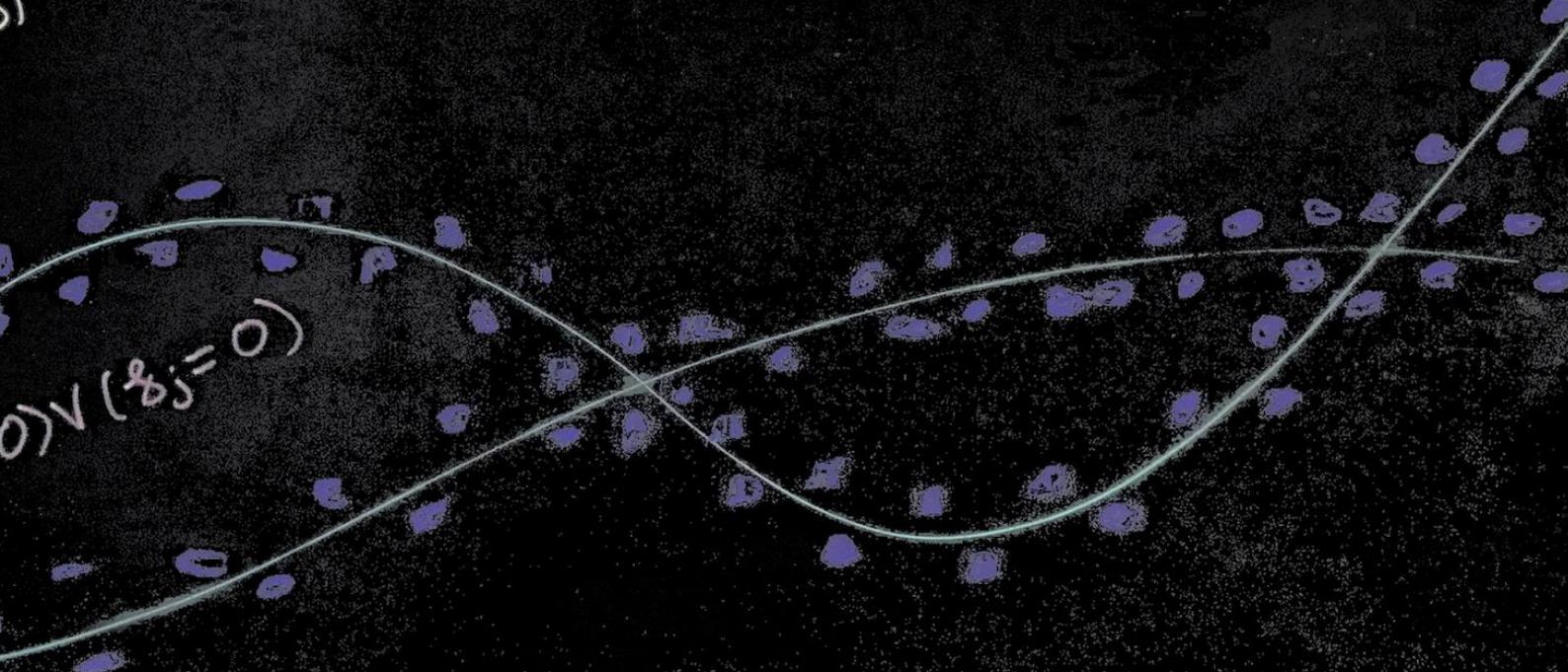


Condition and Homology in Semialgebraic Geometry



Josué Tonelli-Cueto



Condition and Homology in Semialgebraic Geometry

vorgelegt von

M. Sc.

Josué TONELLI CUETO

 ORCID: 0000-0002-2904-1215

von der Fakultät II –Mathematik und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktor der Naturwissenschaften
Dr. rer. nat.

genehmigte Dissertation

PROMOTIONSausschuss:

Vorsitzender: Prof. Dr. John M. SULLIVAN
Gutachter: Prof. Dr. Peter BÜRGISSE
Prof. Dr. Felipe CUCKER
C.R. Dr. Pierre LAIREZ

Tag der wissenschaftlichen Aussprache: 28. November 2019

gefördert durch die Einstein Stiftung Berlin
im Rahmen des Einstein Visiting Fellowships von Felipe Cucker

Berlin 2019

Abstract

The computation of the homology groups of semialgebraic sets (given by Boolean formulas) remains one of the open challenges of computational semialgebraic geometry. Despite the search for an algorithm taking singly exponential time only on the number of variables, as of today, the existing algorithms are symbolic and doubly exponential. In this PhD thesis, we show how to obtain a numerical algorithm running in single exponential time with very high probability, which improves the state-of-the-art. To do so, we explain the underlying ideas, methods and techniques from numerical algebraic geometry, numerical complexity and topological data analysis that made this progress possible. We finish with a list of open problems and questions pointing to a possible future of the numerical computation of topological invariants.

Additionally, in the appendices, we cover the topic of the expected number of real zeros of a random fewnomial system and we give an accessible account of the central theme in Spanish.

Zusammenfassung

Die Berechnung der Homologiegruppen von semialgebraischen Mengen (gegeben durch boolesche Formeln) bleibt eine der offenen Herausforderungen der algorithmischen semialgebraischen Geometrie. Trotz der Suche nach einem Algorithmus mit einfach exponentieller Laufzeit in der Anzahl der Variablen, sind die nach heutigem Stand bekannten Algorithmen symbolisch und doppelt exponentiell. In dieser Doktorarbeit zeigen wir, wie man einen numerischen Algorithmus konstruiert, der mit großer Wahrscheinlichkeit einfach exponentiell ist und somit den Stand der Forschung verbessert. Dazu erklären wir die zugrundliegenden Ideen, Methoden und Techniken von numerischer algebraischen Geometrie, numerischer Komplexität und topologischer Datenanalyse, die dieser Fortschritt möglich machten. Wir enden mit einer Liste offener Probleme und Fragen, die auf eine mögliche Zukunft von Berechnung der topologischen Invarianten weisen.

Außerdem, behandeln wir im Anhange die erwartete Anzahl reeller Nullstellen eines zufälligen Systems polynomialer Gleichungen mit wenigen Termen und geben einen informellen Überblick über das Hauptthema auf Spanisch.

Laburpena

Multzo semialgebraikoak (formula booleanoak emandakoak) homologia-taldeak kalkulatzek jarraitzen du, oraindik ere, geometria semialgebraiko konputacionalaren erronka handienetako bat izaten. Bilatzen den algoritmoak aldagai kopuruan baino ez du hartzen denbora behin esponentziala; hala ere, gaur egun dauden algoritmo guztiak simbolikoak eta bi aldiz esponentzialak dira. Doktorego-tesi honetan erakusten dugu nola lor daitekeen debora behin esponentzialean eta probabilitate handiarekin exekutatzen den zenbakizko algoritmo bat; hori teknikaren egoeraren hobekuntza da. Horretarako, zenbakizko geometria algebraikoaren, zenbakizko konplexutasunaren eta datu-analisi topologikoaren azpian dauden eta aurrerapen hori posible egin duten ideia, metodo eta teknikak azaltzen ditugu. Problemen eta galdera irekien zerrenda batekin bukatzen dugu, zeinek invariante topologikoen zenbakizko konputazioaren etorkizun posible bat adierazten baitute.

Gainera, eranskinetan, ausazko sistema oligonomiko baten zero kopurua aztertzen dugu, eta tesi honen ikuspegi informalak ematen dugu gaztelaniaz.

Resumen

El cálculo de los grupos de homología de conjuntos semialgebraicos (dados por fórmulas booleanas) es todavía uno de los mayores desafíos de la geometría semialgebraica computacional. Aunque se busca un algoritmo que tome a lo sumo tiempo simplemente exponencial en el número de variables, hasta el día de hoy todos los algoritmos existentes son simbólicos y doblemente exponenciales. En esta tesis doctoral, mostramos cómo se puede obtener un algoritmo numérico que tome tiempo simplemente exponencial con alta probabilidad, lo cual es una mejora del estado del arte. Para ello, explicamos las ideas, métodos y técnicas subyacentes procedentes de la geometría algebraica numérica, de la complejidad numérica y del análisis topológico de datos que han hecho posible este progreso. Terminamos con una lista de problemas y preguntas abiertas que indican un posible futuro de la computación numérica de invariantes topológicos.

Además, en los apéndices, estudiamos el número esperado de ceros reales de un sistema oligomórfico aleatorio y damos una visión informal del tema principal de esta tesis en castellano.

А Евгения,
por todo el apoyo y comprensión durante este duro camino

A Leviathan,
por esperarme casi todas las noches aunque llegara de madrugada

A todas aquellas personas que me han acompañado durante todos estos años en Berlín,
although not exclusively, particularly to:

Nela
Justine
Ana
András
JD
Eddie
Giulia
Marek
Rinat
Shane
Qianheng
Robbie

Acknowledgments, agradecimientos eta beste esker onak

Agradezco a mis dos directores de tesis Peter Bürgisser and Felipe Cucker for their constant support, scientific guidance, mathematical discussions and the opportunity to do my PhD under their supervision. Alde batetik, I give thanks to Peter for his attention to detail and his Swiss clock-maker's precision in both mathematics and mathematical writing, eta beste aldetik, Felipe eskertzen dut por todas sus historias, su estilo de trabajo centrado y constante y su acogida tanto en Hong Kong como en Tuileries d'Affiac. At last but not least, I specially give them thanks for passing on their love for complexity, numerical algorithms and random algebraic geometry on to me.



Figure FP: Peter Bürgisser (right) and Felipe Cucker (left) drawn by Jorge Chan

I must specially thank Alperen Ergür for all the days we have shared in the office in Berlin, his mentoring during these years, and all our conversations, mathematical or not. I can certainly claim that without the latter, I would have not developed as much as I did as a mathematician and a person.

I also want to take this chance to specially thank the secretary of the group Beate Nießen for her help with the bureaucracy, which has made my academic life a lot easier than what it would have been without her help.

Some parts of this thesis employ extensively words and expressions que vienen de otras lenguas distintas a la inglesa. Because of this, I must thank the people who checked those. Agradezco a Marta Macho-Stadler por la revision del resumen en castellano, a Julio García de los Salmones (also known as “Puño de Hierro”) por el resumen en euskera; y a Ana Barrena Lertxundi und Philipp Reichenbach por el resumen en alemán. Aditonally, I want to give thanks to Qianheng Cheng for checking my use of Chinese in this writing, to Evgenia Lagoda for checking my use of Russian; and to Mariane Eguía Sarachaga, Justine Mullon and Pierre Lairez for useful discussions about how the title of Chapter 3 should be.

Regarding the thesis, I want to thank Matías Bender, Ricardo Grande and Evgenia Lagoda for useful comments about the introduction (Chapter 0) of this thesis, Alicia Dickenstein for answering my questions regarding her latest work with Bihan and Forsgård [59], Teresa Krick for pointing many typos in the read version, Pierre Lairez for providing me with a digital copy of the master’s thesis of his student Jiadong Han [213], Marta Macho-Stadler for extensive comments on Appendix M, and Frank Sottile for giving me access to the documents attached to the letter of Kushnirenko [268]. Also, I am thankful to Pierre Lairez and to John M. Sullivan for accepting being part of my doctoral committee.

Regarding my academic stays, I want to thank Nicolai Vorobjov for kindly hosting me in Bath for a research visit, and Elias Tsigaridas for his invitation to Paris. Regarding the personal side of these stays, estoy enormemente agradecido por la acogida y el cariño ofrecido por Antonia, Alfonso, Matías, Tomás y Tatiana.

In these years, many people has accompanied and supported me, either directly or indirectly, either by direct interaction or action at a distance. Even if I don’t mention them by name, I am thankful to all of them.

In Berlin, I want to particularly thank the following people: Nela, Justine, Eddie, JD, Rinat, Marek, Shane, Matthias, Robbie, Max, Flavie, Tiho, Mia and Lorena, for all the nights out and all the shared moments; Ana, Dani y Zara, por todos los momentos compartidos durante y después del Soulkino; les compañeres del Círculo Podemos Berlin, especialmente Concha, Raquel, Lluis, Cristina, Pedro, Mariágeles, y de nuevo, Ana y Zara; András, Giulia, Qianheng, Héctor, Marco, Yuya, Levent, Duca and Jorge, for the shared experience in and out of the BMS; Alex and Sophia, for all the movie and aftermovie moments; Qiao, Brent, and again, Héctor and Yuya, for our joint venture as BMS Student Representatives and organizers of the 6th BMS Student Conference; Tommaso, Georg, Irem, Asilya, Konstantin, Barbara, Stefan, Riccardo, Simona, Johanna, Michael, Gregor, and again, András, Giulia, Qianheng, Marco, Duca and Levent, for the collective effort in the organization of the “*What is . . .?*” Seminar; and Matías, Philipp, Paul, Sascha, Mario and Philipp, for the daily life in the working group.

Fuera de Berlín, quiero agradecer particularmente a las siguientes personas: Aitzeder, por seguir siendo mi amigo tras tanto tiempo estando siempre ahí; Marta, Ricardo, Iratxe, Tere, Mikel, Adrián, Maider, Leire, Ion y Miren, por mantener la amistad y el contacto en la distancia; Oihane, Julene, Andrea, y de nuevo, Iratxe y Maider, por mantener el contacto y encontrar tiempo para reunirnos cada año para rememorar viejos tiempos; mis profesores

de la Licenciatura en Matemáticas, en particular, Charo, Luis, Raúl, Ion, Gustavo, Josu, Virginia, Lourdes, Pedro, Eugenio, y de nuevo, Marta, por lo que les debo en mi formación matemática; Jose y Raimundo, por su aprecio desde que soy niño; mi familia, Juan, Isabel, Pablo, Elena, Ana Lara, Paco, Anita, Ramonín y Ramón, por estar ahí; y, especialmente, mis padres, por todo.

And concluding in the obvious way, very special thanks to Евгения and Leviathan.

The completion of this PhD Thesis and the Phase II of the Berlin Mathematical School (BMS) was possible thanks to the doctoral fellowship awarded to me by the *Berlin Mathematical School* within the framework of Felipe Cucker's Einstein Visiting Fellowship "Complexity and accuracy of numerical algorithms in algebra and geometry" and which was funded by the *Einstein Foundation Berlin*.



Der Abschluss dieser Doktorarbeit und der Phase II an der Berlin Mathematical School (BMS) wurde durch ein Stipendium ermöglicht, das mir die *Berlin Mathematical School* im Rahmen des Einstein Visiting Fellowships „Complexity and accuracy of numerical algorithms in algebra and geometry“ von Felipe Cucker vergab und welches durch die *Einstein Stiftung Berlin* gefördert wurde.

Assumptions and conventions

Personal Pronoun Pronouncement

Following Spivak [Q16; *Personal Pronoun Pronouncement*], we will use a genderless pronoun, now known today as the *Spivak pronoun*, to avoid the gender specification whenever we refer to a person of undetermined gender (like a random mathematician or the reader). In this way, we will use “E” instead of “he or she” or “they”, “Em” instead of “him or her” or “them”, and “Eir” instead of “his or her” or “their”.

Conventions on translations and transliterations

Translations Whenever we have consulted a translated work, we cite the translation together with a note indicating which work is a translation of instead of adding a reference to the original work also. See [413] for an example.

Transliterations to the Latin alphabet The general convention has been to use the transliteration preferred by the author if possible, and the most accepted one otherwise. This allows us to be consistent and to avoid referring to the same author by several names. However, this means that the used spelling of the romanized name might differ from that of a particular referred reference, which will be probably the case for names that have changed their transliteration over time (such as names with Cyrillic spelling). If the cited reference is written in the author’s mother tongue, we additionally indicate in parenthesis the spelling of the author’s name in the original alphabet (as it can be seen in the reference [414]).

Assumptions on the reader and mathematical conventions

This thesis, as any other mathematics text in history and in the world, will assume certain knowledge on the part of the reader. With the exception of the last appendix, which requires Spanish knowledge, but no mathematical knowledge; the thesis will assume on the reader the ability to read and understand English¹, some mathematical knowledge and certain mathematical maturity. The latter should be interpreted as having an ability to follow and understand mathematical ideas and proofs and experience reading mathematics at the graduate level at least. The mathematical knowledge needed and some conventions that we will use are explained below.

Algebraic geometry We will not assume any knowledge in algebraic geometry beyond the basic notions such as zero sets and polynomials. A knowledge in real and semialgebraic geometry will be useful to understand the motivation of certain questions from the

¹If the reader has arrived to this point, it means that probably E satisfies this requirement or that E likes to stare at sequences of characters that are incomprehensible for Em.

algebraic geometric perspective, but any necessary prerequisites will be introduced, particularly the notions of semialgebraic set and condition number of real projective algebraic sets.

Algebraic topology We will assume that the reader is familiar with the basics of algebraic topology: homotopies, continuous retractions, homotopy equivalences, singular homology and the Mayer-Vietoris theorem in homology. We will not require any knowledge on homotopy groups, beyond their definition and the fact that they are preserved under homotopy equivalences. The reader can find any unknown notion in the standard references [216] and [346].

Complexity theory We will assume some familiarity with complexity theory, in the sense that we assume that the reader is familiar with how the time complexity of an algorithm is estimated in general. The only point of the thesis were a serious knowledge of complexity theory is needed is in the subsection 0\$2–3 where we give the computer scientific motivation of the problem that this thesis discusses.

Differential and Riemannian geometry We will assume that the reader is comfortable and familiar with the standard concepts of differential and Riemannian geometry that are covered in a usual graduate course in mathematics. The reader can find any unknown notion in the standard references [275] and [381].

We will be working mainly on the sphere \mathbb{S}^n and \mathbb{R}^{n+1} . To be clear, for any smooth map $f : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^q$, including polynomials, we will denote by $D_x f$ the tangent map $T_x \mathbb{S}^n \rightarrow \mathbb{R}^q$ of f , as map on the sphere \mathbb{S}^n , at $x \in \mathbb{S}^n$ and by $\bar{D}_x f$ the tangent map $T_x \mathbb{R}^{n+1} = \mathbb{R}^{n+1} \rightarrow \mathbb{R}^q$ of f , as a map on \mathbb{R}^{n+1} , at $x \in \mathbb{R}^{n+1}$. When $f : M \rightarrow N$ is a smooth map between smooth manifolds M and N such that either M or N is not an Euclidean space, we will denote by $D_x f$ the tangent map $T_x M \rightarrow T_{f(x)} N$ of f at $x \in M$.

Linear algebra We will assume that the reader is familiar with the Singular Value Decomposition (SVD), singular values and orthogonal and unitary transformations. The reader can find any unknown notion in [392].

Probability theory We assume that the reader is familiar with the basic notions of probability theory. By this, we mean that the reader must know the definition and interpretation of probability, random variables and vectors and expectations in the continuous setting. The reader can find any unknown notion in [164; Ch. 1].

Notations

$[m]$	$:= \{1, \dots, m\}$	
$\# A$	cardinal/size of A	
$[m]^{\leq l}$	$:= \{A \subseteq [m] \mid \# A \leq l\}$	
sgn	sign map	p. 68
$\mathcal{A} _B$	$:= \{A \cap B \mid A \in \mathcal{A}\}$, for \mathcal{A} collection of sets	
\preccurlyeq	boundary order on $\{-1, 0, +1\}^q$	(2.10)

Parameters

q	number of polynomials	
\mathbf{d}	$:= (d_1, \dots, d_q)$	
D	$:= \max_{i \in [q]} d_i$	
N_i	$:= \binom{n+d_i}{d_i}$	
N	$:= \sum_{i=1}^q \binom{n+d_i}{d_i} = \sum_{i=1}^q N_i$	
$\Delta_{\mathbf{d}}$	$:= \text{diag}(\sqrt{\mathbf{d}})$	(1.8)

Polynomials

$\mathcal{P}_{\mathbf{d}}[q]$		(0.3)
$\mathcal{H}_{\mathbf{d}}[q]$	\mathbf{d} -homogeneous polynomial q -tuples in X_0, \dots, X_n	(1.1)
$\ \cdot\ _w$	Weyl norm	(1.2)
$\langle \cdot, \cdot \rangle_w$	Weyl inner product	(1.3)
$\text{ev}_x^i, \text{dev}_{x,v}^i$		(1.4)
$R_x(\mathcal{H}_{\mathbf{d}}[q]), L_x(\mathcal{H}_{\mathbf{d}}[q]), C_x(\mathcal{H}_{\mathbf{d}}[q])$		Corollary 1\$^{\text{§1}}\$ 3
$\mathfrak{R}_x, \mathfrak{R}_x^0, \mathfrak{R}_x^1$		Proposition 1\$^{\text{§1}}\$ 6
$f^u := f(uX)$		(1.5)
$f_{\mathbb{S}}$		(1.18)
ρ^h	homogenization map	(1.28)
$H(p)$		(1.30)
$\mathcal{H}_{\mathbf{d}}^\infty[q]$		p. 54
ρ_h		(1.33)
\widehat{f}		(5.13)
$\widehat{\nabla f}$		(5.13)

Boolean formulas

Φ, Ψ, \dots	Boolean formulas (generally)	
ϕ, ψ, \dots	purely conjunctive formulas (generally)	
$\Phi_X(S_1, \dots, S_a)$	value in X of Φ at $(S_1, \dots, S_a) \subseteq X^a$	p. 4
Φ^h		p. 53
$H(\Phi)$		(1.31)
$NF(\phi)$	normal form	Proposition 2 ^{S1} 2.1
$DNF(\Phi)$	disjunctive normal form	Proposition 2 ^{S1} 2.2
$sgn(\phi)$	sign vector of ϕ	p. 71
$sDNF(\Phi)$	strict disjunctive normal form	Lemma 2 ^{S2} 3
$\Phi^{\Gamma B_{\delta, \varepsilon}}$		(4.11)
$\Phi^{\Gamma B_{\delta, \varepsilon}}$		(4.12)

Zero and semialgebraic sets

$Z^S(f)$	zero set of f in the sphere S^n	
$W(p, \Phi)$	semialgebraic set described by (p, Φ)	(0.2)
$S(f, \Phi)$	spherical semialgebraic set described by (f, Φ)	(1.22)
$Z_r^S(f)$	algebraic neighborhood of $Z^S(f)$	(2.4)
$S(f, t, \Phi)$	spherical semialgebraic set described by (f, t, Φ)	(2.5)
$S_r(f, t, \Phi)$	algebraic neighborhood of $S(f, t, \Phi)$	(2.6)
$\Gamma B_{\delta, \varepsilon}(f, \Phi)$	Gabrielov-Vorobjov (δ, ε) -block	Definition 2 ^{S4} 1
$\Gamma B_{\delta, \varepsilon}(f, \Phi)$	Gabrielov-Vorobjov (δ, ε) -approximation	Definition 2 ^{S4} 1
$\mathcal{X}(f, t, \Phi, \mathcal{G})$	approximating cloud of \mathcal{G} -points for (f, t)	(4.1)
$\mathcal{X}_{i,j}^{\infty}(f, t, \mathcal{G})$		Definition 4 ^{S1} 2
$Z^C(f)$	complex zero set of f	
$Z(f)$	zero set of f	

Metric notions

dist	Euclidean distance	
$B(x, r)$	Euclidean ball with center x and radius r	
$\bar{B}(x, r)$	closed Euclidean ball with center x and radius r	
$\mathcal{U}(X, r)$	(Euclidean) r -neighborhood	(3.2)
dist _{S}	geodesic distance on S^n	(1.9)
$B_S(x, r)$	ball with center x and radius r with respect to dist _{S}	
$\bar{B}_S(x, r)$	closed ball with center x and radius r with respect to dist _{S}	
$\mathcal{U}_S(X, r)$	spherical r -neighborhood	(2.3)
dist _W	Distance with respect the Weyl norm	
$B_W(f, r)$	ball with center f and radius r with respect to dist _W	
dist _H	Hausdorff distance	(3.1)
dist _X	distance to X function	

Differential geometry

\mathbb{R}^{n+1}	$(n + 1)$ -dimensional Euclidean space	
\mathbb{S}^n	n -dimensional sphere	
\mathbb{S}_+^n	upper half n -dimensional sphere	
\mathbb{S}_0^n	$(n - 1)$ -dimensional sphere given by $\mathcal{Z}^{\mathbb{S}}(X_0)$	
$T_x \mathcal{M}$	tangent space of \mathcal{M} at x	
$N_x \mathcal{M}$	normal cone of \mathcal{M} at x (in its ambient space)	
$D_x f$	tangent map $T_x \mathcal{M} \rightarrow T_{f(x)} \mathcal{N}$	
	tangent map $T_x \mathbb{S}^n \rightarrow T_{f(x)} \mathcal{N}$, if f polynomial tuple	
$\bar{D}_x f$	tangent map $\mathbb{R}^m \rightarrow \mathbb{R}^{m'}$ at x	
\mathbb{O}		(1.29)
$\overline{\mathbb{O}}$		(4.20)
∇f	gradient vector of f	

Linear algebra

$\mathbf{1}$	vector of ones	
\mathbb{I}	identity matrix	
$\ \cdot\ _F$	Frobenius norm	(1.6)
$\langle \cdot, \cdot \rangle_F$	Frobenius inner product	(1.6)
$\ \cdot\ $	operator norm	(1.7)
$\sigma_i(A)$	i th singular value of A	
A^*	(conjugate) transpose of A	
A^\dagger	pseudoinverse of A	(1.12)
$\text{SNF}(A)$	Smith Normal Form of A	(3.23)
$O(n)$	orthogonal group of order n	
$U(n)$	unitary group of order n	
h_x		(4.23)

Condition numbers and relatives

$\kappa(f, x)$	local condition number of f at x	(1.10)
$\kappa(f)$	global condition number of f	(1.11)
$\mu(f, x)$		(1.15)
$\bar{\gamma}(f, x)$	Smale's gamma	(1.16)
$\gamma(f, x)$	Smale's projective gamma	(1.17)
$\bar{\kappa}(f, x)$	local intersection condition number of f at x	(1.23)
$\bar{\kappa}(f)$	global intersection condition number of f	(1.24)
$\bar{\kappa}_{\text{aff}}(p)$	global affine intersection condition number of p	
$\bar{\kappa}_{\text{aff}}^\infty(p, x)$		(1.36)
$\bar{\kappa}_{\text{aff}}^\infty(p)$		(1.36)
$\mathbb{W}(t)$	separation of t	(2.7)
$\kappa_{\text{aff}}(f, x)$	local affine condition number of f at x	Definition 5 ^{S2} 2

Discriminat sets

$\Sigma_{\mathbf{d}}[q]_x$	local discriminant set at x	(1.13)
$\Sigma_{\mathbf{d}}[q]$	global discriminant set	(1.14)
$\overline{\Sigma}_{\mathbf{d}}[q]_x$		(1.26)
$\overline{\Sigma}_{\mathbf{d}}[q]$		(1.26)
$\overline{\Sigma}_{\mathbf{d}}^{\perp}[q]_x$		(1.27)
$\overline{\Sigma}_{\mathbf{d}}^{\perp}[q]$		(1.27)
$\overline{\Sigma}_{\mathbf{d}}^{\text{aff}}[q]$		(1.34)
$\overline{\Sigma}_{\mathbf{d}}^{\text{aff}}[q]_+$		(1.35)
$\overline{\Sigma}_{\mathbf{d}}^{\text{aff}}[q]_0$		(1.35)

Reach, Čech, Vietoris-Rips and relatives

π_X	nearest point retraction of X	(3.3)
Δ_X	medial axis of X	(3.4)
∇_X		(3.5)
$\tau(X, x)$	local reach of X at x	(3.6)
$\tau(X)$	reach of X	(3.7)
$\tau(X, x; u)$	local reach along u of X at x	(3.8)
$\check{C}_\varepsilon(\mathcal{X})$	Čech complex of \mathcal{X} of radius ε	(3.24)
$\check{\pi}$		(3.25)
$\mathcal{VR}_\varepsilon(\mathcal{X})$	Vietoris-Rips complex of \mathcal{X} of radius ε	(3.26)
\mathfrak{d}_m		(3.27)
$\mathbb{G}_\varepsilon^{\mathcal{VR}}(\mathcal{X})$	Vietoris-Rips graph of \mathcal{X} of radius ε	(3.28)

Algebraic topology

H_\bullet	(singular) homology	
H_k	k th (singular) homology group	(0.1)
β_k	k th Betti number	(0.1)
T_k	k th vector of torsion coefficients	(0.1)
s_k	number of entries in T_k	(0.1)
π_k	k th homotopy group	
$N(C)$	nerve of C	(3.12)
Δ^X	free simplex with vertex set X	(3.13)
$[\mathcal{S}]$	realization of a simplicial complex \mathcal{S}	(3.14)
$\dim \sigma$	dimension of face σ	(3.15)
\mathcal{S}_k	set of k -faces of \mathcal{S}	(3.16)
$C_k^\Delta(\mathcal{S})$	set of simplicial k -chains of \mathcal{S}	(3.17)
∂_k^Δ	k th boundary operator	(3.18,3.19)
$B_k^\Delta(\mathcal{S})$	set of simplicial k -boundaries of \mathcal{S}	(3.20)
$Z_k^\Delta(\mathcal{S})$	set of simplicial k -cycles of \mathcal{S}	(3.21)
$H_k^\Delta(\mathcal{S})$	k th simplicial homology group of \mathcal{S}	(3.22)
β_k^p	k th mod p Betti number	(4.29)

Probability theory

\mathbb{P}	probability	
\mathbb{E}	expectation	
$\mathbb{E}_{x \in K}$	expectation over the uniform distribution on K	
$\mathfrak{x}, \mathfrak{y}$	random vector	
\mathfrak{A}	random matrix	
$\mathfrak{f}, \mathfrak{g}, \mathfrak{p}$	random polynomial tuples	
$N(x, \sigma)$	normal distribution centered at x with standard deviation σ	
$U(\mathbb{S}^{N-1})$	uniform distribution on the sphere \mathbb{S}^{N-1}	
χ_m^2	χ^2 -distribution with m degrees of freedom	
\mathcal{L}_x	concentration function of $x \in \mathbb{R}^k$	(5.3)
$F_{k,l}$	Fisher-Snedecor distribution with k and l degrees of freedom	

Differential tools

N_x^f	Newton vector field of f	(2.1)
$N_x^{f,t,\phi}$	discontinuous Newton vector field of (f, t, ϕ)	(2.8)
$\Pi_{f,\lambda}$	(f, λ) -lartition	Definition 2 ^{S2} 4
\mathcal{J}	strata of $\Pi_{f,\lambda}$ associated to \mathbf{J}	Definition 2 ^{S2} 4
$\Gamma_{f,\lambda}$	(f, λ) -partition	Definition 2 ^{S2} 5
$\Pi_{\mathbf{l},\sigma}$	strata of $\Pi_{f,\lambda}$ associated to (\mathbf{l}, σ)	Definition 2 ^{S2} 5

Special functions

Γ	Euler's Gamma function
----------	------------------------

Grids

$\mathcal{G}_{\bar{\gamma}}$	uniform grid of order $\bar{\gamma}$	(4.19)
$\mathfrak{D}_{\bar{\gamma}}(\bar{\alpha})$	random $\bar{\gamma}$ -grid with failure probability $\bar{\alpha}^{-1}$	p. 143
$\mathcal{R}_{\bar{\gamma}}$	recursive $\bar{\gamma}$ -grid with seeds \mathcal{R}_0 and \mathcal{N}	(4.24)

Subdivision methods

$\square[X]$	boxes $\prod [a_i, b_i]$ included in X	
$\square[F]$	interval approximation of F	(5.4)
$m(J)$	midpoint of $J \in \square[X]$	
$w(J)$	maximum width of $J \in \square[X]$	
$C_f(J)$		(5.5)
$C'_f(J)$		(5.14)

Error analysis

$F, F_{b,t}^{e_0, e_1}$	floating-point number system	(4.30)
$\mathbf{u}, \mathbf{u}_{b,t}$	round-off unit	Definition 4 ^{S3} 1
$\text{fl}, \text{fl}_{b,t}$	rounding map	(4.31)
$\widetilde{\text{op}}$	approximate version of op	(4.32)
fl^a		p. 163
$\mathfrak{z}(k)$		(4.33)
$1 + [\![\cdot]\!]$		p. 163

Other

$\kappa(\theta)$	(4.13)
$\varrho(\theta)$	(4.14)
$\Delta(\theta)$	(4.15)

Contents

Abstract / Zusammenfassung / Laburpena / Resumen	iii
Acknowledgments, agradecimientos eta beste esker onak	vii
Assumptions and conventions	xiii
Notations	xv
0 Introduction	1
0 ^{\$1} Description of the problem	2
0 ^{\$2} Motivation of the problem	6
0 ^{\$3} State-of-the-art and contributions to the problem	16
AI Analytical index	22
1 Condition numbers for the homology of semialgebraic sets	25
1 ^{\$1} Homogeneous polynomials and Weyl norm	26
1 ^{\$2} κ : a condition number for spherical algebraic sets	33
1 ^{\$3} $\bar{\kappa}$: a condition number for spherical semialgebraic sets	49
1 ^{\$4} $\bar{\kappa}_{\text{aff}}$: a condition number for affine semialgebraic sets	53
2 Differential semialgebraic geometry with condition-based inequalities	59
2 ^{\$1} A converse to the Exclusion Lemma	59
2 ^{\$2} Mather-Thom theory and some Whitney stratifications	66
2 ^{\$3} Durfee's theorem	81
2 ^{\$4} Gabrielov-Vorobjov approximation theorem	86
3 Computing the homology of a set par pointillage	99
3 ^{\$1} Approximation of sets by clouds of points	100
3 ^{\$2} Reach: Explicit lower bounds	110
3 ^{\$3} Homology of a cloud of points: the nerve theorem	116
4 Numerical algorithms for the homology of semialgebraic sets	131
4 ^{\$1} Simplicial approximation of semialgebraic sets	132
4 ^{\$2} Algorithms and their complexity	140
4 ^{\$3} Parallelization and numerical stability	154
5 A look into the future	171
5 ^{\$1} Beyond normal distributions: robust tail bounds	171
5 ^{\$2} 1st adaptive case: Plantinga-Vegter algorithm	179
5 ^{\$3} 2nd adaptive case: Han's covering algorithm	190
5 ^{\$4} А пятилетка for the future	198
F Real zeros of random fewnomials	205
F ^{\$1} A history of real fewnomial theory	206
F ^{\$2} Random real algebraic geometry	211

F^{S3}	Probabilistic Kushnirenko Hypothesis III	215
F^{S4}	A random real fewnomial theory?	222
M	¿Cómo computar la “forma” de un conjunto semialgebraico?	227
M^{S1}	Conjuntos semialgebraicos	227
M^{S2}	Grupos de homología	231
M^{S3}	Cálculo numérico	232
	Index	235
	List of algorithms	239
	List of figures	241
	Bibliography	243
	References for used quotes in chapter heads and rhetorics	275
	Used auxiliary resources for \LaTeX	277

Die Wahl eines Stils, einer Wirklichkeit, einer Wahrheitsform, Realitäts- und Rationalitätskriterien eingeschlossen, ist die Wahl von Menschwerk. Sie ist ein sozialer Akt, sie hängt ab von der historischen Situation, sie ist gelegentlich ein relativ bewußter Vorgang [...], sie ist viel öfter direktes Handeln aufgrund starker Intuitionen. »Objektiv« ist sie nur in dem durch die historische Situation vorgegebenen Sinn: auch Objektivität ist ein Stilmerkmal [...].

Paul Feyerabend, Wissenschaft als Kunst

0

Introduction

This dissertation presents the numerical approach to “one of the most fundamental open questions in algorithmic semi-algebraic geometry” [25; §5]: is there a $\text{poly}(q, D)^{\text{poly}(n)}$ -time algorithm for computing the homology groups (or Betti numbers) of a semialgebraic set in \mathbb{R}^n described by a Boolean formula involving q real polynomials of degree at most D ? Our presentation will be a synthesis of the currently existing results: the author’s PhD work in [91, 92, 136], with Peter Bürgisser, Felipe Cucker and Alperen Ali Ergür; and the immediately preceding work in [142, 88], by Peter Bürgisser, Felipe Cucker, Teresa Krick, Pierre Lairez and Michael Shub.

Additional PhD work in [93], with Peter Bürgisser and Alperen Ali Ergür, regarding the number of real zeros of a random fewnomial system can be found in the Appendix F, since it does not follow the main thought stream. Also, in Appendix M, an accessible account of the central theme is given in Spanish¹.

The present introduction will answer in the following three sections the next three fundamental questions:

1. What is precisely the problem we are trying to solve?
2. Why do we care about this problem?
3. What did others do towards the solution of this problem? And what have we done?

After answering these, the analytical index at the end intends to give an overview of the content and structure of the present thesis.

¹The reason for giving it in Spanish and not in English (or German) is that the target audience (relatives and friends back in Spain) is Spanish-speaking, but not always English-speaking.

0\\$1 Description of the problem

To describe the problem at hand, we review the terms appearing in the question above and only then, after the shades of meaning have been clarified, state the question with all its details.

0\\$1–1 Concepts and objects of the problem

The question above mentions three fundamental objects in it: algorithm, homology groups (and Betti numbers), and semialgebraic sets. These concepts are clear to any expert in computational semialgebraic geometry, but they may be unclear to a random mathematician. E might be unfamiliar with some of these notions (as it usually happens with semialgebraic sets) or might give them a meaning that was not intended (as it can happen with such a polysemous concept as homology).²

Algorithm

The notion of algorithm can have many definitions. However, by the Church-Turing thesis [12; Ch. 1], all of the ones reflecting computation in the real world turn out to be equivalent. Moreover, strong Church-Turing thesis [12; Ch. 1] says that all of them have equivalent notions of run-time and computing space, in the sense that the asymptotic complexity classes of complexity (polynomial, singly exponential, etc.) are the same for all models of computation. The interested reader can consult the details about the formal models of computation and their equivalences in any of the standard references, e.g., [12, 308].

Taking advantage of living in the era of computers, our model of computation will be pseudo-code. In the usual setting, we would measure the run-time in terms of the number of bit-operations that the algorithm described by the program in pseudo-code executes. However, in computational semialgebraic geometry, it is more clarifying to consider an algebraic model of computation in which algebraic operations and comparisons between real numbers can be done at unit cost. Because of this, we will assume that the program executed by our pseudo-code can perform arithmetic operations and comparisons with real numbers exactly, we will allow as inputs any real number and we will measure the run-time by the number of arithmetic operations and comparisons. This could be formalized using BSS machines [68; Ch. 4], but this level of formality will not be required by us as we don't intend to prove complexity lower bounds.

The adoption of an algebraic model of computation means stepping out of a realistic model of computation. To be able to translate our algebraic pseudo-code into a real algorithm, we need to accompany our complexity analysis with a bound on the size of the approximations/representations of the real numbers that our programs work with. This is done in two ways:

1. We restrict the real numbers input-output to an *efficiently computable class of real numbers*. By which we mean a set of real numbers represented by bit-strings such that arithmetic operations and comparisons can be done in polynomial-time in terms of the bit-representations. The paradigmatic example of such a model are rational numbers

²The claims between parentheses in the paragraph are based on the author's experience.

with the usual ways we operate and compare them, but there are more sophisticated versions such as Thom's encoding of real algebraic numbers [131]. In this restricted framework, the algorithm becomes efficient (in the bit sense) if one can bound the size of the representations appearing during the execution of the algorithm.

2. We allow the algorithm to use efficiently computable approximations, by which we mean a set of real numbers represented by bit-strings such that approximations to arithmetic operations and comparisons can be done in polynomial-time in terms of the bit-representation. The paradigmatic examples of this approach are fixed-point and floating-point arithmetic. In this approximate framework, the algorithm becomes effective if one can bound the precision needed during the execution in order to guarantee correct approximation of the output.

In our numerical approach, we do the latter (see Chapter 4). Therefore we will be able to make effective the algorithms that we produce.

Homology groups and Betti numbers

By homology, we don't mean any fancy homological theory from algebraic geometry, but the *singular homology* (with integer coefficients) $H_\bullet(X) = (H_k(X))_{k \in \mathbb{N}}$ of a topological space X [216; 2.1]. We will refer to this sequence of singular homology groups of X simply as the *homology* of X . We note that for simplicial complexes and CW complexes, singular homology agrees, respectively, with (the more computational) simplicial and cellular homology [216; Theorems 2.27 and 2.35].

In the cases we will be dealing with, the homology groups will be finitely generated groups. Therefore, by the classification theorem of finitely generated Abelian groups [273; Ch. III. Theorem 7.7], we have that each homology group $H_k(X)$ is isomorphic to

$$\mathbb{Z}^{\beta_k(X)} \oplus \bigoplus_{i=1}^{s_k(X)} \frac{\mathbb{Z}}{\tau_{k,i}(X)\mathbb{Z}} \quad (0.1)$$

where $\beta_k(X)$ and $s_k(X)$ are natural numbers and the $\tau_{k,i}(X)$ are positive integers greater than one such that for all $i < s_k(X)$, $\tau_{k,i}(X)$ divides $\tau_{k,i+1}(X)$. The numbers $\beta_k(X)$, $s_k(X)$ and the $\tau_{k,i}(X)$ are uniquely determined by the homology group $H_k(X)$. We call $\beta_k(X)$ the *kth Betti number* of X , and the vector $\tau_k(X) := (\tau_{k,i}(X))_{i=1}^{s_k(X)}$ the *torsion coefficients* of X . We will encode the homology groups through these numbers.

The homology groups $H_k(X)$ are very robust topological invariants of X , which are not only invariant under homeomorphisms, but also under homotopy equivalences. Furthermore, these topological invariants are "easy" to compute for reasonable spaces, when compared to other topological invariants. However, this easiness of computation comes at a price. Homology groups are difficult to interpret in direct topological terms, as it is not clear which topological information they capture. This situation should be compared with that of homotopy groups which are difficult to compute (they are still unknown for spheres [416]), but which have a direct topological interpretation.

We just briefly recall the interpretation of the first two homology groups and consider an example. For all topological spaces X , $H_0(X)$ is always free and its rank $\beta_0(X)$ counts

the number of path-connected components of X [216; Proposition 2.7]. When X is path-connected, $H_1(X)$ is isomorphic to the Abelianization of the fundamental group of X , $\pi_1(X)$, which consists of all the loops based at some point of X up to homotopy equivalence [216; Theorem 2A.1].

A precise description of simplicial homology, how to compute it and examples will be discussed in Chapter 3. For more details, we refer the interested reader to any of the usual references, such as [216, 346].

Semialgebraic sets

In principle, we could be working over an arbitrary real closed field [70; Ch. 1]. However, for the sake of concreteness and numerical algorithms, we will limit ourselves to the real closed field *par excellence*: the real numbers \mathbb{R} from analysis.

A *semialgebraic set* is a subset of \mathbb{R}^n which can be obtained after performing a finite number of unions, intersections and complements of sets of the form

$$\{x \in \mathbb{R}^n \mid p(x) = 0\}, \{x \in \mathbb{R}^n \mid p(x) \neq 0\}, \\ \{x \in \mathbb{R}^n \mid p(x) > 0\} \text{ and } \{x \in \mathbb{R}^n \mid p(x) \geq 0\},$$

where $p \in \mathbb{R}[X_1, \dots, X_n]$ is a real polynomial. In other words, semialgebraic sets are the sets which can be described by real polynomials, inequalities and their Boolean combinations.

Example 0\\$1.1. The set of polynomials of the form $aX^2 + bX + c$ with a real zero is a semialgebraic set. We can write it as

$$\left(\{(a, b, c) \in \mathbb{R}^3 \mid a = 0\}^C \cap \{(a, b, c) \in \mathbb{R}^3 \mid b^2 - 4ac \geq 0\} \right) \\ \cup \left(\{(a, b, c) \in \mathbb{R}^3 \mid a = 0\} \cap \{(a, b, c) \in \mathbb{R}^3 \mid b = 0\}^C \right) \\ \cup \left(\{(a, b, c) \in \mathbb{R}^3 \mid a = 0\} \cap \{(a, b, c) \in \mathbb{R}^3 \mid b = 0\} \cap \{(a, b, c) \in \mathbb{R}^3 \mid c = 0\} \right). \quad \Delta$$

As we cannot feed semialgebraic sets directly to an algorithm, we need to choose a representation that can be used as an input. We do this by describing semialgebraic sets with Boolean formulas.

A *Boolean formula* supported on $\{\alpha_1, \dots, \alpha_a\}$ is a string Φ constructed recursively by the following rules:

$$\begin{array}{ll} \alpha_k \text{ is a Boolean formula} & (\text{A}) \\ \Phi, \Psi \text{ Boolean formulas} \Rightarrow (\Phi \wedge \Psi) \text{ Boolean formula} & (\wedge) \\ \Phi, \Psi \text{ Boolean formulas} \Rightarrow (\Phi \vee \Psi) \text{ Boolean formula} & (\vee) \\ \Phi \text{ Boolean formula} \Rightarrow (\neg \Phi) \text{ Boolean formula} & (\neg) \end{array}$$

The *atoms* of Φ are the α_i appearing in it and the *size* of Φ , $\text{size}(\Phi)$, is the number (counted with repetition) of atoms and operations (\wedge , \vee and \neg) appearing in Φ . Given sets $S_1, \dots, S_a \subseteq X$, $\Phi_X(S_1, \dots, S_a)$ is the set obtained by interpreting α_i as S_i , \wedge as the set-theoretic intersection \cap , \vee as the set-theoretic union \cup and \neg as the set-theoretic complement C in the ambient set X . When the ambient set X is clear, we omit it.

Remark 0^{§1}1. Taking advantage of the fact that in the operations considered are associative, we will omit parentheses as long as there is no ambiguity. For example, instead of writing

$$(((\neg a_1) \wedge a_2) \vee (a_1 \wedge (\neg a_3))) \vee ((a_1 \wedge a_3) \wedge a_4),$$

we will write

$$(\neg a_1 \wedge a_2) \vee (a_1 \wedge \neg a_3) \vee (a_1 \wedge a_3 \wedge a_4).$$

Also, since the binary operations are commutative, we can further write $\wedge_{i \in I} \phi_i$ to simplify expressions of the form $\phi_{i_1} \wedge \phi_{i_2} \wedge \dots$ and similarly with $\vee_{i \in I} \phi_i$. ¶

Given a q -tuple of real polynomials $p \in \mathbb{R}[X_1, \dots, X_n]^q$, a *Boolean formula* over p is a Boolean formula Φ supported on

$$\{(p_i = 0), (p_i \neq 0), (p_i > 0), (p_i \geq 0), (p_i < 0), (p_i \leq 0) \mid i \in [q]\}.$$

Given $p \in \mathbb{R}[X_1, \dots, X_n]^q$ and a Boolean formula Φ over p , the *realization* of (p, Φ) is the semialgebraic set

$$W(p, \Phi) := \Phi_{\mathbb{R}^n} (p_i^{-1}(0), p_i^{-1}(\mathbb{R} \setminus 0), p_i^{-1}(\mathbb{R}_>), p_i^{-1}(\mathbb{R}_{\geq}), p_i^{-1}(\mathbb{R}_<), p_i^{-1}(\mathbb{R}_{\leq}) \mid i \in [q]). \quad (0.2)$$

A *Boolean description* of a semialgebraic set is a pair (p, Φ) where $p \in \mathbb{R}[X_1, \dots, X_n]^q$ and Φ is a Boolean formula over p such that $W(p, \Phi) = S$.

Example 0^{§1}2. In Example 0^{§1}1, the Boolean description suggested is

$$(\neg(a = 0) \wedge (b^2 - 4ac = 0)) \vee ((a = 0) \wedge \neg(b = 0)) \vee ((a = 0) \wedge (b = 0) \wedge (c = 0)). \quad \Delta$$

Example 0^{§1}3. Let $p \in \mathbb{R}[X_1, \dots, X_n]^q$. One can check that

$$\bigvee_{\sim \in \{>, <\}^q} \bigwedge_{i=1}^q (p_i \sim_i 0) \text{ and } \bigwedge_{i=1}^q ((p_i > 0) \vee (p_i < 0))$$

give descriptions for the same set. However, the first formula has size $2^q q - 1$, while the second one has size $4q - 1$. This shows that not all descriptions of a semialgebraic set are equivalent from a computational complexity viewpoint, and that we should be careful with the assumptions and manipulations of Boolean formulas. △

Remark 0^{§1}2. Boolean formulas can be viewed as formulas or expressions [82; 21.5] in the setting of a Boolean algebra. Alternatively, we could have defined a Boolean straight-line program by changing our description format to that of straight-line programs [82; 4.1] (also known as arithmetic circuits when represented as a graph) and everything, including the proofs and statements in this dissertation, would have carried out in the exact same way.

Although, in general, straight-line programs are more powerful than formulas, it is not clear that this is the case in the Boolean setting. This is so, because the main example of the difference, x^{2^n} , is so due to the ability of straight-line programs to do fast exponentiation. However, in the Boolean setting, where all binary operations are idempotent, exponentiation is a useless operation. ¶

0§1–2 Statement of the problem

With the above definitions and setting, we can now enunciate precisely the open problem that concerns this dissertation, which has two versions: one involving only the Betti numbers (**B**) and other involving also the torsion coefficients (**B**).

We will write computational problems indicating the input, the output, the complexity parameters, the desired run-time and the known run-time. The *desired run-time* indicates the run-time that the community of experts³ in computational semialgebraic geometry hopes for and the *known run-time* the best existing time-complexity bound.

Let $q, n \in \mathbb{N}$ be positive integers, $\mathbf{d} = (d_1, \dots, d_q) \in \mathbb{N}^q$ a q -tuple of positive integers, $D := \max\{d_1, \dots, d_q\}$ and

$$\mathcal{P}_{\mathbf{d}}[q] := \{f \in \mathbb{R}[X_1, \dots, X_n]^q \mid \text{for all } i \in [n], \deg f_i \leq d_i\}, \quad (0.3)$$

the set of q -tuples $f := (f_1, \dots, f_q)$ of real polynomials in the n variables X_1, \dots, X_n such that f_i has at most degree d_i .

(B): Betti numbers of a semialgebraic set.

Input	$p \in \mathcal{P}_{\mathbf{d}}[q]$, Boolean formula Φ over p of size $\leq s$
Output	Betti numbers of $W(p, \Phi)$: $\beta_0(W(p, \Phi)), \dots, \beta_n(W(p, \Phi))$
Complexity parameters	s, q, D, n
Desired run-time	$\text{poly}(s, q, D)^{\text{poly}(n)}$ [25]
Known run-time	$s(qD)^{2^{O(n)}}$ [128, 419] (cf. [34; Ch. 11])

(B): Homology of a semialgebraic set.

Input	$p \in \mathcal{P}_{\mathbf{d}}[q]$, Boolean formula Φ over p of size $\leq s$
Output	Betti numbers of $W(p, \Phi)$: $\beta_0(W(p, \Phi)), \dots, \beta_n(W(p, \Phi))$
Complexity parameters	$Torsion$ coefficients of $W(p, \Phi)$: $T_1(X), \dots, T_n(X)$
Desired run-time	s, q, D, n
Known run-time	$\text{poly}(s, q, D)^{\text{poly}(n)}$
	$s(qD)^{2^{O(n)}}$ [128, 419] (cf. [34; Ch. 11])

0§2 Motivation of the problem

There are many ways of motivating a problem. Some of these ways are more appealing to some people and some to others. Because of this, we don't present one motivation, but several of them. We will consider the following four motivations: the applied, because it may lead to better and faster algorithms in applications; the mathematical, because it will lead to a better understanding of the class of semialgebraic sets that plays an important role in many areas of mathematics; the computer scientific,⁴ because it plays a central role in complexity theory; and the historical,⁵ because the historical development of real and

³Or the author, if a citation is not given.

⁴Among the motivations, this is the most technical one and it requires some familiarity with complexity theory.

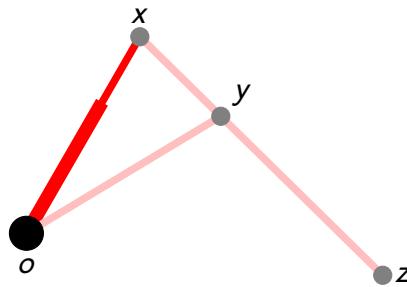
⁵Among the motivations, this is the most literary one and also the longest one. The latter is so because this historical motivations follows very nearly the development.

semialgebraic geometry leads “naturally” to this question. The reader is not supposed to read all the motivations, but only those that appeal to Eir interests.

0^{S2}-1 Applied

In many applications, one is interested in describing the set of possibilities (configuration space) by employing polynomial constraints, i.e., real polynomials and inequalities. This naturally leads to the appearance of semialgebraic sets in many problems. Without being exhaustive in our references, semialgebraic sets play a role in robot motion planning [101, 359, 274], configurations of molecules [274, 294], optimization [75, 66, 235, 267], non-negative rank [170, 266], etc.

Example 0^{S2}1 (A robot arm). Consider the following robot arm



where the black thick node o is fixed and the grey nodes x , y and z are only fixed to the position in the bars. The pink bars \overline{oy} and \overline{xz} are of fixed lengths 2 and 3, respectively, and the red bar \overline{ox} can change its length from 1.5 until 2.5 (in the picture is at length 2) and rotate freely between 0 and 90 degrees. The join y is precisely at distance 1 from x and 2 from z .

When the angle and the length of \overline{ox} vary, the robot arm gets several positions. The possible configurations of the arm can be encoded as a semialgebraic set. In this case, we get the following formula

$$\begin{aligned} (9 < 4(x_1^2 + x_2^2) < 25) \wedge (x_1 > 0) \wedge (x_2 > 0) \\ \wedge (y_1^2 + y_2^2 = 4) \wedge (3y_1 = 2x_1 + z_1) \wedge (3y_2 = 2x_2 + z_2) \\ \wedge ((x_1 - z_1)^2 + (x_2 - z_2)^2 = 9) \end{aligned}$$

where the first line indicate the possible lengths and angles of \overline{ox} , the second line the length of \overline{oy} and the position where y lies on \overline{xz} and the thirs line the length of \overline{xz} . Δ

In many of these applications, once the description as a semialgebraic set has been obtained, many of the problems reduce to either testing whether the semialgebraic set is empty (**G**) or connected, or counting (**D**) or sampling (**E**) connected components. Except for sampling the connected components, all problems reduce to the more general problem of computing the Betti numbers of a semialgebraic set (**B**).

(G): Emptiness of a semialgebraic set.

Input	$p \in \mathcal{P}_d[q]$, Boolean formula Φ over p of size $\leq s$
Output	1 if $W(p, \Phi)$ non-empty, 0 otherwise
Complexity parameters	s, q, D, n
Desired run-time	$sq^{n+1}D^{O(n)}$ [25]
Known run-time	$sq^{n+1}D^{O(n)}$ [26, 28] (cf. [34; Ch. 14])

(D): Number of connected components of a semialgebraic set.

Input Output Complexity parameters Desired run-time Known run-time	$p \in \mathcal{P}_d[q]$, Boolean formula Φ over p of size $\leq s$ Number of connected components of $W(p, \Phi)$: $\beta_0(W(p, \Phi))$ s, q, D, n $sq^{n+1}D^{n \cdot \text{polylog}(n)}$ [25] $sq^{n+1}D^{O(n^2)}$ [30] (cf. [34; Ch. 16])
---	--

(E): Connected components of a semialgebraic set.

Input Output Complexity parameters Desired run-time Known run-time	$p \in \mathcal{P}_d[q]$, Boolean formula Φ over p of size $\leq s$ $x_1, \dots, x_{\beta_0(W(p, \Phi))} \in W(p, \Phi)$ s.t. one and only one x_i per connected comp. of $W(p, \Phi)$ s, q, D, n $sq^{n+1}D^{n \cdot \text{polylog}(n)}$ [25] $sq^{n+1}D^{O(n^2)}$ [30] (cf. [34; Ch. 16])
---	--

As of today, direct applications of computing all Betti numbers of a semialgebraic set are unknown. However, even though direct applications may never appear, the techniques developed while solving the problems (B) and (B) might help to provide better algorithms to any of the problems above or to develop new algorithms for new problems to enter in the applied world.

0\\$2–2 Mathematical

Semialgebraic sets form a very robust class of sets that remains closed under many mathematical operations: unions, intersections, complements, projections... Because of this robustness, the shapes that semialgebraic sets take is vast and is yet to be understood. A solution to the problems (B) and (B) would be an advance in its understanding.

However, in current mathematics, the role of semialgebraic sets is not limited to that of a class of sets that remains to be understood. Semialgebraic sets have a distinguished position in many areas of mathematics: mathematical logic [386, 362], where semialgebraic sets appear in the first-order theory of the reals; real algebraic geometry [47, 70], where they appear in any classification problem; complexity theory [69, 68], where they are central to real complexity theory; discrete geometry [332], where they are key to understand the geometric configurations of a given combinatorial configuration; etc.

Example 0\\$2 (Realization space of a pyramid). Consider a square pyramid, with vertices of the base x_1, x_2, x_3, x_4 and apex y . The realization space should indicate us configurations of the points in which their convex hull gives the square pyramid combinatorially. In general, this means ensuring that (1) all points in a facet lie in the same hyperplane and no other point in that hyperplane, and (2) the points are in convex position. This leads to a semialgebraic set.

The first part of (1) is translated into equating determinants to zero and the second part of (1) together with (2) into imposing positivity condition onto determinants, where signs come from a global orientation. For example, since x_1, x_2, x_3, x_4 lie in the same facet, this

translates into

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix} = 0,$$

but since y does not lie in this facet this translates, after choosing an orientation of the facet,

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_2 & x_3 & x_4 & y \end{pmatrix} > 0.$$

Now, we only need to add further positivity conditions as the rest of the faces are triangles. After choosing an orientation, we get

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_i & x_{i+1} & x_{i+2} & y \end{pmatrix} > 0$$

where we interpret the subindices mod 4 and $i \in [4]$.

This would give a full description of the point configurations of $\{x_1, x_2, x_3, x_4, y\}$ that gives the pyramid with a square base. However, the realization space is the set of those configurations up to natural transformations, which are usually either projective transformations, affine transformations or isometries. In order to do this, we just fix as many parameters as we can using the considered action.

For example, in our case for the affine transformations, we can just assume that $x_2 = 0$, $x_3 = e_1$, $x_4 = e_2$ and $y = e_3$. Doing this, we can see that $x = \begin{pmatrix} a & b & 0 \end{pmatrix}^*$ and that the affine realization space of the pyramid is described by

$$(-a > 0) \wedge (b > 0) \wedge (1 - a - b > 0).$$

Although the realization space in this example is simple, they can be arbitrarily complicated and have any sequence of Betti numbers a simplicial complex can have [332]. Δ

In this way, solving (B) and (B) (both in theory and in practice) provides a computational approach to problems in which the homology of semialgebraic sets plays a fundamental role. An example of this, in a variant of (B) for curves, can be appreciated in [241] to re-study explicitly Gudkov's classical solution to Hilbert's sixteenth problem for curves of degree six [208, 209, 210, 207]. We will come back to this in Chapter 5.

0§2–3 Computer scientific

A *counting problem* refers to a computational problem involving a function that can be interpreted as the counting function for some object. The most famous class of counting problems is #P, but, in (computational) complexity theory, one is also interested in counting problems coming from other areas beyond combinatorics, such as algebraic geometry. This has been done extensively by Meer [287, 288], Bürgisser and Cucker [83, 84, 85], Bürgisser, Cucker and Lotz [89], Scheiblechner [354, 355] (cf. [356]), Bürgisser and Scheiblechner [95, 96], Basu and Zell [42, 43], and Basu [24].

There are many counting problems in semialgebraic geometry (among them, (Ж) and (3)), but we will focus on (Д) and (Б). The first one counts only components (i.e. “intrinsic topological holes” of dimension 0), while the latter counts the “intrinsic topological holes”

of all dimensions of a semialgebraic set. For more counting problems in real and complex algebraic geometry, see [83, 84, 89].

(XK): Size of a semialgebraic set.

Input	$p \in \mathcal{P}_d[q]$, Boolean formula Φ over p of size $\leq s$
Output	$\#W(p, \Phi) \in \mathbb{N} \cup \{\infty\}$
Complexity parameters	s, q, D, n
Desired run-time	$sq^{n+1}D^{n \cdot \text{polylog}(n)}$
Known run-time	$sq^{n+1}D^{O(n^2)}$ [30, 31] $[(\Delta) + \text{dimension}]$

(3): Euler-Poincaré characteristic of a semialgebraic set.

Input	$p \in \mathcal{P}_d[q]$, Boolean formula Φ over p of size $\leq s$
Output	Euler-Poincaré characteristic of $W(p, \Phi)$: $\chi(W(p, \Phi)) = \sum_i (-1)^i \beta_i(W(p, \Phi))$
Complexity parameters	s, q, D, n
Desired run-time	$sq^{n+1}(nD)^{O(n)}$
Known run-time	$s(qnD)^{O(n)}$ [22, 186] ⁶

From the classical point of view (see [12, 308] for basic references), in which we restrict the input of the problem to only integer polynomials, **(Δ)** is FPSPACE-complete (with respect to Cook-reductions⁷) [322, 323, 103] and **(B)** FPSPACE-hard [84], this remains true if we restrict to complex projective varieties [354]. However, this does not relate these problems to the usual counting problems beyond the well-known inclusion $\#P \subseteq \text{FPSPACE}$, and so this only tells us that counting is harder in semialgebraic geometry than in combinatorics.

From the real point of view, as defined in [69, 68], there is a real analogue of $\#P$, $\#P_{\mathbb{R}}$, which was introduced in [287, 288] and studied extensively in [84]. However, with this real analogue, we can only show that **(B)** is $\text{FP}^{\#P_{\mathbb{R}}}$ -hard (due to the proof of [84; Theorem 7.1]). In [42, 43], an alternative real analogue of $\#P$, $\#P_{\mathbb{R}}^{\dagger}$, was given. The main difference between $\#P_{\mathbb{R}}$ and $\#P_{\mathbb{R}}^{\dagger}$ is, roughly speaking, that the first one counts using the set-theoretic cardinal and the second one using the sequence of Betti numbers. The most interesting part of this real alternative analogue to $\#P$ is that it gives the following real version of Toda's theorem (cf. [389]):

$$\text{PH}_{\mathbb{R}}^c \subseteq P_{\mathbb{R}}^{\#P_{\mathbb{R}}^{\dagger}}$$

where $\text{PH}_{\mathbb{R}}^c$ is the compact version of $\text{PH}_{\mathbb{R}}$, meaning that we restrict the domain of each block of quantified variables and of the block of free variables to the corresponding sphere.

To illustrate the above result in a weaker, but more accessible way, we consider, for $I > 0$, the decision problem GDP_I^c whose instances are of the form

$$Q_1 x_1 \in \mathbb{S}^{n_1-1}, \dots, Q_I x_I \in \mathbb{S}^{n_I-1}, (x_1, \dots, x_I) \in W(p, \Phi)$$

⁶The result in [186] is needed to extend the algorithm in [22] from closed to arbitrary semialgebraic sets. However, it should be pointed that historically the substitution was done with the construction in [185] with the proof of homotopy invariance given by [33, 35]. Nevertheless, the construction in [186] is the most general, elegant and efficient one.

⁷By a *Cook-reduction* from P to \tilde{P} , we will mean that there is a polynomial-time algorithm solving P with oracle calls to \tilde{P} . When the restriction of polynomial-time is dropped, we will just say *Turing-reduction*.

where $n = \sum_{i=1}^l n_i$, $Q_i \in \{\forall, \exists\}$, $p \in \mathcal{P}_d[q]$ and Φ a lax formula over p , which is a Boolean formula without negations whose atoms are of the form $(f_i = 0)$, $(f_i \geq 0)$ and $(f_i \leq 0)$. This problem is the compact version of deciding quantified semialgebraic formulas with l alternations, GDP_l , where we quantify over \mathbb{R}^{n_i} instead of \mathbb{S}^{n_i-1} and we don't put restrictions on Φ . In [42, 43], they showed that for fixed $l > 0$, GDP_l^c can be Cook-reduced (in the BSS model of computation) to **(B)**. In other words, **(B)** is strong enough to decide (in an algebraic model of computation) a compact version of the first-order theory of the reals. We note that the opposite reduction is not possible (even if we just ask for a Turing-reduction), because neither **(B)** nor **(D)** can be expressed in the first-order theory of the reals [48, 22].

Putting together what we have said above, the problem **(B)** is a hard problem to which many hard problems in both the classical and real setting can be reduced. This problem is intimately related to the real complexity class $\#P_{\mathbb{R}}^\dagger$, and a positive solution to it would bring an inclusion into $\text{FEXPTIME}_{\mathbb{R}}$ of many known problems and complexity classes in the world of real complexity.

0^{S2}-4 Historical⁸

With the invention of Cartesian coordinates, geometric objects became formulas and formulas geometric objects. This event, which marked the beginning of algebraic geometry, allowed an “easy” algebraic understanding of many of the geometric objects of the past, such as conics. However, with this new understanding, hordes of new “monstrous” algebraic-geometric objects invaded the Greek classical world. Where once the harmony of Plato’s shapes ruled, algebraic varieties created chaos with all their possible (real!) shapes.⁹

This chaos took place even in the world of those algebraic varieties that we can draw and see. At the beginning of the 20th century, there was a very modest success in classifying the zoo of shapes of real algebraic curves and surfaces. The biggest successes were the understanding of curves of degree five (and partially those of degree six) by Harnack [215] and Hilbert [222] and of surfaces of degree three by Schläfli [358], Zeuthen [423] and Klein [259]. In this context, in 1901, Hilbert formulated his famous 23 problems [224, 223], and asked, in the first half of the sixteenth one, how real algebraic smooth curves in \mathbb{P}^2 and real algebraic smooth surfaces in \mathbb{P}^3 can look like (up to isotopy). The problem put special emphasis on curves of degree six and surfaces of degree four.

Despite the early work in the problem by Ragsdale [320] and Rohn [337], the main collective effort went into other Hilbert’s problems. The solution to the seventeenth problem led to the abstract theory of real fields by Artin and Schreier [13]. However, the main focus went on the real version of Hilbert’s tenth problem, which is just nothing more than **(Γ)**, motivated by the threat of undecidability created by the works of Gödel [192], Church [127, 126] and Turing [394]. Fortunately, Tarsky [386],¹⁰ and later also Seidenberg [362], showed

⁸A warning is in order here. The history here will be told from a subjective perspective, starting in the 20th century with Hilbert’s problems (specially the first half of Hilbert’s sixteenth problem [224, 223]) and ignoring the development of non-real algebraic geometry. The arrow of time in this history will be the understanding of shapes (and topological invariants) of real algebraic and semialgebraic sets. For alternative narratives, see [157, 349, 32, 408].

⁹From time to time, the author will take these poetic licenses in this historical narrative to keep it entertaining.

¹⁰Although published in 1951, Tarski’s work goes back to the 30s. The delay was due to the war.

that the first-order theory of the reals was decidable. Unfortunately, the Second World War brought the progress in the problem to a halt.

The Soviets¹¹ against Hilbert's sixteenth problem

With the war over, the only mathematical community that took the challenge of the first half of Hilbert's sixteenth problem was the Soviet one. And the narrative here has to be complemented by the account of the Soviet protagonists themselves in [206], [148] and [408].

In the 50s, continuing with the work of Petrovskii before the war [311], Petrovskii and Olešnik developed bounds for the Euler characteristic of real smooth algebraic sets [312] and, later, Olešnik extended these results to sums of Betti numbers [303, 304]. This brought, for the first time, a restriction on the possible topologies of general real algebraic sets.

In the 60s, Gudkov, following a suggestion of Petrovskii, attacked Hilbert's sixteenth problem for curves of degree six. After more than ten years and a famous mistake,¹² Gudkov completed the classification of real projective algebraic curves of degree six [208, 209, 210]. Meanwhile in the West, Milnor [292] and Thom [387] rediscovered the results of Olešnik on the sum of Betti numbers [303, 304], although providing new proofs which applied also to the singular case.

In the 70s, the major breakthrough in the dissipation of the chaos in real algebraic geometry occurred, motivated by Gudkov's congruence hypothesis [209]. In 1971, Arnold [7] gave a proof of a weaker version of Gudkov's conjecture using techniques from complex algebraic geometry, in the flavour of Thom's proof of Olešnik's bound [387] and Klein's proof of Harnack's inequality [260]. In a sudden boiling of ideas, Rokhlin developed this relation between real and complex algebraic geometry enormously. One year after Arnold, he gave the first proof of Gudkov's congruence hypothesis [341];¹³ just four months afterwards, he gave another simpler proof of a generalization of Gudkov's congruence hypothesis [340, 342];¹⁴ and he completed this by exploring even further the relation between the topology of the real part, its complexification and the relative position [343, 344, 345].

With this explosion of ideas, the 70s and 80s were very successful for the Soviet school of mathematics. The congruences and inequalities were generalized further by Fiedler, Gudkov, Kharlamov, Krakhnov, Nikulin and many others [179, 211, 247, 248, 249, 250, 299]. These works on restrictions culminated with full classifications by Kharlamov, Nikulin and Viro for new degrees at the end of the 70s and the beginning of the 80s. In the zoo of curves, rigid¹⁵ classifications were produced by Kharlamov for curves of degree five [253] and by Nikulin for curves of degree six [298]; and the isotopic classification for curves of

¹¹The term Soviet, instead of Russian, is necessary as not all Soviet mathematicians are Russian. For example, Olga A. Olešnik was from Ukraine and Vladimir A. Rokhlin from Azerbaijan.

¹²This mistake refers to the fact that the original classification of Gudkov in 1954 did not contain the curve of type $1(5) \sqcup 5$, (one oval with five ovals inside and five outside). The later correction of this mistake was surprising, because this type of curve was believed not to exist by Hilbert [224]. The discovery of this mistake and its correction by Gudkov was possible thanks to Morozov [318].

¹³However, this proof had a mistake that it took eight years to be discovered and corrected by Marin [284].

¹⁴Funnily, of congruences mod 16 for Hilbert's 16th problem

¹⁵Rigid isotopy as opposed to topological isotopies, require that the isotopy can be carried out by deforming the coefficient of the defining polynomials and not just the zero set.

degree seven was obtained by Viro [411, 406, 405]. Further, the isotopic classification of curves of degree eight was almost¹⁶ completed by Viro [411, 406], Shustin [371, 372, 373] and Polotovskii [317]. In the zoo of surfaces, Viro gave constructions of M-surfaces in every degree [401]. The partial results on (smooth) surfaces of degree four by Utkin [396, 395, 397, 207] were completed. The isotopic classification of surfaces of degree four was completed by both Kharlamov [246, 251, 252] and Nikulin [298] and the rigid classification by Kharlamov [254].

The emergence of computational semialgebraic geometry

While the Soviet mathematical school was climbing the Everest that the first half of Hilbert's sixteenth problem still is, the Western schools of mathematics started to leave the more pure approaches to semialgebraic geometry, as exemplified by [70], to turn their attention into the existence of efficient algorithms in semialgebraic geometry. This was motivated by the realization that, although in principle every problem expressible in the first-order theory of the reals was solvable by [386, 362], the algorithms by Tarski and Seidenberg would probably solve the problem only after the universe was over, even for small size problems.

At the end of the 70s, these efforts condensed in the so-called Cylindrical Algebraic Decomposition (CAD) developed independently by Collins [128] and Wüthrich [419] which gave a complexity of $O(qD)^{2^{O(n)}}$ to the decision of the first-order theory of the reals. There were some hopes at the time that the lower bounds of Fischer and Rabin [181] could be improved to show the optimality of CAD.¹⁷ Around ten years later, Arnon, Collins and McCallum [9, 8] added some improvements to CAD; Ben-Or, Kozen and Reif [46] showed that the computation could be performed in exponential space; and the lower bounds obtained by Weispfenning [417] and Davenport and Heintz [145] made all the preceding work appear optimal.

However, the Soviet school of mathematics still had one more surprise in store. On the same year that the lower bounds by Weispfenning [417] and Davenport and Heintz [145] appeared, Grigor'ev and Vorobjov [203] (cf. [414, 413]) and Grigor'ev [202] (cf. [200]) developed the *critical points method*, building on previous work in the same decade by Chistov [125], Chistov and Grigor'ev [121, 122, 123, 205, 124] and Grigor'ev [198, 199] on the first-order theory of the complex numbers. In contrast to CAD, the run-time of the critical points method is $O(qD)^{n'}$ where n' is the number of quantifier alternations in the first-order formula. This parameter was very present in the examples of [417, 145].

In the coming decades, both CAD and the critical points method were successively improved. CAD was improved by Hong [225, 226], Collins and Hong [129] and many others [108]. At the beginning of the 21st century, Brown [78] improved CAD for the plane, and new examples were obtained by Brown and Davenport [79] which showed the importance of the order chosen in CAD. The critical points method was improved by Canny [103, 105], by Heintz, Roy and Solernó [219], by Renegar [326, 327, 328] (cf. [325]), where n' is substituted by $\prod_i (n_i + 1)$; and finally by Basu, Pollack and Roy [26, 28], where q and d are separated and the exponent of q is given exactly without Landau notation. However, despite

¹⁶Only the existence of six isotopy types remain to be resolved.

¹⁷"The result of Fischer and Rabin suggests that a bound of this form is likely the best achievable for any deterministic method". [128]

these incredible achievements, the main focus of computational real algebraic and semialgebraic geometry started to shift to the computation of topological invariants at the end of the 80s.

“Turing” goes topological

At the end of the 80s, it was clear that the classical classification project of Hilbert was difficult. After more than three decades of work, this project was completed for the cases originally considered by Hilbert. However, the progress in terms of the degree was small: the classification was only done for curves of degree at most seven and for surfaces of degree at most four. It is not clear if this was the motivation, but around this time, after the successes of CAD and the critical points method, a substantial amount of algorithms addressing the computation of topological invariants emerged, especially concerning connected components (Δ) and the isotopy types of curves.¹⁸

On (Δ), the progress started soon after the development of the critical points method. The problem received an impetus from the applications thanks to the work of Canny [101] showing the relation of the problem to robot motion planning. Soon after this, Canny [103, 102] developed the notion of a roadmap of a semialgebraic set that will play a fundamental role. At the beginning of the 90s, a cluster of results showed that (Δ) could be solved in singly exponential time. Initially, Canny [107, 104] and Heintz, Krick, Roy and Solernó [218]¹⁹ showed that, among other geometric-topological problems, deciding if two points belonged to the same connected component could be done in singly exponential time. Then, almost at the same time, Grigoriev and Vorobjov [412, 204], Canny, Grigoriev and Vorobjov [106] and Heintz, Roy and Solernó [218, 220] (see also [201]) showed that (Δ) could also be done in singly exponential time. By the end of the 90s and beginning of the 2000s, the complexity was improved to the more explicit $O(qD)^{O(n^2)}$ by Basu, Roy and Pollack [27, 29, 30]. The last significant progress in this problem was by Safey el Din and Schost [352, 353] and Basu, Roy, Safey El Din and Schost [40] and Basu and Roy [39] at the beginning of the 2010s. They showed that for algebraic sets, the exponent $O(n^2)$ can be substituted by a quasilinear factor in n , $n \cdot \text{polylog}(n)$. As of today, extending this complexity bound to general semialgebraic sets is seen as the biggest open problem in computational semialgebraic geometry concerning (Δ).

On the isotopy type of real curves, there were some algorithms by Polotovkii [316] at the end of the 70s and Gianni and Traverso [188] at the beginning of the 80s. However, the first algorithm for smooth curves with a complexity estimate was given by Arnon and McCallum [10, 11] relying on their previous work with Collins on CAD [9, 8]. For any kind of curves, it was the algorithm by Roy and Szpirglas [348, 350]. The coming two decades saw an improvement race of the algorithms and their complexity estimates by long sequence of works: Cucker, González-Vega and Rosello [138], Feng [178], González-Vega and El Kahoui [195], González-Vega and Necula [196], Eigenwillig, Kerber and Worner [171], Kerber [243], Diochnos, Emiris and Tsigaridas [158], Cheng, Lazard, Peñaranda, Pouget, Rouillier and Tsigaridas [112], Kerber and Sagraloff [244], Diatta, Rouillier and Roy [154], Mehl-

¹⁸It should be clear that such algorithms contribute to the goal of solving the first half of Hilbert’s sixteenth problem in general and to the computational understanding of the topology of real algebraic varieties.

¹⁹Unfortunately, the pelotita and the bolón didn’t get chosen as standard terminology in [34].

horn, Sagraloff and Wang [289, 290], Kobel and Sagraloff [261], and Diatta, Diatta, Rouillier, Roy and Sagraloff [152]. All this sequence improved the complexity roughly from $O(d^{23})$ to $O(d^6)$.

(B) as the next step in this history

As we have seen above, with the coming of the new century, there were substantial improvements in algorithms solving (Δ) and determining the isotopy type of curves. Regarding Hilbert's sixteenth problem, after the Soviet solution of the cases mentioned explicitly in the problem, the progress has been more modest. However, the chaos of shapes of semialgebraic geometry is far from becoming an understandable cosmos.

From the geometric perspective, the classification of curves of degree 8 is still open, despite recent work by Chevallier [120] and Orevkov [306]; new congruences, by Mikhalkin [291] and Viro and Orevkov [291, 409]; new asymptotics, by Orevkov and Kharlamov [307]; new examples, by Itenberg and Viro [411, 229, 230, 232] and Brugalle [80]. And, in the case of surfaces, the situation is more dramatic, the Betti numbers are not even completely understood: it is still not known whether there is a surface of degree five with 24 or 25 connected components. The best example is until now by Bihan [55] and Orevkov [305] with 23 connected components, which improved on the one before by Kharlamov and Itenberg with 22 components. Further, new limits on the existing construction techniques by Renaudineau and Shaw [324] suggest that new ideas are needed.

From the computational perspective, the situation is more hopeful. On the one hand, there were developments on both the algorithms for isotopy of curves, which we have already discussed, and also some generalizations to surfaces and curves in 3-dimensional space of these algorithms. On the other hand, the exploration on how to compute new Betti numbers started.

At the beginning of the 2000s, algorithms were developed for the computation of topological invariants and piecewise linear approximations²⁰ of surfaces in space. The first algorithms were developed by Fortuna, Gianni, Parenti and Traverso [184], Fortuna, Gianni and Luminati [182], Cheng, Gao and Li [113], Fortuna, Gianni, Luminati and Parenti [183], and, at the end of the 2000s, the first one with a complexity analysis by Alberti, Mourrain and Técourt [3], which was based on previous work by Mourrain and Técourt [293]. The situation for algorithms computing piecewise linear approximation of curves is similar.²¹

In parallel to these developments, one should not ignore the developments coming from other methods in computational geometry (cf. [71]). At the beginning of the 90s, Snyder [376, 377] made substantial work in the isotopic piecewise-linear approximation of curves. In the 2000s, the problem for curves and surfaces was dealt by Boissonnat, Cohen-Steiner and Vegter [72, 73], Plantinga and Vegter [315], Stander and Hart [382], Boissonnat and Oudot [74], and Cheng, Dey, Ramos and Ray [115]. Although the focus of many of these approaches was more on the correctness and applicability to general functions, not only polynomials, many of these methods were fundamental in motivating developments in

²⁰This was necessary, because it is not clear, like it happens in the case of curves, which combinatorial structure captures the topology of the isotopy type of a surface. A torus can be knotted with itself.

²¹See the works by Alcázar and Sendra, Gatellier, Labrouzy, Mourrain and Técourt [187], El Kahoui [173], Diatta, Mourrain and Ruatta [155], and Cheng, Jin and Lazar [114].

computational semialgebraic geometry.

At the end of the 90s, Basu [21, 22] developed the first algorithm computing more topological information (precisely (3)) than just the 0th Betti number in singly exponential time. By the middle of the 2000s, this was later extended to the first two Betti numbers by Basu, Pollack and Roy [33, 35] and then to the first ℓ Betti numbers by Basu [23]. However, in the last work, the complexity is doubly exponential in ℓ . In this period, one should definitely mention that the constructions by Gabrielov and Vorobjov [185, 186] were essential for extending algorithms from closed semialgebraic sets to general semialgebraic sets.

In the last years, Basu and Riener [36, 37, 38] have applied successfully many of the symbolic techniques to the case of symmetric semialgebraic sets described by symmetric polynomials.

At this moment of historical development, (B) is not just important because it is the last step in a sequence of improvements, but because, as of today, (B) resists to all technical improvements coming from CAD and the critical points method. A solution to this problem, in singly exponential time, would require new ideas in computational semialgebraic geometry. These new ideas will give surely a better understanding of the topology of semialgebraic sets and so contribute to the goal of the first half of Hilbert's sixteenth problem.

0§3 State-of-the-art and contributions to the problem

We will recall the state-of-the-art concerning (B) and (B) and then explain our contributions to the problems, which we present in this thesis.

0§3–1 State-of-the-art regarding the problem

In the state-of-the-art regarding (B) and (B), we should distinguish between the symbolic and numerical approaches. We will recall the existing symbolic methods for approaching (B) and their limits, and then explain the existing numerical method, the grid method, the differences that it has with respect symbolic methods and what has been the progress so far regarding (B) and (B).

Symbolic approaches

On the symbolic side, the best existing algorithm for (B) is the algorithm by Basu [23]. It computes the first ℓ Betti numbers of a semialgebraic sets in $(qD)^{n^{O(\ell)}}$ -time. This algorithm is a product of a long sequence of steps, which can be read in the historical motivation, but whose immediate ancestors are the algorithms by Basu [21, 22] and Basu, Pollack and Roy [33, 35] and the constructions by Gabrielov and Vorobjov [185, 186]. We explain the ideas present in these works.

Remark 0§3.1. In the case of complex smooth varieties, Scheiblechner [357] showed that one can solve (B) in singly exponential time and parallel polynomial time. The reason that the techniques of [357] don't apply to the corresponding version of (B) is because they are based on de Rham cohomology which misses the torsion coefficients. However, it would be interesting to study whether the techniques in [357] could be generalized to the real setting, as they differ from the usual ones in computational semialgebraic geometry. ¶

The first paper [21, 22], by Basu, dealt with bounding the homology groups of semi-algebraic sets. This was done by a certain covering and a Mayer-Vietoris argument that allowed to bound the Betti numbers of the union in terms of the Betti numbers of the intersections. Additionally, the techniques developed for the bound are used to compute the Euler-Poincaré characteristic of semialgebraic sets (3) in singly exponential time. The main idea for this was to make use of the additivity of the Euler-Yao characteristic and the fact that the Euler-Poincaré characteristic agrees with the Euler-Yao characteristic for closed subsets. In this way, one could compute the Euler-Poincaré characteristic of $S = \bigcup_{\sigma} S_{\sigma}$, with S_{σ} not necessarily closed, using (under the right hypotheses) the identity

$$\chi(S) = \sum_{\sigma} \chi^*(S_{\sigma})$$

where χ is the Euler-Poincaré characteristic and χ^* is the Euler-Yao characteristic. In order to compute it for each S_{σ} , ideas coming from the critical points method and auxiliary constructions are used.

The second paper [33, 35], by Basu, Pollack and Roy, applied a similar strategy, to that of [21, 22], to compute the 0th and 1st Betti numbers. The main result is the construction, in singly exponential time, of a cover by contractible semialgebraic sets. Then, in a variation of the Nerve's theorem, they show that for a closed set $S = \bigcup_{\alpha} S_{\alpha}$ with the S_{α} closed and contractible, one can compute $\beta_0(S)$ by counting the connected components of the pairwise intersections of the S_{α} , and $\beta_1(S)$ by counting the connected components of the pairwise and triplewise intersections of the S_{α} . This is proven using the so-called Mayer-Vietoris double complex and its associated spectral sequence. Again, the computation of the connected components (4) of the possible intersections is done using the existing algorithms for this problem (such as [30]).

Additionally, in this paper, they gave the first proof that a general semialgebraic set can be substituted by a closed semialgebraic with the same topological invariants. They did this showing that the construction of Gabrielov and Vorobjov [185] also preserved the homotopy type. This idea is fundamental, as almost all of the techniques with the name “Mayer-Vietoris” only work with closed subsets. Interestingly, the construction [185] was developed to bound the sum of the Betti numbers of general semialgebraic sets, which was an open problem at the time.

The third paper [23], by Basu, takes the algebraic-topological techniques in [33, 35] to the limit. The main idea is to consider recursively contractible covers of the intersections of elements of the previous covers. Then, using a suitable truncation of the Mayer–Vietoris double complex and its associated spectral sequences, one is able to recover the first few Betti numbers of the desired set. The doubly exponential explosion in the number of computed Betti numbers is just a consequence of how the inductive construction of contractible covers works.

One can see that in these works the main constructions are algebraic topological. The main part of these algebraic topological arguments deal with how to get the Betti numbers out of the constructed contractible cover (in [35]) when the pairwise intersections are not contractible. With the exception of the contractible cover in [35], the main part of the approaches try solving (5) by reducing, through algebraic topological computations, the prob-

lem to cases that one can deal with by using the usual algorithms in semialgebraic geometry, which mainly are algorithm dealing with **(Д)** and **(Е)**.

Numerical approaches

At the end of the 90s, a new approach of computation was introduced in real algebraic geometry: the numerical one, to which the methods of this thesis belong. We introduce below briefly what make the numerical algorithms numerical instead of symbolic. We also give a short historical development as this was not included in the historical motivation²² and we finish discussing the ideas of the grid method, which is the form that until now the numerical approach has taken within real algebraic and semialgebraic geometry.

Numerical algorithms, condition numbers and condition-based complexity In contrast to the symbolic approaches, the numerical approaches deal with inputs which are assumed to be inexact and with which the performed operations perform inexactly. This makes numerical algorithms different from symbolic ones, since it is possible to have *ill*-posed inputs for which the numerical algorithm cannot give a correct answer (since for these inputs arbitrarily small perturbations dramatically change the answer to the problem). In addition to this, their complexity appears to depend not only on the size of the input, but also on a parameter called *condition number* which measures the sensitivity of the problem, not the algorithm, to variations in the input.

The *condition-based complexity* is a form of parameterized complexity in which the focus is to understand, in terms of the condition number of the data, the complexity of the numerical algorithm: number of operations used, precision needed... In this way, one can understand why the algorithm works fast on certain inputs and slow or not at all on other inputs.

However, one drawback is that we cannot know how the complexity depends, in general, on the size of the input, which is necessary to compare the algorithm with symbolic algorithms, for which this is usually the case. To solve this issue, the usual approach, going back to Goldstine and von Neumann [194], Demmel [150] and Smale [374], is to consider a “reasonable” probability distribution on the input-space and to study the probability distribution of the condition number. This will give a probabilistic complexity analysis that either holds on average (average and smoothed complexity) or with high probability (weak complexity) that is easier to compare with the worst-case complexity estimates of symbolic algorithms, as no condition number appears in the bounds.

We will come back to these ideas in more detail in chapters **1** and **4**.

Some historical remarks about the condition-based complexity paradigm The condition-based complexity paradigm is not new and goes back to the beginning of the theory of computation itself. In the middle of the 20th century, condition numbers were introduced for the resolution of linear systems, respectively, by Turing [393]²³ and von Neumann

²²We should note that the use of an approach to a problem does mean that such approach is part of the historical motivation of the problem. In other words, the historical motivation to approach numerically **(Д)** and **(Е)** is not numerical.

²³See the notes of the 1970’s Turing Lecture by Wilkinson [418] for a first-person account of this discovery.

and Goldstine [297].

In the 80s, Demmel [149, 150] developed the framework of conic condition numbers setting one of the most general frameworks of the condition-based complexity paradigm. However, it was not until the 90s when condition-based complexity reached its age of majority by leaving the realm of numerical linear algebra. On the one hand, Shub and Smale [366, 367, 368, 370, 369] introduced condition numbers into the study of homotopy continuation methods for solving complex systems of polynomials leading to the formulation of the so-called Smale's 17th problem [375]. The problem was solved successfully in the next two decades by Beltrán and Pardo [45], Bürgisser and Cucker [86] and Lairez [272]. On the other hand, Renegar [329, 330, 331] introduced condition numbers into linear programming.²⁴ This work was later further expanded by Cheung and Cucker [116, 117, 118].

Together with the grid method, which we present below, the condition-based complexity paradigm has become pervasive. Much of the current knowledge was condensed in the book [87] by Bürgisser and Cucker, where a complete exposition of the main ideas of the field and further historical comments can be found.

The grid method²⁵ In the realm of real algebraic geometry, condition numbers entered for the first time through the works of Cucker and Smale [143, 144] and Cucker [133]. They considered the problem of feasibility of a set of real polynomial equations. The basic idea of the algorithm was to iteratively refine a grid until either one could certify the existence of a zero, using Smale's α -theory, or that the polynomial was either positive or negative, using Lipschitz properties of the polynomial. Because of this, the numerical approach in real algebraic geometry is called *grid method*.²⁶

The introduction of the grid method was motivated by the observation that the then-existing symbolic methods were not likely stable due to the use of large matrices that had to be inverted.²⁷ The way in which the grid method avoids this is by substituting inverting large matrices by inverting a lot of small matrices, one at each point of the grid. Also, another advantage of the grid method is that it is parallelizable, as one can perform the operations at each point in the grid independently.

Ten years after, the grid method was further developed by Cucker, Krick, Malajovich and Wschebor [139, 140, 141]. They apply it to count solutions of zero-dimensional real polynomial systems. This problem is a particular case of **(X)** in which one restricts inputs to polynomial systems with the same number of equations and variables. The idea of the algorithm is as in [143, 144, 133], to iteratively refine a grid until certain condition holds. However, the main advancement, specially in [140, 141], was a geometric interpretation of the condition number in this setting [140] and a derived probabilistic analysis [140, 141].

²⁴One should mention however the previous work of Goffin [193] that introduced condition numbers in a limited setting of linear programming.

²⁵For comments on the grid method by one of its main characters, Cucker, see his surveys [134] and [135].

²⁶We observe that the expression 'grid method' has a wide meaning. In this thesis, it will just refer to any method based on the introduction of grids on a certain space and operations at each one of its points. Although it should be clear that, in this sense, the grid method was definitely not invented by Cucker and Smale, its application to real algebraic and semialgebraic geometry definitely was.

²⁷The correctness of this intuition was later confirmed by the theoretical results of Nofreini and Townsend [302].

The interaction of the grid method and the computation of topological invariants (of projective real algebraic sets) started with Cucker, Krick and Shub [142]. In [142], they incorporate techniques from topological data analysis such as the reach and the Niyogi-Smale-Weinberger theorem [300; *Proposition 7.1*], relating them to the existing condition number of a real algebraic variety. Among the most interesting results in [142] is the first explicit lower bound on the reach in terms of a parameter depending on the description of the variety: Smale's γ -invariant.

The generalization (from algebraic sets to basic semialgebraic sets) and simplification of the grid method applied to the computation of homology was done by Bürgisser, Cucker and Lairez [88]. In this work, sharper bounds and easier proofs were introduced for many of the results in [142] and the results of topological data analysis in [300]. However, the main progress occurred due to mainly two technical improvements: a bound for the reach of an intersection in terms of the reach of intersections of the boundaries, and a method for choosing the approximating points in the grid based on an inclusion-criterion and not an inclusion-exclusion scheme.

The main similarity between the above numerical algorithms with the symbolic ones in [33, 35, 23] is that the homology is computed by computing a cover of the set. The main difference lies in the fact that the covers in [33, 35, 23] are difficult to describe (each element is a semialgebraic set with its own description) and they are not topologically nice (i.e., they do not satisfy the Leray property), while the covers produced by the grid method [142, 88] are easy to describe (they are just a union of balls) and are topologically nice (i.e. they satisfy the Leray property). This property of the covers produced by the grid method is what allows numerical algorithms to use easier algebraic topological tools to compute the homology and so to be faster.

