On the Probability Distribution of Singular Varieties of Given Corank. ⋆

Carlos Beltrán, Luis Miguel Pardo

Dept. de Matemáticas, Estadística y Computación. F. de Ciencias. U. Cantabria. E–39071 SANTANDER, Spain.

Abstract

We exhibit sharp upper bounds for the probability distribution of the distance from a system of multivariate polynomial equations to the strata of all systems having a critical zero of given corank. We also prove sharp upper bounds for the probability distribution of the condition number of singular systems of multivariate polynomial equations. We finally state a new and sharp technique of the Geometry of Numbers. Using this technique we show that rational systems of multivariate polynomial equations are equidistributed with respect to singular systems having a critical zero of given corank.

Key words: Polynomial Equation Solving, Condition Number, Discrepancy Bounds. 2000 MSC: Primary 14Q20, 65H10, Secondary 11H31, 58C35.

1. Introduction.

In these pages we prove upper bounds for the probability distribution of corank k condition numbers of systems of multivariate polynomial equations. We also prove upper bounds for the probability distribution of the function distance to the strata of the discriminant variety given by systems having a singular zero of given corank. Finally, we improve the techniques of the Geometry of Numbers introduced in (Castro et al., 2002, 2003). This improvement is used to show sharp bounds for the probability distribution of both functions above when restricted to systems of polynomial equations with rational coefficients. These studies are motivated by one of the major challenges in computational algebraic geometry: the design of efficient algorithms that solve systems of multivariate polynomial equations. We devote the first part of this Introduction to remind some of the references relating studies on the distribution of condition numbers to design of efficient algorithms.

⋆ Research was partially supported by MTM2004-01167 and FPU program, Government of Spain.

Email address: beltranc@unican.es, luis.pardo@unican.es (Carlos Beltrán, Luis Miguel Pardo).

Condition numbers have been used in numerical analysis to bound the stability of numerical procedures that solve certain problems (cf. (Turing, 1948) for a seminal work in this respect). Another seminal paper established a more relevant property of Condition Numbers of systems of multivariate polynomial equations. This seminal paper was (Shub and Smale, 1993a). In this paper the authors proved that the condition number $\mu_{\rm norm}$ of systems of multivariate polynomial equations is an upper bound for the complexity of path following methods that solve systems of multivariate polynomial equations. Along this paper we focus on this relation between condition numbers and complexity. Studies on the probability distribution of the condition numbers of $\mu_{\rm norm}$ were done in the series of papers (Shub and Smale, 1993b, 1996, 1994). The first one (i.e. (Shub and Smale, 1993b)) was published in the Proceedings of MEGA'92 which also emphasizes the relation of condition numbers with the design and analysis of efficient methods in Algebraic Geometry. These studies on the probability distribution of $\mu_{\rm norm}$ lead to the design of numerical analysis polynomial equation solvers whose running time is polynomial in the input length on the average (cf (Beltrán and Pardo, 2006b,c)). For instance, for a randomly chosen cubic system of multi–variate polynomial equations the numerical procedure based on path following methods will output a good approximation of a zero of the system in time $O(n^{21})$ with probability greater than $1 - \frac{1}{n^4}$, where n is the number of unknowns.

From a symbolic computation point of view it may be argued that the output of a numerical solver is different to standard symbolic outputs. This argument is based on certain misleading usage of the term "numerical solving". First of all, abstract studies on numerical solvers are based on continuous input and output data types (as in (Blum et al., 1998), for instance). However, continuous input and output data types is not a realistic assumption. Under Church's Thesis, inputs and outputs of any algorithm are discrete subjects that may be represented over a finite alphabet. For instance, input systems of multivariate polynomial equations must be lists of polynomials with coefficients in a computable field. The reader may assume, for instance, that input systems are polynomials with coefficients in a given number field. In order to have discrete data types to represent their outputs, numerical analysis programmers chose floating point encodings. However, floating point IEEE standards (either in single or double precision) are not well suited to deal with approximations of complex zeros of zero–dimensional systems of multivariate polynomial equations. This drawback is caused by Liouville type lower bounds in diophantine approximation (as in (Giusti et al., 1997a) or (Castro et al., 2001). Lower bounds on the precision required to represent approximation to zeros of multivariate polynomial equations are thus available. These lower bounds imply that a precision exponential in the number of variables is some times required (cf. (Castro et al., 2001)). Hence fixed precision as in IEEE standards is not appropriate for multivariate polynomial equation solving. In fact, precision must be flexible enough to be adapted to the condition number of the system (cf. (Castro et al., 2003)). A successful alternative to floating point encodings is that of diophantine approximation (cf. (Castro et al., 2003)). Moreover, using diophantine approximation encoding of approximate zeros the following holds: *approximate zeros and symbolic encodings of the residue class field of the solution are computationally equivalent* (cf. (Castro et al., 2001, Th. 4.1)). This statement simply means that we can compute a primitive element encoding of the residue class field of a zero from the information contained in the digits of an approximate zero, and conversely. Hence, proper implementations of efficient numerical analysis procedures can be oriented to produce efficient methods in Algebraic Geometry whose output contains symbolic information of general purpose.

This symbiosis between numerical and symbolic procedures is of course meaningful when efficiency becomes better than usual. There is, however, a second drawback of these usage of numerical solvers for symbolic purposes. Path following methods are fast on the average but they may become not so efficient when the input system is "close" (in a sense to be specified below) to the discriminant variety. For instance, in (Castro et al., 2001), it was shown a worst case lower bound of μ_{norm} which is doubly exponential in the input length (cf. (Malajovich, 1993) for doubly exponential upper bounds of μ_{norm}). This simply means that in the vicinity of the discriminant variety numerical analysis methods based on the value of μ_{norm} may require running time which is doubly exponential in the input length. In these cases, numerical solvers are not efficient at all.

There is no contradiction between the average polynomial time and the doubly exponential worst case complexity. This simply means that for a randomly chosen input system, numerical solvers run very fast with high probability, providing valuable information on some of the zeros of the system. Therefore, there are input systems with non–singular zeros such that the time of path following algorithms may become much worse than any symbolic procedure (as those examples discussed in (Castro et al., 2001)).

On the other hand, there are symbolic based procedures whose running time is determined by quantities coming from Intersection Theory. This is the case for instance of the procedure developed in the middle nineties by the TERA community (cf. (Pardo, 1995), (Giusti et al., 1995, 1998, 1997a,b)). The running time of the TERA algorithm is polynomial in some quantity called the intrinsic degree of the input system. This intrinsic degree is bounded by the Bézout number of the system and it is not affected by the proximity to the discriminant variety. Roughly speaking, algorithms as the one developed by the TERA community have a running time better than path following methods when the input system is "close" (in terms of the fiber distance) to the discriminant variety. One possible way out could be to use symbolic methods to solve those systems with too large condition number. Moreover, it could also be possible to run symbolic and numerical algorithms in parallel. The first that finishes its computations will provide valuable information about the variety of solutions.

However there are other options for a better understanding of these phenomena. Serious attempts to study the convergence of variations of Newton's Methods near singular zeros have been recently done (cf. (Dedieu and Shub, 2001), (Giusti et al., 2005a,b)). We sincerely believe that these studies will surely lead to the design of efficient numerical solvers near singular zeros. At last these studies would provide a better comprehension on why numerical solving is so sensible to the proximity of singularities. Following the program of Shub & Smale, prior to any design of an efficient procedure, a precise knowledge of the probability distribution of condition numbers is required.

And this is the motivation to write these pages. We want to exhibit the first upper bounds of the corank k condition number of systems of multivariate polynomial equations both in a continuous and a discrete setting. The reason to deal with continuous and discrete estimates in the same manuscript is not spurious. As we already said, computing is discrete and not continuous. Hence continuous upper bounds on the probability distribution of any function do not suffice to explain computational features. We need to supplement continuous estimates with discrete ones in order to have any kind of computational advice. In these pages, this is achieved by means of a transfer method. This transfer method is based on precise results of the Geometry of Numbers that we prove in Section 4.

For every positive integer number $d \in \mathbb{N}$, let $H_d \subseteq \mathbb{C}[X_0, \ldots, X_n]$ be the vector space of all complex homogeneous polynomials of degree d. For every degree list $(d) := (d_1, \ldots, d_n) \in \mathbb{N}^n$, let $\mathcal{H}_{(d)} := \prod_{i=1}^n H_{d_i}$ be the complex vector space of systems $f := [f_1, \ldots, f_n]$ of n homogeneous polynomial equations. For a given polynomial system $f \in \mathcal{H}_{(d)}$, we denote by $V(f) \subseteq \mathbb{P}_n(\mathbb{C})$ the set of projective solutions of f. Namely,

$$V(f) := \{\zeta \in \mathbb{P}_n(\mathbb{C}) : f(\zeta) = 0\}.$$

Finally, let $\mathbb{P}(\mathcal{H}_{(d)})$ be the complex projective space defined by $\mathcal{H}_{(d)}$.

The *discriminant variety* $\Sigma \subseteq \mathbb{P}(\mathcal{H}_{(d)})$ is the algebraic variety of all polynomial systems $f \in \mathbb{P}(\mathcal{H}_{(d)})$ such that $0 \in \mathbb{C}^n$ is a critical value of the polynomial mapping $f : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$. There is a classical decomposition of Σ based on the existence of singularities of given corank. According to (Arnold et al., 1986), for every positive integer $n \in \mathbb{N}$, $1 \leq r \leq n-1$, we denote by Σ^r the algebraic variety of all systems $f \in \mathbb{P}(\mathcal{H}_{(d)})$ such that $V(f)$ has a singularity of corank at least $n - r$. We then have the descending chain of algebraic varieties

$$\Sigma := \Sigma^{n-1} \supseteq \Sigma^{n-2} \supseteq \cdots \supseteq \Sigma^1.$$

The complex vector space $\mathcal{H}_{(d)}$ is usually endowed with an Hermitian inner product $\langle \cdot, \cdot \rangle_\Delta : \mathcal{H}_{(d)}^2 \longrightarrow \mathbb{C}$ which is invariant under the action of the group $\mathcal{U}_{n+1}$ of isometries of $\mathbb{P}_n(\mathbb{C})$. This Hermitian product has been rediscovered several times by several authors like Kostlan, Bombieri or Shub & Smale. For simplicity, we call $\langle \cdot, \cdot \rangle_\Delta$ the *Kostlan* Hermitian product in $\mathcal{H}_{(d)}$ and we denote by Δ the Kostlan matrix (as in (Blum et al., 1998)). Kostlan's Hermitian product induces a complex Riemannian structure in $\mathbb{P}(\mathcal{H}_{(d)})$. We denote the Fubini–Study distance associated to this Riemannian structure as $d_R : \mathbb{P}(\mathcal{H}_{(d)})^2 \longrightarrow \mathbb{R}^+$. As in (Blum et al., 1998), we also introduce a projective distance function $d_{\mathbf{P}} : \mathbb{P}(\mathcal{H}_{(d)}) \longrightarrow \mathbb{R}^+$, given by the following equality:

$$d_{\mathbf{P}}(f, g) := \sin d_R(f, g), \qquad \forall f, g \in \mathbb{P}(\mathcal{H}_{(d)}).$$

Namely, $d_{\mathbf{P}}(f, g)$ is the sinus of the angle of the subspaces generated by f and g. Together with these distance functions, the complex Riemannian structure in $\mathbb{P}(\mathcal{H}_{(d)})$ also defines a volume element $d\nu$ satisfying the following equality:

$$\nu[\mathbb{P}(\mathcal{H}_{(d)})] = \frac{\pi^N}{\Gamma(N+1)},$$

where N is the complex dimension of $\mathbb{P}(\mathcal{H}_{(d)})$.

The first outcome of these pages is the following statement.

