On the roots of a random system of equations. The theorem of Shub & Smale and some extensions.

Jean-Marc Azaïs [*], azais@cict.fr
Mario Wschebor [†], wschebor@cmat.edu.uy

August 20, 2004

Abstract

We give a new proof of a theorem of Shub & Smale [9] on the expectation of the number of roots of a system of m random polynomial equations in m real variables, having a special isotropic Gaussian distribution. Further, we present a certain number of extensions, including the behaviour as $m \to +\infty$ of the variance of the number of roots, when the system of equations is also stationary.

AMS subject classification: Primary 60G60, 14Q99. Secondary: 30C15.
Short Title: Random systems
Key words and phrases: Random polynomials, system of random equations, Rice Formula.

1 Introduction

Let us consider m polynomials in m variables with real coefficients $X_i(t) = X_i(t_1, ..., t_m)$, $i = 1, ..., m$.

[*]Laboratoire de Statistique et Probabilités. UMR-CNRS C5583 Université Paul Sabatier. 118, route de Narbonne. 31062 Toulouse Cedex 4. France.
[†]Centro de Matemática. Facultad de Ciencias. Universidad de la República. Calle Igua 4225. 11400 Montevideo. Uruguay.

We use the notation

$$X_i(t) := \sum_{\|j\| \leq d_i} a_j^{(i)} \; t^j, \tag{1}$$

where $j := (j_1, ..., j_m)$ is a multi-index of non-negative integers, $\|j\| := j_1 + ... + j_m$, $j! := j_1!...j_m!$, $t^j := t_1^{j_1}....t_m^{j_m}$, $a_j^{(i)} := a_{j_1...,j_m}^{(i)}$. The degree of the i-th polynomial is d_i and we assume that $d_i \geq 1 \, \forall i$.

Let $N^X(V)$ be the number of roots lying in the subset V of $\mathbb{R}^m$, of the system of equations

$$X_i(t) = 0, \quad i = 1, ..., m. \tag{2}$$

We will assume throughout that V is a Borel set with the regularity property that its boundary has zero Lebesgue measure. We denote $N^X = N^X(\mathbb{R}^m)$.

We will be interested in random real-valued functions X_i $(i = 1, ...m)$, in which case we will call "random fields" the X_i's, as well as the $\mathcal{R}^m$-valued random function $X(t) = (X_1(t), ..., X_m(t))^T$, $t \in \mathcal{R}^m$. Whenever the X_i's are polynomials we will say that the X_i's and X are "polynomial random fields".

Generally speaking, little is known on the distribution of $N^X(V)$, even for simple choices of the law on the coefficients. In the case of one equation in one variable, a certain number of results have been known since a long time, starting with the work of Marc Kac [6]. See for example the book by Bharucha-Reid & Sambandham [2]

Shub & Smale [9] computed the expectation of N^X when the coefficients are Gaussian, centered independent random variables with certain specified variances (see Theorem 3 below and also the book by Blum *et al.* [3]). Extensions of their work, including new results for one polynomial in one variable, can be found in the review paper by Edelman & Kostlan [5], see also Kostlan [7].

The primary aim of the present paper is to give a new proof of Shub & Smale's Theorem, based upon the so-called Rice formula to compute the moments of the number of roots of random fields. At the same time, this permits certain extensions (some of which are already present in the cited papers by Edelman & Kostlan) to classes of Gaussian polynomials not considered before, and for which some new behaviour of the number of roots can be observed.

Additionally, in Section 6 we consider non-polynomial systems such that the lines are independent and the law of each line is centered Gaussian,

invariant under isometries as well as translations. Under general conditions, we are able to estimate a lower bound for the variance of the number of roots and show that for very general sets, the ratio of the standard deviation over the mean tends to infinity as the number m of variables tends to infinity.

2 Rice formulae

In this section we give a brief account without proofs of Rice formulae, contained in the statements of the following two theorems (Azaïs and Wschebor, [1]).

Theorem 1 *Let V be a compact subset of $\mathcal{R}^m$, $Z : V \to \mathcal{R}^m$ be a random field and $u \in \mathbb{R}^m$ be a fixed point.*

Assume that:

1) Z is Gaussian,

2) $x \rightsquigarrow Z(x)$ is a.s. of class $\mathcal{C}^1$,

3) for each $x \in V$, $Z(x)$ has a non degenerate distribution and denote by $p_{Z(x)}$ its density.

4) $\mathrm{P}\{\exists x \in \dot{V}, Z(x) = u, \det\big(Z'(x)\big) = 0\} = 0$. Here, $\dot{V}$ is the interior of V and Z' denotes the derivative of the field $Z(.)$.

5) $\lambda_m(\partial V) = 0$, where ∂V is the boundary of V and λ_m is the Lebesgue measure on $\mathbb{R}^m$ (we will also use dx instead of $\lambda_m(dx)$). Then, denoting $N_u^Z(V) := \sharp\{x \in V : Z(x) = u\}$, one has

$$\mathrm{E}\left(N_u^Z(V)\right) = \int_I \mathrm{E}\left(|\det(Z'(x))|/Z(x) = u\right)\ p_{Z(x)}(u)dx, \tag{3}$$

and both members are finite. $\mathrm{E}(X/.)$ denotes conditional expectation.

Theorem 2 *Let k, $k \geq 2$ be an integer. Assume the same hypotheses as in Theorem 1 excepting for 3) that is replaced by the stronger one:*

3') for $x_1, ..., x_k \in V$ pairwise different values of the parameter, the distribution of the random vector $\big(Z(x_1), ..., Z(x_k)\big)$ does not degenerate in $(\mathbb{R}^m)^k$

and we denote by $p_{Z(x_1),...,Z(x_k)}$ its density. Then

$$\mathrm{E}\left[\big(N_u^Z(V)\big)\big(N_u^Z(V)-1\big)...\big(N_u^Z(V)-k+1\big)\right] = \int_{V^k} \mathrm{E}\left(\prod_{j=1}^{k} |\det\big(Z'(x_j)\big)| / Z(x_1) = ... = Z(x_k) = u\right) p_{Z(x_1),...,Z(x_k)}(u,...,u)dx_1...dx_k, \quad (4)$$

where both members may be infinite.

If one wants to prove Theorem 1, a direct approach is as follows. Assume that u is not a critical value of Z (This holds true with probability 1 under the hypotheses of Theorem 1). Put $n := N_u^Z(V)$. Since V is compact, n is finite, and if $n \neq 0$, let $x^{(1)},...,x^{(n)}$ be the roots of $Z(x) = u$ belonging to V. One can prove that almost surely $x^{(i)} \notin \partial V$ for all $i = 1,...,n$. Hence, applying the inverse function theorem, if δ is small enough, one can find in V open neighborhoods $U_1,...,U_n$ of $x^{(1)}...,x^{(n)}$ respectively so that:

1. Z is a $\mathcal{C}^1$ diffeomorphism $U_i \to B_m(u,\delta)$, the open ball centered in u with radius δ, for each $i = 1,...,n$.
2. $U_1,...,U_n$ are pairwise disjoint,
3. if $x \notin \bigcup_{i=1}^n U_i$, then $Z(x) \notin B_m(u,\delta)$.