0§3–2 Contributions to the problem

Our contributions to the problem are, mainly, to produce both algebraic topological and semialgebraic tools to compute the homology of semialgebraic sets using the grid method, which allows to give the first algorithm that solves (B) (and so also (B)) in singly exponential time with high probability. This was done in [91, 92] together with Bürgisser and Cucker. Another contribution, which belongs to the different problem of computation of piecewise linear isotopic approximations, is to provide a complexity analysis of an algorithm, the Plantinga-Vegter algorithm. We show that this algorithm works in average polynomial time. The importance of this result lies in the fact that it opens the door, for the first time ever, to numerical algorithms based on the grid method to be shown to run in finite expected time. This was done in [136] together with Cucker and Ergür.

(B) in weak singly exponential time

In [91], the main addition to the grid method was the development of a method to construct a simplicial complex with the same homology as a closed general semialgebraic set. This was done by developing functorial methods in topological data analysis. With this method, we can construct the simplicial complexes just by constructing it for the atoms and then combining the “atomic simplicial complexes” in the same manner the formula of the semialgebraic set combines the atoms. Another crucial step was a quantitative version of

Durfee's theorem [163].

In [92], the main contribution was to develop a quantitative version of the Gabrielov-Vorobjov theorem [186]. In this quantitative version, the original inequalities \ll , meaning sufficiently small in a precise sense, were substituted by simple strict inequalities of the form $<$ and a global upper bound linear in the inverse of the condition number. Here, the application of the Mather-Thom theory introduced in [91] is necessary. With this explicit version, one can just apply the construction of Gabrielov and Vorobjov [186] to pass from the general case to the closed case.

One can see a certain similarity with the symbolic history. In a way, the results in [91] are analogous to those in [23] in the sense that both deal with how to get more topological information out of covers. The reason why [91] leads to a better run-time with high probability is that the covers of the grid method are simpler and so they can be combined in an easier way than those used before in [23]. Similarly, the core results of [92], the quantitative Gabrielov-Vorobjov theorem, are completely analogous to that used in [33, 35] to pass from the general to the closed case. The main difficulty for the grid method is that we cannot leave the realms of the real numbers, while in the symbolic methods the fact that the original inequalities work only for sufficiently small numbers is not relevant algorithmically as one can work with infinitesimals to go around this issue.

Despite all possible similarities, the underlying methods of the symbolic algorithms in [21, 33, 35, 23] are fundamentally different from those of the grid method. This is the main reason behind the progress in [91, 92] that has brought (B) down to weak singly exponential time. These ideas will be exposed in Chapters 1, 2, 3 and 4.

Adaptive grid method

The motivation for the work in [136] was the observation that a condition-based complexity analysis of the Plantinga-Vegter algorithm [315], which computes an isotopic piecewise-linear approximation of implicit curves and surfaces, would be possible. The existing complexity analysis by Burr, Gao and Tsigaridas [98, 99] gave only complexity bounds exponential on the degree. The progress in [136] relied on a condition-based approach and the continuous amortization technique developed by Burr, Krahmer and Yap [100] and Burr [97].

Interestingly, subdivision-based methods such as the Plantinga-Vegter algorithms can be interpreted as adaptive grid methods. The main difference with the usual grid method is that the grid is not refined globally, but locally depending on whether at a given point we need a finer grid. In this way, the main contribution in [136] was that, for the first time, it showed that an algorithm in real numerical algebraic geometry could have finite expected time. Moreover, the probabilistic estimates of [136] didn't come from integral geometry, but from geometric functional analysis like those of Ergür, Paouris and Rojas [175, 176]. This allowed for a probabilistic bound using probability distributions more general than the normal distribution.

However, the most important contributions in [136] are in the future possibilities that it suggests. On the one hand, it shows how the condition-based complexity can be applied to analyze subdivision-based methods. On the other hand, it has opened a roadmap to the development of a numerical algorithm that not only solves (B) in weak singly exponential time, but in average singly exponential time. We explore this possibility in Chapter 5.

AI Analytical index

The following analytical index briefly presents the content of each chapter. It is intended to give an overview of the topics and structure of the thesis.

Chapter 1

The condition number for problems involving semialgebraic sets measures how transversely the zero sets of the polynomials defining it intersect. In the special case of spherical algebraic sets, this condition number is well-behaved and has good properties, both geometric and probabilistic. In the general case, these properties are transmitted in the homogeneous case, almost immediately, and in the affine case, after some effort. A probabilistic analysis of each of these notions of condition numbers is performed for normally distributed random polynomials.

Chapter 2

When the condition number is finite, certain deformations of the semialgebraic set can be done with explicit constants and inequalities, depending linearly on the inverse of the condition number itself. The main tools are differential topology and Mather-Thom theory. For well-posed cases, quantitative versions are given for Durfee's theorem and the Gabrielov-Vorobjov construction.

Chapter 3

The homology of a closed set can be computed using clouds of points (i.e., unions of balls). A measure for the quality of the approximation is the Hausdorff distance. There is a geometric property of the set, the reach or local feature size, which controls the size of correctly-approximating clouds of points (Niyogi-Smale-Weinberger theorem). The reach behaves well with respect to intersections, analytic and basic semialgebraic subsets. The homology of a cloud of points can be computed by considering only the intersection relations of the cover (Nerve theorem). It is enough to consider the pairwise intersections of the cover (Attali-Lieutier-Salinas theorem).

Chapter 4

Numerical algorithms are a valuable tool for solving problems. There is an algorithm for computing the homology of semialgebraic sets which is singly exponential with high probability. We do a condition-based and a probabilistic complexity analysis of this algorithm. The numerical algorithm have parts that are highly parallelizable and it is numerically stable.

Chapter 5

One can perform the probabilistic analysis for the condition number of random polynomials that are not normally distributed. Adaptive methods can provide faster numerical algorithms: this is shown with the Plantinga-Vegter algorithm and the Han covering algorithm. We propose a пятилетка program with questions and problems regarding the computation of topological invariants and the first half of Hilbert sixteenth problem.

Appendix F

The properties of the real zero set of a real system of polynomials is governed by the number of non-zero terms in the system and not necessarily the degree of the terms. The classical results on fewnomial are still far from the resolution of Kushnirenko's hypothesis. Kushnirenko's hypothesis is true on average. Fewnomial systems with very few terms have with very high probability no real zeros. Problems related to a possible probabilistic theory of fewnomials are stated.

Apéndice M

El tema principal de esta tesis es el cálculo numérico de grupos de homología de conjuntos semialgebraicos. Yendo término por término, tratamos de dar una imagen global de cuál es el tema a una persona que no esté familiarizada con las matemáticas.

There was nothing there now except a single Commandment. It ran:

ALL ANIMALS ARE EQUAL
BUT SOME ANIMALS ARE MORE EQUAL
THAN OTHERS.

George Orwell, Animal Farm: A Fairy Story

1

Condition numbers for the homology of semialgebraic sets

Like the animals in George Orwell's *Animal Farm* [Q11], all inputs of a given size are equal, but some inputs are more equal than others for a numerical algorithm. The condition number, which is a measure of numerical sensitivity with respect to the problem, lies at the heart of this difference.

In general, a *condition number* of an input with respect to a problem measures how much the answer to the problem changes depending on how much the input changes. However, we are dealing with problems such as (B) and (B) where the output is discrete. Because of this, in these problems, the *condition number* should bound the inverse of maximum possible variation of the input such that the output does not change.

In this chapter, we will introduce the condition number $\bar{\kappa}_{\text{aff}}$ that will be the basis of our condition-based complexity analyses. To do this, we deal first with the homogeneous and spherical case where the usual condition-based framework for real algebraic geometry has been developed.

First, we introduce the Weyl norm, which will be the “ruler” we will use to measure the variations in the space of polynomials, and the class of KSS random polynomial tuples; second, we introduce the condition number of an homogeneous polynomial tuple; third, we introduce the intersection condition number of an homogeneous polynomial tuple; and fourth and last, we introduce the intersection condition number of a polynomial tuple in the non-homogenous case. In all the cases, we will discuss the properties and deduce the corresponding bounds, deterministic and probabilistic, of all the introduced condition numbers.

1 §1 Homogeneous polynomials and Weyl norm

Fix $q, n \in \mathbb{N}$ and $\mathbf{d} = (d_1, \dots, d_q) \in \mathbb{N}^q$. Consider the space of \mathbf{d} -homogeneous polynomial q -tuples

$$\mathcal{H}_{\mathbf{d}}[q] := \{f \in \mathbb{R}[X_0, X_1, \dots, X_n]^q \mid f_i \text{ homogeneous of degree } d_i\} \quad (1.1)$$

and let $D := \max_{i \in [q]} d_i$. Let $X^\alpha := X_0^{\alpha_0} \cdots X_n^{\alpha_n}$ and write every f_i as $f_i = \sum_{|\alpha|=d_i} f_{i,\alpha} X^\alpha$, so that $f_{i,\alpha}$ denotes the α -coefficient of f_i . The *Weyl norm* is the norm given by

$$\|f\|_W := \sqrt{\sum_{i=1}^q \|f_i\|_W^2} \quad \text{and} \quad \|f_i\|_W := \sqrt{\sum_{|\alpha|=d_i} \binom{d_i}{\alpha}^{-1} f_{i,\alpha}} \quad (1.2)$$

where $\binom{d_i}{\alpha} = \frac{d_i!}{\alpha_0! \alpha_1! \cdots \alpha_n!}$ is the multinomial coefficient. Note that the Weyl norm comes from an inner product, which we will write as

$$\langle f, g \rangle_W = \sum_{i=1}^q \sum_{|\alpha|=d_i} \binom{d_i}{\alpha}^{-1} f_{i,\alpha} g_{i,\alpha} \quad (1.3)$$

for $f, g \in \mathcal{H}_{\mathbf{d}}[q]$.

Remark 1 §1.1. Although the definition above and the results below are stated over the real numbers, the analogous results hold over the complex numbers, when we substitute the the Weyl norm by its complex version. This will only be important when we prove Lemma 1 §2.8, whose easiest proof is by passing through the complex version of the results here. ¶

1 §1–1 The three main properties of the Weyl norm

There are three reasons why the Weyl norm is used. First, it allows one to write nice formulas for the point-wise evaluation and derivation of polynomials. Second, it has an orthogonal invariance, which means it does not favor any direction in the space where we evaluate homogenous polynomials. Third, it controls the norm of the evaluations of the polynomials and their derivatives.

Evaluation and derivation as polynomials

Let $x, v \in \mathbb{S}^n$ be such that $v \in T_x \mathbb{S}^n$ and $i \in [q]$, then define the polynomial tuples

$$\text{ev}_x^i := \langle x, X \rangle^{d_i} e_i \in \mathcal{H}_{\mathbf{d}}[q] \quad \text{and} \quad \text{dev}_{x,v}^i := \sqrt{d_i} \langle x, X \rangle^{d_i-1} \langle v, X \rangle e_i \in \mathcal{H}_{\mathbf{d}}[q] \quad (1.4)$$

where $e_i \in \mathbb{R}^q$ is the vector with one in the i th component and zeros in the rest. We view X as the vector $(X_0, \dots, X_n)^*$ and we write $\langle \cdot, \cdot \rangle$ for the standard inner product of \mathbb{R}^n .

Proposition 1 §1.1. Let $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $x, v \in \mathbb{S}^n$ such that $v \in T_x \mathbb{S}^n$. Then

$$\langle f, \text{ev}_x^i \rangle_W = f_i(x) \quad \text{and} \quad \langle f, \text{dev}_{x,v}^i \rangle_W = \frac{1}{\sqrt{d_i}} D_x f_i(v).$$

In particular, $\|\text{ev}_x^i\|_W = 1$, $\|\text{dev}_{x,v}^i\|_W = 1$ and $\langle \text{ev}_x^i, \text{dev}_{x,v}^i \rangle_W = 0$.

Proof. By the multinomial formula,

$$\text{ev}_x^i = \left(\sum_{k=0}^n x_i X_i \right)^{d_i} e_i = \left(\sum_{|\alpha|=d_i} \binom{d_i}{\alpha} x^\alpha X^\alpha \right) e_i$$

and so, by (1 . 3),

$$\langle f, \text{ev}_x^i \rangle_W = \sum_{|\alpha|=d_i} f_{i,\alpha} x^\alpha = f_i(x).$$

Similarly, one can see that

$$\text{dev}_{x,v}^i = \frac{1}{\sqrt{d_i}} \left(\sum_{|\alpha|=d_i} \binom{d_i}{\alpha} \left(\sum_{k=0}^n \alpha_k x^{\alpha-e_k} v_k \right) X^\alpha \right) e_i,$$

and so, by (1 . 3),

$$\begin{aligned} \langle f, \text{dev}_{x,v}^i \rangle_W \\ = \frac{1}{\sqrt{d_i}} \sum_{|\alpha|=d_i} f_{i,\alpha} \left(\sum_{k=0}^n \alpha_k x^{\alpha-e_k} v_k \right) = \frac{1}{\sqrt{d_i}} \sum_{k=0}^n \left(\sum_{|\alpha|=d_i} \alpha_k f_{i,\alpha} x^{\alpha-e_k} \right) v_k = \frac{1}{\sqrt{d_i}} D_x f_i v, \end{aligned}$$

where the last equality holds because v is orthogonal to x . The last claim follows easily from computing the evaluation and the derivative. \square

Corollary 1^{S1}2. *The set $\{\text{ev}_x^i \mid x \in \mathbb{S}^n, i \in [q]\}$ linearly spans $\mathcal{H}_d[q]$.*

Proof. By Proposition 1^{S1}1, the orthogonal complement of this set is

$$\{f \in \mathcal{H}_d[q] \mid \text{for all } x \in \mathbb{S}^n, f(x) = 0\}.$$

So we only have to show that this is the zero subspace. However, the only homogenous polynomial which vanishes in all points of the sphere is the zero polynomial. Therefore the claim follows. \square

Corollary 1^{S1}3. [87; §16.3]. *For every $x \in \mathbb{S}^n$, there is an orthogonal decomposition*

$$\mathcal{H}_d[q] = C_x(\mathcal{H}_d[q]) \oplus L_x(\mathcal{H}_d[q]) \oplus R_x(\mathcal{H}_d[q])$$

where

$$(R) \quad R_x(\mathcal{H}_d[q]) := \{g \in \mathcal{H}_d[q] \mid g(x) = 0, D_x g = 0\},$$

$$(L) \quad L_x(\mathcal{H}_d[q]) := \{g \in R_x(\mathcal{H}_d[q])^\perp \mid g(x) = 0\} = \text{span}(\text{dev}_{x,v}^i \mid i \in [q], v \in \mathbb{S}^n \cap x^\perp),$$

and

$$(C) \quad C_x(\mathcal{H}_d[q]) := \{g \in R_x(\mathcal{H}_d[q])^\perp \mid D_x g = 0\} = \text{span}(\text{ev}_x^i \mid i \in [q]).$$

Further, $\{\text{ev}_x^i\}_{i \in [q]}$ is an orthonormal basis of $C_x(\mathcal{H}_d[q])$ and, for $\{v_j\}_{j \in [n]}$ an orthonormal basis of $T_x \mathbb{S}^n = x^\perp$, $\{\text{ev}_{x,v_j}^i\}_{i \in [q], j \in [n]}$ is an orthonormal basis of $L_x(\mathcal{H}_d[q])$.

Proof. Fix an orthonormal basis $\{v_j\}_{j \in [n]}$ of x^\perp . Then, by Proposition 1§1.1, we have that $\{\text{ev}_x^i, \text{dev}_{x,v_1}^i, \dots, \text{dev}_{x,v_x}^i\}_{i \in [q]}$ is an orthonormal system. Now, also by Proposition 1§1.1, we have that $R_x(\mathcal{H}_d[q])$ is its orthogonal complement, and so

$$R_x(\mathcal{H}_d[q])^\perp = \text{span}(\text{ev}_x^i, \text{dev}_{x,v_1}^i, \dots, \text{dev}_{x,v_x}^i \mid i \in [q]).$$

Thus $C_x(\mathcal{H}_d[q]), L_x(\mathcal{H}_d[q]) \subseteq \text{span}(\text{ev}_x^i, \text{dev}_{x,v_1}^i, \dots, \text{dev}_{x,v_x}^i \mid i \in [q])$. Now, by Proposition 1§1.1, we have that

$$C_x(\mathcal{H}_d[q]) \perp \text{span}(\text{dev}_{x,v_j}^i \mid i \in [q], j \in [n]) \text{ and } L_x(\mathcal{H}_d[q]) \perp \text{span}(\text{ev}_x^i \mid i \in [q])$$

and

$$C_x(\mathcal{H}_d[q]) \supseteq \text{span}(\text{ev}_x^i \mid i \in [q]) \text{ and } L_x(\mathcal{H}_d[q]) \supseteq \text{span}(\text{dev}_{x,v_j}^i \mid i \in [q], j \in [n]).$$

This concludes the proof. \square

Remark 1§1.2. When $\mathcal{H}_d[q]$ is clear from the context, we will just write C_x, L_x and R_x instead of $C_x(\mathcal{H}_d[q]), L_x(\mathcal{H}_d[q])$ and $R_x(\mathcal{H}_d[q])$. \P

Orthogonal invariance

The natural action of $O(n+1)$ on \mathbb{R}^n extends naturally to an action on $\mathcal{H}_d[q]$ given by pre-composition. Given $f \in \mathcal{H}_d[q]$ and $u \in O(n+1)$, we define

$$f^u := f(uX) \tag{1.5}$$

where uX is the multiplication of the vector $X = (X_0, \dots, X_n)^*$ with u . Note that this means that we are viewing the action of $O(n+1)$ on $\mathcal{H}_d[q]$ as a right action.

Proposition 1§1.4. [87; Theorem 16.3]. Let $f, g \in \mathcal{H}_d[q]$ and $u \in O(n+1)$. Then

$$\langle f^u, g^u \rangle_W = \langle f, g \rangle_W \text{ and } \|p^u\|_W = \|p\|_W.$$

Proof. It is enough to prove that for some generating subset $S \subseteq \mathcal{H}_d[q]$, the claim holds for all $f, g \in S$. Let S be the generating set of Corollary 1§1.2. For all $\text{ev}_x^i \in S$ and $u \in O(n+1)$, $(\text{ev}_x^i)^u = \text{ev}_{u^{-1}x}^i$. Therefore for all $\text{ev}_x^i, \text{ev}_y^j \in S$ and $u \in O(n+1)$,

$$\langle (\text{ev}_x^i)^u, (\text{ev}_y^j)^u \rangle_W = \langle \text{ev}_{u^{-1}x}^i, \text{ev}_{u^{-1}y}^j \rangle_W.$$

If $i \neq j$, this equals zero. If $i = j$, then, by Proposition 1§1.1, it equals

$$\langle u^{-1}x, u^{-1}y \rangle^{d_i} = \langle x, y \rangle^{d_i}$$

where the equality follows from the fact that u is orthogonal. Hence for every $\text{ev}_x^i, \text{ev}_y^j \in S$ and $u \in O(n+1)$, the value of $\langle (\text{ev}_x^i)^u, (\text{ev}_y^j)^u \rangle_W$ is independent of u and so equals $\langle \text{ev}_x^i, \text{ev}_y^j \rangle_W$, as desired. \square

Remark 1§1.3. We note that, in contrast with the unitary action on complex homogeneous polynomials, $\mathcal{H}_d[1]$ is not an irreducible $O(n+1)$ -module. This means that the Weyl norm is not the unique, up to scalar multiplication, orthogonally invariant norm on $\mathcal{H}_d[1]$. Moreover, one can check that the Weyl norm on $\mathcal{H}_d[1]$ is not equal to the L_2 -norm, $\|p\|_2 := \sqrt{\mathbb{E}_{x \in \mathbb{S}^n} \|p(x)\|^2}$, up to any scalar, because while any two monomials are orthogonal with respect to the Weyl inner product, this is not true with respect to the L_2 inner product with the exception of the linear case. \P

Corollary 1^{S1}5. [87; §16.3]. Let $x \in \mathbb{S}^n$ and consider the orthogonal decomposition of $\mathcal{H}_d[q]$ of Corollary 1^{S1}3. Then for all $u \in O(n+1)$,

$$C_x^u = C_{u^{-1}x}, L_x^u = L_{u^{-1}x} \text{ and } R_x^u = R_{u^{-1}x}.$$

In particular, the orthogonal decomposition of $\mathcal{H}_d[q]$ of Corollary 1^{S1}3 remains invariant under those orthogonal transformations that fix x .

Proof. This is immediate from the definitions of Corollary 1^{S1}3 and the fact that the action of $O(n+1)$ on $\mathcal{H}_d[q]$ respects the Weyl inner product, by Proposition 1^{S1}4. \square

Evaluation and derivative bounds

Recall that any space of matrices $\mathbb{R}^{a \times b}$ has an inner product, called *Frobenius inner product*, given by

$$\langle M, \tilde{M} \rangle_F := \text{tr}(M\tilde{M}^*) \quad (1.6)$$

for $M, \tilde{M} \in \mathbb{R}^{a \times b}$. Associated to this inner product, we have the *Frobenius norm* $\|M\|_F$. Another possible norm is the *operator norm* which is given by

$$\|M\| = \max_{v \in \mathbb{S}^n} \|Mv\| \quad (1.7)$$

Recall that for all $M \in \mathbb{R}^{a \times b}$, $\|M\| \leq \|M\|_F$.

Proposition 1^{S1}6. Let $x \in \mathbb{S}^n$. Consider the linear map

$$\begin{aligned} \mathfrak{R}_x : \mathcal{H}_d[q] &\rightarrow \mathbb{R}^{q \times (n+2)} \\ f &\mapsto \begin{pmatrix} \mathfrak{R}_x^0(f) & \mathfrak{R}_x^1(f) \end{pmatrix} := \begin{pmatrix} f(x) & \Delta_d^{-1} D_x f(\mathbb{I} - xx^*) \end{pmatrix} \end{aligned}$$

where

$$\Delta_d = \begin{pmatrix} \sqrt{d_1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \sqrt{d_q} \end{pmatrix}. \quad (1.8)$$

Then \mathfrak{R}_x is an orthogonal projection whose image is given by

$$\text{im } \mathfrak{R}_x = \{(z, M) \in \mathbb{R}^q \times \mathbb{R}^{q \times (n+1)} \mid Mx = 0\}.$$

Proof. Consider an orthonormal basis $\{v_i\}_{i \in [n]}$ of x^\perp . From this basis, one can construct $\{e_k, e_k v_1^*, \dots, e_k v_n^*\}_{k \in [q]}$ which is an orthonormal basis of $\{(z, M) \in \mathbb{R}^q \times \mathbb{R}^{q \times (n+1)} \mid Mx = 0\}$. In the coordinates of this latter basis, by Proposition 1^{S1}1, we have that $\mathfrak{R}_x(f)$ is written as

$$(\langle \text{ev}_x^1, f \rangle \quad \langle \text{dev}_{x,v_1}^1, f \rangle \quad \dots \quad \langle \text{dev}_{x,v_n}^1, f \rangle \quad \dots \quad \langle \text{ev}_x^q, f \rangle \quad \langle \text{dev}_{x,v_1}^q, f \rangle \quad \dots \quad \langle \text{dev}_{x,v_n}^q, f \rangle)^*.$$

Since $\{\text{ev}_x^k, \text{dev}_{x,v_1}^k, \dots, \text{dev}_{x,v_n}^k\}_{k \in [q]}$ is an orthonormal system by Proposition 1^{S1}1, the claim follows. \square

Corollary 1^{S1}7. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then

$$\|f(x)\| \leq \|f\|_W \text{ and } \|\Delta_d^{-1} D_x f\| \leq \|f\|_W$$

where $\|\cdot\|$ is the operator norm and Δ_d as in (1.8).

Proof. $\mathfrak{R}_x^0 : f \mapsto f(x)$ is an orthogonal projection, by Proposition 1§1.6. Therefore the first inequality holds. For all $v \in T_x \mathbb{S}^n \cap \mathbb{S}^n$, $f \mapsto \Delta_{\mathbf{d}}^{-1} D_x f v$ is an orthogonal projection, because, by Proposition 1§1.6, it is a composition of orthogonal projections. Therefore the second inequality follows. \square

Recall that the geodesic distance on \mathbb{S}^n , $\text{dist}_{\mathbb{S}}$, is the distance given

$$\text{dist}_{\mathbb{S}}(x, \tilde{x}) := \arccos \langle x, \tilde{x} \rangle. \quad (1.9)$$

One can see that $\text{dist}_{\mathbb{S}}(x, \tilde{x})$ is the length of the shortest path inside \mathbb{S}^n joining x and \tilde{x} , which is why it is called “geodesic”.

Corollary 1§1.8 (Exclusion lemma). *Let $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $x, \tilde{x} \in \mathbb{S}^n$. Then*

$$\|f(x) - f(\tilde{x})\| \leq \sqrt{D} \|f\|_W \text{dist}_{\mathbb{S}}(x, \tilde{x})$$

where $\text{dist}_{\mathbb{S}}$ is the geodesic distance on \mathbb{S}^n .

Proof. Let $\gamma : [0, 1] \rightarrow \mathbb{S}^n$ be a constant speed geodesic going from x to \tilde{x} . Then

$$\|f(x) - f(\tilde{x})\| = \left\| \int_0^1 D_{\gamma(t)} f \gamma'(t) dt \right\| \leq \text{dist}_{\mathbb{S}}(x, \tilde{x}) \int_0^1 \|D_{\gamma(t)} f\| dt,$$

where we used that $\|\gamma'(t)\| = \text{dist}_{\mathbb{S}}(x, \tilde{x})$ for a constant speed geodesic whose domain is the interval $[0, 1]$. We have $\|D_{\gamma(t)} f\| \leq \sqrt{D} \|\Delta_{\mathbf{d}}^{-1} D_{\gamma(t)} f\| \leq \sqrt{D}$, due to the bound in Corollary 1§1.7. This concludes the proof. \square

However, we can prove an stronger version of the above corollary where we bound the operator norm of all derivatives. For it, we need to sharpen the bound of the operator norm of $D_x f$ in order to be able to apply an inductive argument. Recall that $\bar{D}_x f$ denotes the tangent map of f as a function on \mathbb{R}^{n+1} , while $D_x f$ the tangent map as a function on \mathbb{S}^n .

Proposition 1§1.9. *Let $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $v \in \mathbb{S}^n$. Then $\bar{D}_x f v \in \mathcal{H}_{\mathbf{d}-1}[q]$ and*

$$\|\bar{D}_x f v\|_W \leq D \|f\|_W,$$

where $\Delta_{\mathbf{d}}$ is as in (1.8). Further, $\|\Delta_{\mathbf{d}}^{-1} \bar{D}_x f v\|_W \leq \sqrt{D} \|f\|_W$.

Proof. By Proposition 1§1.4, we can assume without loss of generality that $v = e_0$. Indeed, let $u \in O(n+1)$ be such that $ue_0 = v$, then

$$\|\Delta_{\mathbf{d}}^{-1} \bar{D}_x f v\|_W = \|(\Delta_{\mathbf{d}}^{-1} \bar{D}_x f ue_0)^u\|_W = \|\Delta_{\mathbf{d}}^{-1} \bar{D}_x f^u e_0\|_W \leq \|f^u\|_W = \|f\|_W.$$

Let $M_{\mathbf{d}, \alpha}^i := \binom{d_i}{\alpha}^{\frac{1}{2}} X^\alpha e_i$. Then $\{M_{\mathbf{d}, \alpha}^i \mid i \in [q], |\alpha| = d_i\}$ is an orthonormal basis of $\mathcal{H}_{\mathbf{d}}[q]$. By direct computation,

$$\left\langle M_{\mathbf{d}-1, \alpha}^i, \bar{D}_x f e_0 \right\rangle_W = \left\langle d_i M_{\mathbf{d}-1, \alpha}^i X_0, f \right\rangle_W.$$

Hence the linear map $\mathcal{L} : \mathcal{H}[q] \rightarrow \mathcal{H}_{\mathbf{d}-1}[q]$ given by $f \mapsto \bar{D}_x f v$ can be written as

$$\sum_{i, \alpha} M_{\mathbf{d}-1, \alpha}^i \left(d_i M_{\mathbf{d}-1, \alpha}^i X_0 \right)^*.$$

Now, $\{d_i M_{\mathbf{d}-1,\alpha}^i X_0 \mid i \in [q], |\alpha| = d_i - 1\}$ is an orthogonal system, although not an orthonormal one, such that for each i and α , $\|d_i M_{\mathbf{d}-1,\alpha}^i X_0\| \leq d_i \leq D$. Therefore $\|\mathcal{L}\| \leq D$ and so the main claim follows. For the last claim, note that $\langle d_i M_{\mathbf{d}-1,\alpha}^i X_0, \Delta_{\mathbf{d}}^{-1} f \rangle_W = \langle \sqrt{d_i} M_{\mathbf{d}-1,\alpha}^i X_0, f \rangle_W$ and proceed analogously using the latter expression. \square

Recall that for a k -multilinear map $\mathcal{L} : \mathbb{R}^{n_1+1} \times \cdots \times \mathbb{R}^{n_k+1} \rightarrow \mathbb{R}^q$, its operator norm is given by

$$\|\mathcal{L}\| := \max \{\|\mathcal{L}(v_1, \dots, v_k)\| \mid v_1 \in \mathbb{S}^{n_1}, \dots, v_k \in \mathbb{S}^{n_k}\}.$$

Corollary 1§1.10. *Let $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $x \in \mathbb{S}^n$. Then, for all $k \geq 1$,*

$$\left\| \frac{1}{k!} \Delta_{\mathbf{d}}^{-1} \bar{D}_x^k f \right\| \leq \frac{1}{\sqrt{D}} \binom{D}{k} \|f\|_W$$

where $\|\cdot\|$ is the operator norm for multilinear maps.

Proof. Fix $v_1, \dots, v_k \in \mathbb{S}^n$, then

$$\begin{aligned} \left\| \frac{1}{k!} \Delta_{\mathbf{d}}^{-1} \bar{D}_x^k f(v_1, \dots, v_k) \right\|_W &= \frac{1}{k!} \left\| \Delta_{\mathbf{d}}^{-1} \bar{D}_x^k f(v_1, \dots, v_k) \right\|_W \\ &\leq \frac{D-k}{k!} \left\| \Delta_{\mathbf{d}}^{-1} \bar{D}_x^{k-1} f(v_1, \dots, v_{k-1}) \right\|_W \leq \cdots \leq \frac{(D-k) \cdots (D-2)}{k!} \left\| \Delta_{\mathbf{d}}^{-1} \bar{D}_x f(v_1) \right\|_W \\ &\leq \frac{(D-k) \cdots (D-2) \sqrt{D}}{k!} \|f\|_W = \frac{1}{\sqrt{D}} \binom{D}{k} \|f\|_W \end{aligned}$$

by applying inductively the (first) inequality of Proposition 1§1.9 in the second line and the last inequality in the last line. Then Corollary 1§1.7 and maximising over v_1, \dots, v_k finishes the proof. \square

1§1–2 Random polynomials in $\mathcal{H}_{\mathbf{d}}[q]$

Among all distributions in \mathbb{R}^N , there is one that occupies a special place: the normal distribution. Recall that the *normal distribution* centered at $x \in \mathbb{R}^N$ and with standard deviation $\sigma > 0$, $N(x, \sigma)$, is the absolutely continuous probability distribution on \mathbb{R}^n with density function

$$z \mapsto \frac{1}{(2\pi)^{N/2} \sigma^N} e^{-\frac{\|z-x\|^2}{2\sigma^2}}.$$

The *standard normal distribution* is the normal distribution centered at 0 and with typical deviation 1. A *Gaussian random vector* $\mathfrak{x} \in \mathbb{R}^N$ is a random vector distributed according to the standard normal distribution $N(0, 1)$. To indicate that a random vector $\mathfrak{x} \in \mathbb{R}^N$ has the normal distribution $N(x, \sigma)$, we will simply write $\mathfrak{x} \sim N(x, \sigma)$.

This distribution has many properties that make it special:

1. It is invariant under orthogonal transformations, and so it does not favor any direction in space. I.e., if \mathfrak{x} is a random vector such that $\mathfrak{x} \sim N(0, \sigma)$ and $u \in O(N)$, then $u\mathfrak{x} \sim N(0, \sigma)$.

2. If $\mathbf{x} \in \mathbb{R}^N$ and $\mathbf{y} \in \mathbb{R}^{N'}$ are independent random vectors such that $\mathbf{x} \sim N(\mathbf{x}, \sigma)$ and $\mathbf{y} \sim N(\mathbf{y}, \sigma)$, then

$$\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \sim N\left(\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}, \sigma\right).$$

3. If $\mathbf{x}, \mathbf{y} \in \mathbb{R}^N$ are independent random vectors such that $\mathbf{x} \sim N(\mathbf{x}, \sigma)$ and $\mathbf{y} \sim N(\mathbf{y}, \zeta)$ and $\lambda, \mu \in \mathbb{R}$, then $\lambda\mathbf{x} + \mu\mathbf{y} \sim N(\lambda\mathbf{x} + \mu\mathbf{y}, \sqrt{\lambda^2\sigma^2 + \mu^2\zeta^2})$. In particular, $\mathbf{x} + \mathbf{y} \sim N(\mathbf{x} + \mathbf{y}, \sqrt{\sigma^2 + \zeta^2})$.
4. If $\mathbf{x} \in \mathbb{R}^N$ is a random vector such that $\mathbf{x} \sim N(\mathbf{x}, \sigma)$ and $P : \mathbb{R}^N \rightarrow \mathbb{R}^{N'}$ is an orthogonal projection, then $P\mathbf{x} \sim N(P\mathbf{x}, \sigma)$.
5. If $\mathbf{x} \in \mathbb{R}^N$ is a Gaussian random vector, then $\mathbf{x}/\|\mathbf{x}\|$ has the uniform distribution on the unit sphere \mathbb{S}^{N-1} , $U(\mathbb{S}^{N-1})$.
6. Among all probability distributions on \mathbb{R}^N with the same mean and covariance matrix¹, the normal distribution is the one having maximum entropy [132, Theorem 9.6.5]. In other words, it is the distribution to choose when only the mean and covariance matrix of a distribution are available.

In a finite dimensional real vector space with an inner product, we can define analogously the normal distribution $N(\mathbf{x}, \sigma)$ by considering the corresponding norm instead. This will allow us to talk about *Gaussian random matrices* where the inner product is the Frobenius one and about random polynomials, by considering the Weyl inner product of $\mathcal{H}_d[\mathbf{q}]$. This motivates the following definition.

Definition 1 §1.1. A KSS random polynomial tuple \mathbf{f} is a random polynomial tuple $\mathbf{f} \in \mathcal{H}_d[\mathbf{q}]$ with an absolutely continuous distribution whose density function is given by

$$\delta_{\mathbf{f}}(\mathbf{f}) := \frac{1}{(2\pi)^{N/2}} e^{-\frac{\|\mathbf{f}\|_W^2}{2}}.$$

Remark 1 §1.4. The terms “KSS” is an acronym for Kostlan-Shub-Smale, in honor of the creators of the distribution. See [265], [166] and [367]. ¶

We finish with a proposition that will be useful later, since it gives the probability distribution of the norm of a KSS random polynomial tuple. Recall that the χ^2 -distribution with m degrees of freedom, χ_m^2 , is the probability distribution of the square of the norm of a Gaussian random vector $\mathbf{x} \in \mathbb{R}^m$. One can easily show that its density function is given by

$$\frac{1}{2^{m/2}\Gamma(m/2)} t^{\frac{m}{2}-1} e^{-\frac{t}{2}}$$

for $t > 0$, where $\Gamma(s) := \int_0^\infty x^{s-1} e^{-x} dx$ is Euler’s Γ function.

¹The covariance matrix of a random vector $\mathbf{x} \in \mathbb{R}^N$ is the matrix $\mathbb{E}(\mathbf{x} - \mathbb{E}\mathbf{x})(\mathbf{x} - \mathbb{E}\mathbf{x})^*$. If $\mathbf{x} \sim N(\mathbf{x}, \sigma)$, then $\sigma^2\mathbb{I}$ is the covariance matrix of \mathbf{x} .

Proposition 1^{§1} 11. Let $\mathbf{x} \in \mathbb{R}^m$ be a Gaussian random vector. Then the density function of $\|\mathbf{x}\|$ is given by

$$\delta_{\|\mathbf{x}\|}(t) = \frac{1}{2^{m/2-1}\Gamma(m/2)} t^{m-1} e^{-\frac{t^2}{2}}$$

for $t \geq 0$. Further, for $t \geq 2$,

$$\mathbb{P}(\|\mathbf{x}\| \geq t + \sqrt{m}) \leq e^{1-\frac{t^2}{2}}.$$

Proof. For the first claim, we only apply the change of variables theorem of integration.

For the second one, note that

$$\delta_{\|\mathbf{x}\|}(t + \sqrt{m}) = \frac{1}{2^{m/2-1}\Gamma(m/2)} \frac{(t + \sqrt{m})^{\frac{m-1}{2}}}{e^{\sqrt{m}(t+\sqrt{m})}} e^{\frac{m-t^2}{2}}.$$

Hence

$$\begin{aligned} \mathbb{P}(\|\mathbf{x}\| \geq t + \sqrt{m}) &= \int_t^\infty \delta_{\|\mathbf{x}\|}(s + \sqrt{m}) ds \\ &\leq \int_t^\infty \frac{1}{2^{m/2-1}\Gamma(m/2)} \frac{(s + \sqrt{m})^{\frac{m-1}{2}}}{e^{\sqrt{m}(s+\sqrt{m})}} e^{\frac{m-s^2}{2}} ds \\ &\leq e^{\frac{m-t^2}{2}} \int_t^\infty \frac{1}{2^{m/2-1}\Gamma(m/2)} \frac{(s + \sqrt{m})^{\frac{m-1}{2}}}{e^{\sqrt{m}(s+\sqrt{m})}} ds \\ &= e^{\frac{m-t^2}{2}} \int_{\sqrt{m}(t+\sqrt{m})}^\infty \frac{s^{\frac{m+1}{2}-1} e^{-s}}{2^{m/2-1} m^{\frac{m+1}{4}} \Gamma(m/2)} ds \\ &\leq e^{\frac{m-t^2}{2}} \int_1^\infty \frac{s^{\frac{m+1}{2}-1} e^{-s}}{2^{m/2-1} m^{\frac{m+1}{4}} \Gamma(m/2)} ds \\ &= e^{\frac{m-t^2}{2}} \frac{\Gamma(\frac{m+1}{2})}{2^{m/2-1} m^{\frac{m+1}{4}} \Gamma(m/2)} \leq \frac{e^m}{2^{\frac{m}{2}+1} m^{\frac{m-1}{4}}} e^{-\frac{t^2}{2}} \end{aligned}$$

where the last inequality follows from $\Gamma(\frac{m+1}{2})/\Gamma(\frac{m}{2}) \leq \Gamma(\frac{m}{2}+1)/\Gamma(\frac{m}{2}) = \frac{m}{2}$. To finish the proof, we just observe that $\frac{e^m}{2^{\frac{m}{2}+1} m^{\frac{m-1}{4}}} \leq e$. \square

1^{§2} κ : a condition number for spherical algebraic sets

When can arbitrarily small perturbations of a polynomial tuple $\mathbf{f} \in \mathcal{H}_d[\mathbf{q}]$ alter the local topology of the zero set $\mathcal{Z}^S(\mathbf{f})$ around a point $x \in \mathbb{S}^n$? This can only happen at a singularity, since all regular zeros look locally the same and all non-zeros also look the same. Motivated by this, one defines the following local condition number.

Definition 1^{§2} 1. Let $\mathbf{f} \in \mathcal{H}_d[\mathbf{q}]$ and $x \in \mathbb{S}^n$, the *local condition number* of \mathbf{f} at x , $\kappa(\mathbf{f}, x)$, is the quantity in $(0, \infty]$ given by

$$\kappa(\mathbf{f}, x) := \frac{\|\mathbf{f}\|_W}{\sqrt{\|\mathbf{f}(x)\|^2 + \sigma_q(\Delta_d^{-1} D_x \mathbf{f})^2}} \tag{1.10}$$

where σ_q is the q th singular value, Δ_d as in (1.8) and $D_x \mathbf{f} : T_x \mathbb{S}^n \rightarrow \mathbb{R}^q$ the tangent map.

Since one expects the global topology not to change when the local topology does not change at any point, this motivates the following definition.

Definition 1 §2 2. Let $f \in \mathcal{H}_d[q]$, the *global condition number* of f , $\kappa(f)$, is the quantity in $(0, \infty]$ given by

$$\kappa(f) := \max_{x \in \mathbb{S}^n} \kappa(f, x). \quad (1.11)$$

In the Definition 1 §2 1, we note that, in the denominator of $\kappa(f, x)$, $\|f(x)\|$ controls how near is f of having a zero at x and $\sigma_q(\Delta_d^{-1} D_x f)$ how near of not having full rank $D_x f$ is. Thus $\kappa(f, x)$ is large when f is near of having a singular zero at x . The following proposition is a weak formalization of this observation. Recall that the zero set $\mathcal{Z}(f) := f^{-1}(0)$ of a map $f : M \rightarrow \mathbb{R}^q$, where M is a smooth manifold, is called *regular* if for all $x \in \mathcal{Z}(f)$, $\text{rank } D_x f = q$.

Proposition 1 §2 1. Let $f \in \mathcal{H}_d[q]$. Then $\mathcal{Z}^S(f) := \{x \in \mathbb{S}^n \mid f(x) = 0\}$ has a singularity at $x \in \mathbb{S}^n$ iff $\kappa(f, x) = \infty$. In particular, $\mathcal{Z}^S(f)$ is regular iff $\kappa(f) < \infty$. \square

In the next chapter, we will prove the following theorem which justifies the name condition number at least from the point of view of computing the homology groups.

Theorem 1 §2 2. Let $f \in \mathcal{H}_d[q]$ be such that $\kappa(f) < \infty$. Then for all $g \in B_w(f, \kappa(f)^{-1} \|f\|_w)$, $H_\bullet(\mathcal{Z}^S(f)) \cong H_\bullet(\mathcal{Z}^S(g))$.

We will focus in the properties and possible bounds of the condition number. We will finish with a discussion, showing that many possible alternative definitions are computationally equivalent. Let us note that the definition of this condition number is the consequence of a long sequence of works [143, 144, 133, 139, 140, 141, 142, 88, 91, 92], so our choice of properties is motivated by what this experience has shown to be important in the application of κ as a condition number.

1 §2 – 1 Fundamental properties

There are roughly four main properties of the local condition number that will be fundamental in our work. We go one by one.

Regularity inequality

The regularity inequality relates how near is x from being a zero of f with how near of being singular $D_x f$ is. This will be used whenever we need to justify that we can compute the pseudoinverse of $D_x f$ near the zero set of f . Recall that for a surjective linear map A , the *pseudoinverse*, A^\dagger , is the linear map given by

$$A^\dagger := A^*(AA^*)^{-1} \quad (1.12)$$

for which $AA^\dagger = I$ and $A^\dagger A$ is the orthogonal projection onto $(\ker A)^\perp$.

Proposition 1 §2 3 (Regularity inequality). [91; Proposition 3.6]. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then either

$$\frac{\|f(x)\|}{\|f\|_w} \geq \frac{1}{\sqrt{2}\kappa(f, x)} \text{ or } \frac{\sigma_q(\Delta_d^{-1} D_x f)}{\|f\|_w} \geq \frac{1}{\sqrt{2}\kappa(f, x)}.$$

In particular, if $\sqrt{2}\kappa(f, x) \frac{\|f(x)\|}{\|f\|_W} < 1$, then $D_x f : T_x \mathbb{S}^n \rightarrow \mathbb{R}^q$ is surjective and its pseudoinverse $D_x f^\dagger$ exists.

Proof. Assume that neither of the alternatives holds, then

$$\frac{1}{\kappa(f, x)} = \sqrt{\left(\frac{\|f(x)\|}{\|f\|_W}\right)^2 + \left(\frac{\sigma_q(\Delta_d D_x f)}{\|f\|_W}\right)^2} < \sqrt{\frac{1}{2\kappa(f, x)^2} + \frac{1}{2\kappa(f, x)^2}} = \frac{1}{\kappa(f, x)}$$

which gives a contradiction. Hence at least one of the options should hold. The last claims follows from the fact that a matrix $A \in \mathbb{R}^{q \times (n+1)}$ is surjective iff $\sigma_q(A) > 0$ since $q \leq n$. \square

1st Lipschitz property

The first Lipschitz property of the local condition number tells us that $\kappa(f, x)^{-1} \|f\|_W$ as a function of f is a Lipschitz function. This guarantees that sufficiently small errors in f do not affect dramatically the condition number. Extending by continuity, we take $\kappa(0, x) = \infty$ and $\|0\|_W \kappa(0, x)^{-1} = 0$.

Proposition 1^{S2} 4 (1st Lipschitz property). *Let $x \in \mathbb{S}^n$. Then the map*

$$\begin{aligned} \mathcal{H}_d[q] &\rightarrow [0, \infty) \\ f &\mapsto \frac{\|f\|_W}{\kappa(f, x)} \end{aligned}$$

is 1-Lipschitz with respect to the Weyl norm.

Proof. By Definition 1^{S2} 1 and Proposition 1^{S1} 6, we can write

$$\frac{\|f\|_W}{\kappa(f, x)} = \|(\mathfrak{R}_x^0(f), \sigma_q(\mathfrak{R}_x^1(f)))\|$$

where the right-hand side norm is the usual Euclidean norm. Then, by the triangle inequality,

$$\left| \frac{\|f\|_W}{\kappa(f, x)} - \frac{\|\tilde{f}\|_W}{\kappa(\tilde{f}, x)} \right| \leq \|(\mathfrak{R}_x^0(f) - \mathfrak{R}_x^0(\tilde{f}), \sigma_q(\mathfrak{R}_x^1(f)) - \sigma_q(\mathfrak{R}_x^1(\tilde{f})))\|.$$

We know that σ_q is 1-Lipschitz with respect to the operator norm. Therefore

$$\begin{aligned} \left| \frac{\|f\|_W}{\kappa(f, x)} - \frac{\|\tilde{f}\|_W}{\kappa(\tilde{f}, x)} \right| &\leq \|(\mathfrak{R}_x^0(f) - \mathfrak{R}_x^0(\tilde{f}), \|\mathfrak{R}_x^1(f) - \mathfrak{R}_x^1(\tilde{f})\|)\| \\ &= \|(\mathfrak{R}_x^0(f - \tilde{f}), \|\mathfrak{R}_x^1(f - \tilde{f})\|)\| \leq \|\mathfrak{R}_x(f - \tilde{f})\|_F \leq \|f - \tilde{f}\|_W = \text{dist}_W(f, \tilde{f}) \end{aligned}$$

where, in the second line, the equality follows from the linearity of \mathfrak{R}_x , the first inequality from the inequality between the operator and the Frobenius norms, and the second inequality from Proposition 1^{S1} 6, which claims that \mathfrak{R}_x is an orthogonal projection. The proposition is proven. \square

Corollary 1^{S2} 5. *The map*

$$\begin{aligned} \mathcal{H}_d[q] &\rightarrow [0, \infty] \\ f &\mapsto \frac{\|f\|_W}{\kappa(f)} \end{aligned}$$

is 1-Lipschitz with respect to the Weyl norm.

Proof. Note that $f \mapsto \|f\|_W/\kappa(f)$ is defined as the pointwise minimum of a family of non-negative 1-Lipschitz functions. Hence it is 1-Lipschitz. \square

Corollary 1§2 6. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then $\kappa(f, x) \geq 1$ and $\kappa(f) \geq 1$.

Proof. By applying Proposition 1§2 4 to f and 0, we have

$$\frac{\|f\|_W}{\kappa(f, x)} = \left| \frac{\|f\|_W}{\kappa(f, x)} - \frac{\|0\|_W}{\kappa(0, x)} \right| \leq \|f - 0\|_W = \|f\|_W$$

which gives the desired claim. \square

2nd Lipschitz property

The second Lipschitz property of the local condition number establishes the Lipschitz-ness with respect to the second argument.

Proposition 1§2 7 (2nd Lipschitz property). [88; Proposition 4.7]. Let $f \in \mathcal{H}_d[q]$. The map

$$\begin{aligned} \mathbb{S}^n &\rightarrow [0, 1] \\ x &\mapsto \frac{1}{\kappa(f, x)} \end{aligned}$$

is D-Lipschitz with respect to the geodesic distance on \mathbb{S}^n .

To prove this property, we will use the following lemma.

Lemma 1§2 8. Let $f \in \mathcal{H}_d[q]$ and $A \in \mathbb{R}^{(n+1) \times (n+1)}$ be an antisymmetric matrix. Then $\bar{D}_X f AX \in \mathcal{H}_d[q]$ and $\|\bar{D}_X f AX\| \leq D\|A\|\|f\|_W$.

Proof of Proposition 1§2 7. Let u be any orthogonal transformation taking x to \tilde{x} . Then we have that $\kappa(f, \tilde{x}) = \kappa(f^u, x)$. Therefore, by the 1st Lipschitz property,

$$\left| \frac{1}{\kappa(f, x)} - \frac{1}{\kappa(f, \tilde{x})} \right| = \frac{1}{\|f\|_W} \left| \frac{\|f\|_W}{\kappa(f, x)} - \frac{\|f^u\|_W}{\kappa(f^u, x)} \right| \leq \frac{\|f - f^u\|_W}{\|f\|_W}$$

where we have used that $\|f\| = \|f^u\|$ by Proposition 1§1 4.

Consider now the constant-speed path $u : [0, 1] \rightarrow O(n + 1)$ obtained by doing the planar rotation between x and \tilde{x} from the zero angle to the full angle $\text{dist}_{\mathbb{S}}(x, \tilde{x})$. By the chain rule,

$$\frac{d}{dt} f^{u(t)} = \bar{D}_{u(t)X} f u'(t)X = D_X(f^{u(t)}) u(t)^* u'(t)X.$$

Therefore

$$\|f - f^u\|_W = \left\| \int_0^1 \frac{d}{dt} f^{u(t)} ds \right\|_W \leq \int_0^1 \left\| D_X(f^{u(t)}) u(t)^* u'(t)X \right\|_W ds.$$

Now, note that $\|u(t)^* u'(t)\| = \|u'(t)\| = \text{dist}_{\mathbb{S}}(x, \tilde{x})$ and that $u(t)^* u'(t)$ is antisymmetric, because $u : [0, 1] \rightarrow O(n + 1)$ is a planar rotation going from the angle zero to $\text{dist}_{\mathbb{S}}(x, \tilde{x})$. Hence, by Lemma 1§2 8, $\|f - f^u\|_W \leq D \text{dist}_{\mathbb{S}}(x, \tilde{x}) \|f\|_W$ and the proof concludes. \square

Proof of Lemma 1^{§2}8. The present proof could be carried inside the framework of the reals, but it would be too tedious to do so.² This is why we will work for this proof over the complex numbers. Let $u \in U(n+1)$ be the unitary transformation such that

$$u^*Au = \begin{pmatrix} \sqrt{-1}s_0 & & \\ & \ddots & \\ & & \sqrt{-1}s_n \end{pmatrix} =: \sqrt{-1}S.$$

Then

$$(D_X f AX)^u = D_{uX} f AuX = D_{uX} f u u^*AuX = D_X f^u (\sqrt{-1}S)X$$

and so, by the complex version of Proposition 1^{§1}4, we can assume, without loss of generality, that A is already a purely imaginary diagonal matrix.

By direct computation,

$$(\bar{D}_X f (\sqrt{-1}S)X)_i = \sum_{|\alpha|=d_i} \sqrt{-1}f_{i,\alpha} \left(\sum_{k=0}^n \alpha_k s_k \right) X^\alpha = \sum_{|\alpha|=d_i} \sqrt{-1}f_{i,\alpha} \langle \alpha, s \rangle X^\alpha$$

where we use that both α and s are real in the last equality. Thus

$$\| \bar{D}_X f (\sqrt{-1}S)X \|_W^2 = \sum_{i,\alpha} \binom{d_i}{\alpha}^{-1} |f_{i,\alpha}|^2 |\langle \alpha, s \rangle|^2.$$

By Hölder's inequality, $|\langle \alpha, s \rangle| \leq \|\alpha\|_1 \|s\|_\infty \leq D \|S\|$, and the proof concludes. \square

Condition number theorem

The *local discriminant set* at x is the set

$$\Sigma_d[q]_x := \{g \in \mathcal{H}_d[q] \mid g(x) = 0, \text{rank } D_x g < q\} \quad (1.13)$$

and the *discriminant set* the set

$$\Sigma_d[q] := \bigcup \{\Sigma_d[q]_x \mid x \in \mathbb{S}^n\}. \quad (1.14)$$

Once can see that Proposition 1^{§2}1 can be reformulated as saying that

$$\Sigma_d[q]_x = \{g \in \mathcal{H}_d[q] \mid \kappa(g, x) = \infty\} \text{ and } \Sigma_d[q] = \{g \in \mathcal{H}_d[q] \mid \kappa(g) = \infty\}.$$

This claim can be made stronger by relating the condition number to the distance of f to these sets. This is the so-called condition number theorem, which gives a nice geometric interpretation of the condition number.

Theorem 1^{§2}9 (Local condition number theorem). [87; Proposition 19.6] and [88; Theorem 4.4]. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then

$$\kappa(f, x) = \frac{\|f\|_W}{\text{dist}_W(f, \Sigma_d[q]_x)}$$

where dist_W is the distance with respect to the Weyl norm.

²This is so, because over the complex numbers we can put A in diagonal form without loss of generality, but this is not true over the reals, since its eigenvalues are either zero or imaginary.

Proof. We only have to show that $\kappa(f, x) \leq \frac{\|f\|_W}{\text{dist}_W(f, \Sigma_{\mathbf{d}}[q]_x)}$, since the other inequality follows directly from the 1st Lipschitz property (Proposition 1 §2 4) by letting the other polynomial tuple to be in $\Sigma_{\mathbf{d}}[q]_x$.

Let $v \in (\ker \Delta_{\mathbf{d}}^{-1} D_x f)^{\perp} \cap \mathbb{S}^n$ be such that

$$\|\Delta_{\mathbf{d}}^{-1} D_x f v\| = \sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f)$$

and \tilde{f} be the orthogonal projection of f onto $\{\text{ev}_x^i, \text{dev}_{x,v}^i \mid i \in [q]\}^{\perp}$, i.e.,

$$\tilde{f} := f - \sum_{i \in [q]} \langle f, \text{ev}_x^i \rangle \text{ev}_x^i - \sum_{i \in [q]} \langle f, \text{dev}_{x,v}^i \rangle \text{dev}_{x,v}^i$$

where, by Proposition 1 §1 1, $\langle f, \text{ev}_x^i \rangle = f_i(x)$ and $\langle f, \text{dev}_{x,v}^i \rangle$ is the i th component of $\Delta_{\mathbf{d}}^{-1} D_x f v$.

By the above, this means that $\tilde{f}(x) = 0$ and that

$$\Delta_{\mathbf{d}}^{-1} D_x \tilde{f} = \Delta_{\mathbf{d}}^{-1} D_x f (\mathbb{I} - vv^*)$$

which has q th singular value equal to zero, because v was chosen to be the singular vector associated to the q th singular value of $\Delta_{\mathbf{d}}^{-1} D_x f$. This means that $\kappa(\tilde{f}, x) = \infty$ and so $\tilde{f} \in \Sigma_{\mathbf{d}}[q]_x$. Further, by Proposition 1 §1 1,

$$\begin{aligned} \text{dist}_W(f, \tilde{f}) &= \left\| \sum_{i \in [q]} \langle f, \text{ev}_x^i \rangle \text{ev}_x^i + \sum_{i \in [q]} \langle f, \text{dev}_{x,v}^i \rangle \text{dev}_{x,v}^i \right\|_W \\ &= \sqrt{\|f(x)\|^2 + \|\Delta_{\mathbf{d}}^{-1} D_x f v\|^2} = \frac{\|f\|_W}{\kappa(f, x)} \end{aligned}$$

which implies that $\text{dist}_W(f, \Sigma_{\mathbf{d}}[q]_x) \leq \|f\|_W / \kappa(f, x)$, as desired. \square

Corollary 1 §2 10 (Global condition number theorem). [87; Theorem 19.3] and [88; Theorem 4.4]. Let $f \in \mathcal{H}_{\mathbf{d}}[q]$. Then

$$\kappa(f) = \frac{\|f\|_W}{\text{dist}_W(f, \Sigma_{\mathbf{d}}[q])}$$

where dist_W is the distance with respect to the Weyl norm.

Proof. Just notice that $\text{dist}_W(f, \Sigma_{\mathbf{d}}[q]) = \min_{x \in \mathbb{S}^n} \text{dist}_W(f, \Sigma_{\mathbf{d}}[q]_x)$. \square

In view of the above theorem, we can interpret Theorem 1 §2 2 as saying that no changes in topology will occur as long as we don't cross $\Sigma_{\mathbf{d}}[q]$.

Higher derivative estimate

The higher derivative estimate relates Smale's γ with the condition number. Its usefulness relies on the fact that while for computing Smale's γ one needs to evaluate all higher derivatives of f , this is not necessary to evaluate the condition number. For $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $x \in \mathbb{S}^n$, let us define

$$\mu(f, x) := \frac{\|f\|_W}{\sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f)} = \|f\|_W \|D_x f^\dagger \Delta_{\mathbf{d}}\| \quad (1.15)$$

where Δ_d is as in (1.8). We note that, in general, $\kappa(f, x) \leq \mu(f, x)$, with equality if $f(x) = 0$; and that if $\sqrt{2} \frac{\|f(x)\|}{\|f\|_w} < 1$, $\mu(f, x) \leq \sqrt{2}\kappa(f, x)$, by the regularity inequality (Proposition 1^{§2}3).

Recall that $D_x f$ refers to the tangent map $T_x \mathbb{S}^n \rightarrow \mathbb{R}^q$ and $\bar{D}_x f$ to the tangent map $T_x \mathbb{R}^{n+1} \rightarrow \mathbb{R}^q$. The notion of Smale's gamma gives information about the magnitude of the higher derivatives of an analytic function.

Definition 1^{§2}3. Let $f : \mathbb{R}^m \rightarrow \mathbb{R}^q$ be an analytic function and $x \in \mathbb{R}^m$ be a point. Then Smale's gamma of f at x , $\bar{\gamma}(f, x)$, is the non-negative real number given by

$$\bar{\gamma}(f, x) := \sup_{k \geq 2} \left\| \frac{1}{k!} \bar{D}_x f^\dagger \bar{D}_x^k f \right\|^{\frac{1}{k-1}} \quad (1.16)$$

where $\bar{D}_x^k f$ is the tensor formed by the derivatives of order k of f , \dagger is the pseudoinverse and $\|\cdot\|$ is the operator norm. By convention, $\bar{\gamma}(f, x) = \infty$ when $\bar{D}_x f$ is not surjective.

Together with this notion, we introduce the notion of Smale's projective γ , which is Smale's γ with the derivative substituted by the derivative on the sphere.

Definition 1^{§2}4. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then Smale's projective gamma of f at x , $\gamma(f, x)$, is the non-negative real number given by

$$\gamma(f, x) := \sup_{k \geq 2} \left\| \frac{1}{k!} D_x f^\dagger \bar{D}_x^k f \right\|^{\frac{1}{k-1}} \quad (1.17)$$

where $\bar{D}_x^k f$ is the tensor formed by the derivatives of order k of f , \dagger is the pseudoinverse and $\|\cdot\|$ is the operator norm. By convention, $\bar{\gamma}(f, x) = \infty$ when $D_x f$ is not surjective.

One can easily see that, in general, $\bar{\gamma}(f, x) \leq \gamma(f, x)$. The higher derivative estimate, relates this quantity with μ .

Proposition 1^{§2}11 (Higher derivative estimate). [87; Theorem 16.1] and [88; Proposition 4.1]. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then

$$\bar{\gamma}(f, x) \leq \gamma(f, x) \leq \frac{1}{2} D^{\frac{3}{2}} \mu(f, x).$$

Proof. By Definition 1^{§2}3, it is enough to bound $\left\| \frac{1}{k!} D_x f^\dagger \bar{D}_x^k f \right\|^{\frac{1}{k-1}}$ for $k \geq 2$. Now,

$$\left\| \frac{1}{k!} D_x f^\dagger \bar{D}_x^k f \right\| \leq \|D_x f^\dagger \Delta_d\| \left\| \frac{1}{k!} \Delta_d \bar{D}_x^k f \right\|$$

where $\left\| \frac{1}{k!} \Delta_d \bar{D}_x^k f \right\| \leq \frac{1}{D^{\frac{1}{2}}} \binom{D}{k} \|f\|_w$, by Corollary 1^{§1}10. Thus

$$\left\| \frac{1}{k!} \bar{D}_x f^\dagger \bar{D}_x^k f \right\|^{\frac{1}{k-1}} \leq \left(\frac{1}{D^{\frac{1}{2}}} \binom{D}{k} \right)^{\frac{1}{k-1}} \mu(f, x)^{\frac{1}{k-1}}.$$

Now, $\mu(f, x) \geq \kappa(f, x) \geq 1$, by Corollary 1^{§2}6, and so $\mu(f, x)^{\frac{1}{k-1}} \leq \mu(f, x)$ for $k \geq 2$. Also, one can easily check that

$$\sup_{k \geq 2} \left(\frac{1}{D^{\frac{1}{2}}} \binom{D}{k} \right)^{\frac{1}{k-1}} \leq \frac{1}{2} D^{\frac{3}{2}},$$

since for $k \geq 3$,

$$\left(\frac{1}{D^{\frac{1}{2}}} \binom{D}{k} \right)^{\frac{1}{k-1}} \leq \binom{D}{k}^{\frac{1}{k-1}} \leq \left(\frac{D^k}{k!} \right)^{\frac{1}{k-1}} = \frac{D^{1+\frac{1}{k-1}}}{(k!)^{\frac{1}{k-1}}} \leq \frac{D^{\frac{3}{2}}}{(2^{k-1})^{\frac{1}{k-1}}} < \frac{1}{2} D^{\frac{3}{2}}.$$

□

However, in our case, the following variant will be more useful since we will consider sums of homogeneous polynomials and constants.

Corollary 1 §2 12. [92; Proposition 4.5]. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Define

$$f_{\mathbb{S}} := \left(f, \sum_{i=0}^n x_i^2 - 1 \right). \quad (1.18)$$

Then

$$2\bar{\gamma}(f_{\mathbb{S}}, x) \leq D^{\frac{3}{2}} \mu(f, x) + D^{\frac{1}{2}} \mu(f, x) \frac{\|f(x)\|}{\|f\|_W} + 1. \quad (1.19)$$

Proof. By direct computation,

$$\bar{D}_x^k f_{\mathbb{S}}(u_1, \dots, u_k) = \begin{cases} \begin{pmatrix} \bar{D}_x f(u_1) \\ 2\langle x, u_1 \rangle \end{pmatrix}, & \text{if } k = 1, \\ \begin{pmatrix} \bar{D}_x^2 f(u_1, u_2) \\ 2\langle u_1, u_2 \rangle \end{pmatrix}, & \text{if } k = 2, \\ \begin{pmatrix} \bar{D}_x^k f(u_1, \dots, u_k) \\ 0 \end{pmatrix}, & \text{if } k > 2. \end{cases}$$

Using this equality for $k = 1$ we deduce that $\ker \bar{D}_x f_{\mathbb{S}} = T_x \mathbb{S}^n \cap \ker \bar{D}_x f = \ker D_x f$. Let $V = (\ker D_x f)^\perp \subseteq T_x \mathbb{S}^n$. Then $(\ker \bar{D}_x f_{\mathbb{S}})^\perp = V + \mathbb{R}x$ and, for all $\lambda \in \mathbb{R}$,

$$\bar{D}_x f_{\mathbb{S}}(v + \lambda x) = \begin{pmatrix} D_x f(v) + \lambda \Delta_d^2 f(x) \\ 2\lambda \end{pmatrix} \quad (1.20)$$

where $\bar{D}_x f(x) = \Delta_d^2 f(x)$ follows from Euler's identity for homogeneous functions.

By explicitly inverting the map in (1.20), we obtain

$$(\bar{D}_x f_{\mathbb{S}})^\dagger \begin{pmatrix} w \\ t \end{pmatrix} = D_x f^\dagger \left(w - \frac{t}{2} \Delta_d^2 f(x) \right) + \frac{t}{2} x.$$

Thus

$$(\bar{D}_x f_{\mathbb{S}})^\dagger \frac{\bar{D}_x^k f_{\mathbb{S}}}{k!}(u_1, \dots, u_k) = \begin{cases} D_x f^\dagger \frac{\bar{D}_x^2 f}{2}(u_1, u_2) - \frac{\langle u_1, u_2 \rangle}{2} D_x f^\dagger \Delta_d^2 f(x) + \frac{\langle u_1, u_2 \rangle}{2} x, & \text{if } k = 2, \\ D_x f^\dagger \frac{\bar{D}_x^k f}{k!}(u_1, \dots, u_k), & \text{if } k > 2. \end{cases}$$

Applying the triangle inequality and Definition 1^{S2}3, we obtain

$$\bar{\gamma}(f_{\mathbb{S}}, x) \leq \gamma(f, x) + \frac{1}{2} \|D_x f^\dagger \Delta^2 f(x)\| + \frac{1}{2},$$

which implies

$$2\bar{\gamma}(f_{\mathbb{S}}, x) \leq D^{\frac{3}{2}} \mu(f, x) + D^{\frac{1}{2}} \mu(f, x) \frac{\|f(x)\|}{\|f\|_w} + 1$$

where the first term in the right-hand side follows from the higher derivative estimate (Proposition 1^{S2}11) and the second from the relations

$$\|D_x f^\dagger \Delta_d^2 f(x)\| \leq \|D_x f^\dagger \Delta_d\| \|\Delta_d\| \|f(x)\| = \|f\|_w \|D_x f^\dagger \Delta_d\| D^{\frac{1}{2}} \frac{\|f(x)\|}{\|f\|_w}$$

and the definition of μ . This finishes the proof. \square

1^{S2}-2 Bounds: worst-case and probabilistic

We present two kinds of bounds for the condition number, which try to go around the fact that the possible maximum of κ is infinite. The first one puts a restriction on the $f \in \mathcal{H}_d[q]$ we consider, like restricting the coefficients to be integers of at most a certain size, and looks for a bound that holds for all f satisfying the restriction for which $\kappa(f)$ is finite. The second one considers a random $f \in \mathcal{H}_d[q]$, such as a KSS random polynomial tuple, and looks for a tail bound for the random variable $\kappa(f)$. Each of them represents a different philosophy in the complexity of numerical algorithms.

Gap theorem for integer inputs

The idea of bounding the condition number in terms of the bit size goes back to Renegar [331]. The underlying philosophy is to translate the condition-based estimates of the condition-using complexity theorist to something that the classical computer scientist can understand, like a worst-case bit complexity estimate. In linear programming, the bound by Renegar (see [87; Proposition 7.9] and associated remarks) was successful in providing bounds giving the desired complexity for a series of algorithms using condition numbers. However, in our case, the bounds obtained will not allow us to get good bit complexity estimates for the algorithms under study.

Theorem 1^{S2}13. *Let $f \in \mathcal{H}_d[q]$ be such that all its coefficients are integers of absolute value at most H . Then either $\kappa(f) = \infty$ or*

$$\kappa(f) \leq \sqrt{2DNH} \left(2^{2-\frac{1+n+q}{4}} D^{\frac{3+n+q}{2}} H \sqrt{N} \right)^{(1+n+q)(4D)^{1+n+q}} = O(DHN)^{O(D)^{1+n+q}}.$$

Proof. The proof relies on a generalization of Polya's theorem by Jeronimo, Perruci and Tsigaridas [236; Theorem 1]. To apply their theorem to our case, we note that

$$2D \left(\frac{\|f\|_w}{\kappa(f)} \right)^2 \geq \min_{x \in \mathbb{S}^n} \left(\|f(x)\|^2 + \sigma_q(\Delta_d^{-1} \bar{D}_x f)^2 \right).$$

To obtain the minimum in the right-hand side as a minimum of a polynomial function, consider the map $g : (x, v) \mapsto \|f(x)\|^2 + \|v^* D_x f\|^2$ and minimize it in the compact semialgebraic set C given by

$$\sum_{i=0}^n x_i^2 = 1, \quad \sum_{i=1}^q d_i v_i^2 = 1.$$

Then

$$2D \left(\frac{\|f\|_W}{\kappa(f)} \right)^2 \geq \min_{(x,v) \in C} g(x, v),$$

since $\sigma_q(D_x f) = \min\{\|D_x f v | \|v\| = 1, x \perp v\}$. Now, a direct computation and a rough estimation shows that g is a polynomial of degree $2D$ whose coefficients are integers of absolute value at most $D^2 H^2 N$. Applying [236; Theorem 1], we obtain

$$\min_{(x,v) \in C} g \geq \left(2^{4 - \frac{1+n+q}{2}} (D^2 H^2 N) (2D)^{1+n+q} \right)^{-(1+n+q)2^{1+n+q}(2D)^{1+n+q}}$$

and so the result follows after minor computations and estimations, since for the given f , we have $\|f\|_W \leq H\sqrt{N}$. \square

Remark 1\\$2 1. The above bound is novel and it was a missing ingredient in the existing theory, when compared to the condition-based complexity framework applied to other problems. It clearly does not lead to single exponential bounds of κ , which controls the run time of the algorithm; although it can be used to guarantee that $\log \kappa$, which controls the precision needed by the algorithm, is singly exponential in n , polynomial in the degree D and linear in the bit size $\log H$ of the coefficients of f . \P

Remark 1\\$2 2. [236; Theorem 1] is a very general result that we apply it to a very particular setting. It would be interesting to see, if using the techniques in [236] and in [235], one can provide a better bound such as the one in the question below.

Open problem A. Let $f \in \mathcal{H}_d[q]$ be such that all its coefficients are integers of absolute value at most H . Is it true that either $\kappa(f) = \infty$ or

$$\kappa(f) \leq O(DHN)^{2^{O(n)}}?$$

A bound like the above would give the grid method the same worst case complexity as CAD, for integer inputs. Also, it would make the precision to be linear in the logarithm of the degree, instead of polynomial in the degree. \P

Probabilistic bounds

The problem of computing a bound for $\kappa(f)$ for restricted $f \in \mathcal{H}_d[q]$ is that a bad f can spoil the full basket. In the same way that we don't judge a community by its worst members, we should not just judge a parameter by its worst value. Behind this way of thinking, trying to understand the full statistics of a behaviour and not just the worst behaviour, lies the founding idea of considering probabilistic bounds of κ . We give two ways of arriving to a probabilistic bound: via integral geometry and via geometric analysis.

We observe that there are two frameworks to obtain probabilistic bounds: the average and the smoothed framework. The difference between them relies on the randomness model used to obtain tail bounds of the condition number. In the average framework, introduced by Goldstine and von Neumann [194], Demmel [149] and Smale [374], one considers a random polynomial tuple $\mathbf{f} \in \mathcal{H}_d[q]$ which has a normal or uniform distribution. This random input is suppose to represent the “average” input that one will find and so the usual behaviour that one will find. In the smoothed framework, introduced by Spielman and Teng [380], one considers a random polynomial tuple $\mathbf{f}_\sigma \in \mathcal{H}_d[q]$ of the form $\mathbf{f}_\sigma := \mathbf{f} + \sigma \mathbf{g}$ with $\mathbf{f} \in \mathcal{H}_d[q]$

fixed, $\sigma > 0$ and \mathbf{g} with a normal or uniform distribution. The random \mathbf{f}_σ represents an input \mathbf{f} with some random perturbation, whose magnitude is controlled by σ . In this way, one hopes to get a bound on the worst probabilistic behaviour of a randomly perturbed input. One should note that as σ grows, one recovers the average framework.

Via integral geometry The integral geometric approach relies heavily on the condition number theorem (Corollary 1^{S2}10) and the geometry of the ill-posed set.

Theorem 1^{S2}14. [87; Theorem 21.1] Let $\Sigma \subseteq \mathbb{R}^N$ be a set and $C : \mathbb{R}^N \setminus \{0\} \rightarrow [1, \infty]$ be given by

$$C(\mathbf{x}) := \frac{\|\mathbf{x}\|}{\text{dist}(\mathbf{x}, \Sigma)}.$$

Assume that there is a homogenous polynomial of degree d containing Σ in its zero set.

(A) Let $X \in \mathbb{R}^N$ be a Gaussian random vector. Then for $t \geq (2d + 1)(N - 1)$,

$$\mathbb{P}(C(X) \geq t) \leq 11d(N - 1) \frac{1}{t}$$

and

$$\mathbb{E} \log C(X) \leq \log(N - 1) + \log d + \log(30).$$

(S) Let $x \in \mathbb{S}^N$, $\sigma \in [0, 1]$ and $X_\sigma \in \mathbb{R}^N$ a random vector uniformly distributed in $B(x, \sigma)$. Then for $t \geq (2d + 1)(N - 1)\sigma^{-1}$,

$$\mathbb{P}(C(X_\sigma) \geq t) \leq 11d(N - 1)\sigma^{-1} \frac{1}{t}$$

and

$$\mathbb{E} \log C(X_\sigma) \leq \log(N - 1) + \log d + \log \sigma^{-1} + \log(30). \quad \square$$

In order to apply this theorem, we need to prove that $\Sigma_d[q]$ is contained in some hypersurface. This can be easily done, using techniques from algebraic geometry. However, we omit the proof as these techniques go beyond the scope of this thesis.

Proposition 1^{S2}15. [88; Proposition 4.20] There is an integer polynomial of degree at most $n2^n D^n$ such that $\Sigma_d[q]$ is contained in its zero set.

Proof. The claim is true for $q \leq n+1$ by [88; Proposition 4.20]. To extend it further, recall that for $q \geq n+1$, $\kappa(f, x) = \|f\|/\|f(x)\|$. Therefore the linear projection $\mathcal{H}_d[q] \rightarrow \mathcal{H}_d[n+1]$ maps surjectively $\Sigma_d[q]$ onto $\Sigma_d[n+1]$ for $q \geq n+1$ and the claim holds also for $q \geq n+1$. \square

Combining the above two results, we obtain the following probabilistic bound on κ .

Proposition 1^{S2}16. (A) Let $\mathbf{f} \in \mathcal{H}_d[q]$ be a KSS random polynomial tuple. Then for $t \geq (n2^{n+1}D^n + 1)(N - 1)$,

$$\mathbb{P}(\kappa(\mathbf{f}) \geq t) \leq 11(n2^{n+1}D^n + 1)(N - 1) \frac{1}{t}$$

and

$$\mathbb{E} \log \kappa(\mathbf{f}) \leq \log(N - 1) + n(\log D + 3 \log 2) + \log(30).$$

(S) Let $f \in \mathcal{H}_d[q]$, $\sigma \in [0, 1]$ and $\mathfrak{f}_\sigma \in \mathcal{H}_d[q]$ a random polynomial tuple uniformly distributed in $B_W(f, \sigma)$. Then for $t \geq (n2^{n+1}D^n + 1)(N - 1)\sigma^{-1}$,

$$\mathbb{P}(\kappa(\mathfrak{f}_\sigma) \geq t) \leq 11(n2^{n+1}D^n + 1)(N - 1)\sigma^{-1} \frac{1}{t}$$

and

$$\mathbb{E} \log \kappa(\mathfrak{f}_\sigma) \leq \log(N - 1) + n(\log D + 3 \log 2) + \log \sigma^{-1} + \log(30). \quad \square$$

Remark 1§2 3. The above results do not apply to the local condition number. The main reason is that the above theorem, coming from [90] of Bürgisser, Cucker and Lotz, only covers the case in which Σ is contained in an algebraic hypersurface, but it does not take advantage of the fact that Σ might have higher codimension. An extension of this form was obtained by Lotz [281], but one should still work the details carefully as in the statement of Theorem 1§2 14.

Open problem B. Can the bound in Theorem 1§2 14 be extended to the case in which Σ is a real algebraic variety of degree d and codimension c in such a way that the probability tail bounds are of the form $O(d(N - 1)t^{-c})$?

Also, the following problem might be useful given the multihomogeneous structure of $\Sigma_d[q]$.

Open problem C. Can the bound in Theorem 1§2 14 be improved in the case in which Σ is a real algebraic hypersurface in $\mathbb{R}^{\sum_{i=1}^q N_i}$ given by a multihomogeneous polynomial $h(X_1, \dots, X_q)$ of degree d_i with respect to the block of N_i variables X_i ? More concretely, let $\mathfrak{x}_1, \dots, \mathfrak{x}_q$ be random vectors uniformly distributed in the unit balls. Is it true that

$$\mathbb{P}(C(\mathfrak{x}) \geq t) \leq O\left(\sqrt{q} \max_{i \in [q]}(d_i(N_i - 1)) \frac{1}{t}\right)$$

as one obtains in the reducible case $\Sigma = \cup_{i \in [q]} \Sigma_i$? ¶

Remark 1§2 4. One should notice that $N - 1$ does not appear dividing in the above bounds and successive bounds as it appears in the bounds given in [91, 92]. This is the case, because there was a mistake in the citation of [87; Theorem 21.1] in [91]. However, this mistake does not affect the order of the estimates. ¶

Via geometric functional analysis The geometric functional analysis framework in the probabilistic analysis of κ is quite new. It was introduced by Ergür, Paouris and Røjas [175, 176] for the zero dimensional case and it was applied by Cucker, Ergür and the author [136] to the case of a single polynomial. The advantage of this method is that it can be applied to distributions more general than the normal distribution. We will show this in Chapter 5 in the special case of hypersurfaces. Here, we will provide a tail bound with a very simple proof for the Gaussian case.

Theorem 1§2 17. (A) Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a KSS random polynomial tuple and $x \in \mathbb{S}^n$. Then for $t \geq 2$,

$$\mathbb{P}(\kappa(\mathfrak{f}, x) \geq t) \leq \frac{7}{2} \left(\frac{119N}{n+1} \right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1}.$$

(S) Let $f \in \mathcal{H}_d[q]$, $\sigma > 0$, $\mathfrak{f}_\sigma := f + \sigma \|f\|_{W^q} g$ be a random polynomial tuple such that $g \in \mathcal{H}_d[q]$ is a KSS random polynomial tuple and $x \in \mathbb{S}^n$. Then for $t \geq 2$,

$$\mathbb{P}(\kappa(\mathfrak{f}_\sigma, x) \geq t) \leq \frac{7}{2} \left(\frac{119N}{n+1} \right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1} \left(1 + \frac{1}{\sigma} \right)^{n+1}.$$

In the proof, we will use the following proposition. Recall that $\omega_m := \pi^{\frac{m}{2}} / \Gamma(\frac{m}{2} + 1)$ is the volume of the unit Euclidean m -ball. We also recall Stirling's estimation of Euler's Gamma function:

$$\frac{(2e)^{\frac{x}{2}}}{\sqrt{\pi} x^{\frac{x+1}{2}}} e^{-\frac{1}{6x}} \leq \frac{1}{\Gamma(\frac{x}{2} + 1)} \leq \frac{(2e)^{\frac{x}{2}}}{\sqrt{\pi} x^{\frac{x+1}{2}}} \quad (1.21)$$

for $x > 0$.

Proposition 1^{§2}18. (V) Let $x \in \mathbb{R}^q$, $\sigma > 0$ and $\mathfrak{x} \sim N(x, \sigma)$ be a random vector. Then for all $\varepsilon > 0$,

$$\mathbb{P}_{\mathfrak{x}}(\|\mathfrak{x}\| \leq \varepsilon) \leq \frac{\omega_q}{(2\pi)^{\frac{q}{2}}} \left(\frac{\varepsilon}{\sigma} \right)^q.$$

(M) Let $q \leq n$, $A \in \mathbb{R}^{q \times n}$, $\sigma > 0$ and $\mathfrak{A} \sim N(A, \sigma)$ be a random matrix. Then for all $\varepsilon > 0$,

$$\mathbb{P}_{\mathfrak{A}}(\sigma_q(\mathfrak{A}) \leq \varepsilon) \leq \frac{\sqrt{q}(2\pi)^{\frac{q}{2}}}{2} \left(\frac{e}{2\pi} \right)^{\frac{n}{2}} \omega_{n+1-q} \left(\frac{\varepsilon}{\sigma} \right)^{n+1-q}.$$

Proof of Proposition 1^{§2}18. (V) can be found at the end of [87; Proof of Proposition 4.21], and (M) in [87; Proof of Proposition 4.19] (page 90), where here the factor $(\frac{e}{1-\lambda})^{\frac{(1-\lambda)n}{2}}$, with $\lambda = \frac{q-1}{n}$, is bounded by $e^{\frac{n}{2}}$. \square

Proof of Theorem 1^{§2}17. (A) We do the proof for $q < n + 1$, for $q \geq n + 1$ is analogous.³ By Proposition 1^{§1}11, we can see that

$$\mathbb{P}(\|\mathfrak{f}\|_W \geq t) \leq e^{1 - \frac{t^2}{8}}$$

for $t \geq 2\sqrt{N}$. Now, note that for all $t > 0$ and $u \geq 2\sqrt{N}$,

$$\begin{aligned} & \mathbb{P}(\kappa(\mathfrak{f}, x)) \\ &= \mathbb{P}\left(\|\mathfrak{f}\|_W / \sqrt{\|\mathfrak{R}_x^0(\mathfrak{f})\|^2 + \sigma_q(\mathfrak{R}_x^1(\mathfrak{f}))^2} \geq t\right) && \text{(By Proposition 1^{§1}6)} \\ &\leq \mathbb{P}\left(\|\mathfrak{f}\|_W \geq u \text{ or } \sqrt{\|\mathfrak{R}_x^0(\mathfrak{f})\|^2 + \sigma_q(\mathfrak{R}_x^1(\mathfrak{f}))^2} \leq u/t\right) && \text{(Implication bound)} \\ &\leq \mathbb{P}(\|\mathfrak{f}\|_W \geq u) + \mathbb{P}\left(\sqrt{\|\mathfrak{R}_x^0(\mathfrak{f})\|^2 + \sigma_q(\mathfrak{R}_x^1(\mathfrak{f}))^2} \leq u/t\right) && \text{(Union bound)} \\ &\leq \mathbb{P}(\|\mathfrak{f}\|_W \geq u) + \mathbb{P}(\|\mathfrak{R}_x^0(\mathfrak{f})\| \leq u/t \text{ and } \sigma_q(\mathfrak{R}_x^1(\mathfrak{f})) \leq u/t) && \text{(Implication bound)} \\ &\leq \mathbb{P}(\|\mathfrak{f}\|_W \geq u) + \mathbb{P}(\|\mathfrak{R}_x^0(\mathfrak{f})\| \leq u/t) \mathbb{P}(\sigma_q(\mathfrak{R}_x^1(\mathfrak{f})) \leq u/t) && (\mathfrak{R}_x^0(\mathfrak{f}), \mathfrak{R}_x^1(\mathfrak{f}) \text{ independent}) \\ &\leq e^{1 - \frac{u^2}{8}} + \frac{\sqrt{q}}{2} \omega_q \omega_{n+1-q} \left(\frac{e}{2\pi} \right)^{\frac{n}{2}} \left(\frac{u}{t} \right)^{n+1} && \text{(Proposition 1^{§2}18).} \end{aligned}$$

³And for $q > n + 1$, one can get a tail bound of the order $O(\ln^{\frac{n+1}{2}} t^{-q})$, but this bound will not be useful for us.

We can apply Proposition 1 §2 18, because, by Proposition 1 §1 6, $\mathfrak{R}_x^0(\mathfrak{f})$ and $\mathfrak{R}_x^1(\mathfrak{f})$ come from taking independent orthogonal projections of \mathfrak{f} . This fact guarantees that $\mathfrak{R}_x^0(\mathfrak{f})$ and $\mathfrak{R}_x^1(\mathfrak{f})$ are independent and Gaussian.

Here, we substitute $u = 2\sqrt{2N} \ln^{\frac{1}{2}} t \geq 2\sqrt{N}$ for $t \geq 2$, and we get for $t \geq 2$,

$$\mathbb{P}(\kappa(f, x)) \leq \left(e + \frac{\sqrt{q}}{2} \omega_q \omega_{n+1-q} \left(\frac{e}{2\pi} \right)^{\frac{n}{2}} (8N)^{\frac{n+1}{2}} \right) \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1}$$

since $t^{-N} \leq \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1}$. We substitute now the formula for ω_m and we use the Stirling estimation (1.21), to obtain the bound

$$\begin{aligned} \frac{\sqrt{q}}{2} \omega_q \omega_{n+1-q} \left(\frac{e}{2\pi} \right)^{\frac{n}{2}} &\leq \sqrt{\frac{e\pi}{2(n-q+1)}} \frac{e^n}{(n-q+1)^{\frac{n-q+1}{2}} q^{\frac{q}{2}}} \\ &\leq \sqrt{\frac{e\pi}{2}} \frac{e^n}{(n-q+1)^{\frac{n-q+1}{2}} q^{\frac{q}{2}}}. \end{aligned}$$

We put $\lambda = \frac{q}{n+1} \in [0, 1]$ and observe that

$$(n-q+1)^{\frac{n-q+1}{2}} q^{\frac{q}{2}} = \left((1-\lambda)^{\frac{1-\lambda}{2}} \lambda^{\frac{\lambda}{2}} \right)^{n+1} (n+1)^{\frac{n+1}{2}} \geq \left(\frac{n+1}{2} \right)^{\frac{n+1}{2}}.$$

This gives us

$$\frac{e^n}{(n-q+1)^{\frac{n-q+1}{2}} q^{\frac{q}{2}}} \leq \frac{e^n}{\left(\frac{n+1}{2} \right)^{\frac{n+1}{2}}} \leq e^{n(1-\frac{1}{2} \ln \frac{n+1}{2})} = \frac{1}{e} \left(\frac{2e^2}{n+1} \right)^{\frac{n+1}{2}} \leq \frac{1}{e} \left(\frac{119/8}{n+1} \right)^{\frac{n+1}{2}}$$

and so the desired bound follows using that $e + \sqrt{\frac{\pi}{2e}} < 7/2$ and that $\left(\frac{119N}{n+1} \right)^{\frac{n+1}{2}} \geq 1$.

(S) For the smoothed case, the proof is analogous to the one above. In this case, we have

$$\mathbb{P}(\|\mathfrak{f}_\sigma\|_W \geq t \|f\|_W) \leq \mathbb{P}(\|\mathfrak{g}\|_W \geq (t-1)/\sigma) \leq e^{1 - \frac{(t-1)^2}{8\sigma^2}}$$

for $t \geq 1+2\sigma\sqrt{N}$. We proceed as above, but we use the general version of Proposition 1 §2 18 and we substitute $u = \|f\|(2\sqrt{2N}\sigma \ln^{\frac{1}{2}} t + 1)$. To obtain the same line of arguments as above, one should only notice that $u \leq \|f\|2\sqrt{2N}\ln^{\frac{1}{2}} t(\sigma+1)$ and so one obtains the same as above, but with the extra factor $(1 + \frac{1}{\sigma})^{n+1}$. \square

To pass from the local condition estimates to the global ones, we use a grid-based method which is common in the probabilistic methods coming from geometric functional analysis (see [399; §4.4]).

Theorem 1 §2 19. (A) Let $\mathfrak{f} \in \mathcal{H}_{\mathbf{d}}[q]$ be a KSS random polynomial tuple. Then for $t \geq 4$,

$$\mathbb{P}(\kappa(\mathfrak{f}) \geq t) \leq 21 \left(\frac{1984N}{n+1} \right)^{\frac{n+1}{2}} D^n \frac{\ln^{\frac{n+1}{2}} t}{t}.$$

(S) Let $f \in \mathcal{H}_d[q]$, $\sigma > 0$, $\tilde{f}_\sigma := f + \sigma \|f\| g$ be a random polynomial tuple such that $g \in \mathcal{H}_d[q]$ is a KSS random polynomial tuple. Then for $t \geq 4$,

$$\mathbb{P}(\kappa(\tilde{f}_\sigma) \geq t) \leq 21 \left(\frac{1984N}{n+1} \right)^{\frac{n+1}{2}} D^n \frac{\ln^{\frac{n+1}{2}} t}{t} \left(1 + \frac{1}{\sigma} \right)^{n+1}.$$

For proving the above theorem, we need the following lemma for “constructing” an optimal grid that allows us to sample efficiently in the sphere and pass from the tail bound estimates of the probability of the local condition number to the ones of the global condition number.

Lemma 1^{S2}20. [398; Lemma 5.2] (cf. [399; §4.2]). Let $\delta \in (0, \pi/3)$. Then there is a finite set $N_\delta \subseteq \mathbb{S}^n$ such that for all $y \in \mathbb{S}^n$, $\text{dist}_{\mathbb{S}}(y, N_\delta) < \delta$ and such that

$$\# N_\delta \leq 3 \left(\frac{3}{\delta} \right)^n.$$

Proof of Theorem 1^{S2}19. (A) Fix $t \geq 4$. Let $\mathcal{G} \subseteq \mathbb{S}^n$ be such that for all $y \in \mathbb{S}^n$, $\text{dist}_{\mathbb{S}}(y, \mathcal{G}) < \frac{1}{Dt}$ and define

$$\kappa_{\mathcal{G}}(\tilde{f}) := \max_{x \in \mathcal{G}} \kappa(\tilde{f}, x).$$

By the 2nd Lipschitz property (Proposition 1^{S2}7),

$$\frac{1}{\kappa_{\mathcal{G}}(\tilde{f})} - \frac{1}{\kappa(\tilde{f})} \leq D \frac{1}{Dt} = \frac{1}{t}$$

and so

$$\kappa_{\mathcal{G}}(\tilde{f}) \geq \frac{\kappa(\tilde{f})}{1 + \frac{\kappa(\tilde{f})}{t}} \geq \frac{t}{2}.$$

Hence $\kappa(f) \geq t$ implies $\kappa_{\mathcal{G}}(\tilde{f}) \geq t/2$ and so, by the implication bound,

$$\mathbb{P}(\kappa(\tilde{f}) \geq t) \leq \mathbb{P}(\kappa_{\mathcal{G}}(\tilde{f}) \geq t/2) \leq \# \mathcal{G} \max_{x \in \mathcal{G}} \mathbb{P}(\kappa(\tilde{f}, x) \geq t/2)$$

where the last inequality is the union bound. Without loss of generality, we can assume $\# \mathcal{G} \leq 3(3Dt)^n$, by Lemma 1^{S2}20 (taking $\delta = 1/(Dt)$). Finally, Theorem 1^{S2}17 together with some computations finishes the proof.

(S) Exactly like (A). □

Proof of Lemma 1^{S2}20. Let N_δ be a maximal set of \mathbb{S}^n such that for each distinct $x, \tilde{x} \in N_\delta$, $\text{dist}_{\mathbb{S}}(x, \tilde{x}) \geq \delta$. Such a set exists and its finite, since otherwise we can construct a sequence $\{x_k\}$ in \mathbb{S}^n such that for all distinct $k, l \in \mathbb{N}$, $\text{dist}_{\mathbb{S}}(x_k, x_l) \geq \delta$ contradicting the compactness of \mathbb{S}^n . This set satisfies the first property, since for all $y \in \mathbb{S}^n$, $\text{dist}(y, N_\delta) < \delta$, otherwise $N_\delta \cup \{y\}$ would contradict the maximality of N_δ .

