

A REVIEW OF SOME RECENT RESULTS ON RANDOM POLYNOMIALS OVER \mathbb{R} AND OVER \mathbb{C} .

DIEGO ARMENTANO

ABSTRACT. This article is divided in two parts. In the first part we review some recent results concerning the expected number of real roots of random system of polynomial equations. In the second part we deal with a different problem, namely, the distribution of the roots of certain complex random polynomials. We discuss a recent result in this direction, which shows that the associated points in the sphere (via the stereographic projection) are surprisingly well-suited with respect to the minimal logarithmic energy on the sphere.

1. INTRODUCTION

Let us consider a system of m polynomial equations in m unknowns over a field \mathbb{K} ,

$$(1) \quad f_i(x) := \sum_{\|j\| \leq d_i} a_j^{(i)} x^j \quad (i = 1, \dots, m).$$

The notation in (1) is the following: $x := (x_1, \dots, x_m)$ denotes a point in \mathbb{K}^m , $j := (j_1, \dots, j_m)$ a multi-index of non-negative integers, $\|j\| = \sum_{h=1}^m j_h$, $x^j = x^{j_1} \cdots x^{j_m}$, $a_j^{(i)} = a_{j_1, \dots, j_m}^{(i)}$, and d_i is the degree of the polynomial f_i .

We are interested in the solutions of the system of equations

$$(2) \quad f_i(x) = 0 \quad (i = 1, \dots, m),$$

lying in some subset V of \mathbb{K}^m . Throughout this review we are mainly concerned with the case $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$.

If we choose at random the coefficients $\{a_j^{(i)}\}$, then the solution of the system (2) becomes a random subset of \mathbb{K}^m . This is the main object of this review.

In the first part of this paper we focus on the real case. The main problem we consider is that of understanding $N^f(V)$: the number of solutions lying in the Borel subset V of \mathbb{R}^m .

Key words and phrases. Random Polynomials; System of Random Equations; Bernstein Basis, Logarithmic Energy, Elliptic Fekete Points.

In the second part we deal with a different problem: How are the roots of complex polynomials distributed?

This article is organized as follows:

In *Section 2* we start with some historical remarks on random polynomials. After that we move to the case of random systems of equations. We mention some recent results for centered Gaussian distributions. In *Section 2.1* we consider the non-centered case, which has also been called “smooth-analysis” in the last years. That is, we start with a fixed (non-random) polynomial system, then we perturb it with a polynomial noise, and we ask what can be said about the number of roots of the perturbed system. In *Section 2.2* we review a result which computes the expected number of roots of a random system of polynomial equations expressed in a different basis, namely, the Bernstein basis. Finally in *Section 3* we focus on the complex case. We discuss a recent result concerning the distribution of points in the sphere associated with roots of random complex polynomials.

This review follows the talk given by the author in the colloquium which was held the inauguration of the Franco-Uruguayan Institute of Mathematics, in Punta del Este, Uruguay, on December 2009.

2. THE NUMBER OF REAL ROOTS OF RANDOM POLYNOMIALS

The study of the expectation of the number of real roots of a random polynomial started in the thirties with the work of Block and Polya [7]. Further investigations were made by Littlewood and Offord [14]. However, the first sharp result is due to M. Kac (see Kac[11, 12]), who gives the asymptotic value

$$\mathbb{E}(N^f(\mathbb{R})) \approx \frac{2}{\pi} \log d, \quad \text{as } d \rightarrow +\infty,$$

when the coefficients of the degree d univariate polynomial f are Gaussian centered independent random variables $N(0, 1)$ (see the book by Bharucha–Reid and Sambandham [6]).

