Computing the Homology of Basic Semialgebraic Sets in Weak Exponential Time

Peter Bürgisser, Felipe Cucker, Pierre Lairez

Computing the Homology of Basic Semialgebraic Sets in Weak Exponential Time

PETER BÜRGISSER, Technische Universität Berlin, Germany
FELIPE CUCKER, City University of Hong Kong
PIERRE LAIREZ, Inria, France

We describe and analyze an algorithm for computing the homology (Betti numbers and torsion coefficients) of basic semialgebraic sets which works in weak exponential time. That is, out of a set of exponentially small measure in the space of data, the cost of the algorithm is exponential in the size of the data. All algorithms previously proposed for this problem have a complexity which is doubly exponential (and this is so for almost all data).

CCS Concepts: • **Theory of computation → Computational geometry**; • **Computing methodologies → Hybrid symbolic-numeric methods**.

Additional Key Words and Phrases: Semialgebraic geometry, homology, algorithm

ACM Reference Format:
Peter Bürgisser, Felipe Cucker, and Pierre Lairez. 2018. Computing the Homology of Basic Semialgebraic Sets in Weak Exponential Time. *J. ACM* 66, 1, Article 5 (December 2018), 30 pages. https://doi.org/10.1145/3275242

1 INTRODUCTION

Semialgebraic sets (that is, subsets of Euclidean spaces defined by polynomial equations and inequalities with real coefficients) come in a wide variety of shapes and this raises the problem of describing a given specimen, from the most primitive features, such as emptiness, dimension, or number of connected components, to finer ones, such as roadmaps, Euler-Poincaré characteristic, Betti numbers, or torsion coefficients.

The *Cylindrical Algebraic Decomposition* (CAD) introduced by Collins [23] and Wüthrich [63] in the 1970's provided algorithms to compute these features that worked within time $(sD)^{2^{O(n)}}$ where s is the number of defining equations, D a bound on their degree and n the dimension of the ambient space. Subsequently, a substantial effort was devoted to design algorithms for these problems with *single exponential* algebraic complexity bounds [4, and references therein], that is, bounds of the form $(sD)^{n^{O(1)}}$. Such algorithms have been found for deciding emptiness [6, 37, 49], for counting connected components [7, 19, 20, 38, 39], computing the dimension [9, 41], the Euler-Poincaré characteristic [2], the first few Betti numbers [3], the top few Betti numbers [5] and roadmaps (embedded curves with certain topological properties) [11, 21, 50].

As of today, however, no single exponential algorithm is known for the computation of the whole sequence of the homology groups (Betti numbers and torsion coefficients). For complex smooth projective varieties, Scheiblechner [52] has been able to provide an algorithm computing the Betti numbers (but not the torsion coefficients) in single exponential time relying on the algebraic De Rham cohomology. The same author provided a lower bound for this problem (assuming integer coefficients) in [51], where the problem is shown to be PSpace-hard.

5

Authors' addresses: Peter Bürgisser, Technische Universität Berlin, Institut für Mathematik, Germany, pbuerg@math.tu-berlin.de; Felipe Cucker, City University of Hong Kong, Department of Mathematics, Hong Kong, macucker@cityu.edu.hk; Pierre Lairez, Inria, France, pierre.lairez@inria.fr.

Another line of research, that has developed independently of the results just mentioned, focuses on the complexity and the geometry of numerical algorithms [18, and references therein]. The characteristic feature of these algorithms is the use of approximations and successive refinements. For most problems, a set of *numerically ill-posed* data can be identified, for which arbitrarily small perturbations may produce qualitative errors in the result of the computation. Iterative numerical algorithms may run forever on ill-posed data, and may take increasingly long running time as data become close to ill-posed. The running time is therefore not bounded by a function on the input size only and the usual worst-case analysis is irrelevant. An alternate form of analysis, championed by Smale [60] and going back to [40], bounds the running time of an algorithm in terms of the size of the input and a *condition number*, usually related to, or bounded by, the inverse to the distance of the data at hand to the set of ill-posed data.

Then, the most common way to gauge the complexity of a numerical algorithm is to endow the space of data with a probability measure, usually the standard Gaussian, and to analyze the algorithm's cost in probabilistic terms. More often than not, this analysis results in a bound on the expectation of the cost, that is, in an *average-case analysis*. But recently, Amelunxen and Lotz [1] introduced a new way of measuring complexity. They noticed that a number of algorithms that are known to be efficient in practice have nonetheless a large, or even infinite, average-case complexity. One of the reasons they identified for this discrepancy is the exponentially fast vanishing measure of an exceptional set of inputs on which the algorithm runs in superpolynomial time when the dimension grows. A prototype of this phenomenon is the behavior of the power method to compute a dominant eigenpair of a symmetric matrix. This algorithm is considered efficient in practice, yet it has been shown that the expectation of the number of iterations performed by the power method, for matrices drawn from the orthogonal ensemble, is infinite [42]. Amelunxen and Lotz show that, conditioned to exclude a set of exponentially small measure, this expectation is $O(n^2)$ for $n \times n$ matrices. The moral of the story is that the power method is efficient in practice because it is so in theory if we disregard a vanishingly small set of outliers. This conditional expectation, in the terminology of [1], shows a *weak average polynomial cost* for the power method. More generally, we will talk about a complexity bound being *weak* when this bound holds out of a set of exponentially small measure.

Several problems related to semialgebraic sets have been studied from the numerical point of view we just described, such as deciding emptiness [29], counting real solutions of zero-dimensional systems [26], or computing the homology groups of real projective sets [28]. Our main result follows this stream.

Main result. A *basic semialgebraic set* is a subset of a Euclidean space $\mathbb{R}^n$ given by a system of equalities and inequalities of the form

$$f_1(x) = \cdots = f_q(x) = 0 \text{ and } g_1(x) \succ 0, \ldots, g_s(x) \succ 0 \tag{1}$$

where $F = (f_1, \ldots, f_q)$ and $G = (g_1, \ldots, g_s)$ are tuples of polynomials with real coefficients and the expression $g(x) \succ 0$ stands for either $g(x) \geqslant 0$ or $g(x) > 0$ (we use this notation to emphasize the fact, that will become clear in §4.1.4, that our main result does not depend on whether the inequalities in (1) are strict). Let $W(F, G)$ denote the solution set of the semialgebraic system (1).

For a vector $\boldsymbol{d} = (d_1, \ldots, d_{q+s})$ of $q + s$ positive integers, we denote by $\mathcal{P}_{\boldsymbol{d}}$ (or $\mathcal{P}_{\boldsymbol{d}}[q\,;\, s]$ to emphasize the number of components) the linear space of the $(q + s)$-tuples of real polynomials in n variables of degree at most $d_1, \ldots, d_{q+s}$, respectively. Let D denote the maximum of the d_i. We will assume that $D \geqslant 2$ because a set defined by degree 1 polynomials is convex and its homology is trivial. Let N denote the dimension of $\mathcal{P}_{\boldsymbol{d}}$, that is,

$$N = \sum_{i=1}^{q+s} \binom{n+d_i}{n}. \tag{2}$$

This is the *size* of the semialgebraic system (1), as it is the number of real coefficients necessary to determine it. We endow $\mathcal{P}_{\boldsymbol{d}}$ with the Weyl inner product and its induced norm, see §4.1. We further endow $\mathcal{P}_{\boldsymbol{d}}$ with the standard Gaussian measure given by the density $(2\pi)^{-\frac{N}{2}} \exp\left(-\frac{\|(F,G)\|^2}{2}\right)$ (we note, however, that we could equivalently work with the uniform distribution on the unit sphere in $\mathcal{P}_{\boldsymbol{d}}$). Finally, we distinguish a subset Σ_*^{aff} of $\mathcal{P}_{\boldsymbol{d}}[q\,;\,s]$ of ill-posed data (see §4.1.5 for a precise definition). Pairs (F,G) on this set are those for which the Zariski closure in $\mathbb{R}^n$ of one of the algebraic sets defining the boundary of $W(F,G)$ is not smooth. We will see that Σ_*^{aff} is a hypersurface in $\mathcal{P}_{\boldsymbol{d}}[q\,;\,s]$ and hence has measure zero.

The complexity model we consider is the usual Blum–Shub–Smale model [13] extended (as often) with the ability to compute square roots. What we call "numerical algorithm" is a machine in this model.

Theorem 1.1. *There is a numerical algorithm* Homology *that, given a system $(F,G) \in \mathcal{P}_{\boldsymbol{d}}$ with $q \leqslant n$ equalities and s inequalities, computes the homology groups of $W(F,G)$. Moreover, the number of arithmetic operations in $\mathbb{R}$ performed by* Homology *on input (F,G), denoted* $\operatorname{cost}(F,G)$, *satisfies*

(i) $\operatorname{cost}(F,G) = \left((s+n)D\delta^{-1}\right)^{O(n^2)}$ *where δ is the distance of $\frac{1}{\|(F,G)\|}(F,G)$ to Σ_*^{aff}.*

Furthermore, if (F,G) is drawn from the Gaussian measure on $\mathcal{P}_{\boldsymbol{d}}$, then

(ii) $\operatorname{cost}(F,G) \leqslant \left((s+n)D\right)^{O(n^3)}$ *with probability at least* $1 - \left((s+n)D\right)^{-n}$

(iii) $\operatorname{cost}(F,G) \leqslant 2^{O(N^2)}$ *with probability at least* $1 - 2^{-N}$.

The algorithm is numerically stable.

Nota bene. The notation O will always be understood with respect to N. For example, the bound $\operatorname{cost}(F,G) \leqslant \left((s+n)D\delta^{-1}\right)^{O(n^3)}$ rewords as $\operatorname{cost}(F,G) \leqslant \left((s+n)D\delta^{-1}\right)^{Cn^3}$ for some $C > 0$ as soon as N is large enough, even if some of the parameters s, n or D are fixed.

Point (ii) above does not imply, strictly speaking, weak exponential time because for given n, q, s and $\boldsymbol{d}$, the measure of the exceptional set is bounded by $\left((s+n)D\right)^{-n}$ and this may not be exponentially small in the input size N (for instance, when n is fixed and D and s grow). But Point (iii) shows exactly what we can call *weak exponential complexity*: out of an exponentially small set in the space of data the cost of the latter is bounded by a single exponential function on the input size.

It is difficult to compare our algorithm with previous ones: because of its numeric nature, it only deals with the generic case, at positive distance from ill-posed problems, and its worst-case complexity is unbounded. Nevertheless, it compares favorably with the doubly exponential worst-case bound obtained from the CAD. The latter is reached on generic inputs, whereas we show a single exponential worst-case complexity outside a vanishingly small subset. Another difference with previous works is the fact that our results are valid only for polynomials with real coefficients as our proofs use some analytical techniques. This is in contrast with, for instance, the work by Basu [3, 5] where the results are valid for semialgebraic sets defined over arbitrary real closed fields.

In this work, we approach the topology of a set by approximating it by a union of Euclidean balls in the ambient space, as initiated in the field of topological data analysis [32, e.g.]. Following ideas in [22, 47], for the coverings, we choose a union of balls of sufficiently small radius to which we can apply the Nerve Theorem. In constrast, previous work by Basu et al. [3, 8, 10], with a more algebraic flavor, approaches the topology from inside by computing covering by contractible subsets of the original set.

Lastly, we note that all the ingredients in algorithm Homology easily parallelize. Doing so, we obtain a parallel algorithm working in *weak parallel polynomial complexity*: out of an exponentially small set in the space of data the parallel cost of the algorithm is bounded by a polynomial function on the input size. The PSpace-hardness result by Scheiblechner [51] mentioned above (together with the classical equivalence between space and parallel time [14]) suggests that further complexity improvements are limited as they are unlikely to be below parallel polynomial time.

Overview. This article follows some algorithmic ideas (grid methods, theory of point estimates) introduced by Cucker and Smale [29] and extended by Cucker et al. [26, 28]. In particular, an algorithm for computing the homology of a real *algebraic* subset of $\mathbb{S}^n$ (defined with only equalities, as opposed to *semialgebraic* sets) has been studied in [28]. The spirit and the statement of our main result is very close to this previous work but the methods are substantially renewed. There is a significant overlap with [28] where we felt that the theory could be simplified (§3.3 and §4.1.2), but the specificity of the semialgebraic case called for the application of different tools, such as the reach (§2), continuous Newton method (§3.2), or the relaxation of semialgebraic inequalities (§4.2).

Besides, the numerical stability of the algorithm in Theorem 1.1 will not be discussed here. The precise meaning of this stability and its proof are a straightforward variation of the arguments detailed in [28, §7] which in turn are based on those in [26, 29].

Our method relies on several quantities reflecting corresponding aspects of the conditioning of a semialgebraic system. The first one is the *reach*. This is a measure of curvature for sets without the structure of a manifold. The second one measures how much the solution set of a semialgebraic system is affected by small relaxations of the equalities and inequalities of the system. The third one is the condition number κ_* which reflects the distance of a semialgebraic system to the closest ill-posed system. The facts that κ_* bounds the other two measures and that we can compute it efficiently are cornerstones of our algorithm. In a number of respects, this condition number is a natural extension of the first instances of this notion, for systems of linear equations, introduced by Turing [61] and von Neumann and Goldstine [62].

Sections 2, 3 and 4 study all these notions. They decrease in the generality of the context (closed sets, analytic sets, and semialgebraic sets, respectively) but increase on the computational use of the results.

In a few words, to compute the homology group of an arbitrary basic semialgebraic set W, we first reduce to the case of a closed semialgebraic subset S of a sphere $\mathbb{S}^n$. Then we gather a finite set $\mathcal{X}$ of points in $\mathbb{S}^n$ that is sufficiently dense and retain only the points that are close enough to S. A point is close enough to S if it satisfies the defining equations and inequalities of S up to some ε. Extending a theorem of Niyogi, Smale and Weinberger [48], we argue that this finite set of close enough points is sufficient to compute the homology of S. The condition number κ_* acts as a master parameter: it controls the meaning of "sufficiently dense" and "close enough" and, beyond that, the total complexity of the algorithm and the required precision to run it.

Besides the main result, this work features several notable contributions. First, an extension to sets with positive reach of the Niyogi-Smale-Weinberger theorem about the computation of the homotopy type of a set via an approximation with a finite set (Theorem 2.8). Second, a continuous analogue of Shub and Smale's α-Theorem in which Newton's iteration is replaced with Newton's flow (Theorem 3.1). Third, an inequality relating the reach and the γ-number at a point of a real analytic set (Theorem 3.3). This strenghtens and simplifies a result of Cucker, Krick and Shub [28]. Four, a theory of the conditioning of a semialgebraic system relating the distance to the closest ill-posed problem to the sensitivity of the solution set to small relaxations of the equalities and inequalities of the system (Theorem 4.19). This is reminiscent of the Eckhart–Young theorem for linear systems.

2 APPROXIMATION OF SETS WITH POSITIVE REACH

The *reach* of a closed subset of a Euclidean space E is a notion introduced by Federer [34] to quantify the curvature of objects without the structure of a manifold. We establish a few useful properties of the reach and we use this notion to extend a theorem of Niyogi, Smale and Weinberger [48] that gives a criterion to compute the topology of a compact subset of an Euclidean space by means of a finite covering of balls with the same radius (Theorem 2.8). It will play a fundamental role in our arguments.

2.1 Measures of curvature

For a nonempty subset $W \subseteq E$ and $x \in E$, we denote by $d_W(x) := \inf_{p\in W} \|x-p\|$ the distance of x to W. We note that the function $d_W : E \to \mathbb{R}$ is 1-Lipschitz continuous, that is, $|d_W(x) - d_W(y)| \leqslant \|x-y\|$ for all $x, y \in E$.

Definition 2.1. Let $W \subseteq E$ be a nonempty closed subset. The *medial axis* of W is defined as the closure of the set

$$\Delta_W := \{x \in E \mid \exists p, q \in W, p \neq q \text{ and } \|x-p\| = \|x-q\| = d_W(x)\}\,.$$

The *reach (or local feature size) of* W *at a point* $p \in W$ is defined as $\tau(W,p) := d_{\Delta_W}(p)$. The *(global) reach of* W is defined as $\tau(W) := \inf_{p\in W} \tau(W,p)$. We also set $\tau(\varnothing) := +\infty$.

Note that $\tau(W)$ is also given by $\inf_{x\in\Delta_W} d_W(x)$. We can also characterize $\tau(W)$ as the supremum of all ε such that for every $x \in E$ with $d_W(x) < \varepsilon$, there exists a unique point $p \in W$ with $\|x-p\| = d_W(x)$. We shall denote this unique point by $\pi_W(x)$. This gives a map $\pi_W : T(W) \to W$, where $T(W) := \left\{x \in E \mid d_W(x) < \tau(W)\right\}$ denotes the open neighborhood of W with radius $\tau(W)$.