By construction, the family of sets $\{B_{\mathbb{S}}(x, \delta/2) \mid x \in N_\delta\}$ is disjoint and so

$$\# N_\delta \text{ vol}_n(B_{\mathbb{S}}(e_0, \delta/2)) = \text{vol}_n \bigcup \{B_{\mathbb{S}}(x, \delta/2) \mid x \in N_\delta\} \leq \text{vol}_n(\mathbb{S}^n) = (n+1)\omega_{n+1}.$$

Now, by [87; Lemma 2.31],

$$\text{vol}_n(B_{\mathbb{S}}(e_0, \delta/2)) = n\omega_n \int_0^{\frac{\delta}{2}} \sin^{n-1} s ds \geq \omega_n \int_0^{\frac{\delta}{2}} n \sin^{n-1} s \cos s ds = \omega_n \sin^n \frac{\delta}{2}.$$

Note that $\sin x \geq \frac{3x}{\pi}$ for $x \in (0, \pi/6)$, so $\sin^n \frac{\delta}{2} \geq \left(\frac{3\delta}{2\pi}\right)^n$. Finally, a simple maximization shows that the bound provided is correct. \square

Remark 1§2.5. The geometric functional analysis' approach definitely provides a more elementary proof than the integral geometric approach. This can be a good pedagogical tool when one cannot go into the details of the integral geometric proof. However, the bounds obtained are worse, both in the constants and asymptotically. The latter seems to be an intrinsic characteristic of the method (since similar issues happen in [175, 176]), but it may be because some of the traditionally used probabilistic bounds⁴ are not the best bounds for the job.

Open problem D. Can one obtain tail bounds of the form

$$\mathbb{P}(\kappa(f, x) \geq t) \leq O\left(\text{poly}(N)^{\text{poly}(n)} \frac{1}{t^{n+1}}\right) \text{ and } \mathbb{P}(\kappa(f) \geq t) \leq O\left(\text{poly}(D, N)^{\text{poly}(n)} \frac{1}{t}\right)$$

using the methods of geometric functional analysis? For an approach looking to prove the above estimate, the techniques from [141] might be useful.

Despite all the above said about the drawbacks of the methods from geometric functional analysis, we have to point out that these methods have an advantage over the methods from integral geometry: they are able to handle probability distributions that are not normal. This was shown for the zero dimensional case in [175, 176] and for the case of a single polynomial in [136], which we will cover in Chapter 5. ¶

1§2–3 Alternative definitions of κ

Now that we have gone through all the theory, one might wonder about alternative definitions of κ that might be better from one perspective or another. The following proposition however shows that all natural variations are equivalent up to a reasonable constant or parameter.

Proposition 1§2.21. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. Then:

$$(0) \text{ For } \kappa_0(f, x) := \|f\|_W / \max\{\|f(x)\|, \sigma_q(\Delta_d^{-1} D_x f)\},$$

$$\frac{1}{\sqrt{2}} \kappa_0(f, x) \leq \kappa(f, x) \leq \kappa_0(f, x).$$

$$(1) \text{ For } \kappa_1(f, x) := \|f\|_W / \sqrt{\|f(x)\|^2 + \sigma_q(D_x f)^2},$$

$$\kappa_1(f, x) \leq \kappa(f, x) \leq \sqrt{D} \kappa_1(f, x).$$

$$(2) \text{ For } \kappa_2(f, x) := \|f\|_W / \sqrt{\|f(x)\|^2 + \sigma_q(\Delta_d^{-1} \bar{D}_x f)^2}, \text{ where } \bar{D}_x f \text{ is the derivative of } f \text{ as a map on } \mathbb{R}^{n+1},$$

$$\kappa_2(f, x) \leq \kappa(f, x) \leq \sqrt{1 + D} \kappa_2(f, x).$$

⁴Specially $\mathbb{P}(\mathfrak{x}/\mathfrak{y} \geq t) \leq \mathbb{P}(\mathfrak{x} \geq u \text{ or } \mathfrak{y} \leq ut) \leq \mathbb{P}(\mathfrak{x} \geq u) + \mathbb{P}(\mathfrak{y} \leq ut)$.

(3) For $\kappa_3(f, x) := \|\hat{f}\|_W / \sqrt{\|\hat{f}(x)\|^2 + \sigma_q(\Delta_{\mathbf{d}}^{-1} D_x \hat{f})^2}$ where $\hat{f} := (f_i / \|f_i\|_W)_{i \in [q]}$,

$$\frac{1}{\sqrt{q}} \kappa_3(f, x) \leq \frac{\|f\|_W}{\sqrt{q} \max_{i \in [q]} \|f_i\|_W} \kappa_3(f, x) \leq \kappa(f, x) \leq \frac{\|f\|_W}{\sqrt{q} \min_{i \in [q]} \|f_i\|_W} \kappa_3(f, x).$$

Proof. (0) follows from the inequality between the ℓ_∞ and ℓ_2 -norms in \mathbb{R}^2 , (1) from

$$\frac{1}{\sqrt{D}} \sigma_q(D_x f) \leq \sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f) \leq \sigma_q(D_x f),$$

(2) from

$$\begin{aligned} \sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f) &\leq \sigma_q(\Delta_{\mathbf{d}}^{-1} \bar{D}_x f) = \sigma_q(\Delta_{\mathbf{d}}^{-1} \bar{D}_x f (\mathbb{I} - x x^*) + \Delta_{\mathbf{d}} f(x) x^*) \\ &\leq \sqrt{\sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f)^2 + D \|f(x)\|^2}, \end{aligned}$$

and (3) from

$$\frac{\|f\|_W}{\max_{i \in [q]} \|f_i\|_W} \frac{\|f(x)\|}{\|f\|_W} \leq \|\hat{f}(x)\| \leq \frac{\|f\|_W}{\min_{i \in [q]} \|f_i\|_W} \frac{\|f(x)\|}{\|f\|_W}$$

and

$$\frac{\|f\|_W}{\max_{i \in [q]} \|f_i\|_W} \frac{\sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f)}{\|f\|_W} \leq \sigma_q(\Delta_{\mathbf{d}}^{-1} D_x \hat{f}) \leq \frac{\|f\|_W}{\min_{i \in [q]} \|f_i\|_W} \frac{\sigma_q(\Delta_{\mathbf{d}}^{-1} D_x f)}{\|f\|_W}.$$

□

The above proposition only shows some of the variations, which can be themselves combined. In the end, the reason to choose the definition that we have chosen is conceptual and historical, since it is the one that allows us to develop the theory in its maximum aesthetic appealing.

Remark 1§26. Among the variants of κ above, the only one that is not strongly equivalent is κ_3 . This is so, because κ_3 is small whenever κ is so, but the opposite implication is not true. To see this, note that κ_3 is invariant under scalar multiplication of each component of f , while this property is not true for κ . By taking one component to zero, we can construct a sequence $\{f_k\}$ such that $\{\kappa_3(f_k)\}$ is constant, but $\{\kappa_3(f_k)\}$ goes to infinity. ¶

Remark 1§27. One can observe that Proposition 1§22(2) is just [142; Proposition 6.1]. However, the difference in the constants is due to an error in the proof in [142], in which they used the identity $f_i(e_0) = \partial f / \partial X_0(e_0)$ instead of the correct $f_i(e_0) = d_i \partial f / \partial X_0(e_0)$, due to Euler's identity. ¶

1§3 $\bar{\kappa}$: a condition number for spherical semialgebraic sets

A spherical semialgebraic set is a semialgebraic subset of the sphere described by homogeneous polynomial. Given $f \in \mathcal{H}_{\mathbf{d}}[q]$ and Φ a Boolean formula over f , the *spherical semialgebraic set* described by (f, Φ) , $S(f, \Phi)$, is given by

$$S(f, \Phi) := \mathbb{S}^n \cap W(f, \Phi) \tag{1.22}$$

where $W(f, \Phi)$ was defined in (0 . 2). Instead of defining a condition number for each description (f, Φ) , we will define a condition number associated only to f . This condition number will be finite when for all Φ , the descriptions (f, Φ) is well-posed. The way to achieve this is to focus on the possible boundary pieces. This motivates the following definition.

Definition 1§3 1. Let $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$. The *local intersection condition number* of f at x , $\bar{\kappa}(f, x)$, is the quantity in $[1, \infty]$ given by

$$\bar{\kappa}(f, x) := \max_{L \in [q]^{\leq n+1}} \kappa(f^L, x) \quad (1 . 23)$$

where $[q]^{\leq n+1} := \{K \subseteq [q] \mid \#K \leq n+1\}$ and $f^L = (f_i)_{i \in L}$, and the *global intersection condition number* of f , $\bar{\kappa}(f)$, the quantity given by

$$\bar{\kappa}(f) := \max_{\substack{L \subseteq [q] \\ \#L \leq n+1}} \kappa(f^L) = \max_{y \in \mathbb{S}^n} \bar{\kappa}(f, y). \quad (1 . 24)$$

The first thing we should notice is the following proposition, which explains the term “intersection” in the name of the above condition number. Recall that an intersection $\bigcap_{i \in I} N_i$ of a family of smooth submanifolds $\{N_i\}_{i \in I}$ of a smooth manifold M is called *transversal in* M if for all $x \in \bigcap_{i \in I} N_i$,

$$\sum_{i \in I} \text{codim}_{T_x M} T_x N_i = \text{codim}_{T_x M} \bigcap_{i \in I} T_x N_i. \quad (1 . 25)$$

Proposition 1§3 1. Let $f \in \mathcal{H}_d[q]$. Then $\bar{\kappa}(f) < \infty$ iff the following conditions hold:

- (1) For all $i \in [q]$, $\mathcal{Z}^S(f_i) := S(f, f_i = 0)$ is regular.
- (2) For all $L \subseteq [q]$, the intersection $\bigcap_{i \in L} \mathcal{Z}^S(f_i)$ is transversal in \mathbb{S}^n . □

Remark 1§3 1. One should observe that in the definition of $\bar{\kappa}$, we limit to subsets $L \subseteq [q]$ of size at most $n+1$. However, this is not the case in Proposition 1§3 1. The reason for this is that for $\#L \geq n+1$, $\bigcap_{i \in L} \mathcal{Z}^S(f_i)$ is transversal in \mathbb{S}^n iff $\bigcap_{i \in L} \mathcal{Z}^S(f_i) = \emptyset$. Therefore when $\#L \geq n+1$, $\bigcap_{i \in L} \mathcal{Z}^S(f_i)$ is transversal in \mathbb{S}^n iff for all $H \subseteq L$ with $\#H = n+1$, $\bigcap_{i \in H} \mathcal{Z}^S(f_i)$ is transversal in \mathbb{S}^n .

We have in this case a theorem even more general than Theorem 1§2 2, which involves not only algebraic sets, but all possible semialgebraic sets that can be constructed from f . The proof will be done in the next chapter, together with the one of Theorem 1§2 2.

Theorem 1§3 2. Let $f \in \mathcal{H}_d[q]$ be such that $\bar{\kappa}(f) < \infty$. Then for all Boolean formula Φ over f and every $g \in B_W(f, \bar{\kappa}(f)^{-1} \min; \|f_i\|_W)$, we have $H_\bullet(S(f, \Phi)) \cong H_\bullet(S(g, \Phi))$.

As with Theorem 1§2 2, we can interpret Theorem 1§3 2 as saying that homology will not change as long as we do not cross the set of ill-posed polynomial tuples. In this case, we have that the set of ill-posed sets is given by

$$\bar{\Sigma}_d[q]_x := \bigcup_{L \in [q]^{\leq n+1}} \bar{\Sigma}_d^L[q]_x \text{ and } \bar{\Sigma}_d[q] := \bigcup_{L \in [q]^{\leq n+1}} \bar{\Sigma}_d^L[q] = \bigcup_{z \in \mathbb{S}^n} \bar{\Sigma}_d[q]_z \quad (1 . 26)$$

where

$$\bar{\Sigma}_{\mathbf{d}}^L[q]_x := \{g \in \mathcal{H}_{\mathbf{d}}[q] \mid g^L(x) = 0, \text{rank } D_x g^L < q\} \text{ and } \bar{\Sigma}_{\mathbf{d}}^L[q] := \bigcup_{z \in \mathbb{S}^n} \bar{\Sigma}_{\mathbf{d}}^L[q]_z. \quad (1.27)$$

Transferring the properties from κ to $\bar{\kappa}$ is straightforward, with the exception of the condition number theorem (Theorem 1^{S2 9} and Corollary 1^{S2 10}) that can only be transferred in a weaker sense.

Proposition 1^{S3 3}. *Let $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $x \in \mathbb{S}^n$. Then:*

- **Regularity inequality:** For all $L \in [q]^{\leq n+1}$, either

$$\frac{\|f^L(x)\|}{\|f^L\|_W} \geq \frac{1}{\sqrt{2}\bar{\kappa}(f, x)} \text{ or } \frac{\sigma_q(\Delta_{\mathbf{d}}^{-1}D_x f^L)}{\|f^L\|_W} \geq \frac{1}{\sqrt{2}\bar{\kappa}(f, x)}.$$

In particular, for all $L \in [q]^{\leq n+1}$, if $\sqrt{2}\bar{\kappa}(f, x) \frac{\|f^L(x)\|}{\|f^L\|_W} < 1$, then $D_x f^L : T_x \mathbb{S}^n \rightarrow \mathbb{R}^L$ is surjective and its pseudoinverse $(D_x f^L)^{\dagger}$ exists.

- **1st Lipschitz property:** The maps

$$\begin{aligned} \mathcal{H}_{\mathbf{d}}[q] &\rightarrow [0, \infty) \\ g &\mapsto \frac{\|g\|_W}{\bar{\kappa}(g, x)} \end{aligned} \quad \text{and} \quad \begin{aligned} \mathcal{H}_{\mathbf{d}}[q] &\rightarrow [0, \infty) \\ g &\mapsto \frac{\|g\|_W}{\bar{\kappa}(g)} \end{aligned}$$

are 1-Lipschitz with respect to the Weyl norm. In particular, $\bar{\kappa}(f, x) \geq 1$ and $\bar{\kappa}(f) \geq 1$.

- **2nd Lipschitz property:** The map

$$\begin{aligned} \mathbb{S}^n &\rightarrow [0, 1] \\ y &\mapsto \frac{1}{\bar{\kappa}(f, y)} \end{aligned}$$

is D-Lipschitz with respect to the geodesic distance on \mathbb{S}^n .

- **Weak condition number theorem:**

$$\bar{\kappa}(f, x) \leq \frac{\|f\|_W}{\text{dist}_W(f, \bar{\Sigma}_{\mathbf{d}}[q]_x)} \text{ and } \bar{\kappa}(f) \leq \frac{\|f\|_W}{\text{dist}_W(f, \bar{\Sigma}_{\mathbf{d}}[q])}$$

where dist_W is the distance induced by the Weyl norm.

Proof. They follow straightforwardly from the properties of κ and the definition of $\bar{\kappa}$. Expanding this out, the regularity inequality follows from Proposition 1^{S2 3}, the 1st Lipschitz property from Proposition 1^{S2 4} and Corollaries 1^{S2 5} and 1^{S2 6}, the 2nd Lipschitz property from Proposition 1^{S2 7}, and the weak condition number theorem from Theorem 1^{S2 9} and Corollary 1^{S2 10}. \square

Proposition 1^{S3 4}. *Let $f \in \mathcal{H}_{\mathbf{d}}[q]$ be such that all its coefficients are integers of absolute value at most H. Then either $\bar{\kappa}(f) = \infty$ or*

$$\bar{\kappa}(f) \leq \sqrt{2DNH} \left(2^{2-\frac{n+1}{2}} D^{n+2} H \sqrt{N}\right)^{2(n+1)(4D)^{2(n+1)}} = O(DHN)^{O(D)^{2(n+1)}}.$$

Proof. We take the maximum of all bounds given by Theorem 1§213 noting $\dim \mathcal{H}_d[q]^L \leq N$. \square

Proposition 1§35. (A) Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a KSS random polynomial tuple. Then for $t \geq (n^2(2q)^{n+1}D^n + 1)(N - 1)$,

$$\mathbb{P}(\bar{\kappa}(\mathfrak{f}) \geq t) \leq 11(n^2(2q)^{n+1}D^n + 1)(N - 1)\frac{1}{t}$$

and

$$\mathbb{E} \log \bar{\kappa}(\mathfrak{f}) \leq \log(N - 1) + n(\log D + 6 \log 2) + (n + 1) \log q + \log(30).$$

(S) Let $f \in \mathcal{H}_d[q]$, $\sigma \in [0, 1]$ and $\mathfrak{f}_\sigma \in \mathcal{H}_d[q]$ a random polynomial tuple uniformly distributed in $B_W(f, \sigma)$. Then for $t \geq (n^2(2q)^{n+1}D^n + 1)(N - 1)\sigma^{-1}$,

$$\mathbb{P}(\bar{\kappa}(\mathfrak{f}_\sigma) \geq t) \leq 11(n^2(2q)^{n+1}D^n + 1)(N - 1)\sigma^{-1}\frac{1}{t}$$

and

$$\mathbb{E} \log \bar{\kappa}(\mathfrak{f}_\sigma) \leq \log(N - 1) + n(\log D + 6 \log 2) + (n + 1) \log q + \log \sigma^{-1} + \log(30).$$

Proof. We apply the union bound for a random variable that is the maximum of several random variables together with Proposition 1§216. We then observe that $\dim \mathcal{H}_d[q]^L \leq N$ and

$$\# [q]^{\leq n+1} = \sum_{k=0}^{n+1} \binom{q}{k} \leq 2nq^{n+1}.$$

\square

Proposition 1§36. (A) Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a KSS random polynomial tuple and $x \in \mathbb{S}^n$. Then for $t \geq 2$,

$$\mathbb{P}(\bar{\kappa}(\mathfrak{f}, x) \geq t) \leq 7nq^{n+1} \left(\frac{119N}{n+1} \right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1}.$$

(S) Let $f \in \mathcal{H}_d[q]$, $\sigma > 0$, $\mathfrak{f}_\sigma := f + \sigma \|f\|_W g$ be a random polynomial tuple such that $g \in \mathcal{H}_d[q]$ is a KSS random polynomial tuple and $x \in \mathbb{S}^n$. Then for $t \geq 2$,

$$\mathbb{P}(\bar{\kappa}(\mathfrak{f}_\sigma, x) \geq t) \leq 7nq^{n+1} \left(\frac{119N}{n+1} \right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1} \left(1 + \frac{1}{\sigma} \right)^{n+1}.$$

Proof. Analogous to the one of Proposition 1§35, but applying Theorem 1§217 this time. \square

1§4 $\bar{\kappa}_{\text{aff}}$: a condition number for affine semialgebraic sets

The traditional way to pass from the affine to the homogenous world is homogenization. The homogenization map

$$\begin{aligned} {}^h : \mathcal{P}_d[q] &\rightarrow \mathcal{H}_d[q] \\ p &\mapsto p^h := \left(p_i(X/X_0) X_0^{d_i} \right)_{i \in [q]}, \end{aligned} \tag{1.28}$$

takes each p_i to its homogenization adding the variable X_0 . This map allows us to transform tuples of affine polynomials into tuples of homogeneous polynomials and so transfer the theory developed for the spherical case to the affine case. In this way, the Weyl norm of $p \in \mathcal{P}_d[q]$ is defined by $\|p\|_W := \|p^h\|_W$ and a KSS random polynomial tuple $p \in \mathcal{P}_d[q]$ is defined as a random polynomial tuple such that $p^h \in \mathcal{H}_d[q]$ is a KSS random polynomial tuple.

Together with the above map, we consider the diffeomorphism

$$\begin{aligned} \text{IO} : \mathbb{R}^n &\rightarrow \mathbb{S}_+^n := \{z \in \mathbb{S}^n \mid z_0 > 0\} \\ x &\mapsto \text{IO}(x) := \frac{1}{\sqrt{1 + \|x\|^2}} \begin{pmatrix} 1 \\ x \end{pmatrix}, \end{aligned} \tag{1.29}$$

which takes the affine space \mathbb{R}^n onto the upper half of \mathbb{S}^n , \mathbb{S}_+^n . Note that the maximal circle $\mathbb{S}_0^n := \{z \in \mathbb{S}^n \mid z_0 = 0\}$ corresponds to the points at infinity of \mathbb{R}^n inside the compactification $\mathbb{S}_+^n \cup \mathbb{S}_0^n$, which differs from the usual compactification \mathbb{P}^n . The main reason to compactify in the sphere is that one can still speak of signs of polynomials in \mathbb{S}^n , while this is not possible, in general, in \mathbb{P}^n .

Given a Boolean formula Φ over p , we can naturally consider the Boolean formula Φ^h over p^h obtained by substituting the p_i in Φ by their corresponding homogenization p_i^h . Now, we need to add to the polynomial tuple p^h and the formula Φ^h a polynomial to encode the sign of X_0 . To do this, we consider the polynomial tuple

$$H(p) := (\|p\|_W X_0, p^h) \tag{1.30}$$

and the Boolean formula

$$H(\Phi) := \Phi^h \wedge (H(p)_0 > 0) \tag{1.31}$$

over it. We can see then that

$$\text{IO}(W(p, \Phi)) := S(H(p), H(\Phi)).$$

The way we choose the scaling for X_0 in $H(f)$ is such that that it has the same weight as p^h .

Following the transfer condition, we expect $p \in \mathcal{P}_d[q]$ to be well-conditioned if $H(p)$ is so. This motivates the following definition.

Definition 1§4.1. Let $p \in \mathcal{P}_d[q]$. The *global affine intersection condition number* of p , $\bar{\kappa}_{\text{aff}}(p)$, is the quantity in $[1, \infty]$ given by

$$\bar{\kappa}_{\text{aff}}(p) := \bar{\kappa}(H(p)). \tag{1.32}$$

We note that for this condition number, the following version of Theorem 1 §3 2 holds. This again can be seen as the justification for calling the above quantity condition number.

Theorem 1 §4 1. *Let $p \in \mathcal{P}_d[q]$ be such that $\bar{\kappa}_{\text{aff}}(p) < \infty$. Then for all Boolean formula Φ over f and every $g \in B_W(p, \bar{\kappa}_{\text{aff}}(p)^{-1} \min_i \|p_i\|_W)$, $H_\bullet(W(p, \Phi)) \cong H_\bullet(W(g, \Phi))$.*

Proof. Since $\min_i \|H(p)_i\|_W = \min_i \|p_i\|_W$ and $\text{dist}_W(H(p), H(g)) \leq \sqrt{2} \text{dist}_W(p, g)$, it follows from Theorem 1 §3 2. \square

Before continuing, let $\mathcal{H}_d^\infty[q]$ be the space of d -homogeneous polynomial q -tuples in the variables X_1, \dots, X_n and consider the orthogonal projection

$$\begin{aligned} h : \mathcal{P}_d[q] &\rightarrow \mathcal{H}_d^\infty[q] \\ p &\mapsto p_h := p^h(0, X_1, \dots, X_n) \end{aligned} \tag{1.33}$$

that maps each p_i to its d_i -homogeneous part $(p_i)_h$, which is the polynomial obtained from p_i by eliminating all terms that are not of degree d_i . The behaviour of p at the hyperplane at infinity S_0^n is precisely captured by the behaviour of p_h at S^{n-1} . The following proposition follows immediately from Proposition 1 §3 1

Proposition 1 §4 2. *Let $p \in \mathcal{P}_d[q]$. Then $\bar{\kappa}_{\text{aff}}(p) < \infty$ iff all the following hold:*

- (1) *For all $i \in [q]$, $Z(p_i) \subseteq \mathbb{R}^n$ and $Z^S((p_i)_h) \subseteq S^{n-1}$ are regular.*
- (2) *For all $L \subseteq [q]$, the intersection $\bigcap_{i \in L} Z(p_i)$ is transversal in \mathbb{R}^n and $\bigcap_{i \in L} Z^S((p_i)_h)$ transversal in S^{n-1} .* \square

Due to the above definition, we can see that the set of ill-posed polynomial tuples $\bar{\Sigma}_d^{\text{aff}}[q] := H^{-1}(\Sigma_d[q]) = \{p \in \mathcal{P}_d[q] \mid \bar{\kappa}_{\text{aff}}(p) = \infty\}$ decomposes as

$$\bar{\Sigma}_d^{\text{aff}}[q] = \bar{\Sigma}_d^{\text{aff}}[q]_+ \cup \bar{\Sigma}_d^{\text{aff}}[q]_0 \tag{1.34}$$

with

$$\bar{\Sigma}_d^{\text{aff}}[q]_+ := \{g \in \mathcal{P}_d[q] \mid g^h \in \bar{\Sigma}_d[q]\} \text{ and } \bar{\Sigma}_d^{\text{aff}}[q]_0 := \{g \in \mathcal{P}_d[q] \mid g_h \in \bar{\Sigma}_d^\infty[q]\} \tag{1.35}$$

where $\bar{\Sigma}_d^\infty[q] := \{g \in \mathcal{H}_d^\infty[q] \mid \bar{\kappa}(g) = \infty\}$. Intuitively, $\bar{\Sigma}_d^{\text{aff}}[q]_+$ are those polynomial tuples for which the ill-posedness comes from a non-transversal intersection and $\bar{\Sigma}_d^{\text{aff}}[q]_0$ those for which the ill-posedness arrives from a tangency to the hyperplane at infinity. We can get the following more quantitative statement.

Theorem 1 §4 3. *Let $p \in \mathcal{P}_d[q]$. Then*

$$\bar{\kappa}_{\text{aff}}(p) \leq \max \left\{ \bar{\kappa}(p^h), (2 + 3D) \max_{L \in [q]^{\leq n+1}} \frac{\|p\|_W \bar{\kappa}(p_h^L)}{\|p_h^L\|_W} \right\} \leq (2 + 3D) \frac{\|p\|_W}{\text{dist}_W(p, \bar{\Sigma}_d^{\text{aff}}[q])}$$

Lemma 1 §4 4. *Let $g \in \mathcal{P}_d[q]$, $\alpha > \|g\|_W$ and $x \in S^n$. Then*

$$\kappa((\alpha x_0, g^h), x) \leq \begin{cases} (2 + 3D) \frac{\alpha \kappa(g_h, \pi_{S_0^n}(x))}{\|g_h\|_W} & \text{if } |x_0| \leq \frac{\sqrt{2}}{2} \\ 2 & \text{if } |x_0| \geq \frac{\sqrt{2}}{2} \end{cases}.$$

In particular, $\kappa(\alpha x_0, g^h) \leq (2 + 3D) \frac{\alpha \kappa(g_h)}{\|g\|_W}$.

Proof of Theorem 1§4.3. We observe that, by the weak condition number theorem for $\bar{\kappa}$ (Proposition 1§3.3),

$$\begin{aligned} & \max \left\{ \bar{\kappa}(p^h), (2 + 3D) \max_{L \in [q]^{n+1}} \frac{\|p\|_W \bar{\kappa}(p_h^L)}{\|p_h^L\|_W} \right\} \\ & \leq (2 + 3D) \max \left\{ \frac{\|p\|_W}{\text{dist}_W(p^h, \bar{\Sigma}_{\mathbf{d}}[q])}, \frac{\|p\|_W}{\text{dist}_W(p_h, \Sigma_{\mathbf{d}}^\infty[q])} \right\} \\ & = (2 + 3D) \max \left\{ \frac{\|p\|_W}{\text{dist}_W(p, \bar{\Sigma}_{\mathbf{d}}^{\text{aff}}[q]_+}), \frac{\|p\|_W}{\text{dist}_W(p, \bar{\Sigma}_{\mathbf{d}}^{\text{aff}}[q]_0)} \right\} \\ & = (2 + 3D) \frac{\|p\|_W}{\text{dist}_W(p, \bar{\Sigma}_{\mathbf{d}}^{\text{aff}}[q])}. \end{aligned}$$

Hence we only have to prove the first inequality. By the definition of $\bar{\kappa}_{\text{aff}}$, we have that

$$\bar{\kappa}_{\text{aff}}(p) = \max_{L \in [q]^{n+1}} \max \left\{ \kappa((p^L)^h), \kappa(\|p\|_W x_0, (p^L)^h) \right\}.$$

Therefore it is enough to show that

$$\kappa(\|p\|_W x_0, (p^L)^h) \leq 4D \frac{\|p\|_W}{\|p_h\|_W} \bar{\kappa}(p_h).$$

Now, this is shown by Lemma 1§4.4 by setting $\alpha = \|p\|_W \geq \|p_h\|_W$ and $g = p^L$, and so the proof concludes. \square

Proof of Lemma 1§4.4. Let $H_\alpha(g) := (\alpha x_0, g^h)$, so that $\|H_\alpha(g)\|_W = \sqrt{\alpha^2 + \|g\|_W^2}$. Since $\|H_\alpha(g)(x)\| \geq \alpha|x_0|$, we have

$$\kappa(H_\alpha(g), x) \leq \sqrt{1 + \frac{\|g\|_W^2}{\alpha^2}} |x_0|^{-1} \leq \sqrt{2} |x_0|^{-1}.$$

This shows the inequality for $|x_0| \geq 1/\sqrt{2}$. We assume now $|x_0| \leq 1/2$, so that $\text{dist}_{\mathbb{S}}(x, \mathbb{S}_0^n) \leq \frac{\pi}{3}|x_0|$. By the 2nd Lipschitz property (Proposition 1§2.7),

$$\kappa(H_\alpha(g), \pi_{\mathbb{S}_0^n}(x)) \geq \frac{\kappa(H_\alpha(g), x)}{1 + \frac{\pi}{3} D \kappa(H_\alpha(g), x) |x_0|}.$$

Now, since $\kappa(H_\alpha(g), x)|x_0| \leq \sqrt{2}$, this gives

$$\kappa(H_\alpha(g), \pi_{\mathbb{S}_0^n}(x)) \geq \frac{\kappa(H_\alpha(g), x)}{1 + \frac{\sqrt{2}\pi}{3} D}.$$

To finish the proof it is enough to show that for $y \in \mathbb{S}_0^n$,

$$\kappa(H_\alpha(g), y) \leq 2 \frac{\alpha}{\|g_h\|_W} \kappa(g, y).$$

Now, $\|H_\alpha(g)\|_W \leq \sqrt{2}\alpha$, so it is enough to show that

$$\sigma_{q+1} \left(\Delta_{\mathbf{d}}^{-1} D_y g^h \right) \geq \frac{1}{\sqrt{2}} \sigma_q(\Delta_{\mathbf{d}}^{-1} D_y g_h).$$

Let $\begin{pmatrix} t & \nu^* \end{pmatrix}$ with $\nu \in \mathbb{R}^q$ and $t^2 + \|\nu\|^2 = 1$ be such that

$$\sigma_{q+1} \left(\begin{pmatrix} \alpha e_0^* \\ \Delta_{\mathbf{d}}^{-1} D_y g^h \end{pmatrix} \right) = \left\| \begin{pmatrix} t & \nu^* \end{pmatrix} \begin{pmatrix} \alpha e_0^* \\ \Delta_{\mathbf{d}}^{-1} D_y g^h \end{pmatrix} \right\|.$$

By an easy computation, we can see that if $|t| \leq 1/\sqrt{2}$,

$$\left\| \begin{pmatrix} t & \nu^* \end{pmatrix} \begin{pmatrix} \alpha e_0^* \\ \Delta_{\mathbf{d}}^{-1} D_y g^h \end{pmatrix} \right\| \geq \frac{1}{\sqrt{2}} \sigma_q(\Delta_{\mathbf{d}}^{-1} D_y g^h),$$

and if $|t| \geq 1/\sqrt{2}$,

$$\begin{aligned} \left\| \begin{pmatrix} t & \nu^* \end{pmatrix} \begin{pmatrix} \alpha e_0^* \\ \Delta_{\mathbf{d}}^{-1} D_y g^h \end{pmatrix} \right\| &\geq \sqrt{\alpha^2 \left(|t| - \sqrt{1-t^2} \right)^2 + (1-t^2) \sigma_q(\Delta_{\mathbf{d}}^{-1} D_y g^h)^2} \\ &\geq \frac{1}{\sqrt{2}} \sigma_q(\Delta_{\mathbf{d}}^{-1} D_y g^h), \end{aligned}$$

where the inequality follows from direct minimization and the fact that $\alpha \geq \sigma_q(\Delta_{\mathbf{d}}^{-1} D_y g^h)$, which follows from $\alpha \geq \|g\|_W$ and Corollary 1 §1.7. \square

Remark 1 §4.1. We observe that the last inequality in Theorem 1 §4.3 is precisely [88; Proposition 4.16] when $D \geq 2$. However, we note that our proof is different from the one given in [88], which, in principle, could be extended to more general conic condition numbers. ¶

Motivated by Theorem 1 §4.3, let us define

$$\bar{\kappa}_{\text{aff}}^\infty(p, x) := \max_{L \in [q]^{\leq n+1}} \frac{\|p\|_W \bar{\kappa}(p_h^L, x)}{\|p_h^L\|_W} \quad (1.36)$$

for $p \in \mathcal{P}_{\mathbf{d}}[q]$ and $x \in \mathbb{S}_0^n$, and $\bar{\kappa}_{\text{aff}}^\infty(p) := \max_{y \in \mathbb{S}_0^n} \bar{\kappa}_{\text{aff}}^\infty(p, y)$. With the above result, we can perform the usual complexity analyses as shown above for $\bar{\kappa}$. We only sketch the proofs as they are identical to the ones for κ and $\bar{\kappa}$.

Corollary 1 §4.5. Let $p \in \mathcal{P}_{\mathbf{d}}[q]$ be such that all its coefficients are integers of absolute value at most H . Then either $\bar{\kappa}_{\text{aff}}(p) = \infty$ or

$$\bar{\kappa}_{\text{aff}}(p) \leq \sqrt{2D} NH \left(2^{2-\frac{n+1}{2}} D^{n+2} H \sqrt{N} \right)^{2(n+1)(4D)^{2(n+1)}} = O(DHN)^{O(D)^{2(n+1)}}.$$

Sketch of proof. By Theorem 1 §4.3, we just need to bound for $\bar{\kappa}(p^h)$ and $\bar{\kappa}_{\text{aff}}^\infty(p)$. For the first, we apply Proposition 1 §3.4. For the latter, we proceed as in the proofs of Theorem 1 §2.13 and Proposition 1 §3.4. The bound obtained for $\bar{\kappa}_{\text{aff}}^\infty(p)$ will be like the one above, but with $n-1$ in the place of n . This makes that multiplying by $(2+3D)$ does not affect the final bound that we obtain. \square

Corollary 1 §4.6. (A) Let $\mathfrak{p} \in \mathcal{P}_{\mathbf{d}}[q]$ be a KSS random polynomial tuple. Then for $t \geq (n^2(2(q+1))^{n+1}D^n + 1)(N-1)$,

$$\mathbb{P}(\bar{\kappa}_{\text{aff}}(\mathfrak{p}) \geq t) \leq 55D(n^2(2(q+1))^{n+1}D^n + 1)(N-1) \frac{1}{t}$$

and

$$\mathbb{E} \log \bar{\kappa}_{\text{aff}}(\mathfrak{p}) \leq \log(N-1) + (n+1)(\log D + 9 \log 2) + (n+1) \log(q+1) + \log(30).$$

(S) Let $p \in \mathcal{P}_d[q]$, $\sigma \in [0, 1]$ and $p_\sigma \in \mathcal{P}_d[q]$ a random polynomial tuple uniformly distributed in $B_W(p, \sigma)$. Then for $t \geq (n^2(2(q+1))^{n+1}D^n + 1)(N-1)\sigma^{-1}$,

$$\mathbb{P}(\bar{\kappa}_{\text{aff}}(p_\sigma) \geq t) \leq 55D(n^2(2(q+1))^{n+1}D^n + 1)(N-1)\sigma^{-1} \frac{1}{t}$$

and

$$\mathbb{E} \log \bar{\kappa}_{\text{aff}}(p_\sigma) \leq \log(N-1) + (n+1)(\log D + \log(q+1) + 9\log 2) + \log \sigma^{-1} + \log(30).$$

Sketch of proof. By Theorem 1§43, we have to obtain tail bounds for $\bar{\kappa}(p^h)$ and $\bar{\kappa}_{\text{aff}}^\infty(p)$. For the first, we apply Proposition 1§35. For the latter, we proceed like in the proof of Proposition 1§35 after noting that $\bar{\kappa}_{\text{aff}}^\infty(p) \leq \|p\|_W / \text{dist}_W(\bar{\Sigma}_d^{\text{aff}}[q]_0)$. We use a union bound to reduce from the case of $\bar{\Sigma}_d^{\text{aff}}[q]_0$ to the case of $\{p \in \mathcal{H}_d[q] \mid p^L \in \bar{\Sigma}_d^{\infty, L}[q]\}$. Then we use that $p \mapsto p_h$ is an orthogonal projection to apply the degree bound in Proposition 1§215 to the latter sets. Finally, we use Theorem 1§214. \square

The following probabilistic bound will be useful later.

Corollary 1§47. (A) Let $p \in \mathcal{P}_d[q]$ be a KSS random polynomial tuple and $x \in \mathbb{S}_0^n$. Then for $t \geq 2$,

$$\mathbb{P}(\bar{\kappa}_{\text{aff}}^\infty(p, x) \geq t) \leq 7nq^{n+1} \left(\frac{119N}{n} \right)^{\frac{n}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^n.$$

(S) Let $p \in \mathcal{P}_d[q]$, $\sigma > 0$, $p_\sigma := p + \sigma\|p\|_W g$ be a random polynomial tuple such that $g \in \mathcal{H}_d[q]$ is a KSS random polynomial tuple and $x \in \mathbb{S}_0^n$. Then for $t \geq 2$,

$$\mathbb{P}(\bar{\kappa}_{\text{aff}}^\infty(p_\sigma, x) \geq t) \leq 7nq^n \left(\frac{119N}{n} \right)^{\frac{n}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^n \left(1 + \frac{1}{\sigma} \right)^n.$$

Sketch of proof. To handle

$$\frac{\|p\|_W}{\sqrt{\|p_h^L(x)\|^2 + \sigma_q(\Delta_d^{-1}D_x p_h^L)^2}},$$

we separate numerator and denominator as in the proof of Theorem 1§217. Then the rest is the same, except that we have just n variables now, instead of $n+1$. To handle the maximum, we just apply the union bound as in the proof of Proposition 1§36. \square

Further comments

Many of the results in this chapter can be found in [87] and [88, 91]. However, there are some important additions: the gap theorem (Theorem 1§213, Proposition 1§34 and Corollary 1§45) for integer polynomial tuples, the tail bounds coming from geometric functional analysis (Theorems 1§217 and 1§219, Proposition 1§36 and Corollary 1§47), and the inequality of Theorem 1§43.

In addition to the new results, our presentation differs from those in [87] and [88, 91]. On the one hand, our definition of κ is with the q th singular value, instead of the μ -condition

or the operator norm. This change leads to a clearer form of κ which is easier to parse. We introduce μ afterwards, but only after familiarity with κ has been attained. On the other hand, our focus goes away from the condition number theorem, and more into the properties and possibles bounds of κ . Even though, this means that we acknowledge the beauty of a condition number theorem and the geometric interpretation it gives κ . We don't view this as the center of the theory, since from an algorithmic point of view the other properties are more important than a 'fancy' geometric interpretation. This should be viewed as a break with the philosophy of [87].

It remains an important exercise to develop the above theory in the multihomogeneous setting, meaning that $\kappa(f, x)$ and $\kappa(f)$ should be invariant under the scaling of each polynomial f_i in f . This development would lead to a more robust $\bar{\kappa}$. The reason for this is that semialgebraic sets are defined with atoms involving only one atom at a time.

We note that our approach to condition numbers follows the philosophy of the worst variation. It would be interesting to study weak variations, where we consider the high-probability-variation, following the notion of weak condition number introduced by Lotz and Noferini [282].

There are no dogmas to which we must conform. Our program is simple: to give numerical meaning to as much as possible of classical abstract analysis.

Errett Bishop, Foundations of Constructive Analysis

2

Differential semialgebraic geometry with condition-based inequalities

In semialgebraic geometry, it is usual to have results depending on “weak” inequalities. These inequalities are of the form “for sufficiently small a ” or “for x sufficiently smaller than y ”. Unfortunately, from an applied and computational viewpoint, these statements can be useless, because they don’t give explicit bounds that can be used to obtain numbers satisfying the desired statements. In the symbolic world, one can solve the issue by adding infinitesimals; in the numerical world, we don’t have the luxury of using infinitesimals. Thus we need to make the “weak” inequalities explicit and find explicit values for them.

In this chapter, we will substitute such weak inequalities by strong inequalities depending on the condition number in the case of two theorems: Durfee’s theorem (Theorem 2§3 2) and Gabrielov-Vorobjov approximation theorem (Theorem 2§4 2). Or, paraphrasing Bishop [Q4], we will give “numerical meaning” to these inequalities in the well-posed case. The first result will be fundamental for our constructions of simplicial complexes, and the second one for passing from the arbitrary case to the closed case.

First, we recall Newton’s vector field and use a discontinuous version of it to prove a converse of the Exclusion Lemma (Corollary 1§1 8); second, we present the Thom-Mather theory that will play a fundamental role in this thesis; third, we introduce our main technical tool, (f, λ) -lartitions and (f, λ) -partitions; and four and last, we prove, respectively, Durfee’s and Gabrielov-Vorobjov approximation theorem.

2§1 A converse to the Exclusion Lemma

Given any smooth map $f : \mathbb{S}^n \rightarrow \mathbb{R}^q$, we consider the open set $\Omega_f := \{x \in \mathbb{S}^n \mid D_x f \text{ is surjective}\}$ and, on it, the *Newton vector field* of f as the vector field given by

$$N_x^f := -D_x f^\dagger f(x). \quad (2.1)$$

The main property of this vector field is that for any integral path $t \mapsto z_t$,

$$f(z_t) = f(z_0)e^{-t}. \quad (2.2)$$

This property follows from the chain rule and the properties of the pseudoinverse.

Recall that $B_{\mathbb{S}}$ and $\bar{B}_{\mathbb{S}}$ denote, respectively, the open and closed balls in \mathbb{S}^n with respect the geodesic distance and that, for $r > 0$, the *spherical r-neighborhood* of $X \subset \mathbb{S}^n$ is the set

$$\mathcal{U}_{\mathbb{S}}(X, r) := \{p \in \mathbb{S}^n \mid d_{\mathbb{S}}(p, X) \leq r\} = \bigcup_{x \in X} \bar{B}_{\mathbb{S}}(x, r). \quad (2.3)$$

For $f \in \mathcal{H}_d[q]$, the *algebraic neighborhood* of $\mathcal{Z}^{\mathbb{S}}(f)$ with tolerance r is the set

$$\mathcal{Z}_r^{\mathbb{S}}(f) := \{x \in \mathbb{S}^n \mid \|f(x)\| \leq r\|f\|_W\}. \quad (2.4)$$

The following theorem is a two-way version of the Exclusion Lemma (Corollary 1^{\$1}8) for algebraic sets.

Proposition 2^{\$1}1. *Let $f \in \mathcal{H}_d[q]$ and $r > 0$ be such that $\sqrt{2}\kappa(f)r < 1$. Then*

- (a) $\mathcal{Z}^{\mathbb{S}}(f) \subseteq \mathcal{Z}_r^{\mathbb{S}}(f)$,
- (b) $\mathcal{U}_{\mathbb{S}}(\mathcal{Z}^{\mathbb{S}}(f), r) \subseteq \mathcal{Z}_{D^{1/2}f}^{\mathbb{S}}(f)$, and
- (c) $\mathcal{Z}_r^{\mathbb{S}}(f) \subseteq \mathcal{U}_{\mathbb{S}}\left(\mathcal{Z}^{\mathbb{S}}(f), \sqrt{2}\kappa(f)r\right)$.

Proof. (a) is obvious and (b) is just a reformulation of the Exclusion Lemma (Corollary 1^{\$1}8).

(c). Take $x \in \mathcal{Z}_r^{\mathbb{S}}(f)$ and consider the integral path $t \mapsto x_t$ of the Newton vector field of f starting at x . Since $\sqrt{2}\kappa(f)r < 1$, we have that $\mathcal{Z}_r^{\mathbb{S}}(f) \subseteq \Omega_f$, by Proposition 1^{\$2}3, and so the Newton vector field is defined at every point of $\mathcal{Z}_r^{\mathbb{S}}(f)$. By (2.2), $t \mapsto x_t$ does not leave $\mathcal{Z}_r^{\mathbb{S}}(f)$ and so it can be extended indefinitely obtaining a global integral path $[0, \infty) \ni t \mapsto x_t$.

We have that

$$\|\dot{x}_t\| \leq \|D_{x_t}f^\dagger\| \|f(x_t)\| = \|D_{x_t}f^\dagger\| \|f(x)\| e^{-t} = \frac{\|f\|_W}{\sigma_q(D_{x_t}f)} \frac{\|f(x)\|}{\|f\|_W} e^{-t} \leq \sqrt{2}\kappa(f)r e^{-t},$$

where the first inequality follows from $\dot{x}_t = -D_{x_t}f^\dagger f(x_t)$, which follows from (2.1); the first equality from (2.2), the second equality from the form of the singular values of the pseudoinverse, and the second inequality from Proposition 1^{\$2}3. Therefore

$$\int_0^\infty \|\dot{x}_t\| dt < \sqrt{2}\kappa(f)r$$

and so x_t converges absolutely and $\lim_{t \rightarrow \infty} x_t$ exists. By (2.2), this limit belongs to $\mathcal{Z}^{\mathbb{S}}(f)$. We have thus shown that starting from x we can reach a point of $\mathcal{Z}^{\mathbb{S}}(f)$ following a path in \mathbb{S}^n of length less than $\sqrt{2}\kappa(f)r$. Hence $\text{dist}_{\mathbb{S}}(x, \mathcal{Z}^{\mathbb{S}}(f)) \leq \sqrt{2}\kappa(f)r$ and the claim follows. \square

In the semialgebraic case, we can prove an analog of Proposition 2^{\$1}1 using a discontinuous generalization of the Newton vector field.

2^{§1–1} Boolean formulas over (f, t) and algebraic neighborhoods

We introduce several geometric notions that will be central later on. First, we extend our universe of considered functions from homogeneous polynomials to homogeneous polynomial with constants added. The reason for this is that these polynomials appear in the Gabrielov-Vorobjov construction (see 2^{§4}) and so the theory has to be extended to include them.

Definition 2^{§1}1. Let $f \in \mathcal{H}_d[q]$ and $t \in \mathbb{R}^e$, a *Boolean formula over (f, t)* is a Boolean formula Φ supported on

$$\begin{aligned} & \{(f_i = \|f_i\|_W t_j), (f_i \neq \|f_i\|_W t_j), \\ & (f_i > \|f_i\|_W t_j), (f_i \geq \|f_i\|_W t_j), (f_i < \|f_i\|_W t_j), (f_i \leq \|f_i\|_W t_j) \mid i \in [q], j \in [e]\}. \end{aligned}$$

Given a Boolean formula Φ over (f, t) , the *realization* of (f, t, Φ) , $S(f, t, \Phi)$, is the semialgebraic set

$$S(f, t, \Phi) := \Phi_{\mathbb{S}^n} \left(\hat{f}_i^{-1}(t_j), \hat{f}_i^{-1}(\mathbb{R} \setminus t_j), \right. \\ \left. \hat{f}_i^{-1}(t_j, \infty), \hat{f}_i^{-1}[t_j, \infty), \hat{f}_i^{-1}(-\infty, t_j), \hat{f}_i^{-1}(-\infty, t_j] \mid i \in [q], j \in [e] \right) \quad (2.5)$$

where $\hat{f} = (f_i / \|f_i\|_W)_{i \in [q]}$ and the subscript in $\Phi_{\mathbb{S}^n}$ indicates that we evaluate subsets of the sphere. In other words, $S(f, t, \Phi)$ is the spherical semialgebraic set obtained interpreting (f, t, Φ) in the obvious way.

Remark 2^{§1}1. In the above definition, $t \in \mathbb{R}^e$ gives us the constants that we can modify our original polynomial tuple with. ¶

Now, we introduce some notions for formulas and we define algebraic neighborhoods for closed semialgebraic sets.

Definition 2^{§1}2. Let $f \in \mathcal{H}_d[q]$ and $t \in \mathbb{R}^e$. Then:

- (m) a *monotone formula* over (f, t) is a Boolean formula over (f, t) that contains no negations.
- (l) a *lax formula* over (f, t) is a monotone formula over (f, t) whose atoms are of the form $(f_i = \|f_i\|_W t_j)$, $(f_i \geq \|f_i\|_W t_j)$ and $(f_i \leq \|f_i\|_W t_j)$.
- (pc) a *purely conjunctive formula* over (f, t) is a monotone formula over (f, t) that does not contain disjunctions, i.e., it is a formula of the form $\bigwedge_{i \in I} (f_{a_i} \propto_i \|f_{a_i}\|_W t_{b_i})$ where $a \in [q]^I$, $b \in [e]^I$ and $\propto \in \{=, \neq, >, \geq, <, \leq\}^I$.

Definition 2^{§1}3. Let $f \in \mathcal{H}_d[q]$, $t \in \mathbb{R}^e$, $r > 0$ and ϕ be a lax formula over (f, t) . The *algebraic neighborhood of $S(f, t, \phi)$ with tolerance r* , $S_r(f, t, \phi)$, is the spherical semialgebraic set given by

$$S_r(f, t, \Phi) := \Phi_{\mathbb{S}^n} \left(\hat{f}_i^{-1}[t_j - r, t_j + r], \hat{f}_i^{-1}[t_j - r, \infty), \hat{f}_i^{-1}(-\infty, t_j + r] \mid i \in [q], j \in [e] \right). \quad (2.6)$$

In other words, $S_r(f, t, \Phi)$ is the spherical semialgebraic set obtained by substituting in Φ the atoms $(f_i = \|f_i\|_W t_j)$ by $(f_i \leq \|f_i\|_W(t_j + r)) \wedge (f_i \geq \|f_i\|_W(t_j - r))$, the atoms $(f_i \geq \|f_i\|_W t_j)$ by $(f_i \geq \|f_i\|_W(t_j - r))$ and the atoms $(f_i \leq \|f_i\|_W t_j)$ by $(f_i \leq \|f_i\|_W(t_j + r))$ and interpreting the obtained formula in the obvious way.

To control the well-posedness of (f, t) , we have to consider the *separation*, $\Delta(t)$, of $t \in \mathbb{R}^e$ given by

$$\Delta(t) := \inf_{i \neq j} |t_i - t_j| \quad (2.7)$$

in addition to the condition number $\bar{\kappa}$. This parameter allows us to control that certain intersections, such as $S(f, t, (f_i \geq \|f_i\|_W t_j) \wedge (f_i \leq \|f_i\|_W t_k))$, with $t_j > t_k$, remains empty when passing to algebraic neighborhoods with sufficiently small tolerance. The following technical proposition makes this clear.

Proposition 2^{§1} 2. *Let $f \in \mathcal{H}_d[q]$, $t \in \mathbb{R}^e$ and $r > 0$ be such such that $\Delta(t) > 2r$. Then:*

1. *For every purely conjunctive lax formula ϕ over (f, t) , there exist a purely conjunctive lax formula $\text{NF}(\phi)$, called normal form of ϕ , of the form*

$$\begin{aligned} \text{NF}(\phi) \equiv \bigwedge_{n \in \mathcal{N}_+} (f_n \geq t_{\alpha(n)} \|f_n\|_W) \wedge \bigwedge_{n \in \mathcal{N}_-} (f_n \leq t_{\alpha(n)} \|f_n\|_W) \\ \wedge \bigwedge_{n \in \mathcal{N}_0} ((f_n \geq t_{lb(n)} \|f_n\|_W) \wedge (f_n \leq t_{ub(n)} \|f_n\|_W)) \end{aligned}$$

with $\mathcal{N}_+, \mathcal{N}_-, \mathcal{N}_0 \subseteq [q]$ pairwise disjoint, $\alpha : \mathcal{N}_+ \cup \mathcal{N}_- \rightarrow [e]$ and $lb, ub : \mathcal{N}_0 \rightarrow [e]$ such that for all $n \in \mathcal{N}_0$, $t_{lb(n)} \leq t_{ub(n)}$, and such that

$$S(f, t, \phi) = S(f, t, \text{NF}(\phi)) \text{ and } S_r(f, t, \phi) = S_r(f, t, \text{NF}(\phi)).$$

2. *For every lax formula Φ over (f, t) , there exist a lax formula $\text{DNF}(\Phi)$, called disjunctive normal form of Φ , of the form*

$$\text{DNF}(\Phi) \equiv \bigvee_{\xi \in \Xi} \phi_\xi$$

with ϕ_ξ purely conjunctive and lax in normal form, and such that

$$S(f, t, \Phi) = S(f, t, \text{DNF}(\Phi)) \text{ and } S_r(f, t, \Phi) = S_r(f, t, \text{DNF}(\Phi)).$$

Proof. 1. Since \wedge is commutative, in the sense that permuting atoms do not affect the realization, we can just focus in the case

$$\bigwedge_{k \in K} (f_i \propto_k t_{a(k)} \|f_i\|_W)$$

with $a : K \rightarrow [e]$ and $\propto \in \{\geq, \leq, =\}^K$, which is obtained when gathering all atoms in which a particular f_i appears. Further, by splitting atoms of the form $(f_i = t_{a(k)} \|f_i\|_W)$ into $(f_i \leq t_{a(k)} \|f_i\|_W) \wedge (f_i \geq t_{a(k)} \|f_i\|_W)$, which again does not change the realization at all, we can assume that $\propto \in \{\leq, \geq\}^K$.

Now, we observe that substituting, respectively,

$$\bigwedge_{\substack{k \in K \\ \alpha_k \text{ is } \leq}} (f_i \leq t_{a(k)} \|f_i\|_W) \text{ by } \left(f_i \leq \left(\min_{\substack{k \in K \\ \alpha_k \text{ is } \leq}} t_{a(k)} \right) \|f_i\|_W \right)$$

and

$$\bigwedge_{\substack{k \in K \\ \alpha_k \text{ is } \geq}} (f_i \geq t_{a(k)} \|f_i\|_W) \text{ by } \left(f_i \geq \left(\max_{\substack{k \in K \\ \alpha_k \text{ is } \geq}} t_{a(k)} \right) \|f_i\|_W \right)$$

does not change the realization. Hence we have substituted our initial factor by a factor of the form $(f_i \leq t_{\alpha(i)} \|f_i\|_W)$, $(f_i \geq t_{\alpha(i)} \|f_i\|_W)$ or $((f_i \geq t_{lb(i)} \|f_i\|_W) \wedge (f_i \leq t_{ub(i)} \|f_i\|_W))$. In the first two cases, there is nothing to prove. In the last case, if $t_{lb(j)} > t_{ub(j)}$, then both $S(f, t, \Phi)$ and $S_r(f, t, \Phi)$ are empty, since $\mathbb{W}(t) > 2r$, and we can just take $NF(\phi)$ to be the empty formula. The claim is proven.

2. Using that \wedge is distributive with respect \vee , in the sense that passing from $\Phi_0 \wedge (\Phi_1 \vee \Phi_2)$ to $(\Phi_0 \wedge \Phi_1) \vee (\Phi_0 \wedge \Phi_2)$ does not affect the realization, we can transform Φ into a formula of the form

$$\bigvee_{\xi \in \Xi} \phi_\xi$$

with ϕ_ξ purely conjunctive and such that

$$S(f, t, \Phi) = S\left(f, t, \bigvee_{\xi \in \Xi} \phi_\xi\right) \text{ and } S_r(f, t, \Phi) = S_r\left(f, t, \bigvee_{\xi \in \Xi} \phi_\xi\right).$$

Applying (1) to each ϕ_ξ finishes the proof. \square

Remark 2^{S1}2. We observe that Proposition 2^{S1}2 does not necessarily give efficient algorithms. For example, DNF(Φ) can have size exponential in the size of Φ as one can see by slightly modifying Example 0^{S1}3. ¶

2^{S1}-2 Discontinuous Newton vector field

We can now state and prove the semialgebraic version of Proposition 2^{S1}1.

Proposition 2^{S1}3. Let $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$ and $r > 0$ be such that $\sqrt{2} \bar{\kappa}(f)(r + T) < 1$ and $\mathbb{W}(t) > 2r$. Then, for every lax formula Φ over (f, t) ,

- (a) $S(f, t, \Phi) \subseteq S_r(f, t, \Phi)$,
- (b) $\mathcal{U}_S(S(f, t, \Phi), r) \subseteq S_{D^{1/2}r}(f, t, \Phi)$, and
- (c) $S_r(f, t, \Phi) \subseteq \mathcal{U}_S(S(f, t, \Phi), \sqrt{2} \bar{\kappa}(f)r)$.

We observe that (a) is trivial and that (b) follows immediately from the Exclusion Lemma (Corollary 1^{S1}8). Therefore we will focus on (c). By Proposition 2^{S1}2, we see that it is enough

to prove the above proposition for a purely conjunctive lax formula ϕ in normal form, which has the form

$$\begin{aligned} \phi \equiv \bigwedge_{\nu \in \mathcal{N}_+} (f_\nu \geq t_{\alpha(\nu)} \|f_\nu\|_W) \wedge \bigwedge_{\nu \in \mathcal{N}_-} (f_\nu \leq t_{\alpha(\nu)} \|f_\nu\|_W) \\ \wedge \bigwedge_{\nu \in \mathcal{N}_0} ((f_\nu \geq t_{lb(\nu)} \|f_\nu\|_W) \wedge (f_\nu \leq t_{ub(\nu)} \|f_\nu\|_W)) \end{aligned}$$

with $\mathcal{N}_+, \mathcal{N}_-, \mathcal{N}_0 \subseteq [q]$ pairwise disjoint, $\alpha : \mathcal{N}_+ \cup \mathcal{N}_- \rightarrow [\mathbf{e}]$ and $lb, ub : \mathcal{N}_0 \rightarrow [\mathbf{e}]$ such that for all $\nu \in \mathcal{N}_0$, $t_{lb(\nu)} \leq t_{ub(\nu)}$. We know define the following set-valued maps

$$\begin{aligned} \mathbb{S}^n \ni x \mapsto L_+(x) &:= \{\nu \in \mathcal{N}_+ \mid f_\nu(x) \leq t_{\alpha(\nu)} \|f_\nu\|_W\}, \\ \mathbb{S}^n \ni x \mapsto L_-(x) &:= \{\nu \in \mathcal{N}_- \mid f_\nu(x) \geq t_{\alpha(\nu)} \|f_\nu\|_W\}, \\ \mathbb{S}^n \ni x \mapsto L_{lb}(x) &:= \{\nu \in \mathcal{N}_0 \mid f_\nu(x) \leq t_{lb(\nu)} \|f_\nu\|_W\}, \text{ and} \\ \mathbb{S}^n \ni x \mapsto L_{ub}(x) &:= \{\nu \in \mathcal{N}_0 \mid f_\nu(x) \geq t_{ub(\nu)} \|f_\nu\|_W\}. \end{aligned}$$

For each $x \in \mathbb{S}^n$, $L_+(x)$, $L_-(x)$, $L_{lb}(x)$ and $L_{ub}(x)$ are pairwise disjoint and each of these sets encodes the clauses of ϕ that x does not satisfy or could stop satisfying after a small perturbation.

Consider also the maps $\mathbb{S}^n \ni x \mapsto L(x) := L_-(x) \cup L_+(x) \cup L_{lb}(x) \cup L_{ub}(x)$ and $\mathbb{S}^n \ni x \mapsto \tau(x) \in \mathbb{R}^{L(x)}$ given by

$$\tau_I(x) := \begin{cases} t_{\alpha(I)} \|f_I\|_W, & \text{if } I \in L_+(x) \cup L_-(x) \\ t_{lb(I)} \|f_I\|_W, & \text{if } I \in L_{lb}(x) \\ t_{ub(I)} \|f_I\|_W, & \text{if } I \in L_{ub}(x) \end{cases}.$$

With the help of these maps, we define the *discontinuous Newton vector field* of (f, t, ϕ)

$$N_x^{f,t,\phi} := - \left(D_x f^{L(x)} \right)^\dagger (f^{L(x)}(x) - \tau(x)) \quad (2.8)$$

where $D_x f^{L(x)} = (D_x f_i)_{i \in L(x)}$ selects the rows in $D_x f^{L(x)}$ indexed by $L(x)$. In general, this vector field is not continuous, but its solutions are well-behaved. With this vector field, we can prove Proposition 2^{§1}3.

Lemma 2^{§1}4. (i) Given $x_0 \in S_r(f, t, \phi)$, the integral path $[0, T] \ni t \mapsto x_t$ of the Newton vector field of $f^{L(x_0)} - \tau(x_0)$, $N^{(f^{L(x_0)} - \tau(x_0))}$, starting at x_0 , agrees locally with the integral path of the discontinuous Newton vector field of (f, t, ϕ) , $N^{f,t,\phi}$, starting at x_0 .

- (ii) Let $[0, T] \ni t \mapsto x_t$ be an integral path of $N^{f,t,\phi}$ and $t, t' \in [0, T]$. If $t' > t$, then $L_+(x_{t'}) \supseteq L_+(x_t)$, $L_-(x_{t'}) \supseteq L_-(x_t)$, $L_{lb}(x_{t'}) \supseteq L_{lb}(x_t)$ and $L_{ub}(x_{t'}) \supseteq L_{ub}(x_t)$.
- (iii) Given $x_0 \in S_r(f, t, \phi)$, there is a forward-time integral path of the discontinuous Newton vector field $N^{f,t,\phi}$ of (f, t, ϕ) starting at x_0 that extends indefinitely, i.e., for any time.

Remark 2^{§1}3. Although we could prove uniqueness of time-forward integral paths in Lemma 2^{§1}4, we don't provide such a proof. The main reason for this is that such a uniqueness result is not needed. ¶

Proof of Proposition 2^{§1}3(c). We restrict to the case of a formula ϕ as described above, since it is enough to consider this case.

Let $x \in S_r(f, t, \phi)$. By Lemma 2^{§1}4, we can consider the integral path of $t \mapsto x_t$ starting at this point that extends indefinitely. Further, for all $t > 0$, we have that

$$f_I(x_t) = \begin{cases} \tau_I(x_0) + (f_I(x_0) - \tau_I(x_0))e^{-t} & \text{if } I \in L(x_0) \\ \tau_I(x_t) & \text{if } I \in L(x_t) \setminus L(x_0) \end{cases} \quad (2.9)$$

since, if $I \in L(x_0)$, this follows from the formula for $N^{f,t,\phi}$, and, if not, then when we add I , this holds because $f_I(x_t) = \tau_I(x)$, and so no variation occurs. Because of (2.9), the integral path remains in $S_r(f, t, \phi)$. Arguing as in the proof of Proposition 2^{§1}1, we can see that, by the regularity inequality (Proposition 1^{§3}3),

$$\|\dot{x}_t\| \leq \sqrt{2}\bar{\kappa}(f)r e^{-t}.$$

Therefore

$$\int_0^\infty \|\dot{x}_t\| dt \leq \sqrt{2}\bar{\kappa}(f)r$$

and so the limit $\lim_{t \rightarrow \infty} x_t$ exists and belongs to $S(f, \Phi)$, by (2.9). Now, such a path lies on \mathbb{S}^n and has length at most $\sqrt{2}\bar{\kappa}(f)r$. Hence the claim follows. \square

Proof of Lemma 2^{§1}4. (i). For the considered integral path, we can check that for t sufficiently small, $L(x_t) = L(x_0)$. Indeed, for $I \in L(x_0)$,

$$f_I(x_t) = \tau_I(x_0) + (f_I(x_0) - \tau_I(x_0))e^{-t}$$

and so $I \in L(x_t)$ for $t > 0$, since the inequalities defining $L(x_0)$ will still hold. And for $I \in [q] \setminus L(x_0)$, we have strict inequalities, and so, by continuity, $I \in [q] \setminus L(x_t)$ for t sufficiently small. Hence, along the integral path $t \mapsto x_t$, $N_{x_t}^{f,t,\phi} = N_{x_t}^{f^{L(x_0)} - \tau(x_0)}$ for sufficiently small t . Thus the claim follows.

(ii). We prove the claim only for L_+ , since for the rest the proof is analogous. By (i) and the formula for $f_I(x_t)$ above, we can see that $f_I(x_{s'}) - \tau_I(x_{s'}) = (f_I(x_s) - \tau_I(x_s))e^{s' - s}$ for any $s, s' \in [t, t']$ with $s' > s$ sufficiently near to s and $I \in L(x_s)$. This means that

$$\{s \in [t, t'] \mid \text{for all } s' \in [0, s], L_+(x_{s'}) \supseteq L_+(x_t)\}$$

is open. Since the defining conditions of $L_+(x)$ are closed, it is also closed. Thus it agrees with $[t, t']$ and the claim follows for L_+ .

(iii). By the regularity inequality (Proposition 1^{§3}3) and (i), we can guarantee that a local time-forward integral path starting at x_0 exists and that it does not leave $S_r(f, t, \phi)$. By (ii), we only have to paste finitely many integral paths of the Newton vector field of $f^{L(x_{t_0})} - \tau(x_{t_0})$. Hence we can extend the integral path indefinitely, as desired. \square

One may think that the proof above can be adapted to obtain a continuous retraction of $S_r(f, t, \phi)$ onto $S(f, t, \phi)$ when ϕ is a purely conjunctive lax formula, so that one proves Durfee's theorem (Theorem 2^{§3}2). However, as shown in Example 2^{§1}1 below, the flow of the discontinuous Newton vector field is not continuous in general. This phenomenon motivates the introduction of Mather-Thom theory to be able to work with vector fields better suited for the semialgebraic setting.

Example 2^{§1}1. We consider a pointed cone C (for simplicity, in \mathbb{R}^2) given as $\ell_1 \geq 0 \wedge \ell_2 \geq 0$ where ℓ_1, ℓ_2 are linear functions. In this case, the Newton vector field (over either $\ell_1 = 0$, $\ell_2 = 0$, or $\ell_1 = \ell_2 = 0$) is just the orthogonal projection and the discontinuous Newton field is the orthogonal projection onto the correspondent pieces of the boundary. Figure 2^{§1}1 shows two such situations for cones with different openings. For $S \subset \{1, 2\}$ the region R_S in the figure is the set $\{x \mid L(x) = S\}$.

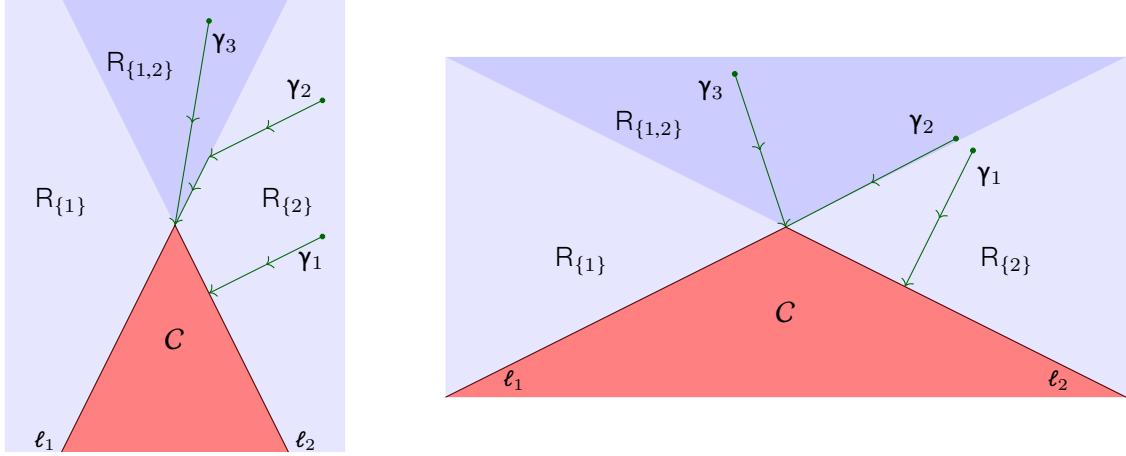


Figure 2^{§1}1: Discontinuous Newton vector field for a convex cone

We observe that in the left-hand drawing the flow of the discontinuous Newton vector field is continuous, while in the right-hand drawing it is not (as illustrated by the integral paths γ_1 and γ_2 whose end points are far away even though their initial points are near). We also observe that this difference is not caused by conditioning as $\bar{\kappa}(\ell_1, \ell_2)$ is the same for both situations (each pair of lines being obtained from the other by a rotation). \triangle

2^{§2} Mather-Thom theory and some Whitney stratifications

Let us start with a motivation. Gradient retractions are central in Morse theory, where they are used to establish homotopy equivalences between fibers of Morse functions at pairs of regular values without critical values in between.

More precisely, it is known that for a submersion $\alpha : \mathcal{M} \rightarrow I$ from a compact manifold \mathcal{M} to an interval $I \subseteq \mathbb{R}$, the gradient of α induces a homotopy equivalence $\alpha^{-1}(t) \subseteq \alpha^{-1}(J)$ for any subinterval $J \subseteq I$ and any $t \in J$. In more general terms, but also using the gradient of α to prove it, this translates into the following statement (a particular case of Ehresmann's Lemma): for a submersion $\alpha : \mathcal{M} \rightarrow I$ from a compact manifold \mathcal{M} to an interval $I \subseteq \mathbb{R}$, the map $\alpha : \mathcal{M} \rightarrow I$ is a trivial fiber bundle. Recall that a *trivial fiber bundle* $\alpha : E \rightarrow B$ is a continuous map of topological spaces for which there is a subspace F of E (the *fiber*) and a homeomorphism $h : E \rightarrow F \times B$ such that the diagram

$$\begin{array}{ccc} E & \xrightarrow{h} & F \times B \\ \alpha \searrow & & \swarrow \pi_B \\ & B & \end{array}$$

commutes. That is, α is a projection in disguise.

The extension of these results to a more general class of maps is part of the so-called Mather-Thom theory [190, 285, 388]¹, which allows one to generalize the results above from smooth to semialgebraic, not necessarily smooth, maps. Below, we outline the main notions of this theory, stating a version of the so-called Thom's first isotopy lemma; show the theory in action by proving Theorems 1^{§2}2 and 1^{§3}2, as promised in the last chapter; and introduce the main technical construction of this chapter.

2^{§2}-1 Whitney stratifications and Thom's first isotopy lemma

The following definition generalizes the notion of a triangulation of \mathcal{M} , by allowing to decompose \mathcal{M} into more general pieces.

Definition 2^{§2}1. [190; Ch. I, §1] A *Whitney stratification* of a subset Ω of a smooth manifold \mathcal{M} of dimension m is a partition \mathcal{W} of Ω into locally closed smooth submanifolds of \mathcal{M} , called *strata*, such that:

- F** (Locally finite) Every $x \in \Omega$ has a neighborhood intersecting finitely many strata only.
- W** (Whitney's condition b) For every strata $\zeta, \sigma \in \mathcal{W}$, every point $x \in \zeta \cap \bar{\sigma}$, every sequence of points $\{x_\ell\}_{\ell \in \mathbb{N}}$ in ζ converging to x , and every sequence of points $\{y_\ell\}_{\ell \in \mathbb{N}}$ in σ converging to x , we have that, in all local charts of \mathcal{M} around x ,

$$\lim_{\ell \rightarrow \infty} \overline{x_\ell, y_\ell} \subseteq \lim_{\ell \rightarrow \infty} T_{y_\ell} \sigma,$$

provided both limits exist. The inclusion should be interpreted in the local coordinates of the chart: $\overline{x_\ell, y_\ell}$ denotes the straight line joining x_ℓ and y_ℓ , $T_{y_\ell} \sigma$ denotes the affine plane tangent to σ at y_ℓ , and the limits are to be interpreted in the corresponding Grassmannians of \mathbb{R}^m .

A *Whitney stratified set* (Ω, \mathcal{W}) of \mathcal{M} is subset Ω of \mathcal{M} together with a Whitney stratification \mathcal{W} .

Remark 2^{§2}1. In many references, e.g., [285; §5], it is usual for the definition of Whitney stratification to include the so-called boundary condition which states that for every pair of strata $\zeta, \sigma \in \mathcal{W}$, $\zeta \cap \bar{\sigma} \neq \emptyset$ implies $\zeta \subseteq \bar{\sigma}$. We omit it from the given definition, because this condition is not needed and “is something of an embarrassment, since it is not preserved under natural operations on stratifications” [190; pp. 16-17]. ¶

Remark 2^{§2}2. We note that Whitney's condition b has not to be checked for every local chart of \mathcal{M} , since it holds for all local charts if it holds for just one local chart of \mathcal{M} [285; Lemma 2.2]. Further, one can check it in the local chart of an ambient manifold containing \mathcal{M} .

¹The core of the theory was introduced by Thom in 1969 [388]. However, the original paper was hard to read. In the Spring of 1970, Mather gave a course at Harvard. The lecture notes of this course became the unofficial reference to the theory, since they explained and expanded in great detail the original ideas of Thom. In 2012, these references were printed officially [285]. Although we used the more accessible book [190], we call the theory ‘Mather-Thom theory’ to acknowledge the two creators of the theory. However, in some other references like the original reference by Mather [285], this theory is called Thom-Whitney theory.

We also note that Whitney's condition b implies the weaker Whitney's condition a [285; Definition 1.1] which states that for every $\zeta, \sigma \in \mathcal{W}$, $x \in \zeta \cap \bar{\sigma}$ and sequence $\{y_\ell\}$ in σ converging to x , we have $T_x \zeta \subseteq \lim_{\ell \rightarrow \infty} T_{y_\ell} \sigma$ whenever the limit exists [285; Proposition 2.4]. ¶

We go through some examples and non-examples to get familiar with the introduced concepts.

Example 2§2.1. For every smooth manifold \mathcal{M} , $(\mathcal{M}, \{\mathcal{M}\})$, is a Whitney stratified set of \mathcal{M} . We will refer to this as the *trivial stratified set of \mathcal{M}* . △

Example 2§2.2. The *sign map* $\text{sgn} : \mathbb{R}^m \rightarrow \{-1, 0, +1\}^m$ which maps each $x \in \mathbb{R}^m$ to the vector of its signs induces a Whitney stratification on \mathbb{R}^m , which it's called the *sign partition*. We note that the Whitney partitions that we will be working with look locally like the sign partition. △

Example 2§2.3 (Spiral). Consider the stratification of \mathbb{R}^2 consisting of the point $\{0\}$, the smooth one-dimensional submanifold $C := \{(e^t \cos(t), e^t \sin(t)) \mid t \in \mathbb{R}\}$, and the open subset $\sigma := \mathbb{R}^2 \setminus (\{0\} \cup C)$. This stratification does not satisfy Whitney's condition b.

Note that C is a logarithmic spiral and that the angle between $\overline{0, x}$ and $T_x C$ is $\pi/4$ for all $x \in C$. This implies that $\lim_{\ell \rightarrow \infty} \overline{0, y_\ell} \not\subseteq \lim_{\ell \rightarrow \infty} T_{y_\ell} C$ for all sequences $\{y_\ell\}$ of points in C , whenever the two limits of lines exist. Therefore Whitney's condition b cannot hold at $0 \in \{0\} \cap \bar{C}$.

The intuitive reason for this violation of Whitney's condition b is that the spiral C oscillates too much around 0. This means that we should see Whitney's condition b as a "smoothness condition" for stratifications, which guarantees that the different strata "paste" nicely to each other. △

Example 2§2.4 (Whitney's umbrella). [190; Ch. I, §1]. Consider the algebraic set $\Omega := \{(x, y, z) \in \mathbb{R}^3 \mid x^2 - zy^2 = 0\}$, which is known as *Whitney's umbrella*. An initial stratification of Ω can be obtained separating the line $L = \{(x, y, z) \in \mathbb{R}^3 \mid x = y = 0\}$ from the surface $S := \Omega \setminus L$. However, one can check that the stratification $\{L, S\}$ of Ω does not satisfy Whitney's condition b at the origin.

Intuitively, the reason for this is different from that for the spiral. The Whitney umbrella does not have wild variations at the origin. However, one can check that Ω looks different locally around $(0, 0, t) \in L$ depending on whether $t < 0$, $t = 0$ and $t > 0$. If $t < 0$, Ω looks locally like a line; if $t > 0$, like two planes intersecting transversely; and if $t = 0$, like an umbrella broken by the wind. This allows to see the failure of Whitney's condition b as the existence of a radical change in the local topology of Ω as we move along L , which again can be seen as a lack of "smoothness" of the stratification $\{L, S\}$.

However, the stratification $\{L, S\}$ can be turned into a Whitney stratification by dividing the line L into $O = \{(0, 0, 0)\}$, $L^+ := \{(0, 0, z) \in L \mid z > 0\}$ and $L^- := \{(0, 0, z) \in L \mid z < 0\}$. Indeed, $\{O, L^+, L^-, S\}$ is a Whitney stratification of Ω and the phenomenon above does not happen. This procedure can be done in general for semialgebraic sets and one can show that every semialgebraic set admits a Whitney stratification [190; Ch. I, (2.7)]. △

The following proposition shows that Whitney stratified sets (and Whitney stratifications) are closed under many of the usual operations.

Proposition 2^{S2}1. [190; Ch. I, (1.2), (1.3) and (1.4)]. Let \mathcal{I} be a finite set.

- (R) Let (Ω, \mathcal{W}) be a locally closed Whitney stratified set of a smooth manifold \mathcal{M} . If U is an open subset of \mathcal{M} , then $(\Omega \cap U, \mathcal{W}|_U)$, where $\mathcal{W}|_U := \{\sigma \cap U \mid \sigma \cap U \neq \emptyset\}$, is a Whitney stratified set of \mathcal{M} .
- (P) For each $i \in \mathcal{I}$, let $(\Omega_i, \mathcal{W}_i)$ be a locally closed Whitney stratified set of a smooth manifold \mathcal{M}_i . Then $(\prod_{i \in \mathcal{I}} \Omega_i, \prod_{i \in \mathcal{I}} \mathcal{W}_i)$ where $\prod_{i \in \mathcal{I}} \mathcal{W}_i := \{\prod_{i \in \mathcal{I}} \sigma_i \mid \sigma_i \in \mathcal{W}_i\}$ is a Whitney stratified set of $\prod_{i \in \mathcal{I}} \mathcal{M}_i$.
- (I) Let \mathcal{M} be a smooth manifold and, for each $i \in \mathcal{I}$, let $(\Omega_i, \mathcal{W}_i)$ be a locally closed Whitney stratified set of \mathcal{M} . If $\mathcal{W}_1, \dots, \mathcal{W}_r$ are transversal, i.e., for every $\sigma_1 \in \mathcal{W}_1, \dots, \sigma_r \in \mathcal{W}_r$, $\cap_{i=1}^r \sigma_i$ is a transversal intersection, then $(\cap_{i \in \mathcal{I}} \Omega_i, \wedge_{i \in \mathcal{I}} \mathcal{W}_i)$ where

$$\bigwedge_{i \in \mathcal{I}} \mathcal{W}_i := \{\cap_{i \in \mathcal{I}} \sigma_i \mid \sigma_i \in \mathcal{W}_i\}$$

is a Whitney stratified set \mathcal{M} . □

Recall that a map is *proper* when its inverse image of any compact subset is compact. Let \mathcal{A} be a partition of A and \mathcal{B} one of B , by a *stratified homeomorphism* $f : (A, \mathcal{A}) \rightarrow (B, \mathcal{B})$, we mean a homeomorphism $f : A \rightarrow B$ that induces a bijection between \mathcal{A} and \mathcal{B} , i.e., for all $\sigma \in \mathcal{A}$, $f(\sigma) \in \mathcal{B}$. The reason we have introduced Whitney stratifications and Whitney stratified sets is the following result, a version of the so-called Thom's first isotopy lemma, which generalizes Ehresmann's Lemma to more general maps.

Theorem 2^{S2}2 (Thom's first isotopy lemma). [190; Ch. II, (5.1.) and (5.2)]. Let \mathcal{M} be a smooth manifold and (Ω, \mathcal{W}) a locally closed Whitney stratified set of \mathcal{M} and let $\alpha : \mathcal{M} \rightarrow \mathbb{R}^k$ be a smooth map such that

- (i) $\alpha : \Omega \rightarrow \mathbb{R}^k$ is proper,
- (ii) $\alpha|_\sigma : \sigma \rightarrow \mathbb{R}^k$ is surjective, for each stratum $\sigma \in \mathcal{W}$; and
- (iii) $\alpha|_\sigma : \sigma \rightarrow \mathbb{R}^k$ is a submersion, for each stratum $\sigma \in \mathcal{W}$.

Then $\alpha : \Omega \rightarrow \mathbb{R}^k$ is a stratified trivial fiber bundle. That is, there exist a Whitney stratified set (F, \mathcal{F}) and a stratified homeomorphism $h = (h_{\mathbb{R}^k}, h_F) : (\Omega, \mathcal{W}) \rightarrow (\mathbb{R}^k \times F, \{\mathbb{R}^k\} \times \mathcal{F})$ such that $\alpha = h_{\mathbb{R}^k}$. □

Remark 2^{S2}3. Note that every submersion is an open map and that \mathbb{R}^k is connected. Therefore to check that $\alpha|_\sigma : \sigma \rightarrow \mathbb{R}^k$ is surjective is enough to check that $\alpha(\sigma)$ is closed. Then, by connectedness, $\alpha(\sigma) = \mathbb{R}^k$, since $\alpha(\sigma)$ is both open and closed. ¶

Remark 2^{S2}4. As the codomain of α is \mathbb{R}^k , it follows from the proof of [190; Ch. II, (5.2)] that we have a trivial fiber bundle and not just a locally trivial fiber bundle. The last sentence follows from noting that the trivial fibration in the statement of [190; Ch. II, (5.2)] is stratified, see [190; Ch. II, (5.1)]. ¶

Remark 2^{S2}5. We observe that, since h is a stratified homeomorphism, it follows that for all $x, y \in \Omega$, $h_F(x) = h_F(y)$ implies that x and y lie in the same stratum of \mathcal{W} . ¶

Remark 2^{§2} 6. We note that for each $x \in \mathbb{R}^k$, we have that $\alpha^{-1}(x) \cong F$. Further, consider the stratification

$$\mathcal{W}_{|\alpha^{-1}(x)} := \{\sigma \cap \alpha^{-1}(x) \mid \sigma \in \mathcal{W}, \sigma \cap \alpha^{-1}(x) \neq \emptyset\}.$$

Then one can see that $\mathcal{W}_{|\alpha^{-1}(x)}$ is a Whitney stratification of $\alpha^{-1}(x)$ and that h_F gives a stratified homeomorphism between $(\alpha^{-1}(x), \mathcal{W}_{|\alpha^{-1}(x)})$ and (F, \mathcal{F}) . Because of this, we can take as (F, \mathcal{F}) any of the fibers of α . \blacksquare

2^{§2}-2 Mather-Thom theory in action: Theorems 1^{§2}2 and 1^{§3}2

We are now in a position to prove Theorems 1^{§2}2 and 1^{§3}2 using Thom's first isotopy lemma, although the former can be proven just with Ehresmann's lemma. We first prove the simpler Theorem 1^{§2}2 and then the harder Theorem 1^{§3}2.

Proof of Theorem 1^{§2}2. Consider the set

$$\Omega := \{(g, x) \in B \times \mathbb{S}^n \mid f(x) = 0\}$$

where $B := B_W(f, \|f\|_W \kappa(f)^{-1})$. If Ω is empty, we are done; so we can assume that Ω is not empty, and we consider the projection

$$\begin{aligned} \alpha : \Omega &\rightarrow B \\ (g, x) &\mapsto g. \end{aligned}$$

For any compact set $K \subseteq \mathcal{H}_d[q] \setminus \Sigma_d[q]$, we have that $\alpha^{-1}(K)$ is a closed subset of $K \times \mathbb{S}^n$ and so compact. Thus α is proper. Further, we can easily see that for $g \in B$, $\alpha^{-1}(g) = \mathcal{Z}^S(g)$. Hence, if we show that α is a trivial fibration, we are done, since all fibers would be homotopy equivalent and thus all of them would have the same homotopy.

To show that α is a trivial fibration, we will apply Thom's first isotopy lemma (Theorem 2^{§2}2). Let $A : B \times \mathbb{S}^n \rightarrow \mathbb{R}^q$ be given by $A(f, x) := f(x)$. For every $(g, x) \in B \times \mathbb{S}^n$,

$$D_{(g,x)} A = \begin{pmatrix} R_x^0 & D_x g \end{pmatrix} : \mathcal{H}_d[q] \times T_x \mathbb{S}^n \rightarrow \mathbb{R}^q$$

where R_x^0 is the evaluation map, defined in Proposition 1^{§1}6. For $(g, x) \in \Omega$, we have that $D_{(g,x)} A$ is surjective, because $D_x g$ is so. To see this, note that $x \in \mathcal{Z}^S(g)$ and that $g \notin \Sigma_d[q]$, by the Condition Number Theorem (Corollary 1^{§2}10). Hence Ω is a smooth manifold. On this manifold, α is smooth and we consider the trivial Whitney stratification $\{\Omega\}$. The last step for applying Thom's first isotopy lemma (Theorem 2^{§2}2) is to show 1) that α is a submersion and 2) that its image is closed in B , by Remark 2^{§2}3.

1) $D_{(g,x)} \alpha$ is the restriction of the projection $\mathcal{H}_d[q] \times T_x \mathbb{S}^n \rightarrow \mathcal{H}_d[q]$ to

$$T_{(g,x)} \Omega = \{(h, v) \in \mathcal{H}_d[q] \times T_x \mathbb{S}^n \mid h(x) + D_x g v = 0\},$$

and so it is surjective whenever $D_x g$ is so. The latter was shown in the above paragraph for $(g, x) \in \Omega$. Thus α is a submersion.

2) Let $\{g_k\}$ be a sequence in $\alpha(\Omega)$ converging to some $g \in B$. Now, due to the axiom of choice, there is a sequence $\{x_k\}$ in \mathbb{S}^n such that $\{(g_k, x_k)\}$ is a sequence in Ω . Since

\mathbb{S}^n is compact, we can assume without loss of generality that $\{x_k\}$ is converging to some $x \in \mathbb{S}^n$, after passing to a subsequence if necessary. Hence $g = \alpha(g, x) \in \alpha(\Omega)$ and we are done. Therefore $\alpha(\Omega)$ is closed in B .

Since the above holds, we can apply Thom's first isotopy lemma (Theorem 2^{§2}2) to the trivial stratification and the proof concludes. \square

The above proof didn't use stratifications. In the next one, we need to be more careful and so we will need to introduce a new notion of formula.

Definition 2^{§2}2. Let $f \in \mathcal{H}_d[q]$. A *strict formula* over f is a monotone formula over f that contains only atoms of the form $(f_i = 0)$, $(f_i > 0)$ and $(f_i < 0)$, and a *saturated formula* over f is a purely conjunctive strict formula ϕ of the form

$$\phi \equiv \bigwedge_{i=1}^q (f_i \propto_i 0)$$

where $\propto_i \in \{>, <, =\}^q$.

The term "strict" alludes to the fact that no lax inequalities are allowed and the term "saturated" to the fact that one cannot add more strict atoms to the formula. Saturated formulas can be encoded by a sign vector, which will be very useful for proofs.

Definition 2^{§2}3. Let $f \in \mathcal{H}_d[q]$ and ϕ a saturated formula over f . The *sign vector*, $\text{sgn}(\phi)$, is the vector $\text{sgn}(\phi) \in \{-1, 0, +1\}^q$ given by

$$\text{sgn}_i(\phi) := \begin{cases} +1, & \text{if } \propto_i \text{ is } > \\ -1, & \text{if } \propto_i \text{ is } < \\ 0, & \text{if } \propto_i \text{ is } = . \end{cases}$$

The *boundary order* on $\{-1, 0, +1\}^q$, \leqslant , is the partial order defined, for $\sigma, \sigma' \in \{-1, 0, +1\}^q$, by

$$\sigma \leqslant \sigma' \Leftrightarrow \text{for all } i \in [q], \sigma_i = 0 \text{ or } \sigma_i = \sigma'_i. \quad (2.10)$$

Note that for all $x \in S(f, \phi)$, where ϕ is a saturated formula over $f \in \mathcal{H}_d[q]$, we have that $\text{sgn}(f(x)) = \text{sgn}(\phi)$, where $\text{sgn}(f(x))$ is just the vector of signs of $f(x)$. In other words, $x \in S(f, \phi)$ iff $\text{sgn}(f(x)) = \text{sgn}(\phi)$.

The following lemmas are instrumental in the proof of Theorem 1^{§3}2.

Lemma 2^{§2}3. Let $f \in \mathcal{H}_d[q]$. For every Boolean formula Φ over f , there is a unique strict formula $s\text{DNF}(\Phi)$, called *strict disjunctive normal form*, of the form

$$s\text{DNF}(\Phi) \equiv \bigvee_{\xi \in \Xi} \phi_\xi$$

where Ξ is finite and the ϕ_ξ are distinct saturated formulas over f such that for all $m \geq 0$ and polynomial tuples $g \in \mathbb{R}[X_0, \dots, X_m]^q$,

$$W(g, \Phi) = W(g, s\text{DNF}(\Phi)).$$

In particular, $S(f, \Phi) = S(f, s\text{DNF}(\Phi))$.

Lemma 2^{§2} 4. Let $f \in \mathcal{H}_d[q]$ and ϕ and ψ be saturated formulas over f .

(a) If $S(f, \phi) \cap \overline{S(f, \psi)} \neq \emptyset$, then $\text{sgn}(\phi) \leq \text{sgn}(\psi)$.

(b) If $\bar{\kappa}(f) < \infty$ and $S(f, \phi) \neq \emptyset$, then the following are equivalent:

- $S(f, \phi) \subseteq \overline{S(f, \psi)}$.
- $S(f, \phi) \cap \overline{S(f, \psi)} \neq \emptyset$.
- $\text{sgn}(\phi) \leq \text{sgn}(\psi)$.

In particular, when $\bar{\kappa}(f) < \infty$ and $\text{sgn}(\phi) \leq \text{sgn}(\psi)$, $S(f, \phi) \neq \emptyset$ implies $S(f, \psi) \neq \emptyset$.

(c) If $\bar{\kappa}(f) < \infty$ and $S(f, \phi) \neq \emptyset$, then

$$\overline{S(f, \phi)} = S\left(f, \bar{\phi}\right) = \bigcup\{S(f, \psi) \mid \text{sgn}(\psi) \leq \text{sgn}(\phi)\}$$

where $\bar{\phi}$ is the purely conjunctive lax formula obtained substituting $(f_i > 0)$ by $(f_i \geq 0)$ and $(f_i < 0)$ by $(f_i \leq 0)$.

Proof of Theorem 1^{§3} 2. Let $B := B_W(f, \min_i \|f_i\|_W \bar{\kappa}(f)^{-1})$ and consider the proper projection

$$\begin{aligned} \alpha : B \times \mathbb{S}^n &\rightarrow B \\ (\mathbf{g}, x) &\mapsto \mathbf{g}. \end{aligned}$$

For each saturated formula ϕ over f , consider the semialgebraic set

$$\Omega(\phi) := \{(\mathbf{g}, x) \in B \times \mathcal{H}_d[q] \mid x \in S(\mathbf{g}, \phi_g)\}.$$

We can see that

$$\mathcal{S} := \{\Omega(\phi) \mid \phi \text{ is a saturated formula over } f, \Omega(\phi) \neq \emptyset\}$$

is a locally finite partition of $B \times \mathcal{H}_d[q]$.

Arguing as in the proof of Theorem 1^{§2} 2, we can show that the zero set of

$$\begin{aligned} A_\phi : B \times \mathbb{S}^n &\rightarrow \mathbb{R}^{L(\phi)} \\ (\mathbf{g}, x) &\mapsto g^{L(\phi)}(x) \end{aligned}$$

where $L(\phi) := \{I \in [q] \mid \text{sgn}_I(\phi) = 0\}$ is a locally closed submanifold and that the restriction $\alpha|_{A_\phi^{-1}(0)}$ is a submersion. Now, since $\Omega(\phi) = A_\phi^{-1}(0) \cap U(\phi)$ where

$$\begin{aligned} U(\phi) := \{(\mathbf{g}, x) \in B \times \mathbb{S}^n \mid \text{for } I \in [q], f_I(x) > 0 \text{ if } \text{sgn}_I(\phi) = +1 \\ \text{and } f_I(x) < 0 \text{ if } \text{sgn}_I(\phi) = -1\}, \end{aligned}$$

the same applies to $\Omega(\phi)$, i.e., $\Omega(\phi)$ is a locally closed submanifold such that $\alpha|_{\Omega(\phi)}$ is a submersion.

