebraic equation. *J. London Math. Soc.*, 13:288–295, 1938.

[10] Hugh Montogmery. Distribution of the zeros of the Riemann zeta function. *Proc. Internat. Congt. Math.*, 1:379–193, 1973.

[11] Basu Saugata, Antonio Lerario, Erik Lundberg, and Chris Peterson. Random fields and the enumerative geometry of lines on real and complex hypersurfaces. *Math. Ann.*, 374:1773–1810, 2019.

[12] Eugene Wigner. On a Class of Analytic Functions from the Quantum Theory of Collisions. *Annals of Mathematics*, 53(1):36–67, 1951.