The first important result in the study of real roots of random system of polynomial equations is due to Shub and Smale [20] in 1992, where the authors computed the expectation of $N^f(\mathbb{R}^m)$ when the coefficients are Gaussian centered independent random variables having variances:

$$(3) \quad \mathbb{E} \left[(a_j^{(i)})^2 \right] = \frac{d_i!}{j_1! \cdots j_m! (d_i - \|j\|)!}.$$

Their result was

$$(4) \quad \mathbb{E}(N^f(\mathbb{R}^m)) = \sqrt{d_1 \cdots d_m},$$

that is, the square root of the Bézout number associated to the system. The proof is based on a double fibration manipulation of the co-area formula. Some extensions of their work, including new results for one polynomial in one variable, can be found in Edelman–Kostlan[10]. There are also other extensions to multi-homogeneous systems in McLennan[16], and, partially, to sparse systems in Rojas[17] and Malajovich–Rojas[15]. A similar question for the number of critical points of real-valued polynomial random functions has been considered in Dedieu–Malajovich[9].

The probability law of the Shub–Smale model defined in (3) has the simplifying property of being invariant under the action of the orthogonal group in \mathbb{R}^m . In Kostlan[13] one can find the classification of all Gaussian probability distributions over the coefficients with this geometric invariant property.

In 2005, Azaïs and Wschebor gave a new and deep insight to this problem. The key point is using the Rice formula for random Gaussian fields (cf. Azaïs–Wschebor[5]). This formula allows one to extend the Shub–Smale result to other probability distributions over the coefficients. A general formula for $\mathbb{E}(N^f(V))$ when the random functions f_i ($i = 1, \dots, m$) are stochastically independent and their law is centered and invariant under the orthogonal group on \mathbb{R}^m can be found in Azaïs–Wschebor[4]. This includes the Shub–Smale formula (4) as a special case. Moreover, Rice formula appears to be the instrument to consider a major problem in the subject which is to find the asymptotic distribution of $N^f(V)$ (under some normalization). The only published results of which the author is aware concern asymptotic variances as $m \rightarrow +\infty$. (See Wschebor[25] for a detailed description in this direction and a simpler proof of Shub–Smale result).

2.1. Non-centered Systems. The aim of this section is to remove the hypothesis that the coefficients have zero expectation.

One way to look at this problem is to start with a non-random system of equations (the “signal”)

$$(5) \quad P_i(x) = 0 \quad (i = 1, \dots, m),$$

perturb it with a polynomial noise $X_i(x)$ ($i = 1, \dots, m$), that is, consider

$$P_i(x) + X_i(x) = 0 \quad (i = 1, \dots, m),$$

and ask what one can say about the number of roots of the new system, or, how much the noise modifies the number of roots of the deterministic part. (For short, we denote $N^f = N^f(\mathbb{R}^m)$).

Roughly speaking, we prove in *Theorem 1* that if the relation signal over noise is neither too big nor too small, in a sense that will be made precise later on, there exist positive constants C, θ , where $0 < \theta < 1$, such that

$$(6) \quad \mathbb{E}(N^{P+X}) \leq C \theta^m \mathbb{E}(N^X).$$

Inequality (6) becomes of interest if the starting non-random system (5) has a large number of roots, possibly infinite, and m is large. In this situation, the effect of adding polynomial noise is a reduction at a geometric rate of the expected number of roots, as compared to the centered case in which all the P_i 's are identically zero.

For simplicity we assume that the polynomial noise X has the Shub-Smale distribution. However, one should keep in mind that the result can be extended to other orthogonally invariant distributions (cf. Armentano–Wschebor[2]).

Before the statement of *Theorem 1* below, we need to introduce some additional notations.

In this simplified situation, one only needs hypotheses concerning the relation between the signal P and the Shub-Smale noise X , which roughly speaking should neither be too small nor too big.

Since X has the Shub-Smale distribution, from (3) we get

$$\text{Var}(X_i(x)) = (1 + \|x\|^2)^{d_i}, \quad \forall x \in \mathbb{R}^m, \quad (i = 1, \dots, m).$$

Define

$$H(P_i) := \sup_{x \in \mathbb{R}^m} \left\{ (1 + \|x\|) \cdot \left\| \nabla \left(\frac{P_i}{(1 + \|x\|^2)^{d_i/2}} \right) (x) \right\| \right\},$$

$$K(P_i) := \sup_{x \in \mathbb{R}^m \setminus \{0\}} \left\{ (1 + \|x\|^2) \cdot \left| \frac{\partial}{\partial \rho} \left(\frac{P_i}{(1 + \|x\|^2)^{d_i/2}} \right) (x) \right| \right\},$$

for $i = 1, \dots, m$, where $\|\cdot\|$ is the Euclidean norm, and $\frac{\partial}{\partial \rho}$ denotes the derivative in the direction defined by $\frac{x}{\|x\|}$, at each point $x \neq 0$.