To apply Thom's first isotopy lemma (Theorem 2^{§2}2), we need to do two things: 1) show that \mathcal{S} satisfies Whitney's condition b and therefore is a Whitney stratification, and 2) show that for each $\Omega(\phi)$, $\alpha(\Omega(\phi))$ is closed in B , by Remark 2^{§2}3.

1) By Lemma 2^{§2}4, we can see that for $\Omega(\phi) \in \mathcal{S}$,

$$\overline{\Omega(\phi)} = \left\{ (\mathbf{g}, x) \in B \times \mathbb{S}^n \mid x \in S(\mathbf{g}, \overline{\Omega(\phi)}) \right\} = \bigcup \{ \Omega(\psi) \in \mathcal{S} \mid \text{sgn}(\psi) \leq \text{sgn}(\phi) \}.$$

This means that we only have to check Whitney's condition b for $(\mathbf{g}, x) \in \Omega(\psi) \cap \overline{\Omega(\phi)}$ with $\text{sgn}(\psi) \leq \text{sgn}(\phi)$. Let us choose some local chart (U, u) around (\mathbf{g}, x) , in which (\mathbf{g}, x) is written as u . We will work in the coordinates of this chart to avoid tedious notation, so that we write u, v, \dots instead of $(\mathbf{g}, x), (h, y), \dots$. Let $\{u_\ell\}$ be the sequence in $\Omega(\psi)$ converging to u and $\{v_\ell\}$ the sequence in $\Omega(\phi)$ converging to u .

On the one hand, we can see that

$$\lim_{\ell \rightarrow \infty} T_{v_\ell} \Omega(\phi) = \lim_{\ell \rightarrow \infty} (v_\ell + \ker D_{v_\ell} A_\phi) = u + \ker D_u A_\phi.$$

On the other hand, since $\overline{u_\ell, v_\ell}$ converges to some line, we can assume without loss of generality that $\frac{u_\ell - v_\ell}{\|u_\ell - v_\ell\|}$ is convergent, after passing to a subsequence if necessary. We can see that its limit is the direction vector of the limiting line $\lim_{\ell \rightarrow \infty} \overline{u_\ell, v_\ell}$. Therefore we only need to show that

$$\lim_{\ell \rightarrow \infty} D_u A_\phi \left(\frac{u_\ell - v_\ell}{\|u_\ell - v_\ell\|} \right) = 0.$$

By continuity, this is the same as

$$\lim_{\ell \rightarrow \infty} D_{v_\ell} A_\phi \left(\frac{u_\ell - v_\ell}{\|u_\ell - v_\ell\|} \right) = 0.$$

Now, since $A_\phi(v_\ell) = 0$, by hypothesis, and $A_\phi(u_\ell) = 0$, since $A_\psi(u_\ell) = 0$ by hypothesis, we have that

$$\begin{aligned} \left\| D_{v_\ell} A_\phi \left(\frac{u_\ell - v_\ell}{\|u_\ell - v_\ell\|} \right) \right\| &\leq \frac{1}{2} \max_{w \in [u_\ell, v_\ell]} \left\| D_w^2 A_\phi \left(\frac{u_\ell - v_\ell}{\|u_\ell - v_\ell\|}, u_\ell - v_\ell \right) \right\| \\ &\leq \frac{1}{2} \max_{w \in [u_\ell, v_\ell]} \|D_w^2 A_\phi\| \|u_\ell - v_\ell\|, \end{aligned}$$

by Taylor's theorem. Hence, the desired limit is zero and Whitney's condition b holds.

2) Take $\Omega(\phi) \in \mathcal{S}$. Let $\mathbf{g} \in B$ be a limit point of $\alpha(\Omega(\phi))$, we only have to show that $S(\mathbf{g}, \phi_g) \neq \emptyset$ in order to show that $\mathbf{g} \in \alpha(\Omega(\phi))$. Take any sequence $\{\mathbf{g}_k\}$ in $\alpha(\Omega(\phi))$ that converges to \mathbf{g} . By the axiom of choice, we have that there is a sequence $\{x_k\}$ in \mathbb{S}^n such that $\{(\mathbf{g}_k, x_k)\}$ lies in $\Omega(\phi)$. By compactness of \mathbb{S}^n , we can assume, after taking a subsequence if necessary, that $\{x_k\}$ converges to some $x \in \mathbb{S}^n$. Now, by the form of the closure of $\Omega(\phi)$, we have that $x \in S(\mathbf{g}, \phi_g)$ and so, by Lemma 2^{§2}4, $x \in S(\mathbf{g}, \psi_g)$ for some saturated formula ψ with $\text{sgn}(\psi) \leq \text{sgn}(\phi)$. But then $S(\mathbf{g}, \psi_g) \neq \emptyset$ and so, by Lemma 2^{§2}4 again, $S(\mathbf{g}, \phi_g) \neq \emptyset$. Thus $\mathbf{g} \in \alpha(\Omega(\phi))$. Since \mathbf{g} was arbitrary, this shows that $\alpha(\Omega(\phi))$ is closed in B .

At this moment, we can apply Thom's first isotopy lemma (Theorem 2^{§2}2) and deduce that $\alpha : B \times \mathbb{S}^n \rightarrow B$ is a stratified trivial fiber bundle. Note that α was already a trivial

fiber bundle, we need Thom's first isotopy lemma to guarantee that it is a stratified trivial fiber bundle. Following Remark 2^{\$2} 6 above, we note that the induced stratification on $\mathbb{S}^n \cong \alpha^{-1}(f)$ is given by

$$\mathcal{W}_f := \{S(f, \phi) \mid \phi \text{ is a saturated formula over } f, S(f, \phi) \neq \emptyset\}$$

and so Thom's first isotopy lemma (Theorem 2^{\$2} 2) tells us that there is a continuous map $h : B \times \mathbb{S}^n \rightarrow \mathbb{S}^n$ such that

$$(\alpha, h) : (B \times \mathbb{S}^n, S) \rightarrow (B \times \mathbb{S}^n, \{B\} \times \{\mathcal{W}_f\})$$

is a stratified homeomorphism.

We manipulate this homeomorphism to prove the desired result. Let Φ be an arbitrary formula over f . By Lemma 2^{\$2} 3, we can assume without loss of generality that Φ is in the saturated disjunctive normal form $\bigvee_{\xi \in \Xi} \Phi_\xi$. Consider the set

$$\Omega(\Phi) := \bigcup_{\xi \in \Xi} \Omega(\Phi_\xi)$$

whose image under (α, h) is $B \times S(f, \Phi)$. Since (α, h) is a homeomorphism, it restricts to a homeomorphism

$$(\alpha', h') : \Omega(\Phi) \rightarrow B \times S(f, \Phi)$$

which induces a homeomorphism between each fiber of α' , $S(g, \Phi_g) = (\alpha')^{-1}(g)$, and $S(f, \Phi)$. Hence they have the same homology and we are done. \square

Proof of Lemma 2^{\$2} 3. We apply Morgan's laws to move negations inwards until they apply to atoms. Then we just substitute $\neg(f_i = 0)$ by $(f_i \neq 0)$, $\neg(f_i \neq 0)$ by $(f_i = 0)$, $\neg(f_i > 0)$ by $(f_i \leq 0)$, $\neg(f_i \geq 0)$ by $(f_i < 0)$, $\neg(f_i < 0)$ by $(f_i \geq 0)$, and $\neg(f_i \leq 0)$ by $(f_i < 0)$. After this, we substitute $(f_i \neq 0)$ by $(f_i > 0) \vee (f_i < 0)$, $(f_i \geq 0)$ by $(f_i > 0) \vee (f_i = 0)$, and $(f_i \leq 0)$ by $(f_i < 0) \vee (f_i = 0)$.

Here, we apply the distributive law to take the disjunctions out, until we arrive to a formula of the form

$$\bigvee_{j \in J} \bigwedge_{k \in K_j} (f_{\alpha_j(k)} \circ_{j,k} 0)$$

where J is a finite set, $\{K_j\}_{j \in J}$ a family of finite sets, $\{\alpha_j : K_j \rightarrow [q]\}_{j \in J}$ a family of maps and $\circ \in \{=, >, <\}^{J \times J}$.

If for some $j \in J$, α_j is not injective, then either some factor is repeated inside $\bigwedge_{k \in K_j} (f_{\alpha_j(k)} \circ_{j,k} 0)$ or there are two factors that cancel each other and so, we can eliminate it. Therefore, without loss of generality, we can assume that $K_j \subseteq [q]$ and that α_j is the inclusion map.

If for some $j \in J$, $K_j \neq [q]$, then substitute $\bigwedge_{k \in K_j} (f_k \circ_{j,k} 0)$ by

$$\bigvee_{\circ' \in \{=, >, <\}^{[q] \setminus K_j} \left(\bigwedge_{k \in K_j} (f_k \circ_{j,k} 0) \wedge \bigwedge_{k \in [q] \setminus K_j} (f_j \circ'_k 0) \right)$$

where all the summands are saturated. So without loss of generality, $K_j = [q]$, and so each $\bigwedge_{k \in [q]} (f_k \propto_{j,k} 0)$ is a saturated formula.

In the last step, we eliminate the repeated summands to arrive to a formula of the desired form. None of the transformations we have done affects the realization, independently of which polynomials we substitute in the place of the f_i , so it satisfies the desired property. Further, by substituting f_i by X_i , we can see that such formula is unique, since

$$W((X_1, \dots, X_q), s\text{DNF}(\Phi)_{(X_1, \dots, X_q)}) \cap \{-1, 0, +1\}^q = \{\text{sgn}(\phi_\xi) \mid \xi \in \Xi\}$$

which determines uniquely $s\text{DNF}(\Phi)$. \square

Proof of Lemma 2^{§2} 4. (a). When we take a limit point of $S(f, \psi)$, the equalities of the form $f_i(x) = 0$ are preserved and the inequalities $f_i(x) > 0$ (resp. $f_i(x) < 0$) are either preserved or they turn into equalities of the form $f_i(x) = 0$. This proves the claim.

(b). The first sequence of implications from the first to the third point follows from (a). For the implication from the third point to the first point, let $x \in S(f, \phi)$ and $L := \{I \in [q] \mid \text{sgn}_I(\phi) = 0\}$. Without loss of generality, assume that $L = [k]$. Then by the regularity inequality (Proposition 1^{§3} 3), $D_x f^L$ is surjective and so, by the implicit function theorem, there is an open neighborhood U of x in \mathbb{S}^n and $u : U \mapsto B(0, 1) \subseteq \mathbb{R}^n$ a diffeomorphism, such that for all $i \in [k]$ and $y \in U$, $u_i(y) = f_i(y)$. By making U smaller if necessary, we can assume that for all $i \in [q]$ and $y \in U$, we have that $f_i(y) > 0$ if $\text{sgn}_i(\phi) = \text{sgn}_i(\psi) = +1$, and $f_i(y) < 0$ if $\text{sgn}_i(\phi) = \text{sgn}_i(\psi) = -1$. Taking the point,

$$x_t = u^{-1} \left(u(x) + \frac{\epsilon}{2} \sum_{I \in L} \text{sgn}_I(\psi) e_I \right)$$

we can see that for $t \in (0, 1)$, $x_t \in S(f, \psi)$, since $\text{sgn}(f(\tilde{x})) = \text{sgn}(\psi)$; and that $\lim_{t \rightarrow 0} x_t = x$. Thus $x \in \overline{S(f, \psi)}$ and the implication holds.

(c). This follows easily from (b), since the sets $S(f, \phi)$, with ϕ a saturated formula over f , cover \mathbb{S}^n . \square

2^{§2–3} (f, λ)-lartitions and (f, λ)-partitions

A polynomial tuple $f \in \mathcal{H}_d[q]$ can partition the sphere \mathbb{S}^n in many ways, according to the values it takes. This motivates the introduction of (f, λ) -lartitions and (f, λ) -partitions. The former divide \mathbb{S}^n according to the values that f takes with respect to some finite grid. The latter consider also the signs that f takes. Depending on the context, one or the other is more useful: (f, λ) -lartitions will appear in the proof of Durfee' theorem (Theorem 2^{§3} 2) and (f, λ) -partitions in the proof of the Gabrielov-Vorobiov approximation theorem (Theorem 2^{§4} 2).

Definition 2^{§2} 4. Let $f \in \mathcal{H}_d[q]$ and $\lambda \in \mathbb{R}^{q \times m}$ be a matrix whose entries satisfy $\lambda_{i,1} < \dots < \lambda_{i,m}$, for each $i \in [q]$. To each point $x \in \mathbb{S}^n$ we associate the following sets:

(J•) For all $k \in [m]$, $J_{\bullet,k}(x) := \{i \in [q] \mid f_i(x)/\|f_i\|_W = \lambda_{i,k}\}$.

(JØ0) $J_{\emptyset,0}(x) := \{i \in [q] \mid f_i(x)/\|f_i\|_W < \lambda_{i,1}\}$.

(JØ1) For all $k \in [m-1]$, $J_{\emptyset,k}(x) := \{i \in [q] \mid \lambda_{i,k} < f_i(x)/\|f_i\|_W < \lambda_{i,k+1}\}$.

$$(J\emptyset 2) J_{\emptyset, m}(x) := \{i \in [q] \mid \lambda_{i,m} < f_i(x)/\|f_i\|_W\}.$$

This defines the ordered partition of $[q]$ (in which we allow empty sets):

$$\mathbf{J}(x) := (J_{\emptyset,0}(x), J_{\bullet,1}(x), J_{\emptyset,1}(x), \dots, J_{\bullet,m-1}(x), J_{\emptyset,m-1}(x), J_{\bullet,m}(x), J_{\emptyset,m}(x)).$$

It is clear that the fibers of $x \mapsto \mathbf{J}(x)$ induce an equivalence relation on \mathbb{S}^n . We define the (f, λ) -lartition $\Pi_{f,\lambda}$ as the set of equivalence classes of this relation.

An ordered partition $\mathbf{J} := (J_{\emptyset,0}, J_{\bullet,1}, J_{\emptyset,1}, \dots, J_{\bullet,m}, J_{\emptyset,m})$ of $[q]$ defines the set

$$\Pi_{\mathbf{J}} := \{x \in \mathbb{S}^n \mid \mathbf{J}(x) = \mathbf{J}\},$$

which is an element of $\Pi_{f,\lambda}$, provided it is non-empty.

Remark 2§2.7. Less formally, the construction of $\Pi_{f,\lambda}$ can be described as follows: the i th row of the matrix $\lambda \in \mathbb{R}^{q \times (m+1)}$ defines a partition of \mathbb{R} into $(-\infty, \lambda_{i,1}), \{\lambda_{i,1}\}, (\lambda_{i,1}, \lambda_{i,2}), \dots, (\lambda_{i,m-1}, \lambda_{i,m}), \{\lambda_{i,m}\}$, and $(\lambda_{i,m}, \infty)$. The product of these partitions of \mathbb{R} , for $i \in [q]$, yields a partition of \mathbb{R}^q . By taking the preimage of this partition with respect to \hat{f} , we obtain $\Pi_{f,\lambda}$. So the sets of this partition just indicate us the location of a value $f(x) = (y_1, \dots, y_q) \in \mathbb{R}^q$ within the discrete grid provided by the matrix λ . ¶

Definition 2§2.5. [92; Definition 3.6]. Let $f \in \mathcal{H}_d[q]$ and $\lambda \in \mathbb{R}^{q \times (m+1)}$ be a matrix whose entries satisfy $0 = \lambda_{i,0} < \lambda_{i,1} < \dots < \lambda_{i,m}$, for each $i \in [q]$. To each point $x \in \mathbb{S}^n$ we associate the following sets:

$$(I\bullet) \text{ For all } 0 \leq k \leq m, I_{\bullet,k}(x) := \{i \in [q] \mid |f_i(x)|/\|f_i\|_W = \lambda_{i,k}\}.$$

$$(I\emptyset 1) \text{ For all } 0 \leq k < m, I_{\emptyset,k}(x) := \{i \in [q] \mid \lambda_{i,k} < |f_i(x)|/\|f_i\|_W < \lambda_{i,k+1}\}.$$

$$(I\emptyset 2) I_{\emptyset,m}(x) := \{i \in [q] \mid \lambda_{i,m} < |f_i(x)|/\|f_i\|_W\}.$$

This defines the ordered partition of $[q]$ (in which we allow empty sets):

$$\mathbf{I}(x) := (I_{\bullet,0}(x), I_{\emptyset,0}(x), I_{\bullet,1}(x), I_{\emptyset,1}(x), \dots, I_{\bullet,m-1}(x), I_{\emptyset,m-1}(x), I_{\bullet,m}(x), I_{\emptyset,m}(x)).$$

The point x also determines the tuple of sign conditions $\sigma(x) \in \{-1, 0, +1\}^q$ given by

$$(S) \sigma_i(x) := \operatorname{sgn}(f_i(x)) \text{ for } i \in [q].$$

It is clear that the fibers of $x \mapsto (\mathbf{I}(x), \sigma(x))$ induce an equivalence relation on \mathbb{S}^n . We define the (f, λ) -partition $\Pi_{f,\lambda}$ as the set of equivalence classes of this relation.

An ordered partition $\mathbf{I} := (I_{\bullet,0}, I_{\emptyset,0}, \dots, I_{\bullet,m}, I_{\emptyset,m})$ of $[q]$ together with a sign vector $\sigma \in \{-1, 0, +1\}^q$ defines the set

$$\Pi_{\mathbf{I},\sigma} := \{x \in \mathbb{S}^n \mid \mathbf{I}(x) = \mathbf{I}, \sigma(x) = \sigma\},$$

which is an element of $\Pi_{f,\lambda}$, provided it is non-empty.

Remark 2§2.8. Note that (f, λ) -partitions are just a particular case of (f, λ) -lartitions. They correspond to the case in which each row of λ is symmetric with respect to the origin. However, in the symmetric setting where this is needed, (f, λ) -partitions are better, because they encode this symmetry in the sign vector σ . ¶

Remark 2^{§2}9. The term “lartition” is just a language play with the notation that we use. While we denote the (f, λ) -partition by $\Pi_{f,\lambda}$, we denote the (f, λ) -lartition by $\Lambda_{f,\lambda}$. So the difference in the initial letter reflects the change in the initial letter of their names. ¶

Example 2^{§2}5. Let $n = 1$, $q = 1$, $f = (XY)$ and $\lambda = (0, \sqrt{3}/4)$. We can see that, in this case, $\Lambda_{f,\lambda}$ has exactly five elements. The zero-dimensional pieces are

$$\{(1, 0), (-1, 0), (0, 1), (0, -1)\} \text{ and } \left\{\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right), \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right), \left(-\frac{\sqrt{3}}{2}, -\frac{1}{2}\right)\right\},$$

and the one-dimensional pieces

$$\{(x, y) \in \mathbb{S}^2 \mid 4xy > \sqrt{3}\}, \{(x, y) \in \mathbb{S}^2 \mid 0 < 4xy < \sqrt{3}\} \text{ and } \{(x, y) \in \mathbb{S}^2 \mid xy < 0\}.$$

This is represented in Figure 2^{§2}2. We can see that none of the strata of $\Lambda_{f,\lambda}$ is connected, so the strata might be topologically complicated. △

Example 2^{§2}6. [92; Example 3.8]. Figure 2^{§2}3 shows, locally, an example of a (f, λ) -partition on \mathbb{S}^2 with $q = 2$, $m = 2$ and $\lambda_{1,i} = \lambda_{2,i} = \lambda_i$. The thick curves correspond to the zero sets for f_1 and f_2 . The dashed lines are level curves (for both f_1 and f_2) with levels $-\lambda_1$ and λ_1 and the dotted curves are the same for the levels $-\lambda_2$ and λ_2 . All these curves partition the picture into 36 two-dimensional open regions, 60 open segments, and 25 points. Each of these 121 regions corresponds to an element in $\Pi_{f,\lambda}$. We write down the details for some of them in Table 2.1. △

The following two theorems give sufficient conditions on $f \in \mathcal{H}_d[q]$ and $\lambda \in \mathbb{R}^{q \times (m+1)}$ for the (f, λ) -lartition and (f, λ) -partition of \mathbb{S}^n to be a Whitney stratification.

Theorem 2^{§2}5. Let $f \in \mathcal{H}_d[q]$ with $\bar{\kappa}(f) < \infty$ and assume $\lambda \in \mathbb{R}^{q \times m}$ satisfies for $i \in [q]$,

$$-\frac{1}{\sqrt{2} \bar{\kappa}(f)} < \lambda_{i,1} < \lambda_{i,2} < \dots < \lambda_{i,m} < \frac{1}{\sqrt{2} \bar{\kappa}(f)}. \quad (2.11)$$

Then the (f, λ) -lartition $\Lambda_{f,\lambda}$ is a Whitney stratification of \mathbb{S}^n . Furthermore, under these conditions, the following holds:

(1) The codimension in \mathbb{S}^n of each stratum π_J equals $\sum_{k=1}^m |\mathbb{J}_{\bullet,k}| = q - \sum_{k=0}^m |\mathbb{J}_{\emptyset,k}|$.

(2) Given $\pi_J \in \Lambda_{f,\lambda}$ and $a \in J_{\emptyset,k}$ for some $k \in [m-1]$, the map

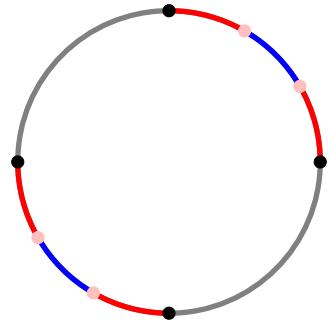
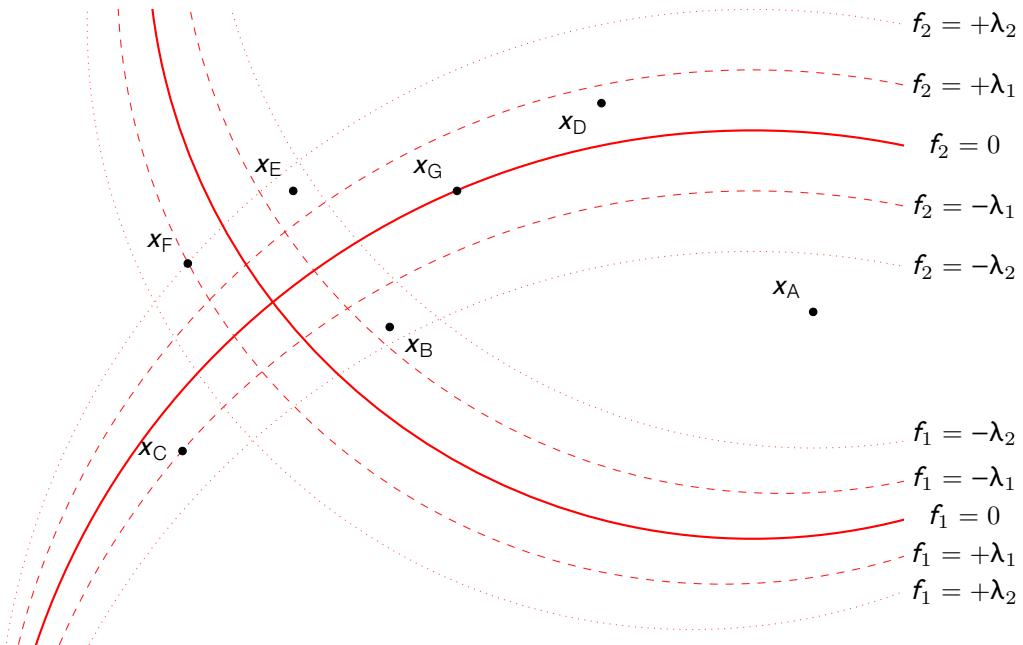
$$\begin{aligned} \hat{f}_{a,J} : \pi_J &\rightarrow (\lambda_{a,k}, \lambda_{a,k+1}) \\ x &\mapsto f_a(x)/\|f_a\|_W \end{aligned}$$

is a surjective submersion.

Theorem 2^{§2}6. [92; Theorem 3.9] Let $f \in \mathcal{H}_d[q]$ with $\bar{\kappa}(f) < \infty$ and assume $\lambda \in \mathbb{R}^{q \times (m+1)}$ satisfies for $i \in [q]$,

$$0 = \lambda_{i,0} < \lambda_{i,1} < \dots < \lambda_{i,m} < \frac{1}{\sqrt{2} \bar{\kappa}(f)}. \quad (2.12)$$

Then the (f, λ) -partition $\Pi_{f,\lambda}$ is a Whitney stratification of \mathbb{S}^n . Furthermore, under these conditions, the following holds:

Figure 2^{S2} 2: $\Pi_{f,\lambda}$ with $f = (XY)$ and $\lambda = (0, \sqrt{3}/4)$ Figure 2^{S2} 3: An example of $\Pi_{f,\lambda}$ (locally) on \mathbb{S}^2 with $q = 2$ and $m = 2$.

	$ _{\bullet,0}$	$ _{\emptyset,0}$	$ _{\bullet,1}$	$ _{\emptyset,1}$	$ _{\bullet,2}$	$ _{\emptyset,2}$	σ
x_A	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset	$\{1, 2\}$	$(-1, -1)$
x_B	\emptyset	\emptyset	\emptyset	$\{1, 2\}$	\emptyset	\emptyset	$(-1, -1)$
x_C	\emptyset	\emptyset	\emptyset	\emptyset	$\{2\}$	$\{1\}$	$(+1, -1)$
x_D	\emptyset	$\{2\}$	\emptyset	\emptyset	\emptyset	$\{1\}$	$(-1, +1)$
x_E	\emptyset	\emptyset	\emptyset	$\{1, 2\}$	\emptyset	\emptyset	$(-1, +1)$
x_F	\emptyset	\emptyset	$\{1\}$	\emptyset	$\{2\}$	\emptyset	$(+1, +1)$
x_G	$\{2\}$	\emptyset	\emptyset	\emptyset	\emptyset	$\{1\}$	$(-1, 0)$

Table 2 . 1: Some points in Figure 2^{S2} 3 and their ordered partition and sign vector.

(1) The codimension in \mathbb{S}^n of each stratum $\Pi_{\mathbf{l}, \sigma}$ equals $\sum_{k=0}^m |\mathbf{l}_{\bullet, k}| = q - \sum_{k=0}^m |\mathbf{l}_{\emptyset, k}|$.

(2) Given $\Pi_{\mathbf{l}, \sigma} \in \Pi_{f, \lambda}$ and $a \in \mathbf{l}_{\emptyset, k}$ for some $k < m$, the map

$$\begin{aligned}\hat{f}_{a, \mathbf{l}, \sigma} : \Pi_{\mathbf{l}, \sigma} &\rightarrow (\lambda_{a, k}, \lambda_{a, k+1}) \\ x &\mapsto |f_a(x)|/\|f_a\|_W\end{aligned}$$

is a surjective submersion.

Remark 2^{S2}10. Recall that the condition “ $a \in J_{\emptyset, k}$ for some $k \in [m-1]$ ” can be less cryptically written as “ $f_a(x)/\|f_a\|_W \in (\lambda_{a, k}, \lambda_{a, k+1})$ for some $x \in \Pi_{\mathbf{l}, \sigma}$ and $k \in [m-1]$ ”, or simply as “ $f_a/\|f_a\|_W \in (\lambda_{a, k}, \lambda_{a, k+1})$ on $\Pi_{\mathbf{l}, \sigma}$ for some $k \in [m-1]$ ”. Similarly, the condition “ $a \in I_{\emptyset, k}$ for some $k < m$ ” can be rewritten as “ $|f_a(x)|/\|f_a\|_W \in (\lambda_{a, k}, \lambda_{a, k+1})$ for some $x \in \Pi_{\mathbf{l}, \sigma}$ and $k < m$ ”, or simply as “ $|f_a|/\|f_a\|_W \in (\lambda_{a, k}, \lambda_{a, k+1})$ on $\Pi_{\mathbf{l}, \sigma}$ for some $k < m$ ”. ¶

The following lemma, which is a simple consequence of the Implicit Function Theorem, will be instrumental in the proof of the above theorems.

Lemma 2^{S2}7. [91; Lemma 4.9]. For given $f \in \mathcal{H}_d[q]$ put $g_i := f_i/\|f_i\|$. Fix $x \in \mathbb{S}^n$, and let $r > 0$ be such that $\sqrt{2} \bar{\kappa}(f)r < 1$. We define the index set

$$S := \{i \in \{1, \dots, q\} \mid |g_i(x)| \leq r\}$$

and set $\bar{u} := g^S(x) \in \mathbb{R}^S$. Then $|S| \leq n$, and there exist an open neighborhood O_x of x in \mathbb{S}^n and $\varepsilon > 0$ with the following properties:

(t1) We have $|g_i(y)| > r$ for all $i \notin S$ and all $y \in O_x$.

(t2) For all i such that $g_i(x) \neq 0$, the sign of g_i does not change on O_x .

(t3) The set $Z_x := \{y \in O_x \mid f^S(y) = f^S(x)\}$ is a smooth submanifold of \mathbb{S}^n of codimension $|S|$, and there exists a diffeomorphism h such that the diagram

$$\begin{array}{ccc} O_x & \xrightarrow{h} & Z_x \times B(\bar{u}, \varepsilon) \\ & \searrow g^S & \swarrow \pi_B \\ & B(\bar{u}, \varepsilon) & \end{array},$$

commutes (that is, for every $i \in S$, g_i becomes a coordinate projection in the coordinates on O_x given by h).

We will call the pair (O_x, h) a *trivializing chart at x* . We can describe a point $y \in O_x$ by its *trivializing coordinates* $(z, u) \in Z_x \times B(\bar{u}, \varepsilon)$, where $u = (u_i)_{i \in S}$ and $h(y) = (z, u)$. In these coordinates, the normalized polynomial $g_i = f_i/\|f_i\|_W$, for $i \in S$, takes the form $(z, u) \mapsto u_i$.

Proof of Theorem 2^{S2}5. In order to show that $\Pi_{f, \lambda}$ is a Whitney stratification, we notice that

$$\Pi_{f, \lambda} = \bigwedge_{i=1}^q \Pi_{f_i, \lambda_i} = \left\{ \cap_{i=1}^q \Pi_i \mid \Pi_i \in \Pi_{f_i, \lambda_i} \right\}$$

where $\lambda_i := (\lambda_{i,1}, \dots, \lambda_{i,m})$ is the i th row of λ and Π_{f_i, λ_i} is the (f_i, λ_i) -partition of \mathbb{S}^n . Thus, by Proposition 2^{§2}1(l), it is enough to show that each Π_{f_i, λ_i} is a Whitney stratification and that $\Pi_{f_1, \lambda_1}, \dots, \Pi_{f_q, \lambda_q}$ are transversal.

Note that Π_{f_i, λ_i} consists of open sets of the form $f_i^{-1}(\mathbf{a}, \mathbf{b})$, with (\mathbf{a}, \mathbf{b}) an open interval, or a hypersurface of the form $f_i^{-1}(\mathbf{t})$, with $\mathbf{t} = \|f_i\|_W \lambda_{i,j}$ for some j . By assumption on λ , this implies that for such \mathbf{t} , $|\mathbf{t}| < \|f_i\|_W / (\sqrt{2} \bar{\kappa}(f))$ and hence, by the regularity inequality (Proposition 1^{§3}3) and the implicit function theorem, all the hypersurfaces are smooth. Whitney's condition b is verified in a straightforward way so that we conclude that Π_{f_i, λ_i} is a Whitney stratification.

We show now that $\Pi_{f_1, \lambda_1}, \dots, \Pi_{f_q, \lambda_q}$ are transversal. Let $\pi_i \in \Pi_{f_i, \lambda_i}$, for $i \in [q]$, and $x \in \cap_{i \leq q} \pi_i$. It is easy to check that $\text{codim } T_x \pi_i = 1$ if $i \in J_{\bullet, k}(x)$ and $\text{codim } T_x \pi_i = 0$ otherwise. Therefore, abbreviating $J_{\bullet, *}(x) := \cup_k J_{\bullet, k}(x)$, we get $\sum_{i=1}^q \text{codim } T_x \pi_i = |J_{\bullet, *}(x)|$. In addition, when π_i is a hypersurface, we have $T_x \pi_i = \ker D_x f_i$, and thus

$$\bigcap_{i=1}^q T_x \pi_i = \bigcap_{i \in J_{\bullet, *}(x)} \ker D_x f_i = \ker D_x f^{J_{\bullet, *}(x)}.$$

By the regularity inequality (Proposition 1^{§3}3), the codimension of the right-hand side is $|J_{\bullet, *}(x)|$. This shows that $\Pi_{f_1, \lambda_1}, \dots, \Pi_{f_q, \lambda_q}$ are in general position. We conclude that $\Pi_{f, \lambda}$ is a Whitney stratification.

The argument above proves also (1).

We prove part (2) in a standard way. First, we show that $\hat{f}_{\mathbf{a}, \mathbf{J}}$ is a submersion, i.e., that its gradient is not tangent to $\pi_{\mathbf{J}}$. Then we show that $\hat{f}_{\mathbf{a}, \mathbf{J}}$ is closed. Once we have done this, Remark 2^{§2}3 finishes the proof, since closed submersions are surjective when the codomain is connected.

To show that $\hat{f}_{\mathbf{a}, \mathbf{J}}$ is a submersion, we fix a point $p \in \pi_{\mathbf{J}}$ and take trivializing coordinates around it, using Lemma 2^{§2}7. In these coordinates, using the notation explained after Lemma 2^{§2}7, $\pi_{\mathbf{I}, \sigma}$ is an open subset of an affine subspace given by

$$\begin{cases} U_i = \lambda_{i,k} & (0 < k \leq m, i \in J_{\bullet, k}) \\ \lambda_{i,k} \leq U_i \leq \lambda_{i,k+1} & (0 \leq k < m, i \geq 1, i \in J_{\emptyset, k}) \end{cases} \quad (2.13)$$

whose tangent space is given by the system

$$\begin{cases} U_i = 0 & (0 \leq k \leq m, i \in J_{\bullet, k}) \end{cases}. \quad (2.14)$$

The map $\hat{f}_{\mathbf{a}, \mathbf{J}}$ in these coordinates becomes the linear map $U_{\mathbf{a}}$. To check that $\hat{f}_{\mathbf{a}, \mathbf{J}}$ is a submersion is then enough to check that $U_{\mathbf{a}}$ is not identically zero in the tangent space in these coordinates. Since $\mathbf{a} \notin \cup_k J_{\bullet, k}$, $U_{\mathbf{a}}$, this is the case and so $\hat{f}_{\mathbf{a}, \mathbf{J}}$ is a submersion.

To show that $\hat{f}_{\mathbf{a}, \mathbf{J}}$ is closed, it is enough to show that for every sequence $\{x_k\}$ in $\pi_{\mathbf{J}}$, if $\{\hat{f}_{\mathbf{a}, \mathbf{J}}(x_k)\}$ has a limit $\lambda \in (\lambda_{\mathbf{a}, k}, \lambda_{\mathbf{a}, k+1})$, then there exists $x \in \pi_{\mathbf{J}}$ such that $\hat{f}_{\mathbf{a}, \mathbf{J}}(x) = \lambda$.

As \mathbb{S}^n is compact, we can assume without loss of generality that $\{x_k\}$ converges to a point $x' \in \overline{\pi_{\mathbf{J}}}$. By continuity, $\hat{f}_{\mathbf{a}, \mathbf{J}}(x') = \lambda$. Passing again to trivializing coordinates and using Lemma 2^{§2}7, we perturb x' to a point x whose components in these coordinates are as

follows:

$$u_i := \begin{cases} u'_i + t & \text{if for some } k \text{ we have } i \in J_{\emptyset, k} \text{ and } u'_i = \lambda_{i,k} \\ u'_i - t & \text{if for some } k \text{ we have } i \in J_{\emptyset, k} \text{ and } u'_i = \lambda_{i,k+1} \\ u'_i & \text{otherwise} \end{cases}$$

with a sufficiently small $t > 0$. This new point x evaluates to the same value as x' under $\hat{f}_{a,J}$, since $u_a = u'_a$ as $u'_a = \lambda \in (\lambda_{a,k}, \lambda_{a,k+1})$ by hypothesis; and it belongs to π_J . Thus it is the desired point and we are done. \square

Proof of Theorem 2^{§2 6}. The proof is analogous to the one of Theorem 2^{§2 6}. Moreover, we can avoid redoing the proof altogether, by noting that for $\mu \in \mathbb{R}^{q \times (2m+1)}$ given by

$$\mu_i := (-\lambda_{i,m}, \dots, -\lambda_{i,1}, 0, \lambda_{i,1}, \dots, \lambda_{i,m})$$

for $i \in [q]$, $\Pi_{f,\mu} = \Pi_{f,\lambda}$. \square

Proof of Lemma 2^{§2 7}. Assume first that S is nonempty. The regularity inequality (Proposition 1^{§3 3}) implies that $D_x f^S$ is surjective, since $\sqrt{2}\kappa(f^S) \frac{\|f^S(x)\|}{\|f^S\|_W} < 1$. So clearly $|S| \leq m$. Hence the derivative of the map g^S at x is surjective as well. The Implicit Function Theorem implies the existence of a diffeomorphism h and a neighborhood O_x satisfying (t3) with Z_x smooth. By shrinking O_x , we can guarantee that properties (t1) and (t2) hold. Finally, the assertion is easily checked when S is empty. \square

2^{§3} Durfee's theorem

A fundamental step in the sampling theory of Chapter 4 that will allow us to construct the simplicial complex homologically equivalent to the considered closed semialgebraic set is that we need that inclusions of the form $S(f, t, \phi) \hookrightarrow S_r(f, t, \phi)$, with ϕ a purely conjunctive lax formula over (f, t) , to give isomorphisms in homology.

The following theorem is a consequence of results by Durfee [163] concerning algebraic neighborhoods of algebraic and semialgebraic sets.

Theorem 2^{§3 1} (Durfee's theorem). [163; §3]. Let $f \in \mathcal{H}_d[q]$, $t \in \mathbb{R}^e$ and ϕ a purely conjunctive lax formula over (f, t) . Then for all sufficiently small $r > 0$, the inclusion $S(f, t, \phi) \hookrightarrow S_r(f, t, \phi)$ is a homotopy equivalence. \square

To apply the above statement, we need a quantified version in which the meaning of “sufficiently small” is quantified. This is handled by the next theorem.

Theorem 2^{§3 2} (Quantitative Durfee's theorem). [91; Proposition 4.6] and [92; Theorem 4.4]. Let $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$ and $r > 0$ be such that $\sqrt{2}\bar{\kappa}(f)(r + T) < 1$ and $\mathbb{L}(t) > 2r$. Then for every purely conjunctive lax formula ϕ over (f, t) , the inclusion $S(f, t, \phi) \hookrightarrow S_r(f, t, \phi)$ is a homotopy equivalence.

We actually will prove a stronger version of this theorem. For $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$, ϕ lax formula over (f, t) and a vector $r \in \mathbb{R}_{>}^q$, we define

$$S_r(f, t, \Phi) := \Phi_{\mathbb{S}^n} \left(\hat{f}_i^{-1}[t_j - r_i, t_j + r_i], \hat{f}_i^{-1}[t_j - r_i, \infty), \hat{f}_i^{-1}(-\infty, t_j + r_i] \mid i \in [q], j \in [e] \right).$$

In a more digestable way, $S_r(f, t, \Phi)$ is the semialgebraic set obtained by substituting in Φ the atoms ($f_i = \|f_i\|_W t_j$) by ($f_i \leq \|f_i\|_W(t_j + r_i)$) \wedge ($f_i \geq \|f_i\|_W(t_j - r_i)$), ($f_i \geq \|f_i\|_W t_j$) by ($f_i \geq \|f_i\|_W(t_j - r_i)$) and ($f_i \leq \|f_i\|_W t_j$) by ($f_i \leq \|f_i\|_W(t_j + r_i)$), and interpreting the obtained formula in the obvious way. Note that the the difference between $S_r(f, t, \Phi)$ and $S_r(f, t, \Phi)$, for $r > 0$, is that while in the latter we do the relaxation with the same r for all polynomials, in the former we do this with a different constant for each polynomial.

Theorem 2^{§3}3 (Strong quantitative Durfee's theorem). *Let $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$ and $r \in \mathbb{R}_{>}^q$ be such that*

$$\sqrt{2} \bar{\kappa}(f)(\|\mathbf{r}\|_\infty + T) < 1 \text{ and } \mathbb{W}(t) > 2\|\mathbf{r}\|_\infty. \quad (2.15)$$

Then for every purely conjunctive lax formula ϕ over (f, t) , the inclusion $S(f, t, \phi) \hookrightarrow S_r(f, t, \phi)$ is a homotopy equivalence.

We move \mathbf{r} to $\varepsilon \mathbf{1}$, with sufficiently small $\varepsilon > 0$, so that we can apply Durfee's theorem (Theorem 2^{§3}1). However, we don't carry out this motion all at once, but one component of \mathbf{r} at a time, so that it can be easily handled with Mather-Thom theory.

Remark 2^{§3}1. We note that Theorem 2^{§3}2 together with its proof can be extended easily to cover the case in which Φ is a lax formula, not necessarily purely conjunctive. However, such an extension would make the proof unnecessarily technical. \blacksquare

2^{§3}-1 Moving \mathbf{r} to the unknown known case²

We write $\mathbf{r} \leq_a \mathbf{r}'$ when $r_a \leq r'_a$ and for $i \neq a$, $r_i = r'_i$. We note that whenever $\mathbf{r} \leq_a \mathbf{r}'$, we have the inclusion

$$S_r(f, t, \phi) \subseteq S_{r'}(f, t, \phi)$$

between the generalized algebraic neighborhoods of $S(f, t, \phi)$. It is enough for us to prove the following proposition, because with it we can prove Theorem 2^{§3}3.

Proposition 2^{§3}4. *Let $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$ and $\mathbf{r}, \mathbf{r}' \in \mathbb{R}_{>}^q$ be such that (2.15) holds for both \mathbf{r} and \mathbf{r}' . If for some $a \in [q]$, $\mathbf{r} \leq_a \mathbf{r}'$, then for every purely conjunctive lax formula ϕ over (f, t) , the inclusion $S_r(f, t, \phi) \hookrightarrow S_{r'}(f, t, \phi)$ is a homotopy equivalence.*

Proof of Theorem 2^{§3}3. Let $\varepsilon > 0$ be such that $S(f, t, \phi) \hookrightarrow S_\varepsilon(f, t, \phi)$ is a homotopy equivalence and such that $\varepsilon \mathbf{1} \leq \mathbf{r}$. This number exists by Durfee's theorem (Theorem 2^{§3}1).

Consider now the sequence $\mathbf{r}^{(0)}, \dots, \mathbf{r}^{(q)} \in (0, \infty)^q$ defined by

$$r_i^{(k)} := \begin{cases} r_i & \text{if } i > k \\ \varepsilon & \text{if } i \leq k \end{cases}$$

for $i \in [q]$ and $k \in \{0, \dots, q\}$. Note that $\mathbf{r}^{(0)} = \mathbf{r}$, $\mathbf{r}^{(q)} = \varepsilon \mathbf{1}$ and that for $k \in [q]$, $\mathbf{r}^{(k)} \leq_k \mathbf{r}^{(k-1)}$. Hence, by Proposition 2^{§3}4, we have a sequence of inclusions

$$S_\varepsilon(f, t, \phi) = S_{\mathbf{r}^{(q)}}(f, t, \phi) \hookrightarrow S_{\mathbf{r}^{(q-1)}}(f, t, \phi) \hookrightarrow \dots \hookrightarrow S_{\mathbf{r}^{(0)}}(f, t, \phi) = S_r(f, t, \phi)$$

where each inclusion is a homotopy equivalence. Thus $S(f, t, \phi) \hookrightarrow S_r(f, t, \phi)$ is a homotopy equivalence and the proof concludes. \square

²The term “unknown known case” is a punchline which points out that the case stated by the non-explicit theorem is a known case, but it is unknown as we don't know when we are in that case explicitly.

2^{§3–2} Moving \mathbf{r} one step at a time (Proof of Proposition 2^{§3}4)

We now apply Mather-Thom theory to prove Proposition 2^{§3}4, and with it, the quantitative Durfee's theorem (Theorem 2^{§3}2 and 2^{§3}3). The main idea is to construct a (f, λ) -lartition that is compatible with the considered semialgebraic sets, so that we can apply Thom's first isotopy lemma (Theorem 2^{§2}2).

By Proposition 2^{§1}2, we can assume, without loss of generality, that ϕ is in normal form. It follows from its proof, that the equality $S_r(f, t, \phi) = S_r(f, t, \text{NF}(\phi))$ still holds if we put \mathbf{r} in the place of r , as long as the inequality $\mathbb{W}(t) > 2\|\mathbf{r}\|_\infty$ holds. Thus assume that ϕ has the form

$$\begin{aligned} \bigwedge_{n \in \mathcal{N}_+} (f_n \geq t_{\alpha(n)} \|f_n\|_W) \wedge \bigwedge_{n \in \mathcal{N}_-} (f_n \leq t_{\alpha(n)} \|f_n\|_W) \\ \wedge \bigwedge_{n \in \mathcal{N}_0} ((f_n \geq t_{lb(n)} \|f_n\|_W) \wedge (f_n \leq t_{ub(n)} \|f_n\|_W)) \end{aligned}$$

with $\mathcal{N}_+, \mathcal{N}_-, \mathcal{N}_0 \subseteq [q]$ pairwise disjoint, $\alpha : \mathcal{N}_+ \cup \mathcal{N}_- \rightarrow [e]$ and $lb, ub : \mathcal{N}_0 \rightarrow [e]$ such that for all $n \in \mathcal{N}_0$, $t_{lb(n)} \leq t_{ub(n)}$.

To make notation less tedious, we will assume that $\|f_a\|_W = 1$ without loss of generality, since $\bar{\kappa}(f)$ is invariant under scaling. Moreover, for fixed a , we will write $r := r_a$, $r' := r'_a$ and

$$C_p := S_{\mathbf{r}_p}(f, t, \phi)$$

for $\mathbf{r}_p := (r_1, \dots, r_{a-1}, p, r_{a+1}, \dots, r_q)$. With these notations, observe that $\mathbf{r}_r = \mathbf{r}$ and $\mathbf{r}_{r'} = \mathbf{r}'$. And so we only need to show that the inclusion $\iota : C_r \rightarrow C_{r'}$ is a homotopy equivalence.

Consider now $\tau, \tau' > \|\mathbf{r}'\|_\infty$ such that $\tau < \tau'$, $\sqrt{2} \bar{\kappa}(f)(\tau + \tau') < 1$ and $\mathbb{W}(t) > 2\tau'$. We define $\lambda \in \mathbb{R}^{q \times 4}$ as follows

$$\lambda_i = \begin{cases} (t_{\alpha(i)} - \tau', t_{\alpha(i)} - \tau, t_{\alpha(i)} - r_i, t_{\alpha(i)}), & \text{if } i \neq a \text{ and } i \in \mathcal{N}_+ \\ (t_{\alpha(a)} - \tau', t_{\alpha(a)} - \tau, t_{\alpha(a)}, t_{\alpha(a)} + \tau), & \text{if } i = a \in \mathcal{N}_+ \\ (t_{\alpha(i)}, t_{\alpha(i)} + r_i, t_{\alpha(i)} + \tau, t_{\alpha(i)} + \tau'), & \text{if } i \neq a \text{ and } i \in \mathcal{N}_- \\ (t_{\alpha(a)} - \tau, t_{\alpha(a)}, t_{\alpha(a)} + \tau, t_{\alpha(a)} + \tau'), & \text{if } i = a \in \mathcal{N}_- \\ (t_{lb(i)} - r_i, t_{lb(i)}, t_{lb(i)} + r_i, t_{lb(i)}), & \text{if } i \neq a, i \in \mathcal{N}_0 \text{ and } lb(i) = ub(i) \\ (t_{lb(a)} - \tau, t_{lb(a)}, t_{lb(a)} + \tau, t_{lb(a)} + \tau'), & \text{if } i = a \in \mathcal{N}_0 \text{ and } lb(a) = ub(a) \\ (t_{lb(i)} - r_i, t_{lb(i)}, t_{ub(i)}, t_{ub(i)} + r_i), & \text{if } i \neq a, i \in \mathcal{N}_0 \text{ and } lb(i) \neq ub(i) \\ (t_{lb(a)} - \tau, t_{lb(a)}, t_{ub(a)}, t_{ub(a)} + \tau), & \text{if } i = a \in \mathcal{N}_0 \text{ and } lb(a) \neq ub(a). \end{cases}$$

The choice of λ is done in a way that the strata of $\Pi_{f, \lambda}$ intersect nicely with the C_p . In other words, so that we can prove Proposition 2^{§3}5 and 2^{§3}6.

For the sake of simplicity, we have to distinguish four cases: 1) $a \in \mathcal{N}_+$, 2) $a \in \mathcal{N}_-$, 3) $a \in \mathcal{N}_0$ with $lb(a) = ub(a)$, and 4) $a \in \mathcal{N}_0$ with $lb(a) < ub(a)$. We will just do the cases 1) and 4), because the case 2) can be easily reduced to the case 1), by changing (f, t) to $(-f, -t)$, and the case 3) is analogous to the case 4).

Case 1) $a \in \mathcal{N}_+$

From now own, we assume that $a \in \mathcal{N}_+$. The following proposition shows how the strata of $\Pi_{f,\lambda}$ intersect the C_ρ .

Proposition 2^{§3}5. (1) C_τ is a union of strata of $\Pi_{f,\lambda}$.

(2) Let $\rho, \rho' \in (0, \tau)$. For each $\pi_J \in \Pi_{f,\lambda}$ such that $\pi_J \subseteq C_\tau$, the following holds:

(i) $\pi_J \cap C_\rho = \emptyset$ iff $\pi_J \cap C_{\rho'} = \emptyset$. In this case, $\pi_J \subseteq f_a^{-1}(t_{\alpha(a)} - \tau)$.

(ii) $\pi_J \cap C_\rho = \pi_J$ iff $\pi_J \cap C_{\rho'} = \pi_J$. In this case, $\pi_J \subseteq f_a^{-1}[t_{\alpha(a)}, \infty)$.

(iii) If $\emptyset \neq \pi_J \cap C_\rho \subsetneq \pi_J$, then $\pi_J \subseteq f_a^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)})$ and

$$\pi_J \cap C_\rho = \pi_J \cap \{x \in \mathbb{S}^n \mid f_a(x) \geq t_{\alpha(a)} - \rho\}.$$

With this proposition, we can proceed to the proof of Theorem 2^{§3}3 in the case in which $a \in \mathcal{N}_+$.

Proof of Theorem 2^{§3}3 for $a \in \mathcal{N}_+$. Consider the closed set

$$\Omega := C_\tau \cap f_a^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)}) \subseteq f_a^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)})$$

and the proper smooth map

$$\begin{aligned} \vartheta : f_a^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)}) &\rightarrow (0, \tau) \\ x &\mapsto t_{\alpha(a)} - f_a(x). \end{aligned}$$

By Proposition 2^{§3}5, Ω is an union of strata of $\Pi_{f,\lambda}$, particularly of those strata in which f_a takes values in $(t_{\alpha(a)} - \tau, t_{\alpha(a)})$. And so, by Theorem 2^{§2}5 and the given assumptions, the hypothesis of Thom's first isotopy lemma (Theorem 2^{§2}2) are satisfied. In particular, this means that there is $F \subseteq \Omega$ and a homeomorphism $h := (\vartheta, h_F) : \Omega \rightarrow (0, \tau) \times F$.

Consider now the linear homotopy

$$\begin{aligned} v : [0, 1] \times [0, \tau] &\rightarrow [0, \tau] \\ (s, y) &\mapsto \begin{cases} y, & \text{if } y \in [0, r] \\ (1-s)y + sr, & \text{if } y \in [r, r'] \\ y + s(r-r') \left(1 - 2\frac{y-r'}{\tau-r'}\right), & \text{if } y \in [r', (r'+\tau)/2] \\ y, & \text{if } y \in [(r'+\tau)/2, \tau] \end{cases} \end{aligned} \tag{2.16}$$

that restricts to a continuous retraction of $[0, r']$ onto $[0, r]$ and that leaves fixed every point in a neighborhood of $\{0, \tau\}$. Using v , we define the map

$$\begin{aligned} \theta : [0, \tau] \times \Omega &\rightarrow \Omega \\ (s, x) &\mapsto h^{-1}(h_F(x), v(s, \vartheta(x))). \end{aligned}$$

This continuous map restricts to a continuous retraction of $\vartheta^{-1}(0, r') = C_{r'} \cap f_a^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)})$ onto $\vartheta^{-1}(0, r) = C_r \cap f_a^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)})$, and it leaves every point in a neighborhood of the boundary of Ω inside C_τ fixed. This statement is due to Proposition 2^{§3}5 and the fact

that Θ respects the strata of $\Pi_{f,\lambda}$, since h is a stratified homeomorphism by Thom's first isotopy lemma (Theorem 2^{S2}2). Because of this last point, it can be extended to a continuous map

$$\begin{aligned}\Theta : [0, \tau] \times C_\tau &\rightarrow C_\tau \\ (s, x) &\mapsto \begin{cases} \Theta(s, x), & \text{if } x \in \Omega \\ x, & \text{otherwise.} \end{cases}\end{aligned}$$

By the above paragraph, Θ still restricts to a continuous retraction of $C_{r'}$ onto C_r . Hence the inclusion $\iota : C_r \rightarrow C_{r'}$ is a homotopy equivalence. \square

Proof of Proposition 2^{S3}5. Since the (f, λ) -lpartition $\Pi_{f,\lambda}$ classifies points in \mathbb{S}^n according to the values that f takes with respect to λ , we can see that our choice guarantees trivially all the claims. We prove only the last claim (2)(iii).

By construction of Π_J , either $\Pi_J \subseteq f^{-1}(t_{\alpha(a)}, \infty)$, $\Pi_J \subseteq f^{-1}(t_{\alpha(a)})$, $\Pi_J \subseteq f^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)})$ or $\Pi_J \subseteq f^{-1}(t_{\alpha(a)} - \tau)$. The rest of the options are excluded, since $\Pi_J \subseteq C_\tau$. Therefore, because $t_{\alpha(a)} - \rho \in (t_{\alpha(a)} - \tau, t_{\alpha(a)})$ and $\emptyset \neq \Pi_J \cap C_\rho \subsetneq \Pi_J$, we must have $\Pi_J \subseteq f^{-1}(t_{\alpha(a)} - \tau, t_{\alpha(a)})$.

Since $\Pi_J \subseteq C_\tau$, all defining inequalities of C_ρ are satisfied, except at most the inequality $f_a \geq t_{\alpha(a)} - \rho$. Thus enforcing this inequality is the only difference between Π_J and $\Pi_J \cap C_\rho$, which gives the stated equality. \square

Case 4) $a \in \mathcal{V}_0$ with $lb(a) < ub(a)$

From now own, we assume that $a \in \mathcal{V}_0$ and that $lb(a) < ub(a)$. As in case 1), we have a proposition relating the strata of $\Pi_{f,\lambda}$ and the C_ρ . Its proof is analogous to that in case 1), and because of that, we omit the proof.

Proposition 2^{S3}6. (1) C_τ is a union of strata of $\Pi_{f,\lambda}$.

(2) Let $\rho, \rho' \in (0, \tau)$. For each $\Pi_J \in \Pi_{f,\lambda}$ such that $\Pi_J \subseteq C_\tau$, the following holds:

- (i) $\Pi_J \cap C_\rho = \emptyset$ iff $\Pi_J \cap C_{\rho'} = \emptyset$. In this case, $\Pi_J \subseteq f_a^{-1}(\{t_{lb(a)} - \tau, t_{ub(a)} + \tau\})$.
- (ii) $\Pi_J \cap C_\rho = \Pi_J$ iff $\Pi_J \cap C_{\rho'} = \Pi_J$. In this case, $\Pi_J \subseteq f_a^{-1}[t_{lb(a)}, t_{ub(a)}]$.
- (iii) If $\emptyset \neq \Pi_J \cap C_\rho \subsetneq \Pi_J$, then $\Pi_J \subseteq f_a^{-1}((t_{lb(a)} - \tau, t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + \tau))$ and

$$\Pi_J \cap C_\rho = \Pi_J \cap \{x \in \mathbb{S}^n \mid t_{lb(a)} - \rho \leq f_a(x) \leq t_{ub(a)} + \rho\}.$$

\square

As in case 1), with this proposition, we can proceed to the proof of Theorem 2^{S3}3.

Proof of Theorem 2^{S3}3 for $a \in \mathcal{V}_0$ with $lb(a) < ub(a)$. Consider the closed set

$$\begin{aligned}\Omega := C_\tau \cap f_a^{-1}((t_{lb(a)} - \tau, t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + \tau)) \\ \subseteq f_a^{-1}((t_{lb(a)} - \tau, t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + \tau))\end{aligned}$$

and the proper smooth map

$$\begin{aligned} \vartheta : f_a^{-1}((t_{lb(a)} - \tau, t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + \tau)) &\rightarrow (0, \tau) \\ x &\mapsto \begin{cases} t_{lb(a)} - f_a(x), & \text{if } f_a(x) < t_{lb(a)} \\ f_a(x) - t_{ub(a)}, & \text{if } f_a(x) > t_{ub(a)}. \end{cases} \end{aligned}$$

By Proposition 2^{S3}6, Ω is an union of strata of $\Pi_{f,\lambda}$, particularly of those strata in which f_a takes values in $(t_{lb(a)} - \tau, t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + \tau)$. And so, by Theorem 2^{S2}5 and the given assumptions, the hypothesis of Thom's first isotopy lemma (Theorem 2^{S2}2) are satisfied. In particular, this means that there is $F \subseteq \Omega$ and a homeomorphism $h := (\vartheta, h_F) : \Omega \rightarrow (0, \tau) \times F$.

With the help of the linear homothopy in (2.16), we define the map

$$\begin{aligned} \theta : [0, \tau] \times \Omega &\rightarrow \Omega \\ (s, x) &\mapsto h^{-1}(h_F(x), v(s, \vartheta(x))). \end{aligned}$$

This continuous map restricts to a continuous retraction of $\vartheta^{-1}(0, r') = C_{r'} \cap f_a^{-1}((t_{lb(a)} - r', t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + r'))$ onto $\vartheta^{-1}(0, r) = C_r \cap f_a^{-1}((t_{lb(a)} - r, t_{lb(a)}) \cup (t_{ub(a)}, t_{ub(a)} + r))$, and it leaves every point in a neighborhood of the boundary of Ω inside C_τ fixed. This statement is due to Proposition 2^{S3}6 and the fact that θ respects the strata of $\Pi_{f,\lambda}$, since h is a stratified homeomorphism by Thom's first isotopy lemma (Theorem 2^{S2}2). Because of this last point, it can be extended to a continuous map

$$\begin{aligned} \Theta : [0, \tau] \times C_\tau &\rightarrow C_\tau \\ (s, x) &\mapsto \begin{cases} \vartheta(s, x), & \text{if } x \in \Omega \\ x, & \text{otherwise.} \end{cases} \end{aligned}$$

By the above paragraph, Θ still restricts to a continuous retraction of $C_{r'}$ onto C_r . Hence the inclusion $\iota : C_r \rightarrow C_{r'}$ is a homotopy equivalence, as desired. \square

2^{S4} Gabrielov-Vorobjov approximation theorem

The main algorithmic techniques to compute the homology that we have available (see Chapter 3) work for closed sets. Unfortunately, many natural and well-posed semialgebraic sets are not closed, such as the semialgebraic described by

$$((X - Y, Y), (X - Y = 0 \wedge Y > 0) \vee (X - Y > 0 \wedge Y = 0)). \quad (2.17)$$

To circumvent this problem we will rely on a beautiful construction by Gabrielov and Vorobjov in [186] that produces closed semialgebraic approximations to semialgebraic sets.

The idea of the construction by Gabrielov and Vorobjov [186] is to produce a sequence of steps, each combining relaxations of closed conditions (equalities and lax inequalities) and strengthenings of open condition (strict inequalities) of the formula. The sequence is such that what is missed at one step is covered by next step of relaxations and strengthenings.

Definition 2^{§4}1. [92; Definition 2.3] Given a monotone formula Φ over $f \in \mathcal{H}_d[q]$ and positive δ and ε , the Gabrielov-Vorobjov (δ, ε) -block $\Gamma B_{\delta, \varepsilon}(f, \Phi)$ is the spherical semialgebraic set defined by the following rewriting of Φ ,

$$\begin{aligned} f_i = 0 &\rightsquigarrow |f_i(x)| \leq \varepsilon \|f_i\|_W, \\ f_i \neq 0 &\rightsquigarrow (f_i(x) \geq \delta \|f_i\|_W) \vee (f_i(x) \leq -\delta \|f_i\|_W), \\ f_i > 0 &\rightsquigarrow f_i(x) \geq \delta \|f_i\|_W, \\ f_i \geq 0 &\rightsquigarrow (f_i(x) \geq \delta \|f_i\|_W) \vee (|f_i(x)| \leq \varepsilon \|f_i\|_W), \\ f_i < 0 &\rightsquigarrow f_i(x) \leq -\delta \|f_i\|_W, \text{ and} \\ f_i \leq 0 &\rightsquigarrow (f_i(x) \leq -\delta \|f_i\|_W) \vee (|f_i(x)| \leq \varepsilon \|f_i\|_W). \end{aligned}$$

Given $\delta, \varepsilon \in (0, \infty)^m$, the Gabrielov-Vorobjov (δ, ε) -approximation $\Gamma B_{\delta, \varepsilon}(f, \Phi)$ (of order m) of $S(f, \Phi)$ is the spherical semialgebraic set given by

$$\Gamma B_{\delta, \varepsilon}(f, \Phi) := \bigcup_{k=1}^m \Gamma B_{\delta_k, \varepsilon_k}(f, \Phi). \quad (2.18)$$

Remark 2^{§4}1. Note that $|f_i(x)| \leq \varepsilon \|f_i\|_W$ is just an abbreviation of $(f_i(x) \leq \varepsilon \|f_i\|_W) \wedge (f_i(x) \geq -\varepsilon \|f_i\|_W)$ and that both Gabrielov-Vorobjov blocks and Gabrielov-Vorobjov approximations are compact subsets of \mathbb{S}^n . ¶

Remark 2^{§4}2. The symbol “ ΓB ” used to denote Gabrielov-Vorobjov blocks and approximations should not be confused with “ ΓB ”, the Greek letter ‘ Γ ’ followed by the Latin letter ‘ B ’. “ ΓB ” comes from the initials in the Cyrillic alphabet of the names of Gabrielov (Габриэлов) and Vorobjov (Воробьев). ¶

The main result of Gabrielov and Vorobjov is the following one.

Theorem 2^{§4}1 (Gabrielov-Vorobjov approximation theorem). [186; Theorem 1.10] Let $f \in \mathcal{H}_d[q]$, Φ be a monotone formula over f , $m \in \mathbb{N}$, and $\delta, \varepsilon \in (0, \infty)^m$. If

$$0 < \varepsilon_1 \ll \delta_1 \ll \dots \ll \varepsilon_m \ll \delta_m \ll 1, \quad (2.19)$$

then, for $k \in \{0, \dots, m-1\}$, there are homomorphisms

$$\phi_k : \pi_k(\Gamma B_{\delta, \varepsilon}(f, \Phi)) \rightarrow \pi_k(S(f, \Phi))$$

and

$$\varphi_k : H_k(\Gamma B_{\delta, \varepsilon}(f, \Phi)) \rightarrow H_k(S(f, \Phi))$$

that are isomorphisms for $k < m-1$ and epimorphisms when $k = m-1$. □

Remark 2^{§4}3. In the above theorem, the expression $0 < a_1 \ll \dots \ll a_t \ll 1$ means that there are functions $h_k : (0, 1)^{t-k} \rightarrow (0, 1)$ such that $0 < a_k < h_k(a_{k+1}, \dots, a_t)$ for all k . Unfortunately, no explicit form for the functions h_k is given in [186], although in principle one should be able to determine them from the proof there. However, let us note that the functions h_k in (2.19) do not depend continuously on the coefficients of f for an arbitrary f . This phenomenon can be seen by taking two orthogonal lines and deforming them continuously onto the same line. ¶

Remark 2^{§4}4. Homotopy groups (without specifying a base point) are only defined for connected spaces. However, the bijection between $\pi_0(\Gamma B_{\delta,\varepsilon}(f, \Phi))$ and $\pi_0(S(f, \Phi))$ identifies the connected components of $\Gamma B_{\delta,\varepsilon}(f, \Phi)$ and those of $S(f, \Phi)$. Therefore we can naturally interpret $\phi_k : \pi_k(\Gamma B_{\delta,\varepsilon}(f, \Phi)) \rightarrow \pi_k(S(f, \Phi))$, for $k > 0$, as the family of maps

$$\{\phi_k : \pi_k(C) \rightarrow \pi_k(\phi_0(C)) \mid C \in \pi_0(\Gamma B_{\delta,\varepsilon}(f, \Phi))\}.$$

The assumption of connectedness in [186; Theorem 1.10] is only for technical ease of the exposition. ¶

The proof of Theorem 2^{§4}1 goes beyond of what we aim to cover. Because of this we invite the interested reader to read it in [186]. The following two examples try to illustrate the theorem.

Example 2^{§4}1. [92; Example 2.6]. Consider the pair (f, Φ) in (2 . 17). For any pair (δ, ε) with $0 < \varepsilon < \delta$ the block $\Gamma B_{\delta,\varepsilon}(f, \Phi)$ is given by

$$\left(|x - y| \leq \varepsilon \sqrt{2} \wedge (y \geq \delta) \right) \vee \left(|y| \leq \varepsilon \wedge (x - y \geq -\delta \sqrt{2}) \right)$$

and looks as in Figure 2^{§4}4. It is clear that this block is homotopically equivalent to $S(f, \Phi)$. △

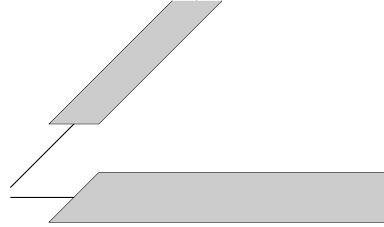


Figure 2^{§4}4: The Gabrielov-Vorobjov construction for two open half-lines

Example 2^{§4}2. [92; Example 2.7] The number m of blocks needed in the Gabrielov-Vorobjov construction to recover the k th homology group of $S(f, \Phi)$ may reach the bound $k + 2$ in Theorem 2^{§4}1. This can be seen in the linear case.

For example, let $f = (X, Y)$ and consider

$$\Phi \equiv (X = 0 \wedge Y = 0) \vee (X = 0 \wedge Y > 0) \vee (X > 0 \wedge Y = 0) \vee (X > 0 \wedge Y > 0)$$

so that $S(f, \Phi)$ is the non-negative quadrant. Now take any sequence $0 < \varepsilon_1 < \delta_1 < \varepsilon_2 < \delta_2 < \varepsilon_3 < \delta_3$.

At the left of Figure 2^{§4}5 we see in light grey shading the block $\Gamma B_{\delta_1, \varepsilon_1}(f, \Phi)$. It is not connected; not even the 0th homology group is correct. At the center of the figure we see that same first block with $\Gamma B_{\delta_2, \varepsilon_2}(f, \Phi)$ superimposed in a darker shade of grey. Now the union of the first two blocks is connected (so H_0 is correct) but not simply connected: the first homology group is wrong. We obtain a contractible set, homotopically equivalent to $S(f, \Phi)$, when we add the third block, at the right of the figure, to the union. △

The main theorem of this chapter makes the «« in the Gabrielov-Vorobjov approximation theorem (Theorem 2^{§4}1) explicit in the case of a well-posed polynomial tuple.

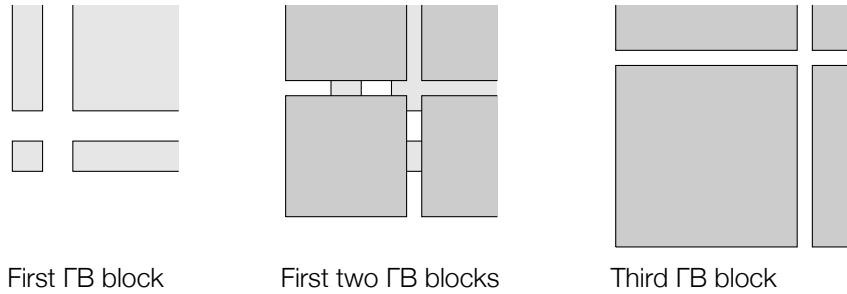


Figure 2^{S4} 5: The Gabrielov-Vorobjov construction for the positive quadrant

Theorem 2^{S4} 2 (Quantitative Gabrielov-Vorobjov approximation theorem). [92; Theorem 2.8]. In Theorem 2^{S4} 1, condition (2.19) can be replaced by

$$0 < \varepsilon_1 < \delta_1 < \dots < \varepsilon_m < \delta_m < \frac{1}{\sqrt{2} \bar{\kappa}(f)} \quad (2.20)$$

when $\bar{\kappa}(f) < \infty$.

Example 2^{S4} 3. [92; Example 2.9]. The simple form of the inequalities in (2.20) requires well-posedness, i.e., $\bar{\kappa}(f) < \infty$. To see this, consider $f = (X, Y, X - Y)$ and

$$\Phi \equiv ((X = 0) \wedge (Y > 0)) \vee ((X - Y = 0) \wedge (Y > 0)).$$

The set $S(f, \Phi)$ consists of two half-lines with a common origin but without this origin. Note that $\bar{\kappa}(f) = \infty$. Figure 2^{S4} 6 shows $S(f, \Phi)$ at the left. The center and right parts of the

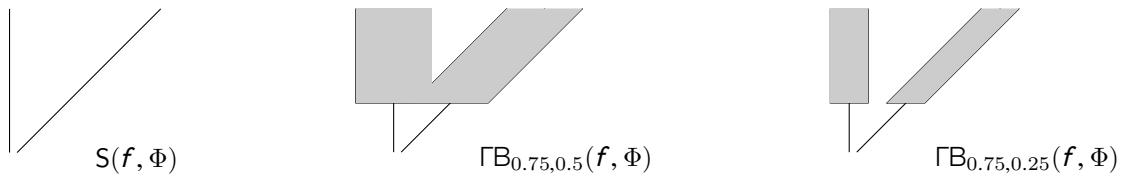


Figure 2^{S4} 6: The Gabrielov-Vorobjov construction for an ill-posed system

figure exhibit two Gabrielov-Vorobjov Approximations for it with $m = 1$ but different pairs (δ, ε) . The middle part shows that the condition $\varepsilon < \delta$ is not strong enough to guarantee the conclusions of Theorem 2^{S4} 1 for $m = 1$. An easy computation shows that, in this case, we need $0 < \varepsilon < \delta/2$ (as in the right part of the figure). \triangle

The idea of the proof of Theorem 2^{S4} 2 is simple. Instead of proving it from scratch, we prove that modifications of (δ, ε) do not alter the homotopy of the Gabrielov-Vorobjov approximations and we use this to reduce to the case in which we can apply Theorem 2^{S4} 1. We first show how we will do transform a pair (δ, ε) satisfying (2.20) into a pair (δ', ε') satisfying (2.19) and then we will show how our basic transformation preserves homotopy.

2^{S4}-1 Moving (δ, ε) to the unknown known case

We write $(\delta, \varepsilon) \leq_{D,i} (\delta', \varepsilon')$ when $\varepsilon = \varepsilon'$, $\delta_j = \delta'_j$ for $j \neq i$, and $\delta_i \geq \delta'_i$. Similarly, we write $(\delta, \varepsilon) \leq_{E,i} (\delta', \varepsilon')$ when $\delta = \delta'$, $\varepsilon_j = \varepsilon'_j$ for $j \neq i$, and $\varepsilon_i \leq \varepsilon'_i$. Note that

the calligraphic index \mathcal{D} indicates a difference in a $\boldsymbol{\delta}$ (and therefore, in an inequality of the corresponding Gabrielov-Vorobjov system), while a calligraphic \mathcal{E} does so for an $\boldsymbol{\varepsilon}$ (and therefore in an equality). These relations capture the notion of a difference in only one entry of $\boldsymbol{\delta}$ or of $\boldsymbol{\varepsilon}$, respectively. The choice of the inequality in the $\boldsymbol{\varepsilon}$ s and the $\boldsymbol{\delta}$ s is different. This is done to ensure that if either $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \leq_{\mathcal{D},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$ or $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \leq_{\mathcal{E},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$, then we have, for all formulas Φ over f , the inclusion

$$\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}}(f, \Phi) \subseteq \Gamma B_{\boldsymbol{\delta}', \boldsymbol{\varepsilon}'}(f, \Phi) \quad (2.21)$$

between the corresponding Gabrielov-Vorobjov approximations. We write

$$(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{D},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$$

to denote that

$$(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \leq_{\mathcal{D},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}') \quad \text{or} \quad (\boldsymbol{\delta}', \boldsymbol{\varepsilon}') \leq_{\mathcal{D},i} (\boldsymbol{\delta}, \boldsymbol{\varepsilon}).$$

This notation is consistent with the meaning of updating $(\boldsymbol{\delta}, \boldsymbol{\varepsilon})$ to $(\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$ by updating (either increasing or decreasing) only $\boldsymbol{\delta}_i$ to $\boldsymbol{\delta}'_i$. We similarly define $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{E},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$.

The following result states the main property of these rewritings.

Proposition 2^{§4}3. [92; Proposition 3.1]. *Let $f \in \mathcal{H}_{\mathbf{d}}[q]$, Φ be a strict formula over f , and $\boldsymbol{\delta}, \boldsymbol{\delta}', \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}' \in \mathbb{R}^m$ be such that both $(\boldsymbol{\delta}, \boldsymbol{\varepsilon})$ and $(\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$ satisfy (2.20). If either $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{D},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$ or $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{E},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$, then the corresponding inclusion (2.21) of Gabrielov-Vorobjov approximations induces a homotopy equivalence.*

Proving Theorem 2^{§4}2 from this proposition is easy.

Proof of Theorem 2^{§4}2. By the definition of \ll , it is clear that there exist at least one $(\tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{\varepsilon}})$ satisfying both (2.19) and (2.20). For any $(\boldsymbol{\delta}, \boldsymbol{\varepsilon})$ satisfying (2.20), we can easily construct a sequence $(\boldsymbol{\delta}^{(0)}, \boldsymbol{\varepsilon}^{(0)}), \dots, (\boldsymbol{\delta}^{(\ell)}, \boldsymbol{\varepsilon}^{(\ell)})$ of pairs satisfying (2.20) such that

1. $(\boldsymbol{\delta}^{(0)}, \boldsymbol{\varepsilon}^{(0)}) = (\boldsymbol{\delta}, \boldsymbol{\varepsilon})$,
2. $(\boldsymbol{\delta}^{(\ell)}, \boldsymbol{\varepsilon}^{(\ell)}) = (\tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{\varepsilon}})$, and
3. for each $p \in \{0, \dots, \ell - 1\}$, there are $k_p \in \{\mathcal{D}, \mathcal{E}\}$ and $i_p \in \{1, \dots, m\}$ such that

$$(\boldsymbol{\delta}^{(p)}, \boldsymbol{\varepsilon}^{(p)}) \xrightarrow{k_p, i_p} (\boldsymbol{\delta}^{(p+1)}, \boldsymbol{\varepsilon}^{(p+1)}).$$

For such a sequence, the isomorphism types of the homology groups of $\Gamma B_{\boldsymbol{\delta}^{(p+1)}, \boldsymbol{\varepsilon}^{(p+1)}}(f, \Phi)$ don't change at each step as a consequence of Proposition 2^{§4}3. Thus $\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}}(f, \Phi)$ has homology groups isomorphic to those of $\Gamma B_{\tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{\varepsilon}}}(f, \Phi)$. The conclusion now follows from applying Theorem 2^{§4}1 to the latter. \square

We next focus on the situations $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{D},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$ and $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{E},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$. These situations correspond to replacing $\boldsymbol{\delta}_i$ in the first one and $\boldsymbol{\varepsilon}_i$ in the second one by some $\zeta \in (\boldsymbol{\varepsilon}_i, \boldsymbol{\delta}_i)$. Even though we are updating only one entry in the pair $(\boldsymbol{\delta}, \boldsymbol{\varepsilon})$, we have to modify the inequalities associated to several polynomials. Instead of doing this replacement simultaneously in

all the inequalities, we do it by steps, in the inequalities corresponding to a single polynomial at a time. With this intuition at hand, we introduce the semialgebraic sets below.

Fix $f \in \mathcal{H}_d[q]$, a strict formula Φ over f , positive numbers $\delta, \varepsilon, \zeta, t$, and $a \in \{0, \dots, q\}$. We define the following spherical semialgebraic sets:

$\Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{D}, a}(f, \Phi)$ is obtained from Φ by rewriting

$$\begin{aligned} f_l = 0 &\rightsquigarrow |f_l(x)| \leq \varepsilon \|f_l\|_W \\ f_l > 0 &\rightsquigarrow \begin{cases} f_l(x) \geq \delta \|f_l\|_W & \text{if } l > a \\ f_a(x) \geq t \|f_a\|_W & \text{if } l = a \\ f_l(x) \geq \zeta \|f_l\|_W & \text{if } l < a \end{cases} \\ f_l < 0 &\rightsquigarrow \begin{cases} f_l(x) \leq -\delta \|f_l\|_W & \text{if } l > a \\ f_a(x) \leq -t \|f_a\|_W & \text{if } l = a \\ f_l(x) \leq -\zeta \|f_l\|_W & \text{if } l < a. \end{cases} \end{aligned} \quad (2.22)$$

$\Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{E}, a}(f, \Phi)$ is obtained from Φ by rewriting

$$\begin{aligned} f_l = 0 &\rightsquigarrow \begin{cases} |f_l(x)| \leq \varepsilon \|f_l\|_W & \text{if } l > a \\ |f_a(x)| \leq t \|f_a\|_W & \text{if } l = a \\ |f_l(x)| \leq \zeta \|f_l\|_W & \text{if } l < a \end{cases} \\ f_l > 0 &\rightsquigarrow f_l(x) \geq \delta \|f_l\|_W \\ f_l < 0 &\rightsquigarrow f_l(x) \leq -\delta \|f_l\|_W. \end{aligned} \quad (2.23)$$

Consider now $\delta, \varepsilon \in (0, \infty)^m$, $c \in \{\mathcal{D}, \mathcal{E}\}$, $i \in \{1, \dots, m\}$, $a \in [q]$ and $\zeta, t > 0$. We define the intermediate Gabrielov-Vorobjov approximations as the sets

$$\Gamma B_{\delta, \varepsilon, \zeta, t}^{c, i, a}(f, \Phi) := \Gamma B_{\delta_i, \varepsilon_i, \zeta, t}^{c, a}(f, \Phi) \cup \bigcup_{j \neq i} \Gamma B_{\delta_j, \varepsilon_j}(f, \Phi). \quad (2.24)$$

In particular, we can see $\Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{D}, i, a}(f, \Phi)$ as the result of having replaced δ_i by ζ in all the inequalities with polynomials f_1, \dots, f_{a-1} , and being in the process of making the replacement in those inequalities with f_a with the parameter t moving from δ_i to ζ .

We now observe that for $\zeta, t, t' > 0$ with $t \leq t'$ we have the inclusions

$$\Gamma B_{\delta, \varepsilon, \zeta, t'}^{\mathcal{D}, i, a}(f, \Phi) \subseteq \Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{D}, i, a}(f, \Phi) \quad \text{and} \quad \Gamma B_{\delta, \varepsilon, \zeta, t'}^{\mathcal{E}, i, a}(f, \Phi) \supseteq \Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{E}, i, a}(f, \Phi). \quad (2.25)$$

The crucial fact to prove Theorem 2^{S4}2 is that these inclusions induce homotopy equivalences.

Proposition 2^{S4}4. [92; Proposition 3.2]. Let $f \in \mathcal{H}_d[q]$, Φ be a strict formula, $\delta, \varepsilon \in \mathbb{R}^m$ satisfying (2.20), and let $i \in [m]$ and $a \in [q]$. Then,

- (1) For all $\zeta \in (\varepsilon_i, \delta_i)$ and $\varepsilon_i < t \leq t' < \varepsilon_{i+1}$ (where $\varepsilon_{m+1} = 1/\sqrt{2} \bar{\kappa}(f)$ by convention), the inclusion $\Gamma B_{\delta, \varepsilon, \zeta, t'}^{\mathcal{D}, i, a}(f, \Phi) \subseteq \Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{D}, i, a}(f, \Phi)$ induces a homotopy equivalence.
- (2) For all $\zeta \in (\varepsilon_i, \delta_i)$ and $\delta_{i-1} < t \leq t' < \delta_i$ (where $\delta_0 = 0$ by convention), the inclusion $\Gamma B_{\delta, \varepsilon, \zeta, t'}^{\mathcal{E}, i, a}(f, \Phi) \supseteq \Gamma B_{\delta, \varepsilon, \zeta, t}^{\mathcal{E}, i, a}(f, \Phi)$ induces a homotopy equivalence.

Again, Proposition **2^{§4}3** easily follows from this result.

Proof of Proposition 2^{§4}3. Assume that $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \leq_{\mathcal{D},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$ holds. Then $\delta_i \geq \delta'_i$ and without loss of generality, $\delta_i > \delta'_i$. The following equalities then follow from the definition of $\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \zeta, t}^{1,i,a}(f, \Phi)$ (we omit the (f, Φ) in what follows for simplicity):

- $\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, 1} = \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}},$
- $\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, a} = \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, a+1}, \quad \text{for all } a \in [q-1],$
- $\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, q} = \Gamma B_{\boldsymbol{\delta}'}, \boldsymbol{\varepsilon} = \Gamma B_{\boldsymbol{\delta}'}, \boldsymbol{\varepsilon}'$,

the last one as, by assumption, $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}'$. These equalities yield the following chain

$$\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}} = \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, 1} \subseteq \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, 1} = \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, 2} \subseteq \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, 2} = \cdots \subseteq \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \delta'_i, \delta_i}^{\mathcal{D}, i, q} = \Gamma B_{\boldsymbol{\delta}'}, \boldsymbol{\varepsilon}',$$

on which all inclusions induce homotopy equivalences by Proposition **2^{§4}4(1)**. Hence Proposition **2^{§4}3** follows in this case.

For the other cases, i.e., when $(\boldsymbol{\delta}', \boldsymbol{\varepsilon}') \leq_{\mathcal{D},i} (\boldsymbol{\delta}, \boldsymbol{\varepsilon})$ or when $(\boldsymbol{\delta}, \boldsymbol{\varepsilon}) \xrightarrow{\mathcal{E},i} (\boldsymbol{\delta}', \boldsymbol{\varepsilon}')$, we proceed analogously. \square

2^{§4}-2 Moving $(\boldsymbol{\delta}, \boldsymbol{\varepsilon})$ one step at a time (Proof of Proposition **2^{§4}4**)

We have now all the tools needed to prove Proposition **2^{§4}4** and with it to finish the proof of the Quantitative Gabrielov-Vorobjov Theorem **2^{§4}2**. We will only prove part (1) of Proposition **2^{§4}4** as part (2) is proven in an analogous way.

We fix $f \in \mathcal{H}_{\mathbf{d}}[q]$, a strict formula Φ over f , tuples $\boldsymbol{\delta}, \boldsymbol{\varepsilon} \in (0, \infty)^m$, an index $i \in [m]$, a point $\zeta \in (\varepsilon_i, \delta_i)$, points $t < t'$ in the interval $(\varepsilon_i, \varepsilon_{i+1})$, and an index $a \in [q]$, as in the statement of Proposition **2^{§4}4** and satisfying the hypothesis given there. Since a is fixed, we can assume $\|f_a\|_W = 1$ without loss of generality after scaling f appropriately.

We also choose positive numbers t_0, t_1 satisfying

$$\varepsilon_i < t_0 < t < t' < t_1 < \varepsilon_{i+1}$$

and define the matrix $\boldsymbol{\lambda} \in \mathbb{R}^{q \times (2m+2)}$ whose l th row λ_l is given by

$$\lambda_l := \begin{cases} (0, \varepsilon_1, \delta_1, \dots, \varepsilon_i, \zeta, \delta_i, \varepsilon_{i+1}, \dots, \varepsilon_m, \delta_m), & \text{if } l \neq a, \\ (0, \varepsilon_1, \delta_1, \dots, \varepsilon_i, t_0, t_1, \varepsilon_{i+1}, \dots, \varepsilon_m, \delta_m), & \text{if } l = a. \end{cases} \quad (2.26)$$

By construction, this $\boldsymbol{\lambda}$ satisfies **(2.12)**. We will assume these conventions throughout this subsection without further mentioning them explicitly. The matrix $\boldsymbol{\lambda}$ determines the $(f, \boldsymbol{\lambda})$ -partition $\Pi_{f, \boldsymbol{\lambda}}$ which, as we saw in Theorem **2^{§2}6**, is a Whitney stratification of \mathbb{S}^n .

Recall the intermediate Gabrielov-Vorobjov approximations

$$\Gamma B_{\tau} := \Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \zeta, \tau}^{\mathcal{D}, i, a}(f, \Phi),$$

defined in **(2.24)**, for $\tau \in [t_0, t_1]$. These are compact subsets of \mathbb{S}^n .

Proposition 2^{S4} 4 claims that $\iota : \Gamma B_{t'} \rightarrow \Gamma B_t$ is a homotopy equivalence. The basic idea for showing this is to apply Theorem 2^{S2} 2 to the stratification provided by $\Pi_{f,\lambda}$. In a first step towards this goal, we describe how the strata $\Pi_{I,\sigma}$ of $\Pi_{f,\lambda}$ intersect ΓB_τ . The findings are summarized in the proposition below, whose easy but somewhat cumbersome proof is postponed to §2^{S4}-2.

Proposition 2^{S4} 5. [92; Proposition 3.11].

(1) ΓB_{t_0} is a union of strata of $\Pi_{f,\lambda}$.

(2) Let $\tau, \tau' \in (t_0, t_1)$. For each $\Pi_{I,\sigma} \in \Pi_{f,\lambda}$ such that $\Pi_{I,\sigma} \subseteq \Gamma B_{t_0}$, the following holds:

(i) $\Pi_{I,\sigma} \cap \Gamma B_\tau = \emptyset$ if and only if $\Pi_{I,\sigma} \cap \Gamma B_{\tau'} = \emptyset$. In this case, $\Pi_{I,\sigma} \subseteq |f_a|^{-1}(t_0)$.

(ii) $\Pi_{I,\sigma} \cap \Gamma B_\tau = \Pi_{I,\sigma}$ if and only if $\Pi_{I,\sigma} \cap \Gamma B_{\tau'} = \Pi_{I,\sigma}$.

(iii) If $\emptyset \neq \Pi_{I,\sigma} \cap \Gamma B_\tau \subsetneq \Pi_{I,\sigma}$, then $\Pi_{I,\sigma} \subseteq |f_a|^{-1}(t_0, t_1)$ and

$$\Pi_{I,\sigma} \cap \Gamma B_\tau = \Pi_{I,\sigma} \cap \{x \in \mathbb{S}^n \mid |f_a(x)| \geq \tau\}.$$

Homotopies preserving $\Pi_{f,\lambda}$

We are now going to construct the maps and homotopies to show that the inclusion $\iota : \Gamma B_{t'} \rightarrow \Gamma B_t$ is a homotopy equivalence. For this, we should construct a continuous map $\rho : \Gamma B_t \rightarrow \Gamma B_{t'}$ and homotopies between the compositions of these maps and the identity maps.

A first approach would be to move around the points of $\Gamma B_t \setminus \Gamma B_{t'}$ and then extend the maps obtained continuously to the whole space. It is easier though to work in the larger space $\Gamma B_{t_0} \cap |f_a|^{-1}(t_0, t_1)$, where we can control what happens at the boundary and thus obtain the continuous extensions.

Consider the open subset $\mathcal{M} := \mathbb{S}^n \setminus f_a^{-1}(0)$ of \mathbb{S}^n together with the smooth map $\mathcal{M} \rightarrow \mathbb{R}$, $s \mapsto |f_a(s)|$, as well as the locally closed set

$$\Omega := \Gamma B_{t_0} \cap |f_a|^{-1}(t_0, t_1) \subseteq \mathcal{M}.$$

By Proposition 2^{S4} 5(1), Ω is the union of certain strata $\Pi_{I,\sigma}$ of $\Pi_{f,\lambda}$, namely of those strata on which $|f_a|$ takes values in (t_0, t_1) . We note that the restriction of $|f_a|$,

$$\begin{aligned} \alpha : \Omega &\rightarrow (t_0, t_1) \\ x &\mapsto |f_a(x)|, \end{aligned}$$

is a proper map. Indeed, the inverse image $\alpha^{-1}(J) = \{x \in \Gamma B_{t_0} \mid f_a(x) \in J\}$ of a compact subset $J \subseteq (t_0, t_1)$ is a closed subset of the compact set ΓB_{t_0} and thus compact itself.

By Theorem 2^{S2} 6, $\Pi_{f,\lambda}$ restricts to a Whitney stratification of Ω and the map α satisfies the hypothesis of Thom's first isotopy lemma (Theorem 2^{S2} 2). Therefore, there is a subset $F \subseteq \Omega$ and a homeomorphism $h : \Omega \rightarrow F \times (t_0, t_1)$ such that the following diagram commutes

$$\begin{array}{ccc} \Omega & \xrightarrow{h} & F \times (t_0, t_1) \\ & \searrow \alpha & \downarrow \pi_{(t_0, t_1)} \\ & & (t_0, t_1). \end{array}$$

Moreover, the stratum in which $x \in \Omega$ lies only depends on $h_F(x)$, that is, if $h_F(x) = h_F(y)$ then x and y belong to the same stratum of $\Pi_{f,\lambda}$. This is so because h is a stratified homeomorphism by Thom's first isotopy lemma (Theorem 2^{S2}2).

Consider the following continuous (piecewise linear) map

$$\begin{aligned} v : [0, 1] \times [t_0, t_1] &\rightarrow [t_0, t_1] \\ (s, y) &\mapsto \begin{cases} y & \text{if } y \in [t', t_1], \\ (1-s)y + st' & \text{if } y \in [t, t'], \\ \frac{t_0+t}{2} + \left((1-s) + s \frac{2t'-t-t_0}{t-t_0} \right) \left(y - \frac{t_0+t}{2} \right) & \text{if } y \in [(t_0+t)/2, t], \\ y & \text{if } y \in [t_0, (t_0+t)/2]. \end{cases} \end{aligned}$$

One easily verifies that this map restricts to a continuous retraction of $[t, t_1]$ onto $[t', t_1]$ that leaves fixed all points in a neighborhood of $\{t_0, t_1\}$. With the help of v , one defines the continuous map

$$\begin{aligned} \psi : [0, 1] \times \Omega &\rightarrow \Omega \\ (s, x) &\mapsto \begin{cases} x, & \text{if } \alpha(x) \notin ((t_0+t)/2, (t_1+t')/2), \\ h^{-1}(h_F(x), v(s, \alpha(x))), & \text{otherwise.} \end{cases} \end{aligned}$$

The properties of v and h imply that this map restricts to a continuous retraction of $\alpha^{-1}[t, t_1]$ onto $\alpha^{-1}[t', t_1]$ that leaves fixed all points in a neighborhood of the boundary $\partial\Omega \cap \Gamma B_{t_0}$ of Ω in ΓB_{t_0} (note $\partial\Omega \subseteq |f_a|^{-1}(\{t_0, t_1\})$).

We also have that $\psi(s, \Pi_{I,\sigma}) \subseteq \Pi_{I,\sigma}$ for all $s \in [0, 1]$, provided $\Pi_{I,\sigma} \subseteq \Omega$. This is so, because the value $h_F(x)$ determines the stratum to which x belongs and moreover $h_F(\psi(s, x)) = h_F(x)$.

