On the Kostlan-Shub-Smale model for random polynomial systems. Variance of the number of roots.

Mario Wschebor
Centro de Matemática. Facultad de Ciencias. Universidad de la República.
Calle Iguá 4225. 11400. Montevideo. Uruguay.
Tel: (5982)5252522. Fax: (5982)5220653.
E mail: wschebor@cmat.edu.uy

February 16, 2005

Abstract

We consider a random polynomial system with m equations and m real unknowns. Assume all equations have the same degree d and the law on the coefficients satisfies the Kostlan-Shub-Smale hypotheses. It is known that $E(N^X) = d^{m/2}$ where N^X denotes the number of roots of the system. Under the condition that d does not grow very fast, we prove that $\limsup_{m\to+\infty} Var(\frac{N^X}{d^{m/2}}) \leq 1$. Moreover, if $d \geq 3$ then $Var(\frac{N^X}{d^{m/2}}) \to 0$ as $m \to +\infty$, which implies $\frac{N^X}{d^{m/2}} \to 1$ in probability.

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

1 Introduction

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

We use the notation

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

where $\mathbf{j} := (j_1, ..., j_m)$ is a multi-index of non-negative integers, $|\mathbf{j}| := j_1 + ... + j_m$, $\mathbf{j}! := j_1!...j_m!$, $t^{\mathbf{j}} := t_1^{j_1}....t_m^{j_m}$, $a_{\mathbf{j}}^{(i)} := a_{j_1...,j_m}^{(i)}$. $\langle ., . \rangle$ and $\|.\|$ denote respectively the usual scalar product and Euclidean norm in $\mathcal{R}^m$. A^T is the transposed matrix of A.

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 $\mathcal{R}^m$, of the system of equations

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

We denote $N^X = N^X(\mathcal{R}^m)$.

Suppose that the coefficients of the polynomials are chosen at random with a given law and we want to study the probability distribution of $N^X(V)$. Generally speaking, little is known on this distribution, even for simple choices of the law on the coefficients. In 1992 Shub and Smale [9] (see also [3] for related problems) proved that if the $a_{\mathbf{j}}^{(i)}$ are centered independent Gaussian random variables, and their variances satisfy

$$Var\left(a_{\mathbf{j}}^{(i)}\right) = \binom{d_i}{j_1.....j_m} = \frac{d_i!}{\mathbf{j}!(d_i - |\mathbf{j}|)!},$$

then, the expectation of the number of roots is:

$$E\left(N^X\right) = \sqrt{D}, \tag{3}$$

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

Some extensions to other distributions of the coefficients can be found in the papers by Edelman and Kostlan [4], Kostlan [7] and Malajovich and Rojas [8], as well as in Azaïs and Wschebor [2], where a quite different proof of (3) has been given.

In what follows we will only consider random polynomial systems satisfying the Shub-Smale hypotheses such that the degrees d_i are all the same, say $d_i = d$ $(i = 1, ...m)$ and $d \geq 2$ (in which case Kostlan had earlier proved formula (3), see [6]).

Let us consider the normalized number of roots

$$n^X = \frac{N^X}{\sqrt{D}}$$

which obviously verifies $E(n^X) = 1$. Our main purpose is to study the asymptotic behaviour of the variance of n^X when the number m of unknowns and equations tends to infinity. Notice that the common degree d may vary with m.

Under the additional condition that d remains bounded as m grows, we prove that $\limsup_{m\to+\infty} Var(n^X) \leq 1$.

More interesting is that if moreover $d \geq 3$, then $\lim_{m\to+\infty} Var(n^X) = 0$, which obviously implies that $n^X \to 1$ in probability, that is, the random variable N^X and its expectation $\sqrt{D} = d^{m/2}$ are equivalent in this sense, as $m \to +\infty$. In other words, for large m the Kostlan-Shub-Smale expectation $d^{m/2}$ is the first order statistical approximation of the random variable N^X. Unfortunately, the proof does not work for quadratic systems and in this case the precise asymptotic behaviour of $Var(n^X)$ remains an open problem.

Essentially the same results hold true - and the proof below works with minor changes - if we allow d tend to infinity not too fast, more precisely, if $d \leq L_1 \exp(L_2\ m^\beta)$ for some $\beta < 1/3$ and positive constants L_1, L_2.

In a certain sense these results are opposite to the behaviour of systems having a probability law invariant under isometries and translations of $\mathcal{R}^m$ (which of course do not include polynomial systems, see [2], Section 6) in which the variance of the normalized number of roots lying in a set tends to infinity at a geometric rate.

Our main tool here are the so-called Rice formulae, which allow to express the moments of the number of roots of a system of random equations by means of certain integrals. Let us give a brief description of Rice formulae.

Let V be a measurable subset of $\mathcal{R}^m$ and $Z : V \to \mathcal{R}^m$ a random field defined on a probability space $(\Omega, \mathcal{A}, P)$.

Under certain assumptions on the probability law of Z and on its paths (that is, the functions $t \rightsquigarrow Z(t)$ defined for fixed $\omega \in \Omega$) one can prove that:

$$E\left(N^Z(V)\right) = \int_V E\left(|\det(Z'(t))|/Z(t) = 0\right)\ p_{Z(t)}(0)dt. \tag{4}$$

where for each $t \in V$, $p_{Z(t)}(x), x \in \mathcal{R}^m$ denotes the density of the probability distribution of the $\mathcal{R}^m$-valued random vector $Z(t)$, $Z'(t)$ is the derivative considered as a linear transformation of $\mathcal{R}^m$ into itself and the function $E(\xi/\eta = x)$ denotes the conditional expectation of the random variable ξ given the value of the random variable η.

With some additional conditions, if k is a positive integer, one also has a similar formula for the k-th factorial moment of $N^Z(V)$:

$$\begin{aligned} & E\left[N^Z(V)\left(N^Z(V)-1\right)...\left(N^Z(V)-k+1\right)\right] \qquad (5) \\ = & \int_{V^k} E\left(\prod_{j=1}^{k} |\det\left(Z'(t_j)\right)|/Z(t_1) = ... = Z(t_k) = 0\right) .p_{Z(t_1),...,Z(t_k)}(0,...,0)\ dt_1...dt_k \end{aligned}$$

where $p_{Z(t_1),...,Z(t_k)}(x_1, ..., x_k)$ denotes the joint density of the random vectors $Z(t_1), ..., Z(t_k)$.

We call (4) and (5) the "Rice formulae". In [1] one can find a proof along with some related subjects.

The main source of difficulties when applying (4) and (5) is the conditional expectation in the integrand. However, if Z is a Gaussian process - this will be our case in the present paper - the situation becomes considerably simpler, since one can get rid of the conditional expectation by using Gaussian regression, a familiar tool in Statistics (see for example [5], Ch. III). We state this as the next (very well known) proposition.