For $r > 0$, put:

$$L(P_i, r) := \inf_{\|x\| \geq r} \frac{P_i(x)^2}{(1 + \|x\|^2)^{d_i}} \quad (i = 1, \dots, m).$$

One can check by means of elementary computations that for each P as above, one has

$$H(P) < \infty, \quad K(P) < \infty.$$

With these notations, we introduce the following hypotheses on the systems as m grows:

$H_1)$

$$(7a) \quad A_m = \frac{1}{m} \cdot \sum_{i=1}^m \frac{H^2(P_i)}{i} = o(1) \quad \text{as } m \rightarrow +\infty$$

$$(7b) \quad B_m = \frac{1}{m} \cdot \sum_{i=1}^m \frac{K^2(P_i)}{i} = o(1) \quad \text{as } m \rightarrow +\infty.$$

 $H_2)$ There exist positive constants r_0, ℓ such that if $r \geq r_0$:

$$L(P_i, r) \geq \ell \quad \text{for all } i = 1, \dots, m.$$

Theorem 1. Under the hypotheses $H_1)$ and $H_2)$, one has

$$(8) \quad \mathbb{E}(N^{P+X}) \leq C \theta^m \mathbb{E}(N^X),$$

where C, θ are positive constants, $0 < \theta < 1$.2.1.1. *Remarks on the statement of Theorem 1.*

- It is obvious that our problem does not depend on the order in which the equations

$$P_i(x) + X_i(x) = 0 \quad (i = 1, \dots, m)$$

appear. However, conditions (7a) and (7b) in hypothesis $H_3)$ do depend on the order. One can state them by saying that there exists an order $i = 1, \dots, m$ on the equations, such that (7a) and (7b) hold true.

- Condition $H_1)$ can be interpreted as a bound on the quotient signal over noise. In fact, it concerns the gradient of this quotient. In (7b) the radial derivative appears, which happens to decrease faster as $\|x\| \rightarrow \infty$ than the other components of the gradient.

Clearly, if $H(P_i), K(P_i)$ are bounded by fixed constants, (7a) and (7b) are verified. Also, some of them may grow as $m \rightarrow +\infty$ provided (7a) and (7b) remain satisfied.

- Hypothesis $H_2)$ goes – in some sense – in the opposite direction: For large values of $\|x\|$ we need a lower bound of the relation signal over noise.
- A result of the type of *Theorem 1* can not be obtained without putting some restrictions on the relation signal over noise. In fact, consider the system

$$(9) \quad P_i(x) + \sigma X_i(x) = 0 \quad (i = 1, \dots, m),$$

where σ is a positive real parameter. If we let $\sigma \rightarrow +\infty$, the relation signal over noise tends to zero and the expected number of roots will tend to $\mathbb{E}(N^X)$. On the other hand, if $\sigma \downarrow 0$, $\mathbb{E}(N^X)$

can have different behaviours. For example, if P is a “regular” system, the expected value of the number of roots of (9) tends to the number of roots of $P_i(x) = 0$, ($i = 1, \dots, m$), which may be much bigger than $\mathbb{E}(N^X)$. In this case, the relation signal over noise tends to infinity.

- As it was mentioned before we can extend *Theorem 1* to other orthogonally invariant distributions. However, for the general version we need to add more hypotheses.

In the next paragraphs we are going to give two simple examples.

For the proof of *Theorem 1* and more examples with different noises see Armentano–Wschebor[2].

2.1.2. *Some Examples.* We assume that the degrees d_i are uniformly bounded.