Since ψ fixes all points in a neighborhood of $\partial\Omega \cap \Gamma B_{t_0}$, it can be extended to the continuous map

$$\begin{aligned} \Psi : [0, 1] \times \Gamma B_{t_0} &\rightarrow \Gamma B_{t_0} \\ (s, x) &\mapsto \begin{cases} \psi(s, x), & \text{if } x \in \Omega, \\ x, & \text{otherwise.} \end{cases} \end{aligned}$$

As we are extending by the identity, all properties of ψ are inherited by Ψ . In other words, Ψ restricts to a continuous retraction of $\Gamma B_{t_0} \cap |f_a|^{-1}[t, \infty) = (\Gamma B_{t_0} \setminus \Omega) \cup \alpha^{-1}[t, t_1]$ onto $\Gamma B_{t_0} \cap |f_a|^{-1}[t', \infty)$ and it preserves the stratification $\Pi_{f,\lambda}$, i.e., we have $\Psi(s, \Pi_{I,\sigma}) \subseteq \Pi_{I,\sigma}$, for all $\Pi_{I,\sigma} \in \Pi_{f,\lambda}$ contained in ΓB_{t_0} and all $s \in [0, 1]$.

We are now ready to conclude. However, as a warning, we note that Ψ does not give a continuous retraction of ΓB_t onto $\Gamma B_{t'}$. The reason is that $\Gamma B_\tau = \Gamma B_{t_0} \cap |f_a|^{-1}[\tau, \infty)$ generally does not hold!

Proof of Proposition 2^{S4}4. We first show that for all $s \in [0, 1]$,

$$\Psi(s, \Pi_{I,\sigma} \cap \Gamma B_t) \subseteq \Pi_{I,\sigma} \cap \Gamma B_t \quad \text{and} \quad \Psi(s, \Pi_{I,\sigma} \cap \Gamma B_{t'}) \subseteq \Pi_{I,\sigma} \cap \Gamma B_{t'}.$$

By Proposition 2^{S4}5(2), there are three possible cases for each of these intersections. We only focus on the third one, (iii), since the other two cases are straightforward. In this

case, we have $\Pi_{\mathbf{I}, \sigma} \cap \Gamma B_t = \Pi_{\mathbf{I}, \sigma} \cap \{x \mid |f_a(x)| \geq t\}$ and $|f_a|(\Pi_{\mathbf{I}, \sigma}) \subseteq (t_0, t_1)$. Thus $\Pi_{\mathbf{I}, \sigma} \subseteq \Omega$ and

$$\Pi_{\mathbf{I}, \sigma} \cap \Gamma B_t = \Pi_{\mathbf{I}, \sigma} \cap |f_a|^{-1}[t, \infty).$$

Since this is the case, again by Proposition 2^{S4}5(2), the same happens for t' and so

$$\Pi_{\mathbf{I}, \sigma} \cap \Gamma B_{t'} = \Pi_{\mathbf{I}, \sigma} \cap |f_a|^{-1}[t', \infty).$$

Since Ψ gives a deformation retract of $\Gamma B_{t_0} \cap \alpha^{-1}[t, t_1]$ onto $\Gamma B_{t_0} \cap \alpha^{-1}[t', t_1]$, it preserves the stratification $\Pi_{f, \lambda}$, and moreover Ψ gives a continuous retraction of $\Pi_{\mathbf{I}, \sigma} \cap |f_a|^{-1}[t, \infty) = \Pi_{\mathbf{I}, \sigma} \cap (\Gamma B_{t_0} \cap |f_a|^{-1}[t, \infty))$ onto $\Pi_{\mathbf{I}, \sigma} \cap |f_a|^{-1}[t', \infty)$. Hence Ψ must preserve $\Pi_{\mathbf{I}, \sigma} \cap \Gamma B_t$ and $\Pi_{\mathbf{I}, \sigma} \cap \Gamma B_{t'}$ and we have shown the claim.

We conclude that $\Psi(s, \Gamma B_t) \subseteq \Gamma B_t$ and $\Psi(s, \Gamma B_{t'}) \subseteq \Gamma B_{t'}$ for all $s \in [0, 1]$.

This allows us to restrict Ψ to obtain continuous maps

$$\begin{aligned} \Theta : [0, 1] \times \Gamma B_t &\rightarrow \Gamma B_t & \text{and} & \Theta' : [0, 1] \times \Gamma B_{t'} &\rightarrow \Gamma B_{t'} \\ (s, x) &\mapsto \Psi(s, x) & & (s, x) &\mapsto \Psi(s, x). \end{aligned}$$

Let $\rho : \Gamma B_t \rightarrow \Gamma B_{t'}$ be the continuous surjection given by

$$x \mapsto \Psi(1, x).$$

By examining the three cases of Proposition 2^{S4}5(2), we see that ρ is well-defined. Recall that $\iota : \Gamma B_{t'} \rightarrow \Gamma B_t$ is the inclusion map. By construction, we have

$$\Theta_0 = \text{id}_{\Gamma B_t}, \quad \Theta_1 = \rho = \iota \circ \rho, \quad \Theta'_0 = \text{id}_{\Gamma B_{t'}}, \quad \text{and} \quad \Theta'_1 = \rho \circ \iota.$$

Hence, both $(\text{id}_{\Gamma B_t}, \iota \circ \rho)$ and $(\text{id}_{\Gamma B_{t'}}, \rho \circ \iota)$ are pairs of homotopic maps. Thus ι induces a homotopy equivalence as desired. \square

Intersecting ΓB with strata (Proof of Proposition 2^{S4}5)

Arguing as in the proof of Lemma 2^{S2}3, we can assume, without loss of generality, that Φ is already in saturated normal form, since this does not change any of the ΓB -sets. So we write

$$\Phi \equiv \bigvee_{\xi \in \Xi} \phi_\xi$$

where each ϕ_ξ is saturated.

As we can take out unions in (2.24), we have

$$\Gamma B_\tau = \Gamma B_{\delta, \epsilon, \zeta, \tau}^{\mathcal{D}, i, a}(f, \Phi) = \bigcup_{\xi \in \Xi} \left(\Gamma B_{\delta_i, \epsilon_i, \zeta, \tau}^{\mathcal{D}, a}(f, \phi_\xi) \cup \bigcup_{j \neq i} \Gamma B_{\delta_j, \epsilon_j}(f, \phi_\xi) \right). \quad (2.27)$$

Hence it is enough to consider how the different strata intersect with the sets in the right-hand side. This is done in Lemmas 2^{S4}6, 2^{S4}7, and 2^{S4}8 below. We recall that we assume $\|f_a\|_W = 1$ without loss of generality.

The first lemma deals with the ΓB blocks of the form $\Gamma B_{\delta_j, \epsilon_j}(f, \phi_\xi)$ with $j \neq i$, the second lemma with those of the form $\Gamma B_{\delta_i, \epsilon_i, \zeta, t_0}^{\mathcal{D}, a}$, and the third lemma with those of the form $\Gamma B_{\delta_i, \epsilon_i, \zeta, \tau}^{\mathcal{D}, a}$ with $\tau \in (t_0, t_1)$. Of these, the third lemma is the most delicate one, as in this case, the ΓB blocks do not decompose as a union of strata.

Lemma 2^{S4} 6. [92; Lemma 3.12]. Let ϕ be a saturated formula over f , let $j \neq i$ and put $\delta := \delta_j$, $\varepsilon := \varepsilon_j$. For every $\eta_{I,\sigma} \in \Pi_{f,\lambda}$ the following are equivalent:

- (0I1) $\eta_{I,\sigma} \cap \Gamma B_{\delta,\varepsilon}(f, \phi) \neq \emptyset$.
- (0I2) $\eta_{I,\sigma} \subseteq \Gamma B_{\delta,\varepsilon}(f, \phi)$.
- (0I3) $\text{sgn}(\phi) \leq \sigma$ and for all $I \in [q]$,

$$\begin{cases} |f_I|/\|f_I\|_W \leq \varepsilon \text{ on } \eta_{I,\sigma}, & \text{if } \text{sgn}_I(\phi) = 0, \\ |f_I|/\|f_I\|_W \geq \delta \text{ on } \eta_{I,\sigma}, & \text{if } \text{sgn}_I(\phi) \neq 0. \end{cases}$$

Proof. The chain of implications from (0I3) to (0I2) to (0I1) follows directly from the definition of $\eta_{I,\sigma}$. Therefore we only show that (0I1) implies (0I3).

Let $x \in \eta_{I,\sigma} \cap \Gamma B_{\delta,\varepsilon}(f, \phi)$. For each $I \in [q]$, we distinguish three cases:

- +) If $\text{sgn}_I(\phi) = 1$, then $x \in \Gamma B_{\delta,\varepsilon}(f, \phi)$ implies $|f_I(x)|/\|f_I\|_W \geq \delta$. Therefore, $\sigma_I = \text{sgn}(f_I(x)) = 1 \geq 1 = \text{sgn}_I(\phi)$ and $|f_I|/\|f_I\|_W \geq \delta$ on $\eta_{I,\sigma}$. The latter because δ appears in λ , and so either all $x \in \eta_{I,\sigma}$ satisfy $|f_I(x)|/\|f_I\|_W \geq \delta$ or none of them does.
-) If $\text{sgn}_I(\phi) = -1$, the argument is analogous to that of the case $\text{sgn}_I(\phi) = 1$.
- 0) If $\text{sgn}_I(\phi) = 0$, then $x \in \Gamma B_{\delta,\varepsilon}(f, \phi)$ implies $|f_I(x)|/\|f_I\|_W \leq \varepsilon$. This, in turn, implies $|f_I|/\|f_I\|_W \leq \varepsilon$ on $\eta_{I,\sigma}$, since ε appears in λ , and so either all $x \in \eta_{I,\sigma}$ satisfy this or none does. Also $0 \leq 0, +1, -1$, and so $\text{sgn}(f_I(x)) \leq \sigma_I$.

□

Lemma 2^{S4} 7. [92; Lemma 3.13]. Let ϕ be a saturated formula over f . For every $\eta_{I,\sigma} \in \Pi_{f,\lambda}$, the following are equivalent:

- (1I1) $\eta_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, t_0}^{\mathcal{D}, a}(f, \phi) \neq \emptyset$.
- (1I2) $\eta_{I,\sigma} \subseteq \Gamma B_{\delta_i, \varepsilon_i, \zeta, t_0}^{\mathcal{D}, a}(f, \phi)$.
- (1I3) $\text{sgn}(\phi) \leq \sigma$ and, for all $I \in [q]$,

$$\begin{cases} |f_I|/\|f_I\|_W \leq \varepsilon_i \text{ on } \eta_{I,\sigma}, & \text{if } \text{sgn}_I(\phi) = 0, \\ |f_I|/\|f_I\|_W \geq \delta_i \text{ on } \eta_{I,\sigma}, & \text{if } \text{sgn}_I(\phi) \neq 0 \text{ and } I > a, \\ |f_I|/\|f_I\|_W \geq t_0 \text{ on } \eta_{I,\sigma}, & \text{if } \text{sgn}_I(\phi) \neq 0 \text{ and } I = a, \\ |f_I|/\|f_I\|_W \geq \zeta \text{ on } \eta_{I,\sigma}, & \text{if } \text{sgn}_I(\phi) \neq 0 \text{ and } I < a. \end{cases}$$

Proof. The proof is analogous to that of Lemma 2^{S4} 6, but longer as we must now divide into cases depending not only on $\text{sgn}_I(\phi)$ but also on whether $I > a$, $I = a$ or $I < a$. □

Lemma 2^{S4} 8. [92; Lemma 3.14]. Let ϕ be a saturated formula over f and $s \in (t_0, t_1)$. For every $\eta_{I,\sigma} \in \Pi_{f,\lambda}$ the following are equivalent:

- (2I1) $\eta_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, s}^{\mathcal{D}, a}(f, \phi) \neq \emptyset$.

(2I2) $\operatorname{sgn}(\phi) \leq \sigma$ and for all $I \in [q]$,

$$\begin{cases} |f_I|/\|f_I\|_W \leq \varepsilon_i \text{ on } \Pi_{I,\sigma}, & \text{if } \operatorname{sgn}_I(\phi) = 0, \\ |f_I|/\|f_I\|_W \geq \delta_i \text{ on } \Pi_{I,\sigma}, & \text{if } \operatorname{sgn}_I(\phi) \neq 0 \text{ and } I > a, \\ |f_I|/\|f_I\|_W > t_0 \text{ on } \Pi_{I,\sigma}, & \text{if } \operatorname{sgn}_I(\phi) \neq 0 \text{ and } I = a, \\ |f_I|/\|f_I\|_W \geq \zeta \text{ on } \Pi_{I,\sigma}, & \text{if } \operatorname{sgn}_I(\phi) \neq 0 \text{ and } I < a. \end{cases}$$

Additionally, if any of the two claims above holds,

$$\Pi_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, \tau}^{\mathcal{D}, a}(f, \phi) = \begin{cases} \Pi_{I,\sigma} \cap \{x \in \mathbb{S}^n \mid |f_a(x)| \geq \tau\}, & \text{if } |f_a|(t_0, t_1) \subseteq \Pi_{I,\sigma}, \\ \Pi_{I,\sigma}, & \text{otherwise.} \end{cases} \quad (2.28)$$

Proof. The implication from (2I1) to (2I2) is shown in a similar way as those from (0I1) to (0I3) in Lemma 2^{§4}6 and from (1I1) to (1I3) in Lemma 2^{§4}7. We next prove the reverse implication.

Assume then that (2I2) holds. From the conditions there and the definition of both $\Pi_{I,\sigma}$ and $\Gamma B_{\delta_i, \varepsilon_i, \zeta, s}^{\mathcal{D}, a}(f, \phi)$, it follows that

$$\Pi_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, s}^{1, a}(f, \phi) = \Pi_{I,\sigma} \cap \{x \in \mathbb{S}^n \mid |f_a(x)| \geq s\}. \quad (2.29)$$

We next divide in cases depending on whether $\Pi_{I,\sigma} \subseteq |f_a|^{-1}(t_0, t_1)$ or not.

⊓ If $|f_a|(t_0, t_1) \not\subseteq \Pi_{I,\sigma}$, then $|f_a| \geq t_1$ on $\Pi_{I,\sigma}$, by (2I2), since t_1 is the next value in λ_a . This shows that

$$\Pi_{I,\sigma} \cap \{x \in \mathbb{S}^n \mid |f_a(x)| \geq s\} = \Pi_{I,\sigma}. \quad (2.30)$$

As $\Pi_{I,\sigma}$ is non-empty, (2I1) follows from (2.29) and (2.30).

⊓ If, instead, $|f_a|(t_0, t_1) \subseteq \Pi_{I,\sigma}$ then, by Theorem 2^{§2}6(2), the map

$$\begin{aligned} \Pi_{I,\sigma} &\rightarrow (t_0, t_1) \\ x &\mapsto |f_a(x)| \end{aligned}$$

is surjective. Hence $\Pi_{I,\sigma} \cap \{x \in \mathbb{S}^n \mid |f_a(x)| \geq \tau\}$ is non-empty and (2I1) also follows in this case.

We have proved (2.28) in passing. \square

Now we finish the proof of Proposition 2^{§4}5 with the help of the above three lemmas.

Proof of Proposition 2^{§4}5. Part (1) follows directly from Lemmas 2^{§4}6 and 2^{§4}7 since these lemmas guarantee that each set in the right-hand side of (2.27) is a union of strata.

We now show part (2). Consider the intersections of $\Pi_{I,\sigma}$ with the decomposition (2.27) for ΓB_τ and ΓB_{t_0} .

If for some $j \neq i$ and $\xi \in \Xi$ we have $\Pi_{I,\sigma} \cap \Gamma B_{\delta_j, \varepsilon_j}(f, \phi_\xi) \neq \emptyset$, then this intersection equals $\Pi_{I,\sigma}$ by Lemma 2^{§4}6 and all the claims of (2) hold trivially since $\Pi_{I,\sigma} \cap \Gamma B_{\delta_j, \varepsilon_j}(f, \phi_\xi)$ does not depend on the value of τ .

Assume instead that for all $j \neq i$ and $\xi \in \Xi$ we have $\Pi_{I,\sigma} \cap \Gamma B_{\delta_j, \varepsilon_j}(f, \phi_\xi) = \emptyset$. Then

$$\Pi_{I,\sigma} \cap \Gamma B_\tau = \bigcup_{\xi \in \Xi} \Pi_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, \tau}^{\mathcal{D}, a}(f, \phi_\xi)$$

and

$$\Pi_{I,\sigma} \cap \Gamma B_{t_0} = \bigcup_{\xi \in \Xi} \Pi_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, t_0}^{\mathcal{D}, a}(f, \phi_\xi).$$

By hypothesis on $\Pi_{I,\sigma}$, we have $\Pi_{I,\sigma} \cap \Gamma B_{t_0} = \Pi_{I,\sigma} \neq \emptyset$ which implies that there exists $\xi \in \Xi$ such that $\Pi_{I,\sigma} \cap \Gamma B_{\delta_i, \varepsilon_i, \zeta, t_0}^{\mathcal{D}, a}(f, \phi_\xi) \neq \emptyset$. Lemma 2^{§4}7 then ensures that the conditions in (1I3) hold true. But these conditions are the same as those in Lemma 2^{§4}8(2I2) except for $I = a$, where the inequality is strict in the latter and lax in the former. This means that $\Pi_{I,\sigma} \cap \Gamma B_{\delta, \varepsilon, \zeta, \tau}^{\mathcal{D}, i, a}(f, \Phi) = \emptyset$ if and only if $|f_a| = t_0$ on $\Pi_{I,\sigma}$. Furthermore, this latter condition is independent of the particular value of τ . If it holds for τ , then it holds for τ' and viceversa. This proves the first claim of (2).

Arguing as above, we have that $\Pi_{I,\sigma} \cap \Gamma B_{\delta, \varepsilon, \zeta, s}^{\mathcal{D}, i, a}(f, \Phi) = \Pi_{I,\sigma}$ if and only if $|f_a| \geq t_1$ on $\Pi_{I,\sigma}$. As this does not depend on the value of τ , we get the second claim of (2).

The third claim of (2) follows directly from the last statement of Lemma 2^{§4}8. \square

Further comments

The results in this chapter go back to [88], Proposition 2^{§1}3; to [91], quantitative Durfee's theorem (Theorem 2^{§3}2); and to [92], quantitative Gabrielov-Vorobjov approximation theorem (Theorem 2^{§4}2). However, the proofs of some of these results are very different.

The original proof of the Proposition 2^{§1}3 in [88] used a continuous version of Smale's α -theory (see [88; §3.2 and §4.2]), and it only applies to semialgebraic sets in which $t = 0$. In contrast to this, our proof used a discontinuous version of the Newton vector field. Further, we were able to improve the inequality from the original $13D^{\frac{3}{2}}\bar{\kappa}(f)^2r < 1$ in [88; Theorem 4.19] to the current $\sqrt{2}\bar{\kappa}(f)r < 1$, in the case $t = 0$.

The proof of Durfee's theorem (Theorem 2^{§3}2) differs significantly from that in [91] (including the adaptation sketched in [92]). Instead of doing the continuous retraction in one step (as done in [91]), we divide it into different steps. This different proof strategy makes the proof more similar to that of the Gabrielov-Vorobjov approximation theorem (Theorem 2^{§4}2), which helps to introduce the proof of this theorem.

The proof given of the Gabrielov-Vorobjov approximation theorem (Theorem 2^{§4}2) is almost identical to that in [92]. Further, there are no significant differences between the two expositions and, except for some minor changes, the text is the same as that of [92].

On top of these differences, we have enlarged significantly the exposition of the Mather-Thom theory done in [91, 92]. Apart from being more systematic, we add some new examples and theorems (such as Theorem 1^{§2}2 and 1^{§3}2) to illustrate better the applications and use of this theory. Further, the reader should note in the proofs of this chapter a repetitive style. This style was intentional and it was to emphasize the main ideas and techniques behind the application of Mather-Thom theory.

Pointiller, est le mode d'expression choisi par le peintre qui pose de la couleur sur une toile par petits points plutôt que de l'étaler à plat.

Paul Signac, D'Eugène Delacroix au néo-impressionnisme

3

Computing the homology of a set *par pointillage*

The idea of approximating images by dots is an old one. This variant of approximating the continuous by the discrete made its first appearance in the mosaics of Antiquity. In engraving, it was introduced by Giulio Campagnola, Ottavio Leoni and others in the 15th century, and it was later perfected, under the name of *stipple engraving*, by Jean Charles Françoise, William Wynne Ryland and Francesco Bartolozzi in the 18th century [Q13; Ch. IX]. In painting, it was introduced, with special attention to the colors, by Georges Seurat and Paul Signac in the 1880s [Q14], marking the birth of the *divisionism* (also called, contemptuously then and popularly now, *pointillism*).

Aside from the history of art, Paul Nipkow was the first in conceiving with his *Elektrisches Teleskop* in 1884 that an image could be recorded using a finite set of *pixels* (*Bildpunkte* for him) [Q10]. His design became the germ that, after the contributions of too many inventors to mention them one by one, gave origin to the screens that inhabit our technological world. In these screens, the paradoxical illusion of a continuous image made out of discrete dots shows how well the discrete can approximate the continuous.

At the beginning of the 21st century, the above idea became the foundation of topological data analysis. In their study of dynamical systems coming from physics, Muldoon, MacKay, Huke and Broomhead [295] had the idea of extracting topological information about the attractor of the system from time-series of data coming from experiments. Although this marks the beginning of topological analysis, they were Robins [333], relying on work by Robins, Meiss and Bradley [334, 335], and Edelsbrunner, Letscher and Zomorodian [168, 168] who laid, respectively, the theoretical and algorithmic foundations of this area.

Nowadays, topological data analysis is an established area of mathematics dealing with theoretical, computational and applied questions about the topological information that can be extracted about a set from a finite cloud of points approximating it. In this chapter, we

will expose the ideas and techniques from topological analysis that we will use. Our intention is not to be complete, but to introduce exactly what we will use later, trying to give some intuition on the techniques.

First, we introduce the Hausdorff distance, the reach and the Niyogi-Smale-Weinberger approximation theorem which allow us to guarantee that an approximation is topologically good; second, we develop some explicit lower bounds¹ on the reach that will allow us to control the size of the approximation explicitly; and third and last, we introduce the Nerve theorem and other algebraic topological results that will allow us to go from the approximation to the homology computationally.

3§1 Approximation of sets by clouds of points

The fundamental result of this section is the Niyogi-Smale-Weinberger theorem (Theorem 3§1 8) of Niyogi, Smale and Weinberger [300, 301] which gives precise sufficient conditions for when a cloud of points is a good topological approximation of a set in terms of two numerical quantities: the Hausdorff distance and the reach.

3§1–1 Hausdorff distance

The Hausdorff distance is one of the possible distances that one can consider between sets of a metric space. It is based on the simple idea that two sets X and Y are near if every point of X is near Y and every point of Y is near of X . Note that this is different from the usual distance between sets,

$$\text{dist}(X, Y) := \inf\{\text{dist}(x, y) \mid x \in X, y \in Y\},$$

for which X and Y are near if a point of X and a point of Y are near.

Definition 3§1.1. Let $X, Y \subseteq \mathbb{R}^m$ be non-empty compact subsets, the *Hausdorff distance* between X and Y , $\text{dist}_H(X, Y)$, is the real number given by

$$\text{dist}_H(X, Y) := \max \{\max\{\text{dist}(x, Y) \mid x \in X\}, \max\{\text{dist}(y, X) \mid y \in Y\}\} \quad (3.1)$$

where dist is the Euclidean distance in \mathbb{R}^m . By convention, we define $\text{dist}_H(\emptyset, X) = \infty$.

Recall the definition of a (*Euclidean*) r -neighborhood of a compact set X ,

$$\mathcal{U}(X, r) := \{z \mid \text{dist}(z, X) \leq r\} = \bigcup_{x \in X} \overline{B}(x, r). \quad (3.2)$$

The following proposition is immediate from the above definition. It gives a useful equivalent formulation of the Hausdorff distance, which helps to develop the intuition about this notion.

Proposition 3§1.1. Let $X, Y \subseteq \mathbb{R}^m$ be compact subsets. Then the following are equivalent:

- $\text{dist}_H(X, Y) \leq r$.
- $X \subseteq \mathcal{U}(Y, r)$ and $Y \subseteq \mathcal{U}(X, r)$.

□

¹Unsurprisingly, these bounds are in terms of the condition number.

The following examples should clarify and justify the use of the Hausdorff distance in our setting.

Example 3^{§1}1. Let $X = [0, 1/2]$ and $Y = [0, 1]$ be subsets of \mathbb{R} , we can see that $\text{dist}(X, Y) = 0$ since $X \subseteq Y$, but $\text{dist}_H(X, Y) = 1/2$, since $Y \subseteq \mathcal{U}(X, r) = [-r, 1/2 + r]$ if and only if $r \geq 1/2$. This exemplifies why dist is not a good measure of how near are two sets and that the Hausdorff distance is able to distinguish a proper subset from a set. Δ

Example 3^{§1}2. Let $X_k = \frac{1}{k}\mathbb{Z} \cap [0, 1] = \{0, 1/k, 2/k, \dots, (k-2)/k, (k-1)/k, 1\}$ and $X = [0, 1]$. We can easily see that $\text{dist}_H(X_k, X) = \frac{1}{2k}$ which goes to zero as k goes to infinity. Hence, in the Hausdorff distance, X_k converges to X . Δ

The above example shows a general phenomenon. Recall that an r -net of set X is a discrete subset $N \subseteq X$ such that for every point $x \in X$, there is a point $y \in N$ such that $\text{dist}(x, y) < r$. It is easy to prove the following.

Proposition 3^{§1}2. *Let $X \subseteq \mathbb{R}^m$ be compact and $N \subset X$ be discrete. Then N is an r -net of X iff $\text{dist}_H(N, X) < r$.* \square

In this way, in the Hausdorff metric, the discrete approximations of a set converge to it. This is the main reason why we use the Hausdorff metric to measure how well a cloud of points approximates a set, since we expect that an ε -net approximates a set better as ε goes to zero. Also, it is robust in the sense that it allows N not to be included in X , as long as it is close to X .

We conclude with the following theorem. On the one hand, it justifies why we speak about Hausdorff distance or metric; on the other hand, it shows that the Hausdorff distance is a metric with very good properties.²

Theorem 3^{§1}3. *[360; Theorems 7.3.1 and 10.7.2] Let $S \subseteq \mathbb{R}^m$ and $\mathcal{K}(S)$ denote the set of non-empty compact subsets of S . Then dist_H is a metric on $\mathcal{K}(S)$. Further, (S, dist) is complete (i.e., S is closed) if and only if $(\mathcal{K}(S), \text{dist}_H)$ is complete.* \square

3^{§1}-2 Nearest-point retraction and reach

In a metric space, like \mathbb{R}^m , Urysohn's lemma is an easy exercise for students as every closed subset X is just the zero set of the non-negative Lipschitz function $\text{dist}_X : z \mapsto \text{dist}(z, X)$. One can see that the neighborhoods $\mathcal{U}(X, r)$ are just the sublevel sets of this function. For small r , we might expect that the topologies of $\mathcal{U}(X, r)$ and of X to be similar, and this can be made precise in topological terms for arbitrary closed sets [333]. However, we will concern ourselves with a restricted class of closed subsets for which we can answer positively the following question: how small should $r > 0$ should be so that X and $\mathcal{U}(X, r)$ have the same homotopy type?

Our approach to answer this question goes back to Federer [177] and relies on the so-called nearest-point retraction.

Definition 3^{§1}2. Let $X \subseteq \mathbb{R}^m$ be closed, the *nearest-point retraction* is the partial map $\pi_X : \mathbb{R}^m \rightarrow X$ defined by

$$\pi_X(z) := \arg \min \{\text{dist}(z, x) \mid x \in X\}. \quad (3.3)$$

²We state the result for subsets of \mathbb{R}^m for concreteness, but it holds for general metric spaces.

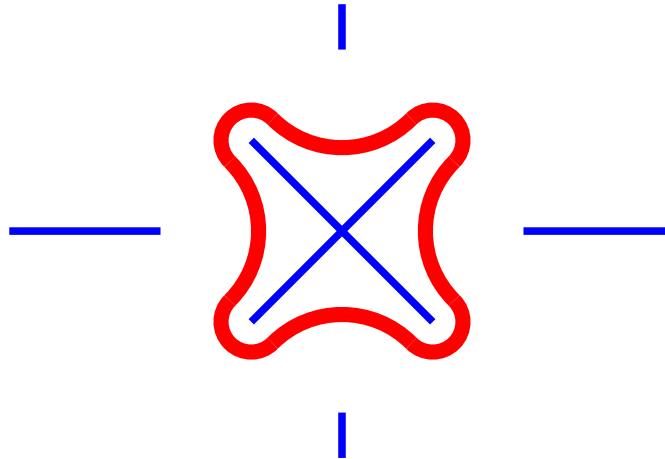


Figure 3§1: X , in red, and part of its medial axis, Δ_X , in blue.

The *medial axis* of X , Δ_X , is the set of those points of \mathbb{R}^m for which π_X is not defined.

Note that $\pi_X(z)$ is the nearest point in X to z , and that this is well-defined if and only if this point is unique. With this observation, we can easily see that

$$\Delta_X = \{z \in \mathbb{R}^m \mid \exists x, \tilde{x} \in X : x \neq \tilde{x} \text{ and } \text{dist}(z, x) = \text{dist}(z, \tilde{x}) = \text{dist}_X(z)\}, \quad (3.4)$$

i.e., that Δ_X is the set of those points with two or more distinct nearest points in X .

Example 3§1.3. In Figure 3§1, one can see in red the set X and in blue its medial axis Δ_X . An observation that should be made in this picture is that the points of X nearer to Δ_X are those of higher curvature. Δ

Proposition 3§1.4. [177; Theorem 4.8(3,4,5)]. Let $X \subseteq \mathbb{R}^m$ be closed. Then:

- (1) The map $\pi_X : \mathbb{R}^m \setminus \Delta_X \rightarrow X$ is a surjective continuous map.
- (2) The map dist_X is a C^1 -function on the interior of $\mathbb{R}^m \setminus (\Delta_X \cup X)$ such that its gradient is given by

$$\nabla_X(z) := \frac{z - \pi_X(z)}{\text{dist}_X(z)}. \quad (3.5)$$

Proof. 1. The surjectivity is obvious, because for all $x \in X$, x is the unique nearest point in X to x and so $\pi_X(x) = x$.

To prove the continuity, we prove that π_X commutes with limits of sequences. Let $\{z_k\}$ be a sequence of points in $\mathbb{R}^m \setminus \Delta_X$ converging to $z \in \mathbb{R}^m \setminus \Delta_X$. Then,

$$\begin{aligned} \text{dist}(\pi_X(z_k), z) &\leq \text{dist}(\pi_X(z_k), z_k) + \text{dist}(z_k, z) \\ &= \text{dist}(z_k, X) + \text{dist}(z_k, z) \leq \text{dist}(z, X) + 2 \text{dist}(z_k, z) \end{aligned}$$

where the first inequality is the triangle inequality, the second one the fact that $u \mapsto \text{dist}(u, X)$ is 1-Lipschitz, and the equality is by the definition of π_X . Since $\{z_k\}_k$ is convergent, $\{\text{dist}(z_k, z)\}_k$ converges to zero. Therefore, on the one hand, $\{\pi_X(z_k)\}_k$ is bounded, and, on the other hand, for every limit point x_* of $\{\pi_X(z_k)\}_k$,

$$\text{dist}(x_*, z) \leq \text{dist}(z, X).$$

The latter implies that $x_* = \pi_X(z)$ since $\pi_X(z)$ is the unique minimizer of $X \ni x \mapsto \text{dist}(x, z)$. We have just proven that $\{\pi_X(z_k)\}$ is a bounded sequence with the unique limit point $\pi_X(z)$. Thus $\lim_{k \rightarrow \infty} \pi_X(z_k) = \pi_X(z)$, as we wanted to show.

2. Observe that dist_X is a 1-Lipschitz function. Also, note that for all $z \in \mathbb{R}^m \setminus \Delta_X$ and all $\lambda \in [0, 1]$,

$$\text{dist}_X((1 - \lambda)z + \lambda\pi_X(z)) = \lambda \text{dist}_X(z),$$

since, otherwise, there will be a nearer point to z in X distinct from $\pi_X(z)$.

By the above, we obtain that for all sufficiently small $t \geq 0$,

$$\text{dist}_X(z - t\nabla_X(z)) = \text{dist}_X(z) - t.$$

Therefore, if dist_X is differentiable at z , then

$$D_z \text{dist}_X(\nabla_X(z)) = 1.$$

But, since $\|D_z \text{dist}_X\| \leq 1$ by the 1-Lipschitzness of dist_X , we must have

$$D_z \text{dist}_X = \nabla_X(z)^*$$

whenever dist_X is differentiable at z .

Finally, since dist_X is Lipschitz, dist_X is differentiable almost everywhere by Rademacher's theorem [217; Theorem 3.1]. But then, by the Fundamental Theorem of Calculus for Lipschitz functions [217; Theorem 3.3] we have that dist_X is differentiable and that ∇_X is its gradient on $\mathbb{R}^M \setminus (X \cup \Delta_X)$, since ∇_X is continuous. \square

This means that as long as we are away from Δ_X , the nearest-point retraction π_X is a good map and it points to the direction we must take to decrease the distance to X the fastest possible way.

Reach

To measure how far from the set the nearest point retraction is defined, one considers the notion of reach.

Definition 3^{§1} 3. [177]. Let $X \subseteq \mathbb{R}^m$ be a closed set. The *local reach* of X at $x \in X$, $\tau(X, x)$, is the non-negative quantity

$$\tau(X, x) := \text{dist}(x, \Delta_X) \tag{3.6}$$

and the *reach* (or *local feature size*) of X , $\tau(X)$, is the non-negative quantity

$$\tau(X) := \inf_{x \in X} \tau(X, x) = \text{dist}(X, \Delta_X). \tag{3.7}$$

The reach is precisely the quantity we were looking for.

Proposition 3^{§1} 5. [88; Proposition 2.2]. Let $X \subseteq \mathbb{R}^m$ be a closed subset such that $\tau(X) > 0$. Then for all $r \in (0, \tau(X))$,

$$\begin{aligned} H_X : [0, 1] \times \mathcal{U}(X, r) &\rightarrow \mathcal{U}(X, r) \\ (t, z) &\mapsto (1 - t)z + t\pi_X(z) \end{aligned}$$

is a continuous retraction of $\mathcal{U}(X, r)$ onto X . In particular, for all $r \in (0, \tau(X))$, $X \hookrightarrow \mathcal{U}(X, r)$ is an homotopy equivalence.

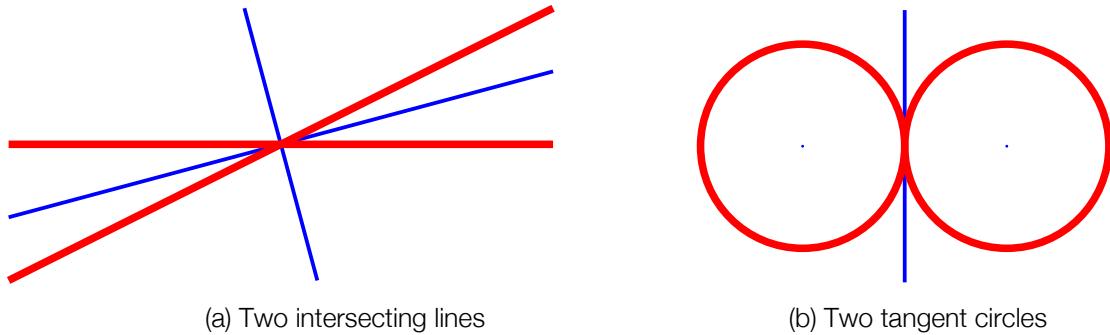


Figure 3§1 2: Sets with reach zero, in red, and their medial axis in blue

Proof. Since $\text{dist}(H_X(t, z), \pi_X(z)) \leq (1-t) \text{dist}(z, \pi_X(z)) = (1-t) \text{dist}_X(z) = (1-t)r \leq r$, H_X is well-defined. The continuity of H_X follows from Proposition 3§1 4 and that is a retraction from the fact that for all $x \in X$, $\pi_X(x) = X$. \square

Observation 3§1 1. Note that an alternative way to define H_X for (t, z) with $z \notin X$ is by

$$H_X(t, z) = z - t \text{dist}_X(z) \nabla_X(z).$$

Since ∇_X is the gradient of dist_X , this shows that we have just done gradient descent. \P

There are many sets with positive reach, among them the ones with maximum reach, i.e., reach equal to infinity, being the convex closed sets. However, let us note that not every set has positive reach as the following two examples shows.

Example 3§1 4. Consider the set which consist in two lines with an small angle of θ between them. In Figure 3§1 2a, one can see the union of the lines, X , in red and the medial axis, Δ_X , in blue. In this case, We observe that Δ_X is not closed, since it misses the intersection point of the lines, and that $\tau(X) = 0$. \triangle

Example 3§1 5. Consider the set consisting on the union of two tangent circles. As in the previous example, in Figure 3§1 2b, the set X in red and the medial axis Δ_X in blue. Similarly to the previous example, Δ_X is not closed, because it misses the intersection point of the circles, and $\tau(X) = 0$. \triangle

Normal vector and the reach along a direction

How far can we leave X from x in the direction given by a vector u before the fastest path to return to X is the reverse of the path traversed til then? This motivates the following definition, which is a directional version of the local reach at a point.

Definition 3§1 4. [177]. Let $X \subseteq \mathbb{R}^m$ be a compact set, $x \in X$ and $u \in \mathbb{S}^{m-1}$. The *local reach along u* of X at x , $\tau(X, x; u)$, is the non-negative quantity defined by

$$\tau(X, x; u) := \sup\{t \geq 0 \mid \text{dist}(x + tu, X) = t\}. \quad (3.8)$$

The importance of the above notion is that it will allow us to work in a easier way with the reach. The following theorem gives the best way of proving lower bounds.

Theorem 3§1 6. [88; Lemma 2.5] and [177; Theorem 4.8(6)]. Let $X \subseteq \mathbb{R}^m$ be closed, $x \in X$ and $u \in \mathbb{S}^n$. Then

- (1) $\tau(X, x; u) = \sup\{t \geq 0 \mid x + tu \notin \Delta_X \text{ and } \pi_X(x + tu) = x\}.$
- (2) If $0 < \tau(X, x; u) < \infty$, then $x + \tau(X, x; u)u \in \overline{\Delta_X}$.
- (3) If $\tau(X, x; u) > 0$, then $\tau(X, x; u) \geq \tau(X, x).$

Proof. (1) Given that $x + tu \notin \Delta_X$, $\text{dist}(x + tu, X) = t$ and $\pi_X(x + tu) = x$ are equivalent. This shows that

$$\tau(X, x; u) \geq \sup\{t \geq 0 \mid x + tu \notin \Delta_X \text{ and } \pi_X(x + tu) = x\}.$$

To prove the equality, assume that it does not hold. In this case, there is t_0 in between these two quantities. For this t_0 , on the one hand, $x + t_0u \in \Delta_X$ and $\text{dist}_X(x + t_0u) = t_0$; on the other hand, there is $\tilde{x} \in X$ different from x such that $\text{dist}(x + t_0u, \tilde{x}) = t_0$.

Let $Y = \{x, \tilde{x}\}$. Then, by elementary geometry, $H := \Delta_Y$ is a hyperplane that passes through $x + t_0u$ and whose complement is the union of two open half-spaces: U comprising those points nearer to x and \tilde{U} comprising those nearer to \tilde{x} . Clearly, $[x, x + t_0u] \subseteq U$. Therefore, for $t > t_0$ sufficiently near t_0 , $t < \tau(X, x; u)$ and

$$\text{dist}(x + tu, X) \leq \text{dist}(x + tu, \tilde{x}) < \text{dist}(x + tu, x) = t,$$

since $x + tu \in \tilde{U}$; and so

$$\text{dist}(x + \tau(X, x; u)u, X) \leq \tau(X, x; u) - t + \text{dist}_X(x + tu) < \tau(X, x; u).$$

This contradicts the definition of $\tau(X, x; u)$. Hence the equality must hold.

(2) Let $z_0 = x + \tau(X, x; u)u$. Assume that $z_0 \notin \overline{\Delta_X}$. Then, in a neighborhood of z_0 , the continuous vector field ∇_X of Proposition 3\\$1.4 is defined. By the Cauchy-Peano theorem [180; Teorema 2.2a],

$$\begin{cases} \alpha'(t) = \nabla_X(\alpha(t)) \\ \alpha(0) = z_0 \end{cases}$$

has at least one local solution $\alpha : (-\delta, \delta) \rightarrow \mathbb{R}^m$ for some $\delta > 0$.

Now, by construction of α ,

$$D_{\alpha(t)} \text{dist}_X(\alpha'(t)) = D_{\alpha(t)} \text{dist}_X(\nabla_X(\alpha(t))) = 1$$

where the last claim follows from Proposition 3\\$1.4(2). Therefore, by the chain rule,

$$(\text{dist}_X \circ \alpha)'(t) = 1 = \|\alpha'(t)\|,$$

where the last inequality follows from $\|\nabla_X\| = 1$.

By the above paragraph,

$$\int_{t_0}^{t_1} \|\alpha'(s)\| ds = \int_{t_0}^{t_1} (\text{dist}_X \circ \alpha)'(t) ds = \text{dist}_X(\alpha(t_1)) - \text{dist}_X(\alpha(t_0)) \leq \text{dist}(\alpha(t_0), \alpha(t_1)).$$

Therefore

$$\text{length } \alpha[t_0, t_1] \leq \text{dist}(\alpha(t_0), \alpha(t_1))$$

where length $\alpha[t_0, t_1]$ is the length of α between t_0 and t_1 . This means that α is a geodesic in \mathbb{R}^m with constant unit speed and so it is of the form

$$\alpha(s) = z_0 + su.$$

But then for $t > \tau(X, x; u)$ sufficiently near to $\tau(X, x; u)$,

$$\nabla_X(x + tu) = \alpha'(t - \tau(X, x; u)) = u$$

and so $\pi_X(x + tu) = x$ contradicting the equality in (1).

(3) We have that

$$\tau(X, x; u) = \text{dist}(x, x + \tau(X, x; u)u) \geq \text{dist}(x, \overline{\Delta_X}) = \text{dist}(x, \Delta_X) = \tau(X, x)$$

where the first equality comes from the definition of $\tau(X, x; u)$, and the first inequality from (2). \square

We finish this section with the following proposition which shows for which vectors u we can guarantee that $\tau(X, x; u) > 0$ when X is a locally closed submanifold around x . Given a smooth submanifold $M \subseteq \mathbb{R}^m$ and $x \in M$, recall that a *normal vector* of M at x is a vector $u \in T_x \mathbb{R}^m$ such that u is orthogonal to $T_x M$. We denote the vector subspace of normal vectors of M at x by $N_x M := T_x M^\perp$.

Proposition 3\\$1.7. *Let $M \subseteq \mathbb{R}^m$ be closed and $x \in X$ be such that M is a regular manifold around x . Then for every $u \in \mathbb{S}^{m-1}$, $\tau(X, x; u) > 0$ iff $u \in N_x M$.*

Proof. By the Constant Rank Theorem [275; Theorem 4.12], there is an open neighborhood $B(x, \varepsilon)$ of x and a smooth map $f : \mathbb{R}^n \rightarrow \mathbb{R}^q$ such that $f^{-1}(0) \cap B(x, \varepsilon) = M \cap B(x, \varepsilon)$ and such that its tangent map of f at every point $z \in B(z, \varepsilon)$, $\bar{D}_z f$, is surjective. In this neighborhood, let

$$P_{f,z} := \mathbb{I} - \bar{D}_z f^\dagger \bar{D}_z f$$

be the orthogonal projection onto $\ker \bar{D}_z f$, which for $z \in M \cap B(x, \varepsilon)$ is just the tangent space of M , $T_z M$. Note that $z \mapsto P_{f,z}$ is differentiable and that the values of its derivative when evaluated at a vector are matrices, of which we will consider the spectral norm.

Consider the following minimization problem

$$\arg \min \{ \text{dist}(x + tu, y) \mid y \in M \}$$

which for $t < \varepsilon/2$ has its solution in $M \cap B(x, \varepsilon)$. Therefore, for such t , by the Lagrange multipliers theorem [275; Exercise 11-11], we have that for any local minimizer in $y \in M \cap B(x, \varepsilon)$, $x + tu - y$ is orthogonal to $T_y M$ or, equivalently,

$$P_{f,y}(x + tu - y) = 0.$$

In the special case in which $y = x$, this gives $P_{f,y}u = 0$ and so $u \in N_x M$ showing one of the implications.

For the other implication, assume that $u \in N_x M$ and that there is another local minimizer $y \in M \cap B(x, \varepsilon)$ different from x . Then

$$y - x + \bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_y f(x - y) - \bar{D}_y f^\dagger f(x) = P_{f,y}(y - x) = t P_{f,y}u = t(P_{f,y} - P_{f,x})u$$

since $f(x) = f(y) = 0$ and $P_{f,x}u = 0$. On the one hand,

$$\|t(P_{f,y} - P_{f,x})u\| \leq t\|P_{f,y} - P_{f,x}\| \leq t \max_{z \in [x,y]} \left\| \bar{D}_z P_f \left(\frac{y-x}{\|y-x\|} \right) \right\| \|y-x\|,$$

where the last inequality follows from Taylor's theorem with remainder; and, on the other hand,

$$\begin{aligned} & \|y-x + \bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_y f(x-y) - \bar{D}_y f^\dagger f(x)\| \\ & \geq \left(1 - \frac{\|\bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_y f(x-y) - \bar{D}_y f^\dagger f(x)\|}{\|x-y\|} \right) \|x-y\| \\ & \geq \left(1 - \frac{1}{2} \max_{z \in [x,y]} \|\bar{D}_y f^\dagger \bar{D}_z^2 f\| \|x-y\| \right) \|x-y\|, \end{aligned}$$

because $\|\bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_y f(x-y) - \bar{D}_y f^\dagger f(x)\| \leq \frac{1}{2} \max_{z \in [x,y]} \|\bar{D}_y f^\dagger \bar{D}_z^2 f\| \|x-y\|^2$ by the Taylor theorem with remainder.

Combining these two inequalities and cancelling $\|y-x\|$, we obtain

$$t \max_{z \in [x,y]} \left\| \bar{D}_z P_f \left(\frac{y-x}{\|y-x\|} \right) \right\| \geq \left(1 - \frac{1}{2} \max_{z \in [x,y]} \|\bar{D}_y f^\dagger \bar{D}_z^2 f\| \|x-y\| \right). \quad (3.9)$$

By continuity of all terms involved, there are $\delta > 0$ and $t_0 > 0$ such that for all y such that $\|y-x\| < \delta$,

$$\max_{z \in [x,y]} \left\| \bar{D}_z P_f \left(\frac{y-x}{\|y-x\|} \right) \right\| < t_0^{-1}$$

and

$$\left(1 - \frac{1}{2} \max_{z \in [x,y]} \|\bar{D}_y f^\dagger \bar{D}_z^2 f\| \|y-x\| \right) > \frac{1}{2}.$$

This means that there can be another local minimizer y in the considered region, only if $t > t_0/2$. Hence x is the unique local minimizer for t sufficiently small, and so $\tau(X, x; u) > 0$ as desired. \square

3^{§1}-3 Niyogi-Smale-Weinberger approximation theorem

The Niyogi-Smale-Weinberger approximation theorem gives a sufficient condition for a cloud of points to approximate the homotopy type of a set. The original versions [300, 301] had more complicated inequalities and proofs than the version given here [88; Theorem 2.8] (cf. [109; Theorem 4.6]).

Theorem 3^{§1} 8 (Niyogi-Smale-Weinberger approximation theorem). [88; Theorem 2.8]. Let $X, X' \subseteq \mathbb{R}^m$ be compact sets. Assume that $\tau(X) > 0$. Then for all $\varepsilon > 0$ such that

$$3 \operatorname{dist}_H(X, X') < \varepsilon < \frac{1}{2} \tau(X), \quad (3.10)$$

X is a deformation retract of $\mathcal{U}(X, \varepsilon)$. In particular, $X \hookrightarrow \mathcal{U}(X, \varepsilon)$ is an homotopy equivalence.

Proof of Theorem 3§1.8. Note that

$$\mathcal{U}(\mathcal{X}, \varepsilon) \subseteq \mathcal{U}(\mathcal{U}(X, \text{dist}_H(\mathcal{X}, X)), \varepsilon) \subseteq \mathcal{U}(X, \text{dist}_H(\mathcal{X}, X) + \varepsilon) \subseteq \mathbb{R}^m \setminus \Delta_X,$$

since, by assumption, $\text{dist}_H(\mathcal{X}, X) + \varepsilon < \tau(X)$. Therefore H_X of Proposition 3§1.5 is well-defined for all $(t, z) \in [0, 1] \times \mathcal{U}(\mathcal{X}, \varepsilon)$. We will show that H_X gives a continuous retraction of $\mathcal{U}(\mathcal{X}, \varepsilon)$ onto X . For this, by Proposition 3§1.5, we only have to show that for all $(t, z) \in [0, 1] \times \mathcal{U}(\mathcal{X}, \varepsilon)$, $H_X(t, z) \in \mathcal{U}(\mathcal{X}, \varepsilon)$. By the way that H_X is constructed, we have to show that for all $z \in \mathcal{U}(X, \varepsilon)$,

$$[z, \pi_X(z)] \subseteq \mathcal{U}(\mathcal{X}, \varepsilon).$$

Let $z \in \mathcal{U}(\mathcal{X}, \varepsilon)$, $z := \pi_X(z)$ and $x \in \mathcal{X}$ be such that $\text{dist}(x, z) \leq \varepsilon$. If $\text{dist}(z, x) \leq \varepsilon$, then $[z, z] \subseteq \bar{B}(x, \varepsilon)$ and we are done. Therefore assume $\text{dist}(z, x) > \varepsilon$ from now on. In this way, let $\tilde{z} \in [z, z]$ be the nearest point to z such that $\text{dist}(\tilde{z}, x) = \varepsilon$. We only have to show that $[\tilde{z}, z] \subseteq \mathcal{U}(\mathcal{X}, \varepsilon)$. In fact, we will show something stronger, namely, that it is contained in just one of the balls that constitute $\mathcal{U}(x, \varepsilon)$.

Let

$$u := \frac{z - z}{\|z - z\|} = \frac{\tilde{z} - z}{\|\tilde{z} - z\|},$$

then, since $z = z + tu$ for some $t > 0$ and $\pi_X(z) = z$, we have $\tau(X, z; u) > 0$. Hence, by Theorem 3§1.6(3),

$$\tau(X, z; u) \geq \tau(X).$$

Consider now, $r := \frac{1}{3}\varepsilon$. On the one hand, $6r < \tau(X)$, therefore $\tau(X, z; u) > 6r$ and we can construct $\mathfrak{z} := z + 6ru$ such that $\pi_X(\mathfrak{z}) = z$. On the other hand, $\text{dist}_H(\mathcal{X}, X) < r$, thus there is $\tilde{x} \in \mathcal{X}$ such that $\text{dist}(\tilde{x}, z) < r$.

We will be done once we show that $\text{dist}(\tilde{x}, \tilde{z}) \leq \varepsilon$. We note now that

$$\text{dist}(\tilde{y}, \tilde{z}) \leq \text{dist}(\tilde{y}, z) + \text{dist}(z, \tilde{z}) \leq r + \text{dist}(z, \tilde{z}) = r + \text{dist}(\mathfrak{z}, z) - \text{dist}(\mathfrak{z}, \tilde{z}) = 7r - \text{dist}(\mathfrak{z}, \tilde{z}),$$

where the middle equality follows from the fact that z , \tilde{z} and \mathfrak{z} are collinear with \tilde{z} in the middle. Because of this, it is enough to show

$$4r \leq \text{dist}(\mathfrak{z}, \tilde{z}),$$

i.e., that \tilde{z} is “far” from \mathfrak{z} .

To end the proof consider the triangle $x\tilde{z}\mathfrak{z}$ whose vertices are x , \tilde{z} and \mathfrak{z} . Now, the angle Θ at \tilde{z} of $x\tilde{z}\mathfrak{z}$ is the same angle at \tilde{z} of the triangle $x\tilde{z}\tilde{z}'$, where \tilde{z}' is the point in $[z, \mathfrak{z}]$ such that $\text{dist}(x, \tilde{z}') = \varepsilon$. This last triangle is isosceles, with the considered angle being a base angle. Thus Θ is acute. We note that in the degenerate situation, $\Theta = \pi/2$ and the argument below still applies.

Since x is “near” X and \mathfrak{z} “far” from X , we have that

$$\text{dist}(x, \mathfrak{z}) \geq \text{dist}_X(\mathfrak{z}) - \text{dist}_X(x) \geq 6r - r = 5r$$

where we have used that $\text{dist}_X(x) \leq \text{dist}_H(\mathcal{X}, X) < r$. Finally, by the cosine theorem applied at Θ , we have

$$\text{dist}(x, \mathfrak{z})^2 = \text{dist}(\tilde{z}, \mathfrak{z})^2 + \text{dist}(\tilde{z}, x)^2 - 2 \text{dist}(\tilde{z}, \mathfrak{z}) \text{dist}(\tilde{z}, x) \cos \Theta \leq \text{dist}(\tilde{z}, \mathfrak{z})^2 + \text{dist}(\tilde{z}, x)^2$$

since Θ is acute. From here, we have

$$\text{dist}(\tilde{z}, \mathfrak{z}) \geq \sqrt{\text{dist}(x, \mathfrak{z})^2 - \text{dist}(\tilde{z}, x)^2} \geq \sqrt{25r^2 - 9r^2} \geq 4r.$$

This concludes the proof.

□

Remark 3^{§1}2. In case the reader does not like proofs à la Peano, i.e., without drawings [Q12], E can see a diagram of the proof in Figure 3^{§1}3. In this diagram, we have not only represented the relations of proximity, but also the metric relations concerning the points involved in the proof. ¶

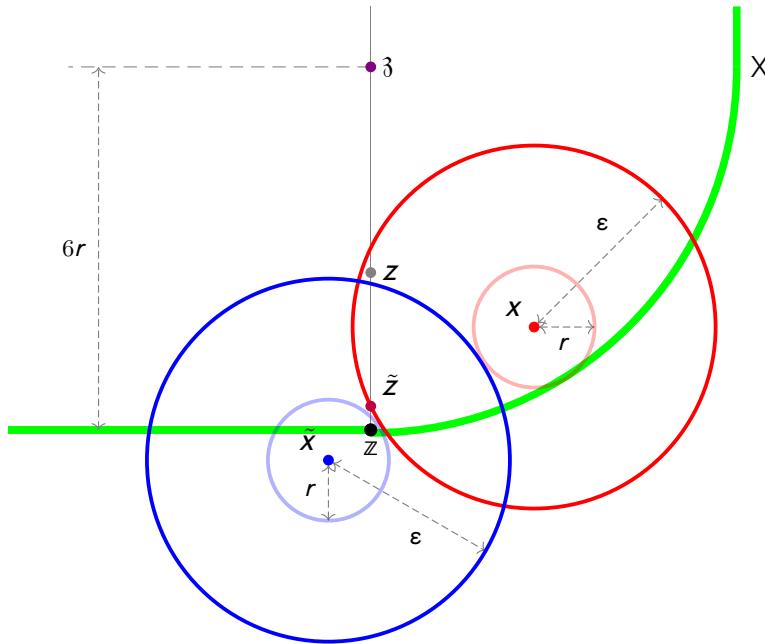


Figure 3^{\$1}3: Diagram of the proof of Theorem 3^{\$1}8

Remark 3^{§1}3. A version of the above theorem (Theorem 3^{§1}8), but with worse constants can be obtained as a corollary of the Chazal-Cohen-Steiner-Lieutier approximation theorem [109; Theorem 4.6]. The proof there is more involved, but it is so because their theorem applies to a more general setting. They do this by using the notions of μ -reach, τ_μ , and weak reach, τ_w , introduced by Chazal and Lieutier [110, 111].

Let us briefly recall these notions. Let $X \subseteq \mathbb{R}^n$ be compact and $z \in \mathbb{R}^m$. Then define $\Gamma_X(z) := \{x \in X \mid \text{dist}(z, x) = \text{dist}(z, X)\}$. Let $\Theta_X(z) \in \mathbb{R}^n$ and $R_X(z) \in [0, \infty)$ to be such that $\bar{B}(\Theta_X(z), R_X(z))$ is the (unique) smallest closed ball containing $\Gamma_X(z)$. Finally, consider the vector field

$$\nabla_X(z) := \frac{z - \Theta_X(z)}{\text{dist}_X(z)},$$

which is well-defined whenever $z \neq \Theta_X(z)$. One can see that for $z \notin \mathbb{R}^m \setminus (X \cup \Delta_X)$ this agrees with the one defined in Proposition 3^{S1}4. However, constructing a flow for this vector field requires technical tools, since it is not continuous in general, and because the continuous retraction it gives is only between neighborhoods. In this setting, the μ -reach (for $\mu \in (0, 1]$) and weak reach are given by

$$\tau_\mu(X) := \text{dist}(X, \{z \in \mathbb{R}^m \mid \|\nabla_X(z)\| < \mu\}) \text{ and } \tau_\mu(X) := \text{dist}(X, \{z \in \mathbb{R}^m \mid \|\nabla_X(z)\| = 0\}).$$

Note that the reach is just the 1-reach.

One can see that, in Example 3§1 4, $\tau_\mu(X) = \infty$ if $\mu \leq \frac{1-\cos \frac{\theta}{2}}{\sqrt{(1-\cos \frac{\theta}{2})^2 + \tan^2 \frac{\theta}{2}}}$ where θ is the acute angle between the red lines and $\tau_\mu(X) = 0$ otherwise. However, in Example 3§1 5, $\tau_w(X) > 0$, but $\tau_\mu(X) = 0$ for all $\mu > 0$. In general, one can show that for every closed semialgebraic set, $\tau_w(X) > 0$ [111; Proposition 3.6], but one should observe that in order to make this computational one needs explicit lower bounds. It is not clear how to extend some of the results that only work for the μ -reach, or how to give bounds for the μ for which the μ -reach is positive. We discuss this problem in Chapter 5. ¶

3§2 Reach: Explicit lower bounds

In this section, we provide lower bounds for the reach of an intersection in terms of the reach of the intersection of the boundaries, a lower bound of the local reach of an analytic set in terms of Smale's gamma, and a lower bound for the class of spherical semialgebraic sets we will be working with.

3§2–1 Reach of intersections

The main theorem we will prove is the following one.

Theorem 3§2 1. [88; Corollary 2.6]. Let $\{X_i\}_{i \in I}$ be a finite family of closed subsets of \mathbb{R}^m and $Y \subseteq \mathbb{R}^m$ another closed subset. Then

$$\tau\left(Y \cap \bigcap_{i \in I} X_i\right) \geq \min_{J \subseteq I} \tau\left(Y \cap \bigcap_{j \in J} \partial X_j\right).$$

In particular, $\tau(\cap_{i \in I} X_i) \geq \min_{J \subseteq I} \tau(\cap_{j \in J} \partial X_j)$.

The theorem will follow from induction from the following proposition.

Proposition 3§2 2. [88; Theorem 2.4]. Let $X, Y \subseteq \mathbb{R}^n$ be closed subsets. Then

$$\tau(Y \cap X) \geq \min\{\tau(Y), \tau(Y \cap \partial X)\}.$$

Proof of Theorem 3§2 1. By Proposition 3§2 2, Theorem 3§2 1 is true for $\# I = 1$. Assume that Theorem 3§2 1 is true for $\# I \leq k$, we will show that then it is true for $\# I \leq k + 1$.

Let $I = I_0 \cup \{i_0\}$. Then, by Proposition 3§2 2,

$$\begin{aligned} \tau\left(Y \cap \bigcap_{i \in I} X_i\right) &= \tau\left(\left(Y \cap \bigcap_{i \in I_0} X_i\right) \cap X_{i_0}\right) \\ &\geq \min\left\{\tau\left(Y \cap \bigcap_{i \in I_0} X_i\right), \tau\left(\left(Y \cap \bigcap_{i \in I_0} X_i\right) \cap \partial X_{i_0}\right)\right\}. \end{aligned}$$

Since $\# I_0 \leq k$, by induction hypothesis,

$$\tau\left(Y \cap \bigcap_{i \in I_0} X_i\right) \geq \min_{J \subseteq I_0} \tau\left(Y \cap \bigcap_{j \in J} \partial X_j\right)$$

and, also by induction hypothesis,

$$\begin{aligned} \tau\left(\left(Y \cap \bigcap_{i \in I_0} X_i\right) \cap \partial X_{i_0}\right) &= \tau\left((Y \cap \partial X_{i_0}) \cap \bigcap_{i \in I_0} X_i\right) \\ &\geq \min_{J \subseteq I_0} \tau\left((Y \cap \partial X_{i_0}) \cap \bigcap_{j \in J} \partial X_j\right) = \min_{J \subseteq I_0} \tau\left(Y \cap \bigcap_{j \in J \cup \{i_0\}} \partial X_j\right). \end{aligned}$$

The first is the minimum over subsets of I that exclude i_0 and the second the minimum over those that contain i_0 . Hence, taking the minimum of both of them, we prove the theorem for $\#I = k + 1$. By the induction principle, the proof is finished. \square

Proof of Proposition 3§2.2. Let $z \in \Delta_{Y \cap X}$ and $x, \tilde{x} \in Y \cap X$ be different points such that $\text{dist}(z, x) = \text{dist}(z, \tilde{x}) = \text{dist}_{Y \cap X}(z)$. As z is arbitrary, it is enough to check that

$$\text{dist}_{Y \cap X}(z) \geq \min\{\tau(Y), \tau(Y \cap \partial X)\}$$

since, then, taking the infimum over z the desired result follows. We consider three cases: 1) $x, \tilde{x} \in \partial X$, 2) $x \notin \partial X$, and 3) $\tilde{x} \notin \partial X$.

Case 1). In this case, x and \tilde{x} are also the nearest points to z in $Y \cap \partial X \subseteq Y \cap X$ and so

$$\text{dist}_{Y \cap X}(z) = \text{dist}_{Y \cap \partial X}(z) \geq \tau(Y \cap \partial Y)$$

which shows our inequality.

Case 2). In this case, x is in the interior of X and so there is some $\varepsilon > 0$ such that

$$Y \cap X \cap B(x, \varepsilon) = Y \cap B(x, \varepsilon),$$

i.e., we cannot distinguish $Y \cap X$ and Y locally around x . Further, $Y \cap B(x, \varepsilon) \subseteq B(x, \varepsilon) \setminus B(z, \text{dist}_{X \cap Y}(z))$, as otherwise x would not be one of the nearest points in $Y \cap X$ to z , which contradicts the way x was chosen.

Let

$$u = \frac{z - x}{\|z - x\|},$$

which is the unit vector of the line joining x to z . By the above paragraph, we must have

$$\pi_{Y \cap X}(x + tu) = \pi_Y(x + tu) \in B(x, \varepsilon) \setminus B(z, \text{dist}_{X \cap Y}(z))$$

for $t \in [0, \min\{\varepsilon/2, \tau(Y)\})$. Thus $\pi_Y(x + tu) = x$, as this is the nearest point in $B(x, \varepsilon) \setminus B(z, \text{dist}_{X \cap Y}(z))$ to $x + tu$. Therefore $\tau(X, x; u) > 0$ and, by Theorem 3§1 6(3),

$$\tau(Y) \leq \tau(Y, x) \leq \tau(Y, x; u).$$

Also $\tau(Y, x; u) \leq \text{dist}(x, z) = \text{dist}_{Y \cap X}(z)$, by Theorem 3§1 6(1), since $\text{dist}(z, x) = \text{dist}(z, \tilde{x})$ and $x, \tilde{x} \in Y$. This finishes the proof.

Case 3). This is the same as case 2), but with \tilde{x} in the place of x .

In all three cases, the given lower bound holds. Hence the proposition is proven. \square

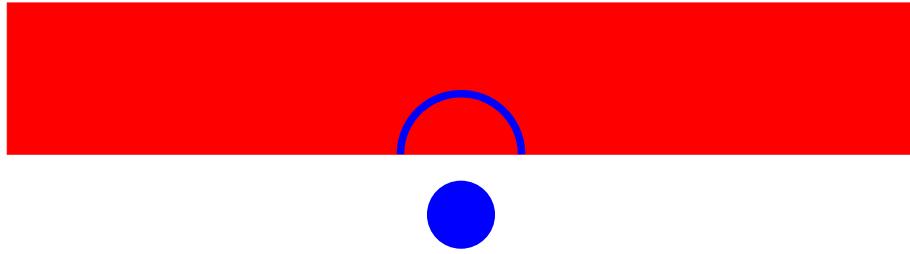


Figure 3§2 4: X , in red, and Y , in blue, from Remark 3§2 1

Remark 3§2 1. Although the proof above might look more complicated than that given in [88; Proof of Theorem 2.4], this is so because there is a small mistake in that proof. In the case 2), it is claimed that $\text{dist}_Y(z) = \text{dist}(z, x) > 0$, written there as $d_W(x) = \|x - p\| > 0$. However, this is false in general, as shown by

$$X := \{x \in \mathbb{R}^2 \mid x_2 \geq 0\} \text{ and } Y = (\mathbb{S}^1 \cap X) \cup \overline{B}((0, -1), 1/2),$$

illustrated, respectively, in red and in blue in Figure 3§2 4. In this example, one can see that $\text{dist}_Y(z) = 1/2 < 1 = \text{dist}(z, x)$ no matter the x that one chooses in $Y \cap X^\circ$. ¶

Remark 3§2 2. A natural question is whether the lower bounds of Theorem 3§2 1 and Proposition 3§2 2 can be extended to the local reach. This motivates the following open problem.

Open problem E. Given $X, Y \subseteq \mathbb{R}^m$ closed subsets and $p \in Y \cap X$, is it true that

$$\tau(Y \cap X, x) \geq \min\{\tau(Y, x), \text{dist}(x, \Delta_{Y \cap X})\}?$$

Or more generally, can we lower-bound $\tau(Y \cap X, x)$ in terms of $\tau(Y \cap X, x)$, $\text{dist}(x, \Delta_{Y \cap X})$ and $\text{dist}_{Y \cap X}(x)$?

We observe that such a claim was made in [214; Theorem 3.10] (cf. [213]), but the proof there has a mistake which cannot be corrected.³ Such a result is fundamental for the construction of adaptive grid algorithms for homology of basic semialgebraic sets. We will discuss this further in Chapter 5. ¶

3§2–2 Reach of analytic sets

Smale's gamma (see Definition 1§2 3) plays a fundamental role in the local analysis of Newton's method. For example, in the zero dimensional cases, one can show that a condition for Newton's method to converge to a zero x of f starting at a point x_0 is that $\text{dist}(x_0, x) < \frac{1}{6}\bar{\gamma}(f, x)^{-1}$ [147; Théorème 91]. Since a point cannot converge to two zeros under Newton's method, this implies immediately the following proposition.

Proposition 3§2 3. Let $f : \mathbb{R}^m \rightarrow \mathbb{R}^m$ be an analytic function and $x \in f^{-1}(0)$ a zero of f . Then $3\bar{\gamma}(f, x)\text{dist}(x, f^{-1}(0) \setminus \{x\}) \geq 1$. □

³On the one hand, it claims $W \cap V \subseteq W \cap \partial V$; on the other hand, it claims that $\Delta_A \subseteq \Delta_B$ whenever $A \subseteq B$. Both of these claims are false, even in very well-behaved settings.

Now, since x is an isolated point of $f^{-1}(0)$ in the above case, this means that

$$\tau(f^{-1}(0), x) = \frac{1}{2} \text{dist}(x, f^{-1}(0) \setminus \{x\}),$$

which can be proven by considering the midpoint between x and one of its nearest points in $f^{-1}(0) \setminus \{x\}$. Therefore, we have the following.

Corollary 3^{§2}4. *Let $f : \mathbb{R}^m \rightarrow \mathbb{R}^m$ be an analytic function and $x \in f^{-1}(0)$ a zero of f . Then $6\bar{\gamma}(f, x)\tau(f^{-1}(0), x) \geq 1$.* \square

The main theorem in this section is a generalization of the above result for positive dimensional zero-sets of analytic functions. This can be interpreted as evidence that the reach is an analogue in the positive dimensional case of the distance between nearest zeros of the zero-dimensional case.

Theorem 3^{§2}5. [88; Theorem 3.3] *Let $f : \mathbb{R}^m \rightarrow \mathbb{R}^q$ be an analytic map and $x \in f^{-1}(0)$ a zero of f . Then*

$$14\bar{\gamma}(f, x)\tau(f^{-1}(0), x) \geq 1$$

whenever $\bar{\gamma}(f, x)$ is finite.

We will prove the above theorem as we proved Proposition 3^{§1}7, but now we have to be more careful in order to obtain explicit lower bounds and not only positivity.

Proof. Let $M = f^{-1}(0)$ and let's proceed as in the proof of Proposition 3^{§1}7. In this case, however, we already have a function which gives globally M as its zero set. As in the proof there, we will consider for each $x \in \mathbb{R}^m$ such that $\bar{D}_x f$ is surjective, the linear map

$$P_{f,x} = I - \bar{D}_x f^\dagger \bar{D}_x f$$

which is the orthogonal projection onto $\ker D_x f$.

We consider the same minimization problem,

$$\arg \min \{\text{dist}(x + tu, y) \mid y \in M\},$$

and we fix $u \in N_x M$ in the following. We will show that

$$14\bar{\gamma}(f, x)\tau(f^{-1}(0), x; u) \geq 1$$

from where the claim will follow by Theorem 3^{§1}6(3).

By Theorem 3^{§1}6(1), the smallest t for which this problem does not have a unique solution satisfies that there is $y \in M$ different from x such that

$$t = \text{dist}(x + tu, x) = \text{dist}(x + tu, y).$$

If $7\bar{\gamma}(f, x)\text{dist}(x, y) \geq 1$, then $2t \geq \text{dist}(x, y)$ finishes the proof. Therefore assume that $7\bar{\gamma}(f, x)\text{dist}(x, y) < 1$ and let $\eta := \bar{\gamma}(f, x)\text{dist}(x, y) < 1/7$.

Arguing as in the proof of Proposition 3^{§1}7, we will arrive again to inequality (3.9). There we need to bound $\max_{z \in [x,y]} \left\| \bar{D}_z P_f \left(\frac{y-x}{\|y-x\|} \right) \right\|$ and $\max_{z \in [x,y]} \|\bar{D}_y f^\dagger \bar{D}_z^2 f\|$ from above.

Applying the usual rules of differentiation, we have that

$$\bar{D}_z P_f(\dot{z}) = -\bar{D}_z f^\dagger \bar{D}_z^2 f(\dot{z}) P_{f,z} - \left(\bar{D}_z f^\dagger \bar{D}_z^2 f(\dot{z}) P_{f,z} \right)^\top$$

for all z and $\dot{z} \in T_z \mathbb{R}^m = \mathbb{R}^m$. Therefore, by Definition 1\\$2 3,

$$\left\| \bar{D}_z P_f(\dot{z}) \right\| = \left\| \bar{D}_z f^\dagger \bar{D}_z^2 f(\dot{z}) P_{f,z} \right\| \leq 2\bar{\gamma}(f, z) \|\dot{z}\|,$$

since for $A = \bar{D}_z f^\dagger \bar{D}_z^2 f(\dot{z}) P_{f,z}$, we have $A^2 = 0$ and so $\|A + A^*\| = \|A\|$. Hence

$$\max_{z \in [x,y]} \left\| \bar{D}_z P_f \left(\frac{y-x}{\|y-x\|} \right) \right\| \leq \max_{z \in [x,y]} 2\bar{\gamma}(f, z)$$

Now, recall that in the proof of Proposition 3\\$1 7, $\max_{z \in [x,y]} \|\bar{D}_y f^\dagger \bar{D}_z^2 f\|$ appears when we bound $\|\bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_x f(x-y) - \bar{D}_y f^\dagger f(x)\|$ using Taylor's theorem with remainder. As f is analytic now, we can just take the full Taylor series to obtain

$$\begin{aligned} & \|\bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_x f(x-y) - \bar{D}_y f^\dagger f(x)\| \\ &= \left\| \sum_{k=2}^{\infty} \frac{1}{k!} \bar{D}_y f^\dagger \bar{D}_y^k f(x-y, \dots, x-y) \right\| \leq \sum_{k=2}^{\infty} \left\| \frac{1}{k!} \bar{D}_y f^\dagger \bar{D}_y^k f(x-y, \dots, x-y) \right\| \\ &\leq \sum_{k=2}^{\infty} \left\| \frac{1}{k!} \bar{D}_y f^\dagger \bar{D}_y^k f \right\| \|x-y\|^k \leq \sum_{k=2}^{\infty} \bar{\gamma}(f, y)^{k-1} \|x-y\|^k \leq \frac{\bar{\gamma}(y, x) \|x-y\|^2}{1 - \bar{\gamma}(f, y) \|x-y\|} \end{aligned}$$

Now, by [147; Lemme 132], we have that, under our hypothesis, for all $z \in [x, y]$,

$$\bar{\gamma}(f, z) \leq \gamma(\eta) \bar{\gamma}(f, x) \tag{3.11}$$

where $\eta := \bar{\gamma}(f, x) \text{dist}(x, y)$ and

$$\gamma(t) := \frac{1}{(1-t)(1-4t+2t^2)}.$$

Hence, we obtain

$$\max_{z \in [x,y]} \left\| \bar{D}_z P_f \left(\frac{y-x}{\|y-x\|} \right) \right\| \leq 2\gamma(\eta) \bar{\gamma}(f, x)$$

and

$$\|\bar{D}_y f^\dagger f(y) + \bar{D}_y f^\dagger \bar{D}_x f(x-y) - \bar{D}_y f^\dagger f(x)\| \leq \frac{\gamma(\eta) \eta}{1 - \gamma(\eta) \eta} \|y-x\|.$$

Combining these two inequalities as in (3.9), we get

$$t \geq \frac{1}{2\gamma(\eta)} \left(1 - \frac{\gamma(\eta) \eta}{1 - \gamma(\eta) \eta} \right) \frac{1}{\bar{\gamma}(f, x)} \geq \frac{1}{7\bar{\gamma}(f, x)}$$

where the right-hand inequality can be checked by direct computation using that $\eta < 1/7$.

Now, this means that $\pi_M(x + tu) = x$ for $t < \frac{1}{7\bar{\gamma}(f, x)}$ and so

$$\tau(M, x; u) \geq \frac{1}{7\bar{\gamma}(f, x)},$$

which by Theorem 3\\$1 6(3) gives the desired result. \square

Remark 3^{§2}3. The above proof is less elementary than that of [88], although it is essentially the same proof. However, there is a conceptual difference. While in the proof in [88] it is not clear why $P_{f,z}$ plays a role, in the proof above, this is clear as it appears as a result of optimizing to find the nearest point in \mathcal{M} to $x + tu$. ¶

Remark 3^{§2}4. Let us note that there is a deep relationship between reach, curvature and bottlenecks. The bound of $\|D_z P_f(\dot{z})\|$ by $2\gamma(f, z)$ gives also a bound of the norm of the so-called second fundamental form. We refer the reader to [1; §3], [88; Proposition 3.4] and [300; Proposition 6.1] for further comments on this. ¶

3^{§2}–3 Reach of spherical semialgebraic sets

We combine Theorems 3^{§2}1 and 3^{§2}5 above to obtain a lower bound for the reach of a spherical semialgebraic set of the form $S(f, t, \phi)$, when f is well-posed and ϕ is a purely conjunctive lax formula.

Theorem 3^{§2}6. [92; Proof of Theorem 2.13]. Let $f \in \mathcal{H}_d[q]$ and $t \in (-T, T)^e$ be such that $\sqrt{2}\bar{\kappa}(f)T < 1$. Then, for all purely conjunctive lax formulas ϕ over (f, t) ,

$$(2 + \sqrt{2}) 7D^{\frac{3}{2}} \bar{\kappa}(f) \tau(S(f, t, \phi)) > 1.$$

Proof. By assumption on ϕ , we can write

$$\phi \equiv \bigwedge_{k \in K} (f_{a(k)} \propto_k t_{b(k)} \| f_{a(k)} \|_W)$$

with K a finite set, $\propto \in \{\geq, \leq, =\}^K$ and maps $a : K \rightarrow [q]$ and $b : K \rightarrow [e]$. Therefore, by Theorem 3^{§2}1,

$$\tau(S(f, t, \phi)) \geq \min_{J \subseteq I} \tau \left(\bigcap_{j \in J} \partial S(f, t, (f_{a(k)} \propto_k t_{b(k)} \| f_{a(k)} \|_W)) \right).$$

Note that, by our assumption and the regularity inequality (Proposition 1^{§3}3), $S(f, t, (f_i = t_j \| f_i \|_W))$ is a regular hypersurface and so, for all $\propto \in \{\geq, \leq, =\}$,

$$\partial S(f, t, (f_i \propto t_j \| f_i \|_W)) = S(f, t, (f_i = t_j \| f_i \|_W)),$$

by the Implicit Function Theorem. Thus

$$\tau(S(f, t, \phi)) \geq \min_{J \subseteq I} \tau \left(\bigcap_{j \in J} S(f, t, (f_{a(k)} = t_{b(k)} \| f_{a(k)} \|_W)) \right).$$

Because of this, it is enough to prove the bound in the case in which ϕ only has equalities, i.e., \propto is $(=, \dots, =)$. We assume this without loss of generality.

If for distinct $k, k' \in K$, $a(k) = a(k')$ and $b(k) \neq b(k')$, then $S(f, t, \phi)$ is empty and we are done. Because of this, we might further assume that ϕ is of the form

$$\phi \equiv \bigwedge_{I \in L} (f_I = t_{b(I)} \| f_I \|_W)$$

with $L \subseteq [q]$ and $b : I \rightarrow [e]$. Further, note that by the regularity inequality (Proposition 1§3), $S(f, t, \phi)$ is empty if $\# L \geq n + 1$. So we can assume, without loss of generality, that $\# L \leq n$ and that $S(f, t, \phi)$ is non-empty.

Let $\tau \in (-T, T)^L$ be such that for $I \in L$, $\tau_I := t_{b(I)} \|f_I\|_W$. Observe that $S(f, t, \phi)$ is the zero set of $f^L - \tau$ in \mathbb{S}^n and of $(f^L - \tau)_{\mathbb{S}} := (f - \tau, \sum_{i=0}^n X_i^2 - 1)$ in \mathbb{R}^{n+1} . Therefore, by Theorem 3§2 5,

$$14 \max_{x \in S(f, t, \phi)} \bar{\gamma}\left(\left(f^L - \tau\right)_{\mathbb{S}}, x\right) \tau\left(\left(f^L - \tau\right)_{\mathbb{S}}^{-1}(0)\right) \geq 1.$$

Now, on the one hand, for all $x \in \mathbb{S}^n$, $\bar{\gamma}\left(\left(f^L - \tau\right)_{\mathbb{S}}, x\right) = \bar{\gamma}(f_{\mathbb{S}}, x)$; and, on the other hand, for $x \in S(f, t, \phi)$, we have

$$\frac{\|f^L(x)\|}{\|f^L\|_W} \leq \frac{\|\tau\|}{\|f^L\|_W} < T \leq \frac{1}{\sqrt{2\kappa(f)}}.$$

Hence, for $x \in S(f, t, \phi)$,

$$2\bar{\gamma}\left(\left(f^L - \tau\right)_{\mathbb{S}}, x\right) \leq D^{\frac{3}{2}}\mu(f, x) + \frac{D^{\frac{1}{2}}\mu(f, x)}{\sqrt{2\kappa(f)}} + 1 \leq \sqrt{2}D^{\frac{3}{2}}\bar{\kappa}(f) + D^{\frac{1}{2}} + 1 \leq (2 + \sqrt{2})D^{\frac{3}{2}}\bar{\kappa}(f),$$

due to Corollary 1§2 12 and the inequality $\mu(f, x) \leq \sqrt{2\kappa(f)}$ which follows from the regularity inequality (Proposition 1§3 3) and $\sqrt{2\kappa(f)}\|f^L(x)\|/\|f^L\|_W < 1$. This finishes the proof. \square

Remark 3§2 5. We note that the hypothesis of Theorem 3§2 6 that requires ϕ to be purely conjunctive cannot be dropped. The reason for this is that in general, the union of semialgebraic sets has zero reach, even in the case that the underlying polynomial tuple is well-conditioned. An explicit example can be

Example 3§2 1. Consider $f = (X+Y, X-Y)$ and $\Phi \equiv ((X+Y \geq 0) \wedge (X-Y \geq 0)) \vee ((X+Y \leq 0) \wedge (X-Y \leq 0))$. One can see that $S(f, \Phi) \subseteq \mathbb{S}^2$ has reach equal to zero, due to the crossing of the two lines at $(0 \ 0 \ 1)^*$. A local image of the set around that point can be seen in Figure 3§2 5. Δ

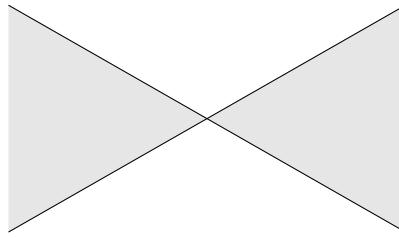


Figure 3§2 5: A semialgebraic set with reach equal to zero

3§3 Homology of a cloud of points: the nerve theorem

Covers play a fundamental role in topology, as in compactness and (topological) dimension. Further, triangulations and CW decompositions can be seen as covers with a strong combinatorial structure. Among all these topological concepts, one that will play a fundamental concept in this thesis will be the nerve of a cover introduced by the topologist Alexandrov.

Definition 3^{§3}1. [5]. Let X be a topological space and C a finite cover of X . The *nerve* of C , $\mathcal{N}(C)$, is the (abstract) simplicial complex given by

$$\mathcal{N}(C) := \left\{ \sigma \subseteq C \mid \bigcap_{C \in \sigma} C \neq \emptyset \right\}. \quad (3.12)$$

One can see that this notion captures the intersection relations of the elements of a cover. A highly non-trivial result is the following theorem,⁴ which says that this intersection relationships capture the homotopy type of the space when the pieces and all intersections are topologically trivial.

Theorem 3^{§3}1 (Nerve theorem). [216; Corollary 4G.3]. Let X be a compact space and C a finite open cover of X satisfying the Leray property:

$$\text{for every } C' \subseteq C, \cap_{V \in C'} V \text{ is contractible.}$$

Then X is homotopy equivalent to $[\mathcal{N}(C)]$.

This form of the nerve theorem is not always the best. Because of that, we will develop below the statement of the theorem that best suits our objectives. Also, we will introduce a graph variant of the nerve that will play an important role in making our algorithms faster.

3^{§3}-1 Simplicial complexes and the computation of their homology

We define what a simplicial complex is, we indicate how the homology of a simplicial complexes is defined and we give an algorithm for computing this homology, based on this definition.

Remark 3^{§3}1. We don't intend to introduce the concepts, but we recall them to fix terminology and notation. ¶

Abstract simplicial complexes and their realizations

Since our focus is computational, we will view simplicial complex just by their combinatorial properties, i.e., by how their faces are contained in other faces. This is modelled by the notion of abstract simplicial complex.

Definition 3^{§3}2. Let X be a finite set. A (*abstract*) *simplicial complex* over X is a set $\mathcal{S} \subseteq \mathcal{P}(X)$ of subsets of X such that for all $\sigma \in \mathcal{S}$ and all $\tilde{\sigma} \subseteq \sigma$, we have $\tilde{\sigma} \in \mathcal{S}$.

Remark 3^{§3}2. We will refer to the elements of \mathcal{S} as the faces of \mathcal{S} and to the elements of a face σ of \mathcal{S} as the vertices of σ . ¶

This is not a topological space. It is just a family of subsets. However, we can associate to it a “canonical” topological space. Consider the *free simplex* with vertex set X , which is defined as the set

$$\Delta^X := \left\{ \sum_{x \in X} t_x[x] \mid \text{for all } x \in X, t_x \geq 0, \sum_{x \in X} t_x = 1 \right\} \subseteq \mathbb{R}^X \quad (3.13)$$

⁴We will sacrifice generality for an easily understandable statement.

formed by the formal convex combinations of the points of X . Here we use the notation $[x]$ to distinguish the vertex $[x]$ in Δ^X from the point x in X . If $X \subseteq \mathbb{R}^m$, this avoids an ambiguous notation.

Now, for every $\sigma \in \mathcal{S}$, the simplex Δ^σ lies inside Δ^X and it is a face of it. Further, this is compatible with intersections, because for all $\sigma, \sigma' \in \mathcal{S}$, $\Delta^{\sigma \cap \sigma'} = \Delta^\sigma \cap \Delta^{\sigma'}$. This motivates the following definition.

Definition 3§3.3. Given a simplicial complex \mathcal{S} over a finite set X , its *realization* is the topological subspace $[\mathcal{S}]$ of Δ^X given by

$$[\mathcal{S}] := \bigcup \{\Delta^\sigma \mid \sigma \in \mathcal{S}\}. \quad (3.14)$$

Whenever we work with topological spaces and continuous maps, the realization of the simplicial complex will be used. For example, this will be done in our statement of the functorial nerve theorem.

Remark 3§3.3. Note that the realization of a simplicial complex above can be viewed as a construction of an equivalent geometric simplicial complex.

Definition 3§3.4. A *geometric simplicial complex* in \mathbb{R}^m is a set S of simplices of \mathbb{R}^m such that

• For every $\sigma \in S$ and every face $\tilde{\sigma}$ of σ , $\tilde{\sigma} \in S$.

• For every $\sigma, \tilde{\sigma} \in S$, $\sigma \cap \tilde{\sigma}$ is a face of σ .

One should note that geometric simplicial complexes are like simplicial complexes, but keeping track of how the simplices lie in some ambient spaces. As this information is irrelevant for the homology of a simplicial complex, we prefer to use abstract simplicial complexes instead of geometric ones. ¶

Homology groups of a simplicial complex

Let us recall how the simplicial homology of a simplicial complex is defined. We consider simplicial subcomplexes of our simplicial complexes and their boundaries. Topological holes are interpreted as those simplicial subcomplexes that behave like a boundary, but they are not a boundary. The main idea behind homology is to find an algebraic way of dealing with the boundary condition, by just counting the faces with orientation.

Consider a simplicial complex \mathcal{S} over a finite set X , the *dimension* of a face σ of \mathcal{S} is given by

$$\dim \sigma := \# \sigma - 1, \quad (3.15)$$

i.e., the number of vertices of σ minus one. We consider the set of k -dimensional faces, or simply k -faces, of \mathcal{S} ,

$$\mathcal{S}_k := \{\sigma \in \mathcal{S} \mid \dim \sigma = k\}, \quad (3.16)$$

and to each of these set of k -faces we associate the free \mathbb{Z} -module

$$C_k^\Delta(\mathcal{S}) := \mathbb{Z}^{\mathcal{S}_k} := \left\{ \sum_{\sigma \in \mathcal{S}_k} n_\sigma \sigma \mid n_\sigma \in \mathbb{Z} \right\} \quad (3.17)$$

of formal combinations of faces. Each of these formal combinations is called a k -chain.

To get a nice formula for the boundary operator, we choose an ordering of X . To define this order, we just number the elements of X by a bijective map $\mathfrak{o} : X \rightarrow \{0, \dots, \#X - 1\}$. This map then induces the map

$$\begin{aligned}\mathfrak{o}_\sigma : \sigma &\rightarrow \{0, \dots, k\} \\ v &\mapsto \#\{x \in \sigma \mid \mathfrak{o}(x) < \mathfrak{o}(v)\}\end{aligned}$$

on each k -face $\sigma \in \mathcal{S}$. One can see that this numbering is compatible with inclusions, in the sense that given faces $\sigma, \tilde{\sigma}$ of \mathcal{S} and $v, w \in \sigma \subseteq \tilde{\sigma}$, $\mathfrak{o}_\sigma(v) < \mathfrak{o}_\sigma(w)$ iff $\mathfrak{o}_{\tilde{\sigma}}(v) < \mathfrak{o}_{\tilde{\sigma}}(w)$.

Once we have fixed this order, we can define the k th boundary operator

$$\partial_k^\Delta : C_k^\Delta(\mathcal{S}) \rightarrow C_{k-1}^\Delta(\mathcal{S}) \tag{3.18}$$

which is the \mathbb{Z} -linear map given on each k -face σ of \mathcal{S} by

$$\partial_k^\Delta(\sigma) = \sum_{v \in \sigma} (-1)^{\mathfrak{o}_\sigma(v)} (\sigma \setminus \{v\}). \tag{3.19}$$

One can easily check that for all $k \geq 0$,

$$\partial_k^\Delta \circ \partial_{k+1}^\Delta = 0$$

which is an algebraic version of the intuitive statement that boundaries of simplicial subcomplexes don't have boundaries. By convention, $\partial_0^\Delta = 0$. This motivates the definition of two submodules of k -chains:

$$B_k^\Delta(\mathcal{S}) := \text{im } \partial_{k+1}^\Delta \tag{3.20}$$

which are called k -boundaries, and

$$Z_k^\Delta(\mathcal{S}) := \ker \partial_k^\Delta \tag{3.21}$$

which are called k -cycles. One can check that these two submodules are independent of the ordering \mathfrak{o} on X , although the ∂_k^Δ are not, and that k -boundaries are always k -cycles.

Coming back to the intuition at the beginning, a topological hole is something that behaves like a boundary but it is not a boundary. In this setting, the first is to be a k -cycle and the second to be a k -boundary. Therefore a “topological k -hole” is a k -cycle that is not a k -boundary. This motivates defining the k th (simplicial) homology group of \mathcal{S} as

$$H_k^\Delta(\mathcal{S}) := \frac{Z_k^\Delta(\mathcal{S})}{B_k^\Delta(\mathcal{S})}. \tag{3.22}$$

One of the most fundamental theorems of algebraic topology is the following one.

Theorem 3^{§3} 2. [216; Theorem 2.27]. *Let \mathcal{S} be a simplicial complex over a finite set X . Then there is a natural isomorphism*

$$H_\bullet^\Delta(\mathcal{S}) \cong H_\bullet([\mathcal{S}])$$

between the simplicial homology of \mathcal{S} and the (singular) homology of $[\mathcal{S}]$. \square

In this way, when we say homology of a simplicial complex, there is no ambiguity to what we refer to. We can mean either the simplicial homology of the simplicial complex or the homology of its realization. Pursuing this, we will write $\beta_k(\mathcal{S})$ instead of $\beta_k([\mathcal{S}])$ and similarly for the torsion coefficients $\tau_k(\mathcal{S}) = (\tau_{k,i}(\mathcal{S}))_{i \in [s_k(\mathcal{S})]}$, when we speak about the homology of a simplicial complex.

Computation of homology groups

How fast can one compute the homology of a simplicial complex is not a settled question, as it depends deeply on the structure of the simplicial complex. Further, one can see that the computation of just the Betti numbers is equivalent to the computation of the rank of sparse matrices [169]. As the latter is still an open problem, we don't pretend to give the best working algorithm, but one that is good enough for our purposes.