When W is a smooth submanifold of E, the reach of W can be characterized in terms of the normal bundle of W as follows. Let $N_\varepsilon(W) := \{(x,v) \in W \times E \mid v \perp T_xW, \|v\| < \varepsilon\}$ denote the open normal bundle of W with radius ε. The reach $\tau(W)$ is the supremum of all ε such that the map $N_\varepsilon(W) \to T(W)$, $(x,v) \mapsto x+v$, is injective [48].

Proposition 2.2. *If* $\tau(W) > 0$, *then* $\pi_W : T(W) \to W$ *is continuous and the map*

$$T(W) \times [0,1] \to T(W),\ (x,t) \longmapsto t\pi_W(x) + (1-t)x$$

is a deformation retract of $T(W)$ *onto* W.

Proof. Concerning the continuity of π_W, let $(x_k)_{k\geqslant 0}$ be a sequence in $T(W)$ converging to some $x \in T(W)$. We have

$$\|\pi_W(x_k) - x\| \leqslant \|\pi_W(x_k) - x_k\| + \|x_k - x\| = d_W(x_k) + \|x_k - x\| \leqslant d_W(x) + 2\|x_k - x\|,$$

where we used the Lipschitz continuity of d_W for the last inequality. Hence the sequence $\pi_W(x_k)$ is bounded. Let $y \in W$ be a limit point of $\pi_W(x_k)$. The above inequality implies that $\|y-x\| \leqslant d_W(x)$, hence $y = \pi_W(x)$. Thus $\pi_W(x)$ is the only limit point of the sequence $\pi_W(x_k)$ and therefore, $\lim_{k\to\infty} \pi_W(x_k) = \pi_W(x)$.

The second claim is obvious. □

We will use the following well-known fact.

Lemma 2.3. *Assume there is an open neighborhood* U *of* $\pi_W(x)$, $x \in E$, *such that* $W \cap U$ *is a smooth submanifold of* E. *Then* $\pi_W(x) - x$ *is normal to the tangent space of* W *at* $\pi_W(x)$. □

The main result of this section is a lower bound on the reach of an intersection $W \cap V$ in terms of the reach of W and the reach of the intersection of W with the boundary ∂V of V.

THEOREM 2.4. *For closed subsets V, W of E we have $\tau(W \cap V) \geqslant \min(\tau(W), \tau(W \cap \partial V))$.*

For the proof, we introduce an auxiliary notion. Let $W \subseteq E$ be a closed subset and $p \in W$. Moreover, consider $u \in E$ with $\|u\| = 1$. It is easy to see that $\{t \geqslant 0 \mid d_W(p + tu) = t\}$ is an interval containing 0. We are interested in those directions u, where this interval has positive length and define the *reach $\tau(W, p, u)$ of W at p along direction u* as the length of this interval, that is,

$$\tau(W, p, u) := \sup \{t \geqslant 0 \mid d_W(p + tu) = t\}.$$

We note that $\pi_W(p + tu) = p$ for any $0 \leqslant t < \tau(W, p, u)$. For example, we have $\tau(\mathbb{R}^n_+, 0, u) > 0$ iff u is in the normal cone of $\mathbb{R}^n_+$ at 0, that is, $u_i \leqslant 0$ for all i. In this case, $\tau(\mathbb{R}^n_+, 0, u) = \infty$. The next lemma is a slight variation of a result by Federer [34].

LEMMA 2.5. *Let $W \subseteq E$ be a closed subset, $p \in W$, and $u \in E$ be a unit vector such that $\tau(W, p, u)$ is positive. Then we have $\tau(W, p) \leqslant \tau(W, p, u)$.*

PROOF. The assertion is trivial if $\tau(W, p, u) = \infty$. So assume that $0 < \tau(W, p, u) < \infty$. Federer, in [34, Theorem 4.8(6)] states that under this assumption, the point $x := p + \tau(W, p, u)u$ lies in the closure of Δ_W. Therefore $\tau(W, p) \leqslant \|x - p\| = \tau(W, p, u)$. □

PROOF OF THEOREM 2.4. Let $x \in \Delta_{W\cap V}$ and p and q be distinct points in $W \cap V$ such that $d_{W\cap V}(x) = \|x - p\| = \|x - q\|$. It is sufficient to prove that

$$\|x - p\| \geqslant \min(\tau(W), \tau(W \cap \partial V)), \tag{3}$$

since the assertion then follows by taking the infimum of $\|x - p\|$ over $x \in \Delta_{W\cap V}$.

If both p and q lie in ∂V, then $x \in \Delta_{W\cap\partial V}$ and $\|x - p\| = d_{W\cap V}(x) = d_{W\cap\partial V}(x) \geqslant \tau(W \cap \partial V)$, which implies (3).

So we may assume that one of p and q, say p, does not lie on ∂V, that is, p is an interior point of V. Consider the unit vector $u := \frac{x-p}{\|x-p\|}$ (note that $x \neq p$). We first observe that $\tau(W \cap V, p, u) \leqslant \|x - p\|$, because of the presence of the point q, see Figure 1. Moreover, $\tau(W \cap V, p, u) > 0$ since $d_W(x) = \|x - p\| > 0$. From this we can we deduce that $\tau(W, p, u) > 0$. Indeed, the sets W and $W \cap V$ coincide on a neighborhood of p, hence the distance functions d_W and $d_{W\cap V}$ coincide for points on the segment $[p, x]$ that are sufficiently close to p. Using Lemma 2.5, we then obtain

$$\tau(W) \leqslant \tau(W, p) \leqslant \tau(W, p, u) \leqslant \|x - p\|,$$

which shows (3) and completes the proof. □

We can extend Theorem 2.4 to the intersections of several closed subsets.

COROLLARY 2.6. *For closed subsets $V_1, \ldots, V_s$ and W of E we have*

$$\tau(W \cap V_1 \cap \cdots \cap V_s) \geqslant \min_{I \subseteq \{1,\ldots,s\}} \tau\Big(W \cap \bigcap_{i\in I} \partial V_i\Big).$$

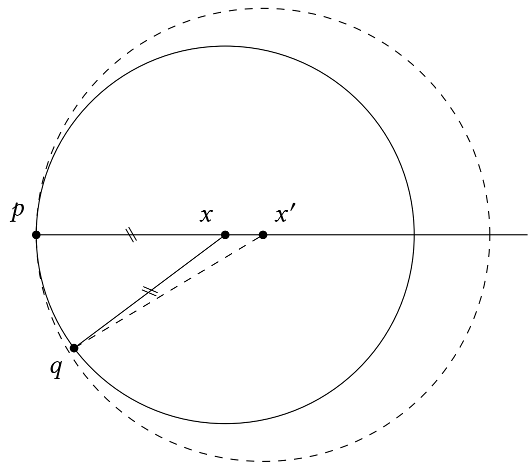

Fig. 1 Illustration of the inequality $\tau(W, p, u) \leqslant \|x - p\|$: A point x' beyond x on the half-line from p to x is closer to q than to p.

Proof. The case $s = 1$ is covered by Theorem 2.4. In general, we argue by induction on s,

$$\begin{aligned}
&\tau(W \cap V_1 \cap \cdots \cap V_{s+1}) \\
&\qquad \geqslant \min\left(\tau(W \cap V_1 \cap \cdots \cap V_s), \tau(W \cap V_1 \cap \cdots \cap V_s \cap \partial V_{s+1})\right) \\
&\qquad \geqslant \min\left(\min_{I \subseteq \{1,\ldots,s\}} \tau\big(W \cap \bigcap_{i \in I} \partial V_i\big), \min_{I \subseteq \{1,\ldots,s\}} \tau\big(W \cap \partial V_{s+1} \cap \bigcap_{i \in I} \partial V_i\big)\right) \\
&\qquad = \min_{I \subseteq \{1,\ldots,s+1\}} \tau\Big(W \cap \bigcap_{i \in I} \partial V_i\Big),
\end{aligned}$$

where we have applied Theorem 2.4 and twice the induction hypothesis. □

We conclude with a relation between the reach of a subset of the unit sphere $\mathbb{S}(E) := \{x \in E \mid \|x\| = 1\}$ and the reach of the cone over it.

Lemma 2.7. *Let $V \subseteq \mathbb{S}(E)$ be closed and $\widehat{V} = \mathbb{R} \cdot V$ be the closed cone in E spanned by V. For any $p \in V$, we have $\tau(V, p) \geqslant \min\{\tau(\widehat{V}, p), 1\}$.*

Proof. We may assume that E equals the span of $\widehat{V}$ because the reach of a subset remains unchanged after restriction to a subspace that contains this subset. It follows from this assumption that, for all $x \in E$, $\pi_{\widehat{V}}(x) = 0$ if and only if $x = 0$.

Elementary geometry shows that for all $x \in E$, whenever $\pi_{\widehat{V}}(x)$ is well-defined and not zero, then $\pi_V(x)$ is well-defined and

$$\pi_V(x) = \frac{\pi_{\widehat{V}}(x)}{\|\pi_{\widehat{V}}(x)\|}.$$

Now let $p \in V$. Recall that the reach $\tau(V, p)$ is the supremum of all $r > 0$ such that π_V is well-defined on $B(p, r)$.

Consider any $r < \min\{\tau(\widehat{V}, p), 1\}$ and let $x \in B(p, r)$. As $r < 1$ we have $x \neq 0$, and as $r < \tau(\widehat{V}, p)$, we have that $\pi_{\widehat{V}}(x)$ is well-defined and not zero (as $x \neq 0$). Which, as we noted above, implies that $\pi_V(x)$ is well-defined. This shows that π_V is well-defined on all of $B(p, r)$ for all $r < \min\{\tau(\widehat{V}, p), 1\}$, from where the claim follows. □

2.2 An extension of the Niyogi-Smale-Weinberger theorem

Again, we work in a Euclidean vector space E. By the *(open) neighborhood* of radius $r \geqslant 0$ around a nonempty set $S \subseteq E$ we understand the set

$$\mathcal{U}(S, r) := \{p \in E \mid d_S(p) < r\}.$$

Niyogi, Smale and Weinberger [48, Prop. 7.1] gave an answer to the following question: given a compact submanifold $S \subseteq E$, a finite set $\mathcal{X} \subset E$ and $\varepsilon > 0$, which conditions do we need to ensure that S is a deformation retract of $\mathcal{U}(\mathcal{X}, \varepsilon)$?

In what follows, we observe their arguments extend to any compact subsets $S, \mathcal{X}$ provided S has positive reach $\tau(S)$. The proof is a variation of the original proof. A much more general extension [22] of the Niyogi-Smale-Weinberger theorem includes our, with slightly worse constants and, naturally, at the cost of a more involved proof.[1]

The *Hausdorff distance* between two nonempty closed subsets $A, B \subseteq E$ is defined as

$$d_H(A, B) := \max\left(\sup_{a \in A} d_B(a), \sup_{b \in B} d_A(b)\right).$$

Theorem 2.8. *Let S and $\mathcal{X}$ be nonempty compact subsets of E. The set S is a deformation retract of $\mathcal{U}(\mathcal{X}, \varepsilon)$ for any ε such that $3\, d_H(S, \mathcal{X}) < \varepsilon < \frac{1}{2}\tau(S)$.*

Proof. For any $x \in \mathcal{U}(\mathcal{X}, \varepsilon)$ we have

$$d(x, S) \leqslant d(x, \mathcal{X}) + d_H(\mathcal{X}, S) < \tfrac{4}{3}\varepsilon < \tau(S),$$

hence $\mathcal{U}(\mathcal{X}, \varepsilon) \subseteq T(S)$. This shows that the map

$$\mathcal{U}(\mathcal{X}, \varepsilon) \times [0, 1] \to E, \quad (x, t) \longmapsto (1 - t)x + t\pi_S(x)$$

is well-defined. The map is also continuous (Proposition 2.2). It remains to prove that its image is included in $\mathcal{U}(\mathcal{X}, \varepsilon)$, that is, for any $v \in \mathcal{U}(\mathcal{X}, \varepsilon)$ the line segment $[v, \pi_S(v)]$ is included in $\mathcal{U}(\mathcal{X}, \varepsilon)$. The argument involves seven points depicted in Figure 2.

Let $v \in \mathcal{U}(\mathcal{X}, \varepsilon)$ and $p := \pi_S(v)$. By definition, there is some $x \in \mathcal{X}$ such that $\|v - x\| < \varepsilon$. If $\|p - x\| < \varepsilon$, then the line segment $[v, p]$ is entirely included in the ball of radius ε around x, which is a part of $\mathcal{U}(\mathcal{X}, \varepsilon)$, and we are done. So we assume that $\|p - x\| \geqslant \varepsilon$. Let u be the unique point in $[v, p]$ such that $\|u - x\| = \varepsilon$. The line segment $[v, u)$ being included in the ball $B(x, \varepsilon) \subseteq \mathcal{U}(\mathcal{X}, \varepsilon)$, it only remains to check that $[u, p]$ is also included in $\mathcal{U}(\mathcal{X}, \varepsilon)$.

Let $r := \frac{1}{3}\varepsilon$. Also, let ℓ be the open half-line starting from p and passing through v and w be the unique point in ℓ such that $\|w - p\| = 6r$. Our assumption states that $6r = 2\varepsilon < \tau(S)$. Also, as $p = \pi_S(v)$, we have $\tau\big(S, p, \frac{w-p}{\|w-p\|}\big) > 0$. By Lemma 2.5, we obtain $\tau(S) \leqslant \tau(S, p) \leqslant \tau\big(S, p, \frac{w-p}{\|w-p\|}\big)$, and therefore $6r < \tau\big(S, p, \frac{w-p}{\|w-p\|}\big)$. This implies that $\pi_S(w) = p$ and $d_S(w) = \|w - p\| = 6r$.

Let $q := \pi_S(x)$. We first note that $\|x - q\| \leqslant r$ because $d_S(x) \leqslant d_H(\mathcal{X}, S) < r$ by our assumption. Next we have

$$\|w - x\| \geqslant \|w - q\| - \|q - x\| \geqslant 5r, \tag{4}$$

because $\|w - q\| \geqslant d_S(w) = 6r$.

Since $d_H(\mathcal{X}, S) \leqslant r$, there is a point $y \in \mathcal{X}$ such that $\|y - p\| \leqslant r$. To conclude the proof, it is enough to prove that $[u, p] \subseteq B(y, \varepsilon)$; since $\|y - p\| \leqslant r < \varepsilon$, it is sufficient to check that $\|y - u\| < \varepsilon$. By the triangle inequality,

$$\|y - u\| \leqslant \|y - p\| + \|p - u\| \leqslant r + \|w - p\| - \|w - u\| = 7r - \|w - u\|. \tag{5}$$

Furthermore, the triangle (xuv) has an acute angle at u, because u is on a sphere of center x and v lies inside this sphere; the same holds true for the triangle (xuw) because u, v and w are on the

[1] We thank Théo Lacombe and a referee for raising this point.

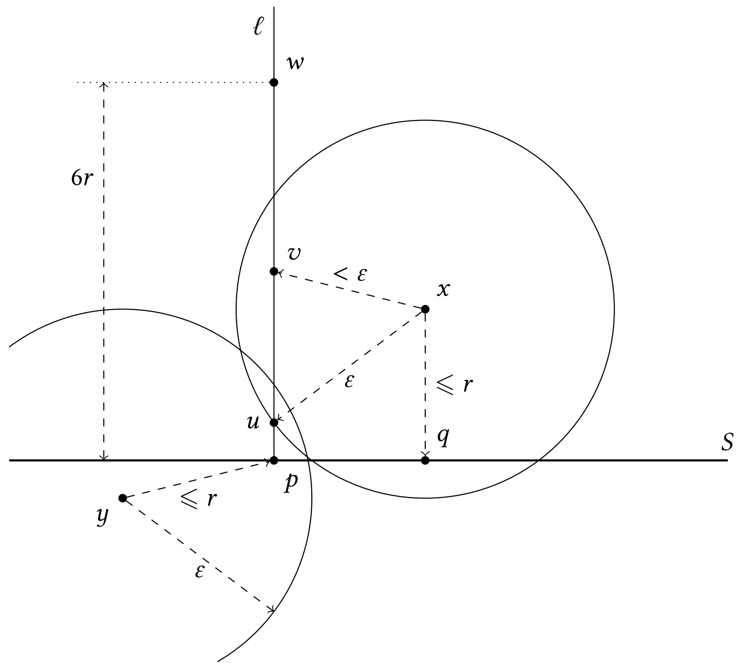

Fig. 2 Schematic view of the proof of Theorem 2.8

same line, in this order (cf. Figure 2). It follows that $\|w-u\|^2 \geqslant \|w-x\|^2 - \|x-u\|^2 > (5r)^2 - \varepsilon^2$, where we used (4) for the second inequality. Therefore, with (5),

$$\|y-u\| < 7r - \sqrt{25r^2 - \varepsilon^2} = 3r = \varepsilon, \tag{6}$$

which concludes the proof. □

3 SHUB–SMALE THEORY AND EXTENSIONS

We recall the definition and basic properties of quantities (α, β and γ numbers) introduced by Shub and Smale to study the complexity of numerical methods for solving polynomial systems. We prove two results. First, an analogue of the α-Theorem for the continuous Newton method, where a continuous Newton's flow replaces the discrete sequence obtained with Newton's iteration. Second, an inequality relating the reach and the γ-number. It strengthens and simplifies a result of Cucker, Krick and Shub [28], for it is pointwise whereas the latter is only global.