Proposition 1 *Let X_1, X_2 be random vectors in $\mathcal{R}^{d_1}, \mathcal{R}^{d_2}$ respectively.*

We assume that the pair (X_1, X_2) has a centered Gaussian distribution in $\mathcal{R}^{d_1+d_2}$ having covariances $\Sigma_{11} = E(X_1X_1^T)$, $\Sigma_{22} = E(X_2X_2^T)$, $\Sigma_{12} = E(X_1X_2^T)$ and that Σ_{22} is non-singular.

Let $g : \mathcal{R}^{d_1} \to \mathcal{R}$ be continuous and polynomially bounded, i.e. $|g(x)| \leq C\left(1 + \|x\|^M\right)$ for some positive constants C, M and any $x \in \mathcal{R}^{d_1}$.

Then, for each $x_2 \in \mathcal{R}^{d_2}$:

$$E\left(g(X_1)/X_2 = x_2\right) = E(g(Z + Ax_2)) \tag{6}$$

where A is the $d_1 \times d_2$ matrix $A = \Sigma_{12}\Sigma_{22}^{-1}$ and Z is a centered Gaussian random vector in $\mathcal{R}^{d_1}$ having covariance $E\left(ZZ^T\right) = \Sigma_{11} - \Sigma_{12}\Sigma_{22}^{-1}\Sigma_{12}^T$.

The proof of (6) is as follows: put $Z = X_1 - AX_2$ and choose A so that $E\left(ZX_2^T\right) = 0$, which gives $A = \Sigma_{12}\Sigma_{22}^{-1}$. Since the distribution of (Z, X_2) is Gaussian and $E\left(ZX_2^T\right) = 0$, it follows that the random vectors Z and X_2 are independent. The computation of $E\left(ZZ^T\right)$ is straightforward.

2 Main result

Theorem 2 *Let the random polynomial system (2) satisfy the Shub-Smale hypotheses, with $d_i = d$ $(i = 1, ...m)$ and $d \geq 2$.*

We assume that $d \leq d_0 < \infty$, where d_0 is some constant (independent of m). Then,

a) $\limsup_{m\to+\infty} Var(n^X) \leq 1$.

b) Under the additional hypothesis that $d \geq 3$, one has $\lim_{m\to+\infty} Var(n^X) = 0$.

Proof. We divide the proof into several steps.

Step 1. Notice that

$$\begin{aligned} Var\left(n^X\right) &= \frac{1}{D} Var\left(N^X\right) \\ &= \frac{1}{D}\left\{E\left[N^X\left(N^X - 1\right)\right] + E\left(N^X\right) - \left(E\left(N^X\right)\right)^2\right\} \\ &= \frac{1}{D}E\left[N^X\left(N^X - 1\right)\right] + \frac{1}{\sqrt{D}} - 1 \end{aligned}$$

so that it suffices to prove:

$$\lim \sup_{m\to+\infty} \frac{1}{D}E\left[N^X\left(N^X - 1\right)\right] \leq 2. \tag{7}$$

to show $a)$ in the statement of the Theorem and

$$\lim \sup_{m\to+\infty} \frac{1}{D}E\left[N^X\left(N^X - 1\right)\right] \leq 1 \tag{8}$$

to get $b)$.

To compute the factorial moment of N^X in the left-hand side of (7) or (8) we use (5) with $k = 2$, that is:

$$\begin{aligned} & E\left[N^X\left(N^X - 1\right)\right] \qquad (9) \\ = & \iint_{\mathcal{R}^m\times\mathcal{R}^m} E\left[\left|\det(X'(s))\det(X'(t))\right|/X(s) = X(t) = 0\right]\ p_{X(s),X(t)}(0,0)\ ds\ dt, \end{aligned}$$

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

Step 2.

A direct computation using the Shub-Smale hypotheses, gives the covariance of the random processes X_i, that is:

$$r^{X_i}(s,t) = E\left[X_i(s)X_i(t)\right] = \left(1 + \langle s,t\rangle\right)^d \quad (s,t \in \mathcal{R}^m, i = 1,...,m). \tag{10}$$

Since the random processes X_i are independent, using the form of the centered Gaussian density, we obtain:

$$\begin{aligned} p_{X(s),X(t)}(0,0) &= \frac{1}{(2\pi)^m \Delta^{m/2}} \qquad (11) \\ &= \frac{1}{(2\pi)^m} \frac{1}{\left[\left(1+\|s\|^2\right)\left(1+\|t\|^2\right)\right]^{\frac{m}{2}d}} \frac{1}{(1-\rho^{2d})^{m/2}} \end{aligned}$$

with the notations

$$\rho = \rho(s,t) = \frac{1+\langle s,t\rangle}{\left(1+\|s\|^2\right)^{1/2}\left(1+\|t\|^2\right)^{1/2}}$$

$$\begin{aligned} \Delta &= \Delta(s,t) = \left(1+\|s\|^2\right)^d \left(1+\|t\|^2\right)^d - \left[1+\langle s,t\rangle\right]^{2d} \\ &= \left(1+\|s\|^2\right)^d \left(1+\|t\|^2\right)^d (1-\rho^{2d}). \end{aligned}$$

Step 3. Let us now turn to the conditional expectation in the right-hand side of (9).

Let us put

$$E\left(\left|\det(X'(s))\det(X'(t))\right| / X(s) = X(t) = 0\right) = E\left(\left|\det(A^s)\det(A^t)\right|\right),$$

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 $X(s) = X(t) = 0$. (Notice that the probability distributions of A^s and A^t depend both on s and on t).

We use the regression formulae (40),(41),(42) in the auxiliary Proposition 3 below, with X_i instead of ξ. An elementary computation gives the following covariances:

$$E\left(A^s_{i\alpha}A^s_{j\beta}\right) = E\left(A^s_{i\alpha}A^t_{j\beta}\right) = E\left(A^t_{i\alpha}A^t_{j\beta}\right) = 0 \text{ if } \quad i \neq j \tag{12}$$

$$E\left(A^s_{i\alpha}A^s_{i\beta}\right) = d\left(1+\|s\|^2\right)^{d-1}\left[\delta_{\alpha\beta} - \overline{s}_\alpha\overline{s}_\beta - d\frac{\rho^{2(d-1)}}{1-\rho^{2d}}\left(\rho\overline{s}_\alpha - \overline{t}_\alpha\right)\left(\rho\overline{s}_\beta - \overline{t}_\beta\right)\right] \tag{13}$$

where $\delta_{\alpha\beta}$ is the Kronecker symbol and $\bar{s}_\alpha = \frac{s_\alpha}{\left(1+\|s\|^2\right)^{1/2}}, \bar{t}_\alpha = \frac{t_\alpha}{\left(1+\|t\|^2\right)^{1/2}}$.