The result in which many computations of homology rely is the following one which relates the Betti numbers and torsion coefficients to linear algebraic invariants of the boundary operators. Recall that the *Smith Normal Form* (SNF) of an integer matrix $A \in \mathbb{Z}^{m \times m'}$ is the unique diagonal matrix

$$\text{SNF}(A) := \begin{pmatrix} \mathbb{I}_{\text{rank } A - s(A)} & & & \\ & \text{SNF}_1(A) & & \\ & & \ddots & \\ & & & \text{SNF}_{s(A)}(A) \\ & & & \mathbb{O} \end{pmatrix} \in \mathbb{Z}^{m \times m'} \quad (3.23)$$

where the $\text{SNF}_i(A)$ are positive integers and $\text{SNF}_i(A)$ divides $\text{SNF}_{i+1}(A)$ for all $i < s(A) \leq \text{rank } A$ and such that

$$A = g \text{ SNF}(A) h$$

for some $g \in \text{GL}_m(\mathbb{Z}) := \{g \in \mathbb{Z}^{m \times m} \mid \det(g) \in \{-1, +1\}\}$ and $h \in \text{GL}_{m'}(\mathbb{Z})$.

Theorem 3§3.3. Let \mathcal{S} be a simplicial complex and $\{\delta_k^\Delta\}_{k \geq 0}$ its family of boundary operators with respect to some order \mathfrak{o} of its vertices. Then:

(β) For every k ,

$$\beta_k(\mathcal{S}) = \#\mathcal{S}_k - \text{rank } \delta_k^\Delta - \text{rank } \delta_{k+1}^\Delta.$$

(T) For every k and every i , $s_k(\mathcal{S}) = s(\delta_{k+1}^\Delta)$ and

$$\tau_{k,i}(\mathcal{S}) = \text{SNF}_i(\delta_{k+1}^\Delta).$$

Proof. By Theorem 3§3.2, and equations (3.20), (3.21) and (3.22), we have that

$$\beta_k([\mathcal{S}]) = \text{rank}_{\mathbb{Z}} \frac{\ker \delta_k^\Delta}{\text{im } \delta_{k+1}^\Delta}.$$

On the one hand, note that $\ker \delta_k^\Delta$ is a submodule of the free module $C_k^\Delta(\mathcal{S})$ and so also free by [273; Ch. III. Theorem 7.1]. Since extending to the rationals preserves the rank of a free module [273; Ch. XIV. Proposition 4.1], we can see that

$$\text{rank}_{\mathbb{Z}} \ker \delta_k^\Delta = \dim_{\mathbb{Q}} \ker \delta_k^\Delta = \#\mathcal{S}_k - \text{rank } \delta_k^\Delta.$$

On the other hand, choose a \mathbb{Z} -basis of $\ker \delta_k^\Delta$ and another \mathbb{Z} -basis of $C_{k+1}^\Delta(\mathcal{S})$ such that $\delta_{k+1}^\Delta : C_{k+1}^\Delta(\mathcal{S}) \rightarrow \ker \delta_k^\Delta$ is in SNF with respect to these bases. Then, by direct computation, we have that

$$\frac{\ker \delta_k^\Delta}{\text{im } \delta_{k+1}^\Delta} \cong \mathbb{Z}^{\text{rank}_{\mathbb{Z}} \ker \delta_k^\Delta - \text{rank } \delta_{k+1}^\Delta} \oplus \bigoplus_{j=1}^{s(\delta_{k+1}^\Delta)} \frac{\mathbb{Z}}{\text{SNF}_j(\delta_{k+1}^\Delta) \mathbb{Z}}.$$

Combining the above two paragraphs, we get the desired result by [273; Ch. III Theorem 7.3 and 7.7]. \square

By the above theorem, computing the homology of a simplicial complex is reduced to computing the Smith normal form of its boundary operators and computing the Betti numbers to computing the rank of its boundary operators. We have then the following two algorithmic schemes for computing the Betti numbers and homology of simplicial complexes.

Algorithm 1: SIMPLICIALBETTI

Input : $\ell \in \mathbb{N}$
simplicial complex \mathcal{S}

```

 $r_0 \leftarrow 0$ 
for  $i \leftarrow 1$  to  $\ell + 1$  do
   $r_k \leftarrow \text{rank } \partial_k^\Delta$ 
   $b_{k-1} \leftarrow \# \mathcal{S}_{k-1} - r_{k-1} - r_k$ 
Output  $b_0, \dots, b_\ell$ 

```

Output : ℓ first Betti numbers $\beta_0(\mathcal{S}), \dots, \beta_\ell(\mathcal{S})$ of \mathcal{S}

Algorithm 2: SIMPLICIALHOMOLOGY

Input : $\ell \in \mathbb{N}$
simplicial complex \mathcal{S}

```

 $r_0 \leftarrow 0$ 
 $t_0 \leftarrow 0$ 
for  $i \leftarrow 1$  to  $\ell + 1$  do
  Compute SNF( $\partial_k^\Delta$ )
   $r_k \leftarrow \text{rank } \partial_k^\Delta$ 
   $s_k \leftarrow s(\partial_k^\Delta)$ 
   $t_k \leftarrow (\text{SNF}_1(\partial_k^\Delta), \dots, \text{SNF}_{s_k}(\partial_k^\Delta))$ 
   $b_{k-1} \leftarrow \# \mathcal{S}_{k-1} - r_{k-1} - r_k$ 
Output  $b_0, \dots, b_\ell$  and  $t_1, \dots, t_\ell$ 

```

Output : ℓ first Betti numbers $\beta_0(\mathcal{S}), \dots, \beta_\ell(\mathcal{S})$
and ℓ first torsion coefficients $T_1(\mathcal{S}), \dots, T_\ell(\mathcal{S})$ of \mathcal{S}

The complexity of algorithms **SIMPLICIALBETTI** and **SIMPLICIALHOMOLOGY** depends on how much time one needs to compute, respectively, the rank and the SNF, where we observe that we don't need the matrices that put the boundary operator in SNF. The following deterministic bound shows that one can bound the computation in terms of the size of the simplicial complex.

Proposition 3^{§3} 4. [142; Proposition 4.6] Algorithms **SIMPLICIALBETTI** and **SIMPLICIALHOMOLOGY** take $O(\sum_{k=0}^{\ell+1} (\# \mathcal{S}_k)^5)$ -time.

Proof. We will use the algorithm of Storjohann [383] for computing the SNF. Since boundary operators have entries of bit-size at most 1, the algorithm takes $\mathcal{O}^\sim(m^{\omega-1}m'M(m'))$ on a matrix $A \in \mathbb{Z}^{m \times m'}$, where \mathcal{O}^\sim indicates that polylog-factors are omitted, ω is the exponent of matrix multiplication and $M(t)$ the complexity of multiplying two integers of bit-size at most t . We know that $\omega \leq 2.8$, by Strassen's algorithm [384], and $M(t) \leq t^2$, by the standard multiplication algorithm. We eliminate the polylog-factors by bounding then by $\mathcal{O}(m^{0.1}m'^{0.1})$. \square

Remark 3§3 4. We note that the above deterministic complexity bound is far from being optimal. The above complexity bound can be improved. Using the algorithms from Giesbrecht [191], we can turn the exponent from a 5 to less than a 4 for homology, and from 5 to less than a 3 for the Betti numbers. \P

Remark 3§3 5. We note that persistent homology gives an alternative way to perform the computation of homology in the cases of interests. The main idea is to update the simplicial complex by successively adding faces to the complex and update the computed topological invariants. In many contexts and for many purposes, this is more efficient than the algorithm described above.

The above applies specially in our setting, since our simplicial complexes will have a natural order of the faces given by their occurrence as we vary the parameter of the Čech or Mayer-Vietoris complex. However, we don't pursue this path as it does not entail a theoretical advantage in the complexity. However, in any future implementation of the algorithms described here, one should take into account these computations of the homology, as they are more efficient in practice. \P

3§3–2 Čech complex and the functorial Nerve theorem

The Čech complex is the nerve of a collection of closed balls of the same size. Because of this, it captures the homology of a cloud of points.

Definition 3§3 5. [167; III.2]. Let $X \subseteq \mathbb{R}^m$ be a finite set of points and $\varepsilon > 0$. The Čech complex of X of radius ε is the simplicial complex

$$\check{C}_\varepsilon(X) := \mathcal{N}\left(\left\{\overline{B}(x, \varepsilon) \mid x \in X\right\}\right) = \{\sigma \subseteq X \mid \cap_{x \in \sigma} \overline{B}(x, \varepsilon) \neq \emptyset\}. \quad (3.24)$$

Theorem 3§3 5. Let $X \subseteq \mathbb{R}^m$ be a finite set of points and $\varepsilon > 0$. Then $\mathcal{U}(X, \varepsilon)$ is homotopy equivalent to $[\check{C}_\varepsilon(X)]$.

Proof. The only issue to apply the nerve theorem (Theorem 3§3 1) directly is that its statement applies to open covers. We now show that this is not an issue for the case at hand.

Note that there is a sufficiently small $\delta > 0$ such that for all $t \in [0, \delta]$, $\check{C}_{\varepsilon+t}(X) = \check{C}_\varepsilon(X)$. This identity allows us to interpret $\check{C}_{\varepsilon+t}(X)$ as the nerve of $\{B(x, \varepsilon + t) \mid x \in X\}$ for all $t \in (0, \delta)$. By making δ smaller if necessary, we can guarantee that for all $t \in [0, \delta]$, $\mathcal{U}(X, \varepsilon) \hookrightarrow \cup\{B(x, \varepsilon + t) \mid x \in X\}$ is a homotopy equivalence, by Durfee's theorem (Theorem 2§3 1). Hence we can apply the nerve theorem (Theorem 3§3 1) and finish the proof. \square

A drawback of the above theorem is that it does not allow us to deal with unions of Čech complexes. In order to do this, we need a version that is functorial, i.e., that involves an explicit map. This is what we do below, giving two proofs. One using the nerve theorem and one using the homological inclusion-exclusion transfer, which will play a fundamental role later.

Functorial nerve theorem

Let $\mathcal{X} \subseteq \mathbb{R}^m$ be a finite set. We want a map

$$\Delta^{\mathcal{X}} \rightarrow \mathbb{R}^m$$

mapping $[\check{C}_{\varepsilon}(\mathcal{X})]$ into $\mathcal{U}(\mathcal{X}, \varepsilon)$ and inducing an isomorphism in homology. An obvious candidate is

$$\begin{aligned} \check{\pi} : \Delta^{\mathcal{X}} &\rightarrow \mathbb{R}^m \\ \sum_{x \in \mathcal{X}} t_x [x] &\mapsto \sum_{x \in \mathcal{X}} t_x x \end{aligned} \tag{3.25}$$

which is the unique affine map sending each vertex $[x]$ to the corresponding point x . We note that the rule of this map is independent of the finite set \mathcal{X} , which is why we omit the subscript.

The next theorem shows that $\check{\pi}$ is the map we are looking for.

Theorem 3^{§3}6 (Homological functorial nerve theorem). [91; Theorem 5.2]. *The restriction $\check{\pi}_* : [\check{C}_{\varepsilon}(\mathcal{X})] \rightarrow \mathcal{U}(\mathcal{X}, \varepsilon)$ of the affine map $\check{\pi}$ induces an isomorphism in homology:*

$$\check{\pi}_* : H_*([\check{C}_{\varepsilon}(\mathcal{X})]) \rightarrow H_*(\mathcal{U}(\mathcal{X}, \varepsilon)).$$

The following lemma is needed to show that $\check{\pi}$ maps $[\check{C}_{\varepsilon}(\mathcal{X})]$ to $\mathcal{U}(\mathcal{X}, \varepsilon)$.

Lemma 3^{§3}7. [91; Lemma 5.1]. *Let $\mathcal{X} \subseteq \mathbb{R}^m$ be a finite set of points and $\varepsilon > 0$. If $\bigcap_{x \in \mathcal{X}} \overline{B}(x, \varepsilon) \neq \emptyset$, then $\text{conv}(\mathcal{X}) \subseteq \mathcal{U}(\mathcal{X}, \varepsilon)$.*

Proof of Lemma 3^{§3}7. Without loss of generality, by Carathéodory's Theorem [424; Proposition 1.15], we can assume that $\text{conv}(\mathcal{X})$ is a simplex. Suppose $\bigcap_{x \in \mathcal{X}} \overline{B}(x, \varepsilon) \neq \emptyset$. For a nonempty $\sigma \subseteq \mathcal{X}$, take $p' \in \bigcap_{x \in \sigma} \overline{B}(x, \varepsilon)$, and let p_σ be the closest point to p' in $\text{conv}(\sigma)$. Then $p_\sigma \in \bigcap_{x \in \sigma} \overline{B}(x, \varepsilon)$. To see this, just note that when moving from p' to p_σ , the distance to each $x \in \sigma$ decreases.

We now consider the barycentric subdivision of $\text{conv}(\mathcal{X})$ with respect to the family of points $\{p_\sigma \mid \sigma \subseteq \mathcal{X}\}$, which is a barycentric subdivision where we take p_σ instead of taking the centroid in the relative interior of each face $\sigma \subseteq \mathcal{X}$. It is sufficient to show that $\text{conv}(\Delta) \subseteq \mathcal{U}(\mathcal{X}, \varepsilon)$ for every maximal simplex of this subdivision. Every such simplex Δ has the form $\text{conv}(p_{\{x_1\}}, p_{\{x_1, x_2\}}, \dots, p_{\mathcal{X}})$, where $x_i \in \mathcal{X}$, so we have $p_{\{x_1, \dots, x_a\}} \in \bigcap_{i=1}^a \overline{B}(x_i, \varepsilon) \subseteq \overline{B}(x_1, \varepsilon)$ for each of its vertices $p_{\{x_1, \dots, x_a\}}$. Therefore, $\Delta \subseteq B(x_1, \varepsilon) \subseteq \mathcal{U}(\mathcal{X}, \varepsilon)$ by convexity. \square

First proof of Theorem 3^{§3}6. Let $\sigma \in \check{C}_{\varepsilon}(\mathcal{X})$. Then $\bigcap_{x \in \sigma} \overline{B}(x, \varepsilon) \neq \emptyset$ and so, by Lemma 3^{§3}7 applied to σ , $\text{conv}(\sigma) \subseteq \mathcal{U}(\sigma, \varepsilon) \subseteq \mathcal{U}(\mathcal{X}, \varepsilon)$. As $[\check{C}_{\varepsilon}(\mathcal{X})] = \bigcup_{\sigma \in \check{C}_{\varepsilon}(\mathcal{X})} \Delta^\sigma$ and

$\text{conv}(\sigma) = \check{\pi}(\Delta^\sigma)$, it follows that $\check{\pi}([\check{C}_\varepsilon(X)]) \subseteq \mathcal{U}(X, \varepsilon)$. Thus $\check{\pi}$ is a continuous map $[\check{C}_\varepsilon(X)] \rightarrow \mathcal{U}(X, \varepsilon)$. It only remains to prove that it induces an isomorphism in homology.

Let $\{\phi_x\}_{x \in X}$ be a partition of unity in $\mathcal{U}(X, \varepsilon)$ subordinate to $\{\bar{B}(x, \varepsilon)\}_{x \in X}$. That is, the ϕ_x are continuous maps $\phi_x : \mathcal{U}(X, \varepsilon) \rightarrow [0, 1]$ such that ϕ_x is zero outside $\bar{B}(x, \varepsilon)$ and $\sum_{x \in X} \phi_x = 1$. (For example, we could take $\phi_x := \frac{\rho_x}{\sum_{x \in X} \rho_x}$ with $\rho_x(p) := \max\{\varepsilon - \|p - x\|, 0\}$.) We define the continuous map

$$\begin{aligned}\varphi : \mathcal{U}(X, \varepsilon) &\rightarrow [\check{C}_\varepsilon(X)] \\ p &\mapsto \sum_{x \in X} \phi_x(p)[x]\end{aligned}$$

and will show that $\check{\pi} \circ \varphi$ is homotopic to the identity $\text{id}_{\mathcal{U}(X, \varepsilon)}$. To do so, consider the linear homotopy

$$t \mapsto t(\check{\pi} \circ \varphi) + (1 - t)\text{id}_{\mathcal{U}(X, \varepsilon)}$$

between $\check{\pi} \circ \varphi$ and $\text{id}_{\mathcal{U}(X, \varepsilon)}$. To show that this linear homotopy restricts to a homotopy of functions $\mathcal{U}(X, \varepsilon) \rightarrow \mathcal{U}(X, \varepsilon)$, we only have to check that for every $p \in \mathcal{U}(X, \varepsilon)$, the segment $[\check{\pi}(\varphi(p)), p]$ is contained in $\mathcal{U}(X, \varepsilon)$.

In order to check this, put $X_0 := \{x \in X \mid \phi_x(p) \neq 0\}$ and note that

$$\check{\pi}(\varphi(p)) = \sum_{x \in X_0} \phi_x(p)x \in \text{conv}(X_0).$$

We have $p \in \bigcap_{x \in X_0} \bar{B}(x, \varepsilon)$ since $\phi_x(p) \neq 0$ implies $d(x, p) < \varepsilon$. By Lemma 3§3.7 we have $\text{conv}(X_0) \subseteq \mathcal{U}(X_0, \varepsilon)$. So $\check{\pi}(\varphi(p)) \in \mathcal{U}(X, \varepsilon)$. Hence there exists $\tilde{x} \in X_0$ such that $\check{\pi}(\varphi(p)) \in \bar{B}(\tilde{x}, \varepsilon)$. Since also $p \in \bar{B}(\tilde{x}, \varepsilon)$, we have $[p, \check{\pi}(\varphi(p))] \subseteq \bar{B}(\tilde{x}, \varepsilon) \subseteq \mathcal{U}(X_0, \varepsilon) \subseteq \mathcal{U}(X, \varepsilon)$.

So we have shown that $\check{\pi} \circ \varphi$ is homotopic to the identity. Therefore,

$$\check{\pi}_* : H_\ell([\check{C}_\varepsilon(X)]) \rightarrow H_\ell(\mathcal{U}(X, \varepsilon))$$

is an epimorphism for every ℓ . Now, by Theorem 3§3.5, $H_\ell([\check{C}_\varepsilon(X)])$ and $H_\ell(\mathcal{U}(X, \varepsilon))$ are isomorphic finitely generated abelian groups. We conclude that $\check{\pi}$ induces an isomorphism in homology, because a surjective homomorphism between isomorphic finitely generated abelian groups is an isomorphism [336; Exercises 4.2(10)]. \square

Homological inclusion-exclusion transfer

The “inclusion-exclusion” in the title above refers to the idea of inferring information on the homology of a space X (or a map between spaces) from the homology of intersections of subspaces, in a manner akin to the combinatorial inclusion-exclusion principle.

Let X be a topological space and $C_\bullet(X)$ be its singular chain complex. For $A, B \subseteq X$ we denote by $C_\bullet(A + B)$ the subcomplex of $C_\bullet(A \cup B)$ generated by the singular simplices that either lie inside A or inside B . We will say that a finite family $\{X_i\}_{i \in I}$ of subsets of X satisfies the *Mayer-Vietoris hypothesis* when, for every non-empty $J \subseteq I$ and $k \in I \setminus J$, the inclusion of chain complexes

$$C_\bullet\left(X_k + \bigcup_{j \in J} X_j\right) \hookrightarrow C_\bullet\left(X_k \cup \bigcup_{j \in J} X_j\right),$$

induces an isomorphism in homology. We will say that it satisfies the *inductive Mayer-Vietoris hypothesis* when, for all finite families $\{F_\ell\}_{\ell \in \mathbb{L}}$ of subsets of I , the family of intersections $\{\cap_{h \in F_\ell} X_h\}_{\ell \in \mathbb{L}}$ satisfies the Mayer-Vietoris hypothesis.

The reason to introduce this last notion is that it gives a common name to the three main situations that we will encounter and in which this condition holds:

- 1) The family $\{X_i\}_{i \in I}$ is a family of open subsets of $\bigcup_{i \in I} X_i$. The inductive Mayer-Vietoris hypothesis holds due to [216; Proposition 2.21].
- 2) The family $\{X_i\}_{i \in I}$ is a family of closed subcomplexes of a CW-complex. The inductive Mayer-Vietoris hypothesis holds due to [346; Cor. 8.44].
- 3) The family $\{X_i\}_{i \in I}$ is a family of closed semialgebraic sets in \mathbb{R}^N . The inductive Mayer-Vietoris hypothesis holds due to the Semialgebraic Triangulation Theorem [70; Theorem 9.2.1] combined with situation 2) above.

In all these three situations, the inductive Mayer-Vietoris hypothesis will allow us to use the Mayer-Vietoris exact sequence in inductive arguments, such as the one for the following theorem.

Theorem 3§3 8 (Homological inclusion-exclusion transfer). [91; Theorem 5.4]. Let X and Y be topological spaces and $\{X_i\}_{i \in I}$, $\{Y_j\}_{j \in J}$ be finite families of subsets of X and Y , respectively, satisfying the inductive Mayer-Vietoris hypothesis. We assume that $X = \bigcup_{i \in I} X_i$ and $Y = \bigcup_{j \in J} Y_j$. Moreover, let $f : X \rightarrow Y$ be a continuous map such that $f(X_i) \subseteq Y_j$ for all $i \in I$. Let k be an integer such that for all nonempty $J \subseteq I$ with $|J| \leq k$, the morphism

$$H_\ell(f) : H_\ell(\cap_{j \in J} Y_j) \rightarrow H_\ell(\cap_{j \in J} Y_j)$$

is an isomorphism for $\ell < k$ and an epimorphism for $\ell = k$. Then

$$H_\ell(f) : H_\ell(X) \rightarrow H_\ell(Y)$$

is an isomorphism for $\ell < k$ and an epimorphism for $\ell = k$.

The following is an immediate consequence of Theorem 3§3 8.

Corollary 3§3 9. [91; Corollary 5.5]. Under the assumptions of Theorem 3§3 8 if, for all nonempty $J \subseteq I$, $f : \cap_{j \in J} X_j \rightarrow \cap_{j \in J} Y_j$ induces an isomorphism in homology, then $f : X \rightarrow Y$ induces an isomorphism in homology. \square

Proof of Theorem 3§3 8. The proof is by induction on the size of I , for arbitrary k . The assertion is trivial when I is a singleton.

Let $I = I' \cup \{i_0\}$ with $i_0 \notin I'$. By assumption, we have $f(\cup_{i \in I'} X_i) \subseteq \cup_{i \in I'} Y_i$, $f(X_{i_0}) \subseteq Y_{i_0}$ and $f(\cup_{i \in I'} (X_{i_0} \cap X_i)) \subseteq \cup_{i \in I'} (Y_{i_0} \cap Y_i)$. By induction hypothesis, the maps

$$\beta_\ell^1 : H_\ell(X_{i_0}) \rightarrow H_\ell(Y_{i_0}) \text{ and } \beta_\ell^2 : H_\ell(\cup_{i \in I'} X_i) \rightarrow H_\ell(\cup_{i \in I'} Y_i)$$

induced by f are isomorphisms for $\ell < k$ and epimorphisms for $\ell = k$, and the maps

$$\alpha_\ell : H_\ell(\cup_{i \in I'} (X_{i_0} \cap X_i)) \subseteq H_\ell(\cup_{i \in I'} (Y_{i_0} \cap Y_i))$$

$$\begin{array}{ccc}
H_\ell \left(\cup_{i \in I'} (X_{i_0} \cap X_i) \right) & \xrightarrow{\alpha_\ell} & H_\ell \left(\cup_{i \in I'} (Y_{i_0} \cap Y_i) \right) \\
\downarrow & & \downarrow \\
H_\ell(X_{i_0}) \oplus H_\ell(\cup_{i \in I'} X_i) & \xrightarrow{\beta_\ell} & H_\ell(Y_{i_0}) \oplus H_\ell(\cup_{i \in I'} Y_i) \\
\downarrow & & \downarrow \\
H_\ell(X_{i_0} \cup (\cup_{i \in I'} X_i)) & \longrightarrow & H_\ell(Y_{i_0} \cup (\cup_{i \in I'} Y_i)) \\
\downarrow \gamma_\ell & & \downarrow \\
H_{\ell-1} \left(\cup_{i \in I'} (X_{i_0} \cap X_i) \right) & \xrightarrow{\alpha_{\ell-1}} & H_{\ell-1} \left(\cup_{i \in I'} (Y_{i_0} \cap Y_i) \right) \\
\downarrow & & \downarrow \\
H_{\ell-1}(X_{i_0}) \oplus H_{\ell-1}(\cup_{i \in I'} X_i) & \xrightarrow{\beta_{\ell-1}} & H_{\ell-1}(Y_{i_0}) \oplus H_{\ell-1}(\cup_{i \in I'} Y_i)
\end{array}$$

Figure 3§3 6: Natural map of Mayer-Vietoris sequences in the proof of Theorem 3§3 8.

are isomorphisms for $\ell < k - 1$ and epimorphisms for $\ell = k - 1$. Here we view $\cap_{j \in J} (X_{i_0} \cap X_j) = X_{i_0} \cap (\cap_{j \in J} X_j)$ as an intersection of $|J| + 1$ subsets, for $J \subseteq I'$ with $|J| \leq k - 1$. (Note that the inductive Mayer-Vietoris hypothesis is necessary to apply the induction step, as it guarantees that the families $\{X_{i_0} \cap X_j\}_{j \in J}$ and $\{Y_{i_0} \cap Y_j\}_{j \in J}$ satisfy the induction hypothesis; this is not necessarily the case with the Mayer-Vietoris hypothesis.)

The map of pairs $f : (\cup_{i \in I'} X_i, X_{i_0}) \rightarrow (\cup_{i \in I'} Y_i, Y_{i_0})$, and the fact that these pairs satisfy the Mayer-Vietoris hypothesis, induce the commutative diagram of Mayer-Vietoris sequences shown in Figure 3§3 6, where α_ℓ , β_ℓ and γ_ℓ are the maps in homology induced by f .

In this figure, the induction hypothesis ensures that α_ℓ is an isomorphism for $\ell < k - 1$, an epimorphism for $\ell = k - 1$, and that β_ℓ is an isomorphism for $\ell < k$ and an epimorphism for $\ell = k$. This gives us two cases to consider: $\ell \leq k - 1$ and $\ell = k$.

If $\ell \leq k - 1$, then $\alpha_{\ell-1}$, $\beta_{\ell-1}$ and β_ℓ are isomorphisms and α_ℓ is an epimorphism. Therefore, by the Five Lemma [347; Proposition 2.72(iii)], γ_ℓ is an isomorphism.

Otherwise, if $\ell = k$, then β_ℓ and $\alpha_{\ell-1}$ are epimorphisms, and $\beta_{\ell-1}$ is an isomorphism. Therefore, by the Four Lemma [347; Proposition 2.72(ii)], γ_ℓ is an epimorphism.

The statement now follows by induction. □

Remark 3§3 6. Theorem 3§3 8 can be considered a homological version of the Vietoris-Begle Theorem [379; p. 344] for homology in terms of coverings. For example, one can see that for a locally trivial fibration $\pi : E \rightarrow B$ with $(k - 1)$ -connected fiber F , the homological inclusion-exclusion transfer implies the homological Vietoris-Begle Theorem since, for every trivializing open subset $U \subseteq B$, $H_\ell(F \times U) \rightarrow H_\ell(U)$ is an isomorphism for $\ell < k$ and an epimorphism for $\ell = k$. ¶

We give now an alternative proof of the functorial nerve theorem (Theorem 3§3 6) that does not use the nerve theorem (Theorem 3§3 5) but the homological inclusion-exclusion transfer we have just proven.

Second proof of Theorem 3§3 6. By Lemma 3§3 7, arguing as in the previous proof, the map

$\check{C}\pi : [\check{C}_\varepsilon(\mathcal{X})] \rightarrow \mathcal{U}(\mathcal{X}, \varepsilon)$ is a well-defined continuous map. Now, using the first part of the proof of Lemma 3^{§3}7, we construct a map $q : \check{C}_\varepsilon(\mathcal{X}) \setminus \{\emptyset\} \rightarrow [\check{C}_\varepsilon(\mathcal{X})]$ such that for each $\sigma \in \check{C}_\varepsilon(\mathcal{X})$,

$$q(\sigma) \in \Delta^\sigma \text{ and } \check{C}\pi(q(\sigma)) \in \bigcap_{x \in \sigma} \overline{B}(x, \varepsilon).$$

Now, let

$$\mathcal{M} := \{(\sigma_1, \dots, \sigma_I) \mid \ell \geq 1; \text{ for all } i, \# \sigma_i = i, \sigma_i \subseteq \sigma_{i+1} \text{ and } \sigma_i \in \check{C}_\varepsilon(\mathcal{X})\}$$

be the set of maximal flags of $\check{C}_\varepsilon(\mathcal{X})$. We have then that

$$\mathcal{T} := \{\text{conv}(q(\sigma_1), \dots, q(\sigma_I)) \mid (\sigma_1, \dots, \sigma_I) \in \mathcal{M}\}$$

and

$$\mathcal{B} := \left\{ \bigcup_{x \in \sigma} \overline{B}(x, \varepsilon) \mid (\sigma_1, \dots, \sigma_I) \in \mathcal{M} \right\}$$

are closed covers of, respectively, $[\check{C}_\varepsilon(\mathcal{X})]$ and $\mathcal{U}(\mathcal{X}, \varepsilon)$. Note that for \mathcal{T} this is so because it is the set of maximal faces of the barycentric subdivision with respect to the family of points given by $\{q(\sigma) \mid \sigma \in \check{C}_\varepsilon(\mathcal{X})\}$.

Furthermore, one can see that for every $(\sigma_1, \dots, \sigma_I) \in \mathcal{M}$,

$$\check{C}\pi(\text{conv}(q(\sigma_1), \dots, q(\sigma_I))) \subseteq B(x_1, \varepsilon) \subseteq \bigcup_{x \in \sigma_I} B(x, \varepsilon)$$

where $\sigma_1 = \{x_1\}$. Hence, by the homological inclusion-exclusion transfer (Corollary 3^{§3}9), it is enough to check that on the intersections $\check{C}\pi$ induces an isomorphism in homology, since both \mathcal{T} and \mathcal{B} satisfy the inductive Mayer-Vietoris hypothesis (as they can be as covers formed by closed semialgebraic sets).

Now, every intersection of elements of \mathcal{T} is a convex set and so contractible; and every intersection of elements of \mathcal{B} is a union of closed balls with non-empty intersection and so contractible (by taking the continuous retraction onto any common point). Thus $\check{C}\pi$ induces trivially an isomorphism in homology for every intersection and we are done. \square

Remark 3^{§3}7. Let us note that the proof above is complete and accessible to every first year algebraic topology student who has covered the basics of homology theory. Standard references in topological data analysis (such as [167]) don't usually prove the nerve theorem at all. In this way, the above proof can be a nice addition to introductory courses in topological data analysis. \P

3^{§3–3} Vietoris–Rips graph and complex

Building the Čech complex requires to check if the intersection of many Euclidean balls is non-empty. From the viewpoint of complexity, this is not a restriction to us, since it can be done in singly exponential time using any algorithm for deciding (Γ) (such as the one in [34; Ch. 14]). However, one may feel uncomfortable to use such a result in our numerical approach, because, on the one hand, it feels contrary to the grid method's philosophy to rely

on an step of high computational cost and, on the other hand, it would make any potential implementation tedious.

Because of the above, we introduce a variation of the Čech complex where we only have to check the pairwise distance of the points in our point clouds. We provide at the end, an approximation theorem that guarantees us that we still get the same homology. We note that functoriality will not be lost, as the new simplicial complex will contain the Čech complex with the isomorphism in homology induced just by inclusion.

Vietoris-Rips complexes and graphs

The main idea of the Vietoris-Rips complex is to get a simpler complex than the Čech complex at the potential cost of losing some topological information, because of the added faces.

Definition 3§3 6. Let $\mathcal{X} \subseteq \mathbb{R}^m$ be a finite set and $\varepsilon > 0$, the *Vietoris-Rips complex* of \mathcal{X} of radius ε , $\mathcal{VR}_\varepsilon(\mathcal{X})$, is the simplicial complex given by

$$\mathcal{VR}_\varepsilon(\mathcal{X}) := \{\sigma \subseteq \mathcal{X} \mid \text{for all } \{x, \tilde{x}\} \subseteq \sigma, \text{dist}(x, \tilde{x}) \leq 2\varepsilon\}. \quad (3.26)$$

One can easily see that $\check{C}_\varepsilon(\mathcal{X}) \subseteq \mathcal{VR}_\varepsilon(\mathcal{X})$, since the condition for the Čech complex requires that the intersection of all the balls to be non-empty while the one of the Vietoris-Rips complex only requires all pairwise intersections to be non-empty. In the other direction, one has the following proposition.

Proposition 3§3 10 (Jung's Theorem). [146; Theorem 2.5]. Let $\mathcal{X} \subseteq \mathbb{R}^m$ be a finite set and $\varepsilon > 0$. Define

$$\vartheta_m := \sqrt{\frac{2m}{m+1}} \in [1, \sqrt{2}). \quad (3.27)$$

Then $\check{C}_\varepsilon(\mathcal{X}) \subseteq \mathcal{VR}_\varepsilon(\mathcal{X}) \subseteq \check{C}_{\varepsilon\vartheta_m}(\mathcal{X})$. □

Remark 3§3 8. We note that the constant ϑ_m is optimal with respect to the inclusion $\mathcal{VR}_\varepsilon(\mathcal{X}) \subseteq \check{C}_{\varepsilon\vartheta_m}(\mathcal{X})$. To see this, we only have to consider the vertices of the standard simplex. ¶

Before continuing, we should observe that all information of the Vietoris-Rips complex is encoded in its graph. This motivates the definition of the Vietoris-Rips graph.

Definition 3§3 7. Let $\mathcal{X} \subseteq \mathbb{R}^m$ be a finite set and $\varepsilon > 0$, the *Vietoris-Rips graph* of \mathcal{X} of radius ε , $\mathbb{G}_\varepsilon^{\mathcal{VR}}(\mathcal{X})$, is the graph with vertex set \mathcal{X} whose edge set is given by

$$E(\mathbb{G}_\varepsilon^{\mathcal{VR}}(\mathcal{X})) := \{\overline{xy} \mid \text{dist}(x, y) \leq 2\varepsilon\}. \quad (3.28)$$

Then the following proposition is straightforward. Recall that a *clique* of a graph is a subset of vertices such that the induced graph is complete, i.e., there is an edge between every two vertices.

Proposition 3§3 11. Let $\mathcal{X} \subseteq \mathbb{R}^m$ be a finite set and $\varepsilon > 0$. Then for all $\sigma \subseteq \mathcal{X}$, $\sigma \in \mathcal{VR}_\varepsilon(\mathcal{X})$ iff σ is a clique of $\mathbb{G}_\varepsilon^{\mathcal{VR}}(\mathcal{X})$. □

One can formalize the above by saying that the Vietoris-Rips complex is the clique complex of the Vietoris-Rips graph. The importance of the Vietoris-Rips graph is that it can be manipulated at a lower cost than the Čech complex and doing so gives improvements both in practice and in theory [425].

Attali-Lieutier-Salinas approximation theorem

In principle, one might consider that the Mayer-Vietoris complex will lose always topological information. However, just by strengthening a little the conditions of the Niyogi-Smale-Weinberger approximation theorem, one can still guarantee that no topological information is lost as shown by Attali, Lieutier and Salinas [14, 15].

Theorem 3^{§3}12 (Attali-Lieutier-Salinas approximation theorem). *Let $X \subseteq \mathbb{R}^m$ be a compact set such that $\tau(X) > 0$ and $\mathcal{X} \subseteq \mathbb{R}^m$ a finite set. Then for all $\varepsilon > 0$ such that*

$$7 \operatorname{dist}_H(\mathcal{X}, X) < \varepsilon < \frac{1}{5}\tau(X), \quad (3.29)$$

X is a deformation retract of $\mathcal{U}(\mathcal{X}, \varepsilon)$ and the inclusion $\iota : \check{C}_\varepsilon(\mathcal{X}) \hookrightarrow \mathcal{VR}_\varepsilon(\mathcal{X})$ is an homotopy equivalence. In particular, X and $\mathcal{VR}_\varepsilon(\mathcal{X})$ have isomorphic homology groups (via $\iota_* \circ (\check{C}\pi_*)^{-1}$).

Proof. Let $\tau := \tau(X)$ and $d := \operatorname{dist}_H(X, \mathcal{X})$. Then combining [15; Lemma 5], [15; Theorem 7] and [15; Lemma 12], with $\mu = 1$, we see that the inclusion $\check{C}_\varepsilon(\mathcal{X}) \hookrightarrow \mathcal{VR}_\varepsilon(\mathcal{X})$ induces an homotopy equivalence whenever $\vartheta_m \varepsilon + \delta < t$ and

$$t - \sqrt{t^2 - (\vartheta_m \varepsilon + \delta)^2} < (2 - \vartheta_m)\varepsilon - 2\delta$$

for some $t < \tau(X)$ and $\delta > d$. Taking δ to d and t to τ , the condition simply becomes $\vartheta_m \varepsilon + d < \tau$ and

$$\tau - \sqrt{\tau^2 - (\vartheta_m \varepsilon + d)^2} < (2 - \vartheta_m)\varepsilon - 2d.$$

Divide now everything by d and rename $x := \varepsilon/d$ and $\alpha = \tau/d$, so that we get $\vartheta_m x + 1 < \alpha$ and

$$\alpha - \sqrt{\alpha^2 - (\vartheta_m x + 1)^2} < (2 - \vartheta_m)x - 2. \quad (3.30)$$

We will show that this condition holds whenever

$$7 < x < \frac{\alpha}{5}$$

from where the above claim follows, because in this case it also holds $3 < x < \alpha/2$ which is the condition (3.10) of the Niyogi-Smale-Weinberger approximation theorem (Theorem 3^{§1}8). The last claim is just applying Theorem 3^{§3}6.

Consider the left hand side as a map $f : (\vartheta_m x + 1, \infty) \rightarrow \mathbb{R}_>$ of α . Then

$$f'(\alpha) = 1 - \frac{\alpha}{\sqrt{\alpha^2 - (\vartheta_m x + 1)^2}} = \frac{-f(\alpha)}{\sqrt{\alpha^2 - (\vartheta_m x + 1)^2}} < 0$$

and so f decreases with α . This means that for $\alpha > 5x$, we have

$$\alpha - \sqrt{\alpha^2 - (\vartheta_m x + 1)^2} < 5x - \sqrt{25x^2 - (\vartheta_m x + 1)^2},$$

and so, for $\alpha > 5x$, (3.30) is implied by

$$5x - \sqrt{25x^2 - (\vartheta_m x + 1)^2} < (2 - \vartheta_m)x - 2$$

which, as $\vartheta_m \in [1, \sqrt{2}]$, is implied by

$$5x - \sqrt{25x^2 - (\sqrt{2}x + 1)^2} < (2 - \sqrt{2})x - 2.$$

Eliminating squares, this expression becomes

$$6(\sqrt{2} - 2)x^2 + 6(2 + \sqrt{2})x + 5 < 0$$

which holds for $x > 7$. The proof is concluded. \square

Remark 3^{§3}9. The above result cannot be found in any of the papers using the grid method to compute homology groups **[142, 88, 91, 92]**. This will allow this thesis to have a considerable improvement over the results there, since our algorithms would only require evaluation of distances to construct the simplicial complexes with the same homology. \P

Further comments

Most of the exposition in this chapter regarding the Niyogi-Smale-Weinberger approximation theorem (Theorem 3^{§1}8) and the lower bounds of the reach follows the lines of **[88]**. However, we have given full proofs of all the statements, since there is no single reference where all details were together. The last section follows mainly the guidelines from **[91]**, from where many statements and proofs (concretely those of the functorial nerve theorem (Theorem 3^{§3}6 and the inclusion-exclusion transfer (Theorem 3^{§3}8 and Corollary 3^{§3}9)) were taken with minor modifications.

The major addition of this chapter is the inclusion of the Vietoris-Rips complex and the Attali-Lieutier-Salinas approximation theorem (Theorem 3^{§3}12) which could lead to an efficient implementation of the algorithms exposed in this thesis and avoid the use of expensive subroutines to construct the simplicial complexes our algorithms rely on.

刘伯承同志经常讲一句四川话：“黃猫、黑猫，只要捉住老鼠就是好猫。”

邓小平，怎样恢复农业生产（一九六二年七月七日）

4

Numerical algorithms for the homology of semialgebraic sets

After the Three Years of Great Famine (三年大饥荒), consequence of the failures of the Great Leap Forward (大跃进) of Mao Zedong (毛泽东), the Chinese Communist Party had to undertake a serious reform of Chinese agriculture and economy to avoid an even greater disaster [Q5]. Liu Shaoqi (刘少奇) and Deng Xiaoping (邓小平) took this challenge and led a sequence of necessary reforms inside China [Q5].

While they were justifying their reform, Deng Xiaoping would pronounce his famous citation of the Sichuan proverb “Yellow cat, black cat; as long as it catches the old rat, good cat” (黃猫、黑猫，只要捉住老鼠就是好猫) during his speech “Restore Agricultural Production” (怎样恢复农业生产) on the 7th of July of 1962 [Q3] (cf. [Q4]). Showcasing his future heterodox approach to economy, although not to politics, he would claim in this speech that “[o]ur sole aim is to win by taking advantage of given conditions” and that “we should not stick to a fixed mode of relations of productions but adopt whatever mode that can help mobilize the masses’ initiative” [Q3].

Leaving aside Chinese history and politics and coming back to the rhetoric of this thesis, we will just make these words ours in the context of computational semialgebraic geometry and say:

符号算法、数值算法，只要能解决未解决的问题就是好算法。¹

And paraphrasing Deng Xiaoping, we say that our sole aim is to solve the problem taking

The introduction of this chapter is unorthodox, but, after several chapters, it is important to recover the focus. For this, we are using this historical metaphor built around the famous Sichuan proverb of the cat. In this way, we hope that the underlying philosophy of this thesis is transmitted better by these catchy phrases. The reader who does not like this rhetorical style should not worry, because the mathematical exposition will be in the same rigorous metaphor-free style as it has been.

¹Symbolic algorithm, numerical algorithm; as long as it can solve the unsolved problem, good algorithm.

advantage of given conditions and that we should not stick to a fixed mode of computation but adopt whatever mode that can help mobilize the answers.

This philosophy means that we should not limit ourselves to the symbolic mode, but embrace any mode that allows us to progress, such as the numerical one. In this chapter, we show the numerical algorithms that improve the current state-of-the-art in the path towards **(B)** and **(B)**. This chapter is the climax of this thesis. Chapters **1**, **2** and **3** were just leading us here.

First, we show the recipe for constructing simplicial approximations ; second, we show how the condition numbers $\bar{\kappa}$ and $\bar{\kappa}_{\text{aff}}$ can be estimated fast; third, we show a numerical algorithm solving **(B)** and **(B)** that runs in singly exponential time with high probability; and fourth and last, we prove that this algorithm is stable, i.e., that it can run in finite precision and produce correct results.

4§1 Simplicial approximation of semialgebraic sets

We begin by showing the basic recipe by which one can obtain a simplicial approximation of a well-posed semialgebraic set. In the next section, we will turn this recipe into effective algorithms. The basic ingredient of our recipe will be spherical r -nets $\mathcal{G} \subseteq \mathbb{S}^n$, from which the simplicial approximations are constructed.

Definition 4§1.1. Let $r > 0$. A spherical r -net is a finite set $\mathcal{G} \subseteq \mathbb{S}^n$ such that for all $x \in \mathbb{S}^n$, $\text{dist}_{\mathbb{S}}(x, \mathcal{G}) < r$.

Remark 4§1.1. We note that a spherical r -net is an r -net of \mathbb{S}^n , but the opposite is not true since the Euclidean distance does not coincide with the geodesic distance on the sphere. However, every r -net of \mathbb{S}^n is a spherical $\frac{\pi r}{2}$ -net. ¶

We divide our recipe in three steps. First, we show how a spherical r -net allows one to produce clouds of points approximating the desired closed semialgebraic sets in the Hausdorff distance; second, we show how to construct a homologically equivalent simplicial complex out of a family of clouds that approximates the atoms and whose intersections approximate the corresponding intersections of atoms; and third and last, we show how to approximate a general semialgebraic set by a closed one using the Gabrielov-Vorobjov approximation. Of course, all this will require the fundamental assumption $\bar{\kappa}(f) < \infty$.

4§1–1 Sampling of spherical semialgebraic sets

The following is the fundamental construction to approximate semialgebraic sets. The idea is to take those points in the spherical r -net \mathcal{G} that are near the semialgebraic set that we want to approximate, where ‘near’ means that they satisfy approximately the defining formula of the semialgebraic set.

Definition 4§1.2. [91; (6.6)]. Let $\mathcal{G} \subseteq \mathbb{S}^n$ be a spherical r -net, $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$ and Φ a lax formula over (f, t) . The *approximating cloud of \mathcal{G} -points for (f, t)* is the set

$$\mathcal{X}(f, t, \Phi, \mathcal{G}) := S_{D^{1/2}r}(f, t, \Phi) \cap \mathcal{G}, \quad (4.1)$$

where $S_{D^{1/2}r}(f, t, \Phi)$ is the algebraic neighborhood of $S(f, t, \Phi)$ defined in (2.6).

In the special case that Φ is an atomic formula of the form $(f_i \propto t_j \| f_i \|_W)$, we write $X_{i,j}^\propto(f, t, \mathcal{G})$ for the corresponding cloud of points.

The following theorem justifies the term ‘approximating’ as it gives the conditions under which the approximating cloud is near the corresponding semialgebraic set with respect to the Hausdorff distance.

Theorem 4^{S1}1 (Sampling theorem). [91; Theorem 6.5] and [92; Theorem 4.7]. Let $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$ and $T, r > 0$ be such that $\sqrt{2}D^{\frac{1}{2}}\bar{\kappa}(f)(r + T) < 1$ and $\mathbb{L}(t) > 2D^{\frac{1}{2}}r$. Then for every spherical r -net $\mathcal{G} \subseteq \mathbb{S}^n$ and lax formula Φ over (f, t) ,

$$\text{dist}_H(X(f, t, \Phi, \mathcal{G}), S(f, t, \Phi)) \leq \sqrt{2}D^{1/2}\bar{\kappa}(f)r.$$

Proof. By Proposition 2^{S1}2, we can assume, without loss of generality, that Φ is in disjunctive normal form. Furthermore, we can assume that Φ is purely conjunctive, since

$$\text{dist}_H(\bigcup_{i=1}^t A_i, \bigcup_{i=1}^t B_i) \leq \max_i \text{dist}_H(A_i, B_i)$$

for any compact sets $A_1, \dots, A_t, B_1, \dots, B_t \subseteq \mathbb{R}^{n+1}$.

By the construction of $X(f, t, \Phi, \mathcal{G})$ and Proposition 2^{S1}3,

$$\begin{aligned} X(f, t, \Phi, \mathcal{G}) &\subseteq S_{D^{1/2}r}(f, t, \Phi) \\ &\subseteq \mathcal{U}_S(S(f, t, \Phi), \sqrt{2}D^{1/2}\bar{\kappa}(f)r) \subseteq \mathcal{U}(S(f, t, \Phi), \sqrt{2}D^{1/2}\bar{\kappa}(f)r). \end{aligned}$$

By assumption on \mathcal{G} , for all $x \in S(f, \Phi)$, there is some $g_x \in \mathcal{G}$ such that $\text{dist}_{\mathbb{S}}(x, g_x) < r$. Thus $g_x \in \mathcal{U}_S(S(f, t, \Phi), r) \subseteq S_{D^{1/2}r}(f, t, \Phi)$, by Proposition 2^{S1}3, and so $g_x \in X(f, t, \Phi, \mathcal{G})$. Hence

$$\begin{aligned} S(f, t, \Phi) &\subseteq \mathcal{U}_S(X(f, t, \Phi, \mathcal{G}), r) \\ &\subseteq \mathcal{U}(X(f, t, \Phi, \mathcal{G}), r) \subseteq \mathcal{U}(X(f, t, \Phi, \mathcal{G}), \sqrt{2}D^{1/2}\bar{\kappa}(f)r), \end{aligned}$$

as $D \geq 1$ and $\bar{\kappa}(f) \geq 1$. The inequality on the Hausdorff distance follows from the two inclusions above by Proposition 3^{S1}1. \square

4^{S1}–2 Simplicial approximation of closed $S(f, t, \Phi)$

The sampling method above allows us to obtain approximations of semialgebraic sets as near as we want with respect to the Hausdorff distance. One interesting property of the method of sampling that we are using is the following identity:

$$X(f, t, \Phi, \mathcal{G}) = \Phi \left(X_{i,j}^=(f, t, \mathcal{G}), X_{i,j}^>(f, t, \mathcal{G}), X_{i,j}^<(f, t, \mathcal{G}) \mid i \in [q], j \in [e] \right). \quad (4.2)$$

Further, note that $X_{i,j}^=(f, t, \mathcal{G}) = X_{i,j}^>(f, t, \mathcal{G}) \cap X_{i,j}^<(f, t, \mathcal{G})$. This means that once we are able to approximate the atomic semialgebraic sets of the form $S(f, t, f_i \geq t_j \| f_i \|_W)$ and $S(f, t, f_i \leq t_j \| f_i \|_W)$, we can approximate all the possible lax semialgebraic sets that can be constructed from (f, t) .

This motivates the assumption on the following theorem, which gives us a way of approximating the homology of a semialgebraic set via a simplicial complex with the same homology.

Theorem 4§1.2 (Čech homology witness theorem). [91; Theorem 2.4] and [92; Theorem 4.6]. Let $f \in \mathcal{H}_d[q]$ and $T > 0$ be such that $2\bar{\kappa}(f)T < 1$, and $\varepsilon > 0$. Let $t \in (-T, T)^e$. Moreover, for $i \in [q]$ and $j \in [e]$, let $X_{i,j}^=, X_{i,j}^>, X_{i,j}^< \subseteq \mathbb{S}^n$ be closed subsets such that for all i, j , $X_{i,j}^= = X_{i,j}^> \cap X_{i,j}^<$ and for all purely conjunctive formula ϕ over (f, t) , we have

$$3 \text{dist}_{\text{H}} \left(\phi \left(X_{i,j}^=, X_{i,j}^>, X_{i,j}^< \mid i \in [q], j \in [e] \right), S(f, t, \phi) \right) < \varepsilon < \min \left\{ \frac{1}{48D^{3/2}\bar{\kappa}(f)}, \frac{\text{U}(t)}{12D^{\frac{1}{2}}} \right\}.$$

Then, for all lax formulas Φ over (f, t) , the set $S(f, t, \Phi)$ and the simplicial complex

$$\Phi \left(\check{C}_\varepsilon(X_{i,j}^=), \check{C}_\varepsilon(X_{i,j}^>), \check{C}_\varepsilon(X_{i,j}^<) \mid i \in [q], j \in [e] \right)$$

have the same homology.

Theorem 4§1.3 (Vietoris-Rips homology witness theorem). Let $f \in \mathcal{H}_d[q]$ and $T > 0$ be such that $2\bar{\kappa}(f)T < 1$, and $\varepsilon > 0$. Let $t \in (-T, T)^e$. Moreover, for $i \in [q]$ and $j \in [e]$, let $X_{i,j}^=, X_{i,j}^>, X_{i,j}^< \subseteq \mathbb{S}^n$ be closed subsets such that for all i, j , $X_{i,j}^= = X_{i,j}^> \cap X_{i,j}^<$ and for all purely conjunctive formula ϕ over (f, t) , we have

$$7 \text{dist}_{\text{H}} \left(\phi \left(X_{i,j}^=, X_{i,j}^>, X_{i,j}^< \mid i \in [q], j \in [e] \right), S(f, t, \phi) \right) < \varepsilon < \min \left\{ \frac{1}{120D^{3/2}\bar{\kappa}(f)}, \frac{\text{U}(t)}{30D^{\frac{1}{2}}} \right\}.$$

Then, for all lax formulas Φ over (f, t) , the set $S(f, t, \Phi)$ and the simplicial complex

$$\Phi \left(\mathcal{VR}_\varepsilon(X_{i,j}^=), \mathcal{VR}_\varepsilon(X_{i,j}^>), \mathcal{VR}_\varepsilon(X_{i,j}^<) \mid i \in [q], j \in [e] \right)$$

have the same homology

Proof of Theorem 4§1.2. Let

$$\mathfrak{C} := \Phi \left(\check{C}_\varepsilon(X_{i,j}^=), \check{C}_\varepsilon(X_{i,j}^>), \check{C}_\varepsilon(X_{i,j}^<) \mid i \in [q], j \in [e] \right).$$

Let $\rho > 0$ be such that

$$1) \sqrt{2}\bar{\kappa}(f)(\rho + T) < 1, \quad 2) \text{U}(t) > 2\rho, \quad \text{and } 3) 6D^{\frac{1}{2}}\varepsilon \leq \rho.$$

Note that such $\rho > 0$ can only exist if

$$6D^{\frac{1}{2}}\varepsilon < \min \left\{ \frac{1}{\sqrt{2}\bar{\kappa}(f)} - T, \frac{\text{U}(t)}{2} \right\}.$$

The assumption on ε implies that

$$6D^{\frac{1}{2}}\varepsilon < \min \left\{ \frac{1}{8D\bar{\kappa}(f)}, \frac{\text{U}(t)}{2} \right\}.$$

Now we note that

$$\min \left\{ \frac{1}{8D\bar{\kappa}(f)}, \frac{\text{U}(t)}{2} \right\} < \min \left\{ \frac{1}{\sqrt{2}\bar{\kappa}(f)} - T, \frac{\text{U}(t)}{2} \right\},$$

since

$$T < \frac{8D - \sqrt{2}}{8\sqrt{2}D} \frac{1}{\bar{\kappa}(f)},$$

which in turn is guaranteed by the assumption $2\bar{\kappa}(f)T < 1$ and $D \geq 1$. This guarantees the existence of the positive number ρ satisfying the desired inequalities.

We can assume, without loss of generality, that Φ is of the form

$$\Phi \equiv \bigvee_{\xi \in \Xi} \phi_\xi$$

where ϕ_ξ is a purely conjunctive lax formula over (f, t) in normal form, since, by Proposition 2^{S1}2 and its proof, this does not change any of the sets involved.

We will use the Inclusion-Exclusion Transfer (Corollary 3^{S3}9) to show that both $S(f, t, \Phi)$ and \mathfrak{C} have the same homology as the algebraic neighborhood $S_\rho(f, t, \Phi)$ for the ρ chosen above. By properties 1) and 2) of ρ , we can use the quantitative Durfee's theorem (Theorem 2^{S3}2) to deduce that, for all $I \subseteq \Xi$, the inclusion

$$\bigcap_{\xi \in I} S(f, t, \phi_\xi) = S(f, t, \wedge_{\xi \in I} \phi_\xi) \subseteq S_\rho(f, t, \wedge_{\xi \in I} \phi_\xi) = \bigcap_{\xi \in I} S_\rho(f, t, \phi_\xi)$$

induces an isomorphism in homology. In addition, we have

$$\bigcup_{\xi \in \Xi} S(f, t, \phi_\xi) = S(f, t, \Phi) \text{ and } \bigcup_{\xi \in \Xi} S_\rho(f, t, \phi_\xi) = S_\rho(f, t, \Phi),$$

so we can apply the Inclusion-Exclusion Transfer to the families $\{S(f, t, \phi_\xi)\}_{\xi \in \Xi}$ and $\{S_\rho(f, t, \phi_\xi)\}_{\xi \in \Xi}$ to deduce that the inclusion

$$S(f, t, \Phi) \hookrightarrow S_\rho(f, t, \Phi) \tag{4.3}$$

induces an isomorphism in homology.

It is enough to show that \mathfrak{C} and $S_\rho(f, t, \Phi)$ have the same homology. To do so, let us denote

$$X^\psi := \psi(X_{i,j}^=, X_{i,j}^>, X_{i,j}^< \mid i \in [q], j \in [e]) \tag{4.4}$$

where ψ is a purely conjunctive formula over (f, t) .

We first prove that for all z in the Euclidean neighborhood $\mathcal{U}(X^\psi, \varepsilon)$, we have that for any purely conjunctive formula ψ over (f, t) ,

$$\text{dist}_S \left(\frac{z}{\|z\|}, S(f, t, \psi) \right) < 6\varepsilon. \tag{4.5}$$

Indeed, for all $y_0, y_1 \in \mathbb{S}^n$,

$$\text{dist}_S(y_0, y_1) \leq \frac{\pi}{2} \text{dist}(y_0, y_1) \leq 2 \text{dist}(y_0, y_1).$$

Consequently,

$$\begin{aligned}
\text{dist}_{\mathbb{S}} \left(\frac{\mathbf{z}}{\|\mathbf{z}\|}, S(f, t, \psi) \right) &\leq 2 \text{dist} \left(\frac{\mathbf{z}}{\|\mathbf{z}\|}, S(f, t, \psi) \right) \\
&< 2 \text{dist} \left(\frac{\mathbf{z}}{\|\mathbf{z}\|}, \mathbf{z} \right) + 2d(\mathbf{z}, \mathcal{X}^\psi) + 2 \text{dist}_{\mathbb{H}}(\mathcal{X}^\psi, S(f, t, \psi)) \\
&\leq 2 \text{dist} \left(\frac{\mathbf{z}}{\|\mathbf{z}\|}, \mathbf{z} \right) + 2d(\mathbf{z}, \mathcal{X}^\psi) + 2\epsilon \\
&= 2 \text{dist}(\mathbf{z}, \mathbb{S}^n) + 2d(\mathbf{z}, \mathcal{X}^\psi) + 2\epsilon \\
&\leq 4 \text{dist}(\mathbf{z}, \mathcal{X}^\psi) + 2\epsilon \\
&\leq 6\epsilon,
\end{aligned}$$

where the second line follows from the triangular inequality for the Hausdorff distance, the third one from $\text{dist}_{\mathbb{H}}(\mathcal{X}^\psi, S(f, t, \psi)) < \epsilon/3$, the fourth one from the fact that $\frac{\mathbf{z}}{\|\mathbf{z}\|}$ is the nearest point to \mathbf{z} in \mathbb{S}^n , the fifth one from $\mathcal{X}^\psi \subseteq \mathbb{S}^n$ and the sixth and last one from $\mathbf{z} \in \mathcal{U}(\mathcal{X}^\psi, \epsilon)$. Hence we have shown (4.5). As the set $\mathcal{U}(\mathcal{X}^\psi, \epsilon)$ is not included in the sphere \mathbb{S}^n , it will be convenient to consider, for any set $S \subseteq \mathbb{S}^n$ the cone

$$\hat{S} := \{\lambda x \mid \lambda > 0, x \in S\}$$

over the spherical set S . Note that the inclusion

$$S \hookrightarrow \hat{S} \tag{4.6}$$

is a homotopy equivalence since the map

$$\begin{aligned}
[0, 1] \times \hat{S} &\rightarrow \hat{S} \\
(t, x) &\mapsto \frac{x}{(1-t) + t\|x\|_2}
\end{aligned}$$

induces a continuous retraction of \hat{S} onto S . These two spaces thus have the same homology. We will write $\hat{\mathcal{U}}$ and \hat{S} to denote the cones over the corresponding neighborhoods. As a consequence of (4.5) we deduce that for any purely conjunctive formula ψ over (f, t) ,

$$\mathcal{U}(\mathcal{X}^\psi, \epsilon) \subseteq \hat{\mathcal{U}}_{\mathbb{S}}(S(f, t, \psi), 6\epsilon) \subseteq \hat{S}_\rho(f, t, \psi),$$

the last by Proposition 2§1.3 and property 3) of ρ . We therefore have the inclusions

$$\begin{array}{ccc}
S(f, t, \psi) & \xhookrightarrow{\quad} & \mathcal{U}(\mathcal{X}^\psi, \epsilon) \\
& \searrow & \downarrow \\
& & \hat{S}_\rho(f, t, \psi)
\end{array} \tag{4.7}$$

the horizontal arrow by hypothesis and the diagonal by composition.

We now note that $S(f, t, \psi) \hookrightarrow \mathcal{U}(\mathcal{X}^\psi, \epsilon)$ induces an isomorphism of homology by the Niyogi-Smale-Weinberger approximation theorem (Theorem 3§1.8) and Theorem 3§2.6 and that so does $S(f, t, \psi) \hookrightarrow \hat{S}_\rho(f, t, \psi)$, now by Theorem 2§3.2, properties 1) and 2) of ρ

and (4.6). This implies that the inclusion $\mathcal{U}(X^\psi, \varepsilon) \hookrightarrow \widehat{S}_\rho(f, t, \psi)$, vertical arrow in (4.7), induces an isomorphism in homology. Thus, the map

$$\check{\pi} : [\check{C}_\varepsilon(X^\psi)] \rightarrow \mathcal{U}(X^\psi, \varepsilon)$$

defined in (3.25) composed with the vertical arrow in (4.7) yields a map

$$\check{\pi} : [\check{C}_\varepsilon(X^\psi)] \rightarrow \widehat{S}_\rho^\circ(f, t, \psi)$$

that induces an isomorphism in homology, by the homological functorial Nerve's theorem (Theorem 3^{S3}6). Summing up, we have shown that for every purely conjunctive formula ψ , the map

$$\check{\pi} : [\check{C}_\varepsilon(X^\psi)] \rightarrow \widehat{S}_\rho^\circ(f, t, \psi)$$

is well-defined and induces an isomorphism in homology.

We come back to the general case. Since

$$\mathfrak{C} = \bigcup_{\xi \in \Xi} \check{C}_\varepsilon(X^{\Phi_\xi}) \text{ and } \widehat{S}_\rho(f, t, \Phi) = \bigcup_{\xi \in \Xi} \widehat{S}_\rho(f, t, \Phi_\xi),$$

the map

$$\check{\pi} : [\mathfrak{C}] \rightarrow \widehat{S}_\rho(f, t, \Phi),$$

defined by the formula in (3.25), is well-defined, as we can guarantee that the image is contained in the codomain by the previous paragraph. This map induces an isomorphism in homology, by the Inclusion-Exclusion Transfer (Corollary 3^{S3}9) applied to the families $\{\check{C}_\varepsilon(X^{\Phi_\xi})\}_{\xi \in \Xi}$ and $\{\widehat{S}_\rho(f, t, \Phi_\xi)\}_{\xi \in \Xi}$. This is so because, as we have just seen, the map $\check{\pi}$ induces an isomorphism in homology for purely conjunctive formulas, together with the equalities

$$\bigcap_{\xi \in J} \check{C}_\varepsilon(X^{\Phi_\xi}) = \check{C}_\varepsilon(X^{\wedge_{\xi \in J} \Phi_\xi}) \text{ and } \bigcap_{\xi \in J} \widehat{S}_\rho(f, t, \Phi_\xi) = \widehat{S}_\rho(f, t, \wedge_{\xi \in J} \Phi_\xi)$$

for all $J \subseteq \Xi$. Using (4.6) again we conclude that \mathfrak{C} and $S_\rho(f, t, \Phi)$ have the same homology.

We can conclude as we have shown that both $S(f, t, \Phi)$ and \mathfrak{C} have the same homology as $S_\rho(f, t, \Phi)$ for the chosen ρ . \square

Proof of Theorem 4^{S1}3. Since the assumptions of Theorem 4^{S1}3 are stronger than the ones of Theorem 4^{S1}2, we can apply the latter theorem. As in the proof of this latter theorem, we can assume, without loss of generality, that Φ is of the form

$$\Phi \equiv \bigvee_{\xi \in \Xi} \Phi_\xi$$

where Φ_ξ is a purely conjunctive lax formula over (f, t) in normal form, by Proposition 2^{S1}2 and its proof. Recall also the notation X^ψ of the proof, given in (4.4), that we will use here.

For each purely conjunctive lax formula ψ over (f, t) , we have the inclusion

$$\check{C}_\varepsilon(X^\psi) \subseteq \mathcal{VR}_\varepsilon(X^\psi)$$

where \mathcal{X}^ψ is as in the proof of Theorem 4§1.2. We have that $\varepsilon > 0$ satisfies the hypothesis of Attali-Lieutier-Salinas approximation theorem (Theorem 3§3.12) for the set $S(f, t, \psi)$ by Theorem 3§2.6 and our assumption. Therefore the above inclusion is an isomorphism in homology.

We can now apply the Inclusion-Exclusion Transfer (Corollary 3§3.9) to the families $\{\check{C}_\varepsilon(\mathcal{X}^{\Phi_\xi})\}_{\xi \in \Xi}$ and $\{\mathcal{VR}_\varepsilon(\mathcal{X}^{\Phi_\xi})\}_{\xi \in \Xi}$ since

$$\bigcap_{\xi \in J} \check{C}_\varepsilon(\mathcal{X}^{\Phi_\xi}) = \check{C}_\varepsilon(\mathcal{X}^{\wedge_{\xi \in J} \Phi_\xi}) \text{ and } \bigcap_{\xi \in J} \mathcal{VR}_\varepsilon(\mathcal{X}^{\Phi_\xi}) = \mathcal{VR}_\varepsilon(\mathcal{X}^{\wedge_{\xi \in J} \Phi_\xi})$$

for all $J \subseteq \Xi$. This finishes the proof. \square

Remark 4§1.2. In the above two proofs, we have used that both the Čech and Vietoris-Rips complexes behave nicely with respect to intersections. Let us note that in general

$$\check{C}_\varepsilon(X_0) \cup \check{C}_\varepsilon(X_1) \subseteq \check{C}_\varepsilon(X_0 \cup X_1) \text{ and } \mathcal{VR}_\varepsilon(X_0) \cup \mathcal{VR}_\varepsilon(X_1) \subseteq \mathcal{VR}_\varepsilon(X_0 \cup X_1)$$

are strict inequalities. \P

Remark 4§1.3. Note that we cannot apply directly neither the Niyogi-Smale-Weinberger approximation theorem (Theorem 3§1.8) nor the Attali-Lieutier-Salinas approximation theorem (Theorem 3§3.12) since, by Example 3§2.1, we have that not all closed semialgebraic sets have positive reach, even when they are well-posed. \P

The following proposition combines the homology witness theorems with the sampling theorem. We can now put together the homology witness theorems and the sampling theorem.

Proposition 4§1.4. *Let $f \in \mathcal{H}_d[q]$, $t \in (-T, T)^e$, $\varepsilon > 0$, and $r > 0$ be such that $2D^{1/2}\bar{\kappa}(f)(r+T) < 1$ and*

$$7\sqrt{2}D^{1/2}\bar{\kappa}(f)r < \varepsilon < \min\left\{\frac{1}{120D^{3/2}\bar{\kappa}(f)}, \frac{\mathbb{U}(t)}{30D^{1/2}}\right\}. \quad (4.8)$$

Then, for every spherical r -net $\mathcal{G} \subseteq \mathbb{S}^n$ and for all lax formulas Φ over (f, t) , the spherical semialgebraic set $S(f, t, \Phi) \subseteq \mathbb{S}^n$, the simplicial complex

$$\Phi\left(\check{C}_\varepsilon(X_{i,j}^=(f, t, \mathcal{G})), \check{C}_\varepsilon(X_{i,j}^>(f, t, \mathcal{G})), \check{C}_\varepsilon(X_{i,j}^<(f, t, \mathcal{G})) \mid i \in [q], j \in [q]\right), \quad (4.9)$$

and the simplicial complex

$$\Phi\left(\mathcal{VR}_\varepsilon(X_{i,j}^=(f, t, \mathcal{G})), \mathcal{VR}_\varepsilon(X_{i,j}^>(f, t, \mathcal{G})), \mathcal{VR}_\varepsilon(X_{i,j}^<(f, t, \mathcal{G})) \mid i \in [q], j \in [q]\right), \quad (4.10)$$

have the same homology.

Proof. This is a straightforward combination of the sampling theorem (Theorem 4§1.1), the Čech homology witness theorem (Theorem 4§1.2) and the Vietoris-Rips homology witness theorem (Theorem 4§1.3). We only use the first theorem to bound the Hausdorff distance appearing in the latter two theorems. \square

4^{S1-3} Simplicial approximation of arbitrary $S(f, \Phi)$

We now adapt the proposition above to the case of an arbitrary semialgebraic set $S(f, \Phi)$. We note that this semialgebraic set might not be closed anymore, this is why we will use the Gabrielov-Vorobjov approximation theorem (Theorem 2^{S4 1}) to pass from the arbitrary case to the closed case. We should observe that when we apply the latter theorem, the obtained Gabrielov-Vorobjov approximations are not any more described by lax formulas over f , but by lax formulas over (f, t) . This is the main reason why the previous theory was developed for this extended family of polynomials, instead of just for homogenous polynomials.

Let $f \in \mathcal{H}_d[q]$ and $\delta, \varepsilon > 0$. To a monotone formula Φ , we associate the lax formula $\Phi^{\Gamma B_{\delta, \varepsilon}}$ over $(f, (-\delta, -\varepsilon, \varepsilon, \delta))$ given by

$$\begin{aligned} \Phi((f_i \leq \varepsilon \|f_i\|_W) \vee (f_i \geq -\varepsilon \|f_i\|_W), (f_i \geq \delta \|f_i\|_W) \vee (f_i \leq -\delta \|f_i\|_W), \\ (f_i \geq \delta \|f_i\|_W), (f_i \geq \delta \|f_i\|_W) \vee (f_i \leq \varepsilon \|f_i\|_W) \vee (f_i \geq -\varepsilon \|f_i\|_W), \\ (f_i \leq -\delta \|f_i\|_W), (f_i \leq -\delta \|f_i\|_W) \vee (f_i \leq \varepsilon \|f_i\|_W) \vee (f_i \geq -\varepsilon \|f_i\|_W) \mid i \in [q]), \end{aligned} \quad (4.11)$$

obtained by the substituting the indicated formulas in the places of the corresponding atoms. Looking at Definition 2^{S4 1}, we note that this is the formula describing a Gabrielov-Vorobjov block, i.e.,

$$\Gamma B_{\delta, \varepsilon}(f, \Phi) = S(f, (-\delta, -\varepsilon, \varepsilon, \delta), \Phi^{\Gamma B_{\delta, \varepsilon}}).$$

Now, let $\boldsymbol{\delta}, \boldsymbol{\varepsilon} \in (0, \infty)^m$. To a monotone formula Φ , we associate the lax formula $\Phi^{\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}}}$ over $(f, (-\delta_m, -\varepsilon_m, \dots, -\delta_1, -\varepsilon_1, \varepsilon_1, \delta_1, \dots, \varepsilon_m, \delta_m))$ given by

$$\bigvee_{i=1}^m \Phi^{\Gamma B_{\delta_i, \varepsilon_i}}. \quad (4.12)$$

As above, looking at Definition 2^{S4 1}, we note that this is the formula describing a Gabrielov-Vorobjov approximation. More explicitly,

$$\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}}(f, \Phi) = S(f, (-\delta_m, -\varepsilon_m, \dots, -\delta_1, -\varepsilon_1, \varepsilon_1, \delta_1, \dots, \varepsilon_m, \delta_m), \Phi^{\Gamma B_{\boldsymbol{\delta}, \boldsymbol{\varepsilon}}})$$

In this context, we introduce the following vectors of numbers depending on a parameter $\theta > 0$:

$$\kappa(\theta) := \theta(-2(n+2), -2(n+2)+1, \dots, -1, 0, 1, \dots, 2(n+2)-1, 2(n+2)) \quad (4.13)$$

$$\varrho(\theta) := \theta(1, 3, \dots, 2n+1, 2n+3) \quad (4.14)$$

$$\Delta(\theta) := \theta(2, 4, \dots, 2(n+1), 2(n+2)). \quad (4.15)$$

The following proposition gives a condition on θ for being able to construct a homologically equivalent simplicial approximation of $S(f, \Phi)$ using the Gabrielov-Vorobjov approximation $\Gamma B_{\Delta(\theta), \varrho(\theta)}(f, \Phi)$.

Proposition 4^{S1 5}. *Let $f \in \mathcal{H}_d[q]$, $\theta > 0$, $\varepsilon > 0$, and $r > 0$ be such that*

$$\theta < \frac{1}{8(n+2)\bar{D}(f)} \text{ and } 7\sqrt{2}\bar{D}^{1/2}\bar{\kappa}(f)r < \varepsilon < \frac{\theta}{30\bar{D}^{\frac{1}{2}}}. \quad (4.16)$$

Then, for every spherical r -net $\mathcal{G} \subseteq \mathbb{S}^n$ and for all monotone formulas Φ over f , the spherical semialgebraic set $S(f, \Phi) \subseteq \mathbb{S}^n$, the simplicial complex

$$\Phi^{\Gamma B_{\Delta(\theta), \exists(\theta)}} \left(\check{C}_\varepsilon(X_{i,j}^\infty(f, \mathbf{x}(\theta), \mathcal{G})) \mid \infty \in \{=, \geq, \leq\}, i \in [q], j \in [4n+9] \right), \quad (4.17)$$

and the simplicial complex

$$\Phi^{\Gamma B_{\Delta(\theta), \exists(\theta)}} \left(\mathcal{VR}_\varepsilon(X_{i,j}^\infty(f, \mathbf{x}(\theta), \mathcal{G})) \mid \infty \in \{=, \geq, \leq\}, i \in [q], j \in [4n+9] \right), \quad (4.18)$$

have the same homology.

Remark 4§1.4. We note that this proposition is just Proposition 4§1.4 with the inequalities adapted for this setting. \blacksquare

Proof. This proposition follows from Proposition 4§1.4. We only have to check the conditions there. Note that in this case, $\mathbb{W}(\mathbf{x}(\theta)) = \theta$ and that we can take T to be $(2n+5)\theta$. Combining the two inequalities in (4.16), we obtain that

$$7\sqrt{2}D^{1/2}\bar{\kappa}(f)r < \varepsilon < \frac{1}{240(n+2)D\bar{\kappa}(f)}.$$

This implies that $2D^{\frac{1}{2}}\bar{\kappa}(f)r < 1/240$, and so

$$2D^{\frac{1}{2}}\bar{\kappa}(f)(r+T) < 1,$$

since $2D^{\frac{1}{2}}\bar{\kappa}(f)T = 2D^{\frac{1}{2}}\bar{\kappa}(f)(2n+5)\theta < 3/4$, by (4.16). This shows the first needed inequality. Now,

$$\min \left\{ \frac{1}{120D^{\frac{3}{2}}\bar{\kappa}(f)}, \frac{\theta}{30D^{\frac{1}{2}}} \right\} = \frac{\theta}{30D^{\frac{1}{2}}}$$

due to (4.16). Therefore (4.16) follows and Proposition 4§1.4 applies. \square

4§2 Algorithms and their complexity

In the previous section, one can glimpse how our algorithms will be. We now provide specific descriptions of our algorithms together with condition-based and probabilistic complexity analyses. We note that all algorithms here work only with high probability. This is the so-called weak complexity framework which was introduced by Amelunxen and Lotz [6].

First, we give efficient constructions of spherical r -nets; second we give an algorithm to estimate the condition number; and third and last, we give our algorithm to compute the homology of a semialgebraic set.

4§2–1 Constructing spherical nets

Unfortunately, the construction in the proof of Lemma 1§2.20 is hard to be made efficient. Here we present three constructive spherical nets: the uniform grid, the random grid and the recursive grid. The first one is based on projecting the uniform grid from the cube onto the sphere, the second one on sampling points uniformly on the sphere, and the third one on pasting smaller copies of a initial spherical 1/3-net to obtain iterative refinements.

Remark 4^{S2} 1. To avoid being repetitious we will employ the uniform $\tilde{\gamma}$ -grid in the presentation of the algorithms. However, one can easily exchange this grid by the recursive $\tilde{\gamma}$ -grid $\mathcal{R}_{\tilde{\gamma}}$ and obtain a similar bound. Additionally, one can employ the random $\tilde{\gamma}$ -grid $\mathfrak{D}_{\tilde{\gamma}}(s)$, but, since this is a grid has the desired properties only with high probability, we omit giving the exact complexity as it would require an unnecessarily lengthier exposition taking into account this particularity. \blacksquare

Uniform grid

The uniform grid is as old as the grid method. We introduced another variant of this grid, different from the one used in [143, 144, 139, 142] and the one used in [88, 91, 92]. This variant is constructed so that it is completely adapted to floating-point arithmetic.

Definition 4^{S2} 1. Let $\tilde{\gamma} \in \mathbb{N}$. The *uniform $\tilde{\gamma}$ -grid*, $\mathcal{G}_{\tilde{\gamma}}$, is the finite set

$$\mathcal{G}_{\tilde{\gamma}} := \pi_{\mathbb{S}^n} \left(\left\{ x \in 2^{1-\tilde{\gamma}-\lceil \frac{1}{2} \log n \rceil} \mathbb{Z}^{n+1} \mid \text{for some } i \in \{0, \dots, n\}, x_i \in \{-1, +1\} \right\} \right) \subseteq \mathbb{S}^n \quad (4.19)$$

obtained by taking all points whose coordinates are integer multiples of $2^{-1-\tilde{\gamma}-\lceil \frac{1}{2} \log n \rceil}$ in the boundary of the cube $[-1, 1]^{n+1}$ and projecting them onto the sphere with the nearest point retraction $\pi_{\mathbb{S}^n} : x \mapsto x/\|x\|$.

It is clear that the uniform $\tilde{\gamma}$ -grid can be efficiently implemented in a computer. The main trick is to use the identity

$$f(x) = f(\pi_{\mathbb{S}^n}(x)) \|x\|^d$$

that holds for a homogeneous polynomial of degree d . This allows us to take full advantage from the fact that x can be written exactly in floating-point arithmetic.

The following proposition shows that this grid has the expected properties.

Proposition 4^{S2} 1. Let $\tilde{\gamma} \in \mathbb{N}$. Then the uniform $\tilde{\gamma}$ -grid $\mathcal{G}_{\tilde{\gamma}}$ is a spherical $2^{-\tilde{\gamma}}$ -net and satisfies that

$$\#\mathcal{G}_{\tilde{\gamma}} \leq 2^{\frac{1}{2}n \log n + 2n + \log n + 2 + n\tilde{\gamma}} \leq O(2^{n \log n + n\tilde{\gamma}}).$$

Proof. Note that the map $\pi_{\mathbb{S}^n} : x \mapsto x/\|x\|$ restricts to a bijective map

$$\overline{\text{IO}} : \partial[-1, 1]^{n+1} \rightarrow \mathbb{S}^n \quad (4.20)$$

which is 1-Lipschitz on each one of the facets of $\partial[-1, 1]^{n+1}$ with respect to, respectively, the Euclidean and geodesic distances.

Let $x \in \mathbb{S}^n$ be an arbitrary point. Then $\overline{\text{IO}}^{-1}(x)$ lies in some facet F of $\partial[-1, 1]^{n+1}$ and there is $y \in 2^{1-\tilde{\gamma}-\lceil \frac{1}{2} \log n \rceil} \mathbb{Z}^{n+1} \cap F$ such that $\text{dist}(x, y) \leq \sqrt{n} 2^{-\tilde{\gamma}-\lceil \frac{1}{2} \log n \rceil} < 2^{-\tilde{\gamma}}$. By the Lipschitz property, we have then that

$$\text{dist}_{\mathbb{S}^n}(x, \overline{\text{IO}}(y)) \leq \text{dist}(\overline{\text{IO}}^{-1}(x), y) < 2^{-\tilde{\gamma}}.$$

Thus $\text{dist}_{\mathbb{S}^n}(x, \mathcal{G}_{\tilde{\gamma}}) < 2^{-\tilde{\gamma}}$ and $\mathcal{G}_{\tilde{\gamma}}$ is a spherical $2^{-\tilde{\gamma}}$ -net.

For the second claim, we note that

$$\#\mathcal{G}_{\tilde{\gamma}} = 2(n+1) \left(2^{\tilde{\gamma}+\lceil \frac{1}{2} \log n \rceil} + 1 \right)^n.$$

The claim follows after some trivial estimates. \square

Let us note that the uniform grid grows faster than the grid in Lemma 1 §2 20. While the latter's growth is exponential in n , the uniform grid's growth is exponential in $n \log n$. This difference shows the loss that one has when covering the sphere by covering efficiently the boundary of a cube.

We will come back to an adaptive version of the uniform grid in Chapter 5 when discussing Han's covering algorithm.

Random grids

We begin with a random spherical net on the sphere which can be constructed in a very fast way by uniformly sampling points in the sphere. This is a very simple case of the random sampling procedure of Niyogi, Smale and Weinberger [300].

Theorem 4 §2 2. [300; Proposition 3.2] Let $n \geq 2$, $r \in (0, 1)$, $\alpha \geq 1$ and $m \in \mathbb{N}$ be such that

$$m \geq 2 \left(\frac{4}{r} \right)^n \left(n \ln \frac{4}{r} + \ln \alpha \right). \quad (4.21)$$

Then the random set

$$\mathfrak{G}_m := \{\mathfrak{x}_1, \dots, \mathfrak{x}_m\}$$

where $\mathfrak{x}_1, \dots, \mathfrak{x}_m$ are i.i.d. random vectors uniformly distributed on the sphere \mathbb{S}^n is a spherical r -net with probability $\geq 1 - 1/\alpha$.

Proof. Let $\mathcal{N} := \mathcal{N}_{r/2}$ be the spherical $r/2$ -net of Lemma 1 §2 20. We will show that with probability $\geq 1 - 1/\alpha$, for each $x \in \mathcal{N}$, there is i such that $\text{dist}_{\mathbb{S}}(x, \mathfrak{x}_i) < r/2$. Since \mathcal{N} is a spherical $r/2$ -net, the triangle inequality implies that \mathfrak{G}_m is a spherical r -net finishing the proof.

Because of the above, we have that

$$\begin{aligned} \mathbb{P}(\mathfrak{G}_m \text{ is not a spherical } r\text{-net}) &\leq \mathbb{P}(\exists x \in \mathcal{N} \mid \forall i, \text{dist}_{\mathbb{S}}(x, \mathfrak{x}_i) > r/2) \quad (\text{Implication bound}) \\ &\leq \#\mathcal{N} \mathbb{P}(\forall i, \text{dist}_{\mathbb{S}}(\mathbf{e}_0, \mathfrak{x}_i) > r/2) \quad (\text{Union bound}) \\ &= \#\mathcal{N} \mathbb{P}(\text{dist}_{\mathbb{S}}(\mathbf{e}_0, \mathfrak{x}_i) > r/2)^n \quad (\text{i.i.d.}) \\ &= \#\mathcal{N} (1 - \mathbb{P}(\text{dist}_{\mathbb{S}}(\mathbf{e}_0, \mathfrak{x}_i) \leq r/2))^n \end{aligned}$$

Now, we observe that

$$\mathbb{P}(\text{dist}_{\mathbb{S}}(\mathbf{e}_0, \mathfrak{x}_i) \leq r/2) = \frac{\text{vol}_n B_{\mathbb{S}}(x, r/2)}{\text{vol}_n \mathbb{S}^n} \geq \frac{1}{3} \left(\frac{r}{3} \right)^n \geq \frac{1}{2} \left(\frac{r}{4} \right)^n,$$

where the first inequality follows from the argument in the proof of Lemma 1 §2 20. By the same lemma, we also have the same bound for $\#\mathcal{N}$. Let $\alpha^{-1} = 2 \left(\frac{4}{r} \right)^n$. We only have to show that

$$\frac{1}{\alpha} (1 - \alpha)^{\frac{1}{\alpha}(\ln \alpha^{-1} + \ln \alpha)} \leq 1/\alpha.$$

But $1 - \alpha \leq e^{-\alpha}$ and so the above inequality holds. \square

Remark 4 §2 2. The proof is just an adaptation of the proof of [300; Lemma 5.1]. We note that this method is a kind of *probabilistic pigeonhole principle*: if $n(\ln n + \ln \alpha)$ pigeons go at random to n pigeonholes, then none of the pigeonholes is empty with probability at least $1 - 1/\alpha$. Note that the number of pigeons is quasi-linear in the number of pigeonholes. \blacksquare

Corollary 4^{S2} 3. Let $n \geq 2$, $\gamma \in \mathbb{N}$, $\alpha \geq 1$ and $m \in \mathbb{N}$ be such that

$$m_\gamma(\alpha) = \lceil 2^{n(\gamma+2)+\log n(\gamma+2)+1} (1 + \ln \alpha) \rceil. \quad (4.22)$$

Then the random set

$$\Omega_\gamma(\alpha) := \{\mathbf{x}_1, \dots, \mathbf{x}_{m_\gamma(\alpha)}\}$$

where the \mathbf{x}_i are i.i.d. random vectors uniformly distributed on the sphere \mathbb{S}^n is a spherical $2^{-\gamma}$ -net with probability $\geq 1 - 1/\alpha$. \square

We will call the random set $\Omega_\gamma(\alpha)$ in \mathbb{S}^n the *random γ -grid with failure probability α^{-1}* . This random construction is very efficient and we can see that its size grows exponentially in n , but not exponentially in $n \log n$ as the uniform γ -grid. An additional nice property is that we can increase the probability of success exponentially, by just doubling the number of sampled points.

Recursive grids

Assume that we start with a spherical $1/3$ -net \mathcal{R}_1 : we will use this original grid to construct finer and finer grids as needed. Such a initial grid can be constructed using the following proposition, which we only need to apply once for each dimension.

Proposition 4^{S2} 4. Let $n \geq 2$. Then

$$\{\mathbf{x}_i \mid i \in [16^{n+1}]\}$$

where the \mathbf{x}_i are i.i.d. random vectors uniformly distributed on the sphere \mathbb{S}^n is a spherical $1/3$ -net with probability at least 0.999.

Proof. This is a particular case of Theorem 4^{S2} 2. \square

Remark 4^{S2} 3. We insist on the fact that we only need to apply the probabilistic construction above once. Once we have the initial spherical $1/3$ -net of \mathbb{S}^n , there is no need of recomputing it. Because of this and for the sake of simplicity, we will ignore this probabilistic step in our complexity analysis. However, we leave as an open problem to construct this grid in deterministic singly exponential time.

Open problem F. Is there a deterministic algorithm running in $2^{O(n)}$ -time that outputs a spherical $1/3$ -net of \mathbb{S}^n ?

We note that the uniform grid has quasi-exponential complexity $2^{O(n \log n)}$, so either one solves the problem or relaxes it to a probabilistic regime as we have done above. \P

We take this initial spherical net \mathcal{R}_1 and we project it onto the ball $\overline{B}(0, 1) \subseteq \mathbb{R}^n$ via the projection

$$\mathbf{x} = \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_n \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_n \end{pmatrix}.$$

This procedure gives an $1/3$ -net $\tilde{\mathcal{R}}$ of $\overline{B}(0, 1)$. To avoid having too many points, we substitute $\tilde{\mathcal{R}}$ by a maximal subset \mathcal{N} satisfying the property that for all $\mathbf{x}, \mathbf{y} \in \mathcal{N}$, $\text{dist}(\mathbf{x}, \mathbf{y}) \geq 23/156$.

We note that that \mathcal{N} can be constructed efficiently from $\tilde{\mathcal{R}}$, by enumerating the points of $\tilde{\mathcal{R}}$ and eliminating points that are too near to the previously listed points. We note that \mathcal{N} would be then a $25/52$ -net of $\bar{B}(0, 1)$, since $1/3 + 23/156 = 25/52$.

The following proposition shows the fundamental step in our construction, we only need to assume for it that \mathcal{N} is a $25/52$ -net.

Proposition 4\\$2.5. *Let $r \in (0, 1/3]$ and consider the map $\text{IO} : \mathbb{R}^n \rightarrow \mathbb{S}^n$ defined in (1.29). Then $\text{IO}((\tan r)\mathcal{N})$ is a $r/2$ -net of $\bar{B}_{\mathbb{S}}(\mathbf{e}_0, r)$ with respect to the geodesic distance of \mathbb{S}^n .*

Proof. The map $\text{IO} : \bar{B}(0, \tan 1/3) \rightarrow \bar{B}_{\mathbb{S}}(\mathbf{e}_0, 1/3)$ is 1-Lipschitz with respect to, respectively, the Euclidean and geodesic distances. Now, $(\tan r)\mathcal{N}$ is a $\frac{25 \tan r}{52}$ -net of $\bar{B}(0, \tan r)$, and so, by the previous statement, $\text{IO}((\tan r)\mathcal{N})$ is a $\frac{25 \tan r}{52}$ -net of $\bar{B}_{\mathbb{S}}(\mathbf{e}_0, r) = \bar{B}(0, \tan r)$. Since

$$\tan r \leq \frac{26}{25}r,$$

for $r \in (0, 1/3]$, and $\frac{26}{25} \cdot \frac{25}{52} = 1/2$, the claim follows. \square

Now, we put a copy of $\text{IO}((\tan r)\mathcal{N})$ at each point of this net. For $x \in \mathbb{S}^n$, define

$$h_x := \begin{cases} \mathbb{I}, & \text{if } x = \mathbf{e}_0 \\ \mathbb{I} - 2 \frac{(x - \mathbf{e}_0)(x - \mathbf{e}_0)^*}{\|x - \mathbf{e}_0\|^2}, & \text{otherwise,} \end{cases} \quad (4.23)$$

so that h_x is an orthogonal transformation mapping x to \mathbf{e}_0 and \mathbf{e}_0 to x .

Definition 4\\$2.2. Let \mathcal{R}_1 be a spherical $1/3$ -net of \mathbb{S}^n and \mathcal{N} a $25/52$ -net of $\bar{B}(0, 1) \subseteq \mathbb{R}^n$. The recursive $\check{\gamma}$ -grid $\mathcal{R}_{\check{\gamma}}$ with seeds \mathcal{R}_1 and \mathcal{N} is the finite set given recursively by

$$\mathcal{R}_{\check{\gamma}} := \bigcup \left\{ h_x \text{IO} \left((\tan 2^{2-\check{\gamma}}/3)\mathcal{N} \right) \mid x \in \mathcal{R}_{\check{\gamma}} \right\} \quad (4.24)$$

for $\check{\gamma} \geq 2$.

In other words, to obtain $\mathcal{R}_{\check{\gamma}}$ from $\mathcal{R}_{\check{\gamma}-1}$, we cover each geodesic ball $\bar{B}_{\mathbb{S}}(x, 2^{1-\check{\gamma}})$ with $x \in \mathcal{R}_{\check{\gamma}-1}$ with geodesic balls $\bar{B}_{\mathbb{S}}(y, 2^{-\check{\gamma}})$ with y coming from a projection of $(\tan 2^{-\check{\gamma}})\mathcal{N}$ around x . Note that there is a certain fractal appeal to this net, since, at each iteration, we are just adding smaller and smaller “copies” of the same net around each point. The following proposition shows the properties of the recursive grid.

Proposition 4\\$2.6. *Let $\check{\gamma} \in \mathbb{N}$. Then any recursive $\check{\gamma}$ -grid $\mathcal{R}_{\check{\gamma}}$ is a spherical $2^{1-\check{\gamma}}/3$ -net and satisfies that*

$$\#\mathcal{R}_{\check{\gamma}} \leq \#\mathcal{R}_1 (\#\mathcal{N})^{\check{\gamma}-1}.$$

In particular, if \mathcal{R}_1 was constructed using Proposition 4\\$2.4 and \mathcal{N} by projecting \mathcal{R}_1 , then $\#\mathcal{R}_{\check{\gamma}} \leq 16^{(n+1)\check{\gamma}}$.

Proof. The proof works by induction. The statements are obvious for \mathcal{R}_1 . Assume that the statement is true for $\check{\gamma}$. Let $x \in \mathbb{S}^n$, then there is $z \in \mathcal{R}_{\check{\gamma}}$ such that $\text{dist}_{\mathbb{S}}(x, z) < 2^{1-\check{\gamma}}/3$. Therefore, by Proposition 4\\$2.5, there is $z' \in h_z \text{IO}((\tan(2^{2-(\check{\gamma}+1)})/3)\mathcal{N}) \subseteq \mathcal{R}_{\check{\gamma}+1}$ such that $\text{dist}_{\mathbb{S}}(x, z') < 2^{-\check{\gamma}/3}$. Thus $\mathcal{R}_{\check{\gamma}+1}$ is a spherical $2^{-\check{\gamma}}/3$ -net. By the induction principle, we are done.