Using the change of variable formula, we have:

$$\int_V |\det\big(Z'(x)\big)| \mathbb{1}_{\{\|Z(x)-u\|<\delta\}} dx = \sum_n^{i=1} \int_{U_i} |\det\big(Z'(x)\big)| dx = \lambda_m(B_m(u,\delta))n.$$

Hence,

$$N_u^Z(V) = n = \lim_{\delta \downarrow 0} \frac{1}{\lambda_m(B_m(u,\delta))} \int_V |\det\big(Z'(x)\big)| \mathbb{1}_{\{\|Z(x)-u\|<\delta\}} dx. \quad (5)$$

If $n = 0$, (5) is obvious. Now an informal computation of $\mathrm{E}(N_u^Z(V))$ can be performed in the following way:

$$\mathrm{E}\big(N_u^Z(V)\big) = \lim_{\delta \downarrow 0} \int_V dx \frac{1}{\lambda_m(B_m(u,\delta))} \int_{B_m(u,\delta)} \mathrm{E}\Big(|\det\big(Z'(x)\big)| / Z(x) = y\Big) p_{Z(x)}(y)dy = \int_V \mathrm{E}\Big(|\det\big(Z'(x)\big)| / Z(x) = u\Big) p_{Z(x)}(u)dx. \quad (6)$$

Instead of formally justifying these equalities, the proof in Azaïs and Wschebor [1] goes in fact through a different path. The proof of Theorem 2 is similar.

For Gaussian fields , an essential simplification in the application of Theorem 1 comes from the fact that, in this case orthogonality implies independence and this is helpful to simplify the conditional expectation in the integrand.

3 Main results

We begin with the statement of Shub & Smale's Theorem.

Theorem 3 ([9]) *Let*

$$X_i(t) = \sum_{\|j\| \le d_i} a_j^{(i)}\ t^j, \quad i = 1, ..., m$$

Assume that the real-valued random variables $a_j^{(i)}$ are independent Gaussian centered, and

$$Var\left(a_j^{(i)}\right) = \binom{d_i}{j_1.....j_m} = \frac{d_i!}{j_1!...j_m!(d_i - \sum_{h=1}^{h=m} j_h)!}.$$

Then,

$$\mathrm{E}\left(N^X\right) = \sqrt{d} \tag{7}$$

where $d = d_1...d_m$ is the Bézout-number of the polynomial system $X(t)$.

A direct computation shows that under the Shub & Smale hypothesis, the X_i's are centered independent Gaussian fields, and the covariance function of X_i is given by

$$r^{X_i}(s,t) = \mathrm{E}\left(X_i(s)X_i(t)\right) = (1 + \langle s,t\rangle)^{d_i},$$

where $\langle s,t\rangle$ denotes the usual scalar product in $\mathbb{R}^m$.

More generally, assume that we only require that the polynomials random fields X_i are independent and that their covariances $r^{X_i}(s,t)$ are invariant under isometries of $\mathbb{R}^m$, i.e. $r^{X_i}(Us,Ut) = r^{X_i}(s,t)$ for any isometry U and any pair (s,t). This implies in particular that the coefficients $a_j^{(i)}$ remain

independent for different i's but can be now correlated from one j to another for the same value of i. It is easy to check that this implies that for each $i = 1, ...m$, the covariance $r^{X_i}(s,t)$ is a function of the triple $(\langle s,t\rangle, \|s\|^2, \|t\|^2)$ ($\|.\|$ is Euclidean norm in $\mathbb{R}^m$). It can also be proved (Spivak [10]) that this function is in fact a polynomial with real coefficients, say $Q^{(i)}$

$$r^{X_i}(s,t) = Q^{(i)}(\langle s,t\rangle, \|s\|^2, \|t\|^2), \tag{8}$$

satisfying the symmetry condition

$$Q^{(i)}(u,v,w) = Q^{(i)}(u,w,v) \tag{9}$$

A simple way to construct a class of covariances of this type is to take

$$Q^{(i)}(u,v,w) = P(u,vw) \tag{10}$$

where P is a polynomial in two variables with non-negative coefficients. In fact, consider the two functions defined on $\mathbb{R}^m \times \mathbb{R}^m$ by means of $(s,t) \rightsquigarrow \langle s,t\rangle$ and $(s,t) \rightsquigarrow \|s\|^2 \|t\|^2$. It is easy to see that both are covariances of polynomial random fields. On the other hand, the set of covariances of polynomial random fields is closed under linear combinations with non-negative coefficients as well as under multiplication, so that $P(\langle s,t\rangle, \|s\|^2 \|t\|^2)$ is also the covariance of some polynomial random field.

One can check that using this recipe one cannot construct all the possible covariances of polynomial random fields. For example, the following polynomial is a covariance (of some polynomial random field).

$$r(s,t) = 1 + \frac{m+1}{m}\langle s,t\rangle^2 - \frac{1}{m}(\|s\|^2\|t\|^2).$$

but, if $m \geq 2$, it can not be obtained from the construction of (10).

The situation becomes simpler if one considers only functions of the scalar product, i.e.

$$Q^{(i)}(u,v,w) = \sum_{k=0}^{d_i} c_k \; u^k.$$

In this case, it is known that the necessary and sufficient condition for it to be a covariance is that $c_k \geq 0 \; \forall k = 0, 1, ..., d_i$. [Shub & Smale corresponds to the choice $c_k = \binom{d_i}{k}$]. Here is a simple proof of this fact using the method of Box & Hunter [4]. The covariance of the random field

$$X(t) = \sum_{\|j\| \leq d} a_j \; t^j, \quad t \in \mathbb{R}^m$$

having the form (1), where the random variables a_j are centered and in L^2 is given by

$$\mathrm{E}\left(X(s)X(t)\right) = \sum_{\|j\|\leq d, \|j'\|\leq d} \gamma_{j,j'} s^j t^{j'} \tag{11}$$

where $\gamma_{j,j'} := \mathrm{E}(a_j a_{j'})$. If $\sum_{k=0}^{d} c_k \ \langle s,t\rangle^k$ is the covariance of a polynomial random field as in (11), one can write:

$$\sum_{\|j\|\leq d, \|j'\|\leq d} \gamma_{j,j'} s^j t^{j'} = \sum_{k=0}^{d} c_k \sum_{\|j\|=k} \frac{k!}{j!} \left(s_1 t_1\right)^{j_1} ... \left(s_m t_m\right)^{j_m} = \sum_{\|j\|\leq d} c_{\|j\|} \frac{\|j\|!}{j!} s^j t^j$$

Identifying coefficients, it follows that $\gamma_{j,j'} = 0$ if $j \neq j'$ and for each $k = 0, 1, ..., d$,

$$c_k = \frac{j!}{k!} \gamma_{j,j} \tag{12}$$

whenever $\|j\| = k$. This shows that $c_k \geq 0$ since $\gamma_{j,j}$ is the variance of the random variable a_j. Reciprocally, if all the c_k re positive, defining $\gamma_{j,j}$ by means of (12) and setting $\gamma_{i,j} = 0$ for $i \neq j$ shows that $\sum_{k=0}^{d} c_k \ \langle s,t\rangle^k$ is the covariance of a polynomial random field.