Theorem 1 *For every positive integer r, $1 \leq r \leq n-1$, and for every positive real number $\varepsilon > 0$, let Σ_ε^r be the tube about Σ^r at distance $\varepsilon > 0$. Namely,*

$$\Sigma_\varepsilon^r := \{f \in \mathbb{P}(\mathcal{H}_{(d)}) : d_{\mathbf{P}}(f, \Sigma^r) < \varepsilon\}.$$

Then, the following inequality holds:

$$\frac{\nu[\Sigma_\varepsilon^r]}{\nu[\mathbb{P}(\mathcal{H}_{(d)})]} \leq 2 \left[\prod_{i=1}^n (d_i + 1)\right] \binom{n+1}{r} \binom{n}{r} \left(\frac{e\ Nn\ d\ \varepsilon}{(n-r)^2}\right)^{2(n-r)^2}$$

Let the reader observe that this statement gives the probability that a randomly chosen input system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ is close (with respect to $d_{\mathbf{P}}$ distance) to the variety Σ^r of systems having a singularity of corank at least $n - r$.

Although condition numbers are metric invariants they are not exactly related to the distance functions d_R and $d_{\mathbf{P}}$. Let $\Delta(d) := Diag(d_1, \ldots, d_n) \in \mathcal{M}_n(\mathbb{R})$ be the diagonal matrix whose entries are given by the list of degrees. For every positive integer r, $2 \leq r \leq n$, and for every input system $f \in \mathbb{P}(\mathcal{H}_{(d)})$, we define the corank $n - r$ condition number of f at a point $\zeta \in V(f)$ by the following equality:

$$\mu_{\text{norm}}^{(r)}(f, \zeta) := \frac{\kappa_D^r(\Delta(d)^{-1/2} T_\zeta f)}{\|\Delta(d)^{-1/2} T_\zeta f\|_F}, \tag{1}$$

where the representatives of f and ζ are chosen such that $\|f\|_\Delta = \|\zeta\|_2 = 1$, $T_\zeta f := d_\zeta f \mid_{\zeta^\perp}$ is the restriction of the differential mapping to the orthogonal complement of ζ, and κ_D^r is Demmel's generalized condition number of linear algebra, as defined in (Kahan, 2000), (Stewart and Sun, 1990), (Beltrán and Pardo, 2005; Beltrán and Pardo, 2006a). Note that $\mu_{\text{norm}}^{(r)}$ equals Shub & Smale condition number μ_{norm} when $r = n$. It extends to the non–linear case the linear algebra condition number κ_D^r discussed in (Beltrán and Pardo, 2006a). And it also satisfies a Condition Number Theorem (cf. Theorem 4 below).

The second main outcome of our manuscript is the following statement that generalizes the main outcome of (Shub and Smale, 1993b).

Theorem 2 *Assume that $d_i \geq 2$ for some i, $1 \leq i \leq n$. Then, the probability that a randomly chosen system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ has a solution ζ satisfying $\mu_{\text{norm}}^{(r)}(f, \zeta) > \varepsilon^{-1}$ is at most*

$$\mathcal{D}\left[2(n^2+n)^{1/2}(rN)^{1/2}\varepsilon\right]^{2(n-r+2)(n-r+1)},$$

where $\mathcal{D} := \prod_{i=1}^n d_i$ is the Bézout number.

This statement generalizes the upper bound of (Shub and Smale, 1993b) to the case of given corank singularities. In fact, Shub–Smale's Theorem (as proved in (Blum et al., 1998)) states that the probability of Theorem 2 for μ_{norm} (that is, the case $r = n$ in our notations) is at most $\mathcal{D}n^3(n+1)N(N-1)\varepsilon^4$. If we apply directly Theorem 2 we obtain $16\mathcal{D}n^4(n+1)^2N^2\varepsilon^4$, which is a similar bound.

As computing is a discrete matter, in coherence with our analysis we consider the class of systems of polynomial equations whose *representative bit length* is bounded by some quantity (cf. Section 4 for details). We thus deal with two main questions:

- What is the probability that an input system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ of representative bit length at most h and dense encoding is close to Σ^r?
- What is the probability that an input system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ of representative bit length at most h and dense encoding is an ill–conditioned system?

The set of points of representative bit length at most h in $\mathbb{P}(\mathcal{H}_{(d)})$ is a finite set. Hence assume that it is endowed with the uniform probability distribution. We prove the following result (see Theorems 11 and 12 below).

Theorem 3 *Assume that $d_i \geq 2$ for some $1 \leq i \leq n$. Let $\varepsilon > 0$ be a positive number. Let $h > 1$ be a positive real number, such that*

$$h = 6 + \frac{3}{2}\log(N+1) + 4(N+n+3)(5+\log(nd+d+1)) + h_1$$

for some positive real number $h_1 > 0$. Then, the probability that a randomly chosen point of representative bit length at most h belongs to the tube of radius ε about Σ^r is at most

$$2\left[\prod_{i=1}^{n}(d_i+1)\right]\binom{n+1}{r}\binom{n}{r}\left(\frac{e\ Nn\ d\ \varepsilon}{(n-r)^2}\right)^{2(n-r)^2}+\frac{1}{2^{h_1}}.$$

Moreover, the probability that a randomly chosen system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ of representative bit length at most h has a solution ζ satisfying $\mu^{(r)}_{\mathrm{norm}}(f,\zeta) > \varepsilon^{-1}$ is at most

$$\mathcal{D}\left[2(n^2+n)^{1/2}(rN)^{1/2}\varepsilon\right]^{2(n-r+2)(n-r+1)}+\frac{1}{2^{h_1}}.$$

These claims in Theorem 3 are essentially obtained by proving that Gaussian rationals are equidistributed with respect to singular systems (in the sense of (Castro et al., 2003) and references therein). In fact, we exhibit the sharpest known estimates for the discrepancy of Gaussian rationals of bounded height with respect to constructible subsets of a complex projective space (see Proposition 5).

This paper is structured as follows. In Section 2 we prove Theorem 1. In Section 3 we prove Theorem 2. Finally, in Section 4 we prove Theorem 3.

2. Proof of Theorem 1.

Let $(\mathbb{P}(\mathcal{H}_{(d)}), can)$ be the projective space with the canonical Riemannian structure. As pointed out in (Castro et al., 2003), the inverse of Kostlan's matrix Δ^{-1} defines an isometry between $(\mathbb{P}(\mathcal{H}_{(d)}), can)$ and $\mathbb{P}(\mathcal{H}_{(d)})$ with Kostlan's Riemannian structure. Moreover, Δ^{-1} is a linear isometry, and hence both the volume and the geometric degree are preserved. Thus, from the main technical tool of (Beltrán and Pardo, 2006a) we have:

$$\frac{\nu[\Sigma^r_\varepsilon]}{\nu[\mathbb{P}(\mathcal{H}_{(d)})]} \le 2\deg(\Sigma^r)\left(\frac{e\ N\ \varepsilon}{codim(\Sigma^r)}\right)^{2codim(\Sigma^r)}, \tag{2}$$

where *degree* refers to geometric degree in the sense of (Heintz, 1983). The rest of the proof is devoted to proving the following two inequalities:

$$codim(\Sigma^r) \ge (n-r)^2, \tag{3}$$

$$\deg(\Sigma^r) \le \left[\prod_{i=1}^{n}(d_i+1)\right]\binom{n+1}{r}\binom{n}{r}(nd)^{2(n-r)^2}. \tag{4}$$

Some notation is needed. Let W_0, W^r, W^r_0 be the sets defined as follows.

$$W_0 := V_{e_0} = \{f \in \mathbb{P}(\mathcal{H}_{(d)}) : f(e_0) = 0\},$$

$$W^r := \{(f,\zeta) \in \mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C}) : f(\zeta) = 0, rank(d_\zeta f) \le r\},$$

$$W^r_0 := \{f \in \mathbb{P}(\mathcal{H}_{(d)}) : f(e_0) = 0, rank(d_{e_0} f) \le r\},$$

$$S^r := \{M \in \mathcal{M}_n(\mathbb{C}) : rank(M) \le r\}.$$

From Krull's Principal Ideal Theorem (cf. for example (Kunz, 1985, Cor. 3.8)), the following property holds.

$$\dim(W^r_0) \ge \dim(W^r) - n. \tag{5}$$

On the other hand, let $L_{e_0}^{\perp} := \{f \in \mathcal{H}_{(d)} : f(e_0) = 0, d_{e_0} f \equiv 0\}$ be the set of systems of order at least 2 in e_0. As noted in (Blum et al., 1998), $W_0 \equiv \mathbb{P}(\mathcal{M}_n(\mathbb{C}) \times L_{e_0}^{\perp})$. Moreover, the following equality also holds.

$$W_0^r \equiv \mathbb{P}(S^r \times L_{e_0}^{\perp}).$$

As proved in (Fulton, 1984), (Bruns and Vetter, 1988), the set S^r is an irreducible algebraic variety of $\mathcal{M}_n(\mathbb{C})$ of complex dimension $n^2 - (n-r)^2$. Thus, W_0^r is also an irreducible algebraic variety of W_0 of complex dimension $N - n - (n-r)^2$. We deduce that W^r is an algebraic variety of complex dimension at most

$$\dim(W^r) \leq \dim(W_0^r) + n = N - (n-r)^2.$$

Let $p_1 : \mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C}) \longrightarrow \mathbb{P}(\mathcal{H}_{(d)})$ be the natural projection. From the Fundamental Theorem of Elimination Theory (see for example (Shafarevich, 1994)), $\Sigma^r := p_1(W^r)$ is an algebraic variety, and its dimension is at most $N - (n-r)^2$. This proves inequality (3). As for inequality (4), let $\widetilde{W}^r \subseteq \mathcal{H}_{(d)} \times \mathbb{C}^{n+1}$ be the set defined as follows.

$$\widetilde{W}^r := \{(f, \zeta) \in \mathcal{H}_{(d)} \times \mathbb{C}^{n+1} : f(\zeta) = 0, rank(d_\zeta f) \leq r\},$$

and let $\widetilde{p}_1 : \mathcal{H}_{(d)} \times \mathbb{C}^{n+1} \longrightarrow \mathcal{H}_{(d)}$ be the canonical projection. Observe that

$$\Sigma^r = \mathbb{P}(\widetilde{p}_1(\widetilde{W}^r)).$$

Hence, $\deg(\Sigma^r) \leq \deg(\widetilde{W}^r)$. Observe that for fixed $(f, \zeta) \in \mathcal{H}_{(d)} \times \mathbb{C}^{n+1}$, the fact that $rank(d_\zeta f) = r$ is equivalent to:

$$\bigvee_{\substack{1 \leq i_1, \ldots, i_r, \leq n \\ 1 \leq j_1, \ldots, j_r \leq n}} \left[\det(M_{i_1, \ldots, i_r}^{j_1, \ldots, j_r}) \neq 0, \bigwedge_{\substack{k_1 \neq i_1, \ldots, i_r \\ k_2 \neq j_1, \ldots, j_r}} \det(M_{i_1, \ldots, i_r, k_1}^{j_1, \ldots, j_r, k_2}) = 0 \right],$$

where $M_{i_1, \ldots, i_r, k_1}^{j_1, \ldots, j_r, k_2}$ holds for the $(r+1) \times (r+1)$ minor of $d_\zeta f \in \mathcal{M}_{n \times (n+1)}(\mathbb{C})$ obtained from the rows $i_1, \ldots, i_r, k_1$ and the columns $j_1, \ldots, j_r, k_2$. From Bézout's Theorem (as in (Heintz, 1983)), we have that

$$\deg(\widetilde{W}^r) = \deg(\widetilde{W}^r \setminus \widetilde{W}^{r-1}) \leq$$

$$\left[\prod_{i=1}^{n} (d_i + 1)\right] \sum_{\substack{1 \leq i_1, \ldots, i_r, \leq n \\ 0 \leq j_1, \ldots, j_r \leq n}} \prod_{\substack{k_1 \neq i_1, \ldots, i_r \\ k_2 \neq j_1, \ldots, j_r}} (d_{i_1} + \cdots + d_{i_r} + d_{k_1}) \leq$$

$$\left[\prod_{i=1}^{n} (d_i + 1)\right] \binom{n+1}{r} \binom{n}{r} ((r+1)d)^{(n-r)(n-r+1)} \leq$$

$$\left[\prod_{i=1}^{n} (d_i + 1)\right] \binom{n+1}{r} \binom{n}{r} (nd)^{2(n-r)^2},$$

as wanted. The theorem easily follows from inequalities (2), (3) and (4).