The bound on the size is obvious from the construction. \square

Remark 4^{S2}4. We note that for n large, concretely, $n > 16$, the recursive $\tilde{\gamma}$ -grid $\mathcal{R}_{\tilde{\gamma}}$ has a smaller size than the uniform $\tilde{\gamma}$ -grid. However, the uniform grid grows at a smaller rate in terms of $\tilde{\gamma}$ than the recursive grid. This situation can change if one finds a different construction of \mathcal{N} . \blacksquare

4^{S2}-2 Estimation of the intersection condition number

Our first algorithm estimates of the intersection condition number $\bar{\kappa}$. The main idea is to use the 2nd Lipschitz property (Proposition 1^{S3}3) which allows us to see the condition number as the inverse of a Lipschitz function on the sphere.

Remark 4^{S2}5. All the algorithms in this section will be given working with $\bar{\kappa}$. However, everything here can be easily translated in terms of κ and of $\bar{\kappa}_{\text{aff}}$. \blacksquare

The following lemma and its proof is very similar to the proof of Theorem 1^{S2}19.

Lemma 4^{S2}7. [91; Corollary 6.2]. Let $f \in \mathcal{H}_d[q]$, $r > 0$ and \mathcal{G} be a spherical r -net. Define

$$\bar{\kappa}_{\mathcal{G}}(f) := \max \{\bar{\kappa}(f, x) \mid x \in \mathcal{G}\}.$$

Then $\bar{\kappa}_{\mathcal{G}}(f) \leq \bar{\kappa}(f)$. Moreover, if $D\bar{\kappa}_{\mathcal{G}}(f)r < 1$, then

$$\bar{\kappa}(f) \leq \frac{\bar{\kappa}_{\mathcal{G}}(f)}{1 - D\bar{\kappa}_{\mathcal{G}}(f)r}.$$

Proof. The first claimed inequality is trivial. To prove the second we apply the 2nd Lipschitz property of $\bar{\kappa}$ (Proposition 1^{S3}3). Let $x_* \in \mathbb{S}^n$ be such that $\bar{\kappa}(f) = \bar{\kappa}(f, x_*)$. Since \mathcal{G} is a spherical r -net, there exists $x \in \mathcal{G}_{\tilde{\gamma}}$ such that $\text{dist}_{\mathbb{S}}(x, x_*) < r_{\tilde{\gamma}}$. Therefore, using the 2nd Lipschitz property, it follows that

$$\frac{1}{\bar{\kappa}_{\mathcal{G}}(f)} - Dr \leq \frac{1}{\bar{\kappa}(f, x)} - Dr \leq \frac{1}{\bar{\kappa}(f, x_*)} = \frac{1}{\bar{\kappa}(f)}.$$

The desired inequality follows. \square

Based on Lemma 4^{S2}7, we propose algorithm $\bar{\kappa}$ -ESTIMATE whose correctness is provided by the lemma itself.

Theorem 4^{S2}8. [91; Proposition 6.3]. Algorithm $\bar{\kappa}$ -ESTIMATE is correct. Its run-time on input (f, ρ, B) is bounded by

$$O \left(q^{n+2} 2^{n \log n + n} D^{2n} (\min\{B, \bar{\kappa}(f)\} \rho^{-1})^n \right) = (qnD \min\{B, \bar{\kappa}(f)\} \rho^{-1})^{O(n)}.$$

Proof. The correctness follows from Lemma 4^{S2}7 and the stopping criterion, noting that at each iteration we have $K = \bar{\kappa}_{\mathcal{G}_{\tilde{\gamma}}}(f) \leq \bar{\kappa}(f)$.

To prove the cost bound assume that, after $\tilde{\gamma}$ iterations, we have

$$\tilde{\gamma} \geq \log_2 (2D\mathcal{K} \rho^{-1}), \tag{4.25}$$

where $\mathcal{K} := \min\{B, K\}$. Then $2^{-\tilde{\gamma}} \leq \frac{\rho}{D\mathcal{K}}$. If $B > K$ then $\mathcal{K} = K$ and the algorithm halts. If $B \leq K$, then the algorithm halts as well. Thus we have shown that the algorithms halts after at most

$$\log_2 (D \min\{B, \bar{\kappa}(f)\} \rho^{-1})$$

iterations.

At any intermediate $\tilde{\jmath}$ th iteration, the number of points in $\mathcal{G}_{\tilde{\jmath}}$ is bounded by

$$O\left(2^{n \log n + n\tilde{\jmath}}\right) \leq O\left(2^{n \log n} (\mathsf{D} \min\{\mathsf{B}, \bar{\kappa}(f)\} \rho^{-1})^n\right), \quad (4.26)$$

by Proposition 4§2.1. For each point $x \in \mathcal{G}_{\tilde{\jmath}}$ we compute the value of $\kappa(f^L, x)$ for

$$\sum_{k=1}^{\min\{q, n+1\}} \binom{q}{k} \leq q^{n+1} \sum_{k=1}^{n+1} \frac{1}{k!} = (e - 1)q^{n+1} \quad (4.27)$$

many subsets L . Each of these computations can be done in $O(N + n^3)$ operations by [272; Lemma 25]. We note that the latter result is for computing approximation $\kappa(f, x)$ up to a constant factor, which would only alter slightly the algorithm and its complexity. For convenience, we ignore this as it only would make things unnecessarily technical. Finally, note that

$$N \leq q \binom{n + D}{n} \leq q \prod_{k=1}^n \left(1 + \frac{D}{k}\right) \leq q(2D)^n, \quad (4.28)$$

from where it follows that each $\kappa(f^L, x)$ is computed with cost $O(q(2D)^n + n^3) \leq O(q(2D)^n)$.

Putting all the previous bounds together we obtain the desired complexity bound. \square

Remark 4§2.6. Algorithm $\bar{\kappa}$ -ESTIMATE estimates $\bar{\kappa}(f)$ up to a precision ρ in finite time, provided this condition number is not too large (not much bigger than B). When $B = \infty$ is given as input, it estimates $\bar{\kappa}(f)$ up to this precision but its running time is not bounded. In particular, if $\bar{\kappa}(f) = \infty$, then the algorithm loops forever. \P

Algorithm 3: $\bar{\kappa}$ -ESTIMATE

Input : $f \in \mathcal{H}_d[q]$
 $\rho \in (0, 1)$
 $B \in (0, \infty]$

```

 $\tilde{\jmath} \leftarrow 0$ 
repeat
|    $\tilde{\jmath} \leftarrow \tilde{\jmath} + 1$ 
|    $K \leftarrow (1 - \rho)^{-1} \max\{\kappa(f^L, x) \mid x \in \mathcal{G}_{\tilde{\jmath}}, L \in [q]^{\leq n+1}\}$ 
until  $DK 2^{-\tilde{\jmath}} \leq \rho(1 + \rho)$  or  $B \leq K$ 
if  $B \leq K$  then
|   return fail
else
|   return K

```

Output : fail or $K \in (0, \infty)$
Postcondition: If fail, then $B \leq K \leq \bar{\kappa}(f)$;
otherwise $\bar{\kappa}(f) \leq K \leq (1 - \rho)^{-1} \bar{\kappa}(f)$

Corollary 4^{S2}9. [91; Proposition 2.2]. Algorithm $\bar{\kappa}$ -ESTIMATE on input $(f, 0.01, \infty)$ returns a number K such that

$$\bar{\kappa}(f) \leq K \leq 1.02 \bar{\kappa}(f)$$

if $\bar{\kappa}(f) < \infty$, or loops forever otherwise. The run-time is bounded by $(qnD\bar{\kappa}(f))^{O(n)}$. \square

4^{S2}-3 Computing the homology of semialgebraic sets

We describe now the algorithm that computes the homology of semialgebraic sets. First, we present the algorithm for spherical semialgebraic sets; second, we show how it is adapted to the affine setting; and third and last, we provide the probabilistic complexity analysis, explaining the philosophy of the weak complexity.

Remark 4^{S2}7. We note that the algorithms here can be modified to produce the algorithm for counting zeros of [139, 140, 141], and for computing the homology of real projective smooth sets [142], basic semialgebraic sets [88] and closed semialgebraic sets [91]. For the sake of brevity, we only give the algorithms for computing the homology of spherical and affine semialgebraic sets, but the interested reader can reconstruct the remaining algorithms easily combining the Sampling Theorem (Theorem 4^{S1}1) and the homology witness theorems (Theorems 4^{S1}2 and 4^{S1}3). \P

Spherical semialgebraic sets

Proposition 4^{S1}5 is the basis of Algorithm SPHERICALHOMOLOGY. However, let us note that Proposition 4^{S1}5 is a combination of the Gabrielov-Vorobjov approximation theorem (Theorem 2^{S4}2), the Sampling Theorem (Theorem 4^{S1}1), and the homology witness theorems (Theorems 4^{S1}2 and 4^{S1}3). Since we can construct spherical nets, this transforms Proposition 4^{S1}5 into Algorithm SPHERICALHOMOLOGY. We note that the choice of the parameters ϵ and θ is arbitrary, but the particular values are not important as long as they satisfy the needed inequalities.

We also give Algorithm SPHERICALLAXHOMOLOGY that computes the homology of semialgebraic sets given by lax formulas, as it is of interest of its own and it has better constants. We will not discuss it further, as the same estimates that apply to Algorithm SPHERICALHOMOLOGY apply to Algorithm SPHERICALLAXHOMOLOGY.

The main theorem concerning algorithm SPHERICALHOMOLOGY is the following one.

Theorem 4^{S2}10. [91, 92; Theorem 1.1(i)]. Algorithm SPHERICALHOMOLOGY is correct. Its run-time on input (f, Φ) is bounded by

$$O\left(q \text{ size}(\Phi) (131nD\bar{\kappa}(f))^{10n(n+2)}\right) = q \text{ size}(\Phi)(nD\bar{\kappa}(f))^{O(n^2)}.$$

Remark 4^{S2}8. Using Remark 3^{S3}4, we can improve the complexity of the algorithm at the cost of allowing an error probability. If we do so, $10n(n+1)$ in the exponent becomes $8n(n+1)$. Moreover, if we are only interested in the Betti numbers, it can be further reduced to $6n(n+1)$. \P

Remark 4^{S2}9. An alternative formulation of Algorithm $\bar{\kappa}$ -ESTIMATE runs with an arbitrary upper bound K of $\bar{\kappa}(f)$. However, for this version, run-time depends on K instead than on $\bar{\kappa}(f)$, unless one imposes that K is a sufficiently good approximation of $\bar{\kappa}(f)$. \P

Algorithm 4: SPHERICALHOMOLOGY

Input : $f \in \mathcal{H}_d[q]$
 Boolean formula Φ over f

Precondition : $\bar{\kappa}(f) < \infty$

eliminate negations in Φ
 $K \leftarrow \bar{\kappa}\text{-ESTIMATE}(f, 0.01, \infty)$
 $\theta \leftarrow 1/(9(n+2)DK)$
 $\mathbb{K}_0 \leftarrow 0$

for $i = 1, \dots, n+2$ **parallelly do**

- $\vartheta_i \leftarrow (2i-1)\theta$
- $\Delta_i \leftarrow 2i\theta$
- $\mathbb{K}_{2i-1} \leftarrow \vartheta_i, \mathbb{K}_{2i} \leftarrow \Delta_i$
- $\mathbb{K}_{2(i+n+2)-1} \leftarrow -\vartheta_i, \mathbb{K}_{2(i+n+2)} \leftarrow -\Delta_i$

$\tilde{n} \leftarrow \lceil \log 2700(n+2)D^2K^2 \rceil$
 $\varepsilon \leftarrow 1/\left(277(n+2)D^{\frac{3}{2}}K\right)$

for $i = 1, \dots, q$ **and** $j = 0, \dots, 4(n+2)$ **do**

- $\mathcal{X}_{i,j}^{\geq} \leftarrow \{x \in \mathcal{G}_{\tilde{n}} \mid f_i(x) \geq (\mathbb{K}_j - D^{\frac{1}{2}}2^{-\tilde{n}})\|f_i\|_W\}$
- $\mathcal{S}_{i,j}^{\geq} \leftarrow \mathcal{VR}_{\varepsilon}(\mathcal{X}_{i,j}^{\geq})$ with faces up to dimension $n+1$
- $\mathcal{X}_{i,j}^{\leq} \leftarrow \{x \in \mathcal{G}_{\tilde{n}} \mid f_i(x) \leq (\mathbb{K}_j + D^{\frac{1}{2}}2^{-\tilde{n}})\|f_i\|_W\}$
- $\mathcal{S}_{i,j}^{\leq} \leftarrow \mathcal{VR}_{\varepsilon}(\mathcal{X}_{i,j}^{\leq})$ with faces up to dimension $n+1$
- $\mathcal{S}_{i,j}^= \leftarrow \mathcal{S}_{i,j}^{\geq} \cap \mathcal{S}_{i,j}^{\leq}$

$\mathcal{S} \leftarrow \Phi^{\Gamma_{B_{D,\Theta}}}(\mathcal{S}_{i,j}^=, \mathcal{S}_{i,j}^{\geq}, \mathcal{S}_{i,j}^{\leq} \mid i \in [q], j \in \{0, \dots, 4(n+2)\})$
 $(\beta_0, \dots, \beta_n; \tau_1, \dots, \tau_n) \leftarrow \text{SIMPLICIALHOMOLOGY}(n, \mathcal{S})$

return $\beta_1, \dots, \beta_n, \tau_1, \dots, \tau_n$

Output : Betti numbers β_0, \dots, β_n of $S(f, \Phi)$
 and torsion coefficients τ_1, \dots, τ_n of $S(f, \Phi)$

Proof. The correctness of the algorithm is guaranteed by Corollary 4\\$2.9 and Proposition 4\\$1.5. We perform the complexity analysis now. The most expensive parts are: 1) call to Algorithm $\bar{\kappa}\text{-ESTIMATE}$, 2) Construction of the $X_{i,j}^{\infty}$, 3) construction of the simplicial complexes $\mathcal{S}_{i,j}^{\infty}$, 4) Construction of \mathcal{S} , and 5) call to Algorithm $\text{SIMPLICIALHOMOLOGY}$. We go one by one.

- 1) The bound in Corollary 4\\$2.9 applies here.
- 2) Each construction requires the evaluation of points coming from \mathcal{G}_I and the corresponding comparison. Evaluating f_1, \dots, f_q at a point $x \in \mathbb{S}^n$ takes $O(N)$ arithmetic operations. This means that we perform

$$O(N \# \mathcal{G}_{\tilde{n}}) \leq O(N 2^{n \log n + n \tilde{n}}) \leq O(q 2^{2n \log n + 13n} D^{3n} K^{2n})$$

Algorithm 5: SPHERICAL LAX HOMOLOGY

Input : $f \in \mathcal{H}_d[q]$
 lax formula Φ over f
Precondition : $\bar{\kappa}(f) < \infty$

$K \leftarrow \bar{\kappa}\text{-ESTIMATE}(f, 0.01, \infty)$
 $\tilde{\eta} \leftarrow \lceil \log 1300 D^2 K^2 \rceil$
 $\varepsilon \leftarrow 1 / (125 D^{\frac{3}{2}} K)$
for $i = 1, \dots, q$ **do**
 $X_i^{\geq} \leftarrow \{x \in \mathcal{G}_{\tilde{\eta}} \mid f_i(x) \geq -D^{\frac{1}{2}} 2^{-\tilde{\eta}} \|f_i\|_W\}$
 $S_i^{\geq} \leftarrow \mathcal{VR}_{\varepsilon}(X_{i,j}^{\geq})$ with faces up to dimension $n+1$
 $X_i^{\leq} \leftarrow \{x \in \mathcal{G}_{\tilde{\eta}} \mid f_i(x) \leq D^{\frac{1}{2}} 2^{-\tilde{\eta}} \|f_i\|_W\}$
 $S_i^{\leq} \leftarrow \mathcal{VR}_{\varepsilon}(X_{i,j}^{\leq})$ with faces up to dimension $n+1$
 $S_i^= \leftarrow S_i^{\geq} \cap S_i^{\leq}$
 $S \leftarrow \Phi(S_i^=, S_i^{\geq}, S_i^{\leq} \mid i \in [q])$
 $(\beta_0, \dots, \beta_n; T_1, \dots, T_n) \leftarrow \text{SIMPLICIALHOMOLOGY}(n, S)$
return $\beta_1, \dots, \beta_n, T_1, \dots, T_n$

Output : Betti numbers β_0, \dots, β_n of $S(f, \Phi)$
 and torsion coefficients T_1, \dots, T_n of $S(f, \Phi)$

arithmetic operations, where the latter bound follows from Proposition 4S²1, the choice of $\tilde{\eta}$ and (4.28). These computations are then followed by

$$2q(n+2) \# \mathcal{G}_{\tilde{\eta}} \leq O\left(qn2^{n \log n + n\tilde{\eta}}\right) \leq O\left(q2^{n \log n + \log n} D^{2n} K^{2n}\right)$$

comparisons, where the inequalities follow from Proposition 4S²1 and the choice of $\tilde{\eta}$ again.

3) In order to construct the faces of $\mathcal{VR}_{\varepsilon}(\mathcal{X})$ up to dimension $\ell+1$ for a cloud of points $\mathcal{X} \subseteq \mathbb{S}^n$, we construct the graph $\mathbb{G}_{\varepsilon}^{\mathcal{VR}}(\mathcal{X})$ and then we find the cliques of size at most $\ell+1$ of this graph. The first step requires

$$O\left(n^2 \binom{\#\mathcal{X}}{2}\right)$$

operations and comparisons to be able to compute and compare with 2ε the distances between any two points of \mathcal{X} . The second step requires to explore all possible subsets of size at most k , this means checking

$$\sum_{i=1}^{\ell+2} \binom{\#\mathcal{X}}{k} \leq (\varepsilon - 1)(\#\mathcal{X})^{\ell+2}$$

subsets of \mathcal{X} , where the inequality is analogous to that in (4.27). Applying this to our setting gives us

$$O\left(qn(\#\mathcal{G}_{\tilde{\eta}})^{n+2}\right) \leq O\left(q(128nDK)^{2n(n+2)}\right)$$

operations in our algorithm. The bound is obtained again using Proposition 4\\$2.1 and the choice of $\tilde{\gamma}$.

4) We construct \mathcal{S} from the $\mathcal{S}_{i,j}^\infty$ using formula $\Phi^{\Gamma B_{A,\Theta}}$. This formula has size $(n+1) \text{size}(\Phi)$. We only have to apply this Boolean formula to each possible face of \mathcal{S} checking if it is there or not. This adds the extra factor $n \text{size}(\Phi)$ to the complexity.

5) By Proposition 3\\$3.4, Algorithm SIMPLICIALHOMOLOGY has run-time bounded by

$$O\left(\sum_{i=0}^{n+1} (\#\mathcal{S}_i)^5\right)$$

where \mathcal{S}_i is the set of i -dimensional faces of \mathcal{S} . Arguing as in 3), we can bound this by

$$O\left((128nD\bar{\kappa}(f))^{10n(n+2)}\right).$$

Combining all this estimates with $K \leq 1.01\bar{\kappa}(f)$ finishes the proof. \square

We will now further discuss on some properties of the algorithm above, so that it can be appreciated better. We will discuss two topics: the computation of the first ℓ homology groups, and the computation of the Betti numbers.

Computation of the first ℓ homology groups It may be the case that we are not interested in computing all the homology groups, but only the first ℓ . This can easily be attained by only constructing the simplicial complexes in Algorithm SPHERICALHOMOLOGY up to the faces of dimension $\ell + 1$ and applying Algorithm SIMPLICIALHOMOLOGY with the needed input change. This will improve the complexity of the algorithm.

Theorem 4\\$2.11. One can modify Algorithm SPHERICALHOMOLOGY to compute only the first ℓ homology groups. The run-time of this modified version on input (f, Φ, ℓ) is bounded by

$$O\left(q \text{size}(\Phi) (128nD\bar{\kappa}(f))^{10n(\ell+2)}\right) = q \text{size}(\Phi)(nD\bar{\kappa}(f))^{O(n\ell)}.$$

Proof. The complexity analysis is just as that of the proof of Theorem 4\\$2.10. The only difference is in point 3) where we only have to construct the face of dimension at most $\ell + 1$ which transform the $(n + 2)$ in the exponent into $(\ell + 2)$. \square

Computation of the Betti numbers If we substitute Algorithm SIMPLICIALHOMOLOGY by Algorithm SIMPLICALBETTI, we can focus on just computing the Betti numbers. Unfortunately, the rank of an integer matrix cannot be deterministically computed significantly faster than the Smith Normal Form. The main issue is that the size of the integers can grow during the computation, which the fast Monte Carlo algorithms [165, 191, 161] avoid by reducing modulo some prime. However, this growth does not happen if we are interested in the mod p Betti numbers for some prime p .

The k th mod p Betti number of X is the integer given by

$$\beta_k^p(X) := \dim_{\mathbb{F}_p} H_k(X) \otimes \mathbb{F}_p = \beta_k(X) + \#\{i \in [s_k(X)] \mid p \text{ divides } T_{k,i}(X)\} \quad (4.29)$$

where $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ is the prime field of size p . Note that we can obtain this number by constructing the chain complex with formal combinations over \mathbb{F}_p instead that over \mathbb{Z} . These can be computed faster.

Theorem 4^{S2}12. One can modify Algorithm SPHERICALHOMOLOGY to compute only the first $\ell \bmod p$ Betti numbers. The run-time of this modified version on input (f, Φ, ℓ, p) is bounded by

$$O\left(q \log(p) \text{size}(\Phi) (128nD\bar{\kappa}(f))^{6n(\ell+2)}\right) = q \log(p) \text{size}(\Phi) (nD\bar{\kappa}(f))^{O(n\ell)}.$$

Proof. One can show an analogue of Theorem 3^{S3}3 in which $\beta_k^p(X)$ is obtained from the \mathbb{F}_p -ranks of the boundary operators in the same way that $\beta_k(X)$ is obtained from the \mathbb{Q} -ranks. This reduces the problem to a rank computation over a finite field. We can use then Gaussian elimination. \square

Remark 4^{S2}10. The probabilistic algorithms for computing rank (by Dumas and Villard [162] and Cheung, Kwok and Lau [119]) can be used to turn the exponent $6n(\ell+2)$ into $2\omega n(\ell+2)$, where ω is the matrix multiplication exponent. \P

Affine semialgebraic sets

The algorithm for affine semialgebraic sets is nothing more than a homogenization, as described in Section 1^{S4}, followed by the Algorithm SPHERICALHOMOLOGY.

Algorithm 6: AFFINEHOMOLOGY

Input : $p \in \mathcal{P}_d[q]$
 Boolean formula Ψ over p

Precondition : $\bar{\kappa}_{\text{aff}}(p) < \infty$

$f \leftarrow H(p)$
 $\Phi \leftarrow \Psi^h$
 $(\beta_0, \dots, \beta_n; T_1, \dots, T_n) \leftarrow \text{SPHERICALHOMOLOGY}(f, \Phi)$
return $\beta_1, \dots, \beta_n, T_1, \dots, T_n$

Output : Betti numbers β_0, \dots, β_n of $W(p, \Psi)$
 and torsion coefficients T_1, \dots, T_n of $W(p, \Psi)$

To this algorithm, the same statements as those to Algorithm SPHERICALHOMOLOGY apply. In particular, we have the following theorem.

Theorem 4^{S2}13. [91, 92; Theorem 1.1(i)]. Algorithm AFFINEHOMOLOGY is correct. Its run-time on input (f, Φ) is bounded by

$$O\left(q \text{size}(\Phi) (128nD\bar{\kappa}_{\text{aff}}(p))^{10n(n+2)}\right) = q \text{size}(\Phi) (nD\bar{\kappa}_{\text{aff}}(p))^{O(n^2)}.$$

Proof. By definition, $\bar{\kappa}_{\text{aff}}(f) = \bar{\kappa}(H(f))$. We apply Theorem 4^{S2}10. \square

The same comments that applied to Algorithm SPHERICALHOMOLOGY apply also to Algorithm AFFINEHOMOLOGY.

Weak exponential complexity of the algorithms

The main motivation for the weak complexity framework of Amelunxen and Lotz [6] is that there are algorithms that are efficient in practice, but whose expected time is infinite. This gap is explained by the existence of algorithms that have good complexity with high probability, but whose expected complexity is infinite. An example of such an algorithm is the power iteration method for computing a leading eigenvector of a Hermitian matrix [6].

This phenomenon is a reverse of the *St. Petersburg paradox* of Bernoulli [50]. In this paradox, a player is guessing the output of a coin. The player wins double what E bet, if Eir guess is correct, and loses Eir bet, otherwise. Although the expected gain of the game is infinite, the actual probability of winning an exponentially large quantity of money decreases exponentially. This means that in practice is hard to actually get an extremely large amount of money playing the game. Even more, it is very likely that one loses all one's money playing the game.

In probabilistic complexity, the bet is exactly the other way around. We want the run-time to be small for a random input. The expected run-time can be large, even infinity, but this can be the consequence of a set of inputs that happens with exponentially small probability. These inputs are really rare, which is why they are called *black swans*. In practice, black swans are extremely rare, and because of this, it is very likely that the run-time is small. We will call this phenomenon the *Leningrad paradox*, since it is dual to the St. Petersburg paradox.

The following two theorems show that both Algorithm **SPHERICALHOMOLOGY** and Algorithm **AFFINEHOMOLOGY** run in weak singly exponential time.

Theorem 4\\$214. Let $\alpha \geq 1$.

(A) Let $f \in \mathcal{H}_d[q]$ be a random KSS polynomial tuple and Φ a Boolean formula over f .

Then the run-time of Algorithm **SPHERICALHOMOLOGY** on input (f, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)} \alpha^{10n(n+1)}$$

with probability at least $1 - 1/\alpha$.

(S) Let $\sigma > 0$, $f \in \mathcal{H}_d[q]$, $f_\sigma \in \mathcal{H}_d[q]$ be a random polynomial tuple uniformly distributed in $B_W(f, \sigma)$ and Φ a Boolean formula over f . Then the run-time of Algorithm **SPHERICALHOMOLOGY** on input (f, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)} \left(\frac{\alpha}{\sigma}\right)^{10n(n+1)}$$

with probability at least $1 - 1/\alpha$.

The constants inside the O -symbols are universal.

Theorem 4\\$215. Let $\alpha \geq 1$.

(A) Let $p \in \mathcal{P}_d[q]$ be a random KSS polynomial tuple and Φ a Boolean formula over p .

Then the run-time of Algorithm **AFFINEHOMOLOGY** on input (p, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)} \alpha^{10n(n+1)}$$

with probability at least $1 - 1/\alpha$.

- (S) Let $\sigma > 0$, $p \in \mathcal{P}_d[q]$, $\mathfrak{p}_\sigma \in \mathcal{P}_d[q]$ be a random polynomial tuple uniformly distributed in $B_W(p, \sigma)$ and Φ a Boolean formula over \mathfrak{p} . Then the run-time of Algorithm **AFFINE-HOMOLOGY** on input (\mathfrak{p}, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)} \left(\frac{\mathfrak{r}}{\sigma}\right)^{10n(n+1)}$$

with probability at least $1 - 1/\mathfrak{r}$.

The constants inside the O -symbols are universal.

Proof of Theorem 4^{S2}14. This is a combination of the probability tail bound of Proposition 1^{S3}5 and the run-time bound of Theorem 4^{S2}10. \square

Proof of Theorem 4^{S2}15. This is a combination of the tail bound of Corollary 1^{S4}6 and the run-time bound of Theorem 4^{S2}13. \square

By choosing a concrete probability measure, we get the following estimate that justifies the claim that Algorithms **SPHERICALHOMOLOGY** and **AFFINEHOMOLOGY** run in weak singly exponential time. We note here that we are using this notion in a different way than the creators (see Remark 4^{S2}11 below). The advantage of the following corollaries is that it puts a probability that goes to zero with $(2qD)^n$, which can be seen as the “symbolic size” of the input.

Corollary 4^{S2}16. [91, 92; Theorem 1.1(ii)].

- (A) Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a random KSS polynomial tuple and Φ a Boolean formula over \mathfrak{f} . Then the run-time of Algorithm **SPHERICALHOMOLOGY** on input (\mathfrak{f}, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)}$$

with probability at least $1 - (2qD)^{-n}$.

- (S) Let $\sigma > 0$, $f \in \mathcal{H}_d[q]$, $\mathfrak{f}_\sigma \in \mathcal{H}_d[q]$ be a random polynomial tuple uniformly distributed in $B_W(f, \sigma)$ and Φ a Boolean formula over \mathfrak{f} . Then the run-time of Algorithm **SPHERICALHOMOLOGY** on input (\mathfrak{f}, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)} \sigma^{-10n(n+1)}$$

with probability at least $1 - (2qD)^{-n}$.

In other words, Algorithm **SPHERICALHOMOLOGY** runs in weak singly exponential time with respect to n and in weak singly polynomial time with respect q and D . \square

Corollary 4^{S2}17. [91, 92; Theorem 1.1(ii)].

- (A) Let $\mathfrak{p} \in \mathcal{P}_d[q]$ be a random KSS polynomial tuple and Φ a Boolean formula over \mathfrak{p} . Then the run-time of Algorithm **AFFINEHOMOLOGY** on input (\mathfrak{p}, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)}$$

with probability at least $1 - (2qD)^{-n}$.

(S) Let $\sigma > 0$, $p \in \mathcal{P}_d[q]$, $\mathfrak{p}_\sigma \in \mathcal{P}_d[q]$ be a random polynomial tuple uniformly distributed in $B_w(p, \sigma)$ and Φ a Boolean formula over \mathfrak{f} . Then the run-time of Algorithm **AFFINE-HOMOLOGY** on input (\mathfrak{p}, Φ) is at most

$$\text{size}(\Phi)(qD)^{O(n^3)}\sigma^{-10n(n+1)}$$

with probability at least $1 - (2qD)^{-n}$.

In other words, Algorithm **AFFINEHOMOLOGY** runs in weak singly exponential time with respect to n and in weak polynomial time with respect q and D . \square

Remark 4§2 11. We note that the interpretation that we do here of the weak complexity of Amelunxen and Lotz [6] is a more liberal interpretation of [6, Definition 1.1]. In our interpretation, we are saying that an algorithm has weak $f(k)$ -time (with respect the input size-controlling parameter k) when it takes $f(k)$ -time with probability at least $1 - 1/f(k^{O(1)})$, where $O(1)$ may not be constant with respect other parameters. We note that this does not always mean weak in the sense of Amelunxen and Lotz, although it has the same underlying philosophy. ¶

4§3 Parallelization and numerical stability

We discuss two advantages of our algorithms for computing homology: parallelization and stability. The former allows us to cut down the running time of the algorithm by distributing the algorithm's work among many processors. This is a typical advantage of the grid method. The latter allows us to run our algorithms in finite precision floating-point, which turns all the above condition-based and probabilistic complexity estimates into bit-complexity estimates. This is a common property of good numerical algorithms.

Since Algorithm **AFFINEHOMOLOGY** is just a call to Algorithm **SPHERICALHOMOLOGY** after homogenization, we only have to analyze this for the latter algorithm.

4§3–1 Parallelization

First, we recall the notion of a parallel algorithm; second, we show that $\bar{\kappa}$ -ESTIMATE can be done in parallel weak polynomial time; third, we show that this is the case also for the construction of the simplicial complex of **SPHERICALHOMOLOGY**; and fourth and last, we discuss which topological invariants can be computed in parallel polynomial time.

Remark 4§3 1. We will give the probabilistic bounds only in the average setting and not in the smoothed setting, since the latter can be obtained from the former by multiplying by an appropriate power of σ . Moreover, we will give only this bound in its simplest form. ¶

What is a parallel algorithm?

Leaving formalities aside, a parallel algorithm is an algorithm in which several computational processes can run simultaneously. There are issues regarding the communication between processors executing the parallel computational process, but we will assume that there is no issue in this regard as it is standard practice in theoretical analysis [67]. Because of this, we are assuming that processors share a common working space that all of them can access. This might be an issue when implementing the algorithm, but one can get around it.

To describe a parallel algorithm, we will incorporate into our pseudocode a parallel loop in which we indicate what each processor does. When a parallel loop is executed, our convention is 1) that each processor has read from the memory whatever values it need to operate with and 2) that each position of the memory can be modified by at most one processor.

Example 4^{§3}1. Let's consider the example of the Algorithm **PARMULTIPLICATION** that multiplies n numbers in parallel. In the second parallel loop, even though x_i might be modified by some processor, every processor needing its value has read it before the parallel loop has started. The reader should consider the practical challenges that this feature of our parallel computational model implies. Δ

Algorithm 7: PARMULTIPLICATION

Input : $x_1, \dots, x_n \in \mathbb{R}$

```

 $\ell \leftarrow \lceil \log n \rceil$ 
for  $i = n + 1, \dots, 2^\ell$  parallelly do
     $x_i \leftarrow 1$ 
for  $i = 1, \dots, \ell$  do
    for  $i = 1, \dots, 2^{\ell-i}$  parallelly do
         $x_i \leftarrow x_{2i-1}x_{2i}$ 
return  $x_1$ 

```

Output : $\prod_{i=1}^n x_i$

To measure the run-time of a parallel algorithm, we will take as the run-time of a parallel loop the run-time of the longest computation in it. However, together with this parallel run-time, we will indicate the minimum number of processors needed. Note that the sequential run-time is the parallel run-time times the number of processors.

Remark 4^{§3}2. Assuming that multiplications are constant-cost, Algorithm **PARMULTIPLICATION** runs in parallel $O(\log(n))$ -time with $O(n)$ processor. Note that the parallel run-time is logarithmic in n while the usual run-time is linear in n under this assumption. Note that the assumption that multiplications are constant-cost is reasonable when we operate with floating-point arithmetic.

However, we should be careful when multiplications are not constant-cost. Assume that x_1, \dots, x_n are integers of bit-size at most b which we multiply with standard multiplication. Then Algorithm **PARMULTIPLICATION** runs in parallel $O(n^2 b^2)$ -time with $O(n)$ processor which equals the sequential run-time $O(n^2 b^2)$. The reason for this is that the size of the numbers is growing and so does the time that each parallel loop requires. Nevertheless, we note that if we use a parallel algorithm for multiplying integers, such as that of Bunimov and Schimmler [81], that takes whose parallel time is bounded by $O(\log b)$, then Algorithm **PARMULTIPLICATION** will run in parallel $O(\log^2(n) \log(b))$ -time. \P

Parallel $\bar{\kappa}$ -ESTIMATE

To parallelize Algorithm $\bar{\kappa}$ -ESTIMATE, we only have to pay attention to how we parallelize the computation of

$$\max\{\kappa(f^L, x) \mid x \in \mathcal{G}_{\tilde{n}}, \#L \leq n+1\}$$

This can be easily done following a trick similar to that of Algorithm PARMULTIPLICATION. Let **PARMAX** be the parallel algorithm obtained from Algorithm PARMULTIPLICATION after substituting the initial 1 assignment by a $-\infty$ assignment and the multiplication $x_{2i-1}x_{2i}$ by the maximum $\max\{x_{2i-1}, x_{2i}\}$. Note that computing the maximum of two numbers can be assumed to have a constant run-time along the full algorithm. With the help of **PARMAX**, we can parallelize Algorithm $\bar{\kappa}$ -ESTIMATE to obtain Algorithm $\bar{\kappa}$ -PARESTIMATE.

Algorithm 8: $\bar{\kappa}$ -PARESTIMATE

Input : $f \in \mathcal{H}_d[q]$
 $\rho \in (0, 1)$
 $B \in (0, \infty]$

```

 $\tilde{n} \leftarrow 0$ 
repeat
     $\tilde{n} \leftarrow \tilde{n} + 1$ 
    for  $x \in \mathcal{G}_{\tilde{n}}$ ,  $L \in [q]^{\leq n+1}$  parallelly do
         $K(x, L) \leftarrow \kappa(f^L, x)$ 
     $K \leftarrow (1 - \rho)^{-1} \text{PARMAX}(K(x, L) \mid x \in \mathcal{G}_{\tilde{n}}, L \in [q]^{\leq n+1})$ 
until  $DK 2^{-\tilde{n}} \leq \rho(1 + \rho)$  or  $B \leq K$ 
if  $B \leq K$  then
    return fail
else
    return  $K$ 

```

Output : fail or $K \in (0, \infty)$

Postcondition: If fail, then $B \leq K \leq \bar{\kappa}(f)$;

otherwise $\bar{\kappa}(f) \leq K \leq (1 - \rho)^{-1} \bar{\kappa}(f)$

Arguing as in Theorem 4§2 8, the following theorem is immediate.

Theorem 4§3 1. *Algorithm $\bar{\kappa}$ -PARESTIMATE is correct. Its parallel run-time on input (f, ρ, B) is bounded by*

$$O(n^3 + N + n \log(qnD \min\{B, \bar{\kappa}(f)\} \rho^{-1}))$$

and its number of processors is bounded by $O(q(nD \min\{B, \bar{\kappa}(f)\} \rho^{-1})^n)$. \square

Using the probabilistic bounds, we can see that the expected parallel run-time is finite and that with high probability the number of processors is singly exponential. This still holds when the input is $H(\rho)$, with $\rho \in \mathcal{P}_d[q]$.

Corollary 4^{S3}2. Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a random KSS polynomial tuple, $\rho \in (0, 1)$ and $B > 0$. Then, on input (\mathfrak{f}, ρ, B) , the parallel run-time and number of processors required by Algorithm $\bar{\kappa}$ -PARESTIMATE are, respectively, at most

$$\mathcal{O}\left(n^3 + N + n \log \left(\min \left\{B, (qD)^{O(n)}\right\} \rho^{-1}\right)\right) \text{ and } \mathcal{O}\left(q \left(qnD \min\{B, (qD)^{O(n)}\} \rho^{-1}\right)^n\right),$$

with probability at least $1 - (2qD)^{-n}$.

Proof. This is Theorem 4^{S3}1 combined with Proposition 1^{S3}5. \square

Parallel construction of the simplicial complex of SPHERICALHOMOLOGY

When we construct the simplicial complex in SPHERICALHOMOLOGY, there are three steps that have to be parallelized: 1) the construction of the cloud of points $X_{i,j}^\infty$, 2) the construction of the Vietoris-Rips graph, and 3) the construction of the final simplicial complex. All of these parts of the algorithm can be easily made parallel.

We show in Algorithm PARHOMOLOGYWITNESS how the parallelization can be done explicitly. Instead of encoding the sets as sets, we encode them as appropriate indicator functions. In this way, in Algorithm PARHOMOLOGYWITNESS, the $X_{i,j}^\infty$ are represented by maps $\mathcal{S}^\infty : \mathcal{G}_{\bar{n}} \rightarrow \{0, 1\}^{q \times (4n+9)}$, the edges of the Vietoris-Rips graph by a map $E : \binom{\mathcal{G}_{\bar{n}}}{2} \rightarrow \{0, 1\}$ and the final simplicial complex as a map $\mathcal{S} : [\mathcal{G}_{\bar{n}}]^{\leq n+2} \rightarrow \{0, 1\}$.

The following theorem is proven in the exact way as Theorem 4^{S2}10.

Theorem 4^{S3}3. Algorithm PARHOMOLOGYWITNESS is correct. Its parallel run-time on input (f, Φ) is bounded by

$$\mathcal{O}(\text{size}(\Phi) + N)$$

and its number of processors by $\mathcal{O}\left(q (131nD\bar{\kappa}(f))^{2n(n+2)}\right)$. \square

Remark 4^{S3}3. The main reason we have omitted the call to Algorithm $\bar{\kappa}$ -PARESTIMATE in Algorithm PARHOMOLOGYWITNESS is to emphasize that the parallel run-time is independent of the condition number. However, one should notice that the number of processors does depend on the condition number. \P

Remark 4^{S3}4. Assume that Φ is already negation free. One can optimize the algorithm in this parallel setting, by evaluating Φ in a parallel way. This would substitute the size of Φ by its depth, which is the maximum number of concatenated parentheses that appear in Φ . Further, even if the depth is not small, by Brent's theorem [82; (21.35)], one can always rewrite Φ in a way that its depth is the logarithm of its size up to a constant factor. \P

Remark 4^{S3}5. If we are interested only in the first ℓ homology groups, there is no need to construct the full $(n+1)$ -dimensional simplicial complex. This brings down the number of processors to $\mathcal{O}\left(q (131nD\bar{\kappa}(f))^{2n(\ell+2)}\right)$, but leaves the parallel run-time unchanged. \P

As above, Theorem 4^{S3}3 with Proposition 1^{S3}5 give the following corollary.

Corollary 4^{S3}4. Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a random KSS polynomial tuple and Φ a Boolean formula over \mathfrak{f} . Then, on input (\mathfrak{f}, Φ) , the parallel run-time and number of processors required by Algorithm PARHOMOLOGYWITNESS are, respectively, at most

$$\mathcal{O}(\text{size}(\Phi) + N) \text{ and } (qD)^{O(n^3)},$$

with probability at least $1 - (2qD)^{-n}$. \square

Algorithm 9: PARHOMOLOGYWITNESS

Input : $f \in \mathcal{H}_d[q]$

Boolean formula Φ over p

$K \in [0, \infty)$

Precondition : $\bar{\kappa}(f) \leq K \leq 1.02\bar{\kappa}(f)$

eliminate negations in Φ

$\theta \leftarrow 1/(9(n+2)DK), \mathbf{x}_0 \leftarrow 0$

for $i = 1, \dots, n+2$ **parallelly do**

$\mathbf{e}_i \leftarrow (2i-1)\theta, \mathbf{d}_i \leftarrow 2i\theta$
 $\mathbf{x}_{2i-1} \leftarrow \mathbf{e}_i, \mathbf{x}_{2i} \leftarrow \mathbf{d}_i, \mathbf{x}_{2(i+n+2)-1} \leftarrow -\mathbf{e}_i, \mathbf{x}_{2(i+n+2)} \leftarrow -\mathbf{d}_i$

$\tilde{y} \leftarrow \lceil \log 2700(n+2)D^2K^2 \rceil$

$\varepsilon \leftarrow 1/(277(n+2)D^{3/2}K)$

Initialize $\mathcal{S}^{\geq}, \mathcal{S}^{\leq} : [\mathcal{G}_{\tilde{y}}]^{\leq n+2} \rightarrow \{0, 1\}^{q \times (4n+9)}$

for $x \in \mathcal{G}_{\tilde{y}}, i = 1, \dots, q$ **and** $j = 0, \dots, 4(n+2)$ **parallelly do**

if $f_i(x) - (\mathbf{x}_j + D^{1/2}2^{-\tilde{y}})\|f_i\|_W > 0$ **then**

$\mathcal{S}_{i,j}^{\geq}(\{x\}) \leftarrow 1, \mathcal{S}_{i,j}^{\leq}(\{x\}) \leftarrow 0$

else if $f_i(x) - (\mathbf{x}_j - D^{1/2}2^{-\tilde{y}})\|f_i\|_W < 0$ **then**

$\mathcal{S}_{i,j}^{\geq}(\{x\}) \leftarrow 0, \mathcal{S}_{i,j}^{\leq}(\{x\}) \leftarrow 1$

else

$\mathcal{S}_{i,j}^{\geq}(\{x\}) \leftarrow 1, \mathcal{S}_{i,j}^{\leq}(\{x\}) \leftarrow 1$

Initialize $E : \binom{\mathcal{G}_{\tilde{y}}}{2} \rightarrow \{0, 1\}$

for $\{x, y\} \in \binom{\mathcal{G}_{\tilde{y}}}{2}$ **parallelly do**

if $\text{dist}(x, y) \leq 2\varepsilon$ **then**

$E(\{x, y\}) \leftarrow 1$

else

$E(\{x, y\}) \leftarrow 0$

for $A \in [\mathcal{G}_{\tilde{y}}]^{\leq n+2}, i = 1, \dots, q$ **and** $j = 0, \dots, 4(n+2)$ **parallelly do**

$\mathcal{S}_{i,j}^{\geq}(A) \leftarrow \text{PARMIN}\left(\mathcal{S}_{i,j}^{\geq}(\{x\}), E(\{x, y\} \mid x \in A, \{x, y\} \in \binom{A}{2})\right)$

$\mathcal{S}_{i,j}^{\leq}(A) \leftarrow \text{PARMIN}\left(\mathcal{S}_{i,j}^{\leq}(\{x\}), E(\{x, y\} \mid x \in A, \{x, y\} \in \binom{A}{2})\right)$

$\mathcal{S}_{i,j}^{\equiv}(A) \leftarrow \min\{\mathcal{S}_{i,j}^{\leq}(A), \mathcal{S}_{i,j}^{\geq}(A)\}$

Initialize $\mathcal{S} : [\mathcal{G}_{\tilde{y}}]^{\leq n+2} \rightarrow \{0, 1\}$

for $A \in \mathcal{G}_{\tilde{y}}^{\leq n+2}$ **parallelly do**

$\mathcal{S}(A) \leftarrow \Phi^{\Gamma_{B_{\Delta, \Theta}}}\left(\mathcal{S}_{i,j}^{\equiv}(A), \mathcal{S}_{i,j}^{\geq}(A), \mathcal{S}_{i,j}^{\leq}(A) \mid i \in [q], j \in \{0, \dots, 4(n+2)\}\right)$

return \mathcal{S}

Output

: Indicator function \mathcal{S} of $(n+1)$ -dimensional simplicial complex
homologically equivalent to $S(f, \Phi)$

Parallel computation of the homology

The parallel computation of the homology or Betti numbers of a simplicial complex can easily be reduced to a parallel computation of, respectively, the SNFs and ranks of the boundary operators. This reduces the problem to the parallel computation of the SNF or rank of an integer matrix. We note that although one can obtain improvements by taking into account the simplicial complex structure, Edelsbrunner and Parsa [169] showed that this would lead to improvements in computations involving sparse matrices.

Despite the numerous successes for these problems for polynomials rings (see [400]), there is not a satisfactory parallel logarithmic time algorithm for the SNF of integer matrices. This phenomenon can be seen as a consequence of the current lack of parallel logarithmic time algorithms for computing the greatest common divisor [361]. Because of this, we will focus on the rank and comment the problem for the SNF.

Betti numbers In an algebraic model of computation, one can parallelize very easily the computation of the coefficients of the characteristic polynomial using the results of Berkowitz's algorithm [49]. With this algorithm, we can easily compute the rank of a matrix.

Theorem 4^{§3}5 (Berkowitz's theorem). *Let \mathbb{F} be a field. There is a parallel algorithm BERKOWITZSAMUELSON that computes the coefficients of the characteristic polynomial of a matrix $A \in \mathbb{F}^{m \times m}$ in parallel run-time $O(\log^2 m)$ with $O(m^4)$ processors, in the algebraic computational model.* \square

Corollary 4^{§3}6. *Let \mathbb{F} be a field. There is a parallel algorithm PARRANK that computes the rank of a matrix $A \in \mathbb{F}^{m \times m'}$ in parallel run-time $O(\log^2 \max\{m, m'\})$ with $O(\max\{m, m'\}^4)$ processors, in the algebraic computational model.*

Proof. We compute AA^* in parallel $O(\log \max\{m, m'\})$ -time with $O(nm)$ processors. This matrix has the same rank as A . Now, the rank of AA^* is equal to degree of the characteristic polynomial minus the order of X in it. The latter can be compute by a binary search. Theorem 4^{§3}5 and Algorithm BERKOWITZSAMUELSON finish the proof. \square

We have now two ways to proceed, as we did with Algorithm PARMULTIPLICATION. On the one hand, the above algorithm allows immediately for the computation of the mod p Betti numbers in parallel time. The key point is that this over a finite field the algebraic model estimates appropriately the run-time with respect the bit-size. On the other hand, using parallel integer arithmetic for addition [286] and multiplication [81], we can translate the algorithm PARRANK into a parallel polynomial-time algorithm.

For the computation of the mod p Betti numbers in parallel time, we obtain the following result.

Theorem 4^{§3}7. *There is an algorithm PARSPHERICALPRIMEBETTI, obtained from combining Algorithms 8, 9 and PARRANK, to compute only the first ℓ mod p Betti numbers. The parallel run-time of this algorithm on input (f, Φ, ℓ, p) is bounded by*

$$O(\text{size}(\Phi) + n^3 + N + n \log(qnD\bar{\kappa}(f)) \log p)$$

and its number of processors by $O(q(131nD\bar{\kappa}(f))^{8n(\ell+2)})$.

Proof. The first part is Theorems 4§3.1 and 4§3.3 and Corollary 4§3.6. \square

We note that if we allow a probability of error, we can produce a Monte Carlo algorithm for the rank reducing modulo a random prime as in [191; Lemma 4.1], but calling Algorithm PARRANK instead. This has the advantage that it is more realistic in practice.

Theorem 4§3.8. *There is an algorithm PARSPHERICALBETTI, obtained from combining Algorithms 8, 9 and PARRANK, to compute only the first ℓ Betti numbers. On input (f, Φ, ℓ, δ) , the algorithm is correct with a probability of δ , its parallel run-time is bounded by*

$$O(\text{size}(\Phi) + n^3 + N + n^2 \log^2(qnD\bar{\kappa}(f)))$$

and its number of processors by $O\left(q(131nD\bar{\kappa}(f))^{8n(\ell+2)} \log(1/\delta)\right)$. \square

Corollary 4§3.9. *Let $f \in \mathcal{H}_d[q]$ is a random KSS polynomial tuple and Φ a Boolean formula over f . Then, on input (f, Φ, ℓ, δ) , the parallel run-time and number of processors required by Algorithm PARSPHERICALBETTI is, respectively, at most*

$$O(\text{size}(\Phi) + N + n^4 \log^2(qD)) \text{ and } (qD)^{O(n^2\ell)} \log(1/\delta),$$

with probability at least $1 - (2qD)^{-n}$. \square

If we use parallel integer arithmetic, we obtain analogous results to above, but without a probability of error. However, this certainty will come at a cost, since it will increase the constants in the exponents appearing in the two results above by a factor of two.

All the above results can be translated to the affine case easily with analogous statements.

Homology In the last years, there have been discovered some parallelizable algorithms for computing the SNF of an integer matrix by Dumas, Saunders and Villard [161], by Jäger [233], and Jäger and Wagner [234]. Further, Dumas, Heckenbach, Saunders and Welker [160] have paid special attention to the computation of the SNF for computing homology groups. However, none of these algorithms has a complexity analysis giving parallel logarithmic run-time. Actually, none of the algorithm has a satisfactory complexity analysis giving an estimation on the parallel run-time, although all of the algorithms can be seen to work very well in practice.

The above pose us to consider the following question, on which the parallelization of the computation of homology relies.

Open problem G. *Is there a parallel algorithm with parallel logarithmic run-time computing the SNF of a (possibly sparse) integer matrix? In particular, is there a parallel algorithm with parallel logarithmic run-time computing the greatest common divisor of n integers?*²

²We note that this particular case of computing the SNF is still open. As of today, the best parallel algorithm for computing the GCD is by Sedjelmaci [361] and it runs in sublinear, but not logarithmic, parallel time.

Remark 4^{§3} 6. We note that the claims in [88, 91, 92] about the easy parallelization of the Algorithms **SphericalHomology** and **AffineHomology**, regarding the torsion coefficients, are false. This should serve as a cautionary tale regarding assuming easy parallelizations without references.³ ¶

4^{§3}–2 Numerical stability

We now perform an error analysis to show that Algorithms **SphericalHomology** and **AffineHomology** can output correct answers when run with finite precision. Doing this error analysis is essential to transform our run-time bounds, where we count arithmetic operations with real numbers at unit cost, into effective bounds that allow the algorithm to work in practice. In other words, we don't do this tedious technical task because we like it, but because we must do it to show that the algorithm is numerically stable. We will follow mainly the lines of Cucker, Krick, Malajovich and Wschebor [139] for their algorithm for counting zeros.

First, we introduce the floating-point framework of numerical computation; second, we provide some error bounds for the computation of some basic objects (scalar products, evaluations of polynomials and their derivatives); third, we perform an error analysis of Algorithms **SphericalHomology**; and fourth and last, we state the error analysis for Algorithm **AffineHomology**.

Floating-point framework of numerical computation and error analysis

The floating-point framework of numerical computation is the bread and butter of the numerical analyst. With it, one can perform an error analysis of numerical algorithms where one sees how the errors grow as we perform the algorithm.

First, we introduce the floating-point number system, which is the approximation system for numbers, second, the floating point model of computation, which is the set of assumptions on precision of basic operations that we assume; and third, error analysis, where we state some results regarding the error assumptions of scalar products and matrix multiplications.

Floating-point number system In a fixed precision number system, the point does not move. However, this can be annoying for writing numbers such as 0.00000283. This motivates scientific notation in which the former number is written as $0.283 \cdot 10^{-5}$. The floating-point number system is the formalization of this system of encoding numbers. All of this has to be seen as an abstraction of the IEEE floating-point standard, which happens in real computers. For more details, we refer the reader to [221; Ch. 2].

Definition 4^{§3} 1. [221; §2.1] A *floating-point number system* in base b , with precision t and exponent range $[e_0, e_1]$ is the subset of \mathbb{R} given by

$$F_{b,t}^{e_0, e_1} := \{\pm m \cdot b^{e-t} \mid e \in [e_0, e_1] \cap \mathbb{Z}, m \in [0, b^t - 1] \cap \mathbb{N}\} \subseteq [b^{e_0-1}, b^{e_1}(1-b^{-t})]. \quad (4.30)$$

³Let us remark that computing the SNF efficiently is a highly non-trivial problem. The first polynomial-time algorithm is from 1979 by Kannan and Bachem [242] and it is still unknown whether any algorithm proposed before that year is polynomial-time (see [415; Ch. 5] for an overview of the history of polynomial-time algorithms for computing the SNF of integer matrices).

The *range* of $F_{b,t}^{e_0, e_1}$ is the interval $[b^{e_0-1}, b^{e_1}(1 - b^{-t})]$ and the *round-off unit* of $F_{b,t}^{e_0, e_1}$ is $\mathbf{u}_{b,t} := \frac{1}{2}b^{1-t}$.

We note that every number in F as above can be written in the form

$$\pm 0.d_1 d_2 \dots d_t \cdot b^e$$

with $0.d_1 d_2 \dots d_t$ a number written in base b , where each d_i is an integer between 0 and $b - 1$, and $e \in [e_0, e_1] \cap \mathbb{Z}$. These numbers tend to accumulate around zero and become more disperse when we go far from zero.

Together with $F_{b,t}^{e_0, e_1}$, we consider the *rounding map*

$$\text{fl}_{b,t} : \mathbb{R} \rightarrow F_{b,t}^{-\infty, \infty} := \{mb^{e-t} \mid e \in \mathbb{Z}, m \in [1 - b^t, b^t - 1] \cap \mathbb{Z}\} \quad (4.31)$$

that maps each $x \in \mathbb{R}$ to a nearest point in $F_{b,t}$. The main property of this map is that it gives good relative error approximations.

Theorem 4§3 10. [221; Theorem 2.2]. Let $b, t \in \mathbb{N}$. Then for all $x \in \mathbb{R}$,

$$\text{fl}_{b,t}(x) = x(1 + \delta)$$

for some $\delta \in (-\mathbf{u}_{b,t}, \mathbf{u}_{b,t})$. In particular, $|\text{fl}_{b,t}(x) - x| < \mathbf{u}_{b,t}|x|$. \square

We note that it might be the case that $\text{fl}_{b,t}(x)$ is too big or too small to lie inside $F_{b,t}^{e_0, e_1}$. In this case, if $|\text{fl}_{b,t}(x)| > \max\{|y| \mid y \in F_{b,t}^{e_0, e_1}\}$, we will say that x *overflows* with respect to $F_{b,t}^{e_0, e_1}$, and if $0 < |\text{fl}_{b,t}(x)| < \max\{|y| \mid y \in F_{b,t}^{e_0, e_1} \setminus \{0\}\}$, we will say that x *underflows* with respect to $F_{b,t}^{e_0, e_1}$. This might be problematic, as the rounding becomes $\pm\infty$ when x overflows and ± 0 when it underflows.

To avoid tedious notation, we will omit all subindices and superindices from now on. We will focus mainly on the round-off error unit \mathbf{u} , which will be the quantity of major concern.

Arithmetic in floating point We note that given $x, y \in F$, we want to compute fast a good approximation of $x \text{ op } y$, where $\text{op} \in \{+, -, \cdot, /\}$, and we also want that this approximation stays in F . The main idea is that we want our approximate operation $\widetilde{\text{op}}$ to behave like $\text{fl}(x \text{ op } y)$. This motivates the following assumption:

Standard model of arithmetic. For each $\text{op} \in \{+, -, \cdot, /\}$, there is an approximate operation $\widetilde{\text{op}} : F \times F \rightarrow F$ such that for all $x, y \in F$,

$$x \widetilde{\text{op}} y = (x \text{ op } y)(1 + \delta) \quad (4.32)$$

for some $\delta \in (-\mathbf{u}, \mathbf{u})$.

This means that we can assume that $x \widetilde{\text{op}} y = \text{fl}(x \text{ op } y)$ in some sense. We will further assume that the above holds also for the square root operation.

It is important to observe that for the floating point number system $F_{b,t}^{e_0, e_1}$, one can perform the above operations in run-time bounded by

$$\mathcal{O}((t \log b)^2 + \max\{\log |e_0|, \log |e_1|\}) = \mathcal{O}(\log^2 \mathbf{u}^{-1} + \max\{\log |e_0|, \log |e_1|\}),$$

using standard arithmetic. This means that run-time of the numerical algorithm can be bounded by the algebraic run-time times the above quantity, once we have a bound on how small the round-off unit has to be and how big is the exponent range.

Error analysis Let $F(x_1, \dots, x_n)$ be some quantity or vector that we want to compute from x_1, \dots, x_n using the operations $+, -, \cdot, /$ and $\sqrt{}$. We will refer to the value computed by some round-off algorithm as $\text{fl}^a(F(x_1, \dots, x_n))$, which is a floating point approximation obtained by computing F from the values $\text{fl}(x_1), \dots, \text{fl}(x_n)$ using the approximate operations $\tilde{+}, \tilde{-}, \tilde{\cdot}, \tilde{/}$ and $\tilde{\sqrt{}}$. Note that $\text{fl}^a(F(x_1, \dots, x_n))$ and how good it approximates $F(x_1, \dots, x_n)$ depends not only on the parameters of the floating point system, but also on the round-off algorithm.

Note that $\text{fl}^a(x \text{ op } y) = \text{fl}(x) \tilde{\text{op}} \text{fl}(y)$. So we should not confuse $\text{fl}^a(x \text{ op } y)$ and $x \tilde{\text{op}} y$. The former gives the floating point approximation of the operation between two arbitrary real numbers, while the latter assumes that these numbers are already written in floating point.

Our objective is to obtain round-off algorithms such that in the inequality

$$\|F(x_1, \dots, x_n) - \text{fl}^a(F(x_1, \dots, x_n))\| \leq G_F(x_1, \dots, x_n)\mathbf{u}$$

the value of $G_F(x_1, \dots, x_n)$ is small without worsening much the run-time. A usual parameter that appears in error bounds is

$$\beta(k) := \frac{k\mathbf{u}}{1-k\mathbf{u}}, \quad (4.33)$$

which is defined only if $k\mathbf{u} < 1$.

The following proposition is the basic approximation operation.

Proposition 4^{S3}11. $(\pm) |\text{fl}^a(x \pm y) - (x \pm y)| \leq (|x| + |y|)\beta(2)$.

$$(\cdot) |\text{fl}^a(x \cdot y) - (x \cdot y)| \leq |xy|\beta(3).$$

$$(/) |\text{fl}^a(x/y) - (x/y)| \leq |x/y|\beta(3).$$

$$(\sqrt{}) |\text{fl}^a(\sqrt{x}) - (\sqrt{x})| \leq |\sqrt{x}|\beta(1).$$

□

Remark 4^{S3}7. We note that sums are unstable when $x + y$ is much smaller than $|x| + |y|$, i.e., when cancellation occurs. ¶

Instead of writing $(1 + \rho)$ where $\rho \in [-\beta(k), \beta(k)]$, we will just write $(1 + \llbracket k \rrbracket)$. The following proposition gives the major properties of this new symbol.

Proposition 4^{S3}12. [221; Lemma 3.1 and 3.3]. Let $k, l \in \mathbb{N}$, the following holds

$$\begin{aligned} (1 + \llbracket k \rrbracket)(1 + \llbracket l \rrbracket) &= (1 + \llbracket k + l \rrbracket) \\ (1 + \llbracket k \rrbracket)(1 + \llbracket l \rrbracket)^{-1} &= (1 + \llbracket k + l \rrbracket), \quad \text{if } l \leq k \\ (1 + \llbracket k \rrbracket)(1 + \llbracket l \rrbracket)^{-1} &= (1 + \llbracket k + 2l \rrbracket), \quad \text{if } l > k \\ \beta(k)\beta(l) &\leq \beta(\min\{k, l\}), \quad \text{if } \max\{k, l\}\mathbf{u} < 1/2 \\ k\beta(l) &\leq \beta(kl), \quad \text{if } kl\mathbf{u} < 1 \\ \beta(k) + \beta(l) &\leq \beta(k + 1), \quad \text{if } (k + 1)\mathbf{u} < 1 \\ \beta(k) + \beta(l) + \beta(k)\beta(l) &\leq \beta(k + l), \quad \text{if } (k + l)\mathbf{u} < 1. \end{aligned}$$

In particular, let $\rho \in \{-1, +1\}^m$, then

$$\prod_{i=1}^n (1 + \llbracket 1 \rrbracket)^{\rho_i} = (1 + \llbracket n \rrbracket)$$

□

Using the above propositions, one can easily prove the followings proposition that will be very useful for us. We will focus on the computation of inner products, norms and products of matrices. Since the error bounds presented here are standard, we omit the proofs.

Theorem 4§3 13. [221; §3.1]. *There is a round-off algorithm computing the inner product $\langle x, y \rangle$ for $x, y \in \mathbb{R}^a$ such that*

$$\text{fl}^a(\langle x, y \rangle) = \langle x, y \rangle + \lceil \log a \rceil + 3 \lceil |x|, |y| \rceil$$

where $|z| := (|z_1| \dots |z_a|)^*$. The algorithm has run-time bounded by $O(a)$.

Moreover, let $\hat{x}, \hat{y} \in F$, be such that for all $i \in [n]$,

$$\hat{x}_i = (1 + \lceil k \rceil)x_i \text{ and } \hat{y}_i = (1 + \lceil l \rceil)y_i,$$

then

$$\text{fl}^a(\langle x, y \rangle) = \langle x, y \rangle + \lceil \log a \rceil + 1 + k + l \lceil |x|, |y| \rceil.$$

Sketch of proof. Adding from left to right, we can easily see that

$$\text{fl}^a(\langle x, y \rangle) = \langle x, y \rangle + \lceil a + k + l \rceil.$$

The desired result follows from putting the sum into a tree. Note that the original result is the result for the case $k = l = 1$. \square

Corollary 4§3 14. *There is a round-off algorithm computing the norm $\|x\|$ for $x \in \mathbb{R}^a$ such that*

$$\text{fl}^a(\|x\|) = \|x\|(1 + \lceil 4 + \log a \rceil).$$

The algorithm has run-time bounded by $O(a)$. \square

The most important consequence of this result are the following two propositions.

Proposition 4§3 15. *There is a round-off algorithm computing $f(x)/\|f\|_w$ for $f \in \mathcal{H}_d[q]$ and $x \in \mathbb{S}^n$ such that*

$$\|\text{fl}^a(f(x)/\|f\|_w) - f(x)/\|f\|_w\| \leq \lceil D + 4\lceil \log(N) \rceil + 15 \rceil$$

The algorithm has run-time bounded by $O(N)$.

Proof. For evaluation, we use the usual algorithm. Consider the monomial vector (x^α) , then $f_i(x) = \langle (f_{i,\alpha}), (x^\alpha) \rangle$. Note that for each α , $\text{fl}^a(x^\alpha) = x^\alpha(1 + \lceil D \rceil)$. Therefore, by Theorem 4§3 13, we get

$$\text{fl}^a(f_i(x)) = f_i(x) + \|f_i\|_w \lceil D + \lceil \log(N_i) \rceil + 3 \rceil,$$

where we used Corollary 1§1 7 to bound $\langle (|f_{i,\alpha}|), \text{fl}^a((x^\alpha)) \rangle$. By Corollary 4§3 14, we have that

$$\|\text{fl}^a(\|f\|_w) - \|f\|_w\| \leq \|f\|_w \lceil \log(N) \rceil + 4,$$

and so that

$$\text{fl}^a(f_i(x)/\|f\|_w) = f_i(x)/\|f\|_w + \|f_i\|_w/\|f\|_w \lceil D + 4\lceil \log(N) \rceil + 15 \rceil.$$

Combining these relations, we get

$$\|\text{fl}^a(f(x)/\|f\|_W) - f(x)/\|f\|_W\| \leq [\mathbb{D} + 4\lceil \log(N) \rceil + 15],$$

as desired. \square

Proposition 4^{S3}16. *There is a round-off algorithm computing $\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W$ such that*

$$\|\text{fl}^a(\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W) - \Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W\| \leq [\mathbb{D} + 4\lceil \log(N) \rceil + 20].$$

The algorithm has run-time bounded by $O(nN)$.

Sketch of proof. The proof is analogous to the previous one for computing $\Delta_{\mathbf{d}}^{-1}\bar{D}_x f$. The extra constant comes from the multiplication with the orthogonal projection. \square

Error analysis of Algorithm SPHERICALHOMOLOGY

We note that in Algorithm SPHERICALHOMOLOGY, the numerical errors can only occur at three points: 1) Call to the Algorithm $\bar{\kappa}$ -ESTIMATE, 2) Construction of the clouds of points $X_{i,j}^\infty$, and 3) Construction of the Vietoris-Rips graphs. The remaining operations are symbolic and, hence, don't have numerical errors. The main result we will obtain is the following theorem.

Theorem 4^{S3}17. *There is a round-off version of Algorithm SPHERICALHOMOLOGY with the same asymptotic complexity as Algorithm SPHERICALHOMOLOGY which is guaranteed to work correctly when the round-off error unit satisfies*

$$u \leq \frac{1}{O(qnD\bar{\kappa}(f))}.$$

The above theorem will follow from performing an error analysis on the parts of Algorithm SPHERICALHOMOLOGY mentioned above.

Computation of $\bar{\kappa}(f, x)$ and $\bar{\kappa}(f)$ The main issue with Algorithm $\bar{\kappa}$ -ESTIMATE is the computation of $\kappa(f^L, x)$ for $f \in \mathcal{H}_{\mathbf{d}}[q]$, $x \in \mathbb{S}^n$ and $L \in [q]^{\leq n+1}$. This will be the main result here.

Lemma 4^{S3}18. *There is a round-off algorithm computing $\kappa(f, x)$ for $f \in \mathcal{H}_{\mathbf{d}}[q]$ and $x \in \mathbb{S}^n$ such that*

$$\text{fl}^a(\kappa(f, x)) = \kappa(f, x)(1 + [\mathbb{O}(n^2(D + \log(N)))]).$$

The algorithm takes $O(n^3 + nN)$ operations.

Proof. Using Propositions 4^{S3}15 and 4^{S3}16, we can evaluate $f(x)/\|f\|_W$ and $\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W$. We use now a backward stable version of the QR algorithm, as described in [221; Ch. 19], for which we have then

$$\text{fl}^a(\sigma_q(\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W)) = \sigma_q(\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W)(1 + [\mathbb{O}(n^2(D + \log(N)))])$$

since $\|\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W\| \leq 1$, by Corollary 1^{S1}7.

We finish computing the norm of $(\text{fl}^a(f(x)/\|f\|_W), \text{fl}^a(\sigma_q(\Delta_{\mathbf{d}}^{-1}D_x f / \|f\|_W)))$ and inverting it. \square

Theorem 4§3 19. *There is a round-off version of Algorithm $\bar{\kappa}$ -ESTIMATE with the same asymptotic complexity as Algorithm $\bar{\kappa}$ -ESTIMATE which is guaranteed to work correctly when the round-off unit satisfies*

$$\mathbf{u} \leq \frac{1}{O(n^2(D + \log(N)))}.$$

Proof. We only need to strengthen the inequality $2DK < 1$ in Algorithm $\bar{\kappa}$ -ESTIMATE to $3DK < 1$. Now, by Lemma 4§3 18,

$$\text{fl}^a(\bar{\kappa}(f, x)) = \bar{\kappa}(f, x)(1 + \lceil O(n^2(D + \log(N))) \rceil).$$

Taking u as chosen with a sufficiently large constant guarantees that

$$\text{fl}^a(\bar{\kappa}(f, x)) = \bar{\kappa}(f, x)(1 \pm 0.01)$$

and so the correctness of the upper bound K . \square

Construction of the cloud of points We will now assume that we are working in base 2 for the sake of simplicity. To avoid numerical errors, we will substitute certain choices in Algorithm SPHERICALHOMOLOGY by choices that can be represented exactly. So we have the following new choices:

$$\begin{aligned} \theta &\leftarrow 2^{-\lceil \log(9(n+2)DK) \rceil} \\ \tilde{\gamma} &\leftarrow \lceil \log(9(n+2)DK) + \lceil \log(30D^{\frac{1}{2}}) \rceil + \lceil \log(\sqrt{2}K) \rceil + \lceil \log D^{\frac{1}{2}} \rceil + 8 \rceil \end{aligned}$$

With these choices, we have that all the \mathbf{x}_i have an exact representation in the floating-point system.

Now, instead of checking

$$f_i(x)/\|f_i\| \geq \mathbf{x}_j - D^{\frac{1}{2}}2^{-\tilde{\gamma}} \text{ and } f_i(x)/\|f_i\| \leq \mathbf{x}_j + D^{\frac{1}{2}}2^{-\tilde{\gamma}},$$

we will check

$$\text{fl}^a(f_i(x)/\|f_i\|) \geq \mathbf{x}_j - 2^{-\tilde{\gamma}_0} \text{ and } \text{fl}^a(f_i(x)/\|f_i\|) \leq \mathbf{x}_j + 2^{-\tilde{\gamma}_0},$$

where $\tilde{\gamma}_0 = \lceil \log(9(n+2)DK) \rceil + \lceil \log(30D^{\frac{1}{2}}) \rceil + \lceil \log(\sqrt{2}K) \rceil + 7$. The sum/difference on the right-hand side has an exact floating-point representation as long as

$$u \leq \frac{1}{O(nD\bar{\kappa}(f))}$$

since $\mathbf{x}_i = \pm k_i 2^{-\lceil \log(9(n+2)DK) \rceil}$ for some non-negative integer k_i of size $O(n)$. With these substitutions, we obtain sets $\text{fl}^a(\mathcal{X}_{i,j}^\infty)$, and for Ψ a lax formula over (f, \mathbf{x}) , sets $\text{fl}^a(\mathcal{X}(\Psi))$ constructed from the $\text{fl}^a(\mathcal{X}_{i,j}^\infty)$ using the formula Φ .

We now prove a floating-point version of the sampling theorem (Theorem 4§1 1), taking advantage of the fact that the inequalities in it were asymmetric.

Proposition 4§3 20 (Floating sampling). *Assume that $\lceil D + 4\lceil \log N \rceil + 15 \rceil < 2^{-\tilde{\gamma}_0-1}$. In the above setting,*

$$\text{dist}_H(\text{fl}^a(\mathcal{X}(\Psi)), \mathcal{S}(f, \mathbf{x}, \Psi)) < 2^{-\lceil \log(9(n+2)DK) \rceil - \lceil \log(30D^{\frac{1}{2}}) \rceil - 6}.$$

Proof. The proof is as that of the sampling theorem , so we reduce to the purely conjunctive case without loss of generality. If $x \in X_{i,j}^{\leq}$, then

$$f_i(x)/\|f_i\| \leq \kappa_j + \left(2^{-\tilde{y}_0} + [\![D + 4\lceil \log N \rceil + 15]\!] f_i(x)/\|f_i\|\right),$$

by Proposition 4^{S3}15. By Corollary 1^{S1}7, $|f_i(x)/\|f_i\|| < 1$, and so, by our assumption,

$$f_i(x)/\|f_i\| \leq \kappa_j - 2^{1-\tilde{y}_0}.$$

Analogously, if $x \in X_{i,j}^{\geq}$,

$$f_i(x)/\|f_i\| \geq \kappa_j - 2^{1-\tilde{y}_0}$$

By Proposition 2^{S1}3, this implies that

$$\text{fl}^a(X(\Psi)) \subseteq \mathcal{U}\left(S(f, \kappa, \Psi), \sqrt{2} \bar{\kappa}(f) 2^{1-\tilde{y}_0}\right) \subseteq \mathcal{U}\left(S(f, \kappa, \Psi), 2^{-[\log(9(n+2)DK)] - [\log(30D^{\frac{1}{2}})] - 6}\right)$$

Now, for all $x \in S(f, \kappa, \Phi)$, there is some $g_x \in G_{\mathbb{N}}$ such that $\text{dist}_{\mathbb{S}}(x, g_x) < 2^{-\tilde{y}}$. Therefore, by Proposition 2^{S1}3, $g_x \in S_{D^{\frac{1}{2}} 2^{-\tilde{y}}}(f, \kappa, \Psi)$. Now, arguing as above, this means that

$$g_x \in \text{fl}^a(X(\Psi))$$

since the absolute error for evaluating $\text{fl}^a(f_i(g_x))/\|f_i\|_w$ is at most $2^{-\tilde{y}_0-1}$, as proven above, and $D^{\frac{1}{2}} 2^{-\tilde{y}} \leq 2^{-\tilde{y}_0-1}$. Hence

$$S(f, \kappa, \Psi) \subseteq \mathcal{U}_S(\text{fl}^a(X(\Psi)), 2^{-\tilde{y}}) \subseteq \mathcal{U}\left(\text{fl}^a(X(\Psi)), 2^{-[\log(9(n+2)DK)] - [\log(30D^{\frac{1}{2}})] - 6}\right),$$

as desired. \square

Construction of the Vietoris-Rips graphs

We have constructed the clouds of points. We next construct the Vietoris-Rips graphs of these clouds. We will assume that we work with the uniform grid for simplicity. For a general grid, one has to add a long argument about the floating-point approximation of the points in the grid.

For this, let us note, that by the Vietoris-Rips homology witness theorem (Theorem 4^{S1}3) it is enough to choice $\varepsilon > 0$ such that

$$2^{-[\log(9(n+2)DK)] - [\log(30D^{\frac{1}{2}})] - 3} < \varepsilon < 2^{-[\log(9(n+2)DK)] - [\log(30D^{\frac{1}{2}})]}. \quad (4.34)$$

Therefore we make the choice

$$\varepsilon \leftarrow 2^{-[\log(9(n+2)DK)] - [\log(30D^{\frac{1}{2}})] - 1}$$

The points in $\text{fl}^a(X_{i,j}^{\infty})$ are not in floating-point form. However, they are points of the form $\tilde{x}/\|\tilde{x}\|$ with $\tilde{x} \in 2^{1-\tilde{y}-[\frac{1}{2}\log n]} \mathbb{Z}^{n+1} \subseteq F^{n+1}$. Moreover, all the points can be expressed in floating-point form with the same exponent. Because of this, we can translate

$$\left\| \frac{\tilde{x}}{\|\tilde{x}\|} - \frac{\tilde{y}}{\|\tilde{y}\|} \right\| \leq 2\varepsilon$$

into the condition

$$\|\tilde{x}\|^2 \|\tilde{y}\|^2 (1 - 2\epsilon^2)^2 \leq \langle \tilde{x}, \tilde{y} \rangle \text{ and } \langle \tilde{x}, \tilde{y} \rangle > 0.$$

The latter can be checked exactly as long as

$$\mathbf{u} < \frac{1}{O(nD\bar{\kappa}(f))}.$$

This shows that the Vietoris-Rips complex can be constructed under the finite-precision assumption.

Error analysis of Algorithm AFFINEHOMOLOGY

Since Algorithm **AFFINEHOMOLOGY** applies Algorithm 4 after homogenization. The latter needs the computation of $\|f\|_W$, but this can be done with the help of Corollary 4§3 14. Because of this, we get the following theorem.

Theorem 4§3 21. *There is a round-off version of Algorithm **AFFINEHOMOLOGY** with the same asymptotic complexity as Algorithm **AFFINEHOMOLOGY** which is guaranteed to work correctly when the round-off unit satisfies*

$$u \leq \frac{1}{O(qnD\bar{\kappa}_{\text{aff}}(f))}.$$

Using the probabilistic results of Chapter 1, in particular, Corollary 1§4 6, we obtain the following easy corollary.

Corollary 4§3 22. *Let $\mathfrak{f} \in \mathcal{P}_d[q]$ be a KSS random polynomial tuple. The expected precision of the round-off version of Algorithm **AFFINEHOMOLOGY** on input (\mathfrak{f}, Φ) is at most*

$$\log(N) + n \log(qD).$$

□

Similar results can be obtained for the smoothed version using also Corollary 1§4 6. This shows that on average the precision needed by Algorithm **AFFINEHOMOLOGY** to compute homology is linear in the number of variables and logarithmic in the remainder of the parameters.

Remark 4§3 8. We could use Corollary 1§4 5 to obtain a run-time bound for integer polynomial tuples. We only note that for these, we can bound the precision needed to be linear in the bit-size of the coefficients and $\log(N)$, polynomial in D and exponential in n . ▀

Further comments

Most of the content in this chapter can be found in [92]. However, there are some exceptions: the Vietoris-Rips homology witness theorem (Theorem 4§1 3), the random and recursive grids, which were adapted, respectively, from [300] and [214, 213], and the detailed parallelization and stability analyses.

Regarding the parallelization, it is clear that the claims in [88, 91, 92] regarding the existence of parallel polynomial-time algorithm for computing the SNF of an integer matrix are false. However, the parallelization can be obtained for the Betti numbers.

Regarding the stability of the algorithm, we observe that there are certain issues not appearing in [139] that come from the change in how we construct the approximating clouds of points and the need to not miss any edge in the Vietoris-Rips graph. However, one can manage the analysis by the use of similar techniques to those in [139]. Nevertheless, one should note that the avoidance of the use of Smale's α -theory provides an improvement in the amount of needed precision.

Statt des törichten Ignorabimus heisse im Gegenteil unsere Lösung:

*Wir müssen wissen,
Wir werden wissen.*

David Hilbert, Naturerkennen und Logik (8. September 1930)

5

A look into the future

As a human activity, mathematics is something that is done. No matter how much understanding one collects, there will be open questions that one is unable to answer. The health of a mathematical area is, therefore, judged by the vitality of its ongoing research and not by its achievements alone. When a mathematical area runs out of impetus, it can die. In the best cases, the area dies of success—the old achievements tear apart the area into many new directions that cannot be anymore under the same roof. In the worst cases, the progress seems impossible—the absence of new ideas makes the area sterile and hard to inhabit.

The objective of this chapter is to show that the study of grid methods in numerical real algebraic geometry is in good health. We do this by showing results that point out to the fact that there are still major developments to come. We accompany this exposition by a research program, which we call *пятилетка*, that points out to many future possible lines of research that the author intends to work in.

First, we show that is possible to obtain probability tail bounds for the condition number of random polynomials that do not follow the KSS random model; second, we show that there can be algorithms in numerical real algebraic geometry for which the expected run-time is finite; third, expanding on the latter point, by showing that one can estimate the condition number in average exponential time and in average parallel polynomial time (with average exponential number of processors); fourth and last, we give the *пятилетка* program pointing to the possibility of a numerical algorithm for computing the homology of semialgebraic sets in average singly exponential time and studying the classification of real algebraic and semialgebraic sets from a computational approach.

5§1 Beyond normal distributions: robust tail bounds

We will show bounds for the condition number of random hypersurfaces. These bounds are based in the techniques developed by Ergür, Rojas and Paouris [175, 176], but they were

given in the form presented here mainly by Cucker, Ergür and the author [136]. We now fulfill the promise that we made in the probabilistic analysis via geometric functional analysis of Section 1§2.

First, we introduce the random model we will be working with, dobro random polynomials, and discuss some of their properties; second, we give the tail bounds for the local and global condition number; and third, we discuss the optimality of the bound for the local condition number by computing tight estimates in the Gaussian case.

5§1–1 Dobro random polynomials

The main range of random variables that we will deal with are random variables that behave like Gaussian random variables.

Definition 5§1.1. Let $\mathfrak{x} \in \mathbb{R}$ be a random variable. Then we say that:

(P1) \mathfrak{x} is *centered* if $\mathbb{E}\mathfrak{x} = 0$.

(P2) \mathfrak{x} is called *subgaussian* if there exist a K such that for all $I \geq 1$,

$$\left(\mathbb{E}|\mathfrak{x}|^I \right)^{\frac{1}{I}} \leq K\sqrt{I}.$$

The smallest such K is called the Ψ_2 -norm of \mathfrak{x} .

(P3) \mathfrak{x} satisfies the *anti-concentration property with constant ρ* if, for all $\varepsilon > 0$,

$$\max \{ \mathbb{P} (|\mathfrak{x} - u| \leq \varepsilon) \mid u \in \mathbb{R} \} \leq \rho\varepsilon.$$

Remark 5§1.1. The subgaussian property (P2) has many equivalent definitions. We refer the interested reader to [399; §2.5]. ¶

These properties generalize properties that a Gaussian variable has.

Proposition 5§1.1. Let $\mathfrak{x} \in \mathbb{R}$ be a random variable. If $\mathfrak{x} \sim N(0, \sigma)$, then \mathfrak{x} is a centered, subgaussian random variable that satisfies the anti-concentration inequality with Ψ_2 -norm σ and concentration constant $\frac{1}{\sqrt{2\pi}\sigma}$. □

The above motivates the following definition, which gives the class of polynomials that our probabilistic analysis will apply to.

Definition 5§1.2. [136; Definition 3.1]. A *dobro random polynomial* $\mathfrak{f} \in \mathcal{H}_d$ with parameters K and ρ is a random polynomial

$$\mathfrak{f} := \sum_{|\alpha|=d} \binom{d}{\alpha}^{\frac{1}{2}} c_\alpha X^\alpha \tag{5.1}$$

such that the c_α are independent centered subgaussian random variables with Ψ_2 -norm $\leq K$ and anti-concentration property with constant ρ . A *dobro random polynomial* $\mathfrak{f} \in \mathcal{P}_d$ is a polynomial f such that its homogenization \mathfrak{f}^h is so.

Remark 5§1.2. The term ‘dobro’ (‘добрo’) is a Russian word which means good. ¶

One important feature of this class is that it allows many random polynomials, including the KSS random polynomials.

Example 5^{§1}1 (KSS random polynomials). Any KSS random polynomial is a dobro random polynomial with parameters $K = 1$ and $\rho = 1/\sqrt{2\pi}$ since each c_α in (5 . 1) is Gaussian with unit standard deviation. Δ

Example 5^{§1}2 (Weyl random polynomial). [136]. A *Weyl random polynomial* is a random polynomial f such the c_α in (5 . 1) are i.i.d. random variables with uniform distribution in $[-1, 1]$. Every Weyl random polynomial is a dobro random polynomial with parameters $K = 1$ and $\rho = 1/2$.

We observe that this probabilistic model can be seen as the limit of the sequence of random polynomials $(f^{(b)})$ where the $c_\alpha^{(b)}$ are independent random variables uniformly distributed in $[-2^b, 2^b]$. This last model is discrete and it would be interesting to extend the techniques to such random models. Δ

Example 5^{§1}3 (ℓ -exponential random polynomial). [136]. An ℓ -exponential random polynomial is a random polynomial f such the c_α in (5 . 1) are i.i.d. random variables with density function given by

$$z \mapsto \begin{cases} \Gamma(1 + \frac{1}{\ell})^{-1} e^{-t^\ell}, & \text{if } t \geq 0 \\ 0, & \text{otherwise.} \end{cases}$$

For $\ell \geq 2$, an ℓ -exponential random polynomial is a dobro random polynomial with parameter $K = 1$ and $\rho = 6/5$. Δ

Dobro random polynomials form a robust class under a wider class of transformations.

Proposition 5^{§1}2. Let $f = \sum_{|\alpha|=d} f_\alpha X^\alpha \in \mathcal{H}_d$ be a dobro random polynomial with parameters K and ρ . Then:

- (1) For all $\lambda \in \mathbb{R} \setminus 0$, λf is a dobro random polynomial with parameters λK and $\lambda^{-1} \rho$.
- (2) Let $(\lambda_\alpha)_{|\alpha|=d}$ be a sequence of non-zero real numbers. Then

$$\sum_{|\alpha|=d} \lambda_\alpha f_\alpha X^\alpha$$

is a dobro random polynomial with parameters $(\max |\lambda_\alpha|) K$ and $(\min |\lambda_\alpha|)^{-1} \rho$.

Proof. The effect on K follows from the fact that the expectation is linear. The effect on ρ follows from the fact that for all $\lambda \neq 0$,

$$\max \{ \mathbb{P} (|\lambda x - u| \leq \varepsilon) \mid u \in \mathbb{R} \} = \max \{ \mathbb{P} (|x - u| \leq \lambda^{-1} \varepsilon) \mid u \in \mathbb{R} \}. \quad \square$$

Remark 5^{§1}3. The parameter our analysis will depend on is the product $K\rho$. Note that this parameter is invariant under scaling and does not vary much if we scale the coefficients of the dobro random polynomial in a way that the coefficients are not far from a uniform scaling. The latter shows a certain robustness of the parameter.

For this parameter, it is easy to see that we have $K\rho \geq \frac{1}{4}$ [175; (1)]. \P

5^{§1}-2 Tail bounds for the condition of a dobro random polynomial

The main theorem here looks very similar to Theorem 1^{§2}17, both in its statement and in its proof. The main difference is that now we are dealing with just one polynomial and that this polynomial is more generally a dobro random polynomial and not just a KSS random polynomial.

Theorem 5^{§1}3. [136; Theorem 7.1 and 7.10].

(A) Let $\mathfrak{f} \in \mathcal{H}_d[1]$ be a dobro random polynomial with parameters K and ρ , and $x \in \mathbb{S}^n$.

Then for $t \geq e$,

$$\mathbb{P}(\kappa(\mathfrak{f}, x) \geq t) \leq 2(30K\rho)^{n+1} \left(\frac{N}{n+1} \right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1}.$$

(S) Let $f \in \mathcal{H}_d[1]$, $\sigma > 0$, $\mathfrak{f}_\sigma := f + \sigma \|f\|_{\mathcal{W}} \mathfrak{f}$ be a random polynomial such that $\mathfrak{f} \in \mathcal{H}_d[1]$ is a dobro random polynomial with parameters K and ρ , and $x \in \mathbb{S}^n$. Then for $t \geq e$,

$$\mathbb{P}(\kappa(\mathfrak{f}_\sigma, x) \geq t) \leq 2(30K\rho)^{n+1} \left(\frac{N}{n+1} \right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t} \right)^{n+1} \left(1 + \frac{1}{\sigma} \right)^{n+1}.$$

The proof of Theorem 5^{§1}3 relies on two basic results from geometric functional analysis. The first one controls the tail bound of the norm, just as Proposition 1^{§1}11 did, and the second one the concentration of a projection, just as Proposition 1^{§2}18 did.

Theorem 5^{§1}4. Let $\mathfrak{x} \in \mathbb{R}^N$ be a random vector whose components \mathfrak{x}_i are independent centered sub-Gaussian random variables with ψ_2 -norm $\leq K$. Then for all $t \geq 5K\sqrt{N}$,

$$\mathbb{P}(\|\mathfrak{x}\| \geq t) \leq e^{-\frac{t^2}{(5K)^2}}. \quad (5.2)$$

Proof of Theorem 5^{§1}4. Note that $\|\mathfrak{x}\| \geq t$ is equivalent to $e^{s^2 \|\mathfrak{x}\|^2} \geq e^{s^2 t^2}$. Therefore, by Markov's inequality [164],

$$\mathbb{P}(\|\mathfrak{x}\| \geq t) \leq e^{-s^2 t^2} \mathbb{E} e^{s^2 \|\mathfrak{x}\|^2}.$$

Now, by independence,

$$\mathbb{E} e^{s^2 \|\mathfrak{x}\|^2} = \prod_{i=1}^N \mathbb{E} e^{s^2 \mathfrak{x}_i^2}.$$

For each i ,

$$\mathbb{E} e^{s^2 \mathfrak{x}_i^2} = \sum_{l=0}^{\infty} \frac{s^{2l} \mathbb{E} \mathfrak{x}_i^{2l}}{l!} \leq \sum_{l=1}^{\infty} \frac{s^{2l} K^{2l} (2l)!}{l!} \leq \sum_{l=0}^{\infty} (2eK^2 s^l)^l$$

where the first inequality follows from the definition of subgaussian and the second one from Stirling's approximation $l! \geq (l/e)^l$.

Let $s^2 = 1/(4eK^2)$. Then, substituting above, we get

$$\mathbb{P}(\|\mathfrak{x}\| \geq t) = 2^N e^{-t^2/(4eK^2)}.$$

Now, we can see that for $t \geq \sqrt{8e \ln(2)}K\sqrt{N}$, we have

$$\mathbb{P}(\|\mathfrak{x}\| \geq t) = e^{-t^2/(8eK^2)}.$$

Hence the proposition holds for the constant in the statement. \square

Definition 5^{§1}3. The *concentration function* of a random vector $\mathfrak{x} \in \mathbb{R}^k$ is the function

$$\mathcal{L}_{\mathfrak{x}}(\varepsilon) := \max_{u \in \mathbb{R}^k} \mathbb{P}(\|\mathfrak{x} - u\| \leq \varepsilon). \quad (5.3)$$

Theorem 5^{§1}5 (Rudelson-Vershynin concentration theorem). [351; Corollary 1.4] and [280; Theorem 1.1]. Let $\mathfrak{x} \in \mathbb{R}^N$ be a random vector whose components \mathfrak{x}_i are independent random variables with the anti-concentration property with constant $\leq \rho$. Then for all $k \in [n]$, all orthogonal projections $P : \mathbb{R}^N \rightarrow \mathbb{R}^k$ and every $\varepsilon > 0$,

$$\mathcal{L}_{P\mathfrak{x}}(\varepsilon) \leq \left(\frac{6\rho\varepsilon}{\sqrt{k}}\right)^k.$$

Proof. The constant comes from [280]. There the authors showed that it is enough to take $2\sqrt{\pi e}$. We bounded this number by the nearest integer. \square

Remark 5^{§1}4. The above explicit values for the constants were missing in the statements in [136]. We give explicit constants, so that one can get explicit probability estimates. In order to find the explicit values, we rework the usual arguments in [399] for Theorem 5^{§1}4 and we used the constant in [280] for Theorem 5^{§1}5. ¶

Proof of Theorem 5^{§1}3. (A) Note that in the case of a single polynomial, we have that $\kappa(\mathfrak{f}, x) = \|\mathfrak{f}\|_W / \|\mathfrak{R}_x \mathfrak{f}\|$, where \mathfrak{R}_x is the orthogonal projection of Proposition 1^{§1}6 and $\|\mathfrak{R}_x \mathfrak{f}\|$ the Euclidean norm of $\mathfrak{R}_x \mathfrak{f} \in \mathbb{R}^{n+1}$. Therefore for all $t > 0$ and $u \geq 5K\sqrt{N}$,

$$\begin{aligned} \mathbb{P}(\kappa(\mathfrak{f}, x) \geq t) &= \mathbb{P}(\|\mathfrak{f}\|_W / \|\mathfrak{R}_x(\mathfrak{f})\| \geq t) \\ &\leq \mathbb{P}(\|\mathfrak{f}\|_W \geq u \text{ or } \|\mathfrak{R}_x(\mathfrak{f})\| \leq u/t) \quad (\text{Implication bound}) \\ &\leq \mathbb{P}(\|\mathfrak{f}\|_W \geq u) + \mathbb{P}(\|\mathfrak{R}_x(\mathfrak{f})\| \leq u/t) \quad (\text{Union bound}) \\ &\leq e^{-\frac{u^2}{(5K)^2}} + \mathbb{P}(\|\mathfrak{R}_x(\mathfrak{f})\| \leq u/t) \quad (\text{Theorem 5^{§1}4}) \\ &\leq e^{-\frac{u^2}{(5K)^2}} + \left(\frac{6\rho u}{\sqrt{n+1} t}\right)^{n+1} \quad (\text{Theorem 5^{§1}5}). \end{aligned}$$

Substituting $5K\sqrt{N \ln t} \geq 5K\sqrt{N}$ in the place of u , we obtain

$$\mathbb{P}(\kappa(\mathfrak{f}, x) \geq t) \leq t^{-N} + (30K\rho)^{n+1} \left(\frac{N}{n+1}\right)^{\frac{n+1}{2}} \left(\frac{\ln^{\frac{1}{2}} t}{t}\right)^{n+1}.$$

The bound $t^{-N} \leq t^{-(n+1)}$ finishes the proof.