Notice that the foregoing argument shows at the same time that if the polynomial random field $\{X(t) : t \in \mathbb{R}^m\}$ is Gaussian and has $\sum_{k=0}^{d_i} c_k \ \langle s,t\rangle^k$ as covariance function, then its coefficients are independent random variables. A description of the homogeneous polynomial covariances that are invariant under isometries has been given by Kostlan [7], part II.

We now state an extension of the Shub & Smale theorem, valid under more general conditions.

Theorem 4 *Assume that the X_i are independent centered Gaussian polynomial random fields with covariances $r^{X_i}(s,t) = Q^{(i)}(\langle s,t\rangle, \|s\|^2, \|t\|^2)$ $(i = 1, ..., m)$.*

Let us denote by $Q^{(i)}_u, Q^{(i)}_w, Q^{(i)}_{uv}, ...$ the partial derivatives of $Q^{(i)}$ and set

$$q_i(x) := \frac{Q^{(i)}_u}{Q^{(i)}}$$

$$r_i(x) := \frac{Q^{(i)}\left(Q^{(i)}_{uu} + 2Q^{(i)}_{uv} + 2Q^{(i)}_{uw} + 4Q^{(i)}_{vw}\right) - \left(Q^{(i)}_u + Q^{(i)}_v + Q^{(i)}_w\right)^2}{(Q^{(i)})^2}$$

where the functions in the right-hand sides are always computed at the triplet (x, x, x).

Put:

$$h_i(x) := 1 + x\frac{r_i(x)}{q_i(x)}.$$

Then for all Borel sets V *with boundary having zero Lebesgue measure, we have*

$$\mathrm{E}\big(N^X(V)\big) = (2\pi)^{-m/2} L_{m-1} \int_V \big(\prod_{i=1}^m q_i(\|t\|^2)\big)^{1/2} E_h(\|t\|^2) dt. \qquad (13)$$

Here

$$E_h(x) := \mathrm{E}\big((\sum_{i=1}^m h_i(x)\xi_i^2)^{1/2}\big)$$

where $\xi_1, ..., \xi_m$ *are i.i.d. standard normal in* $\mathbb{R}$ *and*

$$L_n := \prod_{j=1}^n K_j$$

with $K_j = \mathrm{E}(\|\eta_j\|)$ *with* η_j *standard normal in* $\mathbb{R}^j$.

Elementary computations give the identities:

$$K_m = \sqrt{2}\frac{\Gamma((m+1)/2)}{\Gamma(m/2)}$$

$$L_m = \frac{1}{\sqrt{2\pi}} 2^{\frac{m+1}{2}} \Gamma(\frac{m+1}{2}).$$

We define the integral

$$J_m := \int_0^{+\infty} \frac{\rho^{m-1}}{(1+\rho^2)^{(m+1)/2}} d\rho = \sqrt{\pi/2}\frac{1}{K_m}$$

that will appear later on. We need also the surface area σ_{m-1} of the unit sphere S^{m-1} in $\mathbb{R}^m$, $\sigma_{m-1} = \frac{2\pi^{m/2}}{\Gamma(m/2)}$.

Remark on formula (13). Note that formula (13) takes simpler forms

in some special cases. For example, when the functions $h_i(x)$ do not depend on i, denoting by $h(x)$ their common value, we have

$$E_h(x) = \sqrt{h(x)} K_m.$$

Under the hypothesis that $Q^{(i)}(u, v, w) = Q^{d_i}(u)$, we have $q_i(x) = d_i q(x) = d_i \frac{Q'(x)}{Q(x)}$, $h_i(x) = h(x) = 1 - x \frac{Q'^2(x) - Q(x)Q''(x)}{Q(x)Q'(x)}$. Then, for the expectation of the total number of roots i.e. in case $V = \mathbb{R}^m$, using polar coordinates, we get from the last theorem the formula:

$$\begin{aligned} \mathrm{E}(N^X) &= (2\pi)^{-m/2} \sqrt{d_1 ... d_m} L_m \sigma_{m-1} \int_0^\infty \rho^{m-1} q(\rho^2)^{m/2} \sqrt{h(\rho^2)} d\rho \\ &= \sqrt{2/\pi} K_m \sqrt{d_1 ... d_m} \int_0^\infty \rho^{m-1} q(\rho^2)^{m/2} \sqrt{h(\rho^2)} d\rho. \quad (14) \end{aligned}$$

4 Proof of Theorem 4

Consider the normalized Gaussian fields

$$Z_i(t) := \frac{X_i(t)}{\left(Q^{(i)}(\|t\|^2, \|t\|^2, \|t\|^2)\right)^{1/2}}$$

which have variance 1. Denote $Z(t) = (Z_1(t)\ , ...,\ Z_m(t))^T$. Applying Rice Formula for the expectation of the number of zeros of Z (Theorem 1):

$$\mathrm{E}\left(N^X(V)\right) = \mathrm{E}\left(N^Z(V)\right) = \int_V \mathrm{E}\left(|\det(Z'(t)|\, / Z(t) = 0\right) \frac{1}{(2\pi)^{\frac{m}{2}}} dt,$$

where $Z'(t) := [Z_1'(t) \vdots \vdots \vdots Z_m'(t)]$ is the matrix obtained by concatenation of the vectors $Z_1'(t), ..., Z_m'(t)$. Note that since $\mathrm{E}\left(Z_i^2(t)\right)$ is constant, it follows that $\mathrm{E}\big(Z_i(t) \frac{\partial Z_i}{\partial t_j}(t)\big) = 0$ for all $i, j = 1, ..., m$. Since the field is Gaussian this implies that $Z_i(t)$ and $Z_i'(t)$ are independent and given that the coordinate fields $Z_1, ...Z_m$ are independent, one can conclude that for each t, $Z(t)$ and $Z'(t)$ are independent. So

$$\mathrm{E}\left(N^X(V)\right) = \mathrm{E}\left(N^Z(V)\right) = \frac{1}{(2\pi)^{\frac{m}{2}}} \int_V \mathrm{E}\left(|\det(Z'(t)|\right) dt. \quad (15)$$