For the first example, let

$$P_i(x) = \|x\|^{d_i} - r^{d_i},$$

where d_i is even and r is positive and remains bounded as m varies. Then, one has:

$$\begin{aligned} \frac{\partial}{\partial \rho} \left(\frac{P_i}{(1 + \|x\|^2)^{d_i/2}} \right) (x) &= \frac{d_i \|x\|^{d_i-1} + d_i r^{d_i} \|x\|}{(1 + \|x\|^2)^{\frac{d_i}{2}+1}} \leq \frac{d_i(1 + r^{d_i})}{(1 + \|x\|^2)^{3/2}} \\ \nabla \left(\frac{P_i}{(1 + \|x\|^2)^{d_i/2}} \right) (x) &= \frac{d_i \|x\|^{d_i-2} + d_i r^{d_i}}{(1 + \|x\|^2)^{\frac{d_i}{2}+1}} x \end{aligned}$$

which implies

$$\left\| \nabla \left(\frac{P_i}{(1 + \|x\|^2)^{d_i/2}} \right) (x) \right\| \leq \frac{d_i(1 + r^{d_i})}{(1 + \|x\|^2)^{3/2}}.$$

Again, since the degrees d_1, \dots, d_m are bounded by a constant that does not depend on m , H_1) follows. H_2) also holds under the same hypothesis.

Notice that an interest in this choice of the P_i 's lies in the fact that obviously the system $P_i(x) = 0$ ($i = 1, \dots, m$) has an infinite number of roots (all points in the sphere of radius r centered at the origin are solutions), but the expected number of roots of the perturbed system is geometrically smaller than the Shub–Smale expectation, when m is large.

Our second example is the following: Let T be a polynomial of degree d in one variable that has d distinct real roots. Define:

$$P_i(x_1, \dots, x_m) = T(x_i) \quad (i = 1, \dots, m).$$

One can easily check that the system verifies our hypotheses, so that there exist C, θ positive constants, $0 < \theta < 1$ such that

$$\mathbb{E}(N^{P+X}) \leq C \theta^m d^{m/2},$$

where we have used the Shub–Smale formula when the degrees are all the same. On the other hand, it is clear that $N^P = d^m$ so that the diminishing effect of the noise on the number of roots can be observed. A number of variations of these examples for P can be constructed, but we will not pursue the subject here.

2.2. Other Polynomial Basis. Up to now all probability measures were introduced in a particular basis, namely, the monomial basis $\{x^j\}_{\|j\| \leq d}$. However, in many situations, polynomial systems are expressed in different basis, for example, orthogonal polynomials, harmonic polynomials, Bernstein polynomials, etc. So, it is a natural question to ask: *What can be said about $N^f(V)$ when the randomization is performed in a different basis?*

For the case of random orthogonal polynomials see Barucha-Reid and Sambandham[6], and Edelman–Kostlan[10] for random harmonic polynomials.

In this section following Armentano–Dedieu[3] we give an answer to the average number of real roots of a random system of equations expressed in the Bernstein basis. Let us be more precise:

The Bernstein basis is given by:

$$b_{d,k}(x) = \binom{d}{k} x^k (1-x)^{d-k}, \quad 0 \leq k \leq d,$$

in the case of univariate polynomials, and

$$b_{d,j}(x_1, \dots, x_m) = \binom{d}{j} x_1^{j_1} \dots x_m^{j_m} (1 - x_1 - \dots - x_m)^{d-\|j\|}, \quad \|j\| \leq d,$$

for polynomials in m variables, where $j = (j_1, \dots, j_m)$ is a multi-integer, and $\binom{d}{j}$ is the multinomial coefficient.

Let us consider the set of real polynomial systems in m variables,

$$f_i(x_1, \dots, x_m) = \sum_{\|j\| \leq d_i} a_j^{(i)} b_{d,j}(x_1, \dots, x_m) \quad (i = 1, \dots, m).$$

Take the coefficients $a_j^{(i)}$ to be independent Gaussian standard random variables.

Define

$$\tau : \mathbb{R}^m \rightarrow \mathbb{P}(\mathbb{R}^{m+1})$$

by

$$\tau(x_1, \dots, x_m) = [x_1, \dots, x_m, 1 - x_1 - \dots - x_m].$$

Here $\mathbb{P}(\mathbb{R}^{m+1})$ is the projective space associated with \mathbb{R}^{m+1} , $[y]$ is the class of the vector $y \in \mathbb{R}^{m+1}$, $y \neq 0$, for the equivalence relation defining this projective space. The (unique) orthogonally invariant probability measure in $\mathbb{P}(\mathbb{R}^{m+1})$ is denoted by λ_m .