3.1 Measures of proximity

Let E be a Euclidean space and $F \colon E \to \mathbb{R}^m$ be an analytic map such that $m \leqslant \dim E$. It is well-known that, under certain conditions, the (Moore-Penrose) Newton iteration with initial point x_0, given by

$$x_{k+1} := x_k - \mathrm{D}F(x_k)^\dagger F(x_k) \tag{7}$$

is well-defined for all $k \geqslant 0$ and converges quadratically fast to a zero ζ of F. In this case, we say that x_0 is an *approximate zero* of F with *associated zero* ζ (see [18, Def. 15.1] for the formal definition). Here $\mathrm{D}F(x)^\dagger \colon \mathbb{R}^m \to E$ is the *Moore-Penrose inverse* of the full-rank matrix $\mathrm{D}F(x)$ (we say that (7) is undefined if it is not of full rank).

An obvious question is whether we can, for a given x_0, ensure the convergence of Newton's iteration. That is, whether we can check that x_0 is an approximate zero of f. An answer to this question was provided by Smale [59] for the zero-dimensional case ($m = \dim E$) and extended by Shub and Smale [58] to the underdetermined case ($m < \dim E$). They defined the quantities (all norms are the spectral one)

$$\begin{aligned} \gamma(F,x) &:= \sup_{k\geqslant 2} \left\| \tfrac{1}{k!} \mathrm{D}F(x)^\dagger \mathrm{D}^k F(x) \right\|^{\frac{1}{k-1}}, \\ \beta(F,x) &:= \left\| \mathrm{D}F(x)^\dagger F(x) \right\|, \\ \alpha(F,x) &:= \gamma(F,x)\beta(F,x), \end{aligned} \tag{8}$$

and proved that there exists a universal constant $\alpha_\bullet$, around $\frac{1}{8}$, such that if $\alpha(F,x_0) < \alpha_\bullet$ then x_0 is an approximate zero of F. The quantities β and γ are not without meaning themselves. Clearly, $\beta(F,x)$ is the length of the Newton step at x. Also, in the zero-dimensional case, Smale's γ-Theorem shows that, for a zero ζ of F, all points on the ball around ζ with radius $\frac{3-\sqrt{7}}{2\gamma(F,\zeta)}$ are approximate zeros of F.

3.2 Continuous α-theory

While the Shub–Smale theory focuses primarily on the discrete iteration (7), the numbers α and β also give quantitative information on the convergence of the continuous analogue of Newton's iteration. To the best of our knowledge, this has never been highlighted before.

We consider again a point x_0 in E such that $\mathrm{D}F(x_0)$ is surjective. We define x_t with the following system of ordinary differential equations, for t in the maximal domain of solution containing 0,

$$\dot{x}_t = -\mathrm{D}F(x_t)^\dagger F(x_t), \tag{9}$$

where $\dot{x}_t$ denotes $\frac{\mathrm{d}}{\mathrm{d}t} x_t$. We also denote $\alpha_t := \alpha(F, x_t)$ and β_t and γ_t accordingly. It may be that γ_t (and thus α_t) is not differentiable everywhere. However, γ_t is at least locally Lipschitz continuous (cf. Lemma 3.2), which implies absolute continuity and, in turn, that γ_t is differentiable almost everywhere and that $\gamma_t - \gamma_0 = \int_0^t \dot{\gamma}_t \mathrm{d}t$ [46, IX§4]. This regularity is good enough for our purposes. In all our arguments below, at a point t where γ_t is not differentiable, an inequality like $\dot{\gamma}_t \leqslant 5\gamma_t^2 \beta_t$ actually means

$$\limsup_{\varepsilon\to 0} \frac{\gamma_{t+\varepsilon} - \gamma_t}{\varepsilon} \leqslant 5\gamma_t^2 \beta_t.$$

The *domain of definition* Ω of the differential equation is the open set of all $x \in E$ such that $\mathrm{D}F(x)$ is surjective.

Theorem 3.1. *If $\alpha_0 < \frac{1}{13}$, then x_t is defined for all $t \geqslant 0$ and*

(i) $F(x_t) = F(x_0)e^{-t}$;
(ii) $\|x_t - x_0\| \leqslant 2\beta_0(1 - e^{-t})$;
(iii) x_t converges when $t \to \infty$.

Lemma 3.2. *For all $t \geqslant 0$ where x_t is defined, we have (i) $\|\dot{x}_t\| = \beta_t$, (ii) $\dot{\gamma}_t \leqslant 5\gamma_t^2\beta_t$, (iii) $t \mapsto \gamma_t$ is locally Lipschitz, (iv) $\dot{\beta}_t \leqslant -\beta_t + 3\gamma_t\beta_t^2$, and (v) $\dot{\alpha}_t \leqslant -\alpha_t + 8\alpha_t^2$.*

Proof. (i) It follows from (9).

(ii) Let $y = x_{t+\varepsilon}$ for some small positive ε. Let $u = \|x - y\|\gamma_t = \gamma_t\|\dot{x}_t\|\varepsilon + O(\varepsilon^2)$. By [30, Lemme 131],

$$\gamma(F, y) - \gamma(F, x_t) \leqslant \left(\frac{1}{(1-u)(1-4u+2u^2)} - 1\right)\gamma(F, x_t)$$
$$= 5u\gamma_t + O(\varepsilon^2),$$

so that $\gamma_{t+\varepsilon} - \gamma_t \leqslant 5\gamma_t^2\|\dot{x}_t\|\varepsilon + O(\varepsilon^2)$. With the equality $\|\dot{x}_t\| = \beta_t$, this gives the claim when taking the limit for $\varepsilon \longrightarrow 0$.

(iii) This follows from (ii).

(iv) Let $A_t := \mathrm{D}F(x_t)$, $B_t := A_t^\dagger F(x_t)$, and $P_t := \mathrm{id}_E - A_t^\dagger A_t$ (the orthogonal projection on $\ker A_t$). Then $\dot{A}_t = \mathrm{D}^2F(x_t)(\dot{x}_t)$ and (we drop the index t) [36, Thm. 4.3]

$$\tfrac{\mathrm{d}}{\mathrm{d}t}A^\dagger = -A^\dagger\dot{A}A^\dagger + P(A^\dagger\dot{A})^TA^\dagger.$$

This formula derives from the equality $A^\dagger = A^T(AA^T)^{-1}$ which holds because A is surjective.

Using that $\mathrm{D}F(x)\mathrm{D}F(x)^\dagger = \mathrm{id}_E$ and given the differential equation (9) for x_t, we check that, for any $t \in I$,

$$\tfrac{\mathrm{d}}{\mathrm{d}t}F(x_t) = \mathrm{D}F(x_t)(\dot{x}_t) = -\mathrm{D}F(x_t)\mathrm{D}F(x_t)^\dagger F(x_t) = -F(x_t). \tag{10}$$

Using this equality we deduce that

$$\begin{aligned}\dot{B} &= A^\dagger\tfrac{\mathrm{d}}{\mathrm{d}t}F(x) + \left(\tfrac{\mathrm{d}}{\mathrm{d}t}A^\dagger\right)F(x)\\ &= -A^\dagger F(x) + \left(-A^\dagger\dot{A}A^\dagger + P(A^\dagger\dot{A})^TA^\dagger\right)F(x)\\ &= -B + \left[-\mathrm{D}F(x)^\dagger\mathrm{D}^2F(x)(\dot{x}) + P(\mathrm{D}F(x)^\dagger\mathrm{D}^2F(x)(\dot{x}))^T\right]B.\end{aligned}$$

Let C denote the operator inside the square brackets. Since the two terms in C have orthogonal images, we easily obtain

$$\|C\| \leqslant \sqrt{2}\,\|\mathrm{D}F(x)^\dagger\mathrm{D}^2F(x)(\dot{x})\| \leqslant 2\sqrt{2}\gamma\|\dot{x}\| < 3\gamma\beta.$$

Since $\dot{\beta}_t = \frac{1}{\beta_t}\langle\dot{B}_t, B_t\rangle$, we obtain item (iv).

(v) From the previous inequalities,

$$\dot{\alpha}_t = \dot{\gamma}_t\beta_t + \gamma_t\dot{\beta}_t \leqslant 8\gamma_t^2\beta_t^2 - \gamma_t\beta_t,$$

which is exactly the claim. □

Proof of Theorem 3.1. Let $I = [0, \tau)$ be the maximum domain of solution of the differential equation (9) with the fixed initial condition x_0. We will shortly see that $\tau = \infty$.

By Equation (10) we have that, for any $t \in I$, $\frac{\mathrm{d}}{\mathrm{d}t}F(x_t) = -F(x_t)$. This gives the first claim.

After some calculation, using Lemma 3.2(v), we check that $\frac{\mathrm{d}}{\mathrm{d}t}\frac{e^{-t}}{\alpha_t} \geqslant -8e^{-t}$. It follows that for $t \in I$,

$$\alpha_t \leqslant \frac{\alpha_0 e^{-t}}{1 - 8\alpha_0}. \tag{11}$$

After some calculation, using Lemma 3.2(iv), we obtain that $\frac{\mathrm{d}}{\mathrm{d}t}\log\beta_t \leqslant -1 + 3\alpha_t$, and therefore, for $t \in I$,

$$\beta_t \leqslant \beta_0\exp\left(\tfrac{3\alpha_0}{1-8\alpha_0} - t\right) \leqslant 2\beta_0 e^{-t}, \tag{12}$$

where we used that $\alpha_0 \leqslant \frac{1}{13}$ for the second inequality. Using Lemma 3.2(i), we compute that $-\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{\gamma_t} \leqslant 5\beta_t$, and it follows with (11) that for $t \in I$,

$$\gamma_t \leqslant \frac{\gamma_0}{1 - 10\beta_0\gamma_0} \leqslant \tfrac{13}{3}\gamma_0. \tag{13}$$

By Inequality (12) and Lemma 3.2(i), $\|\dot{x}_t\| = \beta_t$ is bounded for $t \in I$. Therefore, if the interval $I = [0,\tau)$ is bounded, then x_t approaches, as $t \to \tau$, a point y in the complement of Ω, the domain of definition of the differential equation [15, IV.5, Th. 2]. Therefore, $\gamma_0\|y-x\| \leqslant 2\beta_0\gamma_0 = 2\alpha_0 < 1-\frac{1}{2}\sqrt{2}$, and [30, Lemme 123] implies that $\mathrm{D}F(y)$ is surjective, which contradicts $y \notin \Omega$. We have thus shown that $\tau = \infty$.

Next, with Lemma 3.2(i), it follows that, for $t \in I$,

$$\|x_t - x_0\| \leqslant \int_0^t \|\dot{x}_s\| \mathrm{d}s \leqslant 2\beta_0(1-e^{-t}).$$

which is the second claim. Similarly, Equation (12) shows that the integral $\int_0^\infty \dot{x}_s \mathrm{d}s$ is absolutely convergent, therefore x_t has a limit when $t \to \infty$. □

3.3 An inequality relating the reach and the γ-number

We keep assuming that E is a Euclidean space and $F\colon E \to \mathbb{R}^m$ an analytic map, with $m \leqslant \dim E$. We will prove the following local inequality, which is a refinement of a result first proved by Cucker, Krick and Shub [28]. The proof is also much simpler.

Theorem 3.3. *Let $\mathcal{M} \subseteq E$ be the zero set of the analytic map $F\colon E \to \mathbb{R}^m$ and $p \in \mathcal{M}$. Then we have $\tau(\mathcal{M},p)\gamma(F,p) \geqslant \frac{1}{14}$ if $\gamma(F,p) < \infty$.*

For $p \in E$ such that $\operatorname{rank} \mathrm{D}F(p) = m$, let $\pi_p\colon E \to E$ denote the orthogonal projection onto the kernel of $\mathrm{D}F(p)$, that is, $\pi_p = \mathrm{id}_E - \mathrm{D}F(p)^\dagger \mathrm{D}F(p)$. Note that if $\gamma(F,p) < \infty$ then locally around p, $\mathcal{M}$ is a smooth manifold and $\ker \mathrm{D}F(p)$ is the tangent space $T_p\mathcal{M}$ at p.

Proposition 3.4. *The derivative of the rational map $\pi\colon E \to \mathrm{End}(E)$, $p \mapsto \pi_p$ at $p \in E$ has an operator norm bounded by $2\gamma(F,p)$. Here $\mathrm{End}(E)$ is endowed with the spectral norm.*

Proof. Let $p \in \mathcal{M}$. The derivative of π at p, $\mathrm{D}\pi(p) : E \to \mathrm{End}(E)$, evaluated at $\dot{p} \in E$ yields [36, Cor. 4.2],

$$\mathrm{D}\pi(p)(\dot{p}) = -\mathrm{D}F(p)^\dagger \cdot \mathrm{D}^2F(p)(\dot{p}) \cdot \pi_p - (\mathrm{D}F(p)^\dagger \cdot \mathrm{D}^2F(p)(\dot{p}) \cdot \pi_p)^T.$$

Since $\left\|\frac{1}{2}\mathrm{D}F(p)^\dagger \mathrm{D}^2F(p)\right\| \leqslant \gamma(F,p)$, by the definition (8) of $\gamma(F,p)$, it follows that $\|D\pi(p)\| \leqslant 4\gamma(F,p)$. We obtain the sharper bound $2\gamma(F,p)$ by observing that $\|A + A^T\| = \|A\|$ for any map $A \in \mathrm{End}(E)$ such that $A^2 = 0$, which holds for $A = \mathrm{D}F(p)^\dagger\, \mathrm{D}^2F(p)(\dot{p})\, \pi_p$. □

It is worth noting that the derivative $\mathrm{D}\pi(p)$ is an incarnation of the second fundamental form $B_p\colon T_p\mathcal{M} \times T_p\mathcal{M} \to T_p\mathcal{M}^\perp$ of $\mathcal{M}$ at p and one can see that $\|\mathrm{D}\pi(p)\| = \|B_p\|$. Proposition 3.4 means that the norm of the second fundamental form of $\mathcal{M}$ at p, a classical measure of curvature in differential geometry, is bounded by $2\gamma(F,p)$. This is related to [48, Prop. 6.1], where this norm is upper bounded by $1/\tau(\mathcal{M})$.

Proof of Theorem 3.3. We fix $p \in \mathcal{M}$ such that $\gamma(p) < \infty$. Since $\tau(p) = \inf_{u \in \Delta_\mathcal{M}} \|u-p\|$, it is enough to prove that $\gamma(p)\|u-p\| \geqslant \frac{1}{14}$ for any given $u \in \Delta_\mathcal{M}$. To shorten notation, we write $\gamma(p)$ for $\gamma(F,p)$.

Let $u \in \Delta_\mathcal{M}$. By definition, there exist distinct points x and y in $\mathcal{M}$ such that $d_\mathcal{M}(u) = \|u-x\| = \|u-y\|$. Using the triangle inequality (three times) we see that

$$\max(\|x-y\|, \|p-x\|, \|p-y\|) \leqslant 2\|u-p\|.$$

Therefore, denoting

$$\eta := \gamma(p)\max(\|x-y\|, \|p-x\|, \|p-y\|),$$

we obtain $\gamma(p)\|u-p\| \geqslant \frac{1}{2}\eta$. If $\eta \geqslant \frac{1}{7}$, then we are done, so we can assume that $\eta < \frac{1}{7}$.

Let $B \subseteq E$ be the ball of center p and radius $\eta/\gamma(p)$ (in particular $x, y \in B$). Since $\eta \leqslant \frac{1}{7}$, γ is bounded on B by $K\gamma(p)$, where $K := \frac{1}{(1-\eta)(1-4\eta+2\eta^2)}$ [30, Lemme 131]. In particular, $\gamma(x)$ and $\gamma(y)$ are finite, so that x and y are regular points of $\mathcal{M}$.