A straightforward computation shows that the (α, β)- entry, $\alpha, \beta = 1, ..., m$, in the covariance matrix of $Z_i'(t)$ is

$$\mathrm{E}\left(\frac{\partial Z_i}{\partial t_\alpha}(t)\frac{\partial Z_i}{\partial t_\beta}(t)\right) = \frac{\partial^2}{\partial s_\alpha \partial t_\beta} r^{Z_i}(s,t) \mid_{s=t} = r_i(\|t\|^2)t_\alpha t_\beta + q_i(\|t\|^2)\delta_{\alpha\beta},$$

where $\delta_{\alpha,\beta}$ denotes the Kronecker symbol. This can be rewritten as

$$\mathrm{Var}\big(Z_i'(t)\big) = q_i I_m + r_i t t^T,$$

where the functions in the right-hand side are to be computed at the point $\|t\|^2$. Let U be the orthogonal transformation of $\mathbb{R}^m$ that gives the coordinates in a basis with first vector $\frac{t}{\|t\|}$, we get

$$\mathrm{Var}\big(UZ_i'(t)\big) = Diag\big((r_i.\|t\|^2 + q_i), q_i, ..., q_i\big)$$

so that

$$\mathrm{Var}\big(\frac{UZ_i'(t)}{\sqrt{q_i}}\big) = Diag\big(h_i, 1, ..., 1\big)$$

Put now

$$T_i := \frac{UZ_i'(t)}{\sqrt{q_i}}$$

and set

$$T := [T_1 \vdots \vdots \vdots T_m]$$

We have

$$|\det\big(Z'(t)\big)| = |\det\big(T\big)| \prod_{i=1}^{m} q_i^{1/2}. \tag{16}$$

Now, we write

$$T = \begin{bmatrix} W_1 \\ \cdots \\ \cdots \\ \cdots \\ W_m \end{bmatrix},$$

where the W_i are random row vectors. Because of the properties of independence of all the entries of T, we know that :

- $W_2, ..., W_m$ are independent standard Gaussian vectors in $\mathbb{R}^m$

- W_1 is independent from the other W_i, $i \geq 2$, with distribution $N\big(0, Diag(h_1, ..., h_m)\big)$

Now $\mathrm{E}\big(|\det(T)|\big)$ is calculated as the expectation of the volume of the parallelotope generated by $W_1, ..., W_m$ in $\mathbb{R}^m$. That is,

$$|\det(T)| = \|W_1\| \prod_{j=2}^{m} d(W_j, S_{j-1}),$$

where S_{j-1} denotes the subspace of $\mathbb{R}^m$ generated by $W_1, ..., W_{j-1}$ and d denotes the Euclidean distance. Using the invariance under isometries of the standard normal distribution of $\mathbb{R}^m$ we know that, conditioning on $W_1, ..., W_{j-1}$, the projection $P_{S_{j-1}^{\perp}}(W_j)$ of W_j on the orthogonal $S_{j-1}^{\perp}$ of S_{j-1} has a distribution which is standard normal on the space $S_{j-1}^{\perp}$ which is of dimension $m - j + 1$ with probability 1. Thus $\mathrm{E}\big(d(W_j, S_{j-1})/W_1, ..., W_{j-1}\big) = K_{m-j+1}$. By successive conditionings on W_1, W_1, W_2 etc... , we get:

$$\mathrm{E}\big(|\det(T)|\big) = \mathrm{E}\big((\sum_{i=1}^{m} h_i(x)\xi_i^2)^{1/2}\big) \times \prod_{j=1}^{m-1} K_j,$$

where $\xi_1, ..., \xi_m$ are i.i.d. standard normal in $\mathbb{R}$. Using (16) and (15) we obtain (13) . □

5 Examples

5.1 Shub & Smale

In this case we have $Q^{(i)} = Q^{d_i}$ with $Q(u, v, w) = 1 + u$. We get

$$h(x) = q(x) = \frac{1}{1+x},$$

and (7) follows from formula (14).

A simple variant of Shub & Smale theorem corresponds to taking $Q^{(i)}(u) = 1 + u^d$ for all $i = 1, ..., m$ (here all the X_i's have the same law), which yields

$$q(x) = q_i(x) = \frac{du^{d-1}}{1+u^d} \;\; ; \;\; h(x) = h_i(x) = \frac{d}{1+u^d}$$

$$\mathrm{E}(N^X) = \sqrt{\frac{2}{\pi}} K_m \int_0^{+\infty} \frac{\rho^{md-1}}{(1+\rho^{2d})^{(m+1)/2}} d\rho = d^{(m-1)/2}$$

which differs by a constant factor from the analogous Shub & Smale result for $(1+u)^d$ which is $d^{m/2}$.

5.2 Linear systems with a quadratic perturbation

Consider linear systems with a quadratic perturbation

$$X_i(s) = \xi_i + < \eta_i, s > + \zeta_i \|s\|^2,$$

where the ξ_i, ζ_i, η_i, $i = 1, ..., m$ are independent and standard normal in $\mathbb{R}, \mathbb{R}$ and $\mathbb{R}^m$ respectively. This corresponds to the covariance
$r^{X_i}(s,t) = 1 + \langle s, t \rangle + \|s\|^2 \|t\|^2$.

If there is no quadratic perturbation, it is obvious that the number of roots is almost surely equal to 1.

For the perturbed system, applying Theorem 4 and performing the computations required in this case, we obtain:

$$q(x) = \frac{1}{1+x+x^2};\ r(x) = \frac{4}{1+x+x^2} - \frac{(1+2x)^2}{(1+x+x^2)^2};\ h(x) = \frac{1+4x+x^2}{1+x+x^2}$$

and

$$\mathrm{E}(N^X) = \frac{H_m}{J_m} \quad \text{with} \quad H_m = \int_0^{+\infty} \frac{\rho^{m-1}(1+4\rho^2+\rho^4)^{\frac{1}{2}}}{(1+\rho^2+\rho^4)^{\frac{m}{2}+1}}\ d\rho.$$

An elementary computation shows that $\mathrm{E}(N^X) = o(1)$ as $m \to +\infty$ (see the next example for a more precise behavior). In other words, the probability that the perturbed system has no solution tends to 1 as $m \to +\infty$.