3. Proof of Theorem 2

Given any pair $(f,x) \in \mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C})$, we denote by $T_x f := (d_x f) \mid_{x^\perp}$ the restriction of the differential $d_x f$ to the tangent space $x^\perp$, where f, x are any fixed affine representations such that $\|f\|_\Delta = \|x\|_2 = 1$. Sometimes we identify $T_x f$ with the differential matrix in any orthogonal basis of $x^\perp$. In the case that $x = e_0 := (1 : 0 : \cdots : 0)$, we identify

$$T_{e_0} f \equiv \begin{pmatrix} \frac{\partial f_1}{X_1}(e_0) & \cdots & \frac{\partial f_1}{X_n}(e_0) \\ \vdots & & \vdots \\ \frac{\partial f_n}{X_1}(e_0) & \cdots & \frac{\partial f_n}{X_n}(e_0) \end{pmatrix},$$

for any fixed representation $f \in \mathcal{H}_{(d)}$, $\|f\|_\Delta = 1$. Let $W \subseteq \mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C})$ be the so–called incidence variety. Namely,

$$W := \{(f,\zeta) \in \mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C}) : f(\zeta) = 0\}.$$

The following result easily follows from the definition as observed in (Shub and Smale, 1993b), (Blum et al., 1998).

Proposition 1 *The incidence variety W is a differentiable manifold of (complex) dimension N.*

Let $p_1 : W \longrightarrow \mathbb{P}(\mathcal{H}_{(d)})$ be the projection onto the first coordinate. We can obviously identify $p_1^{-1}(f)$ and $V(f)$. Let $e_0 := (1 : 0 : \cdots : 0)$ be this fixed projective point. We denote by V_{e_0} the set of systems that have e_0 as a solution.

For every positive integer $2 \leq r \leq n$, we define the sets $(\Sigma^{r-1})' \subseteq W$ as follows:

$$(\Sigma^{r-1})' := \{(f,\zeta) \in W : rank(T_\zeta f) \leq r-1\},$$

Observe that we have $\Sigma^{r-1} := p_1((\Sigma^{r-1})')$.

The following statement is a Condition Number Theorem for singularities of given corank. This kind of results can be studied in a much more general framework, see (Dedieu, 1996) and references therein.

Theorem 4 *For $f \in \mathbb{P}(\mathcal{H}_{(d)})$ and $\zeta \in V(f)$, the following equality holds:*

$$\mu_{\text{norm}}^{(r)}(f,\zeta) = \frac{1}{d_{\mathbf{P}}(f, p_1(\{(f,x) \in (\Sigma^{r-1})' : x = \zeta\}))}.$$

Proof. The condition number $\mu_{\text{norm}}^{(r)}$ (defined in equation (1)) is invariant under the action of the unitary group $\mathcal{U}_{n+1}$. Hence, it suffices to prove the Theorem for the case $\zeta = e_0$. Let $f \in \mathbb{P}(\mathcal{H}_{(d)})$ be a system of homogeneous polynomial equations such that $f(e_0) = 0$. As in the proof of (Blum et al., 1998, Lemma 17, p.225), we have:

$$d_{\mathbf{P}}(f, p_1(\{(f,x) \in (\Sigma^{r-1})' : x = e_0\})) = d_F(\Delta(d)^{-1/2} T_{e_0} f, S^{r-1}),$$

where $S^{r-1} \subseteq \mathcal{M}_n(\mathbb{C})$ holds for the set of affine square matrices of rank at most $r-1$, and d_F is the Frobenius distance in $\mathcal{M}_n(\mathbb{C})$. Now, let $\sigma_1 \geq \cdots \geq \sigma_n \geq 0$ be the singular values of $\Delta(d)^{-1/2} T_{e_0} f$. From (Stewart and Sun, 1990, Th. 4.18), the following chain of equalities holds:

$$\frac{1}{d_F(\Delta(d)^{-1/2} T_{e_0} f, S^{r-1})} = \frac{1}{\sqrt{\sigma_r^2 + \cdots + \sigma_n^2}} = \frac{\kappa_D^r(\Delta(d)^{-1/2} T_{e_0} f)}{\|\Delta(d)^{-1/2} T_{e_0} f\|_F} = \mu_{\text{norm}}^{(r)}(f, e_0),$$

and the statement follows. □

Let $\varepsilon > 0$ be a positive real number, and let $\chi_\varepsilon^{(r)}$ be the characteristic function of the set

$$\{f \in \mathbb{P}(\mathcal{H}_{(d)}) : \exists \zeta \in V(f), \mu_{\mathrm{norm}}^{(r)}(f, \zeta) > \varepsilon^{-1}\}.$$

We are interested in upper bounds for

$$\mathcal{A}_{\varepsilon,(d)}^r := \frac{1}{\nu[\mathbb{P}(\mathcal{H}_{(d)})]} \int_{f \in \mathbb{P}(\mathcal{H}_{(d)})} \chi_\varepsilon^{(r)}(f) \; d\mathbb{P}(\mathcal{H}_{(d)}),$$

Observe that $\mathcal{A}_{\varepsilon,(d)}^r$ describes the probability distribution of the condition number $\mu_{\mathrm{norm}}^{(r)}$. Moreover, for $r = n$, the number $\mathcal{A}_{\varepsilon,(d)}^n$ is the quantity studied in (Shub and Smale, 1993b), (Blum et al., 1998).

We prove the following proposition (cf. also (Blum et al., 1998, Th. 1, pg. 256)).

Proposition 2 *With the notations above, the following inequality holds.*

$$\mathcal{A}_{\varepsilon,(d)}^r \leq \frac{\nu[\mathbb{P}_n(\mathbb{C})]}{\nu[\mathbb{P}(\mathcal{H}_{(d)})]} \int_{\substack{f \in V_{e_0} \\ \mu_{\mathrm{norm}}^{(r)}(f, e_0) > \varepsilon^{-1}}} \det((T_{e_0} f)(T_{e_0} f)^*) \; dV_{e_0}.$$

Moreover,

$$\nu[(\Sigma_{\mathcal{M}}^{r-1})_\varepsilon] = \nu[\mathbb{P}_n(\mathbb{C})] \int_{\substack{M \in \mathbb{P}(\mathcal{M}_n(\mathbb{C})) \\ \kappa_D^r(M) > \varepsilon^{-1}}} \det(MM^*) \; d\mathbb{P}(\mathcal{M}_n(\mathbb{C})),$$

where M is chosen such that $\|M\|_F = 1$.

Proof. We consider the set $\{(f, \zeta) \in W : \mu_{\mathrm{norm}}^{(r)}(f, \zeta) > \varepsilon^{-1}\}$, which is unitarily invariant in the sense of (Blum et al., 1998). Then, from (Blum et al., 1998, Prop.2 p. 244) we have:

$$\int_{f \in \mathbb{P}(\mathcal{H}_{(d)})} \chi_\varepsilon^{(r)}(f) \; d\mathbb{P}(\mathcal{H}_{(d)}) \leq$$

$$\int_{f \in \mathbb{P}(\mathcal{H}_{(d)})} \sharp\{\zeta \in V(f) : \mu_{\mathrm{norm}}^{(r)}(f, \zeta) > \varepsilon^{-1}\} \; d\mathbb{P}(\mathcal{H}_{(d)}) =$$

$$\nu[\mathbb{P}_n(\mathbb{C})] \int_{\substack{f \in V_{e_0} \\ \mu_{\mathrm{norm}}^{(r)}(f, e_0) \varepsilon^{-1}}} \det((T_{e_0} f)(T_{e_0} f)^*) \; dV_{e_0},$$

and the inequality of the statement follows. The equality follows since the inequality above is an equality when $(d) = (1, \ldots, 1)$. □

Lemma 5 *Assume that there exists an index $1 \leq i \leq n$ such that $d_i > 1$. Let r be a positive integer, $2 \leq r \leq n$. Then, the following integral equality holds:*

$$\nu[\mathbb{P}_n(\mathbb{C})] \int_{\substack{f \in V_{e_0} \\ \mu_{\mathrm{norm}}^{(r)}(f, e_0) > \varepsilon^{-1}}} \det((T_{e_0} f)(T_{e_0} f)^*) \; dV_{e_0} =$$

$$= 2\pi\nu[\mathbb{P}_{N-n^2-n}(\mathbb{C})]\mathcal{D}\int_0^1 (1-s^2)^{N-n^2-n}s^{2n^2+2n-1}\nu[(\Sigma_{\mathcal{M}}^{r-1})_{\varepsilon/s}]\ ds,$$

where $(\Sigma_{\mathcal{M}}^{r-1})_{\varepsilon/s}$ is the following subset of the projective space of matrices:

$$(\Sigma_{\mathcal{M}}^{r-1})_{\varepsilon/s} := \{M \in \mathbb{P}(\mathcal{M}_{n\times(n+1)}) : \kappa_D^n(M) > s/\varepsilon\}$$

Proof. Let $L_{e_0} \subseteq \mathcal{H}_{(d)}$ be the vectorial subspace given by the following equality:

$$L_{e_0} := \{f = [f_1,\ldots,f_n] \in \mathcal{H}_{(d)} : f_i = X_0^{d_i-1}\sum_{j=1}^n a_{ij}X_j\}.$$

Namely, L_{e_0} is the set of homogeneous polynomial systems vanishing at e_0 such that they are linear on all the variables but X_0. As noted in (Shub and Smale, 1993b), (Blum et al., 1998), the following map is a norm preserving linear isomorphism:

$$\begin{array}{rcl} \psi_{e_0} : L_{e_0} & \longrightarrow & \mathcal{M}_n(\mathbb{C}). \\ f & \mapsto & \Delta(d)^{-1/2}T_{e_0}f \end{array}$$

We may also consider the orthogonal projection $\pi_{L_{e_0}} : \mathcal{H}_{(d)} \longrightarrow L_{e_0}$. For every positive integer $m \geq 0$, we denote by ϑ^m the volume of the m–dimensional sphere in $\mathbb{R}^{m+1}$. Also, let $T_\varepsilon \subseteq \mathcal{M}_n(\mathbb{C})$ be the subset of the space of complex matrices defined as follows:

$$T_\varepsilon := \{M \in \mathcal{M}_n(\mathbb{C}), \|M\|_F \leq 1, \frac{\kappa_D^r(M)}{\|M\|_F} > \varepsilon^{-1}\}.$$

The proof of the lemma follows the steps of the proof of (Blum et al., 1998, Th. 1 pg. 256). Namely, we lift the integral to the sphere $S_{e_0} := \{f \in \mathcal{H}_{(d)} : f(e_0) = 1, \|f\|_\Delta = 1\}$, and then we apply the Coarea Formula to the orthogonal projection $\pi_{L_{e_0}}$ and the isometry ψ_{e_0}. Thus, the main strategy in (Blum et al., 1998) implies

$$\int_{\substack{f\in V_{e_0}\\ \mu_{\rm norm}^{(r)}(f,e_0)>\varepsilon^{-1}}} \det((T_{e_0}f)(T_{e_0}f)^*)\ dV_{e_0} =$$

$$= \frac{\vartheta^{2N-2n^2-2n+1}}{2\pi}\mathcal{D}\int_{M\in T_\varepsilon} \det(MM^*)(1-\|M\|_F^2)^{N-n^2-n}\ d\mathcal{M}_n(\mathbb{C}).$$