We now give a lower and an upper bound for $\|\pi_x(u-y)\|$. Let $y' = x + \pi_x(y-x)$. By Lemma 2.3, the vector $u - x$ is normal to $\mathcal{M}$ at x, that is $\pi_x(u-x) = 0$; thus $\pi_x(u-y) = x - y'$, and then we have the lower bound

$$\|x-y\| - \|y-y'\| \leqslant \|\pi_x(u-y)\|. \tag{14}$$

Similarly, the vector $u - y$ is normal to $\mathcal{M}$ at y, that is $\pi_y(u-y) = 0$; hence the upper bound

$$\|\pi_x(u-y)\| = \|\pi_x(u-y) - \pi_y(u-y)\| \leqslant \|\pi_x - \pi_y\| \cdot \|u-y\|.$$

Combined with (14), we obtain

$$\|x-y\| - \|y-y'\| \leqslant \|\pi_x - \pi_y\|\|u-y\|. \tag{15}$$

Further, we aim at bounding $\|y-y'\|$. By definition of y', using that $F(x) = F(y) = 0$, and expanding $F(y)$ into a power series at x, we can write

$$\begin{aligned} y - y' &= \mathrm{D}F(x)^\dagger \mathrm{D}F(x)(y-x) - \mathrm{D}F(x)^\dagger F(y) \\ &= \mathrm{D}F(x)^\dagger \mathrm{D}F(x)(y-x) - \mathrm{D}F(x)^\dagger \sum_{k\geqslant 0} \tfrac{1}{k!}\mathrm{D}^k F(x)(y-x,\ldots,y-x) \\ &= -\sum_{k\geqslant 2} \tfrac{1}{k!}\mathrm{D}F(x)^\dagger \mathrm{D}^k F(x)(y-x,\ldots,y-x). \end{aligned}$$

Hence

$$\begin{aligned} \|y-y'\| &\leqslant \sum_{k\geqslant 2} \left\|\tfrac{1}{k!}\mathrm{D}F(x)^\dagger \mathrm{D}^k F(x)\right\| \|y-x\|^k \\ &\leqslant \|y-x\| \sum_{k\geqslant 2} \big(\gamma(x)\|y-x\|\big)^{k-1} \\ &= \frac{\gamma(x)\|x-y\|^2}{1-\gamma(x)\|x-y\|} \leqslant \frac{K\eta}{1-K\eta}\|x-y\|, \end{aligned} \tag{16}$$

the last inequality following from $\gamma(x)\|x-y\| \leqslant K\gamma(p)\|x-y\| \leqslant K\eta$ and the monotonicity of the function $t \mapsto t/(1-t)$.

Lastly, we bound $\|\pi_x - \pi_y\|$. By Proposition 3.4, we can upper bound

$$\|\pi_x - \pi_y\| \leqslant \sup_{z\in[x,y]} \|\mathrm{D}\pi(z)\| \cdot \|x-y\| \leqslant \sup_{z\in[x,y]} 2\gamma(z) \cdot \|x-y\| \leqslant 2K\gamma(p)\|x-y\|. \tag{17}$$

Combining (15), (16) and (17), we obtain

$$\left(1 - \frac{\eta K}{1-\eta K}\right)\|x-y\| \leqslant 2K\gamma(p)\|x-y\|\,\|u-y\|.$$

Dividing by the nonzero $\|x-y\|$ and noting $\|u-y\| \leqslant \|u-p\|$, this implies

$$\frac{1}{14} \leqslant \frac{1}{2K}\left(1 - \frac{\eta K}{1-\eta K}\right) \leqslant \gamma(p)\|u-p\|,$$

where the left-hand inequality is easily checked numerically. □

4 CONDITION NUMBER OF SEMIALGEBRAIC SYSTEMS

We focus now on semialgebraic sets, and more specifically, on *spherical* semialgebraic sets $S(F,G)$ given by homogeneous semialgebraic systems (F,G); cf. (20). We do so since, eventually (see §5.3 below), we will reduce the computation of the homology of semialgebraic sets and its complexity analysis to the same tasks for the spherical case. We define a condition number κ_* for homogeneous semialgebraic systems and relate it to three different measures of conditioning: the distance to the closest ill-posed system in the space of semialgebraic systems (Theorem 4.10); the reach of the set $S(F,G)$ (Theorem 4.12); and the sensitivity of $S(F,G)$ to small relaxations of the equalities and inequalities of the system (F,G) (Theorem 4.19). We also bound the degree of the hypersurface of ill-posed systems (Proposition 4.20). We finally give a notion of condition number for affine semialgebraic systems that is based on the one for the homogeneous case.

4.1 Measures of condition

4.1.1 The μ numbers. To a degree pattern $\boldsymbol{d}=(d_1,\dots,d_q)$ we associate the linear space $\mathcal{H}_{\boldsymbol{d}}[q]$ of the polynomial systems $F=(f_1,\dots,f_q)$ where $f_i\in\mathbb{R}[X_0,X_1,\dots,X_n]$ is homogeneous of degree d_i. Let $D=\max_{1\leqslant i\leqslant q} d_i$. We endow $\mathcal{H}_{\boldsymbol{d}}[q]$ with a Euclidean inner product, the *Weyl inner product*, defined as follows. For homogeneous polynomials $h=\sum_{|\boldsymbol{a}|=d} h_{\boldsymbol{a}}X^{\boldsymbol{a}}$ and $h'=\sum_{|\boldsymbol{a}|=d} h'_{\boldsymbol{a}}X^{\boldsymbol{a}}$ in $\mathbb{R}[X_0,\dots,X_n]$, where we write $\boldsymbol{a}=(a_0,\dots,a_n)\in\mathbb{N}^{n+1}$ and $|\boldsymbol{a}|\coloneqq a_0+\cdots+a_n$, we define

$$\langle h,h'\rangle \coloneqq \sum_{|\boldsymbol{a}|=d}\binom{d}{\boldsymbol{a}}^{-1} h_{\boldsymbol{a}}h'_{\boldsymbol{a}},$$

where $\binom{d}{\boldsymbol{a}}\coloneqq\frac{d!}{a_0!a_1!\dots a_n!}$ is the multinomial coefficient. For any q-tuples of homogeneous polynomials $F,F'\in\mathcal{H}_{\boldsymbol{d}}[q]$ with degree pattern $\boldsymbol{d}$, say $F=(f_1,\dots,f_q)$ and $F'=(f'_1,\dots,f'_q)$, we define

$$\langle F,F'\rangle \coloneqq \sum_{j=1}^{q}\langle f_j,f'_j\rangle.$$

In other words, the Weyl inner product is a dot product with respect to a specifically weighted monomial basis. Its *raison d'être* is the fact that it is invariant under orthogonal transformations of the homogeneous variables $(X_0,\dots,X_n)$. That is, that for any orthogonal transformation $u:\mathbb{R}^{n+1}\to\mathbb{R}^{n+1}$ and any $F\in\mathcal{H}_{\boldsymbol{d}}[q]$, we have $\|F\|=\|F\circ u\|$. In all of what follows, all occurrences of norms in spaces $\mathcal{H}_{\boldsymbol{d}}[q]$ refer to the norm induced by the Weyl inner product.

For a point $x\in\mathbb{R}^{n+1}$ and a system $F\in\mathcal{H}_{\boldsymbol{d}}[q]$, let $\mathrm{D}F(x)$ denote the derivative of F at x, which is a linear map $\mathbb{R}^{n+1}\to\mathbb{R}^q$. We also define the diagonal normalization matrix

$$\Delta \coloneqq \begin{pmatrix}\sqrt{d_1} & & \\ & \ddots & \\ & & \sqrt{d_q}\end{pmatrix}.$$

The *condition number* $\mu_{\mathrm{norm}}(F,x)$ of $F\in\mathcal{H}_{\boldsymbol{d}}[q]$ at $x\in\mathbb{S}^n$ has been well studied [54–58], see also [18]. We define it as ∞ when the derivative $\mathrm{D}F(x)$ of F at x is not surjective, and otherwise as

$$\mu_{\mathrm{norm}}(F,x)\coloneqq\|F\|\left\|\mathrm{D}F(x)^{\dagger}\Delta\right\|, \tag{18}$$

where the norm $\|\mathrm{D}F(x)^{\dagger}\Delta\|$ is the spectral norm. We also define the following variant of μ_{norm}, more specific to homogeneous systems,

$$\mu_{\mathrm{proj}}(F,x)\coloneqq\mu_{\mathrm{norm}}(F|_{T_x},x)=\|F\|\left\|\mathrm{D}F(x)|_{T_x}^{\dagger}\Delta\right\|,$$

where $T_x = \{x\}^\perp$ and $\mathcal{T}_x := x + T_x$. (The number $\mu_{\text{norm}}(F|_{\mathcal{T}_x}, x)$ is well-defined after identifying $\mathcal{T}_x$ with $\mathbb{R}^n$.)

The following inequality is a useful result from the Shub–Smale theory [58, Lemma 2.1(b)].

Proposition 4.1. *Let $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ and $x \in \mathbb{R}^{n+1}$ be a zero of F. Then*

$$\gamma(F,x) \leqslant \tfrac{1}{2} D^{\frac{3}{2}} \mu_{\text{norm}}(F,x). \qquad \square$$

4.1.2 The κ number. The numbers $\mu_{\text{norm}}(F,x)$ and $\mu_{\text{proj}}(F,x)$ measure the sensitivity of the zero x of F when F is slightly perturbed. They are consequently useful at a zero, or near a zero, of the system F. To deal with points in $\mathbb{S}^n$ far away from the zeros of F, in particular to understand how much F needs to be perturbed to make such a point a zero, a more global notion of conditioning is needed. The following is (modulo replacing μ_{norm} by μ_{proj}) the condition measure introduced in [25] (see also [18, §19] and [26, 27]).

Definition 4.2. The *real homogeneous condition number* of $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ at $x \in \mathbb{S}^n$ is

$$\kappa(F,x) := \left(\frac{1}{\mu_{\text{proj}}(F,x)^2} + \frac{\|F(x)\|^2}{\|F\|^2} \right)^{-1/2},$$

where we use the conventions $\infty^{-1} := 0$, $0^{-1} := \infty$, and $\kappa(0,x) := \infty$. We further define $\kappa(F) := \max_{x \in \mathbb{S}^n} \kappa(F,x)$.

If $q > n$ (that is, if the system F is overdetermined) then $\mathrm{D}F(x)|_{T_x}$ cannot be surjective and $\kappa(F,x) = \frac{\|F\|}{\|F(x)\|}$ for all $x \in \mathbb{S}^n$. Thus, $\kappa(F) < \infty$ if and only if F has no zeros in $\mathbb{S}^n$.

The special case $F(x) = 0$ is worth highlighting.

Lemma 4.3. *For any $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ and $x \in \mathbb{S}^n$, if $F(x) = 0$, then*

$$\kappa(F,x) = \mu_{\text{proj}}(F,x) = \mu_{\text{norm}}(F,x).$$

Proof. The first equality follows from the definition of κ. For the second, recall that the pseudo-inverse $\mathrm{D}F(x)^\dagger$ is the inverse of $\mathrm{D}F(x)$ restricted as a map $(\ker \mathrm{D}F(x))^\perp \to \mathbb{R}^q$. If $F(x) = 0$, then $\mathrm{D}F(x)(x) = 0$, by homogeneity, therefore the orthogonal complement of the kernel of $\mathrm{D}F(x)$ is included in T_x. It follows that $\mathrm{D}F(x)|_{T_x}^\dagger = \mathrm{D}F(x)^\dagger$ and then $\mu_{\text{proj}}(F,x) = \mu_{\text{norm}}(F,x)$. $\square$

For $x \in \mathbb{S}^n$, let Σ_x be the set of all $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ such that $\kappa(F,x) = \infty$, that is $F(x) = 0$ and $\mathrm{D}F(x)|_{T_x}$ is not surjective. The *set of ill-posed algebraic systems* is defined as $\Sigma := \bigcup_{x \in \mathbb{S}^n} \Sigma_x$. It is the set of all $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ such that $\kappa(F) = \infty$. We have

$$\Sigma = \left\{ F \in \mathcal{H}_{\boldsymbol{d}}[q] \mid \exists x \in \mathbb{S}^n\ F(x) = 0 \text{ and } \mathrm{D}F(x)|_{T_x} \text{ is not surjective} \right\}. \tag{19}$$

The set Σ is semialgebraic and invariant under scaling of each of the q components. Note that in the case $q > n$, the set Σ_x just consists of the $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ such $F(x) = 0$, and Σ equals the set of $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ that possess a real zero in $\mathbb{S}^n$.

Theorem 4.4. *For any nonzero $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ and any $x \in \mathbb{S}^n$,*

$$\kappa(F,x) = \frac{\|F\|}{d(F,\Sigma_x)} \quad \text{and} \quad \kappa(F) = \frac{\|F\|}{d(F,\Sigma)},$$

where the distance $d(F,\cdot)$ is defined via the norm induced by the Weyl inner product.

Proof. The assertion is obvious in the case $q > n$. We therefore assume $q \leqslant n$. The special case $q = n$ is Prop. 19.6 in [18]. One can check that the same proof works in the case $q \leqslant n$. $\square$

Corollary 4.5. *For any $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ and any $x \in \mathbb{S}^n$, $\kappa(F,x) \geqslant 1$.*

Proof. Since $0 \in \Sigma_x$, this follows directly from Theorem 4.4. □

Remark 4.6. Proposition 6.1 in [28] shows that for the condition number $\kappa_{\mathrm{norm}}(F,x)$ defined as in Definition 4.2 above, but with μ_{proj} replaced by μ_{norm}, we have

$$\frac{\|F\|}{\sqrt{2}\, d(F,\Sigma_x)} \leqslant \kappa_{\mathrm{norm}}(F,x) \leqslant \frac{\|F\|}{d(F,\Sigma_x)}.$$

This shows that there is no essential difference between κ and κ_{norm}: they are the same up to a factor of at most $\sqrt{2}$. It also shows that, for all $x \in \mathbb{S}^n$, $\mu_{\mathrm{norm}}(F,x) \leqslant \mu_{\mathrm{proj}}(F,x)$. So the bound in Proposition 4.1 holds with $\mu_{\mathrm{proj}}(F,x)$ as well.

However, a bound on μ_{proj} in terms of μ_{norm} is not possible. Indeed, take $f_1(x,y,z) := x+y$ and $f_2(x,y,z) := y^2+z^2+xy$. Further, take $e_0 := (1,0,0)$. Then

$$\mathrm{D}F(e_0) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathrm{D}F(e_0)_{|e_0^\perp} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix},$$

where the left-hand matrix is of full rank, but the right-hand matrix is rank deficient. Hence $\mu_{\mathrm{norm}}(F,e_0) < \infty$, but $\mu_{\mathrm{proj}}(F,e_0) = \infty$. We introduced μ_{proj} in our development because it allows for sharper statements and easier proofs.

Proposition 4.7. *For $F \in \mathcal{H}_{\boldsymbol{d}}[q]$, the map $\mathbb{S}^n \to \mathbb{R}$, $x \mapsto \kappa(F,x)^{-1}$ is D-Lipschitz continuous with respect to the Riemannian metric on $\mathbb{S}^n$.*

Proof. Let $x,y \in \mathbb{S}^n$. Let $u \in \mathscr{O}(n+1)$ be the rotation that maps x to y and that is the identity on $\{x,y\}^\perp$. By the invariance of Weyl's inner product under the action of $\mathscr{O}(n+1)$,

$$d(F,\Sigma_y) = d(F\circ u, \Sigma_x).$$

Since the function $g \mapsto d(g,\Sigma_x)$ is 1-Lipschitz, we obtain with Theorem 4.4 that

$$\begin{aligned} \|F\| \left| \frac{1}{\kappa(F,x)} - \frac{1}{\kappa(F,y)} \right| &= |d(F,\Sigma_x) - d(F,\Sigma_y)| \\ &= |d(F,\Sigma_x) - d(F\circ u,\Sigma_x)| \leqslant \|F - F\circ u\|. \end{aligned}$$

We conclude the proof with the next lemma. □

Lemma 4.8. *For any $F \in \mathcal{H}_{\boldsymbol{d}}[q]$ and any $x,y \in \mathbb{S}^n$,*

$$\|F - F\circ u\| \leqslant D\|F\| d_{\mathbb{S}}(x,y),$$

where $u \in \mathscr{O}(n+1)$ is the unique rotation that maps x to y and leaves invariant $\{x,y\}^\perp$.

Proof. We first notice that

$$\|F - F\circ u\|^2 = \sum_i \|f_i - f_i \circ u\|^2$$

so it is enough to prove the claim when $q = 1$.

We prove a corresponding, more general statement over $\mathbb{C}$ and, to this end, we consider the space of complex homogeneous coefficients of degree d endowed with Weyl's Hermitian inner product. The latter is invariant under the action of the unitary group $\mathscr{U}(n+1)$, therefore, without loss of generality, we may assume that the matrix of u is the diagonal matrix $\mathrm{diag}(e^{i\theta}, e^{-i\theta}, 1, \dots)$, where $\theta = d_{\mathbb{S}}(x,y)$. We write $f = \sum_{|\boldsymbol{a}|=d} c_{\boldsymbol{a}} X^{\boldsymbol{a}}$ and then

$$f - f\circ u = \sum_{|\boldsymbol{a}|=d} \left(1 - e^{i(a_0-a_1)\theta}\right) c_{\boldsymbol{a}} X^{\boldsymbol{a}}.$$

Since

$$\left|1 - e^{i(a_0-a_1)\theta}\right| \leqslant |(a_0 - a_1)\theta| \leqslant D\,\theta,$$

we obtain the claim. □

4.1.3 Condition number of homogeneous semialgebraic systems. We consider (closed) *homogeneous semialgebraic systems*, i.e., systems of the form

$$f_1(x) = 0, \ldots, f_q(x) = 0 \text{ and } g_1(x) \geqslant 0, \ldots, g_s(x) \geqslant 0, \tag{20}$$

where the f_i and the g_j are homogeneous polynomials in $\mathbb{R}[X_0, X_1, \ldots, X_n]$. The system is an element $(F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\,s]$. The set of solutions $x \in \mathbb{S}^n$ of system (20), which we will denote by $S(F, G)$, is a *spherical basic semialgebraic set.* Needless to say, we do allow for the possibility of having $q = 0$ or $s = 0$. This corresponds with systems having only inequalities (resp. only equalities).