With the above notation the following theorem holds:

Theorem 2. (1) *For any Borel set V in \mathbb{R}^m we have*

$$\mathbb{E}(N^f(V)) = \lambda_m(\tau(V))\sqrt{d_1 \dots d_m}.$$

In particular

$$(2) \mathbb{E}(N^f) = \sqrt{d_1 \dots d_m},$$

$$(3) \mathbb{E}(N^f(\Delta^m)) = \sqrt{d_1 \dots d_m}/2^m, \text{ where}$$

$$\Delta^m = \{x \in \mathbb{R}^m : x_i \geq 0 \text{ and } x_1 + \dots + x_m \leq 1\},$$

(4) *When $m = 1$, for any interval $I = [\alpha, \beta] \subset \mathbb{R}$, one has*

$$\mathbb{E}(N^f(I)) = \frac{\sqrt{d}}{\pi} (\arctan(2\beta - 1) - \arctan(2\alpha - 1)).$$

The fourth assertion in *Theorem 2* is deduced from the first assertion but it also can be derived from Crofton's formula (see for example Edelman–Kostlan[10]).

For the proof of *Theorem 2* see Armentano–Dedieu[3]

3. DISTRIBUTION OF COMPLEX ROOTS OF RANDOM POLYNOMIALS

In this part we will see that points in the sphere associated with roots of Shub–Smale complex analogue random polynomials via the stereographic projection, are surprisingly well-suited with respect to the minimal logarithmic energy on the sphere. That is, they provide a fairly good approximation to a classical minimization problem over the sphere, namely, the Elliptic Fekete points problem.

Next paragraphs follows closely Armentano–Beltrán–Shub[1], where one can find proofs and more detailed references.

Given $x_1, \dots, x_N \in \mathbb{S}^2 = \{x \in \mathbb{R}^3 : \|x\| = 1\}$, let

$$(10) \quad V(x_1, \dots, x_N) = \ln \prod_{1 \leq i < j \leq N} \frac{1}{\|x_i - x_j\|} = - \sum_{1 \leq i < j \leq N} \ln \|x_i - x_j\|$$

be the logarithmic energy of the N -tuple x_1, \dots, x_N . Let

$$V_N = \min_{x_1, \dots, x_N \in \mathbb{S}^2} V(x_1, \dots, x_N)$$

denote the minimum of this function. N -tuples minimizing the quantity (10) are usually called Elliptic Fekete Points. The problem of

finding (or even approximate) such optimal configurations is a classical problem (see White[23] for its origins).

During the last decades this problem has attracted much attention, and the number of papers concerning it has grown amazingly. The reader may see Kuijlaars-Saff[19] for a nice survey.

In the list of Smale's problems for the XXI Century [22], problem number 7 reads:

Can one find $x_1, \dots, x_N \in \mathbb{S}^2$ such that

$$(11) \quad V(x_1, \dots, x_N) - V_N \leq c \ln N,$$

c a universal constant?

More precisely, Smale demands a real number algorithm in the sense of Blum–Cucker–Shub–Smale[8] that with input N returns a N -tuple x_1, \dots, x_N satisfying equation (11), and such that the running time is polynomial on N .

One of the main difficulties when dealing with this problem is that the value of V_N is not even known up to logarithmic precision. In Rakhmanov–Saff–Zhou[18] the authors proved that if one defines C_N by

$$(12) \quad V_N = -\frac{N^2}{4} \ln \left(\frac{4}{e} \right) - \frac{N \ln N}{4} + C_N N,$$

then,

$$-0.112768770\dots \leq \liminf_{N \rightarrow \infty} C_N \leq \limsup_{N \rightarrow \infty} C_N \leq -0.0234973\dots$$

Let X_1, \dots, X_N be independent random variables with common uniform distribution over the sphere. One can easily show that the expected value of the function $V(X_1, \dots, X_N)$ in this case is,

$$(13) \quad \mathbb{E}(V(X_1, \dots, X_N)) = -\frac{N^2}{4} \ln \left(\frac{4}{e} \right) + \frac{N}{4} \ln \left(\frac{4}{e} \right).$$

Thus, this random choice of points in the sphere with independent uniform distribution already provides a reasonable approach to the minimal value V_N , accurate to the order of $O(N \ln N)$.