5.3 More general perturbed systems

Let us consider the covariances given by the polynomials

$$Q^i(u,v,w) = Q(u,v,w) = 1 + 2u^d + (vw)^d.$$

This corresponds to adding a perturbation depending on the product of the norms of s, t to the modified Shub & Smale systems considered in our first example. We know that for the unperturbed system, one has $\mathrm{E}(N^X) =$

$d^{\frac{m-1}{2}}$. Note that the factor 2 in Q has only been added for computational convenience and does not modify the random variable N^X of the unperturbed system. For the perturbed system, we get

$$q(x) = \frac{2dx^{d-1}}{(1+x^d)^2} \quad ; \quad r(x) = \frac{2d(d-1)x^{d-2}}{(1+x^d)^2} \quad ; \quad h(x) = d.$$

Therefore,

$$\begin{aligned} \mathrm{E}(N^X) &= \sqrt{\frac{2}{\pi}} K_m \int_0^{+\infty} \rho^{m-1} \left(\frac{2d\rho^{2(d-1)}}{(1+\rho^{2d})^2} \right)^{\frac{m}{2}} \sqrt{d}\, d\rho \\ &= \sqrt{\frac{2}{\pi}} K_m 2^{m/2} d^{\frac{m+1}{2}} \int_0^{+\infty} \frac{\rho^{md-1}}{(1+\rho^{2d})^m} d\rho. \quad (17) \end{aligned}$$

The integral can be evaluated by an elementary computation and we obtain

$$\mathrm{E}(N^X) = 2^{-\frac{m-2}{2}} d^{\frac{m-1}{2}},$$

which shows that the mean number of zeros is reduced by the perturbation at a geometrical rate as m grows.

5.4 Polynomial in the scalar product, real roots

Consider again the case in which the polynomials $Q^{(i)}$are all equal and the covariances depend only on the scalar product, i.e. $Q^{(i)}(u,v,w) = Q(u)$. We assume further that the roots of Q, that we denote $-\alpha_1, ..., -\alpha_d$, are real $(0 < \alpha_1 \leq .... \leq \alpha_d)$. We get

$$q(x) = \sum_{h=1}^{d} \frac{1}{x+\alpha_h} \quad ; \; r(x) = \sum_{h=1}^{d} \frac{1}{(x+\alpha_h)^2} \quad ; \; h(x) = \frac{1}{q_i(x)} \sum_{h=1}^{d} \frac{\alpha_h}{(x+\alpha_h)^2}.$$

It is easy now to write an upper bound for the integrand in (13) and compute the remaining integral, thus obtaining the inequality

$$\mathrm{E}(N^X) \leq \sqrt{\frac{\alpha_d}{\alpha_1}} d^{m/2},$$

which is sharp if $\alpha_1 = ... = \alpha_d$.

If we further assume that $d = 2$, with no loss of generality $Q(u)$ has the form $Q(u) = (u+1)(u+\alpha)$ with $\alpha \in [0,1]$. Replacing q by $\frac{1}{x+1} + \frac{1}{x+\alpha}$ in formula (14) we get:

$$\begin{aligned} \mathrm{E}(N^X) &= \sqrt{2/\pi} K_m \\ &\int_0^\infty \rho^{m-1} \Big(\frac{1}{1+\rho^2} + \frac{1}{\alpha+\rho^2}\Big)^{(m-1)/2} \Big(\frac{1}{(1+\rho^2)^2} + \frac{\alpha}{(\alpha+\rho^2)^2}\Big)^{1/2} d\rho. \end{aligned} \tag{18}$$

One can compute the limit of the right-hand side as $\alpha \to 0$. For this purpose, notice that the function $\alpha \to \frac{\alpha}{(\alpha+\rho^2)^2}$ attains its maximum at $\alpha = \rho^2$ and is dominated by $\frac{1}{4\rho^2}$. We divide the integral in the right-hand member of (18) into two parts, setting for some $\delta > 0$

$$I_{\delta,\alpha} := \int_0^\delta \rho^{m-1} \Big(\frac{1}{1+\rho^2} + \frac{1}{\alpha+\rho^2}\Big)^{(m-1)/2} \Big(\frac{1}{(1+\rho^2)^2} + \frac{\alpha}{(\alpha+\rho^2)^2}\Big)^{1/2} d\rho,$$

and

$$J_{\delta,\alpha} := \int_\delta^{+\infty} \rho^{m-1} \Big(\frac{1}{1+\rho^2} + \frac{1}{\alpha+\rho^2}\Big)^{(m-1)/2} \Big(\frac{1}{(1+\rho^2)^2} + \frac{\alpha}{(\alpha+x\rho^2)^2}\Big)^{1/2} d\rho.$$

By dominated convergence,

$$J_{\delta,\alpha} \to \int_\delta^{+\infty} \Big(\frac{2\rho^2+1}{\rho^2+1}\Big)^{(m-1)/2} \frac{d\rho}{1+\rho^2},$$

as $\alpha \to 0$. On the other hand

$$I^-_{\delta,\alpha} \le I_{\delta,\alpha} \le I^+_{\delta,\alpha}$$

where

$$\begin{aligned} I^-_{\delta,\alpha} &:= \int_0^\delta \Big(\frac{\rho^2}{1+\rho^2} + \frac{\rho^2}{\alpha+\rho^2}\Big)^{(m-1)/2} \frac{\sqrt{\alpha}}{\rho^2+\alpha} d\rho \\ &= \int_0^{\delta/\alpha} \Big(\frac{\alpha z^2}{1+\alpha z^2} + \frac{\alpha z^2}{\alpha(z^2+1)}\Big)^{(m-1)/2} \frac{dz}{z^2+1} \to J_m, \end{aligned} \tag{19}$$

as $\alpha \to 0$, and

$$\begin{aligned} I^+_{\delta,\alpha} &:= \int_0^\delta \Big(\frac{\rho^2}{1+\rho^2} + \frac{\rho^2}{\alpha+\rho^2}\Big)^{(m-1)/2} \Big(\frac{1}{1+\rho^2} + \frac{\sqrt{\alpha}}{\rho^2+\alpha}\Big) d\rho \\ &\to \int_0^\delta \Big(\frac{2\rho^2+1}{\rho^2+1}\Big)^{(m-1)/2} \frac{d\rho}{1+\rho^2} + J_m, \end{aligned} \tag{20}$$

as $\alpha \to 0$. Since δ is arbitrary, the integral in the right-hand size of (20) can be chosen arbitrarily small. Using the identity $K_m J_m = \sqrt{\pi/2}$, we get

$$\mathrm{E}(N^X) \to \upsilon := 1 + \frac{1}{J_m} \int_0^{+\infty} \big(\frac{2\rho^2+1}{\rho^2+1}\big)^{(m-1)/2} \frac{d\rho}{1+\rho^2}$$

as $\alpha \to 0$. Since $\frac{2\rho^2}{\rho^2+1} < \frac{2\rho^2+1}{\rho^2+1} < 2$:

$$1 + 2^{(m-1)/2} < \upsilon < 1 + \frac{2^{(m-1)/2}}{J_m} \frac{\pi}{2}.$$

5.5 An analytic example

Our main result can be extended to random analytic functions in an obvious manner.