To a homogeneous semialgebraic system (F, G) we associate a condition number $\kappa_*(F, G)$ as follows. For a subtuple $L = (g_{j_1}, \ldots, g_{j_\ell})$ of G, let F^L denote the system obtained from F by appending the polynomials from L, that is,

$$F^L := \left(f_1, \ldots, f_q, g_{j_1}, \ldots, g_{j_\ell}\right) \in \mathcal{H}_{\boldsymbol{d}}[q + \ell]$$

(where now $\boldsymbol{d}$ denotes the appropriate degree pattern in $\mathbb{N}^{q+\ell}$). Abusing notation, we will frequently use set notations $L \subseteq G$ or $g \in G$ to denote subtuples or coefficients of G.

Definition 4.9. Let $q \leqslant n + 1$, $(F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\,s]$. The *condition number of the homogeneous semialgebraic system* (F, G) is defined as

$$\kappa_*(F, G) := \max_{\substack{L \subseteq G \\ q+|L| \leqslant n+1}} \kappa\left(F^L\right).$$

We define Σ_* as the set of all $(F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\,s]$ such that $\kappa_*(F, G) = \infty$.

Clearly, Σ_* is semialgebraic and invariant under scaling of the $q + s$ components.

Theorem 4.10. *For any nonzero $\psi = (F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\,s]$,*

$$\kappa_*(\psi) \leqslant \frac{\|\psi\|}{d(\psi, \Sigma_*)}.$$

Proof. For a subset L of the indices $\{1, \ldots, s\}$, let $p_L \colon \mathcal{H}_{\boldsymbol{d}}[q\,;\,s] \to \mathcal{H}_{\boldsymbol{d}}[q + |L|]$ be the projection $(F, G) \mapsto F^L$. Clearly $\Sigma_* = \cup_L p_L^{-1}(\Sigma_L)$, where Σ_L is the set of ill-posed data in the appropriate space $\mathcal{H}_{\boldsymbol{d}}[q + |L|]$. In particular $d(\psi, \Sigma_*) \leqslant d(p_L(\psi), \Sigma_L)$. Then, by Theorem 4.4,

$$\kappa_*(F, G) = \max_{\substack{L \subseteq G \\ q+|L| \leqslant n+1}} \frac{\|F^L\|}{d(F^L, \Sigma_L)} \leqslant \frac{\|\psi\|}{d(\psi, \Sigma_*)}.$$ □

Note that we do not define condition for the very overdetermined case $q > n + 1$, but it is important to include the overdetermined case $q + |L| = n + 1$ in the definition of $\kappa_*(F, G)$. To see why, consider the case of three polynomials f, g_1, g_2 around a point $x \in \mathbb{S}^2$ as in Figure 3.

This system is ill-posed as arbitrarily small perturbations of (f, G) may result in an empty intersection around x, and hence, a different topology of $S(f, G)$. But none of the condition numbers $\kappa(f, g_1)$ and $\kappa(f, g_2)$ capture this fact as x is a well-posed zero for both systems. The following lemma is related to this matter.

Lemma 4.11. *Let (F, G) be a homogeneous semialgebraic system with $\kappa_*(F, G) < \infty$. For any $L \subseteq G$ such that $|L| \geqslant n + 1 - q$, the set $S(F^L, \varnothing)$ is empty.*

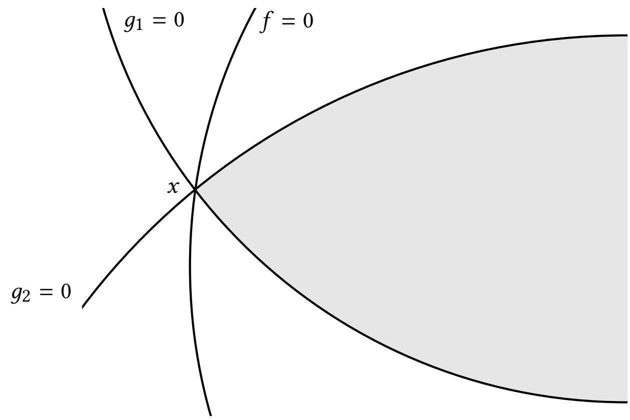

Fig. 3 The shaded area is where $g_1 \geqslant 0$ and $g_2 \geqslant 0$. Locally, the only solution point is the intersection $\{x\}$ of $f = g_1 = g_2 = 0$.

Proof. We choose $L' \subseteq L$ such that $|L'| = n+1-q$. Because of the dimensions involved, $\mathrm{D}F^{L'}(x)|_{T_x}$ cannot be surjective, thus $\kappa(F^{L'}, x) = \|F^{L'}\|/\|F^{L'}(x)\|$ for any $x \in \mathbb{S}^n$. Moreover $\kappa(F^{L'}) \leqslant \kappa_*(F, G) < \infty$, by definition of κ_*. Therefore $F^{L'}$ has no zero on $\mathbb{S}$. In particular $S(F^L, \varnothing)$, the zero set of F^L, is empty. □

We elaborate on Theorem 3.3, relating γ and τ, to obtain the following result that relates κ_* and τ. It gives a computational handle on τ which is otherwise hard to get.

Theorem 4.12. *For any homogeneous semialgebraic system (F, G) defining a semialgebraic set $S := S(F, G) \subseteq \mathbb{S}^n$, if $\kappa_*(F, G) < \infty$, then*

$$D^{\frac{3}{2}}\, \tau(S)\, \kappa_*(F, G) \geqslant \tfrac{1}{7}.$$

Proof. We first study the case where $G = \varnothing$. Let $\widehat{S} \subseteq \mathbb{R}^{n+1}$ be the cone over S, that is, the zero set of F in $\mathbb{R}^{n+1}$. For any $x \in S$, $\tau(S, x) \geqslant \min(1, \tau(\widehat{S}, x))$, by Lemma 2.7. Therefore,

$$\tau(S) = \min_{x \in S} \tau(S, x) \geqslant \min\left(1, \min_{x \in S} \tau(\widehat{S}, x)\right).$$

Using also that $\kappa(F, x) \geqslant 1$ (Corollary 4.5), we obtain that

$$\tau(S)\kappa(F) \geqslant \min\left(1, \min_{x \in S} \tau(\widehat{S}, x)\kappa(F, x)\right). \tag{21}$$

Recall from Lemma 4.3 that $\kappa(F, x) = \mu_{\mathrm{proj}}(F, x) = \mu_{\mathrm{norm}}(F, x)$ for all $x \in S$. Combining this with Proposition 4.1, we obtain that $D^{\frac{3}{2}}\kappa(F, x) \geqslant 2\gamma(F, x)$ for all $x \in S$. We conclude that

$$D^{\frac{3}{2}} \min_{x \in S} \tau(\widehat{S}, x)\kappa(F, x) \;\geqslant\; \min_{x \in S}\; 2\tau(\widehat{S}, x)\gamma(F, x) \;\geqslant\; \tfrac{1}{7},$$

where we have applied Theorem 3.3 to $\widehat{S}$ for the right-hand side inequality. Combining this with (21), we obtain $D^{\frac{3}{2}}\tau(S)\kappa(f) \geqslant \frac{1}{7}$.

We turn now to the general case $S := S(F, G) \subseteq \mathbb{S}^n$. For $g \in G$ we define $P_g := \{x \in \mathbb{S}^n \mid g(x) \geqslant 0\}$ and $W := S(F, \varnothing)$ so that $S = W \cap \left(\cap_{g \in G} P_g\right)$. We claim that for any $L \subseteq G$,

$$W \cap \bigcap_{g \in L} \partial P_g = S(F^L, \varnothing). \tag{22}$$

The left-to-right inclusion is clear since ∂P_g is contained in the zero set of g. Conversely, let $x \in S(F^L, \varnothing)$ (in particular, $q + |L| \leqslant n$, by Lemma 4.11). The derivative $\mathrm{D}F^L(x)$ is surjective, because $\kappa(F^L, x) < \infty$. In particular, for any $g \in L$, $Dg(x) \neq 0$ and since $g(x) = 0$ it follows that the sign of g changes around x. Thus $x \in \partial P_g$ and Equation (22) follows.

Theorem 2.6 implies that

$$\tau(S) \;\geqslant\; \min_{L \subseteq G} \tau\Big(W \cap \bigcap_{g \in L} \partial P_g\Big) = \min_{L \subseteq G} \tau\big(S\big(F^L, \varnothing\big)\big). \tag{23}$$

It suffices to take the minimum over the $L \subseteq G$ such that $q + |L| \leqslant n + 1$ because $S(F^L, \varnothing) = \varnothing$ for larger L. We obtain from the case $G = \varnothing$ above,

$$7\, D^{\frac{3}{2}} \tau(S) \;\geqslant\; \min_L 7\, D^{\frac{3}{2}} \tau(S(F^L, \varnothing)) \geqslant \frac{1}{\max_L \kappa(F^L)} = \frac{1}{\kappa_*(F, G)},$$

which completes the proof. □

4.1.4 Strict inequalities. We prove here that replacing inequalities $g_i(x) \geqslant 0$ by strict inequalities $g_i(x) > 0$ in the definition (20) of a spherical basic set $S(F, G)$ does not change its homotopy type, provided $\kappa_*(F, G) < \infty$.

The argument is based on a general reasoning in topology. Recall that a closed subset B of a topological space X is called *collared in* X if there exists a homeomorphism $h\colon [0, 1) \times B \to V$ onto an open neighborhood V of B in X such that $h(0, b) = b$ for all $b \in B$.

Lemma 4.13. *If $B \subseteq X$ is collared in X and $X \setminus B \subseteq X' \subseteq X$, then X' and X are homotopically equivalent.*

Proof. Let $\tau\colon V \to [0, 1]$ and $u\colon V \to B$ denote the components of the inverse of h, so that $h(\tau(x), u(x)) = x$ for any $x \in V$. We define the map $\phi : [0, 1] \times X \to X$ by

$$\phi_t(x) := \begin{cases} h(t, u(x)) & \text{if } x \in V \text{ and } \tau(x) < t, \\ x & \text{otherwise.} \end{cases}$$

The idea is that ϕ_t pushes X increasingly far away from B as t increases. It is easy to verify that ϕ is continuous, $\phi_0 = \mathrm{id}_X$, $\phi_t(x) = x$ for $x \in X \setminus V$, and $\phi_1(X) = X \setminus V$. In other words, $\phi_t\colon X \to X$ defines a deformation retraction of X to $X \setminus V$.

Moreover, we have $\phi_t(X') \subseteq X'$, since $\phi_t(X') \subseteq X \setminus B \subseteq X'$ for $t > 0$. In addition, $X \setminus V \subseteq \phi_t(X') \subseteq X \setminus V$. Therefore, the restrictions of ϕ_t define a deformation retraction of X' to $X \setminus V$. We conclude that X' and X are homotopically equivalent. □

We apply this now to basic semialgebraic sets.

Proposition 4.14. *Let $(F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\, s]$ be such that $\kappa_*(F, G) < \infty$. Put $S := S(F, G)$, let $r \leqslant s$, and let $S' \subseteq S$ be the solution set in $\mathbb{S}^n$ of the semialgebraic system*

$$f_1 = \cdots = f_q = 0,\; g_1 \geqslant 0, \ldots, g_r \geqslant 0 \text{ and } g_{r+1} > 0, \ldots, g_s > 0.$$

Moreover, let ∂S denote the boundary of S in $S(F, \varnothing)$. Then $S \setminus \partial S \subseteq S'$, ∂S is collared in S, and S' is homotopically equivalent to S.

Proof. Let $x \in S$ and $L \subseteq G$ be maximal such that $F^L(x) = 0$. Note, this implies $|L| \leqslant n - q$. Since $\mu_{\mathrm{proj}}(F^L, x) = \kappa(F^L, x) < \infty$, the derivatives at x of the components of F^L are linearly independent. Therefore, the components of F^L are part of some regular system of parameters $(f_1, \ldots, f_q, v_1, \ldots, v_{n-q})$ of $\mathbb{S}^n$ at x such that S is defined locally around x by

$$f_1 = \cdots = f_q = 0 \text{ and } v_1 \geqslant 0, \ldots, v_{|L|} \geqslant 0,$$

and ∂S is defined locally around x by additional requiring $v_j(x) = 0$ for some $j \leqslant |L|$. Therefore, if $x \notin \partial S$, we must have $v_i(x) > 0$ for all i, and hence $g_j(x) > 0$ for all j. This shows the first assertion $S \setminus \partial S \subseteq S'$.

This reasoning also proves that locally around x, the set S is diffeomorphic to some $(-1,1)^a \times [0,1)^b$ with $a, b \in \mathbb{N}$. Therefore, ∂S is locally collared in S. By Brown's Collaring Theorem [16, 24], ∂S is collared in S, which proves the second assertion. The third assertion follows by applying Lemma 4.13 to $X = S$, $B = \partial S$ and $X' = S'$. □

4.1.5 Condition number of affine semialgebraic systems. We now consider basic semialgebraic subsets of $\mathbb{R}^n$, rather than $\mathbb{S}^n$. Given a degree pattern $\boldsymbol{d} = (d_1, \dots, d_{q+s})$, the homogeneization of polynomials (with respect to that pattern) yields an isomorphism of linear spaces

$$\mathcal{P}_{\boldsymbol{d}}[q\,;s] \to \mathcal{H}_{\boldsymbol{d}}[q\,;s], \quad \psi = (F,G) \mapsto \psi^{\mathsf{h}} = (F^{\mathsf{h}}, G^{\mathsf{h}}),$$

where F^h denotes the homogeneization of F with homogeneizing variable X_0. The Weyl inner product on $\mathcal{H}_{\boldsymbol{d}}[q\,;s]$ induces an inner product on $\mathcal{P}_{\boldsymbol{d}}[q\,;s]$ such that the above map is isometric.

Definition 4.15. Let $(\boldsymbol{d}, 1) := (d_1, \dots, d_{q+s}, 1) \in \mathbb{N}^{q+s+1}$ be the degree pattern obtained from $\boldsymbol{d}$ by appending 1. Consider the *scaled homogeneization map*

$$H : \mathcal{P}_{\boldsymbol{d}}[q\,;s] \to \mathcal{H}_{(\boldsymbol{d},1)}[q\,;s+1], \quad \psi \mapsto (\psi^{\mathsf{h}}, \|\psi^{\mathsf{h}}\| X_0), \tag{24}$$

that is, the system $H(F,G)$ is the homogeneization of (F,G) to which we add the inequality $X_0 \geqslant 0$ with a suitable coefficient. For $\psi \in \mathcal{P}_{\boldsymbol{d}}[q\,;s]$, we define $\kappa_*^{\mathrm{aff}}(\psi) := \kappa_*(H(\psi))$ and call $\Sigma_*^{\mathrm{aff}} := H^{-1}(\Sigma_*)$ the *set of ill-posed affine semialgebraic systems.*

By construction, $\|H(\psi)\|^2 = 2\|\psi\|^2$. We note that Σ_*^{aff} is a semialgebraic set in $\mathcal{P}_{\boldsymbol{d}}[q\,;s]$ that is invariant under scaling of each of the $q+s$ components.

Proposition 4.16. *For any nonzero $\psi \in \mathcal{P}_{\boldsymbol{d}}[q\,;s]$,*

$$\kappa_*^{\mathrm{aff}}(\psi) \leqslant \frac{4D\|\psi\|}{d(\psi, \Sigma_*^{\mathrm{aff}})}.$$

Proof. Fix $\psi \in \mathcal{P}_{\boldsymbol{d}}[q\,;s]$ and put $r := \|\psi\| > 0$. Further, assume $\Phi \in \mathcal{H}_{\boldsymbol{d},1}[q\,;s+1]$ is an element of Σ_* that minimizes the distance to $H(\psi)$. Theorem 4.10 implies that

$$\kappa_*^{\mathrm{aff}}(\psi) = \kappa_*(H(\psi)) \leqslant \frac{\|H(\psi)\|}{\|H(\psi) - \Phi\|}. \tag{25}$$

We write $\Phi = (\Phi_1, \lambda)$, where $\Phi_1 \in \mathcal{H}_{\boldsymbol{d}}[q\,;s]$ and $\lambda \in \mathcal{H}_1[1]$. We may assume that $\lambda \neq 0$: otherwise, we can replace Φ with $\Phi' := (0, rX_0)$, which is an element of Σ_* that is at least as close to $H(\psi) = (\psi^{\mathsf{h}}, rX_0)$ as Φ, since $\|H(\psi) - \Phi'\| = r \leqslant \|H(\psi) - \Phi\|$.