Then, the resulting integral on the space of square matrices is reduced (again by the Coarea Formula) to an integral on the sphere $S(\mathcal{M}_n(\mathbb{C})) := \{M \in \mathcal{M}_n(\mathbb{C}) : \|M\|_F = 1\}$, obtaining:

$$\int_{\substack{f\in V_{e_0}\\ \mu_{\rm norm}^{(r)}(f,e_0)>\varepsilon^{-1}}} \det((T_{e_0}f)(T_{e_0}f)^*)\ dV_{e_0} =$$

$$= \frac{\vartheta^{2N-2n^2-2n+1}}{2\pi}\mathcal{D}\int_0^1 (1-s^2)^{N-n^2-n}s^{2n^2+2n-1}\mathcal{J}_{s,\varepsilon}\ dt,$$

where for $0 < s < 1$, $\mathcal{J}_{s,\varepsilon}$ is the integral expression defined as follows:

$$\mathcal{J}_{s,\varepsilon} := \int_{\substack{M\in S(\mathcal{M}_n(\mathbb{C}))\\ \kappa_D^r(M)>s\varepsilon^{-1}}} \det(MM^*)\ dS(\mathcal{M}_n(\mathbb{C})).$$

Now, observe that

$$\mathcal{J}_{s,\varepsilon} = 2\pi \int_{\substack{M\in\mathbb{P}(\mathcal{M}_n(\mathbb{C}))\\ \kappa_D^r(M)>s\varepsilon^{-1}}} \det(MM^*)\ d\mathbb{P}(\mathcal{M}_n(\mathbb{C})),$$

where the affine representant $M \in \mathcal{M}_n(\mathbb{C})$ is chosen such that $\|M\|_F = 1$. The claim follows from Proposition 2, since

$$\vartheta^{2N-2n^2-2n+1} = 2\pi\nu[\mathbb{P}_{N-n^2-n}(\mathbb{C})].$$

□

Proof of Theorem 2. From (Beltrán and Pardo, 2006a, Cor. 40), we have:

$$\frac{\nu[(\Sigma_{\mathcal{M}}^{r-1})_\varepsilon]}{\nu[\mathbb{P}(\mathcal{M}_{n\times(n+1)}(\mathbb{C}))]} \leq 2\left(\frac{en(n+1)r^{1/2}}{(n-r+1)(n-r+2)}\ \varepsilon\right)^{2(n-r+1)(n-r+2)}.$$

Then, we prove that

$$\mathcal{A}^r_{\varepsilon,(d)} \leq 2\mathcal{D}\ D(N,n,r)\left(\frac{en(n+1)r^{1/2}}{(n-r+2)(n-r+1)}\varepsilon\right)^{2(n-r+2)(n-r+1)},$$

where

$$D(N,n,r) = \frac{\Gamma(N+1)\Gamma(n^2+n-(n-r+2)(n-r+1))}{\Gamma(n^2+n)\Gamma(N-(n-r+2)(n-r+1)+1)}.$$

In fact, this is a direct consequence of Proposition 2 and Lemma 5, knowing that

$$\int_0^1 (1-s^2)^{N-n^2-n} s^{2n^2+2n-1-2(n-r+2)(n-r+1)}\ ds =$$

$$= \frac{1}{2}\frac{\Gamma(N-n^2-n+1)\ \Gamma(n^2+n-(n-r+2)(n-r+1))}{\Gamma(N-(n-r+2)(n-r+1)+1)}.$$

In order to simplify this formula, just observe that if we denote $a = (n-r+2)(n-r+1) \in [2, n^2-n]$,

$$D(N,n,r) = \frac{N\cdots(N-a+1)}{(n^2+n-1)\cdots(n^2+n-a)} \leq \left(\frac{N}{n^2+n-a}\right)^a.$$

Hence, we have that

$$\mathcal{A}^r_{\varepsilon,(d)} \leq 2\left(en(n+1)r^{1/2}\frac{1}{a}\left(\frac{N}{n^2+n-a}\right)^{1/2}\varepsilon\right)^{2(n-r+2)(n-r+1)}.$$

Let $g(a) := \frac{1}{a}\left(\frac{N}{n^2+n-a}\right)^{1/2}$ be this function. Elementary calculations show that

$$g(a) \leq g(2) = \frac{N^{1/2}}{2(n^2+n-2)^{1/2}}, \qquad \forall\ a,\ 2\leq a\leq n^2-n.$$

Thus,

$$\mathcal{A}^r_{\varepsilon,(d)} \leq \left(\frac{e(n^2+n)r^{1/2}N^{1/2}}{2^{1-\frac{1}{2a}}(n^2+n-2)^{1/2}}\varepsilon\right)^{2(n-r+2)(n-r+1)}.$$

The bound of the Theorem follows from the facts that

$$\frac{(n^2+n)}{(n^2+n-2)^{1/2}} \leq \sqrt{\frac{3}{2}}(n^2+n)^{1/2},$$

and

$$\frac{e}{2^{1-\frac{1}{2a}}}\sqrt{\frac{3}{2}} \leq \frac{e\sqrt{3}}{2^{3/4+1/2}} < 2.$$

4. Proof of Theorem 3

A semi–algebraic set is a subset $\mathcal{W}$ of some affine real space $\mathbb{R}^{m+1}$ that can be defined by a quantified first–order formula over the reals. Let $\mathcal{F} := \{f_1, \ldots, f_s\} \subseteq \mathbb{R}[X_0, \ldots, X_m]$ be a finite set of polynomials. A semialgebraic set $\mathcal{W} \subseteq \mathbb{R}^{m+1}$ is called an $\mathcal{F}$–cell if there is a list of sign conditions

$$\underline{\epsilon} := (\epsilon_1, \ldots, \epsilon_s) \in \{<, =, >\}^s,$$

such that

$$\mathcal{W} := \{x \in \mathbb{R}^{m+1} : f_i(x)\ \epsilon_i\ 0,\ 1 \leq i \leq s\}.$$

An $\mathcal{F}$–definable semi–algebraic set is a finite union of $\mathcal{F}$–cells.

Definition 6 *Let $s, d \in \mathbb{N}$ be two positive integer numbers. A semi–algebraic subset $\mathcal{W} \subseteq \mathbb{R}^{m+1}$ is called (s,d)–definable if there is a finite set of polynomials $\mathcal{F} \subseteq \mathbb{R}[X_0, \ldots, X_m]$ satisfying:*

- *$\mathcal{W}$ is $\mathcal{F}$–definable,*
- *$\sharp(\mathcal{F}) = s$,*
- *$\deg(f_i) \leq d,\ \forall f \in \mathcal{F}$.*

We say that a semi–algebraic subset $\mathcal{W} \subseteq \mathbb{R}^{m+1}$ is the M–projection of an (s,d)–definable semi–algebraic set if there is an (s,d)–definable subset $\mathcal{W}' \subseteq \mathbb{R}^{M+m+1}$ such that the following equality holds:

$$\mathcal{W} := \{x \in \mathbb{R}^{m+1} : \exists y \in \mathbb{R}^M \text{ such that } (y, x) \in \mathcal{W}')\}.$$

For every non–negative integer $i \geq 0$, we denote by K_i the volume of the unit ball in $\mathbb{R}^i$. The following Theorem improves the discrepancy bounds obtained in (Castro et al., 2003).

Theorem 7 *Let $m \geq 1$ be a positive integer and let $\mathcal{W} \subseteq \mathbb{R}^m$ be the M–projection of an (s,d)–definable semi–algebraic set. Let $H \geq 0$ be a positive real number. Let $N(\mathcal{W}, H) := \sharp[\mathcal{W} \cap \mathbb{Z}^m \cap B_m(0,H)]$ be the number of points of integer coordinates in the intersection $\mathcal{W} \cap B_m(0,H)$. Let $C(s,d,M)$ be the constant defined as follows:*

$$C(s,d,M) := (4sd+1)^{2(M+2)}.$$

Then, the following inequality holds:

$$|N(\mathcal{W}, H) - \nu_m[\mathcal{W} \cap B(0,H)]| \leq C(s,d,M) \sum_{i=0}^{m-1} K_i \binom{m}{i} H^i.$$

In the case that $\mathcal{W}$ is an (s,d)–definable semi–algebraic set, the constant $C(s,d,M)$ may be replaced by

$$ds + 1.$$

Finally, if $\mathcal{W}$ is convex, then the constant $C(s,d,M)$ may be replaced by 1.

Proof. Let M, s, d be fixed. For every positive integer $n \geq 1$, we denote by $\delta(n, H)$ the following quantity:

$$\delta(n, H) := \sup_{\mathcal{W}'}\{|\sharp[\mathcal{W}' \cap \mathbb{Z}^n \cap B_n(0, H)] - \nu_n[\mathcal{W}' \cap B_n(0, H)]|\},$$

where the maximum is taken over all the choices of $\mathcal{W}'$, where $\mathcal{W}' \subseteq \mathbb{R}^n$ is the M–projection of an (s, d) semi–algebraic set. We prove the following inequality by induction on n:

$$\delta(n, H) \leq C(s, d, M) \sum_{i=0}^{n-1} K_i \binom{n}{i} H^i. \tag{6}$$

First, let $n = 1$. In this case we obviously have,

$$|\sharp[\mathcal{W}' \cap \mathbb{Z} \cap B_1(0, H)] - \nu_1[\mathcal{W}' \cap B_1(0, H)]| \leq \beta_0(\mathcal{W}'),$$

where $\beta_0(\mathcal{W}')$ is the number of connected components of $\mathcal{W}'$. Now, from (Castro et al., 2003, Th. 9) and references therein, this last is at most $C(s, d, M)$. Thus, inequality (6) holds for $n = 1$. Now, we prove the following inequality:

$$\delta(n, H) \leq C(s, d, M)K_{n-1}H^{n-1} + \sum_{x \in \mathbb{Z} \cap [-H,H]} \delta(n - 1, \sqrt{H^2 - x^2}). \tag{7}$$

In fact, let $\mathcal{W}' \subseteq \mathbb{R}^n$ be the M–projection of some (s, d)–definable semi–algebraic set. For every point $x \in \mathbb{R}$, let $\mathcal{W}'_x$ be the set defined as follows:

$$\mathcal{W}'_x := \{y \in \mathbb{R}^{n-1} : (x, y) \in \mathcal{W}'\}.$$

For every point $y \in \mathbb{R}^{n-1}$, let $\mathcal{W}'^y$ be the following set.

$$\mathcal{W}'^y := \{x \in \mathbb{R} : (x, y) \in \mathcal{W}'\}.$$

Observe that for every choice of x or y, the sets $\mathcal{W}'_x, \mathcal{W}'^y$ are also M–projections of (s, d)–definable sets. We denote by H_x the number $\sqrt{H^2 - x^2}$, and by H^y the number $\sqrt{H^2 - \|y\|^2}$. Let us introduce two auxiliary quantities:

$$S_1 := \left|\sharp[\mathcal{W}' \cap \mathbb{Z}^n \cap B_n(0, H)] - \sum_{x \in \mathbb{Z} \cap [-H,H]} \nu_{n-1}[\mathcal{W}'_x \cap B_{n-1}(0, H_x)]\right|,$$

and

$$S_2 := \left|\sum_{x \in \mathbb{Z} \cap [-H,H]} \nu_{n-1}[\mathcal{W}'_x \cap B_{n-1}(0, H_x)] - \nu_n[\mathcal{W}' \cap B_n(0, H)]\right|.$$

Observe that $|\sharp[\mathcal{W}' \cap \mathbb{Z}^n \cap B_n(0, H)] - \nu_n[\mathcal{W}' \cap B_n(0, H)]| \leq S_1 + S_2$. We bound each term separately. On one hand, S_1 equals the absolute value of

$$\sum_{x \in \mathbb{Z} \cap [-H,H]} \sharp[\mathcal{W}'_x \cap \mathbb{Z}^{n-1} \cap B_{n-1}(0, H_x)] - \sum_{x \in \mathbb{Z} \cap [-H,H]} \nu_{n-1}[\mathcal{W}'_x \cap B_{n-1}(0, H_x)].$$