On one side, this probability distribution has an important property, namely, invariance under the action of the orthogonal group on the sphere. However, on the other hand this probability distribution lacks on correlation between points. More precisely, in order to obtain well-suited configurations one needs some kind of repelling property between points, and in this direction independence is not favorable. Hence, it is a natural question whether other handy orthogonally invariant

probability distributions may yield better expected values. Here is where complex random polynomials comes into account.

Given $z \in \mathbb{C}$, let

$$\hat{z} := \frac{(z, 1)}{1 + |z|^2} \in \mathbb{C} \times \mathbb{R} \cong \mathbb{R}^3$$

be the associated points in the Riemann Sphere, i.e. the sphere of radius $1/2$ centered at $(0, 0, 1/2)$. Finally, let

$$X = 2\hat{z} - (0, 0, 1) \in \mathbb{S}^2$$

be the associated points in the unit sphere.

Given a polynomial f in one complex variable of degree N , we consider the mapping

$$f \mapsto V(X_1, \dots, X_N),$$

where X_i ($i = 1, \dots, N$) are the associated roots of f in the unit sphere. Notice that this map is well defined in the sense that it does not depend on the way we choose to order the roots.

Theorem 3. *Let $f(z) = \sum_{k=0}^N a_k z^k$ be a complex random polynomial, such that the coefficients a_k are independent complex random variables, such that the real and imaginary parts of a_k are independent (real) Gaussian random variables centered at 0 with variance $\binom{N}{k}$. Then, with the notations above,*

$$\mathbb{E}(V(X_1, \dots, X_N)) = -\frac{N^2}{4} \ln\left(\frac{4}{e}\right) - \frac{N \ln N}{4} + \frac{N}{4} \ln \frac{4}{e}.$$

Comparing *Theorem 3* with equations (12) and (13), we see that the value of V is surprisingly small at points coming from the solution set of this random polynomials. More precisely, necessarily many random realizations of the coefficients will produce values of V below the average and very close to V_N , possibly close enough to satisfy equation (11).

Notice that, taking the homogeneous counterpart of f , *Theorem 3* can be restated for random homogeneous polynomials and considering its complex projective solutions, under the identification of $\mathbb{IP}(\mathbb{C}^2)$ with the Riemann sphere. In this fashion, the induced probability distribution over the space of homogeneous polynomials in two complex variables corresponds to the classical unitarily invariant Hermitian structure of the respective space (see Blum–Cucker–Shub–Smale[8]). Therefore, the probability distribution of the roots in $\mathbb{IP}(\mathbb{C}^2)$ is invariant under the action of the unitary group.

It is not difficult to prove that the unitary group action over $\mathbb{IP}(\mathbb{C}^2)$ correspond to the special orthogonal group of the unit sphere. Hence,

the distribution of the associated random roots on the sphere is orthogonally invariant. Thus, *Theorem 3* is another geometric confirmation of the repelling property of the roots of this Gaussian random polynomials.

For a proof of *Theorem 3* and a more detailed discussion on this account see Armentano–Beltrán–Shub[1]. See also Shub–Smale[21].