Since Σ_* is invariant under the scaling of each component, the minimality of Φ implies that λ and $rX_0 - \lambda$ are orthogonal, that the angle α between λ and X_0 satisfies $\alpha \leqslant \pi/2$, and, as a consequence, that

$$\alpha \leqslant \tfrac{\pi}{2} \sin\alpha \leqslant \tfrac{\pi}{2} \tfrac{\|rX_0 - \lambda\|}{r}. \tag{26}$$

Let $u \in \mathscr{O}(n+1)$ be the rotation that leaves $\{X_0, \lambda\}^\perp$ invariant and such that $\lambda \circ u = \|\lambda\| X_0$. Then $\Phi \circ u = (\Phi_1 \circ u, \lambda \circ u) \in \Sigma_*$ since Σ_* is invariant under the action of $\mathscr{O}(n+1)$. If we write $\Phi_1 \circ u = \varphi^{\mathsf{h}}$ with $\varphi \in \mathcal{P}_{\boldsymbol{d}}[q\,;s]$, then $H(\varphi) = (\varphi^{\mathsf{h}}, \|\varphi^{\mathsf{h}}\| X_0)$ lies in Σ_*, since Σ_* is invariant under the scaling of its last component and $\lambda \neq 0$. We therefore obtain,

$$\begin{aligned} d(\psi, \Sigma_*^{\mathrm{aff}}) &\leqslant \|\psi - \varphi\| = \|\psi^{\mathsf{h}} - \varphi^{\mathsf{h}}\| \leqslant \|\psi^{\mathsf{h}} - \psi^{\mathsf{h}} \circ u\| + \|\psi^{\mathsf{h}} \circ u - \Phi_1 \circ u\| \\ &= \|\psi^{\mathsf{h}} - \psi^{\mathsf{h}} \circ u\| + \|\psi^{\mathsf{h}} - \Phi_1\|. \end{aligned}$$

By Lemma 4.8 and Inequality (26), we obtain that

$$\|\psi^{\mathsf{h}} - \psi^{\mathsf{h}} \circ u\| \leqslant \alpha D r \leqslant \tfrac{\pi}{2} D \|rX_0 - \lambda\|.$$

Since $\|rX_0 - \lambda\|$ and $\|\psi^{\mathsf{h}} - \Phi_1\|$ are both bounded by $\|H(\psi) - \Phi\|$, we get

$$d(\psi, \Sigma_*^{\mathrm{aff}}) \leqslant \left(\tfrac{\pi}{2} D + 1\right) \|H(\psi) - \Phi\| = \left(\tfrac{\pi}{2} D + 1\right) \sqrt{2}\, \|\psi\| \frac{\|H(\psi) - \Phi\|}{\|H(\psi)\|}.$$

We conclude with Inequality (25). □

4.2 Neighbourhoods of spherical basic semialgebraic sets

The goal of this section is to compare two natural ways of defining neighborhoods of a spherical semialgebraic set $S(F, G)$: by relaxing the arguments of the polynomials in F and G (the common, tube-like neighborhood), or by relaxing their values.

For a subset $A \subseteq \mathbb{S}^n$ we denote by

$$\mathcal{U}_{\mathbb{S}}(A, r) := \{x \in \mathbb{S} \mid d_{\mathbb{S}}(x, A) < r\}$$

the open *r-neighborhood* of A with respect to the geodesic distance $d_{\mathbb{S}}$ on the sphere $\mathbb{S}^n$. Also, for a homogeneous system $(F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\, s]$ and $r > 0$, we define the *r-relaxation of* $S(F, G)$:

$$\mathrm{Approx}(F, G, r) := \{x \in \mathbb{S}^n \mid \forall f \in F \;\; |f(x)| < \|f\| r \text{ and } \forall g \in G\, g(x) > -\|g\| r\}.$$

It is clear that $S(F, G) \subseteq \mathrm{Approx}(F, G, r)$ for any $r > 0$. It is easy to see that $\mathrm{Approx}(F, G, r)$ converges to S with respect to the Hausdorff distance, when $r \to 0$. The next two results quantify more precisely this behaviour in terms of the condition number $\kappa_*(F, G)$. Recall, D denotes the maximum degree of the components of F and G.

Proposition 4.17. *For any $r > 0$,*

$$\mathcal{U}_{\mathbb{S}}\left(S(F, G), D^{-\frac{1}{2}} r\right) \subseteq \mathrm{Approx}(F, G, r).$$

Proof. For any homogeneous polynomial h of degree d and any $x, y \in \mathbb{S}^n$,

$$|h(x) - h(y)| \leqslant \sqrt{d}\, \|h\|\, d_{\mathbb{S}}(x, y).$$

(This is shown in [18, Lemma 19.22]. The additional hypothesis $d_{\mathbb{S}}(x, y) < 1/\sqrt{2}$ there can be easily removed by splitting the path from x to y in smaller segments.) Hence, for any $x \in S$ and $y \in \mathbb{S}^n$ such that $d_{\mathbb{S}}(x, y) < \frac{1}{\sqrt{D}} r$, any $f \in F$ and $g \in G$, we have $|f(y)| \leqslant r\|f\|$ and $g(y) > g(x) - r\|g\| \geqslant -r\|g\|$. □

Lemma 4.18. *Let $H \subseteq L \subseteq G$ be such that $|H| = n - q + 1$, and $0 < r < \frac{1}{\kappa(F^H)}$. Then* $\mathrm{Approx}(F^L, G \setminus L, r) = \varnothing$.

Proof. Since $\kappa(F^H) < \infty$ we have $S(F^H, \varnothing) = \varnothing$, by Lemma 4.11. Assume there is a point $x \in \mathrm{Approx}(F^L, G \setminus L, r)$. Then, as $H \subseteq L$ we have that $|h(x)| \leqslant r\|h\|$ for all $h \in F^H$ and it follows that

$$\frac{1}{\kappa(F^H)} \leqslant \frac{1}{\kappa(F^H, x)} = \frac{\|F^H(x)\|}{\|F^H\|} \leqslant r.$$

This is in contradiction with the hypothesis on r and hence $\mathrm{Approx}(F^L, G \setminus L, r)$ is empty. □

Theorem 4.19. *Let $q \leqslant n + 1$. For any positive number $r < \left(13 D^{\frac{3}{2}} \kappa_*^2\right)^{-1}$ we have*

$$\mathrm{Approx}(F, G, r) \;\subseteq\; \mathcal{U}_{\mathbb{S}}(S(F, G), 3\kappa_* r).$$

Proof. We will abbreviate $S := S(F,G)$ and $\kappa_* := \kappa_*(F,G)$. The proof is by induction on the difference $\ell := n - q + 1$ between the number of variables and the number of equations. Before dealing with the basis of the induction, we note that the assumption on r implies that $\kappa_* < \infty$.

If $\ell = 0$, then $\kappa(F) = \kappa_* < \infty$ and, because of our hypothesis, $r < \frac{1}{\kappa_*}$. We deduce from Lemma 4.18, with $L = H = \varnothing$ that $\operatorname{Approx}(F,G,r) = \varnothing$. The desired inclusion is therefore trivially true.

Now we assume $\ell > 0$, i.e., $q \leqslant n$, and consider a point $x \in \operatorname{Approx}(F,G,r)$. It is enough to show that

$$d_{\mathbb{S}}(x,S) < 3\kappa_* r. \tag{27}$$

To do so, we focus on the set of inequalities

$$L := \left\{ g \in G \mid |g(x)| < r\|g\| \right\}.$$

By construction, we have $x \in \operatorname{Approx}(F^L, G \setminus L, r)$, and moreover $g(x) \geqslant r\|g\| > 0$ for all $g \in G \setminus L$. We further note that $|L| \leqslant n - q$, otherwise there would exist $H \subseteq L$ with $|H| = n - q + 1$ and, we would use again Lemma 4.18 to deduce that $\operatorname{Approx}(F,G,r) = \varnothing$, in contradiction with the fact that $x \in \operatorname{Approx}(F,G,r)$. We next divide by cases.

Case 1: $L \neq \varnothing$. As $|F^L| \leqslant n + 1$ we may apply the induction hypothesis to the larger set F^L of equations and the smaller set $G \setminus L$ of inequalities; note that $\kappa_*(F^L, G \setminus L) \leqslant \kappa_*(F,G)$ so the hypothesis on r is still true for $(F^L, G \setminus L)$. The induction hypothesis yields

$$\operatorname{Approx}(F^L, G \setminus L, r) \subseteq \mathcal{U}_{\mathbb{S}}\left(S(F^L, G \setminus L), 3\kappa_*(F^L, G \setminus L) r \right) \subseteq \mathcal{U}_{\mathbb{S}}\left(S, 3\kappa_* r \right).$$

Hence we obtain (27) and are done in this case.

Case 2: $L = \varnothing$. We put $u := \|F(x)\|/\|F\|$. Then $u \leqslant r$ since $x \in \operatorname{Approx}(F,G,r)$. Moreover, $\kappa_* u \leqslant \kappa_* r < \frac{1}{13}$ by assumption. By definition,

$$\kappa(F,x)^2 \geqslant \frac{1}{\mu_{\mathrm{proj}}(F,x)^{-2} + u^2} \geqslant \frac{1}{2} \min\left\{ \mu_{\mathrm{proj}}(F,x)^2, u^{-2} \right\}.$$

This minimum equals $\mu_{\mathrm{proj}}(F,x)^2$ since $\kappa_* u \leqslant \frac{1}{13}$, so we get

$$\sqrt{2}\,\kappa_* \geqslant \sqrt{2}\,\kappa(F) \geqslant \sqrt{2}\,\kappa(F,x) \geqslant \mu_{\mathrm{proj}}(F,x) = \mu_{\mathrm{norm}}(\widetilde{F}, x),$$

where $\widetilde{F} := F|_{\mathcal{T}_x}$ denotes the restriction of F to the affine space $\mathcal{T}_x$. From the inequality above, Proposition 4.1, and $u < r$, it follows that

$$\begin{aligned} \alpha(\widetilde{F}, x) &\leqslant \frac{1}{2} D^{\frac{3}{2}} \mu_{\mathrm{norm}}(\widetilde{F}, x)^2 u \leqslant D^{\frac{3}{2}} \kappa_*^2 r, \\ \beta(\widetilde{F}, x) &\leqslant \mu_{\mathrm{norm}}(\widetilde{F}, x) u \leqslant \sqrt{2}\kappa_* r. \end{aligned} \tag{28}$$

From the assumption on r, we get $\alpha(\widetilde{F}, x) \leqslant \frac{1}{13}$, which makes possible the application of Theorem 3.1. We also note that $\beta(\widetilde{F}, x) < \frac{1}{13}$. As in §3.2, we define x_t in the affine space $\mathcal{T}_x$ by the system of differential equations

$$\dot{x}_t = -\mathrm{D}\widetilde{F}(x_t)^\dagger \widetilde{F}(x_t), \quad x_0 = x.$$

Note that $x_t \neq 0$ for all $t \geqslant 0$ as $\|z\| \geqslant 1$ for all $z \in \mathcal{T}_x$. We define $y_t := x_t/\|x_t\| \in \mathbb{S}^n$. By Theorem 3.1, there is a limit point $x_\infty \in \mathcal{T}_x$, which is a zero of $\widetilde{F}$, and which satisfies $\|x_\infty - x\| < 2\beta(\widetilde{F}, x)$. In particular, y_∞ is a zero of F and

$$d_{\mathbb{S}}(y_\infty, x) \leqslant \|x_\infty - x\| \leqslant 2\beta(\widetilde{F}, x) \leqslant 2\sqrt{2}\kappa_* r < 3\kappa_* r,$$

where we used (28) for the second inequality. If $g(y_\infty) \geqslant 0$ for all $g \in G$, then $y_\infty \in S$ and $d_{\mathbb{S}}(x,S) \leqslant d_{\mathbb{S}}(x, y_\infty)$, hence (27) and we are done.

So suppose that $g(y_\infty) < 0$ for some $g \in G$ and let $s > 0$ be the smallest real number such that $g(y_s) = 0$ for some $g \in G$. By construction, the set $H := \{g \in G \mid g(y_s) = 0\}$ is nonempty and element of $G \setminus H$ is positive at y_s. Also, for every $f \in F$,

$$|f(y_s)| = \frac{|f(x_s)|}{\|x_s\|^{\deg f}} \leqslant |f(x_s)| = |f(x)|e^{-s} \leqslant \|f\|re^{-s}$$

where the second equality is due to Theorem 3.1(i). Therefore, $y_s \in \mathrm{Approx}(F^H, G \setminus H, re^{-s})$.

Using again Lemma 4.18 we deduce that $|H| < n-q+1 = \ell$. We can therefore apply the induction hypothesis to the larger set F^H of equations and the smaller set $G \setminus H$ of inequalities; note that $re^{-s} < r$ and $\kappa_*(F^H, G \setminus H) \leqslant \kappa_*$. Thus we obtain

$$\mathrm{Approx}(F^H, G \setminus H, re^{-s}) \subseteq \mathcal{U}_{\mathbb{S}}\left(S(F^H, G \setminus H), 3\kappa_*(F^H, G \setminus H)r\right) \subseteq \mathcal{U}_{\mathbb{S}}\left(S, 3\kappa_* r\right),$$

the latter because $S(F^H, G \setminus H) \subseteq S$ and $\kappa_*(F^H, G \setminus H) \leqslant \kappa_*$. We conclude that

$$d_{\mathbb{S}}(y_s, S) < 3\kappa_* re^{-s}.$$

Also, by Theorem 3.1(ii),

$$d_{\mathbb{S}}(y_s, x) \leqslant \|x_s - x\| \leqslant 2\beta(\widetilde{F}, x)(1 - e^{-s}) < 2\sqrt{2}\kappa_* r(1 - e^{-s}),$$

the last inequality by (28). We finally deduce that

$$d_{\mathbb{S}}(x, S) \leqslant d_{\mathbb{S}}(x, y_s) + d_{\mathbb{S}}(y_s, S) < \left(2\sqrt{2}(1 - e^{-s}) + 3e^{-s}\right)\kappa_* r < 3\kappa_* r,$$

which shows (27) and finishes the proof. □

4.3 The geometry of ill-posedness

In order to analyze the set $\Sigma \subseteq \mathcal{H}_{\boldsymbol{d}}[q]$ of ill-posed inputs, cf. (19), we first study its complex version, defined as

$$\Sigma^{\mathbb{C}} := \left\{F \in \mathcal{H}_{\boldsymbol{d}}^{\mathbb{C}}[q] \mid \exists x \in \mathbb{P}^n \; F(x) = 0,\ \operatorname{rank} \mathrm{D}F(x)_{|T_x} < q\right\}.$$

Here $\mathbb{P}^n$ denotes the complex projective space of dimension n. Note that because of Euler's formula [18, (16.3)] we have

$$\Sigma^{\mathbb{C}} := \left\{F \in \mathcal{H}_{\boldsymbol{d}}^{\mathbb{C}}[q] \mid \exists x \in \mathbb{P}^n \; F(x) = 0,\ \operatorname{rank} \mathrm{D}F(x) < q\right\}.$$

In the special case $q = n + 1$, we have $\Sigma^{\mathbb{C}} := \{F \in \mathcal{H}_{\boldsymbol{d}}^{\mathbb{C}}[n+1] \mid \exists x \in \mathbb{P}^n \; F(x) = 0\}$. It is well known that this is the zero set of the multivariate resultant, which is an irreducible polynomial with integer coefficients and degree $\sum_{i=1}^{n+1} \prod_{k \neq i} d_k$ [35, §13.1], which is at most $(n+1)D^n$. An extension of this result to the case $q \leqslant n$ appears in [28, Proposition 5.3]. We further generalize this result to $q \leqslant n + 1$, slightly improving the bound in passing.