$$E\left(A^t_{i\alpha}A^t_{i\beta}\right) = d\left(1+\|t\|^2\right)^{d-1}\left[\delta_{\alpha\beta} - \bar{t}_\alpha\bar{t}_\beta - d\frac{\rho^{2(d-1)}}{1-\rho^{2d}}\left(\rho\bar{t}_\alpha - \bar{s}_\alpha\right)\left(\rho\bar{t}_\beta - \bar{s}_\beta\right)\right] \tag{14}$$

$$\begin{aligned} E\left(A^s_{i\alpha}A^t_{i\beta}\right) &= d\left(1+\|s\|^2\right)^{\frac{d-1}{2}}\left(1+\|t\|^2\right)^{\frac{d-1}{2}}. \\ &\quad .\left[\rho^{d-1}\delta_{\alpha\beta} - \rho^{d-2}\bar{t}_\alpha\bar{s}_\beta + d\frac{\rho^{d-2}}{1-\rho^{2d}}\left(\rho\bar{s}_\alpha - \bar{t}_\alpha\right)\left(\rho\bar{t}_\beta - \bar{s}_\beta\right)\right] \end{aligned} \tag{15}$$

Still, to simplify somewhat the expression of $E\left(|\det(A^s)\det(A^t)|\right)$ we put, for $i, \alpha = 1, ..., m$:

$$\begin{aligned} Y^s_{i\alpha} &= \frac{1}{\sqrt{d}}\frac{1}{\left(1+\|s\|^2\right)^{\frac{d-1}{2}}}A^s_{i\alpha} \\ Y^t_{i\alpha} &= \frac{1}{\sqrt{d}}\frac{1}{\left(1+\|t\|^2\right)^{\frac{d-1}{2}}}A^t_{i\alpha} \end{aligned}$$

and express - for each pair $s, t \in \mathcal{R}^m$, the random matrices whose determinants are to be computed, in an orthonormal basis of $\mathcal{R}^m$, say $\{v_1, v_2, ..., v_m\}$, such that $\{v_1, v_2\}$ generates the same subspace than $\{s, t\}$ (Notice that s and t are linearly independent in the integrand of (9), excepting for a negligible set of pairs (s, t)).

So, we may write

$$E\left(\left|\det(A^s)\det(A^t)\right|\right) = D\ E\left(\left|\det(Y^s)\det(Y^t)\right|\right)\left[\left(1+\|s\|^2\right)\left(1+\|t\|^2\right)\right]^{m\frac{d-1}{2}} \tag{16}$$

where the centered Gaussian matrices Y^s, Y^t satisfy the following covariance relations:

- $$E\left(Y^s_{i\alpha}Y^s_{j\beta}\right) = E\left(Y^s_{i\alpha}Y^t_{j\beta}\right) = E\left(Y^t_{i\alpha}Y^t_{j\beta}\right) = 0\ if\quad i \neq j \tag{17}$$

- if either α or β is ≥ 3, then:
$$E\left(Y^s_{i\alpha}Y^s_{i\beta}\right) = E\left(Y^t_{i\alpha}Y^t_{i\beta}\right) = \delta_{\alpha\beta}, \quad E\left(Y^s_{i\alpha}Y^t_{i\beta}\right) = \rho^{d-1}\delta_{\alpha\beta} \tag{18}$$

- if $\alpha, \beta = 1, 2$, then:
$$E\left(Y^s_{i\alpha}Y^s_{i\beta}\right) = \delta_{\alpha\beta} - \bar{s}_\alpha\bar{s}_\beta - d\frac{\rho^{2(d-1)}}{1-\rho^{2d}}\left(\rho\bar{s}_\alpha - \bar{t}_\alpha\right)\left(\rho\bar{s}_\beta - \bar{t}_\beta\right) \tag{19}$$
$$E\left(Y^t_{i\alpha}Y^t_{i\beta}\right) = \delta_{\alpha\beta} - \bar{t}_\alpha\bar{t}_\beta - d\frac{\rho^{2(d-1)}}{1-\rho^{2d}}\left(\rho\bar{t}_\alpha - \bar{s}_\alpha\right)\left(\rho\bar{t}_\beta - \bar{s}_\beta\right) \tag{20}$$

$$E\left(Y^s_{i\alpha}Y^t_{i\beta}\right) = \rho^{d-1}\delta_{\alpha\beta} - \rho^{d-2}\bar{t}_\alpha\bar{s}_\beta + d\frac{\rho^{d-2}}{1-\rho^{2d}}\left(\rho\bar{s}_\alpha - \bar{t}_\alpha\right)\left(\rho\bar{t}_\beta - \bar{s}_\beta\right) \quad (21)$$

Replacing in (9), on account of (11) and (16) we obtain:

$$E\left[N^X\left(N^X-1\right)\right] = \frac{D}{(2\pi)^m}\iint_{\mathcal{R}^m\times\mathcal{R}^m} \frac{E\left(\left|\det(Y^s)\det(Y^t)\right|\right)}{\left[\left(1+\|s\|^2\right)\left(1+\|t\|^2\right)\right]^{\frac{m}{2}}\left(1-\rho^{2d}\right)^{m/2}}\,ds\,dt \quad (22)$$

We break the integral in (22) into two terms, writing:

$$\frac{1}{D}E\left[N^X\left(N^X-1\right)\right] = \iint_{\rho^2>\frac{1}{m^\gamma}} \ldots \quad + \quad \iint_{\rho^2\leq\frac{1}{m^\gamma}} \ldots. \quad = I_1 + I_2 \quad (23)$$

where γ is a positive number to be chosen later on.

We will show in step 4 that $\lim_{m\to+\infty} I_1 = 0$. In step 5 we will prove that $\limsup_{m\to+\infty} I_2 \leq 2$ in all cases and $\limsup_{m\to+\infty} I_2 \leq 1$ under the additional hypothesis $d \geq 3$.

Step 4. Let us consider I_1 and assume s and t are points in $\mathcal{R}^m, s,t \neq 0$.
Using the definition of ρ given in Step 2, one can check the identity

$$1-\rho^2 = \frac{\|s-t\|^2 + \|s\|^2\|t\|^2\sin^2\varphi}{\left(1+\|s\|^2\right)\left(1+\|t\|^2\right)} \quad (24)$$

where φ is the angle formed by the vectors $\overrightarrow{Os}$ and $\overrightarrow{Ot}$ in $\mathcal{R}^m$.

Next, we write the Laplace expansion of $\det(Y^s)$ with respect to its first two columns, using the notation

$$\Delta^s_{ij} = \det\begin{pmatrix} Y^s_{i1} & Y^s_{i2} \\ Y^s_{j1} & Y^s_{j2}\end{pmatrix}$$

for $i<j$ and $\widetilde{\Delta^s}_{ij}$ for the $(m-2)\times(m-2)$- determinant that results from suppressing in Y^s columns 1 and 2 and rows i and j.