Thus,

$$S_1 \leq \sum_{x \in \mathbb{Z} \cap [-H,H]} |\sharp[\mathcal{W}'_x \cap \mathbb{Z}^{n-1} \cap B_{n-1}(0, H_x)] - \nu_{n-1}[\mathcal{W}'_x \cap B_{n-1}(0, H_x)]| \leq$$

$$\sum_{x\in\mathbb{Z}\cap[-H,H]} \delta(n-1,H_x).$$

On the other hand, S_2 equals

$$\left|\sum_{x\in\mathbb{Z}\cap[-H,H]} \int_{y\in\mathbb{R}^{n-1}} \chi_{\mathcal{W}'^y\cap B_1(0,H^y)}(x)\ dy + \int_{y\in\mathbb{R}^{n-1}} \int_{x\in B_1(0,H^y)} \chi_{\mathcal{W}'^y}(x)\ dx\ dy\right| \leq$$

$$\int_{y\in\mathbb{R}^{n-1}\cap B_{n-1}(0,H)} |\sharp[\mathcal{W}'^y\cap\mathbb{Z}\cap B_1(0,H^y)] - \nu_1[\mathcal{W}'^y\cap B_1(0,H^y)]|\ dy \leq$$

$$K_{n-1}H^{n-1} \max_{y\in B_{n-1}(0,H)} \delta(1,H^y) \leq C(s,d,M)K_{n-1}H^{n-1},$$

and inequality (7) follows. From inequality (7) and induction hypothesis we have that:

$$\frac{\delta(n,H)}{C(s,d,M)} \leq K_{n-1}H^{n-1} + \sum_{i=0}^{n-2} K_i \binom{n-1}{i} \sum_{x\in\mathbb{Z}\cap[-H,H]} (H^2-x^2)^{i/2}.$$

Now, for every non–negative integer $i \geq 0$, we have that

$$\sum_{x\in\mathbb{Z}\cap[-H,H]} (H^2-x^2)^{i/2} \leq H^i + 2\int_0^{\lfloor H\rfloor} (H^2-t^2)^{i/2}\ dt \leq$$

$$H^i + 2\int_0^H (H^2-t^2)^{i/2}\ dt = H^i + B\left(\frac{1}{2},\frac{i}{2}+1\right)H^{i+1},$$

where $B(\cdot,\cdot)$ is the Beta Function. Hence,

$$\frac{\delta(n,H)}{C(s,d,M)} \leq K_{n-1}H^{n-1} + \sum_{i=0}^{n-2} K_i\binom{n-1}{i}\left[H^i + B\left(\frac{1}{2},\frac{i}{2}+1\right)H^{i+1}\right] =$$

$$= 1 + \sum_{i=1}^{n-1} K_i\left[\binom{n-1}{i} + \frac{K_{i-1}}{K_i}\binom{n-1}{i-1}B\left(\frac{1}{2},\frac{i+1}{2}\right)\right]H^i.$$

Now, observe that for every positive integer value of i,

$$\frac{K_{i-1}}{K_i} = B\left(\frac{1}{2},\frac{i+1}{2}\right)^{-1}, \quad \textit{and} \quad \binom{n-1}{i} + \binom{n-1}{i-1} = \binom{n}{i}.$$

Thus, we have proved that

$$\frac{\delta(n,H)}{C(s,d,M)} \leq 1 + \sum_{i=1}^{n-1} K_i\binom{n}{i}H^i = \sum_{i=0}^{n-1} K_i\binom{n}{i}H^i,$$

as wanted. The rest of the claims can be proved exactly by the same arguments, but using the more sharp bound for the number of connected components β_0 in the case $n=1$ when $\mathcal{W}$ is a (s,d)–definable semi–algebraic set (see (Castro et al., 2003, Th. 9), for example) or when $\mathcal{W}$ is convex. □

The following Corollary easily follows from Theorem 7.

Corollary 3 *With the notations and assumptions of Theorem 7 above, let $\delta(\mathcal{W},H) := |N(\mathcal{W},H) - \nu_m[\mathcal{W}\cap B_m(0,H)]|$ be this number. Then, the following properties hold.*

- *If* $0 < H < 1$*, then* $\delta(\mathcal{W}, H) \leq \max\{1, K_m\}$.
- *If* $H \geq 1$*, then*
$$\delta(\mathcal{W}, H) \leq C(s, d, M) 6mH^{m-1}\left(1 + \frac{1}{H}\right)^{m-1}.$$
- *Moreover, if* $H \geq m^2$*, then*
$$\delta(\mathcal{W}, H) \leq C(s, d, M) 2mK_{m-1}H^{m-1},$$

where $C(s, d, M)$ *is the constant of Theorem 7.*

Proof. We just prove the third statement. We must check that for $H \geq m^2$, the following inequality holds.
$$\sum_{i=0}^{m-1} K_i \binom{m}{i} H^i \leq 2mK_{m-1}H^{m-1}. \tag{8}$$
The case $m = 1$ is immediate. As for the case $m > 1$, let $T_i := K_i\binom{m}{i}H^i$ be the i–esim term of the sum on the left–hand side of equation (8). Observe that
$$\frac{T_i}{T_{i+1}} = B\left(\frac{1}{2}, \frac{i+2}{2}\right)^{-1} \frac{i+1}{m-i}\frac{1}{H}.$$
From Gautschi's Inequalities (see (Elezović et al., 2000, Th. 3) for very sharp bounds), we know that
$$B\left(\frac{1}{2}, \frac{i+2}{2}\right)^{-1} = \frac{\Gamma\left(\frac{i+3}{2}\right)}{\sqrt{\pi}\Gamma\left(\frac{i+2}{2}\right)} \leq \sqrt{\frac{i}{2} + \frac{1}{2} + \frac{1}{\pi}}\sqrt{\frac{1}{\pi}} \leq \sqrt{\frac{i+2}{2\pi}}.$$
Thus, if $H \geq m^2$, we obtain that $T_i \leq \frac{T_{i+1}}{\sqrt{m}}$ and the following inequality holds.
$$\sum_{i=0}^{m-1} T_i \leq T_{m-1}\sum_{i=0}^{m-1}\frac{1}{\sqrt{m}^{m-1-i}} = T_{m-1}\frac{\sqrt{m} - \frac{1}{\sqrt{m}^{m-1}}}{\sqrt{m} - 1} \leq 2T_{m-1}.$$
Hence, we have proved equation (8). □

Let $\mathbb{Q}[i]$ be the field of Gaussian rational numbers and $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$ the ring of Gaussian integers which is a principal ideal domain and unique factorization domain with units $S^1(1) = \{a \in \mathbb{Z}[i] : |a| = 1\} = \{1, -1, i, -i\}$.

By a $\mathbb{Z}[i]-$lattice in $\mathbb{C}^{m+1}$ we mean the free $\mathbb{Z}[i]-$module generated by a basis β of $\mathbb{C}^{m+1}$ as complex vector space. Namely, if $\beta = \{v_0, \ldots, v_m\}$ is a basis of $\mathbb{C}^{m+1}$ as complex vector space, the $\mathbb{Z}[i]-$lattice it generates is the lattice:
$$\Lambda(\beta) = \{\lambda_0 v_0 + \cdots + \lambda_m v_m : \lambda_i \in \mathbb{Z}[i], 0 \leq i \leq m\}$$
Let $\Lambda \subseteq \mathbb{C}^{m+1}$ be a $\mathbb{Z}[i]-$lattice and let $x \in \Lambda$ be a non-zero element. Let $\langle x\rangle \subseteq \mathbb{C}^{m+1}$ be the $\mathbb{Q}[i]-$vector space generated by x. Namely, $\langle x\rangle = \{\lambda x : \lambda \in \mathbb{Q}[i]\}$. The $\mathbb{Z}[i]-$module $\langle x\rangle \cap \Lambda$ is a torsion free submodule of rank 1 of Λ. Hence it has basis with a single element. We say that x is visible from the origin in Λ if $\{x\}$ is a basis of the $\mathbb{Z}[i]-$module $\langle x\rangle \cap \Lambda$. Note that a non-zero point $x \in \Lambda$ is visible from the origin in Λ if and only if:
$$\|x\| = \min\{\|y\| : y \in \langle x\rangle \cap \Lambda\}.$$

Equivalently, let $\beta = \{v_0, \ldots, v_m\} \subseteq \mathbb{C}^{m+1}$ be a basis of $\mathbb{C}^{m+1}$ as complex vector space such that $\Lambda = \Lambda(\beta)$. Let $x \in \Lambda$ be a non-zero point and let $\lambda_0, \ldots, \lambda_m \in \mathbb{Z}[i]$ be the (unique) Gaussian integers such that:

$$x = \lambda_0 v_0 + \ldots + \lambda_m v_m.$$

Then, x is visible from the origin if and only if

$$gcd_{\mathbb{Z}[i]}(\lambda_0, \ldots, \lambda_m) \in S^1(1),$$

where $gcd_{\mathbb{Z}[i]}(\lambda_0, \ldots, \lambda_m)$ means the greatest common divisor of $\lambda_0, \ldots, \lambda_m$ in $\mathbb{Z}[i]$ (a factorial domain).

We shall make use of the following functions. As usual, $r_2(n)$ will denote the number of points in $S^1(\sqrt{n})$, where $S^1(\sqrt{n}) = \{a + bi \in \mathbb{Z}[i] : |a + bi| = \sqrt{n}\}$. Namely,

$$r_2(n) := \sharp\{a + bi \in \mathbb{Z}[i] : |a|^2 + |b|^2 = n\}.$$

This function has been well studied since Gauss. It is closely related to the factorization of n in $\mathbb{Z}$.

Let $\mathbb{P}_m(\mathbb{C})$ be the complex projective space and let $\pi : \mathbb{C}^{m+1} \setminus \{0\} \longrightarrow \mathbb{P}_m(\mathbb{C})$ be the canonical projection. Let $\mathbb{P}_m(\mathbb{Q}[i])$ be the $m-$dimensional projective space defined by the field of Gaussian rationals. We equally denote by π the canonical projection $\pi : \mathbb{Q}[i]^{m+1} \setminus \{0\} \longrightarrow \mathbb{P}_m(\mathbb{Q}[i])$. Note that the restriction $\pi_{|\mathbb{Z}[i]^{m+1}\setminus\{0\}}$ is also onto. For every point $x \in \mathbb{P}_m(\mathbb{Q}[i])$ we define its absolute height as the minimum of the norms of the points in $\pi^{-1}(\{x\}) \cap (\mathbb{Z}[i])^{m+1}$. In other words, for every $x \in \mathbb{P}_m(\mathbb{Q}[i])$ there are exactly four visible points $\{x_1, -x_1, ix_1, -ix_1\} \subseteq \mathbb{Z}[i]^{m+1}$ such that $\pi(x_1) = x$ and the absolute height of x is defined as

$$H(x) = \|x_1\|_2,$$

where $\|.\|_2$ is the standard Hermitian norm in $\mathbb{C}^{m+1}$. Finally, we define the *bit length* of the projective point $x \in \mathbb{P}_m(\mathbb{Q}[i])$ as the logarithm of its absolute height. Namely,

$$bl(x) := \log_2 H(x).$$

Observe that $bl(x)$ is essentially equivalent to the number of bits required to represent the projective point x in a Turing machine.