Proposition 4.20. *For any $q \leqslant n + 1$, the variety $\Sigma^{\mathbb{C}} \subseteq \mathcal{H}_{\boldsymbol{d}}^{\mathbb{C}}[q]$ is a hypersurface defined by an irreducible polynomial with integer coefficients of degree at most $n2^nD^n$.*

Proof. We abbreviate $\mathcal{H} := \mathcal{H}_{\boldsymbol{d}}^{\mathbb{C}}[q]$ and first assume $q \leqslant n$. Consider the incidence variety

$$\widetilde{\Sigma^{\mathbb{C}}} := \left\{(F, x, v) \in \mathcal{H} \times (\mathbb{C}^{n+1} \setminus \{0\}) \times (\mathbb{C}^q \setminus \{0\}) \,\middle|\, F(x) = 0 \text{ and } v^T \cdot \mathrm{D}F(x) = 0\right\}. \qquad (29)$$

The projection $\widetilde{\Sigma^{\mathbb{C}}} \to (\mathbb{C}^{n+1} \setminus \{0\}) \times (\mathbb{C}^q \setminus \{0\})$, $(F, x, v) \mapsto (x, v)$ is surjective. Moreover, the fibers are linear subspaces of $\mathcal{H}$ of codimension $n + q$ This implies that $\widetilde{\Sigma^{\mathbb{C}}}$ is irreducible [53, §6.3, Thm. 8] and $\dim \widetilde{\Sigma^{\mathbb{C}}} = (n+1) + q + \dim \mathcal{H} - n - q = \dim \mathcal{H} + 1$. The image of the projection $\widetilde{\Sigma^{\mathbb{C}}} \to \mathcal{H}$, $(F, x, v) \mapsto F$ equals $\Sigma^{\mathbb{C}}$, which is therefore irreducible. Moreover, since the fibers of this projection are generically of dimension 2, it follows that $\dim \Sigma^{\mathbb{C}} = \dim \widetilde{\Sigma^{\mathbb{C}}} - 2 = \dim \mathcal{H} - 1$. Hence

$\Sigma^{\mathbb{C}}$ is indeed an irreducible hypersurface in $\mathcal{H}$. That its defining equation has integer coefficients follows from elimination theory [45, §2.C] and the fact that $\widetilde{\Sigma^{\mathbb{C}}}$ is defined by polynomials with integer coefficients.

For bounding the degree, we consider a variant of $\widetilde{\Sigma^{\mathbb{C}}}$ in a product of projective spaces. More specifically, we consider the variety S of all $(F, x, u) \in \mathbb{P}(\mathcal{H}) \times \mathbb{P}^n \times \mathbb{P}^{q-1}$, which are solutions of the multihomogeneous equations

$$\begin{cases} f_i(x) = 0 & \text{for } 1 \leqslant i \leqslant q, \\ \displaystyle\sum_{i=1}^{q} u_i\, x_0^{D-d_i} \frac{\partial f_i}{\partial x_j}(x) & \text{for } 1 \leqslant j \leqslant n. \end{cases} \tag{30}$$

We note that the projection $(F, x, u) \mapsto F$ maps $S \cap \{X_0 \neq 0\}$ to $\Sigma^{\mathbb{C}}$ and hits all $F \in \Sigma^{\mathbb{C}}$ except those in a lower dimensional subvariety.

We take now hyperplanes $H_1, \ldots, H_{N-1} \subseteq \mathcal{H}$ in general position, where $N := \dim \mathbb{P}(\mathcal{H})$. Let us denote by $\widetilde{H}_k$ the inverse image of H_k under the projection $(F, x, u) \mapsto F$. Then we have

$$\deg \Sigma^{\mathbb{C}} = |H_1 \cap \ldots \cap H_{N-1} \cap \Sigma^{\mathbb{C}}| \;\leqslant\; |\widetilde{H}_1 \cap \ldots \cap \widetilde{H}_{N-1} \cap S| =: M. \tag{31}$$

The number M of intersections points on the right-hand side can be computed with the multiprojective Bézout's theorem, see e.g. [53, §4.2.1][44]. According to this, M equals the coefficient of the monomial $a^N b^n c^{q-1}$ in the product (a, b, c are formal variables)

$$a^{N-1} \prod_{i=1}^{q} (a + d_i b) \prod_{i=1}^{n} (a + (D-1)b + c). \tag{32}$$

For this, note that the equations for $\widetilde{H}_k$ have the multidegree $(1, 0, 0)$, and the equations in (30) have the multidegree $(1, d_i, 0)$ and $(1, D-1, 1)$ with respect to (the coefficients of) F, x, and u, respectively. The coefficient M can be bounded as

$$M \;\leqslant\; q \binom{n}{q-1} D^{q-1} D^{n-q+1} + n \binom{n-1}{q-1} D^q D^{n-q} \;\leqslant\; n 2^n D^n.$$

Indeed, when expanding (32), the left-hand contribution arises from selecting a in exactly one of the q factors in the left product and selecting c in exactly $q-1$ among the n factors of the right product. The right-hand contribution arises from selecting a in exactly one of the n factors in the right product and selecting c in exactly $q-1$ among the remaining $n-1$ factors of the right product.

In the case $q = n+1$ we consider the incidence variety $S := \{(F, x) \mid F(x) = 0\} \subseteq \mathbb{P}(\mathcal{H}) \times \mathbb{P}^n$ and argue similarly. In particular, the multiprojective Bézout's theorem implies that $\deg \Sigma^{\mathbb{C}}$ equals the coefficient of the monomial ab^n in the product $\prod_{i=1}^{n+1}(a + d_i b)$. This leads to the well known formula $\deg \Sigma^{\mathbb{C}} = \sum_i \prod_{k \neq i} d_i$. Since this is bounded by $(n+1)D^n$, the degree bound in this case follows as well. □

The weaker bound $\deg \Sigma^{\mathbb{C}} \leqslant D^{q+n}$, which is good enough for our purpose, can be obtained with a significantly simpler argument. From (29) we obtain with Bézout's Inequality $\deg \widetilde{\Sigma^{\mathbb{C}}} \leqslant D^q \cdot D^n$ [17, §8.2]. (Note that on an open subset we only need n equations out of $v^T \cdot \mathrm{D}F(x) = 0$.) We conclude that $\deg \Sigma^{\mathbb{C}} \leqslant \deg \widetilde{\Sigma^{\mathbb{C}}} \leqslant D^{q+n}$ [17, Lemma 8.32].

Corollary 4.21. *The set $\Sigma_* \subseteq \mathcal{H}_{\boldsymbol{d}}[q\,;\,s]$ of ill-posed homogeneous systems is included in the zero set of a nonzero polynomial with integer coefficients of degree at most $n2^n(s+1)^{n+1}D^n$. The same holds true for the set $\Sigma_*^{\mathrm{aff}} \subseteq \mathcal{P}_{\boldsymbol{d}}[q\,;\,s]$ of ill-posed affine systems.*

Algorithm 1 Covering

Input. A homogeneous semialgebraic system $(F, G) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\,s]$ with $q \leqslant n$.
Precondition. $\kappa_*(F, G)$ is finite.
Output. A finite subset $\mathcal{X}$ of $\mathbb{S}^n$ and an $\varepsilon > 0$.
Postcondition. $\mathcal{U}(\mathcal{X}, \varepsilon)$ is homotopically equivalent to $S(F, G)$.

function Covering(F, G)
  $r \leftarrow 1$
  repeat
    $r \leftarrow r/2$.
    $k_* \leftarrow \max \left\{ \kappa(F^L, x) \;\middle|\; x \in \mathcal{G}_r \text{ and } L \subseteq G \text{ such that } |L| \leqslant n + 1 - q \right\}$
  until $71\, D^{\frac{5}{2}} k_*^2 r < 1$
  return the set $\mathcal{X} := \mathcal{G}_r \cap \operatorname{Approx}(F, G, D^{\frac{1}{2}} r)$ and the real number $\varepsilon := 5Dk_* r$
end function

Proof. For a subset $L = \{i_1, \ldots, i_\ell\}$ of $\{1, \ldots, s\}$, let p_L be the projection

$$p_L \colon \mathcal{H}_{\boldsymbol{d}}[q\,;\,s] \to \mathcal{H}_{\boldsymbol{d}}[q + \ell],\ (f_1, \ldots, f_q, g_1, \ldots, g_s) \in \mathcal{H}_{\boldsymbol{d}}[q\,;\,s] \mapsto (f_1, \ldots, f_q, g_{i_1}, \ldots, g_{i_\ell})$$

By definition of Σ_* and κ_*, Σ_* is the union of the sets $p_L^{-1}(\Sigma_L)$ for all L with $q + |L| \leqslant n+1$, where Σ_L is the appropriate set of ill-posed data in $\mathcal{H}_{\boldsymbol{d}}[q + \ell]$. The number of such subsets L is at most $(s+1)^{n+1-q}$ and we conclude with the fact that, for each of them, $\Sigma_L \subseteq \Sigma_L^{\mathbb{C}} \cap \mathcal{H}_{\boldsymbol{d}}[q + \ell]$ and the latter is the set of real zeros of a polynomial of degree $n2^nD^n$ by Proposition 4.20.

To settle the affine case, note that the scaled homogeneization map (24) has the structure $H \colon \mathbb{R}^N \to \mathbb{R}^N \times \mathbb{R}$, $a \mapsto (a, \|a\|)$ and that Σ_* is scale invariant. By definition, $\Sigma_*^{\text{aff}} = H^{-1}(\Sigma_*)$. Suppose that the polynomial P vanishes on Σ_* and let $P(a, t) = \sum_i P_i(a) t^i$ be its decomposition into homogeneous parts. Then each P_i vanishes on $H^{-1}(\Sigma_*)$. □

5 ALGORITHMS

5.1 The covering algorithm

The main stepping stone towards computing the homology groups of a spherical semialgebraic set S is the computation of a finite set $\mathcal{X}$ and a real $\varepsilon > 0$ such that S is homotopically equivalent to $U_\varepsilon(\mathcal{X})$. We will do so using Theorems 2.8 and 4.19 in conjunction.

For $0 < r < 1$ we define $\mathcal{G}_r$ as the image in $\mathbb{S}^n$ under the map $y \mapsto \frac{y}{\|y\|}$ of the set of points $x \in \mathbb{Z}^{n+1}$ with $\|x\|_\infty = \lceil \frac{\sqrt{n}}{r} \rceil$. We easily check that

$$\mathbb{S}^n \subseteq \bigcup_{x \in \mathcal{G}_r} B_{\mathbb{S}}(x, r), \tag{33}$$

where $B_{\mathbb{S}}(x, r) := \{ y \in \mathbb{S}^n \mid d_{\mathbb{S}}(x, y) < r \}$. Moreover $|\mathcal{G}_r| = (n/r)^{O(n)}$.

Proposition 5.1. *On input F and G, Algorithm* Covering *outputs a finite set $\mathcal{X}$ and an $\varepsilon > 0$ such that $\mathcal{U}(\mathcal{X}, \varepsilon)$ is homotopically equivalent to $S(F, G)$. Moreover, the computation performs $\big((s+n)D\kappa_*\big)^{O(n)}$ arithmetic operations, where $s = |G|$ and $\kappa_* = \kappa_*(F, G)$, and the number $|\mathcal{X}|$ of points in $\mathcal{X}$ is $(nD\kappa_*)^{O(n)}$.*

Proof. Let $\kappa_* := \kappa_*(F, G)$, $S := S(F, G)$ and let r and k_* be the values of the corresponding variables after the *repeat* loop terminates in Algorithm Covering. By design,

$$71\, D^{\frac{5}{2}} k_*^2 r < 1. \tag{34}$$

We will first show that

$$\kappa_* \leqslant (1 + \tfrac{1}{100})k_*. \tag{35}$$

Let $L \subseteq G$ and $y \in \mathbb{S}^n$ be such that $\kappa_* = \kappa(F^L) = \kappa(F^L, y)$. Because of (33) there is some $x \in \mathcal{G}_r$ such that $d_{\mathbb{S}}(x, y) < r$, and $\kappa(F^L, x) \leqslant k_*$ by the definition of k_*. Since the map $x \mapsto 1/\kappa(F^L, x)$ is D-Lipschitz continuous (Proposition 4.7), we have

$$\kappa_* = \kappa(F^L, y) \leqslant \frac{\kappa(F^L, x)}{1 - D\kappa(F^L, x)r} \leqslant \frac{k_*}{1 - Dk_* r}.$$

Inequality (34) shows that

$$Dk_* r < \frac{1}{71\, D^{\frac{3}{2}} k_*} \leqslant \frac{1}{101}$$

the last as $D \geqslant 2$ and $k_* \geqslant 1$, and Inequality (35) follows.

Let $\mathcal{X} := \mathcal{G}_r \cap \operatorname{Approx}(F, G, D^{\frac{1}{2}} r)$ and $\varepsilon := 5Dk_* r$, that is, the finite set and the real number output by the algorithm. We will now prove that $\mathcal{U}(\mathcal{X}, \varepsilon)$ is homotopically equivalent to S. By Theorem 2.8, it is enough to prove the inequalities

$$3d_H(\mathcal{X}, S) < \varepsilon < \frac{1}{2}\tau(S). \tag{36}$$

The second inequality follows from Inequalities (34), (35) and Theorem 4.12:

$$\varepsilon = 5Dk_* r < \frac{5}{71}\, \frac{1}{D^{\frac{3}{2}} k_*} \leqslant \frac{505}{7100}\, \frac{1}{D^{\frac{3}{2}} \kappa_*} \leqslant \frac{3535}{7100}\tau(S) \leqslant \frac{1}{2}\tau(S).$$

Concerning the inequality $3d_H(\mathcal{X}, S) < \varepsilon$, let $x \in S$. Because of (33), there is some $y \in \mathcal{G}_r$ with $d_{\mathbb{S}}(x, y) < r$. Hence y lies in $\operatorname{Approx}(F, G, D^{\frac{1}{2}} r)$, by Proposition 4.17. Thus $y \in \mathcal{X}$ and $d(x, \mathcal{X}) < d_{\mathbb{S}}(x, y) < r < \frac{1}{3}\varepsilon$.

Next, let $x \in \mathcal{X}$. Then, $x \in \operatorname{Approx}(F, G, D^{\frac{1}{2}} r)$ and

$$13\, D^{\frac{3}{2}} \kappa_*^2 (D^{\frac{1}{2}} r) < 71\, D^{\frac{5}{2}} \kappa_*^2 r < 1$$

the last by Inequality (34). Hence, Theorem 4.19 applies and shows that

$$d(x, S) \leqslant d_{\mathbb{S}}(x, S) \leqslant 3\kappa_* D^{\frac{1}{2}} r \leqslant (3 + \tfrac{3}{100})k_* D^{\frac{1}{2}} r < \frac{1}{3}\varepsilon,$$

where we used $D \geqslant 2$ for the last inequality. Thus we have shown that $d_H(\mathcal{X}, S) < \frac{1}{3}\varepsilon$. This concludes the proof of (36) and of the homotopy equivalence.

Lastly, we deal with the complexity analysis. We can approximate $\kappa(F^L, x)$ within a factor of 2 in $O(N + n^3)$ operations [43, §2.5] and this is enough for our needs. For simplicity, we will do as if we could compute κ exactly.

The *repeat* loop performs $O(\log(D\kappa_*))$ iterations. Each iteration can be done in $O(|\mathcal{G}_r| M(N + n^3))$ operations, where $M = \sum_{i=0}^{n+1-q} \binom{s}{i} \leqslant (s+1)^{n+1-q}$. Moreover, $|\mathcal{X}| \leqslant |\mathcal{G}_r| = (nD\kappa_*)^{O(n)}$ and $N + n^3 = (nD)^{O(n)}$. Therefore, the total number of operations is bounded by $\big((s+n)D\kappa_*\big)^{O(n)}$. □

5.2 Homology of a union of balls

Once in the possession of a pair $(\mathcal{X}, \varepsilon)$ such that S is a deformation retract of $\mathcal{U}(\mathcal{X}, \varepsilon)$, the computation of the homology groups of S is a known process. One computes the nerve $\mathcal{N}$ of the covering $\{B(x, \varepsilon) \mid x \in \mathcal{X}\}$ (this is a simplicial complex whose elements are the subsets N of $\mathcal{X}$ such that $\cap_{x \in N} B(x, \varepsilon)$ is not empty) and from it, its homology groups $H_k(\mathcal{N})$. Since the intersections of any collection of balls is convex, the Nerve Theorem [e.g. 12, Thm. 10.7] ensures that

$$H_k(\mathcal{N}) \simeq H_k(\mathcal{U}(\mathcal{X}, \varepsilon)) \simeq H_k(S)$$

Algorithm 2 HOMOLOGY

Input. A semialgebraic system $(F, G) \in \mathcal{P}_{\boldsymbol{d}}[q+s]$ with $q \leqslant n$.
Output. The homology groups of the set $\{f_1 = \cdots = f_q = 0 \text{ and } g_1 > 0, \ldots, g_q > 0\} \subseteq \mathbb{R}^n$.

```
function HOMOLOGY(F, G)
    (X, ε) ← COVERING(H(F, G))
    N ← the nerve of U(X, ε)
    return the homology groups of N
end function
```

the last because S is a deformation retract of $\mathcal{U}(\mathcal{X}, \varepsilon)$.

The process is described in detail in of [28, §4] where the proof for the following result can be found (see also [31, 33] for improved algorithms for computing the nerve of a covering).