Consider the case

$$Q^{(i)}(u,v,w) = \exp\big(d_i(u+\beta vw)\big) \quad ; \quad d_i > 0, \beta \geq 0. \tag{21}$$

The case $d_i = 1 \ \forall i = 1, ..., m, \beta = 0$ has been treated by Edelman & Kostlan [5]. We have $\mathrm{E}(N^X) = +\infty$ but it is possible to get a closed expression for $\mathrm{E}\big(N^X(V)\big)$. We have

$$q_i(x) = d_i \quad ; \quad r(x) = 4d_i\beta \quad ; \quad h(x) = 1 + 4\beta x.$$

Hence

$$\mathrm{E}\big(N^X(V)\big) = \int_V g_m(t)dt,$$

with

$$g_m(t) = \frac{\Gamma(m+1)}{\Gamma(m/2+1)} \frac{1}{(4\pi)^{m/2}} \sqrt{d_1 ... d_m} (1+4\beta\|t\|^2)^{1/2} = \frac{L_m}{(2\pi)^{m/2}} \sqrt{d_1 ... d_m} (1+4\beta\|t\|^2)^{1/2}.$$

Notice that if $\beta = 0$, the integrand is constant.

6 Systems of equations having a probability law invariant under isometries and translations

In this section we assume that $X_i : \mathbb{R}^m \to \mathbb{R}$, $i = 1, ...m$ are independent Gaussian centered random fields with covariance of the form

$$r^{X_i}(s,t) = \gamma_i(\|t-s\|^2), \quad (i=1,...m). \tag{22}$$

We will assume that γ_i is of class $\mathcal{C}^2$ and, with no loss of generality, that $\gamma_i(0) = 1$.

In what follows, V is a Borel subset of $\mathbb{R}^m$ with positive Lebesgue measure and the regularity property that its boundary has zero Lebesgue measure. For the computation of the expectation of the number of roots of the system of equations

$$X_i(t) = 0, \quad (i=1,...m)$$

that belong to the set V, we may use the same procedure as in Theorem 4, obtaining:

$$\mathrm{E}\big(N^X(V)\big) = (2\pi)^{-m/2}\mathrm{E}\big(|\det(X'(0))|\big)\lambda_m(V) \tag{23}$$

where we have used that the law of the random field $\{X(t) : t \in \mathbb{R}^m\}$ is invariant under translation and that $X(t)$ and $X'(t)$ are independent. One easily computes, for $i, \alpha, \beta = 1, ..., m$

$$\mathrm{E}\left(\frac{\partial X_i}{\partial t_\alpha}(0)\frac{\partial X_i}{\partial t_\beta}(0)\right) = \left.\frac{\partial^2 r^{X_i}}{\partial s_\alpha \partial t_\beta}\right|_{t=s} = -2\gamma_i'(0)\delta_{\alpha\beta},$$

which implies, again using the same method as in the proof of Theorem 4 :

$$\mathrm{E}\big(|\det(X'(0))|\big) = 2^{m/2}L_m\prod_{i=1}^m |\gamma_i'(0)|^{1/2}$$

and replacing in (23)

$$\mathrm{E}\big(N^X(V)\big) = \pi^{-m/2}\left[\prod_{i=1}^m |\gamma_i'(0)|^{1/2}\right]L_m\lambda_m(V). \tag{24}$$

Our next task is to give a formula for the variance of $N^X(V)$ and use it to prove that -under certain additional conditions - the variance of

$$n^X(V) = \frac{N^X(V)}{\mathrm{E}\big(N^X(V)\big)}$$

- which has obviously mean value equal to 1- grows exponentially when the dimension m tends to infinity. In other words, one should expect to have large fluctuations of $n^X(V)$ around its mean for systems having large m. Moreover

this exponential growth implies that an exact expression of the variance would not improve bounds on the probabilities of the kind $\mathrm{P}\{N^X(V) > A\}$ that follow from (24) and the Markov inequality.

Our additional requirements are the following:

1) All the γ_i coincide : $r^{X_i}(s,t) = r(s,t) = \gamma_i(\|t-s\|^2) = \gamma(\|t-s\|^2)$, $i = 1, ..., m$,

2) the function γ is such that $(s,t) \rightsquigarrow \gamma(\|t-s\|^2)$ is a covariance for all dimensions m.

It is well known [8] that γ satisfies 2) and $\gamma(0) = 1$ if and only if there exists a probability measure G on $[0, +\infty)$ such that

$$\gamma(x) = \int_0^{+\infty} e^{-xw} G(dw) \quad \text{for all } x \geq 0. \tag{25}$$

Theorem 5 *Let $r^{X_i}(s,t) = \gamma(\|t-s\|^2)$ for $i = 1, ..., m$ where γ is of the form (25). We assume further that*

1. *G is not concentrated at a single point and*

$$\int_0^{+\infty} x^2 G(dx) < \infty.$$

2. *$\{V_m\}_{m=1,2...}$ is a sequence of Borel sets, $V_m \subset \mathbb{R}^m$, $\lambda_m(\partial V_m) = 0$ and there exist two positive constants δ, Δ such that for each m, V_m contains a ball with radius δ and is contained in a ball with radius Δ.*

Then,

$$\mathrm{Var}\big(n^X(V_m)\big) \to +\infty, \tag{26}$$

exponentially fast as $m \to +\infty$.

Proof: To compute the variance of $N^X(V)$ note first that

$$\begin{aligned}\mathrm{Var}\left(N^X(V)\right) \\ = \mathrm{E}\Big(N^X(V)\big(N^X(V)-1\big)\Big) + \mathrm{E}\big(N^X(V)\big) - \big[\mathrm{E}\big(N^X(V)\big)\big]^2,\end{aligned} \tag{27}$$

so that to prove (26), it suffices to show that

$$\frac{\mathrm{E}\Big(N^X(V)\big(N^X(V)-1\big)\Big)}{\big[\mathrm{E}\big(N^X(V)\big)\big]^2}\to+\infty \tag{28}$$

exponentially fast as $m\to+\infty$. The denominator in (28) is given by formula (24). For the numerator, we can apply Theorem 2 with $k=2$ to obtain:

$$\begin{aligned}&\mathrm{E}\big(N^X(V)\,\big(N^X(V)-1\big)\,\big)\\&=\iint_{V\times V}\mathrm{E}\big(\,|\det(X'(s))\det(X'(t))|\,/X(s)=X(t)=0\big)\,p_{X(s),X(t)}(0,0)\,ds\,dt,\end{aligned} \tag{29}$$

where $p_{X(s),X(t)}(.,.)$ denotes the joint density of the random vectors $X(s),X(t)$.