So, using the Cauchy-Schwartz inequality and the fact that for fixed i,j the random variables Δ^s_{ij} and $\widetilde{\Delta^s}_{ij}$ are independent, it follows that

$$\begin{aligned} E\left[\left(\det(Y^s)\right)^2\right] &\leq E\left[\left(\sum_{1\leq i<j\leq m}\left|\Delta^s_{ij}\right|\left|\widetilde{\Delta^s}_{ij}\right|\right)^2\right] \quad (25) \\ &\leq E\left[\sum_{1\leq i<j\leq m}\left(\Delta^s_{ij}\right)^2\left(\widetilde{\Delta^s}_{ij}\right)^2\right] = \sum_{1\leq i<j\leq m} E\left[\left(\Delta^s_{ij}\right)^2\right]E\left[\left(\widetilde{\Delta^s}_{ij}\right)^2\right] \end{aligned}$$

It is well-known and easy to prove that $E\left[\left(\widetilde{\Delta^s}_{ij}\right)^2\right] = (m-2)!$ since the elements of the corresponding random matrix are i.i.d. standard Gaussian. For the computation of $E\left[\left(\Delta_{ij}^s\right)^2\right]$ we must look at the covariance structure of the first two columns of Y^s. We have:

$$
\begin{aligned}
E\left[\left(\Delta_{ij}^s\right)^2\right] &= E\left[\left(Y_{i1}^s Y_{j2}^s - Y_{i2}^s Y_{j1}^s\right)^2\right] \\
&= E\left[\left(Y_{i1}^s\right)^2\right] E\left[\left(Y_{j2}^s\right)^2\right] + E\left[\left(Y_{i2}^s\right)^2\right] E\left[\left(Y_{j1}^s\right)^2\right] - 2E\left(Y_{i1}^s Y_{i2}^s\right) E\left(Y_{j1}^s Y_{j2}^s\right) \\
&= C_{11}^i C_{22}^j + C_{22}^i C_{11}^j - 2C_{12}^i C_{12}^j
\end{aligned}
$$

with the notation $C_{\alpha\beta}^i = E\left(Y_{i\alpha}^s Y_{i\beta}^s\right)$ $(\alpha, \beta = 1, 2; i = 1, ..., m)$.

Now use formula (19) to compute the $C_{\alpha\beta}^i$'s.

We obtain:

$$
\begin{aligned}
E\left[\left(\Delta_{ij}^s\right)^2\right] &= \frac{2}{1+\|s\|^2}\left[1 - d\frac{\rho^{2(d-1)}}{1-\rho^{2d}}\left(1-\rho^2\right)\right] \\
&= 2\frac{1-\rho^2}{1+\|s\|^2}\frac{1+2\rho^2+...+(d-1)\rho^{2(d-2)}}{1+\rho^2+....+\rho^{2(d-1)}} \leq 2\frac{1-\rho^2}{1+\|s\|^2}(d-1)
\end{aligned}
$$

Replacing in (25) we have:

$$
E\left[\left(\det(Y^s)\right)^2\right] \leq (d-1)\frac{1-\rho^2}{1+\|s\|^2}m!
$$

Using the same method for $E\left[\left(\det(Y^t)\right)^2\right]$ we obtain for I_1 the bound:

$$
\begin{aligned}
I_1 &\leq \frac{(d-1)m!}{(2\pi)^m}\iint_{\rho^2 > \frac{1}{m^\gamma}} \frac{1-\rho^2}{\left(1+\|s\|^2\right)^{\frac{m+1}{2}}\left(1+\|t\|^2\right)^{\frac{m+1}{2}}}\frac{1}{\left(1-\rho^4\right)^{\frac{m}{2}}}\,ds\,dt \\
&\leq \frac{(d-1)m!}{(2\pi)^m}\frac{1}{(1+\frac{1}{m^\gamma})^{\frac{m}{2}}}\iint_{\mathcal{R}^m\times\mathcal{R}^m}\frac{ds\,dt}{\left(1+\|s\|^2\right)^{\frac{m+1}{2}}\left(1+\|t\|^2\right)^{\frac{m+1}{2}}}\frac{1}{\left(1-\rho^2\right)^{\frac{m}{2}-1}} \\
&= \frac{(d-1)m!}{(2\pi)^m}\frac{1}{(1+\frac{1}{m^\gamma})^{\frac{m}{2}}}\iint_{\mathcal{R}^m\times\mathcal{R}^m}\frac{ds\,dt}{\left(1+\|s\|^2\right)^{\frac{3}{2}}\left(1+\|t\|^2\right)^{\frac{3}{2}}\left(\|s-t\|^2+\|s\|^2\|t\|^2\sin^2\varphi\right)^{\frac{m}{2}-1}}
\end{aligned}
$$

$$
\begin{aligned}
I_1 \leq\ & \frac{(d-1)m!}{(2\pi)^m}\frac{1}{(1+\frac{1}{m^\gamma})^{\frac{m}{2}}} \\
& \cdot\int_{\mathcal{R}^m}\frac{ds}{\left(1+\|s\|^2\right)^{\frac{3}{2}}}\int_{\mathcal{R}^m}\frac{dt}{\left(1+\|t\|^2\right)^{\frac{3}{2}}\left(\|s-t\|^2+\|s\|^2\|t\|^2\sin^2\varphi\right)^{\frac{m}{2}-1}}
\end{aligned} \tag{26}
$$

The inner integral in (26) depends only on $\|s\|$ so that it is enough to compute it for $s = (\|s\|, 0, ..., 0)$ in which case it can be written as:

$$
\int_{\mathcal{R}^m}\frac{dt_1..., dt_m}{\left(1+\|t\|^2\right)^{\frac{3}{2}}\left[\left(t_1-\|s\|\right)^2+t_2^2+...+t_m^2+\|s\|^2\left(t_2^2+...+t_m^2\right)\right]^{\frac{m}{2}-1}}
$$

$$= \int_{\mathcal{R}} dt_1 \sigma_{m-2} \int_0^{+\infty} \frac{u^{m-2} du}{(1+t_1^2+u^2)^{\frac{3}{2}} \left[(t_1 - \|s\|)^2 + u^2 \left(1+\|s\|^2\right) \right]^{\frac{m}{2}-1}} \tag{27}$$

where $\sigma_{m-1} = \frac{2\pi^{m/2}}{\Gamma(m/2)}$denotes the geometric measure of the sphere $\mathcal{S}^{m-1}$ embedded in $\mathcal{R}^m$. Making the change of variables $u\left(1+\|s\|^2\right)^{\frac{1}{2}} = |t_1 - \|s\|| \ y$, the inner integral in (27) becomes:

$$\frac{|t_1 - \|s\||}{\left(1+\|s\|^2\right)^{\frac{m}{2}-1}} \int_0^{+\infty} \frac{y^{m-2} \ dy}{\left[1+t_1^2+\frac{|t_1-\|s\||^2 y^2}{1+\|s\|^2}\right]^{\frac{3}{2}} (1+y^2)^{\frac{m}{2}-1}}$$

and replacing in (26) and (27) we get the bound:

$$\begin{aligned} I_1 \quad &\leq \quad C_m \int_0^{+\infty} \frac{v^{m-1}}{(1+v^2)^{\frac{m+2}{2}}} dv \int_{-\infty}^{+\infty} |t_1 - v| \, dt_1 \int_0^{+\infty} \frac{y^{m-2} \ dy}{\left[1+t_1^2+\frac{|t_1-v|^2 y^2}{1+v^2}\right]^{\frac{3}{2}} (1+y^2)^{\frac{m}{2}-1}} \\ &\leq \quad C_m \int_0^{+\infty} \frac{v^{m-1}}{(1+v^2)^{\frac{m+2}{2}}} dv \int_{-\infty}^{+\infty} \frac{dt_1}{1+t_1^2} \int_0^{+\infty} \frac{dw}{(1+w^2)^{\frac{3}{2}}} \end{aligned}$$

with

$$C_m = \frac{(d-1)m!}{(2\pi)^m} \frac{1}{(1+\frac{1}{m^\gamma})^{\frac{m}{2}}} \sigma_{m-1}\sigma_{m-2}$$

This shows that $\frac{I_1}{C_m}$ is bounded by a constant not depending on m.
Applying Stirling's formula, it follows that

$$I_1 \leq K_1 m^2 e^{-\frac{1}{2} \ m^{1-\gamma}} \tag{28}$$

for some positive constant K_1.

Step 5. Let us now turn to I_2, the second integral in (23).
We introduce the following additional notations:

- $Y^s_{\bullet j}$ (resp. $Y^t_{\bullet j}$) denotes the j's column of the matrix Y^s (resp. Y^t).
- V^s_j (resp V^t_j) $(j = 0, 1, ..., m-1)$ denotes the linear subspace of $\mathcal{R}^m$ generated by the set of random vectors $\left\{Y^s_{\bullet j+1}, ..., Y^s_{\bullet m}\right\}$ (resp. $\left\{Y^t_{\bullet j+1}, ..., Y^t_{\bullet m}\right\}$).
- δ denotes Euclidean distance in $\mathcal{R}^m$.
- π^s_j (resp. π^t_j) denotes the orthogonal projection in $\mathcal{R}^m$ onto $(V^s_j)^\perp$ (resp. $(V^t_j)^\perp$), the orthogonal complement of V^s_j (resp. V^t_j). Since almost surely V^s_2 and V^t_2 have dimension $m-2$, $(V^s_j)^\perp$ and $(V^t_j)^\perp$ have, almost surely, dimension 2.
- Take an orthonormal basis of $(V^s_2)^\perp$ (resp. $(V^t_j)^\perp$) , say (v^s_1, v^s_2) (resp. (v^t_1, v^t_2)), measurable with respect to $(Y^s_{\bullet 3}, ..., Y^s_{\bullet m})$ (resp. $(Y^t_{\bullet 3}, ..., Y^t_{\bullet m})$.

We will be using the fact that the sets of random vectors

$$\left\{Y^s_{\bullet 1}, Y^s_{\bullet 2}, Y^t_{\bullet 1}, Y^t_{\bullet 2}\right\}, \left\{Y^s_{\bullet 3}, ..., Y^s_{\bullet m}, Y^t_{\bullet 3}, ..., Y^t_{\bullet m}\right\}$$

are independent (c.f. (18)).

Then, we may write

$$|\det(Y^s)| = \left[\prod_{j=1}^{m-1} \delta(Y^s_{\bullet j}, V^s_j)\right] \|Y^s_{\bullet m}\|.$$

and

$$\begin{aligned} & E\left[|\det(Y^s)| \left|\det(Y^t)\right|\right] & (29) \\ = & E\left(E\left[|\det(Y^s)| \left|\det(Y^t)\right| / Y^s_{\bullet 3}, ..., Y^s_{\bullet m}, Y^t_{\bullet 3}, ..., Y^t_{\bullet m}\right]\right) \\ = & E\left(\left[\prod_{j=3}^{m-1} \left[\delta(Y^s_{\bullet j}, V^s_j)\delta(Y^t_{\bullet j}, V^t_j)\right]\right] \|Y^s_{\bullet m}\| \left\|Y^t_{\bullet m}\right\| \mathfrak{E}_{12}\right) \end{aligned}$$

where $\mathfrak{E}_{12}$ is the conditional expectation:

$$\mathfrak{E}_{12} = E_{slC}\left(\prod_{j=1}^{2} \left[\delta(Y^s_{\bullet j}, V^s_j)\delta(Y^t_{\bullet j}, V^t_j)\right]\right) \tag{30}$$

where E_{slC} means conditional expectation given $Y^s_{\bullet 3}, ..., Y^s_{\bullet m}, Y^t_{\bullet 3}, ..., Y^t_{\bullet m}$

Next we consider the asymptotic behaviour of $\mathfrak{E}_{12}$ as $m \to +\infty$ for those pairs (s,t) appearing in the integral I_2, that is, such that $\rho^2 \leq \frac{1}{m^\gamma}$.

Put

$$Z^s_{\bullet j} = \pi^s_2(Y^s_{\bullet j}),\ Z^t_{\bullet j} = \pi^t_2(Y^t_{\bullet j}) \quad j = 1, 2$$

so that

$$Z^s_{\bullet j} = \sum_{h=1}^{2} \left\langle Y^s_{\bullet j}, v^s_h\right\rangle\ v^s_h = \sum_{h=1}^{2} \lambda^s_{jh}\ v^s_h$$

and similarly replacing s by t.