REFERENCES

- [1] ARMENTANO D., BELTRÁN C. AND SHUB M., *Minimizing the discrete logarithmic energy on the sphere: The role of random polynomials*. Transaction of the American Mathematical Society, to appear.
- [2] ARMENTANO D. AND M. WSCHEBOR, *Random systems of polynomial equations. The expected number of roots under smooth analysis*. Bernoulli 15, No. 1, (2009), 249-266.
- [3] ARMENTANO D. AND DEDIEU J.P., *On the Average Number of real roots of a Bernstein polynomial system*. Journal of Complexity, v.25 n.4, p.339-342, 2009.
- [4] AZAÏS J.-M AND WSCHEBOR M., *On the Roots of a Random System of Equations. The Theorem of Shub and Smale and Some Extensions*, *Found. Comput. Math.*, (2005), 125-144.
- [5] AZAÏS J.-M AND WSCHEBOR M., *Level sets and extrema of random processes and fields*. John Wiley and Sons 2009.
- [6] BHARUCHA-REID A. T. AND SAMBANDHAM M., *Random Polynomials*, Probability and Mathematical Statistics, Academic Press, Orlando, FL, 1986.
- [7] BLOCH A. AND POLYA G., *On the number of real roots of a random algebraic equation*. Proc. Cambridge Philos. Soc., 33:102114, 1932.
- [8] BLUM L., CUCKER F., SHUB M. AND SMALE S., *Complexity and real computation*, Springer-Verlag, New York, 1998.
- [9] DEDIEU J.-P. AND MALAJOVICH G., *On the number of minima of a random polynomial*. Journal of Complexity 24 (2008) 89-108.
- [10] EDELMAN A. AND KOSTLAN E, *How many zeros of a random polynomial are real?*, *Bull. Amer. Math. Soc. (N.S.)* **32**,(1), (1995), 1-37.
- [11] KAC M., *On the average number of real roots of a random algebraic equation*. Bull. Am. Math. Soc. 49 (1943) 314-320 and 938.
- [12] KAC M., *On the average number of real roots of a random algebraic equation (II)*. Proc. London Math. Soc. 50 (1949) 390-408.
- [13] KOSTLAN E., *On the expected number of real roots of a system of random polynomial equations*. In: Foundations of Computational Mathematics, Hong Kong 2002, 149-188. World Sci. Pub., 2002.
- [14] LITTLEWOOD, J. E. AND OFFORD, A. C., *On the number of real roots of a random algebraic equation*. J. London Math. Soc., 13:288295, 1938.
- [15] MALAJOVICH G. AND ROJAS J.M, *High probability analysis of the condition number of sparse polynomial systems*, in *Theoret. Comput. Sci.*, 315(2-3), pp. 524-555, (2004).
- [16] MCLENNAN A., *The expected number of real roots of a multihomogeneous system of polynomial equations*, in *Amer. J. Math.*, 124(1), pp. 49-73, (2002).

- [17] ROJAS J.M., *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., pp. 689-699, Amer. Math. Soc., Providence, RI, (1996).
- [18] RAKHMANOV E.A., SAFF E.B. AND ZHOU Y.M. , *Minimal discrete energy on the sphere*, Math. Res. Letters **1** (1994), 647–662.
- [19] SAFF, E.B. AND KUIJLAARS, A.B.J., *Distributing many points on a sphere*. Math. Intelligencer 19 (1997), no. 1, 5–11.
- [20] SHUB M. AND SMALE S., *Complexity of Bezout's theorem. II. Volumes and probabilities*, Computational algebraic geometry (Nice, 1992), Progr. Math., vol. 109, Birkhäuser Boston, Boston, MA, 1993, pp. 267–285.
- [21] ———, *Complexity of Bezout's theorem. III. Condition number and packing*, J. Complexity **9** (1993), no. 1, 4–14, Festschrift for Joseph F. Traub, Part I.
- [22] SMALE S., *Mathematical problems for the next century*, Mathematics: frontiers and perspectives, Amer. Math. Soc., Providence, RI, 2000, pp. 271–294.
- [23] WHYTE L.L., *Unique arrangements of points on a sphere*, Amer. Math. Monthly **59** (1952), 606–611.
- [24] WSCHEBOR M., *On the Kostlan-Shub-Smale model for random polynomial systems. Variance of the number of roots*, in *J. of Complexity*, 21, pp. 773-789, (2005).
- [25] WSCHEBOR M., *Systems of random equations. A review of some recent results*. In and out of equilibrium. 2, 559–574, Progr. Probab., 60, Birkhuser, Basel, 2008.

CENTRO DE MATEMÁTICA, UNIVERSIDAD DE LA REPÚBLICA. MONTEVIDEO,
URUGUAY