Let $\widetilde{\mathcal{W}} \subseteq \mathbb{C}^{m+1}$ be a subset. For every positive integer H, we denote by $N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H)$ the following number:

$$N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H) := \sharp(\widetilde{\mathcal{W}} \cap \mathbb{Z}[i]^{m+1} \cap B_2(0, H) \setminus \{0\})$$

where $B_2(0, H)$ is the closed ball in $\mathbb{C}^{m+1}$ of radius H centered at the origin. Namely,

$$N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H) := \sharp\{x \in \widetilde{\mathcal{W}} \cap \mathbb{Z}[i]^{m+1} : 0 < \|x\|_2 \leq H\}.$$

Let $\mathcal{W} \subseteq \mathbb{P}_m(\mathbb{C})$ be a subset of the complex projective space. We denote by $\mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H)$ the number of points in $\mathcal{W} \cap \mathbb{P}_m(\mathbb{Q}[i])$ of absolute height at most H. Namely,

$$\mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H) = \sharp\{x \in \mathcal{W} \cap \mathbb{P}_m(\mathbb{Q}[i]) : H(x) \leq H\}.$$

The following statement relates $N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H)$ and $\mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H)$.

Proposition 4 *With the above notations and assumptions, the following equality holds for every $H > 1$.*

$$N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H) = \sum_{n \leq H^2} \mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H/\sqrt{n}) r_2(n)$$

Proof. First of all, we introduce some notations. We denote by $\widetilde{\mathcal{W}}(H)$ the set of all non–zero points in $\widetilde{\mathcal{W}} \cap \mathbb{Z}[i]^{m+1} \cap B(0,H)$ and by $\widetilde{\mathcal{W}}^v(H)$ we denote the set of all visible points of $\mathbb{Z}[i]^{m+1}$ that belong to $\widetilde{\mathcal{W}} \cap B(0,H)$. Note that

$$4\mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, s) = \sharp\widetilde{\mathcal{W}}^v(s) \tag{9}$$

for every real number $s \geq 1$. Now we consider the disjoint union

$$A := \bigcup_{n \leq H^2} \widetilde{\mathcal{W}}^v(H/\sqrt{n}) \times S^1(\sqrt{n}),$$

and we define the following mapping

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & \widetilde{\mathcal{W}}(H) \\ & (y,\lambda) & \mapsto & \lambda y \end{array}$$

This mapping is well-defined, because for every $\lambda \in S^1(\sqrt{n})$ and $y \in \widetilde{\mathcal{W}}^v(H/\sqrt{n})$ we clearly have $\lambda y \in \widetilde{\mathcal{W}} \cap \mathbb{Z}[i]^{m+1}$ and

$$|\lambda| \|y\|_2 \leq \sqrt{n} H/\sqrt{n} = H.$$

Now we show that the mapping φ is onto. Given $x \in \widetilde{\mathcal{W}}(H)$, $x = (x_0, \ldots, x_n) \in \mathbb{Z}[i]^{m+1}$, let $\lambda \in \mathbb{Z}[i]$ be the greatest common divisor of the coordinates of x. Namely,

$$\lambda = gcd_{\mathbb{Z}[i]}(x_0, \ldots, x_n),$$

and define $y_i = \lambda^{-1} x_i \in \mathbb{Z}[i]$, $y = (y_0, \ldots, y_n) \in \mathbb{Z}[i]^{m+1}$. As $\widetilde{\mathcal{W}}$ is a cone, we have $y \in \widetilde{\mathcal{W}}$. The point y is a visible point and $\|y\|_2 = \frac{\|x\|_2}{|\lambda|} \leq \frac{H}{|\lambda|}$. Putting $n = |\lambda|^2 \in \mathbb{N}$ we have shown that φ is onto. Let $x \in \widetilde{\mathcal{W}}(H)$ be a point and let $(y, \lambda) \in \varphi^{-1}(\{x\})$ be any point such that $\varphi(y, \lambda) = x$. Then, we see that

$$\varphi^{-1}(\{x\}) = \{(u^{-1}y, u\lambda) : u \in S^1(1)\}.$$

For if $\varphi(y, \lambda) = \varphi(z, \theta) = x$ we have $\lambda y = \theta z$ and $y, z \in \mathbb{Z}[i]^{m+1}$ are two visible points. Thus, as they define the same projective point there is some unit $u \in \mathbb{Z}[i]^*$ such that $z = uy$. Hence, $\theta = u^{-1}\lambda$ and we are over. Thus, we conclude $\sharp\varphi^{-1}(\{x\}) = 4, \forall x \in \widetilde{\mathcal{W}}(H)$ and, hence,

$$\frac{1}{4}\left(\sum_{n \leq H^2} \sharp\left[\widetilde{\mathcal{W}}^v(H/\sqrt{n}) \times S^1(\sqrt{n})\right]\right) = \sharp\widetilde{\mathcal{W}}(H).$$

In other words,

$$\sum_{n \leq H^2} \frac{1}{4}\sharp(\widetilde{\mathcal{W}}^v(H/\sqrt{n}))r_2(n) = N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H).$$

Thus, using equality (9) we conclude the wanted inequality

$$N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, H) = \sum_{n \leq H^2} \mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H/\sqrt{n}) r_2(n).$$

□

We shall introduce now some basic facts on Dirichlet L–functions. Let χ_4 be the Legendre-Jacobi-Kronecker primitive character *mod* 4, given by the following equalities:

$$\chi_4(n) = \begin{cases} 0 & if gcd(n,4) > 1 \\ 1 & if n \equiv 1 \; mod 4 \\ -1 & if n \equiv 3 \; mod 4, \end{cases}$$

where $n \in \mathbb{N}$ is a positive integer number. Let L_4 be the Dirichlet L-function given by:

$$L_4(s) := \sum_{n\geq 1} \frac{\chi_4(n)}{n^s} = \prod_p (1 - \chi_4(p)p^{-s})^{-1}, \qquad s > 1.$$

Using the formula for multiplication of Dirichlet series, we observe that:

$$L_4(s) \left(\sum_{n\geq 1} \frac{\mu(n)\chi_4(n)}{n^s} \right) = \sum_{n\geq 1} \left(\sum_{d|n} \mu(n/d)\chi_4(n/d)\chi_4(d) \right) n^{-s}$$

$$= \sum_{n\geq 1} \frac{\chi_4(n) \sum_{d|n} \mu(d)}{n^s} = 1.$$

Thus, the following equality holds:

$$\frac{1}{L_4(s)} = \sum_{n\geq 1} \frac{\mu(n)\chi_4(n)}{n^s} \tag{10}$$

Let ζ be Riemann's Zeta function. From (Hardy and Wright, 1979, Th. 287), for every real number $s > 1$ the following equality holds:

$$\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}. \tag{11}$$

The following statement is also a well-known result that may be found in (Hardy and Wright, 1979, Th. 306), for instance.

$$\sum_{n\geq 1} \frac{r_2(n)}{n^s} = 4\zeta(s)L_4(s) \tag{12}$$

We are now in conditions to prove the following statement:

Proposition 5 *Let $N \geq 2$ be a positive integer and let $\mathcal{W} \subset \mathbb{P}_N(\mathbb{C})$ be a subset of the complex projective space. Assume that the cone $\widetilde{\mathcal{W}} \subset \mathbb{C}^{N+1}$ is an M-projection of an $(s,d)-$definable semi-algebraic complex subset, and let $H > 1$ be a real number. Then, the following inequality holds:*

$$\left| \mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H) - \frac{\pi\nu[\mathcal{W}]}{4\zeta(N+1)L_4(N+1)(N+1)} H^{2N+2} \right| \leq$$

$$C(s,d,M) \left[8(N+1)^2 H^4 + \frac{1}{4} \sum_{i=3}^{2N+1} K_i \binom{2N+2}{i} \zeta(i/2)^2 H^i \right],$$

where $C(s,d,M)$ is like in Theorem 7 and ζ is Riemann's Zeta function.

Proof. For the proof we will make use of the Dirichlet series described above. From the multiplication formula for Dirichlet L–series (cf. (Hardy and Wright, 1979, Th. 284)) and identity (12), the following identity holds for every $s > 1$:

$$\sum_{n\geq 1} \frac{a_n}{n^s} = \frac{1}{4\zeta(s)L_4(s)}, \tag{13}$$

where a_n satisfies the following equality:

$$\sum_{d|n} a_{\frac{n}{d}} r_2(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & otherwise. \end{cases} \tag{14}$$

Hence the sequence $\{a_n\}_{n\in\mathbb{N}}$ satisfies the following recurrence rule:

$$a_1 = \frac{1}{r_2(1)} = \frac{1}{4}; \qquad a_n = -\sum_{\substack{d|n \\ d\neq n}} a_d r_2\left(\frac{n}{d}\right),\ for\ n \geq 2.$$

Additionally, using the multiplication formula for Dirichlet L–series and identities (10) and (11) we may conclude:

$$a_n = \frac{1}{4}\sum_{d|n} \mu(d)\mu\left(\frac{n}{d}\right)\chi_4\left(\frac{n}{d}\right) \tag{15}$$

Let $\rho \in \mathbb{R}$ be the real number defined as $\rho = \frac{1}{H^2}$. Let $f, g : (0,\infty) \longrightarrow \mathbb{Z}$ be the mappings defined by the following identities,

$$f(s) := N_{\mathbb{Z}[i]}(\widetilde{\mathcal{W}}, s^{-1/2}), \qquad g(s) := \mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, s^{-1/2}), \qquad \forall s > 0.$$

Then, Proposition 4 reads:

$$f(\rho) = \sum_{n\leq H^2} g(n\rho)r_2(n). \tag{16}$$

Now, observe that the sum on the right hand side of this equality may be seen as an infinite sum for if $n > H^2$, then $\frac{H}{\sqrt{n}} < 1$ and $g(n\rho) = \mathcal{N}_{\mathbb{Z}[i]}\left(\mathcal{W}, \frac{H}{\sqrt{n}}\right) = 0$. Thus, equality (16) can also be written as:

$$f(\rho) = \sum_{n\geq 1} g(n\rho)r_2(n). \tag{17}$$

As in the proof of (Hardy and Wright, 1979, Th. 268), we have:

$$\sum_{n\geq 1} f(n\rho)a_n = \sum_{n\geq 1} a_n \left(\sum_{k\geq 1} r_2(k)g(kn\rho)\right) = \sum_{m\geq 1}\left(\sum_{d|m} a_{\frac{m}{d}} r_2(d)\right) g(m\rho).$$

From equality (14) we conclude the following inverse relation between f and g:

$$\sum_{n\geq 1} a_n f(n\rho) = g(\rho).$$

Now we consider the following difference

$$S := \left|\rho^{N+1} g(\rho) - \frac{\pi\nu[\mathcal{W}]}{4(N+1)\zeta(N+1)L_4(N+1)}\right| =$$

$$= \left| \sum_{n\geq 1} \frac{a_n}{n^{N+1}} \left[(n\rho)^{N+1} f(n\rho) - \frac{\pi\nu[\mathcal{W}]}{N+1} \right] \right|.$$

We define the following two terms:

$$S_1 := \left| \sum_{n\leq H^2} \frac{a_n}{n^{N+1}} \left[(n\rho)^{N+1} f(n\rho) - \frac{\pi\nu[\mathcal{W}]}{N+1} \right] \right|,$$

$$S_2 := \left| \sum_{n> H^2} \frac{a_n}{n^{N+1}} \frac{\pi\nu[\mathcal{W}]}{N+1} \right|.$$

We have that $S \leq S_1 + S_2$. Then, we bound each S_i separately. For S_1 we have

$$S_1 \leq \sum_{n\leq H^2} \frac{|a_n|}{n^{N+1}} \left| (n\rho)^{N+1} f(n\rho) - \frac{\pi\nu[\mathcal{W}]}{N+1} \right|.$$

From Theorem 7, we have:

$$\frac{1}{C(s,d,M)} \left| (n\rho)^{N+1} f(n\rho) - \frac{\pi\nu[\mathcal{W}]}{N+1} \right| \leq$$

$$(n\rho)^{N+1} + \sum_{i=0}^{2N+1} K_i \binom{2N+2}{i} (n\rho)^{N+1-\frac{i}{2}}.$$