Conditionally on $Y^s_{\bullet 3}, ..., Y^s_{\bullet m}, Y^t_{\bullet 3}, ..., Y^t_{\bullet m}$ the random variables $\lambda^s_{jh}, \lambda^t_{jh}$ $(j, h = 1, 2)$ have joint Gaussian centered distribution and the covariances are easily computed from (17), (19), (20), (21). We have:

$$\begin{aligned} E_{slC}\left(\lambda^s_{jh}\lambda^s_{j'h'}\right) &= E_{slC}\left(\sum_{i,i'=1}^{m} Y^s_{ij} v^s_{ih} Y^s_{i'j'} v^s_{i'h'}\right) & (31) \\ &= \sum_{i=1}^{m} E\left(Y^s_{ij} Y^s_{ij'}\right) v^s_{ih} v^s_{ih'} = E\left(Y^s_{ij} Y^s_{ij'}\right) \delta_{hh'} \end{aligned}$$

where the last equality follows from the fact that $E\left(Y^s_{ij} Y^s_{ij'}\right)$ does not depend on i (c.f. (19). In the same way:

$$E_{slC}\left(\lambda^t_{jh}\lambda^t_{j'h'}\right) = E\left(Y^t_{ij} Y^t_{ij'}\right) \delta_{hh'} \tag{32}$$

$$E_{slC}\left(\lambda_{jh}^{s}\lambda_{j'h'}^{t}\right)=E\left(Y_{ij}^{s}Y_{ij'}^{t}\right)\left\langle v_{h}^{s},v_{h'}^{t}\right\rangle \tag{33}$$

Notice that $\mathfrak{E}_{12}$ is the conditional expectation of the product of the areas of the random paralellograms - say Δ_s (resp. Δ_t) $\{\lambda_1 Z_{\bullet 1}^s+\lambda_2 Z_{\bullet 2}^s : 0\le\lambda_1,\lambda_2\le 1\}$ (resp. $\{\lambda_1 Z_{\bullet 1}^t+\lambda_2 Z_{\bullet 2}^t : 0\le\lambda_1,\lambda_2\le 1\}$) and

$$\Delta_s=\left|\det((\lambda_{ij}^s))\right|,\ \Delta_t=\left|\det((\lambda_{ij}^t))\right|$$

If $d\ge 3$ for all $i=1,...,m$, using the form of the covariances (19),(20),(21), one can show that Δ_s and Δ_t are asymptotically independent, and more precisely that

$$E_{slC}\left(\Delta_s\Delta_t\right)=E(\overline{\Delta}_s)E(\overline{\Delta}_t)+\zeta_m$$

where

- $|\zeta_m|\le z_m$ where $\{z_m\}$ is a numerical sequence, $\lim_{m\to+\infty}z_m=0$.
- $\overline{\Delta}_s$ is obtained in the same way as Δ_s replacing the 2×2 matrix $((\lambda_{jh}^s))$ by $((\overline{\lambda}_{jh}^s))$ having the covariance

$$E\left(\overline{\lambda}_{jh}^{s}\overline{\lambda}_{j'h'}^{s}\right)=\left(\delta_{jj'}-\overline{s}_j\overline{s}_{j'}\right)\delta_{hh'}\quad (j,h,j',h'=1,2) \tag{34}$$

  The invariance under isometries of the standard Gaussian distribution implies that

$$E(\overline{\Delta}_s)=\frac{1}{\left(1+\|s\|^2\right)^{1/2}}E\left(\|\eta_1\|\right)E\left(\|\eta_2\|\right)$$

  where we use η_k $(k=1,2,...)$ to denote a standard Gaussian variable in $\mathcal{R}^k$. (Notice that $E\left(\|\eta_1\|\right)=\sqrt{2/\pi},\ E\left(\|\eta_2\|\right)=\sqrt{\pi/2}$).
- $\overline{\Delta}_t$ has the same properties than $\overline{\Delta}_s$, mutatis mutandis.

  So,

$$\mathfrak{E}_{12}=\frac{1}{\left(1+\|s\|^2\right)^{1/2}\left(1+\|t\|^2\right)^{1/2}}\left[E\left(\|\eta_1\|\right)E\left(\|\eta_2\|\right)\right]^2+\overline{\zeta}_m. \tag{35}$$

  with $\left|\overline{\zeta}_m\right|\le\overline{z}_m$ where $\{\overline{z}_m\}$ is a numerical sequence, $\lim_{m\to+\infty}\overline{z}_m=0$.

The above calculation fails if $d=2$, as one can see in formula (21) since in this case $E\left(Y_{i\alpha}^sY_{i\beta}^t\right)$ does not tend to zero as $\rho\to 0$ and one can not assure asymptotic independence of Δ_s and Δ_t.

So, when d can take the value 2, we use the Cauchy-Schwartz inequality, and obtain the more rough bound:

$$\begin{aligned}\mathfrak{E}_{12}&\le\left[E_{slC}(\Delta_s^2)E_{slC}(\Delta_t^2)\right]^{1/2}\\&=\frac{2}{\left(1+\|s\|^2\right)^{1/2}\left(1+\|t\|^2\right)^{1/2}}\left[E\left(\|\eta_1\|\right)E\left(\|\eta_2\|\right)\right]^2+\zeta_m^*.\end{aligned} \tag{36}$$

where $|\zeta_m^*| \leq z_m^*$ and $\{z_m^*\}$ is a numerical sequence, $\lim_{m\to+\infty} z_m^* = 0$.

The last equality follows easily from (31), (32), (33).

Next we consider

$$E\left(\left[\prod_{j=3}^{m-1}\left[\delta(Y_{\bullet j}^s, V_j^s)\delta(Y_{\bullet j}^t, V_j^t)\right]\right]\|Y_{\bullet m}^s\|\left\|Y_{\bullet m}^t\right\|\right) \tag{37}$$

It will be useful in our computations below to denote $\|.\|_j$ ($j = 1, 2, ...$) the Euclidean norm in $\mathcal{R}^j$. When $j = m$, we simply put $\|.\| = \|.\|_m$ as we did until now.

We now use again Gaussian regression and the covariance formulae (18). This permits to write for $j = 3, ..., m$:

$$Y_{\bullet j}^t = Y_{\bullet j}^t - \rho^{d-1}Y_{\bullet j}^s + \rho^{d-1}Y_{\bullet j}^s = \left(1-\rho^{2(d-1)}\right)^{1/2}\left[\zeta_j + \frac{\rho^{d-1}}{\left(1-\rho^{2(d-1)}\right)^{1/2}}Y_{\bullet j}^s\right]$$

where the $2(m-2)$ random vectors $\zeta_3, Y_{\bullet 3}^s, ..., \zeta_m, Y_{\bullet m}^s$ are independent and each one of them has standard normal distribution in $\mathcal{R}^m$. Also ζ_j is independent of $(Y_{\bullet j+1}^t, ..., Y_{\bullet m}^t)$ for $j = 3, ..., m-1$.

In formula (37) we successively compute the conditional expectation given the random vectors $Y_{\bullet j+1}^s, ..., Y_{\bullet m}^s, Y_{\bullet j+1}^t, ..., Y_{\bullet m}^t$ for $j = 3, ..., m$.