Next we compute the ingredients of the integrand in (29). Because of invariance under translations, the integrand is a function of $\tau=t-s$. We denote with $\tau_1,...,\tau_m$ the coordinates of τ.

The Gaussian density is immediate:

$$p_{X(s),X(t)}(0,0)=\frac{1}{(2\pi)^m}\frac{1}{[1-\gamma^2(\|\tau\|^2)]^{m/2}}. \tag{30}$$

Let us turn to the conditional expectation in (29). We put

$$\mathrm{E}\big(\,|\det(X'(s))\det(X'(t))|\,/X(s)=X(t)=0\big)=\mathrm{E}\big(\,\big|\det(A^s)\det(A^t)\big|\,\big),$$

where $A^s=((A^s_{i\alpha})),A^t=((A^t_{i\alpha}))$ are $m\times m$ random matrices having as joint - Gaussian - distribution the conditional distribution of the pair $X'(s),X'(t)$ given that $X(s)=X(t)=0$. So, to describe this joint distribution we must compute the conditional covariances of the elements of the matrices $X'(s)$ and $X'(t)$ given the condition $\mathcal{C}:\{X(s)=X(t)=0\}$. This is easily done using standard regression formulae:

$$\mathrm{E}\left(\frac{\partial X_i}{\partial s_\alpha}(s)\frac{\partial X_i}{\partial s_\beta}(s)/\mathcal{C}\right)=\frac{\partial^2 r}{\partial s_\alpha\partial t_\beta}\bigg|_{t=s}-\frac{1}{1-(r(s,t))^2}\frac{\partial r}{\partial s_\alpha}(s,t)\frac{\partial r}{\partial s_\beta}(s,t)$$

$$\mathrm{E}\left(\frac{\partial X_i}{\partial s_\alpha}(s)\frac{\partial X_i}{\partial t_\beta}(t)/\mathcal{C}\right)=\frac{\partial^2 r}{\partial s_\alpha\partial t_\beta}(s,t)+\frac{1}{1-(r(s,t))^2}\frac{\partial r}{\partial s_\alpha}(s,t)\frac{\partial r}{\partial t_\beta}(s,t)r(s,t).$$

Replacing in our case, we obtain

$$\mathrm{E}\big(A^s_{i\alpha}A^s_{i\beta}\big) = \mathrm{E}\big(A^t_{i\alpha}A^t_{i\beta}\big) = -2\gamma'(0)\delta_{\alpha\beta} - 4\frac{\gamma'^2\tau_\alpha\tau_\beta}{1-\gamma^2}, \tag{31}$$

$$\mathrm{E}\big(A^s_{i\alpha}A^t_{i\beta}\big) = -4\gamma''\tau_\alpha\tau_\beta - 2\gamma'\delta_{\alpha\beta} - 4\frac{\gamma\gamma'^2\tau_\alpha\tau_\beta}{1-\gamma^2}, \tag{32}$$

and for every $i \neq j$:

$$\mathrm{E}\big(A^s_{i\alpha}A^s_{j\beta}\big) = \mathrm{E}\big(A^t_{i\alpha}A^t_{j\beta}\big) = \mathrm{E}\big(A^s_{i\alpha}A^t_{j\beta}\big) = 0,$$

where $\gamma = \gamma(\|\tau^2\|)$, $\gamma' = \gamma'(\|\tau^2\|)$, $\gamma'' = \gamma''(\|\tau^2\|)$.

Take now an orthonormal basis of $\mathbb{R}^m$ having the unit vector $\frac{\tau}{\|\tau\|}$ as first element. Then the variance $(2m)\times(2m)$ matrix of the pair A^s_i, A^t_i - the $i-$th rows of A^s and A^t respectively - takes the following form:

$$T = \left[\begin{array}{cccc|cccc} U_0 & \cdots & . & . & U_1 & \cdots & . & . \\ . & V_0 & \cdots & . & . & V_1 & \cdots & . \\ . & . & \ddots & . & . & . & \ddots & . \\ . & . & \cdots & V_0 & . & . & \cdots & V_1 \\ \hline U_1 & \cdots & . & . & U_0 & \cdots & . & . \\ . & V_1 & \cdots & . & . & V_0 & \cdots & . \\ . & . & \ddots & . & . & . & \ddots & . \\ . & . & \cdots & V_1 & . & . & \cdots & V_0 \end{array}\right],$$

where

$$\begin{aligned} U_0 &= U_0(\|\tau\|^2) = -2\gamma'(0) - 4\frac{\gamma'^2\,\|\tau\|^2}{1-\gamma^2}\ ; \\ V_0 &= -2\gamma'(0)\ ; \\ U_1 &= U_1(\|\tau\|^2) = -4\gamma''\,\|\tau\|^2 - 2\gamma' - 4\frac{\gamma\gamma'^2\|\tau\|^2}{1-\gamma^2}; \\ V_1 &= V_1(\|\tau\|^2) = -2\gamma'; \end{aligned}$$

and there are zeros outside the diagonals of each one of the four blocks. Let us perform a second regression of $A^t_{i\alpha}$ on $A^s_{i\alpha}$, that is, write the orthogonal decompositions

$$A^t_{i\alpha} = B^{t,s}_{i\alpha} + C_\alpha A^s_{i\alpha} \quad (i,\alpha = 1,m),$$

where $B_{i\alpha}^{t,s}$ is centered Gaussian independent of the matrix A^s, and

$$\begin{aligned} \text{For } \alpha = 1, \quad C_1 &= \frac{U_1}{U_0}, \quad \mathrm{Var}(B_{i1}^{t,s}) = U_0\big(1 - \frac{U_1^2}{U_0^2}\big); \\ \text{For } \alpha > 1, \quad C_\alpha &= \frac{V_1}{V_0}, \quad \mathrm{Var}(B_{i\alpha}^{t,s}) = V_0\big(1 - \frac{V_1^2}{V_0^2}\big). \end{aligned}$$

Conditioning we have :

$$\mathrm{E}\big(|\det(A^s)||\det(A^t)|\big) = \mathrm{E}\big[|\det(A^s)|\mathrm{E}\big(|\det((B_{i\alpha}^{t,s} + C_\alpha A_{i\alpha}^s)_{i,\alpha=1,..,m})|/A^s\big)\big]$$

with obvious notations. For the inner conditional expectation, we can proceed in the same way as we did in the proof of Theorem 4 to compute the determinant, obtaining a product of expectations of Euclidean norms of non-centered Gaussian vectors in $\mathbb{R}^k$ for $k = 1, ..., m$. Now we use the well-known inequality

$$\mathrm{E}\big(\|\xi + v\|\big) \geq \mathrm{E}\big(\|\xi\|\big)$$

valid for ξ standard Gaussian in $\mathbb{R}^k$ and v any vector in $\mathbb{R}^k$, and it follows that

$$\mathrm{E}\big(|\det(A^s)||\det(A^t)|\big) \geq \mathrm{E}\big(|\det(A^s)|\big)\mathrm{E}\big(|\det(B^{t,s})|\big).$$