The first term of this sum comes from the fact that we are counting only non–zero affine points. On the other hand, from Identity (15) above we have:

$$|a_n| \leq \frac{1}{4} \sum_{d|n} \left| \mu(d)\mu\left(\frac{n}{d}\right) \chi_4\left(\frac{n}{d}\right) \right| \leq \frac{1}{4} d(n),$$

where $d(n)$ is the number of divisors of n. We then conclude:

$$\frac{S_1}{C(s,d,M)} \leq \frac{1}{4} \left(\rho^{N+1} \sum_{n\leq H^2} d(n) + \sum_{i=0}^{2N+1} K_i \binom{2N+2}{i} \rho^{N+1-i/2} \sum_{n\leq H^2} \frac{d(n)}{n^{i/2}} \right).$$

From (Hardy and Wright, 1979, Th. 289), we have that for every $i \geq 3$,

$$\sum_{n\leq H^2} \frac{d(n)}{n^{i/2}} \leq \sum_{n\geq 1} \frac{d(n)}{n^{i/2}} = \zeta(i/2)^2.$$

On the other hand, for $i = 0, 1, 2$, we have that

$$\sum_{n\leq H^2} d(n) \leq \sum_{n\leq H^2} n \leq \sum_{n\leq H^2} H^2 = \lfloor H^2 \rfloor H^2 \leq H^4 = \frac{1}{\rho^2};$$

$$\sum_{n\leq H^2} \frac{d(n)}{n^{1/2}} \leq \sum_{n\leq H^2} n^{1/2} \leq \lfloor H^2 \rfloor H \leq H^3 = \frac{1}{\rho^{3/2}};$$

$$\sum_{n\leq H^2} \frac{d(n)}{n} \leq \sum_{n\leq H^2} 1 = \lfloor H^2 \rfloor \leq H^2 = \frac{1}{\rho}.$$

Thus, we conclude

$$\frac{S_1}{C(s,d,M)} \leq \frac{1}{4}\left(4N+6+\pi(2N+2)(2N+1)\right)\rho^{N-1}+$$

$$+\frac{1}{4}\sum_{i=3}^{2N+1} K_i \binom{2N+2}{i} \rho^{N+1-i/2}\zeta\left(\frac{i}{2}\right)^2 .$$

As for S_2, we have:

$$S_2 \leq \frac{\pi\nu[\mathcal{W}]}{N+1}\sum_{n\geq \rho^{-1}} \frac{|a(n)|}{n^{N+1}}.$$

When $N \geq 2$, we can roughly bound this quantity as follows,

$$S_2 \leq \frac{\pi\nu[\mathcal{W}]}{4(N+1)}\sum_{n\geq\rho^{-1}}\frac{n}{n^{N+1}} \leq \frac{\pi\nu[\mathcal{W}]}{4(N+1)}\left[\rho^N + \sum_{n\geq\rho^{-1}+1}\frac{1}{n^N}\right] \leq$$

$$\frac{\pi\nu[\mathcal{W}]}{4(N+1)}\left[\rho^N + \int_{n\geq\rho^{-1}}\frac{1}{t^N}\,dt\right] = \frac{\pi\nu[\mathcal{W}]}{4(N+1)}\left[\rho^N + \frac{\rho^{N-1}}{N-1}\right].$$

Replacing ρ^{-1} by H^2 in these estimates, the claim of the proposition follows bounding the term

$$\frac{C(s,d,M)}{4}\left(4N+6+\pi(2N+2)(2N+1)\right)H^4 + \frac{\pi\nu[\mathcal{W}]}{4(N+1)}\left[H^2+\frac{H^4}{N-1}\right]$$

by the quantity $8C(s,d,M)(N+1)^2H^4$. □

The following Corollary easily follows from Proposition 5, by the same method that Corollary 3.

Corollary 6 *Let $N \geq 2$ be a positive integer and let $\mathcal{W} \subset \mathbb{P}_N(\mathbb{C})$ be a subset of the complex projective space. Assume that the cone $\widetilde{\mathcal{W}} \subset \mathbb{C}^{N+1}$ is an M-projection of an $(s,d)-$definable semi-algebraic complex subset, and let $H > 4(N+1)^2$ be a real number. Then, the following inequality holds:*

$$\left|\mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W},H) - \frac{\pi\nu[\mathcal{W}]}{4\zeta(N+1)L_4(N+1)(N+1)}H^{2N+2}\right| \leq$$

$$8C(s,d,M)(N+1)K_{2N+1}H^{2N+1},$$

where $C(s,d,M)$ is like in Theorem 7 and ζ is Riemann's function.

Finally, we will make use of the following Lemma.

Lemma 8 *Let $A,B,C,D,\alpha_1,\alpha_2$ be real positive numbers such that the following inequalities hold.*

$$|A-B| \leq \alpha_1, \qquad |C-D| \leq \alpha_2, \qquad |A| \leq |C|.$$

Then, the following inequality also holds:

$$\left|\frac{A}{C}-\frac{B}{D}\right| \leq \frac{\alpha_1+\alpha_2}{|D|}.$$

Theorem 9 *Let $N \geq 2$ and let $\mathcal{W} \subset \mathbb{P}_N(\mathbb{C})$ be a subset of the complex projective space. Assume that the cone $\widetilde{\mathcal{W}} \subset \mathbb{C}^{N+1}$ is an M-projection of an $(s,d)-$definable semi-algebraic complex subset, and let $H > 4(N+1)^2$ be a real number. Then, the following inequality holds:*

$$\left| \frac{\mathcal{N}_{\mathbb{Z}[i]}(\mathcal{W}, H)}{\mathcal{N}_{\mathbb{Z}[i]}(\mathbb{P}_N(\mathbb{C}), H)} - \frac{\nu[\mathcal{W}]}{\nu[\mathbb{P}_N(\mathbb{C})]} \right| \leq \frac{60C(s,d,M)(N+1)^{3/2}}{H},$$

where $C(s,d,M)$ is like in Theorem 7.

Proof. The Theorem is a direct consequence of Corollary 6 and Lemma 8. In fact, we can easily check that $L_4(N+1) \leq \zeta(N+1)$. Moreover,

$$\frac{K_{2N+1}}{\nu[\mathbb{P}_N(\mathbb{C})]} = \frac{\sqrt{\pi}\Gamma(N+1)}{\Gamma(N+3/2)} \leq \frac{\sqrt{\pi}}{\sqrt{N+3/4}}.$$

This last inequality follows from Gautschi's Inequalities (see (Elezović et al., 2000)). □

We can also write the *bit length* version of this Theorem:

Theorem 10 *Let $\mathcal{W} \subset \mathbb{P}_N(\mathbb{C})$ be a subset of the complex projective space. Assume that the cone $\widetilde{\mathcal{W}} \subset \mathbb{C}^{N+1}$ is an M-projection of an $(s,d)-$definable semi-algebraic complex subset, and let $h \geq 2 + 2\log(N+1)$ be a positive real number. Let $P \in [0,1]$ be the probability that a randomly chosen point of bit length at most h belongs to $\mathcal{W}$. Then, the following inequality holds:*

$$\left| P - \frac{\nu[\mathcal{W}]}{\nu[\mathbb{P}_N(\mathbb{C})]} \right| \leq \frac{60C(s,d,M)(N+1)^{3/2}}{2^h},$$

where $C(s,d,M)$ is like in Theorem 7.

The following corollary follows from Theorem 10 and (Beltrán and Pardo, 2006a, Th. 1).

Corollary 7 *Let $V \subset \mathbb{P}_N(\mathbb{C})$ be a proper algebraic variety of complex codimension m of the complex projective space, such that V can be expressed as the solution set of a system of s equations of degree at most d. Let*

$$V_\varepsilon := \{x \in \mathbb{P}_N(\mathbb{C}) : d_{\mathbf{P}}(x, V) \leq \varepsilon\},$$

and let $h > 2 + 2\log(N+1)$ be a positive real number. Let $P_\varepsilon \in [0,1]$ be the probability that a randomly chosen point of bit length at most h belongs to V_ε. Then, the following inequality holds:

$$P_\varepsilon \leq \frac{\nu[V_\varepsilon]}{\nu[\mathbb{P}_N(\mathbb{C})]} + \frac{60C(2, 2\max\{2,d\}, 2N+2)(N+1)^{3/2}}{2^h},$$

where $C(2, 2\max\{2,d\}, 2N+2)$ is the constant of Theorem 7. Moreover,

$$P_\varepsilon \leq 2d^s \left(\frac{eN\varepsilon}{m}\right)^{2m} + \frac{60C(2, 2\max\{2,d\}, 2N+2)(N+1)^{3/2}}{2^h}.$$

Proof. We apply Theorem 10 to V_ε. Observe that the cone $\widetilde{V_\varepsilon}$ of V_ε can be expressed as the $(2N+2)$–projection of an $(2, 2\max\{2,d\})$–definable set. In fact, a point $x \in \mathbb{C}^{N+1}$

belongs to $\widetilde{V}_\varepsilon$ if and only if there exists a point $y \in \mathbb{C}^{N+1} \equiv \mathbb{R}^{2N+2}$ such that $y \in V$ and $d_{\mathbf{P}}(x, y) < \varepsilon$. Now, this last condition can be expressed as

$$\varepsilon^2 > d_{\mathbf{P}}(x,y)^2 = 1 - \frac{|\langle x, y\rangle|^2}{|x|^2|y|^2}.$$

Hence, we add to the equations describing V an inequality of degree 4. Now, V can be seen as the vanishing of s complex equations of degree d, that is $2s$ real equations of the same degree. This can be replaced by only one equation: The sum of squares of all of them, that is only one equation of degree $2d$. As for the second part of the Corollary, note that from (Beltrán and Pardo, 2006a), the quantity $\frac{\nu[V_\varepsilon]}{\nu[\mathbb{P}_N(\mathbb{C})]}$ is bounded by $2\mathcal{D}\left(\frac{eN\varepsilon}{m}\right)^{2m}$, where $\mathcal{D} \leq d^s$ holds for the Bezóut number. □

As an immediate consequence we also obtain the two following statements.

Corollary 8 *Let $V \subset \mathbb{P}_N(\mathbb{C})$ be a proper algebraic variety of complex codimension m of the complex projective space, such that V can be expressed as the solution set of a system of s equations of degree at most d. Let*

$$V_\varepsilon := \{x \in \mathbb{P}_N(\mathbb{C}) : d_{\mathbf{P}}(x, V) \leq \varepsilon\},$$

be the tube of radius ε about V. Let $h > 1$ be a positive real number, such that

$$h = 6 + \frac{3}{2}\log(N+1) + 4(N+2)(6 + \log d) + h_1,$$

for some positive real number $h_1 > 0$. Let $P_\varepsilon \in [0, 1]$ be the probability that a randomly chosen point of bit length at most h belongs to V_ε. Then, the following inequality holds:

$$P_\varepsilon \leq \frac{\nu[V_\varepsilon]}{\nu[\mathbb{P}_N(\mathbb{C})]} + \frac{1}{2^{h_1}}.$$

Moreover,

$$P_\varepsilon \leq 2d^s\left(\frac{eN\varepsilon}{m}\right)^{2m} + \frac{1}{2^{h_1}}.$$

Recall we have denoted by $\Delta \in \mathcal{M}_{N+1}(\mathbb{C})$ Kostlan's matrix, as defined in (Blum et al., 1998). Let $f \in \mathbb{P}(\mathcal{H}_{(d)})$ be such that

$$f \in \pi\left(\Delta^{-1}\mathbb{Z}^{N+1}\right),$$

where $\pi : \mathbb{C}^{N+1} \longrightarrow \mathbb{P}(\mathcal{H}_{(d)})$ is the natural projection. We define the *representative bit length* of f as the (usual) bit length of Δf. In order to understand this definition, let Δ^{-1} be the mapping defined as follows.

$$\begin{array}{rccc} \Delta^{-1} : & (\mathbb{P}(\mathcal{H}_{(d)}), can) & \longrightarrow & \mathbb{P}(\mathcal{H}_{(d)}) \\ & f & \mapsto & \Delta^{-1}f, \end{array}$$

where $(\mathbb{P}(\mathcal{H}_{(d)}), can)$ holds for the projective space $\mathbb{P}(\mathcal{H}_{(d)})$ endowed with its canonical Riemannian structure (namely, the structure inherited from the usual Hermitian product $\langle\cdot,\cdot\rangle_2$ in $\mathbb{C}^{N+1} \equiv \mathcal{H}_{(d)}$). As observed in (Castro et al., 2003), Δ^{-1} is an isometry. The *representative bit length* of $f \in \mathbb{P}(\mathcal{H}_{(d)})$, is exactly the bit length of the pre–image of f by Δ^{-1}. Hence, the *representative bit length* of $f \in \mathbb{P}(\mathcal{H}_{(d)})$ is essentially equivalent to the number of bits required to represent f in a Turing machine, via the isometry Δ^{-1}.