Then, for $j \geq 3$:

$$\begin{aligned}
& E\left[\delta(Y_{\bullet j}^s, V_j^s)\delta(Y_{\bullet j}^t, V_j^t)/Y_{\bullet j+1}^s, ..., Y_{\bullet m}^s, Y_{\bullet j+1}^t, ..., Y_{\bullet m}^t\right] \qquad (38)\\
= \;& \left(1-\rho^{2(d-1)}\right)^{1/2} E\left[\left\|\pi_j^s(Y_{\bullet j}^s)\right\|\left\|\pi_j^t(\zeta_j) + \frac{\rho^{d-1}}{\left(1-\rho^{2(d-1)}\right)^{1/2}}\pi_j^t(Y_{\bullet j}^s)\right\|/Y_{\bullet j+1}^s, ..., Y_{\bullet m}^s, Y_{\bullet j+1}^t, ..., Y_{\bullet m}^t\right]\\
= \;& \left(1-\rho^{2(d-1)}\right)^{1/2} E\left[\|\xi\|_j\left\|\eta + \frac{\rho^{d-1}}{\left(1-\rho^{2(d-1)}\right)^{1/2}}\zeta\right\|_j\right]
\end{aligned}$$

where each one of the random vectors ξ, η, ζ has a standard normal distribution in $\mathcal{R}^j$ and η is independent of the pair (ξ, ζ).

So, we are led to study the functions $H_j : \mathcal{R} \to \mathcal{R}^+$

$$\begin{aligned}
H_j(a) &= E\left[\|\xi\|_j\,\|\eta + a\,\zeta\|_j\right] \qquad (39)\\
&= E\left(\|\xi\|_j\left[(\eta_1 + a\,\|\zeta\|_j)^2 + \eta_2^2 + ... + \eta_j^2\right]^{1/2}\right)
\end{aligned}$$

with $j \geq 3$,where $\eta = (\eta_1, \eta_2, ..., \eta_j)^T$. Note that we are using the invariance under isometries of the distribution of η. With the aim of simplying somewhat the reading of this proof, we have included at the end, in a separate proposition, the properties of H_j that we will use.

To bound (37), we use (38) and (43),(44), (45), (46) and the Taylor expansion at zero of the functions H_j.

We obtain:

$$E\left(\left[\prod_{j=3}^{m-1}\left[\delta(Y^s_{\bullet j},V^s_j)\delta(Y^t_{\bullet j},V^t_j)\right]\right]\|Y^s_{\bullet m}\|\left\|Y^t_{\bullet m}\right\|\right)$$

$$= \left(1-\rho^{2(d-1)}\right)^{\frac{m-2}{2}} H_3\left(\frac{\rho^{d-1}}{\left(1-\rho^{2(d-1)}\right)^{\frac{1}{2}}}\right).$$

$$.\prod_{j=4}^{m}\left\{\left[E(\|\xi\|_j)\right]^2\left[1+\frac{1}{2}\frac{H''(0)}{\left[E(\|\xi\|_j)\right]^2}\frac{\rho^{2(d-1)}}{1-\rho^{2(d-1)}}+\frac{1}{6}\frac{H'''(\tau)}{\left[E(\|\xi\|_j)\right]^2}\frac{\rho^{3(d-1)}}{\left[1-\rho^{2(d-1)}\right]^{\frac{3}{2}}}\right]\right\}$$

where τ denotes some intermediate value between 0 and $\frac{\rho^{d-1}}{\left(1-\rho^{2(d-1)}\right)^{1/2}}$.

For $\rho^2 \leq \frac{1}{m^\gamma}$ we obtain the inequalities:

$$E\left(\left[\prod_{j=3}^{m-1}\left[\delta(Y^s_{\bullet j},V^s_j)\delta(Y^t_{\bullet j},V^t_j)\right]\right]\|Y^s_{\bullet m}\|\left\|Y^t_{\bullet m}\right\|\right)$$

$$\leq H_3\left(\frac{\rho^{d-1}}{\left(1-\rho^{2(d-1)}\right)^{\frac{1}{2}}}\right).$$

$$.\exp\left[-\frac{m-2}{2}\rho^{2(d-1)}+\frac{1}{2}\sum_{j=3}^{m}\left(1+\frac{C_2}{j}\right)\frac{\rho^{2(d-1)}}{1-\rho^{2(d-1)}}+\frac{C_3}{6}\frac{\rho^{3(d-1)}}{\left[1-\rho^{2(d-1)}\right]^{3/2}}(m-2)\right]\prod_{j=3}^{m}\left[E(\|\xi\|_j)\right]^2$$

$$\leq \exp\left[C_2\frac{\log m}{m^\gamma}+C_4\frac{1}{m^{\frac{3\gamma}{2}-1}}\right]\prod_{j=3}^{m}\left[E(\|\xi\|_j)\right]^2$$

where C_4 is a universal constant.

Check the formula

$$\frac{\prod_{j=1}^m E(\|\eta_j\|)}{(2\pi)^{m/2}}\int_{\mathcal{R}^m}\frac{dt}{\left(1+\|t\|^2\right)^{\frac{m+1}{2}}}=1.$$

Finally, choosing γ so that $\frac{2}{3}<\gamma<1$ and taking again into account that $d\geq 2$ in the general case, using inequality (36) and replacing in (29) we obtain the bound $\limsup_{m\to+\infty} I_2 \leq 2$ which together with (28) shows part a) in the statement of the Theorem. When $d\geq 3$ we use (35) and obtain part b).

Proposition 3 *If $\xi:\mathcal{R}^m\to\mathcal{R}$ is a centered Gaussian random process with a regular covariance $r(s,t)=E\left(\xi(s)\xi(t)\right)$ and the 2-dimensional distribution of $(\xi(s),\xi(t))$ does not degenerate, then for $\alpha,\beta=1,...,m$ we have:*

$$E\left(\partial_\alpha\xi(s)\partial_\beta\xi(s)/\xi(s)=\xi(t)=0\right)=\frac{\partial^2 r}{\partial s_\alpha\partial t_\beta}(s,s)-C^{s,t}_\alpha\frac{\partial r}{\partial s_\beta}(s,s)-D^{s,t}_\alpha\frac{\partial r}{\partial s_\beta}(s,t) \tag{40}$$

$$E\left(\partial_\alpha \xi(t)\partial_\beta \xi(t)/\xi(s)=\xi(t)=0\right)=\frac{\partial^2 r}{\partial t_\alpha \partial s_\beta}(t,t)-C_\alpha^{t,s}\frac{\partial r}{\partial t_\beta}(t,t)-D_\alpha^{t,s}\frac{\partial r}{\partial t_\beta}(t,s) \tag{41}$$

$$E\left(\partial_\alpha \xi(s)\partial_\beta \xi(t)/\xi(s)=\xi(t)=0\right)=\frac{\partial^2 r}{\partial s_\alpha \partial t_\beta}(s,t)-C_\alpha^{t,s}\frac{\partial r}{\partial t_\beta}(s,t)-D_\alpha^{t,s}\frac{\partial r}{\partial t_\beta}(t,t) \tag{42}$$

In these formulae, $\partial_\alpha \xi(s)$ denotes the first partial derivative of ξ with respect to the α-coordinate of the argument, $\frac{\partial r}{\partial s_\beta}(s,t)$ the first partial derivative of r with respecto to the β-coordinate of the first variable, $\frac{\partial^2 r}{\partial s_\alpha \partial t_\beta}(s,t)$ the crossed partial derivative of r with respect to the α-coordinate of the first variable and the β-coordinate of the second, etc.