PROPOSITION 5.2. *Given a finite set $\mathcal{X} \subseteq \mathbb{R}^{n+1}$ and a positive real number ε, one can compute the homology of $\cup_{x \in \mathcal{X}} B(x, \varepsilon)$ with $|\mathcal{X}|^{O(n)}$ operations.* □

5.3 Homology of affine semialgebraic sets

A pair $(F, G) \in \mathcal{P}_{\boldsymbol{d}}[q\,;\,s]$ defines a basic semialgebraic set $W(F, G) \subseteq \mathbb{R}^n$ as in (1) which is diffeomorphic to the subset of $\mathbb{S}^n$ defined by $F^{\mathrm{h}} = 0$, $G^{\mathrm{h}} \succ 0$ and $X_0 > 0$. As in §4.1.5, let $H(F, G) \in \mathcal{H}_{(\boldsymbol{d},1)}[q\,;\,s+1]$ denote this system of homogeneous polynomials (with $X_0 > 0$ replaced by $\|(F, G)\| X_0 > 0$, which does not change the solution set). Proposition 4.14 tells us that, unless this system is ill-posed, we may replace $X_0 > 0$ with $X_0 \geqslant 0$ and any $g > 0$ with $g \geqslant 0$ without changing the homology of the solution set. In other words, if $\kappa_*^{\mathrm{aff}}(F, G) < \infty$, then the spherical set $S(H(F, G))$ is homotopically equivalent to $W(F, G)$.

Based on the tools introduced above, we may compute the homology of $W(F, G)$, assuming that $\kappa_*^{\mathrm{aff}}(F, G) < \infty$, by computing the nerve of a suitable covering of $S(H(F, G))$ obtained with Algorithm COVERING. This leads to Algorithm HOMOLOGY below whose analysis will prove Theorem 1.1.

PROOF OF THEOREM 1.1 (I). By Proposition 5.1, the cost of computing the covering $\mathcal{X}$ is bounded by $\left((s+n)D\kappa_*^{\mathrm{aff}}\right)^{O(n)}$, where $\kappa_*^{\mathrm{aff}} := \kappa_*^{\mathrm{aff}}(F, G)$, and $|\mathcal{X}| = (nD\kappa_*^{\mathrm{aff}})^{O(n)}$. By Proposition 5.2, the cost of computing the nerve $\mathcal{N}$ and its homology groups is $|\mathcal{X}|^{O(n)}$. Hence, the total cost of the algorithm is bounded by $\left((s+n)D\kappa_*^{\mathrm{aff}}\right)^{O(n^2)}$. Together with Proposition 4.16, this leads to the conclusion. □

The probabilistic analysis is based on the following result by Bürgisser and Cucker [18, Theorem 21.1] and follows a line of similar results that rely on the same ideas. We will be consequently brief. We rephrased the statement in terms of the isotropic Gaussian distribution instead of the uniform distribution on the sphere. The scale invariance of the statement makes both formulations equivalent.

THEOREM 5.3. *Let $\Sigma \subseteq \mathbb{R}^{p+1}$ be contained in a real algebraic hypersurface, given as the zero set of a homogeneous polynomial of degree d and let $a \in \mathbb{R}^{p+1}$ be a centered isotropic Gaussian random variable. Then for all $t \geqslant (2d+1)p$,*

$$\operatorname{Prob}\left(\frac{\|a\|}{d(a, \Sigma)} \geqslant t\right) \leqslant \frac{11dp}{t}.$$ □

PROOF OF THEOREM 1.1 (II) AND (III). Let $\psi = (F, G) \in \mathcal{P}_{\boldsymbol{d}}[q\,;\,s]$ be a centered isotropic Gaussian random variable. By Theorem 1.1 (i), the number of operations performed by algorithm HOMOLOGY is

$$\operatorname{cost}(\psi) = \left((s+n)D\frac{\|\psi\|}{d(\psi, \Sigma_*^{\mathrm{aff}})}\right)^{Cn^2},$$

for some $C > 0$.

By Theorem 5.3 and Corollary 4.21,

$$\operatorname{Prob}\left(\operatorname{cost}(\psi) \geqslant \left(\left((s+n)Dt\right)^{Cn^2}\right)\right) \leqslant \frac{11n2^n(s+1)^{n+1}D^nN}{t} = \frac{((s+n)D)^{O(n)}}{t},$$

where $N := \dim \mathcal{P}_{\boldsymbol{d}}[q\,;\,s] \leqslant (s+n)(D+1)^n$. We obtain Theorem 1.1(ii) with $t = ((s+n)D)^{cn}$ and Theorem 1.1(iii) with $t = 2^{cN}$, for some c large enough. For the latter, we use that $\left((s+n)D\right)^{O(n)} = 2^{O(N)}$ and that $n^2 = O(N)$. □

ACKNOWLEDGMENTS

We are grateful to Josué Tonelli-Cueto and Mohab Safey El Din for helpful discussions, to Teresa Krick for her careful reading, and to Théo Lacombe and the referees for relevant remarks.

This work has been supported by the Einstein Foundation, Berlin, by the DFG research grant no. BU 1371/2-2, and by the Research Grants Council of the Hong Kong SAR project no. CityU-11202017.

REFERENCES

[1] D. Amelunxen and M. Lotz. 2017. Average-case complexity without the black swans. *J. Complexity* 41 (2017), 82–101.

[2] Saugata Basu. 1996. On Bounding the Betti Numbers and Computing the Euler Characteristic of Semi-Algebraic Sets. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. ACM, 408–417.

[3] Saugata Basu. 2006. Computing the First Few Betti Numbers of Semi-Algebraic Sets in Single Exponential Time. *J. Symb. Comput.* 41, 10 (2006), 1125–1154. https://doi.org/10.1016/j.jsc.2006.07.001

[4] S. Basu. 2008. Algorithmic semi-algebraic geometry and topology—recent progress and open problems. In *Surveys on discrete and computational geometry*. Contemp. Math., Vol. 453. Amer. Math. Soc., Providence, RI, 139–212.

[5] S. Basu. 2008. Computing the top Betti numbers of semialgebraic sets defined by quadratic inequalities in polynomial time. *Found. Comput. Math.* 8 (2008), 45–80.

[6] S. Basu, R. Pollack, and M.-F. Roy. 1996. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM* 43 (1996), 1002–1045.

[7] S. Basu, R. Pollack, and M.-F. Roy. 1999. Computing roadmaps of semi-algebraic sets on a variety. *J. Amer. Math. Soc.* 33 (1999), 55–82.

[8] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. 2005. Computing the First Betti Number and the Connected Components of Semi-Algebraic Sets. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing (STOC '05)*. ACM, New York, NY, USA, 304–312. https://doi.org/10.1145/1060590.1060636

[9] S. Basu, R. Pollack, and M.-F. Roy. 2006. Computing the Dimension of a Semi-Algebraic Set. *J Math Sci* 134, 5 (2006), 2346–2353. https://doi.org/10.1007/s10958-006-0111-0

[10] S. Basu, R. Pollack, and M.-F. Roy. 2008. Computing the first Betti number of a semi-algebraic set. *Found. Comput. Math.* 8, 1 (2008), 97–136.

[11] S. Basu, M.-F. Roy, M. Safey El Din, and É Schost. 2014. A Baby Step–Giant Step Roadmap Algorithm for General Algebraic Sets. *Found Comput Math* 14, 6 (2014), 1117–1172. https://doi.org/10.1007/s10208-014-9212-1

[12] A. Björner. 1995. Topological methods. In *Handbook of Combinatorics*, R. Graham, M. Grotschel, and L. Lovasz (Eds.). North-Holland, Amsterdam, 1819–1872.

[13] Lenore Blum, Michael Shub, and Steve Smale. 1989. On a Theory of Computation and Complexity over the Real Numbers: NP-Completeness, Recursive Functions and Universal Machines. *Bull. Amer. Math. Soc.* 21, 1 (1989), 1–46. https://doi.org/10.1090/S0273-0979-1989-15750-9

[14] A. Borodin. 1977. On relating time and space to size and depth. *SIAM J. Comp.* 6 (1977), 733–744.

[15] Nicolas Bourbaki. 2004. *Functions of a real variable.* Springer-Verlag, Berlin. https://doi.org/10.1007/978-3-642-59315-4

[16] Morton Brown. 1962. Locally Flat Imbeddings of Topological Manifolds. *Ann. of Math. (2)* 75 (1962), 331–341. https://doi.org/10.2307/1970177

[17] P. Bürgisser, M. Clausen, and A. Shokrollahi. 1996. *Algebraic Complexity Theory.* Grundlehren der mathematischen Wissenschaften, Vol. 315. Springer-Verlag.

[18] P. Bürgisser and F. Cucker. 2013. *Condition.* Grundlehren der mathematischen Wissenschaften, Vol. 349. Springer-Verlag, Berlin.
[19] John Canny. 1993. Computing roadmaps of general semi-algebraic sets. *Comput. J.* 36 (1993), 504–514. https://doi.org/10.1093/comjnl/36.5.504
[20] J. Canny, D. Yu. Grigorev, and N. N. Vorobjov, Jr. 1992. Finding connected components of a semialgebraic set in subexponential time. *Appl. Algebra Engrg. Comm. Comput.* 2, 4 (1992), 217–238. https://doi.org/10.1007/BF01614146
[21] J. F. Canny. 1991. Computing Roadmaps of General Semi-Algebraic Sets. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Lecture Notes in Computer Science).* Springer, Berlin, Heidelberg, 94–107. https://doi.org/10.1007/3-540-54522-0_99
[22] Frédéric Chazal, David Cohen-Steiner, and André Lieutier. 2009. A Sampling Theory for Compact Sets in Euclidean Space. *Discrete Comput. Geom.* 41, 3 (2009), 461–479. https://doi.org/10.1007/s00454-009-9144-8
[23] G.E. Collins. 1975. *Quantifier elimination for real closed fields by cylindrical algebraic deccomposition.* Lect. Notes in Comp. Sci., Vol. 33. Springer-Verlag, 134–183.
[24] Robert Connelly. 1971. A New Proof of Brown's Collaring Theorem. *Proc. Am. Math. Soc.* 27, 1 (1971), 180. https://doi.org/10.2307/2037284
[25] F. Cucker. 1999. Approximate zeros and condition numbers. *J. Complexity* 15 (1999), 214–226.
[26] F. Cucker, T. Krick, G. Malajovich, and M. Wschebor. 2008. A numerical algorithm for zero counting. I: Complexity and accuracy. *J. Complexity* 24 (2008), 582–605.
[27] F. Cucker, T. Krick, G. Malajovich, and M. Wschebor. 2009. A numerical algorithm for zero counting. II: Distance to ill-posedness and smoothed analysis. *J. Fixed Point Theory Appl.* 6 (2009), 285–294.
[28] Felipe Cucker, Teresa Krick, and Michael Shub. 2018. Computing the Homology of Real Projective Sets. *Found. Comput. Math.* 18, 4 (2018), 929–970. https://doi.org/10.1007/s10208-017-9358-8
[29] F. Cucker and S. Smale. 1999. Complexity Estimates depending on Condition and round-off error. *J. ACM* 46 (1999), 113–184.
[30] Jean-Pierre Dedieu. 2006. *Points Fixes, Zéros et La Méthode de Newton.* Mathématiques & Applications, Vol. 54. Springer. https://doi.org/10.1007/3-540-37660-7
[31] H. Edelsbrunner. 1995. The Union of Balls and Its Dual Shape. *Discrete Comput. Geom.* 13, 3 (1995), 415–440. https://doi.org/10.1007/BF02574053
[32] Herbert Edelsbrunner and Ernst P. Mücke. 1994. Three-Dimensional Alpha Shapes. *ACM Trans Graph* 13, 1 (Jan. 1994), 43–72. https://doi.org/10.1145/174462.156635
[33] H. Edelsbrunner and N. R. Shah. 1992. Incremental Topological Flipping Works for Regular Triangulations. ACM Press, 43–52. https://doi.org/10.1145/142675.142688
[34] Herbert Federer. 1959. Curvature Measures. *Trans. Am. Math. Soc.* 93, 3 (1959), 418–491.
[35] Israel M. Gelfand, Mikhail M. Kapranov, and Andrei V. Zelevinsky. 1994. *Discriminants, Resultants, and Multidimensional Determinants.* Birkhäuser Boston Inc., Boston, MA.
[36] Gene H. Golub and Victor Pereyra. 1973. The Differentiation of Pseudo-Inverses and Nonlinear Least Squares Problems Whose Variables Separate. *SIAM J. Numer. Anal.* 10, 2 (1973), 413–432.
[37] D. Yu. Grigor'ev and N. N. Vorobjov. 1988. Solving Systems of Polynomial Inequalities in Subexponential Time. *Journal of Symbolic Computation* 5, 1 (1988), 37–64. https://doi.org/10.1016/S0747-7171(88)80005-1
[38] D.Yu. Grigoriev and N.N. Vorobjov. 1992. Counting connected components of a semialgebraic set in subexponential time. *Computational Complexity* 2 (1992), 133–186.
[39] Joos Heintz, Marie-Françoise Roy, and Pablo Solernó. 1994. Single exponential path finding in semi-algebraic sets. II. The general case. In *Algebraic geometry and its applications (West Lafayette, IN, 1990).* Springer, New York, 449–465.
[40] M.R. Hestenes and E. Stiefel. 1952. Methods of conjugate gradients for solving linear systems. *J. Research Nat. Bur. Standards* 49 (1952), 409–436 (1953).
[41] P. Koiran. 1999. The real dimension problem is $\mathsf{NP}_{\mathbb{R}}$-complete. *J. Complexity* 15 (1999), 227–238.
[42] E. Kostlan. 1988. Complexity theory of numerical linear algebra. *J. of Computational and Applied Mathematics* 22 (1988), 219–230.
[43] Pierre Lairez. 2017. Rigid Continuation Paths I. Quasilinear Average Complexity for Solving Polynomial Systems. arXiv:1711.03420
[44] Alexander Morgan and Andrew Sommese. 1987. A Homotopy for Solving General Polynomial Systems That Respects M-Homogeneous Structures. *Appl. Math. Comput.* 24, 2 (1987), 101–113.
[45] D. Mumford. 1976. *Algebraic Geometry I, Complex Projective Varieties.* Springer-Verlag.
[46] I. P. Natanson. 1955. *Theory of Functions of a Real Variable.* Frederick Ungar Publishing Co., New York.
[47] Partha Niyogi, Stephen Smale, and Shmuel Weinberger. 2008. Finding the Homology of Submanifolds with High Confidence from Random Samples. *Discrete Comput. Geom.* 39, 1 (2008), 419–441. https://doi.org/10.1007/s00454-008-9053-2

[48] P. Niyogi, S. Smale, and S. Weinberger. 2008. Finding the homology of submanifolds with high confidence from random samples. *Discrete Comput. Geom.* 39 (2008), 419–441.

[49] J. Renegar. 1992. On the Computational Complexity and Geometry of the First-order Theory of the Reals. Part I. *Journal of Symbolic Computation* 13 (1992), 255–299.

[50] Mohab Safey El Din and Éric Schost. 2017. A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets. *J. ACM* 63, 6 (2017), 48:1–48:37. https://doi.org/10.1145/2996450

[51] P. Scheiblechner. 2007. On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety. *J. Complexity* 23 (2007), 359–379.

[52] P. Scheiblechner. 2012. Castelnuovo-Mumford regularity and computing the de Rham cohomology of smooth projective varieties. *Found. Comput. Math.* 12 (2012), 541–571.

[53] I.R. Shafarevich. 1994. *Basic Algebraic Geometry. 1: Varieties in Projective Space* (2 ed.). Springer-Verlag.

[54] M. Shub and S. Smale. 1993. Complexity of Bézout's Theorem I: geometric aspects. *J. Amer. Math. Soc.* 6 (1993), 459–501.

[55] M. Shub and S. Smale. 1993. Complexity of Bézout's Theorem II: volumes and probabilities. In *Computational Algebraic Geometry (Progress in Mathematics)*, F. Eyssette and A. Galligo (Eds.), Vol. 109. Birkhäuser, 267–285.

[56] M. Shub and S. Smale. 1993. Complexity of Bézout's Theorem III: condition number and packing. *Journal of Complexity* 9 (1993), 4–14.

[57] M. Shub and S. Smale. 1994. Complexity of Bézout's Theorem V: polynomial time. *Theoret. Comp. Sci.* 133 (1994), 141–164.

[58] M. Shub and S. Smale. 1996. Complexity of Bézout's Theorem IV: probability of success; extensions. *SIAM J. of Numer. Anal.* 33 (1996), 128–148.

[59] Steve Smale. 1986. Newton's Method Estimates from Data at One Point. In *The Merging of Disciplines: New Directions in Pure, Applied, and Computational Mathematics (Laramie, Wyo., 1985)*. Springer, New York, 185–196.

[60] S. Smale. 1997. Complexity theory and Numerical Analysis. In *Acta Numerica*, A. Iserles (Ed.). Cambridge University Press, 523–551.

[61] A.M. Turing. 1948. Rounding-off errors in matrix processes. *Quart. J. Mech. Appl. Math.* 1 (1948), 287–308.

[62] J. von Neumann and H.H. Goldstine. 1947. Numerical inverting matrices of high order. *Bulletin of the Amer. Math. Soc.* 53 (1947), 1021–1099.

[63] H.R. Wüthrich. 1976. Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper. In *Komplexität von Entscheidungsproblemen (Lect. Notes in Comp. Sci.)*, E. Specker and V. Strassen (Eds.), Vol. 43. Springer-Verlag, 138–162.