Note that the set of points $f \in \mathbb{P}(\mathcal{H}_{(d)})$ of *representative bit length* at most h is the image by Δ^{-1} of the set of points $f \in (\mathbb{P}(\mathcal{H}_{(d)}), can)$ of *bit length* at most h.

Then, Theorem 3 is an immediate consequence of the two following results.

Theorem 11 *Let $\varepsilon > 0$ be a positive number. Let $h > 1$ be a positive integer, such that*

$$h = 6 + \frac{3}{2}\log(N+1) + 4(N+n+3)(4+\log(dr+d+1)) + h_1$$

for some positive real number $h_1 > 0$. Then, the probability that a randomly chosen point of representative bit length at most h belongs to the tube of radius ε about Σ^r is at most

$$2\left[\prod_{i=1}^{n}(d_i+1)\right]\binom{n+1}{r}\binom{n}{r}\left(\frac{e\ Nn\ d\ \varepsilon}{(n-r)^2}\right)^{2(n-r)^2} + \frac{1}{2^{h_1}}.$$

Proof. This result is a direct consequence of Theorems 1 and 10 . In fact, it suffices to prove that the cone of the tube of radius ε about Σ^r is the $(2N+2n+4)$–projection of a $(2, 2(r+1)d)$–definable set. In order to see this, observe that a system $g \in \mathcal{H}_{(d)}$ belongs to this tube if and only if there exists a pair $(f, \zeta) \in \mathcal{H}_{(d)} \times \mathbb{C}^{n+1}$ such that:

$$\|\zeta\| = 1, \qquad f(\zeta) = 0, \qquad rank(d_\zeta f) \le r, \qquad \sqrt{1 - \frac{|\langle f, g\rangle_\Delta|^2}{\|f\|_\Delta^2\|g\|_\Delta^2}} < \varepsilon.$$

Now, the first three conditions can be expressed as the vanishing of a system of one real equation and $n + \binom{n+1}{r}\binom{n}{r}$ complex equations of degree at most $(r+1)d$. This may be replaced by a real equation of degree at most $2(r+1)d$. Thus the theorem follows since the constant of Theorem 10 becomes

$$(16(r+1)d+1)^{4(N+n+3)}.$$

□

Theorem 12 *Assume that $d_i \ge 2$ for some $1 \le i \le n$. Let $2 \le r \le n$ be a positive integer. Let $h > 0$ be a positive number, such that*

$$h = 6 + \frac{3}{2}\log(N+1) + 4(N+n+3)\log(16nd+1) + h_1,$$

for some positive real number $h_1 > 0$. Then, the probability that a randomly chosen system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ of representative bit length at most h has a solution ζ satisfying $\mu_{\mathrm{norm}}^{(r)}(f,\zeta) > \varepsilon^{-1}$ is at most

$$\mathcal{D}\left[2(n^2+n)^{1/2}(rN)^{1/2}\varepsilon\right]^{2(n-r+2)(n-r+1)} + \frac{1}{2^{h_1}}.$$

Proof. Let Q_ε be the probability that a randomly chosen system $f \in \mathbb{P}(\mathcal{H}_{(d)})$ of representative bit length at most h has a solution ζ satisfying $\mu_{\mathrm{norm}}^{(r)}(f,\zeta) > \varepsilon^{-1}$. Let $\mathcal{S}_\varepsilon$ be the cone in $\mathbb{C}^{N+1}$ of this set of polynomial systems. We prove that $\mathcal{S}_\varepsilon$ is the $2N+2n+4$–projection of a $(2, 2nd)$–definable algebraic set. In fact, let $(f, \zeta) \in \mathbb{C}^{N+1} \times \mathbb{C}^{n+1}$ be a point such that $f(\zeta) = 0$, $\zeta \ne 0$. Then, from Theorem 4 we know that $\mu_{\mathrm{norm}}^{(r)}(f,\zeta) > \varepsilon^{-1}$ if and only if there exists $g \in \mathbb{P}(\mathcal{H}_{(d)})$ such that $\zeta \in V(g)$ and $rank(T_\zeta g) \le r-1$, and $d_{\mathbf{P}}(f,g) < \varepsilon$. Hence, the condition $f \in \mathcal{S}_\varepsilon$ is equivalent to the existence of points

$\zeta \in \mathbb{C}^{n+1}$, $g \in \mathbb{C}^{N+1}$ such that $f(\zeta) = 0, g(\zeta) = 0, \|\zeta\| = 1, rank(T_\zeta g) \leq r-1$ and $d_{\mathbf{P}}(f,g) < \varepsilon$. Now, as observed in (Blum et al., 1998),

$$d_{\mathbf{P}}(f,g) = \sqrt{1 - \frac{\langle f,g \rangle_\Delta^2}{\|f\|_\Delta^2 \|g\|_\Delta^2}}.$$

The condition $f(\zeta) = 0, g(\zeta) = 0, \|\zeta\| = 1, rank(T_\zeta g) \leq r-1$ can be expressed as the vanishing of one real equation and $2n + \binom{n+1}{r}\binom{n}{r}$ complex equations of degree at most nd. This is equivalent to the vanishing of 1 real equation of degree at most $2nd$. Moreover, the condition $d_{\mathbf{P}}(f,g) < \varepsilon$ can be expressed as an inequality of degree 4. Thus, $\mathcal{S}_\varepsilon$ is the $2N + 2n + 4$–projection of an $(2, 2nd)$–definable algebraic set, as wanted. The theorem follows from Theorem 10 and Theorem 2. □

References

Arnold, V., Varchenko, A., Goussein-Zadé, S., 1986. Singularités des aplications différentiables. Éditions Mir, Moscou.

Beltrán, C., Pardo, L., 2006a. Estimates on the distribution of the condition number of singular matrices. Found. Comput. Math. To appear.

Beltrán, C., Pardo, L., 2006b. On Smale's 17th problem: A uniform algorithm in probabilistic polynomial time. Found. Comput. Math. Submitted.

Beltrán, C., Pardo, L., 2006c. On the complexity of non–universal polynomial equation solving: old and new results. In: Foundations of Computational Mathematics: Santander 2005. L. Pardo, A. Pinkus, E. Süli, M. Todd editors. Cambridge University Press, pp. 1–35.

Beltrán, C., Pardo, L. M., 2005. Upper bounds on the distribution of the condition number of singular matrices. C. R. Math. Acad. Sci. Paris 340 (12), 915–919.

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

Bruns, W., Vetter, U., 1988. Determinantal rings. Vol. 1327 of Lecture Notes in Mathematics. Springer-Verlag, Berlin.

Castro, D., Montaña, J. L., Pardo, L. M., San Martín, J., 2002. The distribution of condition numbers of rational data of bounded bit length. Found. Comput. Math. 2 (1), 1–52.

Castro, D., Pardo, L. M., Hägele, K., Morais, J. E., 2001. Kronecker's and Newton's approaches to solving: a first comparison. J. Complexity 17 (1), 212–303.

Castro, D., Pardo, L. M., San Martín, J., 2003. Systems of rational polynomial equations have polynomial size approximate zeros on the average. J. Complexity 19 (2), 161–209.

Dedieu, J.-P., 1996. Approximate solutions of numerical problems, condition number analysis and condition number theorem. In: The mathematics of numerical analysis (Park City, UT, 1995). Vol. 32 of Lectures in Appl. Math. Amer. Math. Soc., Providence, RI, pp. 263–283.

Dedieu, J.-P., Shub, M., 2001. On simple double zeros and badly conditioned zeros of analytic functions of n variables. Math. Comp. 70 (233), 319–327.

Elezović, N., Giordano, C., Pečarić, J., 2000. The best bounds in Gautschi's inequality. Math. Inequal. Appl. 3 (2), 239–252.

Fulton, W., 1984. Intersection theory. Vol. 2 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Springer-Verlag, Berlin.

Giusti, M., Heintz, J., Hägele, K., Montaña, J. L., Morais, J. E., Pardo, L. M., 1997a. Lower bounds for Diophantine approximations. J. Pure Appl. Algebra 117/118, 277–317.

Giusti, M., Heintz, J., Morais, J. E., Morgenstern, J., Pardo, L. M., 1998. Straight-line programs in geometric elimination theory. J. Pure Appl. Algebra 124 (1-3), 101–146.

Giusti, M., Heintz, J., Morais, J. E., Pardo, L. M., 1995. When polynomial equation systems can be "solved" fast? In: Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995). Vol. 948 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 205–231.

Giusti, M., Heintz, J., Morais, J. E., Pardo, L. M., 1997b. Le rôle des structures de données dans les problèmes d'élimination. C. R. Acad. Sci. Paris Sér. I Math. 325 (11), 1223–1228.

Giusti, M., Lecerf, G., Salvy, B., Yakoubsohn, J., 2005a. On location and approximation of clusters of zeros: case of embedding dimension one. Found. Comp. Mathematics to appear.

Giusti, M., Lecerf, G., Salvy, B., Yakoubsohn, J.-C., 2005b. On location and approximation of clusters of zeros of analytic functions. Found. Comput. Math. 5 (3), 257–311.

Hardy, G. H., Wright, E. M., 1979. An introduction to the theory of numbers, 5th Edition. The Clarendon Press Oxford University Press, New York.

Heintz, J., 1983. Definability and fast quantifier elimination in algebraically closed fields. Theoret. Comput. Sci. 24 (3), 239–277.

Kahan, W., 2000. Huge generalized inverses of rank-deficient matrices., unpublished Manuscript.

Kunz, E., 1985. Introduction to commutative algebra and algebraic geometry. Birkhäuser Boston Inc., Boston, MA.

Malajovich, G., 1993. On the complexity of path-following Newton algorithms for solving systems of polynomial equations with integer coefficients. PhD Thesis. Univ. Rio de Janeiro.

Pardo, L. M., 1995. How lower and upper complexity bounds meet in elimination theory. In: Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995). Vol. 948 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 33–69.

Shafarevich, I. R., 1994. Basic algebraic geometry. 1, 2nd Edition. Springer-Verlag, Berlin.

Shub, M., Smale, S., 1993a. Complexity of Bézout's theorem. I. Geometric aspects. J. Amer. Math. Soc. 6 (2), 459–501.

Shub, M., Smale, S., 1993b. Complexity of Bezout's theorem. II. Volumes and probabilities. In: Computational algebraic geometry (Nice, 1992). Vol. 109 of Progr. Math. Birkhäuser Boston, Boston, MA, pp. 267–285.

Shub, M., Smale, S., 1994. Complexity of Bezout's theorem. V. Polynomial time. Theoret. Comput. Sci. 133 (1), 141–164, selected papers of the Workshop on Continuous Algorithms and Complexity (Barcelona, 1993).

Shub, M., Smale, S., 1996. Complexity of Bezout's theorem. IV. Probability of success; extensions. SIAM J. Numer. Anal. 33 (1), 128–148.

Stewart, G. W., Sun, J. G., 1990. Matrix perturbation theory. Computer Science and Scientific Computing. Academic Press Inc., Boston, MA.

Turing, A. M., 1948. Rounding-off errors in matrix processes. Quart. J. Mech. Appl. Math. 1, 287–308.