As for the regression coefficients $C_\alpha^{s,t}$, $D_\alpha^{s,t}$ they are given by:

$$C_\alpha^{s,t}=\frac{r(t,t)\frac{\partial r}{\partial s_\alpha}(s,s)-r(s,t)\frac{\partial r}{\partial s_\alpha}(s,t)}{r(s,s)r(t,t)-r^2(s,t)}$$

$$D_\alpha^{s,t}=\frac{-r(s,t)\frac{\partial r}{\partial s_\alpha}(s,s)+r(s,s)\frac{\partial r}{\partial s_\alpha}(s,t)}{r(s,s)r(t,t)-r^2(s,t)}.$$

■

Proof. We apply the regression formula (6), taking into account that differentiation under the expectation sign permits to express the covariances in terms of the covariance function r:

$$\begin{aligned}
E\left(\partial_\alpha \xi(s)\xi(t)\right) &= \frac{\partial r}{\partial s_\alpha}(s,t)\\
E\left(\partial_\alpha \xi(s)\partial_\beta \xi(t)\right) &= \frac{\partial^2 r}{\partial s_\alpha \partial t_\beta}(s,t).
\end{aligned}$$

■

Proposition 4 *Let us consider the functions H_j ($j \geq 3$), defined in the proof of the Theorem.*

Then:

- $$H_j(0)=\left[E(\|\xi\|_j)\right]^2 \tag{43}$$

- $$H_j'(a)=E\left(\|\xi\|_j \|\zeta\|_j \left[(\eta_1+a\|\zeta\|_j)^2+\eta_2^2+...+\eta_j^2\right]^{-1/2}(\eta_1+a\|\zeta\|_j)\right).$$

  so that
  $$H'(0)=0. \tag{44}$$

-
$$\frac{H_j''(0)}{\left[E(\|\xi\|_j)\right]^2} \leq 1 + \frac{C_2}{j} \quad \textit{for} \quad j = 3, 4, .. \tag{45}$$

where C_2 *is some universal constant.*

- *for* $j \geq 4$ *and any* a,
$$\frac{\left|H_j'''(a)\right|}{\left[E(\|\xi\|_j)\right]^2} \leq C_3 \tag{46}$$

where C_3 *is some universal constant.*

Proof. (43) and (44) are immediate from the definition of H_j and its derivative.

To prove (45), we compute $H_j''(a)$:

$$H_j''(a) = E\left(\|\xi\|_j \|\zeta\|_j^2 \left[(\eta_1 + a\|\zeta\|_j)^2 + \eta_2^2 + ... + \eta_j^2\right]^{-3/2} (\eta_2^2 + ... + \eta_j^2)\right)$$

which implies:

$$\begin{aligned} 0 &\leq H_j''(a) \leq E\left(\|\xi\|_j \|\zeta\|_j^2 (\eta_2^2 + ... + \eta_j^2)^{-1/2}\right) \\ &= E\left(\|\xi\|_j \|\zeta\|_j^2\right) E\left((\eta_2^2 + ... + \eta_j^2)^{-1/2}\right) < \infty \text{ since } j \geq 3. \end{aligned}$$

Also,

$$\begin{aligned} H_j''(0) &= E(\|\xi\|_j \|\zeta\|_j^2)\ (j-1)\ E(\frac{\eta_1^2}{\|\eta\|^3}) \\ &= \frac{j-1}{j} E(\|\xi\|_j \|\zeta\|_j^2) E(\frac{1}{\|\eta\|}) \leq \frac{j-1}{j} m_{2,j}^{1/2} m_{4,j}^{1/2} m_{-1,j} \end{aligned}$$

on applying Schwarz inequality and putting, for $j - 1 + k \geq 0$:

$$m_{k,j} = E(\|\xi\|_j^k) = \frac{\sigma_{j-1}}{(2\pi)^{j/2}} \int_0^{+\infty} u^{j-1+k} e^{-\frac{u^2}{2}} du$$

An elementary computation shows that

$$\begin{aligned} m_{k,j} &= \frac{\sigma_{j-1}}{(2\pi)^{j/2}} (j+k-2)!! \text{ if } j+k-1 \text{ is odd,} \\ m_{k,j} &= \frac{\sigma_{j-1}}{(2\pi)^{j/2}} (j+k-2)!! \sqrt{\frac{\pi}{2}} \text{ if } j+k-1 \text{ is even and } \neq 0 \\ m_{k,j} &= \frac{\sigma_{j-1}}{(2\pi)^{j/2}} \sqrt{\frac{\pi}{2}} \text{ if } j+k-1 = 0. \end{aligned}$$

In these formulae for integer n we use the notation:

$$n!! = \prod_{0 \leq \nu < n/2} (n - 2.v).$$

Using Stirling's formula we obtain (45).

As for the last part of the statement, for $j \geq 4$ we have:

$$H_j'''(a) = -3\ E\left[\|\xi\|_j \|\zeta\|_j^3 \frac{(\eta_2^2 + ... + \eta_j^2)(\eta_1 + a\|\zeta\|_j)}{\left[(\eta_1 + a\|\zeta\|_j)^2 + \eta_2^2 + ... + \eta_j^2\right]^{5/2}}\right]$$

which implies the bound

$$\begin{aligned} \left|H_j'''(a)\right| &\leq 3\ E\left[\|\xi\|_j \|\zeta\|_j^3 \frac{1}{\eta_2^2 + ... + \eta_j^2}\right] \\ &\leq 3\ m_{2,j}^{1/2} m_{6,j}^{1/2} m_{-2,j-1} \end{aligned}$$

and again the formulae for $m_{k,j}$ plus a direct computation show (46). ■

2.1 References.

[1] J-M. Azaïs and M. Wschebor. On the distribution of the maximum of a gaussian field with d parameters, *The Annals of Applied Probability*, Vol. 15, No. 1 A, 254-278, 2005.

[2] J-M Azaïs and M. Wschebor. On the roots of a random system of equations. The theorem of Shub & Smale and some extensions. *Found. Comp. Math*, to appear, 2005.(see also preprint in http://www.cmat.edu.uy/ ˜wschebor/)

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

[4] 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.

[5] Feller, W. *An Introduction to Probability Theory and Its Applications. Vol. II*, John Wiley & Sons, 1966.

[6] E. Kostlan. On the distribution of roots of random polynomials, in *From Topology to Computation, Proceedings of the Smalefest*, M.W.Hirsch, J. E. Mardsen and M. Shub (eds), pp 419-431, 1993.

[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] G. Malajovich and J. M. Rojas. High probability analysis of the condition number of sparse polynomial systems. *Theor. Comp. Sc.*, 315, 525-555, 2004.

[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.