Since the elements of A^s (resp. $B^{t,s}$) are independent, centered Gaussian with known variance, we obtain:

$$\mathrm{E}\,\big|\det(A^s)\det(A^t)\big| \geq U_0 V_0^{m-1}\big(1 - \frac{U_1^2}{U_0^2}\big)^{1/2}\big(1 - \frac{V_1^2}{V_0^2}\big)^{(m-1)/2} L_m^2.$$

Going back to (28) and on account of (24) and (29) we have

$$\frac{\mathrm{E}\big(N^X(V)\,\big(N^X(V) - 1\big)\,\big)}{\mathrm{E}\big(N^X(V)\big)^2} \geq \big(\lambda_m(V)\big)^{-2} \iint_{V\times V} dsdt \left[\frac{1 - V_1^2 V_0^{-2}}{1 - \gamma^2}\right]^{m/2} H(\|\tau\|^2). \tag{33}$$

Let us put $V = V_m$ in (33) and study the integrand in the right hand member. The function

$$H(x) = \left(\frac{U_0^2(x) - U_1^2(x)}{V_0^2 - V_1^2(x)}\right)^{1/2}$$

is continuous for $x > 0$. Let us show that it does not vanish if $x > 0$.

It is clear that $U_1^2 \leq U_0^2$ on applying the Cauchy-Schwarz inequality to the pair of variables A_{i1}^s, A_{i1}^t. The equality holds if and only if the variables

A^s_{i1}, A^t_{i1} are linearly dependent. This would imply that the distribution - in $\mathbb{R}^4$ - of the random vector

$$\zeta := \big(X(s), X(t), \partial_1 X(s), \partial_1 X(t)\big)$$

would degenerate for $s \neq t$ (we have denoted ∂_1 differentiation with respect to the first coordinate). We will show that this is not possible. Notice first that for each $w > 0$, the function

$$(s,t) \rightsquigarrow e^{-\|t-s\|^2 w}$$

is positive definite, hence the covariance of a centered Gaussian stationary field defined on $\mathbb{R}^m$, say $\{Z^w(t) : t \in \mathbb{R}^m\}$ whose spectral measure has the non-vanishing density:

$$f^w(x) = (2\pi)^{-m/2}(2w)^{-m/2} \exp\Big(-\frac{\|x\|^2}{4w}\Big) \quad (x \in \mathbb{R}^m).$$

The field $\{Z^w(t) : t \in \mathbb{R}^m\}$ satisfies the conditions of Proposition 3.1 of Azaïs & Wschebor [1] so that the distribution of the 4-tuple

$$\zeta^w := \big(Z^w(s), Z^w(t), \partial_1 Z^w(s), \partial_1 Z^w(t)\big)$$

does not degenerate for $s \neq t$. On account of (25) we have,

$$\mathrm{Var}(\zeta) = \int_0^{+\infty} \mathrm{Var}(\zeta^w) G(dw),$$

where integration of the matrix is integration term by term. This implies that the distribution of ζ does not degenerate for $s \neq t$ and that $H(x) > 0$ for $x > 0$.

We now show that for $\tau \neq 0$:

$$\frac{1 - V_1^2(\|\tau\|^2)V_0^{-2}}{1 - \gamma^2(\|\tau\|^2)} > 1$$

which is equivalent to

$$-\gamma'(x) < -\gamma'(0)\gamma(x) \quad , \quad \forall x > 0. \tag{34}$$

The left-hand member of (34) can be written as

$$-\gamma'(x) = \frac{1}{2} \iint_0^{+\infty} \big(w_1 \exp(-x w_1) + w_2 \exp(-x w_2)\big) G(dw_1) G(dw_2)$$

and the right-hand member

$$-\gamma'(0)\gamma(x) = \frac{1}{2}\iint_0^{+\infty} \big(w_1 \exp(-xw_2) + w_2 \exp(-xw_1)\big) G(dw_1)G(dw_2),$$

so that

$$-\gamma'(0)\gamma(x)+\gamma'(x) = \frac{1}{2}\iint_0^{+\infty} (w_2-w_1)\big(\exp(-xw_1)-\exp(-xw_2)\big) G(dw_1)G(dw_2),$$

which is ≥ 0 and is equal to zero only if G is concentrated at a point, which is not the case. This proves (34). Now, using the hypotheses on the inner and outer diameter of V_m, the result follows by a compactness argument. $\square$.

Remark: On studying the behaviour of the function $H(x)$ as well as the ratio

$$\frac{1 - V_1^2(x)V_0^{-2}}{1 - \gamma^2(x)}$$

at zero one can show that the result holds true if we let the radius δ of the ball contained in V_m tend to zero not too fast as $m \to +\infty$.

Similarly, one can let Δ tend to $+\infty$ in a controlled way and use the same calculations to get asymptotic lower bounds for the variance as $m \to +\infty$.

6.1 Acknowledgments

This work was supported by ECOS action U03E01. The authors thank two anonymous referees for their remarks that have contributed to improve the final version and for drawing our attention to the paper by Kostlan [7]

References

[1] J-M. Azaïs and M. Wschebor. On the distribution of the maximum of a gaussian field with d parameters. *Ann. Appl. Probability, to appear*, 2004. see also preprint http://www.lsp.ups-tlse.fr/Azais/publi/ds1.pdf.

[2] A. T. Bharucha-Reid and M. Sambandham. *Random polynomials*. Probability and Mathematical Statistics. Academic Press Inc., Orlando, FL, 1986.

[3] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.

[4] G. Box and J. Hunter. Multi-factor experimental designs for exploring response surfaces. *Ann. Math. Stat.*, 28:195–241, 1957.

[5] A. Edelman and E. Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc. (N.S.)*, 32(1):1–37, 1995.

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

[7] E. Kostlan. On the expected number of real roots of a system of random polynomial equations. In *Foundations of computational mathematics (Hong Kong, 2000)*, pages 149–188. World Sci. Publishing, River Edge, NJ, 2002.

[8] I. J. Schoenberg. Metric spaces and completely monotone functions. *Ann. of Math. (2)*, 39(4):811–841, 1938.

[9] M. Shub and S. Smale. Complexity of Bezout's theorem. II. Volumes and probabilities. In *Computational algebraic geometry (Nice, 1992)*, volume 109 of *Progr. Math.*, pages 267–285. Birkhäuser Boston, Boston, MA, 1993.

[10] M. Spivak. *A comprehensive introduction to differential geometry. Vol. V*. Publish or Perish Inc., Wilmington, Del., second edition, 1979.