(S) The smoothed case follows a similar pattern. We only need to substitute Theorems 5^{§1}4 and 5^{§1}5 by versions for \mathfrak{f}_σ . These are easy to obtain. By the triangle inequality and Theorem 5^{§1}4, we have that

$$\mathbb{P}(\|\mathfrak{f}_\sigma\|_W \geq t\|\mathfrak{f}\|_W) \leq \mathbb{P}(\|\mathfrak{f}\|_W \geq (t-1)\sigma^{-1}) \leq e^{-\frac{(t-1)^2}{(50K)^2}}$$

for $t \geq 1 + 5K\sigma\sqrt{N}$. Theorem 5^{§1}5 applies directly to \mathfrak{f}_σ .

The rest of the proof is as above, but substituting u by $1 + 5\sigma K\sqrt{N \ln t} \leq (1\sigma)5\sigma K\sqrt{N \ln t}$ now. \square

Once we have the bound for the local condition number, we can give the bound for the global one as we did in Theorem 1^{§2}19.

Theorem 5^{§1}6. (A) Let $\mathfrak{f} \in \mathcal{H}_d[1]$ be a dobro random polynomial with parameters K and ρ . Then for $t \geq e$,

$$\mathbb{P}(\kappa(\mathfrak{f}) \geq t) \leq 12(180K\rho)^{n+1} \left(\frac{N}{n+1}\right)^{\frac{n+1}{2}} D^n \frac{\ln^{\frac{n+1}{2}} t}{t}.$$

(S) Let $f \in \mathcal{H}_d[1]$, $\sigma > 0$, $\mathfrak{f}_\sigma := f + \sigma \|f\|_{W^1} g$ be a random polynomial such that $g \in \mathcal{H}_d[1]$ is a dobro random polynomial with parameters K and ρ . Then for $t \geq e$,

$$\mathbb{P}(\kappa(\mathfrak{f}_\sigma) \geq t) \leq 12(180K\rho)^{n+1} \left(\frac{N}{n+1}\right)^{\frac{n+1}{2}} D^n \frac{\ln^{\frac{n+1}{2}} t}{t} \left(1 + \frac{1}{\sigma}\right)^{n+1}.$$

Proof. We let \mathcal{G} be $N_{1/(Dt)}$ of Lemma 1^{§2}20. Following the proof of Theorem 1^{§2}19, we conclude that

$$\mathbb{P}(\kappa(\mathfrak{f}) \geq t) \leq \#\mathcal{G} \max_{x \in \mathcal{G}} \mathbb{P}(\kappa(\mathfrak{f}, x) \geq t/2).$$

Now, we just use that $\#\mathcal{G} \leq (2Dt)^n$ by Lemma 1^{§2}20 and the bound from Theorem 5^{§1}3. \square

5^{§1}-3 Tail bounds for the local condition of a KSS random polynomial

Note that we can write the local condition number of a single polynomial $f \in \mathcal{H}_d[1]$ as

$$\kappa(f, x) = \sqrt{1 + \frac{\|Q_x(f)\|^2}{\|\mathfrak{R}_x(f)\|^2}}$$

where \mathfrak{R}_x is the orthogonal projection from Proposition 1^{§1}6 and $Q_x : \mathcal{H}_d[1] \rightarrow \mathbb{R}^{N-n-1}$ is the orthogonal projection complementary to \mathfrak{R}_x . This implies the following proposition.

Proposition 5^{§1}7. Let $\mathfrak{f} \in \mathcal{H}_d[1]$ be a KSS random polynomial and $x \in \mathbb{S}^n$. Then $\kappa(\mathfrak{f}, x)$ has the same probability distribution as

$$\sqrt{1 + \left(\frac{N}{n+1} - 1\right)^{-1} \mathfrak{F}}$$

where $\mathfrak{F} \in [0, \infty)$ is a random variable with the Fisher–Snedecor distribution with $N - n - 1$ and $n + 1$ degrees of freedom. \square

Recall that the Fisher–Snedecor distribution $F_{k,l}$ with k and l degrees of freedom appears when we take random variables of the form $\frac{x}{\sqrt{k}}$ with x and y independent random

variables with a χ^2 -distribution with, respectively, k and l degrees of freedom. It is known that its density function is given by

$$\frac{\Gamma\left(\frac{k+l}{2}\right)}{\Gamma\left(\frac{k}{2}\right)\Gamma\left(\frac{l}{2}\right)} \left(\frac{k}{l}\right)^{\frac{k}{2}} t^{\frac{k}{2}-1} \left(1 + \frac{k}{l}t\right)^{-\frac{k+l}{2}}$$

for $t > 0$. We can give now an explicit formula for the density of the local condition number of a KSS random polynomial.

Theorem 5^{§1}8. *Let $f \in \mathcal{H}_d$ be a KSS random polynomial of degree $d > 1$ and $x \in \mathbb{S}^n$. Then the density function of $\kappa(f, x)$, $\delta_{\kappa(f,x)}(t)$, is given by*

$$\begin{aligned} \frac{2\Gamma\left(\frac{N}{2}\right)}{\Gamma\left(\frac{N-n-1}{2}\right)\Gamma\left(\frac{n+1}{2}\right)} \left(\frac{N-n-1}{n+1}\right)^{N-n-1} \\ \left(1 - \frac{1}{t^2}\right)^{\frac{N-n-1}{2}-1} \left(1 + \left(\frac{N-n-1}{n+1}\right)^2 \left(1 - \frac{1}{t^2}\right)\right)^{-\frac{N}{2}} t^{-n-2} \end{aligned}$$

for $t \geq 1$.

Remark 5^{§1}5. The assumption on the degree is equivalent to $N > n + 1$. Note that if this does not hold, i.e., $N = n + 1$, the condition number is always one. ¶

Proof. We just apply the change of variables theorem from integration to the density function of the Fischer-Snedecor distribution. □

We do some estimation of this formula, so that it can be digested in an easier way.

Corollary 5^{§1}9. *Let $f \in \mathcal{H}_d$ be a KSS random polynomial of degree $d > 1$ and $x \in \mathbb{S}^n$. Then for all $t \geq \sqrt{2}$,*

$$\begin{aligned} \frac{1}{e^{12}\sqrt{\pi(n+1)}} \left(\frac{N}{n+1}\right)^{\frac{n+1}{2}} \left(\frac{n+1}{N-n+1}\right)^{n+1} t^{-(n+2)} \\ \leq \delta_{\kappa(f,x)}(t) \leq \\ \frac{12}{5\sqrt{\pi}} \frac{1}{\sqrt{n+1}} \left(\frac{2eN}{n+1}\right)^{\frac{n+1}{2}} \left(\frac{n+1}{N-n+1}\right)^{n+1} t^{-(n+2)}. \end{aligned}$$

Proof. First, using Stirling's approximation (1.21), we have that

$$\frac{1}{\sqrt{\pi}} \frac{N^{\frac{N-1}{2}}}{(N-n-1)^{\frac{N-n-2}{2}} (n+1)^{\frac{n}{2}}} \leq \frac{\Gamma\left(\frac{N}{2}\right)}{\Gamma\left(\frac{N-n-1}{2}\right)\Gamma\left(\frac{n+1}{2}\right)} \leq \frac{6}{5\sqrt{\pi}} \frac{N^{\frac{N-1}{2}}}{(N-n-1)^{\frac{N-n-2}{2}} (n+1)^{\frac{n}{2}}}.$$

Second, we have the equality

$$\begin{aligned} \left(1 - \frac{1}{t^2}\right)^{\frac{N-n-1}{2}-1} \left(1 + \left(\frac{N-n-1}{n+1}\right)^2 \left(1 - \frac{1}{t^2}\right)\right)^{-\frac{N}{2}} \\ = \left(\frac{N-n-1}{n+1}\right)^{-N} \left(1 - \frac{1}{t^2}\right)^{-\frac{n+3}{2}} \left(1 + \frac{1}{\left(1 - \frac{1}{t^2}\right) \left(\frac{N-n-1}{n+1}\right)^2}\right)^{-\frac{N}{2}}. \end{aligned}$$

Third, for $t \geq \sqrt{2}$, we have that

$$1 \leq \left(1 - \frac{1}{t^2}\right)^{-\frac{n+3}{2}} \leq 2^{\frac{n+3}{2}}$$

and

$$\begin{aligned} 1 &\leq \left(1 + \frac{1}{\left(1 - \frac{1}{t^2}\right) \left(\frac{N-n-1}{n+1}\right)^2}\right)^{\frac{N}{2}} \\ &\leq \left(1 + \frac{1}{\frac{1}{2} \left(\frac{N-n-1}{n+1}\right)^2}\right)^{\frac{N}{2}} \leq \left(e^{2\left(\frac{n+1}{N-n-1}\right)^2}\right)^{-\frac{N}{2}} = e^{\frac{N(n+1)^2}{(N-n-1)^2}} \leq e^{12}, \end{aligned}$$

where the last inequality follows from $N/(N-n-1) = 1 + (n+1)/(N-n-1) \leq 3$ and $(n+1)/(N-n-1) \leq 2/n$, since $N \geq \binom{n+2}{2}$ under our assumptions.

To obtain the inequalities in the statement, apply the above three estimates together with

$$1 \leq \left(\frac{N}{N-n-1}\right)^{\frac{N-n-2}{2}} = \left(1 + \frac{1}{\frac{N-n-1}{n+1}}\right)^{\frac{N-n-2}{2}} \leq e^{\frac{N-n-2}{N-n-1} \frac{n+1}{2}} \leq e^{\frac{n+1}{2}}.$$

This finishes the proof. \square

The above translates immediately into the following estimates of the tail bound.

Corollary 5^{§1}10. Let $\mathfrak{f} \in \mathcal{H}_d$ be a KSS random polynomial of degree $d > 1$ and $x \in \mathbb{S}^n$. Then for all $t \geq \sqrt{2}$,

$$\begin{aligned} &\frac{1}{e^{12}\sqrt{\pi}(n+1)^{\frac{3}{2}}} \left(\frac{N}{n+1}\right)^{\frac{n+1}{2}} \left(\frac{n+1}{N-n+1}\right)^{n+1} t^{-(n+1)} \\ &\leq \mathbb{P}(\kappa(\mathfrak{f}, x) \geq t) \leq \\ &\quad \frac{12}{5\sqrt{\pi}} \frac{1}{\sqrt{n+1}} \left(\frac{2eN}{n+1}\right)^{\frac{n+1}{2}} \left(\frac{n+1}{N-n+1}\right)^{n+1} t^{-(n+1)}. \end{aligned}$$

Proof. We integrate the density function on $[t, \infty)$. \square

When we compare these bounds with the bound in Theorem 5^{§1}3, we can see that the main difference between the two bounds is, on the one hand, the occurrence of $\ln^{\frac{1}{2}} t$, and, on the other hand, the above factor

$$\left(\frac{n+1}{N-n+1}\right)^{n+1}.$$

An easy estimation, using $N \geq \binom{n+2}{2}$, shows that

$$\left(\frac{n+1}{N-n+1}\right)^{n+1} \leq \left(\frac{2}{n}\right)^{n+1},$$

which means that as n goes to infinity, the upper bound goes to zero. Note that this does not happen with the bound in Theorem 5^{§1}3. This motivates the following question.

Open problem H. Can one tighten the bound in Theorem 5^{§1}3 to match the bound in Corollary 5^{§1}10? Or there are differences arising from the differences between the class of dobro random polynomials and KSS random polynomials?

5^{§2} 1st adaptive case: Plantinga-Vegter algorithm

The Plantinga-Vegter algorithm [315] is a subdivision based algorithm which computes an isotopic piece-wise linear approximation of an implicit curve in the plane or an implicit surface in 3-dimensional space. Among many other algorithms for this purpose (see [71]), the Plantinga-Vegter algorithm is interesting because it guarantees a global isotopy without guaranteeing the isotopy locally.

In this section, we give a condition-based complexity analysis of the subdivision procedure of the Plantinga-Vegter algorithm, which was proposed by Burr, Gao and Tsigaridas [98]. A consequence of this analysis is that it will give a bound for the expected complexity of the algorithm for dobro random polynomials. This analysis was given for the first time by Cucker, Ergür and the author [136]. Its importance is two-fold. On the one hand, this is the first case of an algorithm in numerical real algebraic geometry with finite expected time. On the other hand, it provided an explanation of why the Plantinga-Vegter algorithm was efficient in practice.

First, we introduce the Plantinga-Vegter algorithm (PV Algorithm from now on) and its subdivision procedure; second, we introduce the specific; and third and last, we give the complexity analysis, both condition-based and probabilistic.

5^{§2–1} The PV Algorithm

We are interested in the problem of computing an isotopic piece-wise linear approximation to a real smooth hypersurface in \mathbb{R}^n described implicitly by a map $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and a region $[-\mathbf{a}, \mathbf{a}]^n$. We will further assume that the zero set $\mathcal{Z}(f)$ intersects transversely all the boundary pieces of $[-\mathbf{a}, \mathbf{a}]^n$.

To evaluate f , we will assume that we can use interval arithmetic to compute the map and its gradient vector. For $X \subseteq \mathbb{R}^m$, let $\square[X]$ be the set of full-dimensional cubes $\prod_{i=1}^m [\mathbf{a}_i, \mathbf{b}_i]$ included in X . Recall that an *interval approximation* of a function $F : \mathbb{R}^m \rightarrow \mathbb{R}^{m'}$ is a map

$$\square[F] : \square \mathbb{R}^m \rightarrow \square \mathbb{R}^{m'} \tag{5.4}$$

such that for all $J \in \square \mathbb{R}^m$, $F(J) \subseteq \square[F](J)$. Intuitively, we should think that J gives error bounds for the midpoint $m(J)$ and $\square[F](J)$ error bounds for $F(m(J))$. See [321] for more details and [422] and [421; §4] for further discussion on how realistic the interval arithmetic model is.

Explicitly, let $h, h' : \mathbb{R}^n \rightarrow (0, \infty)$ be positive maps, we will assume that we have interval approximations $\square[hf] : \square[-\mathbf{a}, \mathbf{a}]^n \rightarrow \mathbb{R}$ and $\square[h'\nabla f] : \square[-\mathbf{a}, \mathbf{a}]^n \rightarrow \mathbb{R}^n$ of, respectively, hf , the function f scaled with h ; and the gradient of f scaled with h' , $h'\nabla f$. The PV Algorithm on $[-\mathbf{a}, \mathbf{a}]^n$ will subdivide this region into smaller and smaller n -cubes until the condition

$$C_f(J): \text{either } 0 \notin \square[hf](I) \text{ or } 0 \notin \langle \square[h'\nabla f](J), \square[h'\nabla f](J) \rangle \tag{5.5}$$

is satisfied in each of the n -cubes J of the obtained subdivision of $[-a, a]^n$, where ∇f is the gradient vector of f and $\langle \cdot, \cdot \rangle$ the Euclidean inner product. Later, we will be precise on the exact interval approximations and positive functions h, h' that we will consider in our analysis.

Let us deepen in the meaning of $C_f(J)$. The first half of $C_f(J)$ tells that f has no zeros in J . This allows us to discard boxes far away from $\mathcal{Z}(f)$. The second half tells that no pair of gradient vectors of f are orthogonal in J . This second condition is where the key point lies. On the one hand, it implies that every zero of f in J is smooth, if there is any; on the other hand, and more importantly, it implies that there is a vector v such that f is increasing along any straight path $t \mapsto p + tv$ in J .

Below, we introduce Algorithm **PVSUBDIVISION**. The subroutine **STANDARDSUBDIVISION** subdivides a n -cube J into 2^n n -cubes whose edge-length is half of that of the original cube. However, one can use other subdivisions without altering the correctness or effectiveness of the algorithm.

Algorithm 10: PVSUBDIVISION

Input : $f : \mathbb{R}^n \rightarrow \mathbb{R}$ with interval approximations $\square[hf]$ and $\square[h'\nabla f]$
 $a \in (0, \infty)$

Precondition : $\mathcal{Z}(f)$ is smooth inside $[-a, a]^n$
 $\mathcal{Z}(f)$ intersects transversely all boundary pieces of $[-a, a]^n$

```

 $\tilde{\mathcal{S}} \leftarrow \{[-a, a]^n\}$ 
 $\mathcal{S} \leftarrow \emptyset$ 
repeat
  Take  $B$  in  $\tilde{\mathcal{S}}$ 
   $\tilde{\mathcal{S}} \leftarrow \tilde{\mathcal{S}} \setminus \{B\}$ 
  if  $C_f(B)$  true then
     $\mathcal{S} \leftarrow \mathcal{S} \cup \{B\}$ 
  else
     $\tilde{\mathcal{S}} \leftarrow \tilde{\mathcal{S}} \cup \text{STANDARDSUBDIVISION}(B)$ 
until  $\tilde{\mathcal{S}} = \emptyset$ 
return  $\mathcal{S}$ 

```

Output : Subdivision $\mathcal{S} \subseteq \square[-a, a]^n$ of $[-a, a]^n$

Postcondition: For all $B \in \mathcal{S}$, $C_f(B)$ is true

Algorithm **PVSUBDIVISION** gives only a subdivision. This subdivision should be postprocessed in order to produce the piece-wise linear isotopic approximation of the hypersurface. This postprocessing is only available for $n \leq 3$, see [315] for the details. It is still an open problem for $n \geq 4$.

Open problem I. Generalize the postprocessing algorithm of Plantinga and Vegter for Algorithm **PVSUBDIVISION** to higher dimensions.

Remark 5^{§2}1. Although Algorithm PV_{SUBDIVISION} is not the whole PV Algorithm, its complexity captures the complexity of the full PV Algorithm. Because of this, our complexity analysis will focus on Algorithm PV_{SUBDIVISION}. \P

5^{§2}-2 Specifications for the PV algorithm

We now specify a particular interval approximation to which our complexity analysis of the PV algorithm will apply. We additionally provide a reformulation of condition $C_f(J)$ into condition $C'_f(J)$, which will be easier to deal with for the produced interval approximation and our complexity analysis.

Interval approximation construction

Our interval approximation will be based on finding h and h' such that both hf and $h'\nabla f$ are Lipschitz. This will allow us to construct the interval approximation by combining an evaluation in the midpoint of the box plus an error box. Recall that for $J \in \square \mathbb{R}^n$, $w(J)$ is the width of J and $m(J)$ the midpoint of J .

Theorem 5^{§2}1. [136; §4.2]. Let

$$h(x) = \frac{1}{\|f\|_W(1 + \|x\|)^{(d-1)/2}} \text{ and } h'(x) = \frac{1}{d\|f\|_W(1 + \|x\|)^{d/2-1}}.$$

Then

$$J \mapsto (hf)(m(J)) + (1 + \sqrt{d})\sqrt{n} w(J) \left[-\frac{1}{2}, \frac{1}{2} \right] \quad (5.6)$$

and

$$J \mapsto (h'\nabla f)(m(J)) + (1 + \sqrt{d-1})\sqrt{n} w(J) \left[-\frac{1}{2}, \frac{1}{2} \right]^n \quad (5.7)$$

are respectively interval approximations $\square[hf](J)$ and $\square[h'\nabla f](J)$ of hf and $h'\nabla f$, respectively, such that for all $J \in \square \mathbb{R}^n$,

$$\text{dist}_H((hf)(m(J)), \square[hf](J)) \leq \frac{1}{2}(1 + \sqrt{d})\sqrt{n} w(J) \quad (5.8)$$

and

$$\text{dist}_H((h'\nabla f)(m(J)), \square[h'\nabla f](J)) \leq \frac{1}{2}(1 + \sqrt{d-1})n w(J). \quad (5.9)$$

Remark 5^{§2}2. The interval approximations in [98] are based on Taylor expansion at the midpoint, so they are different from ours. However, our complexity analysis also applies to the interval approximations considered in [98]. \P

Recall the map $\text{IO} : \mathbb{R}^n \rightarrow \mathbb{S}_+^n$ from (1.29) that gives a diffeomorphism between \mathbb{R}^n and the upper half of \mathbb{S}^n , \mathbb{S}_+^n . We note that

$$\|\text{D}_x \text{IO}\| = 1/\sqrt{1 + \|x\|^2}. \quad (5.10)$$

By direct computation, we easily see that for $f \in \mathcal{P}_d$ and $x \in \mathbb{R}^n$,

$$f^h(\text{IO}(x)) = f(x)/(1 + \|x\|^2)^{d/2}, \quad (5.11)$$

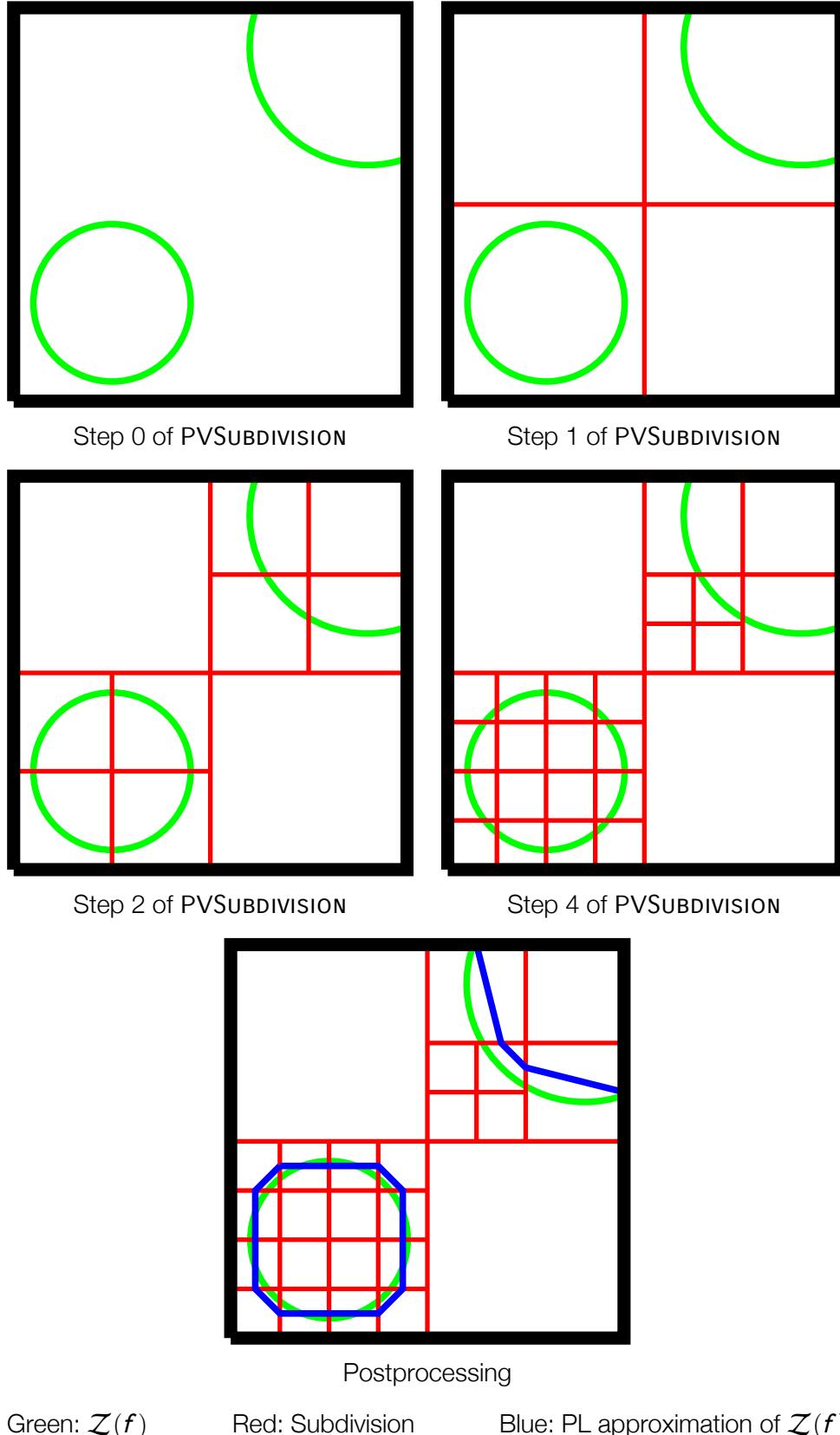


Figure 5\\$2.1: PV Algorithm applied to the polynomial $f = X^4 - 6X^3 + 2X^2Y^2 - 6X^2Y - 34X^2 - 6XY^2 - 320XY + 376X + Y^4 - 6Y^3 - 34Y^2 + 376Y + 3128$ in $[-10, 10]^2$.

and

$$D_{IO(x)} f^h D_x IO = \frac{\bar{D}_x f}{(1 + \|x\|^2)^{d/2}} - \frac{d f(x) x^*}{(1 + \|x\|^2)^{d/2+1}}. \quad (5.12)$$

Let us write

$$\widehat{f}(x) := \frac{f(x)}{\|f\|_W (1 + \|x\|^2)^{(d-1)/2}} \text{ and } \widehat{\nabla f} := \frac{\nabla f(x)}{d \|f\|_W (1 + \|x\|^2)^{d/2-1}}. \quad (5.13)$$

The following proposition and its corollary are the key pieces of the proof.

Proposition 5^{§2}2. [136; Proposition 4.1]. *Let $f \in \mathcal{P}_{d1}[k]$ be a polynomial map. Then the map*

$$\mathbf{F} : x \mapsto \frac{f(x)}{\|f\|_W (1 + \|x\|^2)^{(d-1)/2}}$$

is $(1 + \sqrt{d})$ -Lipschitz and, for all x , $\|\mathbf{F}(x)\| \leq \sqrt{1 + \|x\|^2}$.

Proof. For the Lipschitz property, it is enough to bound the norm of the derivative of the map by $1 + \sqrt{d}$. Due to (5.11),

$$\mathbf{F}(x) = \sqrt{1 + \|x\|^2} \frac{f^h(IO(x))}{\|f\|_W}.$$

Thus, by Corollary 1^{§1}7, we conclude the inequality.

By direct computation, the derivative of \mathbf{F} equals

$$\frac{f^h(IO(x))}{\|f\|_W} \frac{x^\top}{\sqrt{1 + \|x\|^2}} + \sqrt{1 + \|x\|^2} \frac{D_{IO(x)} f^h}{\|f\|_W} D_x IO.$$

Now, $\|f^h(IO(x))\|/\|f\|_W \leq 1$ and $D_{IO(x)} f^h \leq \sqrt{d} \|f\|_W$, by Corollary 1^{§1}7. Thus, by (5.10), we conclude that \mathbf{F} is $(1 + \sqrt{d})$ -Lipschitz after taking norms. \square

Corollary 5^{§2}3. [136; Corollary 4.2]. *Let $f \in \mathcal{P}_d$. Then \widehat{f} and $\widehat{\nabla f}$ are Lipschitz with Lipschitz constants $(1 + \sqrt{d})$ and $(1 + \sqrt{d-1})$, respectively, and for all x , $|\widehat{f}(x)|, \|\widehat{\nabla f}(x)\| \leq \sqrt{1 + \|x\|^2}$.*

Proof. The claims about \widehat{f} are immediate from Proposition 5^{§2}2. For the claims about $\widehat{\nabla f}$, observe that $\nabla f \in \mathcal{P}_{(d-1)1}[n]$ and $\|\nabla f\| \leq d \|f\|_W$. Thus Proposition 5^{§2}2 completes the proof. \square

Proof of Theorem 5^{§2}1. By Corollary 5^{§2}3 and our choice of h and h' , $hf = \widehat{f}$ and $h'\nabla f = \widehat{\nabla f}$ are Lipschitz. The rest is straightforward from the bound on the Lipschitz constants. \square

A weaker $C_f(J)$

We show that if an interval approximation satisfies (5.8) and (5.9), as the one constructed in Theorem 5^{§2}1, we can substitute condition $C_f(J)$ by a weaker, but easier to check, condition $C'_f(J)$.

Theorem 5§2 4. [136; Theorem 4.3]. Let $J \in \square \mathbb{R}^n$ and assume that our interval approximations $\square[hf]$ and $\square[h'\nabla f]$ of hf and $h'f$ satisfy (5 . 8) and (5 . 9). If

$$C'_f(J) : \begin{cases} \text{either } |h(m(J))f(m(J))| > (1 + \sqrt{d})\sqrt{n} w(J) \\ \quad \text{or } \|h'((m(J)))\nabla f(m(J))\| > \sqrt{2}(1 + \sqrt{d - 1})n w(J) \end{cases} \quad (5.14)$$

holds, then so does $C_f(J)$.

Lemma 5§2 5. Let $x \in \mathbb{R}^n$ and $s \in [0, 1/\sqrt{2}]$. Then for all $v, w \in B(x, s\|x\|)$, we have $\langle v, w \rangle > \|v\|\|w\|(1 - 2s^2) \geq 0$.

Proof of Theorem 5§2 4. When the condition on $h(m(J))f(m(J))$ is satisfied, (5 . 8) guarantees that $0 \notin \square[hf](J)$. Whenever the condition on $h'((m(J)))\nabla f(m(J))$ is satisfied, (5 . 9) and Lemma 5§2 5, with $s = 1/\sqrt{2}$, guarantee that $0 \notin \langle \square[h'Df](J), \square[h'Df](J) \rangle$. Hence $C'_f(J)$ implies $C_f(J)$ under the given assumptions. \square

Proof of Lemma 5§2 5. Let $s = \cos \theta$, so that $\theta \in [0, \pi/4]$, $c = \sqrt{1 - c^2}$ and $K_c := \{u \in \mathbb{R}^n \mid \langle x, u \rangle \geq \|x\|\|u\|c\}$ the convex cone of those vectors u whose angle with x , \widehat{xu} , is at most θ .

Given $v, w \in K_c$, we have, by the triangle inequality, that $\widehat{vw} \leq \widehat{vx} + \widehat{xw} \leq 2\theta \leq \pi/2$. Thus

$$\cos \widehat{vw} \geq \cos(\widehat{vx} + \widehat{xw}) \geq \cos 2\theta = 1 - 2s^2 \geq 0.$$

And so, it is enough to show that $B_{c\|x\|}(x) \subseteq K_c$ or, equivalently, that $d(x, \partial K_c) \leq c\|x\|$.

Now, $d(x, \partial K_c) = \min\{\|x - u\| \mid \langle x, u \rangle = \|x\|\|u\|c\}$ where the latter equals the distance of x to a line having an angle θ with x , which is $\|x\|s$. \square

5§2–3 Complexity analysis

We note that the complexity of Algorithm PVSUBDIVISION reduces to bounding the number of n -cubes of the output subdivision. This is so, because the run-time is bounded by

$$(\text{Cost of testing } C_f(J)) \cdot \#(\text{output subdivision}).$$

Further, by subdividing cubes in parallel, we can parallelize Algorithm PVSUBDIVISION obtaining a parallel algorithm whose parallel run-time is bounded by

$$(\text{Cost of testing } C_f(J)) \cdot \log \#(\text{output subdivision}).$$

and its number of processors by $O(\#(\text{output subdivision}))$.

For performing this complexity analysis, we will begin with a review of the so-called local size bound framework, employed by Burr, Gao and Tsigaridas [98, 99], and on which our condition-based and probabilistic complexity analyses will rely. After this, we introduce the condition number adapted to this setting and we perform the complexity analyses.

Local size bound framework

The local size bound framework is based on the following fundamental notion introduced by Burr [97].

Definition 5^{§2}1. [98; Definition 3.1] A *local size bound* for f is a function $b_f : \mathbb{R}^n \rightarrow [0, \infty)$ such that for all $x \in \mathbb{R}^n$,

$$b_f(x) \leq \inf \{ \text{vol}(J) \mid x \in J \in \square \mathbb{R}^n \text{ and } C_f(J) \text{ false} \} .$$

The intuition behind the local size bound is that it gives a bound on how small should a box be before it satisfies the condition $C_f(J)$. More explicitly, if $x \in J \in \square \mathbb{R}^n$ and $\text{vol}(J) < b_f(x)$, then $C_f(J)$ holds. Note that the precondition on the input of Algorithm PV_{SUBDIVISION} forces that $b_f(x)$ is always positive. This idea provides the following easy upper bound.

Proposition 5^{§2}6. [98; Proposition 4.1] The number of n -cubes of the final subdivision of Algorithm PV_{SUBDIVISION} on input (f, a) , regardless of how the subdivision step is done, is at most

$$(2a)^n / \inf\{b_f(x) \mid x \in [-a, a]^n\}.$$

□

The bound above is worst-case, it considers the worst $b_f(x)$ over the $x \in [-a, a]^n$. Continuous amortization, developed by Burr [97] and Burr, Krahmer and Yap [100], provides the following refined complexity estimate which is adaptive.

Theorem 5^{§2}7. [98; Proposition 5.2][100, 97, 98] The number of n -cubes of the final subdivision of Algorithm PV_{SUBDIVISION} on input (f, a) is at most

$$\max \left\{ 1, \int_{[-a, a]^n} \frac{2^n}{b_f(x)} dx \right\} .$$

Moreover, the bound is finite if and only if the algorithm terminates.

□

Remark 5^{§2}3. Although we don't give a proof, the complexity analysis in the next section shares many similarities with the complexity analysis that leads to Theorem 5^{§2}7. ¶

To effectively use either Proposition 5^{§2}6 or Theorem 5^{§2}7 we need explicit estimates for the local size bound.

Condition number and constructions of local size bounds

We introduce the condition number and give two constructions of the local size bound, under different hypothesis of the construction of the interval approximation. The first construction is the one by Burr, Gao and Tsigaridas [98] and the second one the one by Cucker, Ergür and the author [136]. We show how both of them are bounded by the condition number.

Condition number Relying on Definition 1^{§2}1, we introduce now the condition number adapted to our setting.

Definition 5^{§2}2. [136; Definition 5.1]. Given $f \in \mathcal{P}_d$, the *local affine condition number* of f at $x \in \mathbb{R}^n$ is $\kappa_{\text{aff}}(f, x) := \kappa(f^h, \mathcal{IO}(x))$.

The following result is a version of the regularity inequality with the functions introduced in (5.13).

Proposition 5^{§2} 8. [136; Proposition 5.5]. Let $f \in \mathcal{P}_d$ and $x \in \mathbb{R}^n$. Then either

$$\left| \widehat{f}(x) \right| > \frac{1}{2\sqrt{2d} \kappa_{\text{aff}}(f, x)} \text{ or } \left\| \widehat{\nabla f}(x) \right\| > \frac{1}{2\sqrt{2d} \kappa_{\text{aff}}(f, x)}.$$

Proof. Without loss of generality assume that $\|f\|_W = 1$. Let $y := \text{IO}(x)$, $F := f^h$ and assume that the first inequality does not hold. Then, by (5.11),

$$|F(y)| \leq \frac{1}{2\sqrt{2d} \kappa(F, y) \sqrt{1 + \|x\|^2}}$$

By (5.12), (5.10) and the regularity inequality (Proposition 1^{§2} 3), we get

$$\frac{1}{\sqrt{2} \kappa(F, y)} \leq \left\| \frac{\nabla_x f}{(1 + \|x\|^2)^{d/2}} - \frac{df(x)x}{(1 + \|x\|^2)^{d/2+1}} \right\| \left(\frac{1 + \|x\|^2}{\sqrt{d}} \right).$$

We divide by \sqrt{d} and use the triangle inequality to obtain

$$\frac{1}{\sqrt{2d} \kappa(F, y)} \leq \frac{\|\nabla_x f\|}{d(1 + \|x\|^2)^{d/2-1}} + \frac{|f(x)|}{(1 + \|x\|^2)^{(d-1)/2}} \frac{\|x\|}{\sqrt{1 + \|x\|^2}}.$$

Using (5.11) and our initial assumption on the second term in the sum, which we subtract, we get the desired inequality since $\|x\| < \sqrt{1 + \|x\|^2}$. \square

We note that the geometric interpretation of $\kappa_{\text{aff}}(f, x)$ was already discussed in detail in Section 1^{§2}. Because of that, we don't repeat it.

Construction of Burr, Gao and Tsigaridas The construction of Burr, Gao and Tsigaridas is given by the following function:

$$C(f, x) := \min \left\{ \frac{2^{n-1}d / \ln(1 + 2^{2-2n}) + \sqrt{n}/2}{\text{dist}(x, \mathcal{Z}^C(f))}, \frac{2^{2n}(d-1) / \ln(1 + 2^{2-4n}) + \sqrt{n/2}}{\text{dist}((x, x), \mathcal{Z}^C(g_f))} \right\}$$

where g_f is the polynomial $\langle \nabla f(X), \nabla f(Y) \rangle$.

Theorem 5^{§2} 9. [98; Corollaries 3.6 and 3.7] Assume that the interval approximation is as in [98; Remark 2.2]. Then

$$x \mapsto 1/C(f, x)^n$$

is a local size bound function for f . \square

The main intuition behind $C(f, x)$ is that its inverse tell us how near is the point x of being a singular point of the complex zero set $\mathcal{Z}^C(f)$ of f . By the local condition number theorem (Theorem 1^{§2} 9), the inverse of κ_{aff} measures how near is f of having a singular zero at x , which seems like a Copernican inversion of the situation for C .

The following result allows us to control C by the means of κ_{aff} .

Theorem 5^{S2}10. [136; Theorem 6.5] Let $d > 1$ and $f \in \mathcal{P}_d$. Then, for all $x \in \mathbb{R}^n$,

$$C(f, x) \leq 2^{3n} d^2 \kappa_{\text{aff}}(f, x).$$

Proof. Note that Corollary 5^{S2}3 holds over the complex numbers as well. Due to this and the fact that $\mathcal{Z}^{\mathbb{C}}(f) = \mathcal{Z}^{\mathbb{C}}(\widehat{f})$, we have that

$$|\widehat{f}(x)| \leq (1 + \sqrt{d}) \operatorname{dist}(x, \mathcal{Z}^{\mathbb{C}}(f)).$$

Now, if $\sqrt{2}(1 + \sqrt{d - 1}) \operatorname{dist}((y_1, y_2), (x, x)) < \|\widehat{\nabla f}(x)\|$, then $\sqrt{2}(1 + \sqrt{d - 1}) \|y_i - x\| < \|\widehat{\nabla f}(x)\|$. Thus, by Corollary 5^{S2}3, $\sqrt{2} \|\widehat{\nabla f}(y_i) - \widehat{\nabla f}(x)\| < \|\widehat{\nabla f}(x)\|$ and so, by Lemma 5^{S2}5, $0 \neq \langle \widehat{\nabla f}(y_1), \widehat{\nabla f}(y_2) \rangle$. Hence

$$\|\widehat{\nabla f}(x)\| \leq \sqrt{2}(1 + \sqrt{d - 1}) \operatorname{dist}(x, \mathcal{Z}^{\mathbb{C}}(g_f)).$$

The bound now follows from Proposition 5^{S2}8, together with $2^{3(n-1)}d + \sqrt{n} \leq 2^{3n-2}d$ and

$$\min \left\{ \frac{2^{n-1}d}{\ln(1 + 2^{2-2n})} + \frac{\sqrt{n}}{2}, \frac{2^{2n}(d-1)}{\ln(1 + 2^{2-4n})} + \sqrt{\frac{n}{2}} \right\} \leq 2^{3n-4}d + \frac{\sqrt{n}}{2},$$

for which we use that $1/\ln(1 + 2^{2-2n}) \leq 2^{2n-3}$ and $1/\ln(1 + 2^{2-4n}) \leq 2^{4n-3}$. \square

Let us observe that one of the reasons to prefer $\bar{\kappa}_{\text{aff}}$ over C is that the former is easier to compute and it has better variation properties, as shown by the 1st and 2nd Lipschitz properties (see Propositions 1^{S2}4 and 1^{S2}7).

Remark 5^{S2}4. The most remarkable fact is to show that the original quantity introduced by Burr, Gao and Tsigaridas can be controlled by κ_{aff} . \P

Construction of Cucker, Ergür and Tonelli-Cueto We show now that one can construct a local size bound directly from the condition number itself.

Theorem 5^{S2}11. [136; Theorem 6.6] Assume that the interval approximation is as in Theorem 5^{S2}1. Then

$$x \mapsto 1 / \left(2^{5/2} d n \kappa_{\text{aff}}(f, x) \right)^n$$

is a local size bound for f .

Proof. Let $x \in \mathbb{R}^n$. As, by Theorem 5^{S2}4, $C'_f(J)$ implies $C_f(J)$, it is enough to compute the minimum volume of $J \in \mathcal{I}_n$ containing x such that $C'_f(J)$ is false. This will still give a local size function for f .

Since $x \in J$, $\|x - m(J)\| \leq \sqrt{n} w(J)/2$. Hence, by Corollary 5^{S2}3 and Proposition 5^{S2}8, either

$$|\widehat{f}(m(J))| \geq \frac{1}{2\sqrt{2d} \kappa_{\text{aff}}(f, x)} - (1 + \sqrt{d}) \sqrt{n} w(J)/2$$

or

$$|\widehat{\nabla f}(m(J))| \geq \frac{1}{2\sqrt{2d} \kappa_{\text{aff}}(f, x)} - (1 + \sqrt{d-1}) \sqrt{n} w(J)/2.$$

This means that $C'_f(J)$ is true if either

$$2\sqrt{2d}(1+\sqrt{d})\sqrt{n}\kappa_{\text{aff}}(f, x)w(J) < 1 \text{ or } 2\sqrt{2d}(1+\sqrt{d-1})n\kappa_{\text{aff}}(f, x)w(J) < 1.$$

Hence we get that $C'_f(J)$ is true when both conditions are satisfied and the inequality $1 + \sqrt{d} \leq 2\sqrt{d}$ finishes the proof. \square

Worst-case complexity

If we assume our input to be integer polynomials, one can obtain the following worst-case complexity bound. This result was the original bound by Burr, Gao and Tsigaridas that is unable to explain the efficiency of the Plantinga-Vegter algorithm in practice.

Theorem 5^{§2}12. [98; Theorem 4.3] *The number of n -cubes in the final subdivision of Algorithm PV_{SUBDIVISION} on input (f, a) , with f an integer polynomial with coefficients of bit size at most τ and $a \in \mathbb{N}$, is at most*

$$2^{O(nd^{n+1}(n\tau+nd\log(nd)+9n+d)\log a)}$$

if the interval approximation is as in [98; Remark 2.2]. \square

Remark 5^{§2}5. The current techniques are able to only bound $\sup_{x \in [-a, a]^n} C(f, x)$ for f an integer polynomial, which is large whenever $C(f, x)$ is large for some x . These techniques cannot take advantage of quantities of the form $\int_{[-a, a]^n} C(f, x)^n dx$ with f an integer polynomial and $a \in \mathbb{N}$, which to be large need $C(f, x)$ to be large for many x . \P

Condition-based complexity

The following result is the first result in numerical real algebraic geometry where the complexity bound depends on the average of the condition number. This is interesting as this can be seen as a real analogue to the well-known Shub's estimation on the number of iterations for complex adaptive homotopy continuation [365]. In this way, the continuous amortization of Burr, Krahmer and Yap [100, 97], from where the result below comes, should be seen as not only as an important complexity analysis technique in the theory of subdivisions methods, but as a fundamental technique for future algorithms in numerical real algebraic geometry.

Theorem 5^{§2}13. [136; Theorem 6.7] *The number of n -cubes in the final subdivision of Algorithm PV_{SUBDIVISION} on input (f, a) is at most*

$$d^n \max\{1, a^n\} 2^{n\log n + 9n/2} \mathbb{E}_{x \in [-a, a]^n} (\kappa_{\text{aff}}(f, x)^n)$$

if the interval approximation is as in Theorem 5^{§2}1, and at most

$$d^{2n} \max\{1, a^n\} 2^{3n^2 + 2n} \mathbb{E}_{x \in [-a, a]^n} (\kappa_{\text{aff}}(f, x)^n)$$

if the interval approximation is as in [98; Remark 2.2].

Proof. This is just Theorems 5^{§2}7, 5^{§2}10 and 5^{§2}11 combined with the fact that the integral $\int_{[-a, a]^n} \kappa_{\text{aff}}(f, x)^n dx$ is just $(2a)^n \mathbb{E}_{x \in [-a, a]^n} (\kappa_{\text{aff}}(f, x)^n)$. \square

Probabilistic complexity

The next two theorems fulfill the promise of the finite expected run-time of the PV Algorithm. Theorem 5^{§2}14 gives a bound in the average setting and Theorem 5^{§2}15 in the smoothed setting, introduced by Spielman and Teng [380]. We note that for fixed n , all the bounds are polynomial in the degree d which explains the efficiency of the PV Algorithm in practice. Also, the randomness model is that of dobro random polynomials, and so more robust than the traditional setting with KSS random polynomials.

Theorem 5^{§2}14. [136; Theorem 3.1]. Let $\mathfrak{f} \in \mathcal{P}_d$ be a dobro random polynomial with parameters K and ρ . The expected number of n -cubes in the final subdivision of Algorithm PV_{SUBDIVISION} on input $(\mathfrak{f}, \mathbf{a})$ is at most

$$d^{\frac{n^2+3n}{2}} \max\{1, a^n\} 2^{\frac{n^2+16n \log(n)}{2}-1} (K\rho)^{n+1}$$

if the interval approximation is as in Theorem 5^{§2}1 and

$$d^{\frac{n^2+5n}{2}} \max\{1, a^n\} 2^{\frac{7n^2+9n \log(n)}{2}-1} (K\rho)^{n+1}$$

if the interval approximation is as in [98; Remark 2.2].

Theorem 5^{§2}15. [136; Theorem 3.2]. Let $f \in \mathcal{P}_d$, $\sigma > 0$, and $\mathfrak{f} \in \mathcal{P}_d$ a dobro random polynomial with parameters K and ρ . Then the expected number of n -cubes of the final subdivision of Algorithm PV_{SUBDIVISION} for input $(\mathfrak{f}_\sigma, \mathbf{a})$ where $\mathfrak{f}_\sigma := f + \sigma \|f\|_{W^1}$ is at most

$$d^{\frac{n^2+3n}{2}} \max\{1, a^n\} 2^{\frac{n^2+16n \log(n)}{2}-1} (K\rho)^{n+1} \left(1 + \frac{1}{\sigma}\right)^{n+1}$$

the interval approximation is as in Theorem 5^{§2}1 and

$$d^{\frac{n^2+5n}{2}} \max\{1, a^n\} 2^{\frac{7n^2+9n \log(n)}{2}-1} (K\rho)^{n+1} \left(1 + \frac{1}{\sigma}\right)^{n+1}$$

if the interval approximation is as in [98; Remark 2.2].

The proof of the two theorems above is just an easy consequence of Theorem 5^{§2}13 combined with the following theorem.

Theorem 5^{§2}16. (A) Let $\mathfrak{f} \in \mathcal{H}_d$ be a dobro random polynomial with parameters K and ρ . Then

$$\mathbb{E}_{\mathfrak{f}} \mathbb{E}_{x \in [-a, a]^n} (\kappa_{\text{aff}}(\mathfrak{f}, x)^n) \leq d^{\frac{n^2+n}{2}} 2^{\frac{n^2+5n+3 \log(n)+12}{2}} (K\rho)^{n+1}.$$

(S) Let $f \in \mathcal{H}_d$, $\sigma > 0$, $\mathfrak{f}_\sigma := f + \sigma \|f\|_{W^1}$ be a random polynomial such that $\mathfrak{g} \in \mathcal{H}_d[1]$ is a dobro random polynomial with parameters K and ρ . Then for $t \geq e$,

$$\mathbb{E}_{\mathfrak{f}_\sigma} \mathbb{E}_{x \in [-a, a]^n} (\kappa_{\text{aff}}(\mathfrak{f}_\sigma, x)^n) \leq d^{\frac{n^2+n}{2}} 2^{\frac{n^2+5n+3 \log(n)+12}{2}} (K\rho)^{n+1} \left(1 + \frac{1}{\sigma}\right)^{n+1}.$$

Proof. (A) By the Fubini-Tonelli theorem,

$$\mathbb{E}_{\mathfrak{f}} \mathbb{E}_{x \in [-a, a]^n} (\kappa_{\text{aff}}(\mathfrak{f}, x)^n) = \mathbb{E}_{x \in [-a, a]^n} \mathbb{E}_{\mathfrak{f}} (\kappa_{\text{aff}}(\mathfrak{f}, x)^n)$$

so it is enough to have a uniform bound for

$$\mathbb{E}_f (\kappa_{\text{aff}}(\mathfrak{f}, x)^n) = \int_1^\infty \mathbb{P} (\kappa_{\text{aff}}(\mathfrak{f}, x)^n \geq t) dt.$$

Now, by Theorem 5§1 3(A), this is bounded by

$$e^n + 2 \left(\frac{30K\rho\sqrt{N}}{\sqrt{n(n+1)}} \right)^{n+1} \int_1^\infty \frac{\ln(t)^{\frac{n+1}{2}}}{t^{1+1/n}} dt.$$

After the change of variables $t = e^{ns}$ the integral becomes

$$n \int_0^\infty (ns)^{\frac{n+1}{2}} e^{-s} ds = n^{\frac{n+3}{2}} \Gamma\left(\frac{n+3}{2}\right),$$

where Γ is Euler's Gamma function. Using the Stirling estimates for it, we obtain

$$\Gamma\left(\frac{n+3}{2}\right) \leq \sqrt{2\pi} \left(\frac{n+3}{2e}\right)^{\frac{n+2}{2}} \leq 4 \left(\frac{n+3}{4}\right)^{\frac{n+2}{2}}$$

and $N \leq (2d)^n$. Combining all these inequalities, we obtain the desired upper bound.

(S) As (A), but applying Theorem 5§1 3(S) instead. □

Remark 5§2 6. We note again that an important improvement over [136] is that we give explicit constants and no undetermined universal constants. ¶

5§3 2nd adaptive case: Han's covering algorithm

Around the same time that Cucker, Ergür and the author used the continuous amortization of Burr, Krahmer and Yap [100, 97] to show that the complexity of an adaptive algorithm in numerical real algebraic geometry could be controlled by $\mathbb{E}_{x \in \mathbb{S}^n} \kappa(f, x)^n$, Han (under the supervision of Lairez) [213, 214]¹ made a similar discovery. His motivation came from a search for an adaptive version of the algorithms presented in Chapter 4. However, Han didn't consider the question of the probabilistic algorithm and his proposed covering algorithm for homology computation had complexity proportional to $\mathbb{E}_{x \in \mathbb{S}^n} \kappa(f, x)^{2n}$ which does not have finite expectation².

Han's clear insight was to point out a fundamental property that we want a non-uniform cover to have in adaptive grid/subdivision methods.

¹We warn the reader about the numerous mistakes of these references. This means that any statement can be false beyond trivial corrections. See the footnote in Remark 3§2 2 for an example of such a case.

²Despite it is claimed that the algorithm runs in time bounded by $\mathbb{E}_{x \in \mathbb{S}^n} \kappa(f, x)^n$, [213, 214] contains an error in the proof and the given bound is the correct one. Also, we note that, due to the footnote at Remark 3§2 2, the correctness of the algorithm is not yet proven.

Definition 5^{§3}1. Let (X, d) be a metric space, $f : X \rightarrow (0, 1]$ a Lipschitz function, $C > 0$ and $\mathcal{B} := \{\bar{B}(x, r_x) \mid x \in \mathcal{G}\}$ a cover of X by closed balls. We say that \mathcal{B} has the *Han's* (f, C) -property if for all $x \in \mathcal{G}$,

$$r_x \leq C^{-1}f(x). \quad (5.15)$$

This property is very desirable, since it guarantees nice properties of the resulting adaptive subdivision/grid. This makes having a general algorithm to produce these covers an important step towards general adaptive subdivision/grid methods.

We present here the main ideas of Han's covering algorithm for the cube and the sphere. As an application, we will show that these can be used for estimating the condition number $\bar{\kappa}(f)$ in expected single exponential time and expected parallel polynomial time with expected single exponential number of processors.

First, we introduce Han's covering algorithm in the cube; second, we apply it to the sphere using a variation of the uniform grid; third and last, we use this to create an algorithm to estimate $\bar{\kappa}$ with finite expectation.

Han's covering algorithm for the cube

Han's covering algorithm in the cube follows a similar pattern to Algorithm PVSUBDIVISION. Based on this, we write Algorithm CUBICALHANCOVERING below. We focus our complexity analysis on the size of the output subdivision.

Algorithm 11: CUBICALHANCOVERING

Input : $f : [-a, a]^n \rightarrow (0, 1]$
 $a, C \in (0, \infty)$

Precondition : f is L-Lipschitz with respect to the ∞ -norm

```

 $\tilde{\mathcal{S}} \leftarrow \{[-a, a]^n\}$ 
 $\mathcal{S} \leftarrow \emptyset$ 
repeat
| Take B in  $\tilde{\mathcal{S}}$ 
|  $\tilde{\mathcal{S}} \leftarrow \tilde{\mathcal{S}} \setminus \{B\}$ 
| if  $w(B) \leq 2C^{-1}f(m(B))$  then
| |  $\mathcal{S} \leftarrow \mathcal{S} \cup \{B\}$ 
| else
| |  $\tilde{\mathcal{S}} \leftarrow \tilde{\mathcal{S}} \cup \text{STANDARDSUBDIVISION}(B)$ 
until  $\tilde{\mathcal{S}} = \emptyset$ 
return  $\mathcal{S}$ 

```

Output : Subdivision \mathcal{S} of $[-a, a]$

Postcondition: For every $B \in \mathcal{S}$, $w(B) \leq 2C^{-1}f(m(B))$,
i.e., \mathcal{S} has Han's (f, C) -property with respect the ∞ -norm

Theorem 5§3 1. Algorithm CUBICALHANCOVERING is correct. The number of n -cubes of the final subdivision of Algorithm CUBICALHANCOVERING on input (f, a, C) is at most

$$\max \{ a^n (2C + 3L)^n \mathbb{E}_{x \in [-a, a]^n} f(x)^{-n}, 1 \}.$$

Moreover, if $C > L$, the number of n -cubes of any subdivision satisfying the postcondition of Algorithm CUBICALHANCOVERING is at least

$$a^n (C - L)^n \mathbb{E}_{x \in [-a, a]^n} f(x)^{-n}.$$

For proving this theorem, we will use the following technical lemma which can be viewed as the main tool of the continuous amortization of Burr, Krahmer and Yap [100].

Lemma 5§3 2. Let (X, d) be a metric space, $f : X \rightarrow (0, 1]$ an L -Lipschitz map, $C > 0$, $x \in X$ and $r_x > 0$. Assume that (x, r_x) satisfies inequality (5.15) and that there is some $y_x \in \bar{B}(x, 2r_x)$ such that

$$2r_x \geq C^{-1}f(y_x). \quad (5.16)$$

Then for all $z \in B(x, r_x)$,

$$r_x^{-1} \leq (2C + 3L)f(z)^{-1}. \quad (5.17)$$

Proof of Theorem 5§3 1. Note that the correctness is trivial, because f attains a global minimum in the compact set $[-a, a]^n$. Let B_∞ denote the ball of the ∞ -norm and \mathcal{S} the subdivision obtained by Algorithm CUBICALHANCOVERING. Assume also that $\mathcal{S} \neq \{[-a, a]^n\}$.

By construction, for all $\bar{B}_\infty(x, r_x) \in \mathcal{S}$, we have that $r_x \leq C^{-1}(x)$, since $w(\bar{B}_\infty(x, r_x)) = 2r_x$ and $x = m(\bar{B}_\infty(x, r_x))$. Now, let $\bar{B}_\infty(y_x, 2r_x)$ be the parent box of $\bar{B}_\infty(x, r_x)$, i.e.,

$$\bar{B}_\infty(x, r_x) \in \text{STANDARDSUBDIVISION}(\bar{B}_\infty(y_x, 2r_x))$$

with $\bar{B}_\infty(y_x, 2r_x)$ appearing before in the execution of Algorithm CUBICALHANCOVERING. Since $\bar{B}_\infty(y_x, 2r_x) \notin \mathcal{S}$, this means that the condition

$$w(\bar{B}_\infty(x, r_x)) < 2f(m(\bar{B}_\infty(y_x, 2r_x)))$$

did not hold. Thus $2r_x > f(y_x)$.

By the above, we are in the situation of Lemma 5§3 2 for each $\bar{B}_\infty(x, r_x) \in \mathcal{S}$. Hence for all $\bar{B}_\infty(x, r_x) \in \mathcal{S}$, we have that

$$1 = \int_{\bar{B}_\infty(x, r_x)} (2r_x)^{-n} dz \leq 2^{-n} (2C + 3L)^n \int_{\bar{B}_\infty(x, r_x)} f(z)^{-n} dz$$

by the inequality (5.17) of Lemma 5§3 2. Therefore

$$\begin{aligned} \#\mathcal{S} &= \sum_{\bar{B}_\infty(x, r_x) \in \mathcal{S}} 1 = \sum_{\bar{B}_\infty(x, r_x) \in \mathcal{S}} \int_{\bar{B}_\infty(x, r_x)} (2r_x)^{-n} \\ &\leq 2^{-n} (2C + 3L)^n \sum_{\bar{B}_\infty(x, r_x) \in \mathcal{S}} \int_{\bar{B}_\infty(x, r_x)} f(z)^{-n} dz = 2^{-n} (2C + 3L)^n \int_{[-a, a]^n} f(z)^{-n} dz, \end{aligned}$$

as desired.

For the universal lower bound, note that for $z \in \overline{B}_\infty(x, r_x)$ with $r_x \leq C^{-1}f(x)$, we have that

$$r_x^{-1} \geq (C - L)f(z)^{-1}$$

due to $Cr_x \leq f(x) \leq f(z) + Lr_x$. Then one proves the claim analogously. \square

Proof of Lemma 5^{§3}2. By the triangle inequality, for all $z \in \overline{B}(x, r_x)$,

$$2Cr_x \geq f(y_x) \geq f(z) - Ld(y_x, z) \geq f(z) - L(d(z, x) + d(x, y_x)) \geq f(z) - 3Lr_x.$$

From here the claim follows. \square

Remark 5^{§3}1. Let us note that we could obtain in the upper bound $2(C + L)$ instead of $(2C + 3L)$. However, we proceed as we do to show the underlying general principle illustrated by Lemma 5^{§3}2. \P

The following corollary is immediate.

Corollary 5^{§3}3. *Let $f : [-a, a]^n \rightarrow (0, 1]$ have evaluation cost $\text{cost}(f)$. Assume the operations with real numbers are constant cost. Then Algorithm CUBICALHANCOVERING on input (f, a, C) has run-time bounded by*

$$O(\text{cost}(f) \max \{a^n(2C + 3L)^n \mathbb{E}_{x \in [-a, a]^n} f(x)^{-n}, 1\}).$$

Moreover, there is a parallel version of Algorithm CUBICALHANCOVERING, PARCUBICALHANCOVERING, whose parallel run-time is at most

$$\begin{aligned} O(\text{cost}(f) \max \{n \log(a(2C + 3L)) + \log \mathbb{E}_{x \in [-a, a]^n} f(x)^{-n}, 0\}) \\ = O(\text{cost}(f) \max \{n \log(a(2C + 3L)) + n \mathbb{E}_{x \in [-a, a]^n} \log(1/f(x)), 0\}) \end{aligned}$$

and whose required number of processors is at most

$$O(\max \{a^n(2C + 3L)^n \mathbb{E}_{x \in [-a, a]^n} f(x)^{-n}, 1\}). \quad \square$$

Remark 5^{§3}2. We note that it would be possible to employ interval arithmetic, floating-point, etc. to evaluate approximately f and obtain a round-off version of Algorithm CUBICALHANCOVERING. \P

Han's covering algorithm for the sphere

The original Han's covering algorithm was for the sphere. However, the version proposed by Han [214, 213] is non-constructive as it relies on the same construction employed in the proof of Lemma 1^{§2}20. We now give a constructive version, in which the grid can be constructed efficiently (in practice). We note that this is non-trivial, since we cannot cover the sphere with balls whose pairwise intersections have measure zero. However, we avoid this issue at the cost of some optimality, by constructing Algorithm SPHERICALHANCOVERING relying on Algorithm CUBICALHANCOVERING.

Recall the bijective map $\overline{\mathcal{O}} : \partial[-1, 1]^{n+1} \rightarrow \mathbb{S}^n$, from (4.20), given by $x \mapsto x/\|x\|$.

We note that Algorithm SPHERICALHANCOVERING is just like applying Algorithm CUBICALHANCOVERING in the boundary of the cube $\partial[-1, 1]^{n+1}$ and then projecting it onto the sphere. Recall also that for each facet F of $\partial[-1, 1]^{n+1}$, the map $\overline{\mathcal{O}}|_F$ is 1-Lipschitz. With all this in mind, we prove the following theorem.

Algorithm 12: SPHERICALHANCOVERING

Input : $f : \mathbb{S}^n \rightarrow (0, 1]$

$C \in (0, \infty)$

Precondition : f is L-Lipschitz with respect to the geodesic distance $\text{dist}_{\mathbb{S}}$

```

 $\tilde{\mathcal{A}} \leftarrow \overline{\text{IO}} \left( \left( 2\mathbb{Z}^{-\lceil \frac{1}{2} \log n \rceil} + 1 \right) \cap \partial[-1, 1]^{n+1} \right) \times \{1\}$ 
 $\mathcal{A} \leftarrow \emptyset$ 
repeat
  Take  $(x, r_x)$  in  $\tilde{\mathcal{A}}$ 
   $\tilde{\mathcal{A}} \leftarrow \tilde{\mathcal{A}} \setminus \{(x, r_x)\}$ 
  if  $r_x \leq C^{-1}f(x)$  then
     $\mathcal{A} \leftarrow \mathcal{A} \cup \{(x, r_x)\}$ 
  else
     $i \leftarrow \arg \max \{|x_i| \mid i \in \{0, \dots, n\}\}$ 
     $\tilde{x} \leftarrow x / |x_i|$ 
     $\tilde{\mathcal{A}} \leftarrow \tilde{\mathcal{A}} \cup \overline{\text{IO}} \left( \left\{ \left( \tilde{x} + \sum_{j \neq i} \sigma_j \frac{r_x}{2} 2^{-\lceil \frac{1}{2} \log n \rceil} e_i, \frac{r_x}{2} \right) \mid \sigma_j \in \{-1, 1\} \right\} \right)$ 
until  $\tilde{\mathcal{A}} = \emptyset$ 
return  $\mathcal{A}$ 

```

Output : $\mathcal{A} \subset \mathbb{S}^n \times (0, 1/3]$

Postcondition: $\{B(x, r_x) \mid (x, r_x) \in \mathcal{A}\}$ has Han's (f, C) -property

Theorem 5§3 4. Algorithm SPHERICALHANCOVERING is correct. The number of n -cubes of the final subdivision of Algorithm SPHERICALHANCOVERING on input (f, C) is at most

$$\max \left\{ 2^{1+n} n^{1+\frac{n}{2}}, 2n^{1+\frac{n}{2}} (4C + 3L)^n \mathbb{E}_{x \in \partial[-1, 1]^n} f(\overline{\text{IO}}(x))^{-n} \right\}.$$

Proof. We note that $f \circ \overline{\text{IO}}$ is $\sqrt{n}L$ -Lipschitz with respect to the ∞ -norm in each facet. Since we are starting not with $\partial[-1, 1]^n$ or its facets, but with $2^{1+n} n^{1+\frac{n}{2}}$ initial cubes, we should account for this, which is done in the first term of the maximum. For the other term, we apply Theorem 5§3 1 to each of these initial n -cubes and then we apply the additive property of integrals. Just note that instead of (C, L) , we should substitute $(2^{\lceil \frac{1}{2} \log n \rceil} C, \sqrt{n}L)$. For the correctness, note that

$$\overline{B}_{\infty} \left(\frac{x}{\|x\|}, r_x 2^{-\lceil \frac{1}{2} \log n \rceil} \right) \subseteq \overline{B} \left(\frac{x}{\|x\|}, r_x \right)$$

implies that the final subdivision gives the desired covering. \square

We now translate the above theorem into a proper statement over the sphere.

Theorem 5§3 5. Algorithm SPHERICALHANCOVERING is correct. The number of n -cubes of the final subdivision of Algorithm SPHERICALHANCOVERING on input (f, C) is at most

$$\max \left\{ 2^{1+n} n^{1+\frac{n}{2}}, 2(n+1)^{n+1} (4C + 3L)^n \mathbb{E}_{x \in \mathbb{S}^n} f(x)^{-n} \right\},$$

Moreover, if $C > L$, the number of balls of any covering satisfying the postcondition of Algorithm SPHERICALHANCOVERING is at least

$$2\sqrt{n}(C - L)^n \mathbb{E}_{x \in \mathbb{S}^n} f(x)^{-n}.$$

Remark 5^{§3}3. We note that an upper bound for the size of the covering produced by Algorithm SPHERICALHANCOVERING is exponential in $O(n \log n)$, while the lower bound for a covering satisfying the same property is exponential in $O(n)$. The reason for this is the same as for why this happens with the uniform grid. There is a loss at covering the sphere by covering the cube. \blacksquare

We recall the following easy consequence of [87; 2.31], which gives an estimation of the volume of a n -ball.

Lemma 5^{§3}6. Let $r \in [0, 1/2]$ and $x \in \mathbb{S}^n$. Then

$$0.9 \omega_n r^n \leq \omega_n \sin^n r \leq \text{vol}_n(B_{\mathbb{S}}(x, r)) \leq \omega_n r^n \quad (5.18)$$

where ω_n is the volume of the n -dimensional ball $B(0, 1)$. \square

Proof of Theorem 5^{§3}5. For the upper bound, we only need to apply the change of variables theorem on each facet F of $\partial[-1, 1]^{n+1}$. Without loss of generality, let $F = 1 \times [-1, 1]^n$. Now, by a straightforward computation, for $x \in \{1\} \times \mathbb{R}^n$ and $v \in 0 \times \mathbb{S}^{n-1}$,

$$D_x \overline{\text{IO}} v = \frac{1}{\|x\|} \left(v - \frac{-\langle x, v \rangle}{\|x\|^2} \right),$$

and therefore

$$\|D_x \overline{\text{IO}} v\| = \frac{\sqrt{\|x\|^2 - \langle x, v \rangle^2}}{\|x\|^2} \in \left[\frac{\sqrt{\|x - e_0\| + \|x\|^2}}{\|x\|^2}, \frac{1}{\|x\|} \right].$$

This implies that

$$\left| \det D_x \overline{\text{IO}} \right| = \frac{\sqrt{\|x\|^2 + \|x - e_0\|}}{\|x\|^{n+1}} \geq \frac{1}{\|x\|^n},$$

and so that

$$\int_{x \in F} f(\overline{\text{IO}}(x))^{-n} dx \leq \int_{y \in \overline{\text{IO}}(F)} f(y)^{-n} \left\| \overline{\text{IO}}^{-1}(y) \right\|^n dy \leq \int_{y \in \overline{\text{IO}}(F)} f(y)^{-n} (n+1)^{\frac{n}{2}} dy.$$

Hence the upper bound follows.

The proof of the universal lower bound is analogous to the proof of the lower bound in Theorem 5^{§3}1. We only need to use the estimation in Lemma 5^{§3}6 to lower bound 1 by $\omega_n^{-1} \int_{B_{\mathbb{S}}(x, r_x)} r_x^{-n}$ and some inequalities between volumes of Euclidean balls. \square

Corollary 5^{§3}7. Let $f : [-a, a]^n \rightarrow (0, 1]$ have evaluation cost $\text{cost}(f)$. Assume the operations with real numbers are constant cost. Then Algorithm SPHERICALHANCOVERING on input (f, C) has run-time bounded by

$$O \left(\text{cost}(f) \max \left\{ 2^{1+n} n^{1+\frac{n}{2}}, 2(n+1)^{n+1} (4C + 3L)^n \mathbb{E}_{x \in \mathbb{S}^n} f(x)^{-n} \right\} \right).$$

Moreover, there is a parallel version of Algorithm SPHERICALHANCOVERING, PARSPHERICALHANCOVERING, whose parallel run-time is at most

$$\begin{aligned} \mathcal{O}(\text{cost}(f) \max\{n \log((n+1)(4C+3L)) + \log \mathbb{E}_{x \in \mathbb{S}^n} f(x)^{-n}, n \log n\}) \\ = \mathcal{O}(\text{cost}(f) \max\{n \log((n+1)(4C+3L)) + n \mathbb{E}_{x \in \mathbb{S}^n} \log(1/f(x)), n \log n\}) \end{aligned}$$

and whose required number of processors is at most

$$\mathcal{O}\left(\max\left\{2^{1+n}n^{1+\frac{n}{2}}, 2(n+1)^{n+1}(4C+3L)^n \mathbb{E}_{x \in \mathbb{S}^n} f(x)^{-n}\right\}\right). \quad \square$$

Remark 5§3 4. As with Algorithm CUBICALHANCOVERING, the same notions regarding round-off versions applies to Algorithm SPHERICALHANCOVERING. ¶

Fast estimation of $\bar{\kappa}(f)$ and $\bar{\kappa}_{\text{aff}}(f)$

One important application of the coverings obtained by Han's covering algorithms is that they allow us to compute very fast the minimum of a Lipschitz function $f : X \rightarrow (0, 1]$, which was one of the main motivations of Han's work [213, 214]. Now, by the 2nd Lipschitz property (Proposition 1§3 3), the map

$$\mathbb{S}^n \ni x \mapsto \bar{\kappa}(f, x)^{-1} \in [0, 1]$$

is D-Lipschitz with respect to the geodesic distance $\text{dist}_{\mathbb{S}}$.

Lemma 5§3 8. [213]. Let (X, d) be a metric space, $f : X \rightarrow (0, 1]$ an L-Lipschitz map, $C > 0$ and $\mathcal{B} = \{\bar{B}(x, r_x) \mid x \in \mathcal{G}\}$ a cover of X . If \mathcal{B} has Han's (f, C) -property, then

$$\left(1 - \frac{L}{C}\right) \min_{x \in \mathcal{G}} f(x) \leq \min_{x \in X} f(x) \leq \min_{x \in \mathcal{G}} f(x).$$

Proof. Since f is L-Lipschitz, for all $x \in \mathcal{G}$ and all $z \in \bar{B}(x, r_x)$,

$$f(z) \geq f(x) - Lr_x \geq f(x) - LC^{-1}f(x) = \left(1 - \frac{L}{C}\right) f(x),$$

by inequality (5 . 15). The claim is now obvious. □

In view of the above, we propose Algorithm $\bar{\kappa}$ -FASTESTIMATE that is a variation of Algorithm $\bar{\kappa}$ -ESTIMATE using Han's covering algorithm. We note that one can modify Algorithm $\bar{\kappa}$ -FASTESTIMATE to allow the algorithm to stop when the condition number is bigger than a certain threshold $B > 0$.

Theorem 5§3 9. Algorithm $\bar{\kappa}$ -FASTESTIMATE is correct. Its run-time on input (f, p) is bounded by

$$\mathcal{O}\left((N + n^3) \max\left\{2^n n^{1+\frac{n}{2}}, (n+1)^{n+1}(7D+1)^n \mathbb{E}_{x \in \mathbb{S}^n} \bar{\kappa}(f, x)^n\right\}\right).$$

Further, this algorithm admits a parallel version, $\bar{\kappa}$ -FASTPARESTIMATE, whose parallel run-time is bounded by parallel run-time is at most

$$\mathcal{O}\left((N + n^3) \max\{n \log((n+1)(7D+1)) + \log \mathbb{E}_{x \in \mathbb{S}^n} \bar{\kappa}(f, x)^n, n \log n\}\right)$$

and whose required number of processors is at most

$$\mathcal{O}\left(\max\left\{2^{1+n}n^{1+\frac{n}{2}}, 2(n+1)^{n+1}(7D+1)^n \mathbb{E}_{x \in \mathbb{S}^n} \bar{\kappa}(f, x)^n\right\}\right).$$

Proof. Correctness follows from Lemma 5^{S3}8. For the complexity estimates, use Theorem 5^{S3}5, Corollary 5^{S3}7, for the size complexity of Algorithm SPHERICALHANCOVERING, and [272; Lemma 25], for the complexity of evaluation of $\bar{\kappa}(f, x)$ as we did in the proof of Theorem 4^{S2}8. \square

The following is the most important result.

Theorem 5^{S3}10. *Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a KSS random polynomial tuple. Then the expected run-time of Algorithm $\bar{\kappa}$ -FASTESTIMATE on input \mathfrak{f} is bounded by*

$$\mathcal{O}\left((N + n^3)n^2q^{n+1}(7D + 1)^n(119nN)^{\frac{n+1}{2}}\right) = (qnDN)^{O(n)},$$

and the expected parallel run-time and number of processors of Algorithm $\bar{\kappa}$ -FASTEESTIMATE are bounded, respectively, by

$$\mathcal{O}(n(N + n^3)\log(qnDN))$$

and by

$$\mathcal{O}\left(n^2q^{n+1}(7D + 1)^n(119nN)^{\frac{n+1}{2}}\right) = (qnDN)^{O(n)}.$$

For $\mathfrak{f}_\sigma := f + \sigma\|f\|_W\mathfrak{f}$, the same bounds hold with an additional factor $(1 + \frac{1}{\sigma})^{n+1}$.

Proof. The proof is as that of Theorem 5^{S2}16, a simple application of the Fubini-Tonelli theorem. For this, we have to use the tail bounds from Proposition 1^{S3}6. \square

Making a variation of the above, we can apply the same strategy to $\bar{\kappa}_{\text{aff}}$. The idea is to bound, on the one hand, $\bar{\kappa}(p^h)$, and, on the other hand, $\bar{\kappa}_{\text{aff}}^\infty(p)$, see (1.36).

Theorem 5^{S3}11. *There is an algorithm, $\bar{\kappa}_{\text{aff}}$ -FASTEESTIMATE, which admits a parallel version, $\bar{\kappa}_{\text{aff}}$ -FASTEESTIMATE, that for $p \in \mathcal{P}_d[q]$ and $\rho \in (0, 1)$, computes a positive number such that $K \leq \bar{\kappa}_{\text{aff}}(p) \leq (1 - \rho)^{-1}K$. For these algorithms, the following hold. Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a KSS random polynomial tuple. Then the expected run-time of Algorithm $\bar{\kappa}_{\text{aff}}$ -FASTEESTIMATE on input \mathfrak{f} is bounded by*

$$\mathcal{O}\left((N + n^3)n^2q^{n+1}(7D + 1)^n(119nN)^{\frac{n+1}{2}}\right) = (qnDN)^{O(n)},$$

Algorithm 13: $\bar{\kappa}$ -FASTEESTIMATE

Input : $f \in \mathcal{H}_d[q]$
 $\rho \in (0, 1)$

$\mathcal{A} \leftarrow \text{SPHERICALHANCOVERING}(\bar{\kappa}(f, x)^{-1}, D\rho^{-1})$
 $K \leftarrow (1 - \rho)^{-1} \max\{\kappa(f^L, x) \mid (x, r_x) \in \mathcal{A}, L \in [q]^{\leq n+1}\}$

Output : $K \in (0, \infty)$
Postcondition: $\bar{\kappa}(f) \leq K \leq (1 - \rho)^{-1}\bar{\kappa}(f)$

and the expected parallel run-time and number of processors of Algorithm $\bar{\kappa}_{\text{aff}}\text{-FASTPARESTIMATE}$ are bounded, respectively, by

$$O(n(N + n^3) \log(qnDN))$$

and by

$$O\left(n^2 q^{n+1} (7D + 1)^n (119nN)^{\frac{n+1}{2}}\right) = (qnDN)^{O(n)}.$$

For $f_\sigma := f + \sigma \|f\|_W \tilde{f}$, the same bounds holds with an additional factor $(1 + \frac{1}{\sigma})^{n+1}$.

Proof. We use Algorithm $\bar{\kappa}\text{-FASTESTIMATE}$ to bound $\bar{\kappa}(f^h)$ and $\bar{\kappa}_{\text{aff}}^\infty(p)$. For the first, the bound is as above; for the latter, we should use the tail bound of Corollary 1§4.7. \square

An interesting consequence of these two results is the following one, which we state without details.

Theorem 5§3.12. *There is an algorithm that computes a positive lower bound of the reach of a spherical smooth algebraic set in finite average time that is singly exponential time in the number of variables and polynomial in the degree and number of polynomials.*

Proof. We have to use the bound of Theorem 3§2.5 together with the higher derivative estimate (Theorem 1§2.12). \square

5§4 А пятилетка³ for the future

We now present our ambitious research program пятилетка. The program will be divided in five parts. The main focus of this program is the development of an algorithm computing homology of semialgebraic sets in average singly exponential time and its application to a computational approach to classification problems in real algebraic geometry.

5§4–1 Пятилетка I: Homology in average singly exponential time

With the development of the main results of this thesis in Chapter 4, the old non-adaptive grid method achieved a milestone. In this setting, there are problems related to quantified formulas that the author currently works in. However, the development of the condition-based complexity analysis of the PV Algorithm together with a finite bound for the expectation in [136] (Section 5§2) was a completely unexpected result.

This result suggests the following major problem of the program.

Pyatiletka problem I.A. *Find a numerical algorithm computing the homology groups of semialgebraic sets that, for a KSS random polynomial tuple $p \in \mathcal{P}_d[q]$ and a Boolean formula Φ of size s , runs in expected $s(qnD)^{n^{O(1)}}$ -time.*

Pyatiletka problem I.B. *Find a numerical parallel algorithm computing the homology groups of semialgebraic sets that, for a KSS random polynomial tuple $p \in \mathcal{P}_d[q]$ and a Boolean formula Φ of size s , runs in expected $s(qnD)^{O(1)}$ with $s(qnD)^{n^{O(1)}}$ expected number of processors.*

³Five-year plan.

We note that as of today the above two problems remain unsolved even in the case of counting zeros. This forces us to pose the following problem.

Pyatiletka problem II.A. *Find a numerical algorithm computing counting the zeros of an algebraic set that, for a KSS random polynomial tuple $\mathfrak{p} \in \mathcal{P}_d[n]$, runs in expected $(nD)^{n^{O(1)}}$ -time.*

Pyatiletka problem II.B. *Find a numerical parallel algorithm counting the zeros of an algebraic set that, for a KSS random polynomial tuple $\mathfrak{p} \in \mathcal{P}_d[n]$, runs in expected parallel $(nD)^{O(1)}$ -time with $(nD)^{n^{O(1)}}$ expected number of processors.*

In any of the above problems, Algorithms PV_{SUBDIVISION} and SPHERICALHAN_{COVERING} can provide subdivisions with very good properties. Unfortunately, it is not clear how to use such properties in order to obtain a topological reconstruction, which is similar to the situation with the PV Algorithm, see Open problem I in Section 5^{§2}.

5^{§4–2} Пятилетка II: A condition number for adaptive algorithms

In adaptive subdivisions methods, a new condition-based quantity appears:

$$\mathbb{E}_{x \in \mathbb{S}^n} \kappa(f, x)^n. \quad (5.19)$$

The main difference with the usual maximum-based quantity $\kappa(f)$ is that this quantity has finite expectation, by Theorem 1^{§2}17. However, let us note that for a KSS random polynomial $\mathfrak{f} \in \mathcal{H}_d[1]$,

$$\mathbb{E}_{x \in \mathbb{S}^n} \kappa(f, x)^\alpha \quad (5.20)$$

is finite if and only if $\alpha < n + 1$, due to Corollary 5^{§1}10. We note that this is the main difficulty towards the solution of Pyatiletka problems I and II, since following the usual recipe (assuming everything works) gives an algorithm whose complexity is controlled by

$$\mathbb{E}_{x \in \mathbb{S}^n} \kappa(f, x)^{2n} \quad (5.21)$$

which we expect to be infinite.

We note that the condition-based quantity (5.19) is still to be understood, and it will play a fundamental role in the understanding of subdivisions.

Pyatiletka problem III. *Develop a condition-based complexity theory for adaptive subdivision/grid methods. More concretely, analyze as many adaptive subdivisions methods as possible using condition-based quantities of the form (5.19).*

This will lead to many probabilistic analysis of existing algorithm and will explain the success of adaptive subdivision problems in solving problems, like it did with the PV Algorithm. Among the possible candidates for this are the algorithms of Xu and Yap [420]⁴, and Jin and Cheng [237, 238]. It is clear that these analysis might not only help to solve the Pyatiletka problem III, but also the Pyatiletka problems I and II as they will probably allow the exploration of new ideas of how to exploit good subdivisions.

⁴The author is currently working in this analysis [391].

Also, let us note that (5.19) is infinite if and only if $\kappa(f)$ is so. However, we can take the derivative of (5.19) with respect to f , since expectations and derivatives commute. The latter suggest a purely metric approach to classifying isotopy types in the complement of the discriminant.

Pyatiletka problem IV. *Compute the derivative of (5.19) with respect to f . Can this be used to develop homotopy preprocessing algorithms in numerical real algebraic geometry? And for studying the number of rigid isotopy types of a smooth algebraic set?*

Since $\kappa(f, x)$ is a metrical quantity in nature, the above would lead to the creation of a metric algebraic geometry, where the properties of algebraic sets are studied through the study of the distance and other metric properties.

5§4–3 Пятилетка III: Robust probabilistic framework

Another important development in [136] (Section 5§1), following the work of Ergür, Paouris and Rojas [175, 176], was the development of bounds for the more general class of dobro random polynomials. Unfortunately, the bounds are not for dobro polynomial tuples. This motivates the following question.

Pyatiletka problem V. *Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a dobro random polynomial tuple and $x \in \mathbb{S}^n$. Obtain tail bounds for $\kappa(\mathfrak{f}, x)$ like those in Theorem 1§2 17.*

There are other possible ways to proceed. It is clear that the techniques from geometric functional analysis are more versatile. This means that they work with more norms than just norms coming from an Euclidean product. In this respect, we propose the following problem.

Pyatiletka problem VI. *Explore how replacing the Weyl norm of $\mathcal{H}_d[q]$ (and $\mathcal{P}_d[q]$) by a different norm affects the complexity of numerical algorithms.*

One can see that as long as a norm allows us to control evaluations and derivatives, one should be able to obtain a version of the exclusion lemma, the 1st and 2nd Lipschitz properties and the higher derivative estimate for the corresponding condition number. In this aspect, there are two kinds of norms that one consider: functional norms in the space that the algorithm works in and p -norms of the coefficients of the polynomials.

For functional norms, there are some early results in work of Cucker, Ergür and the author [137] that shows that one gets significant improvements in the exponents that appear in the complexity analysis⁵. For p -norms of coefficients of polynomials, the author [390] has preliminary results showing that it is possible to eliminate the scaling of the coefficients in the random model.

An additional problem, which is completely unexplored, is the following one.

Pyatiletka problem VII. *Let $\mathfrak{f} \in \mathcal{H}_d[q]$ be a random polynomial tuple distributed according to some discrete probability law and $x \in \mathbb{S}^n$. Can we say something in general about the tail bounds for $\kappa(\mathfrak{f}, x)$?*

⁵Where significant means that exponents that are of the form $O(n^2)$ become of the form $O(n)$.

The above problem could lead to a development to hybrid symbolic-numerical algorithms that run in average singly exponential time and worst-case doubly exponential for a random integer polynomial tuple. We pose this as a problem.

Pyatiletka problem VII. *Find a hybrid symbolic-numerical algorithm computing the homology of semialgebraic sets that, for $\mathfrak{p} \in \mathcal{P}_{\mathbf{d}}[q]$ with random integer coefficients i.i.d. on $[-2^b, 2^b]$ and a Boolean formula Φ of size s , runs in expected $s(qnD)^{n^{O(1)}} 2^{O(b)}$ -time and worst $s(qnD)^{2^{O(n)}} 2^{O(b)}$ -time.*

5^{§4–4} Пятилетка IV: Real algorithms

In one of his famous criticisms to non-constructive mathematics, Bishop [Q2] claimed that “classical mathematics concerns itself with operations that can be carried out by God” while constructive mathematics concerns itself with “operations that can be carried out by finite beings, man’s mathematics for short”. As of today, the status of Bishop’s “man’s mathematics” can be seen that is properly realized in the numerous constructive algorithms of real algebraic geometry, which are beautifully described by Basu, Pollack and Roy in their book [34].

However, in the current computational world, we cannot conform ourselves with algorithms that are good in theory, but that no one has seen them work. Making fun of Bishop’s discourse [Q2], who cares about the operations that finite beings that live thousands of years can do? As life is short, the following problem is very important.

Pyatiletka problem IX. *If existing, can the algorithm of the Pyatiletka problems I, II and VII be implement in practice so that they can be run in a computer?*

One might expect that numerical algorithms have a better chance of being efficient in practice, but the author has a certain bias. A project of interest is the following one.

Pyatiletka problem X. *Can any of the Algorithms $\bar{\kappa}$ -ESTIMATE, SPHERICALHOMOLOGY, AFFINEHOMOLOGY, CUBICALHANCOVERING and their variants across this thesis be implement in practice so that it can be run in a computer?*

An important tool for this last Pyatiletka problem could be the C++ code *Ripser* by Bauer [44], which allows for fast computation of the homology of Vietoris-Rips complexes.

5^{§4–5} Пятилетка V: Computational Hilbert 16th problem

Coming back to the introduction, we consider the understanding of the topology of real algebraic and semialgebraic sets as one of the motivations of computational semialgebraic geometry. The most general way in which an algebraic geometer understands a classification problem is by having an explicit list of objects’ types and a list of invariants that when computed indicates to which type in the list is the studied object equivalent. We generalize this notion to the computational setting. Although the definition below is only for isotopy types of hypersurfaces, it can be extended to more general settings easily.

Definition 5^{§4}1. *A computational classification of the isotopy type of hypersurfaces consists of the following three computable maps:*

(c) A map

$$\text{class} : \mathbb{N} \times \mathbb{N} \rightarrow \{\mathcal{A} \subseteq \mathbb{R}[X_k \mid k \in \mathbb{N}] \mid \#\mathcal{A} < \infty\}$$

such that for each (d, n) , $\text{class}(d, n) \subseteq \mathbb{R}[X_0, \dots, X_n]_d := \{f \in \mathbb{R}[X_0, \dots, X_n] \mid \deg f = d\}$ contains a representative of each isotopy class of real hypersurfaces of degree d in $n + 1$ homogeneous variables.

(i) A map

$$\text{idem} : \bigcup_{d,n} \{d\} \times \{n\} \times \mathbb{R}[X_0, \dots, X_n]_d \rightarrow \mathbb{R}[X_k \mid k \in \mathbb{N}]$$

such that for all $d, n \in \mathbb{N}$ and $f \in \mathbb{R}[X_0, \dots, X_n]_d$, $\text{idem}(d, n, f) \in \text{class}(d, n)$ with f and $\text{idem}(f)$ having the same isotopy type.

A *computational weak classification* of the isotopy types of hypersurfaces of the following three computable maps:

(c) A map

$$\text{class} : \mathbb{N} \times \mathbb{N} \rightarrow \{\mathcal{A} \subseteq \mathbb{R}[X_k \mid k \in \mathbb{N}] \mid \#\mathcal{A} < \infty\}$$

such that for each (d, n) , $\text{class}(d, n) \subseteq \mathbb{R}[X_0, \dots, X_n]_d := \{f \in \mathbb{R}[X_0, \dots, X_n] \mid \deg f = d\}$ contains a representative of each isotopy class of real hypersurfaces of degree d in $n + 1$ homogeneous variables.

(d) A map

$$\text{comp} : \bigcup_{d,n} \{d\} \times \{n\} \times \mathbb{R}[X_0, \dots, X_n]_d \times \mathbb{R}[X_0, \dots, X_n]_d \rightarrow \{0, 1\}$$

such that for all $d, n \in \mathbb{N}$ and $f, g \in \mathbb{R}[X_0, \dots, X_n]_d$, $\text{comp}(d, n, f, g) = 1$ iff f and g have the same isotopy type.

We should see that we are not interested in having the list anymore, but in just being able to produce the list and indicate the equivalent element in the list that can be produced. In other words, asking about the existence of efficient computational classifications is the same as wondering about the existence of systematic classification techniques for topology in real algebraic geometry.

In the case of curves, Orevkov and Kharlamov [307] prove that the number of isotopy types is

$$2^{\Theta(d^2)}.$$

For hypersurfaces (and even more general sets), Basu and Vorobjov [41] showed that the number of homotopy types is bounded by

$$N^{O(Nn)} = d^{O(d^n)}.$$

Based on this, we conjecture the following problem.

Pyatiletka problem XI. Is there a (weak) computational classification of the isotopy type of hypersurfaces such that class can be computed in $2^{d^{O(n)}}$ -time? And in parallel $d^{O(n)}$ -time?

Remark 5^{§4}1. We note that the statement of the problem does not contradict the results of Diatta and Lerario [153], since they prove that certain curves are exponentially rare, but this is expected from the number of isotopy types. ¶

However, the real dream is the following Pyatiletka problem.

Pyatiletka problem XII. *Is there a (weak) computational classification of the isotopy type of hypersurfaces that can be efficiently implemented in practice to classify currently unknown cases until now?*

An additional side quest of interest, given how little is known about algebraic curves in 3-dimensional space (see [410, 403, 402]) is the following problem, which might be easier than the two previous ones.

Pyatiletka problem XIII. *Find an algorithm computing the knot group of algebraic curves in \mathbb{S}^3 that, for a KSS random polynomial tuple $\mathbf{f} \in \mathcal{H}_{\mathbf{d}}[2]$, has run-time polynomial in D .*

Of course the Пятилетка program is ambitious, and most likely many of its goals will not be achieved. But when one ventures to look into the future, one should do it with the biggest possible ambition. The circumstances that might come may destroy our program, but for now, let me just say:

Пятилетка в четыре года!⁶

Further comments

Most of the exposition of Sections 5^{§1} and 5^{§2} is from [136]. The main exceptions are the computation of the probability tail for the local condition number of a KSS random polynomial and the exact constants in our probabilistic estimates. Regarding Han's covering algorithm, we followed the ideas in [213, 214], but many of the results and exposition in the corresponding section are novel.

⁶Five-year plan in four years!

My fuzzy mathematical idea was as follows:

*"We know that poly-nomials (**много**-члены) have a lot of (i.e. **много**) roots, so probably few-nomials (**мало**-члены) have only a few (i.e. **мало**) roots".*

Anatoli G. Kushnirenko, Letter to Professor Sottile



Real zeros of random fewnomials

A *fewnomial* is a polynomial with few terms. A *fewnomial system* with t exponent vectors is a polynomial system of equations

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_n = 0 \end{cases}$$

for which there is a subset $A \subseteq \mathbb{Z}^n$ of size t such that the system f is supported on A , i.e., each polynomial f_i is of the form

$$f_i := \sum_{\alpha \in A} f_{i,\alpha} X^\alpha.$$

In the complex case (see Theorem **F^{S1} 1**), the number of complex zeros in $(\mathbb{C}^*)^n$ of a generic¹ complex fewnomial system supported on A is $n! \text{vol}_n \text{conv}(A)$. In the real case (see Theorem **F^{S1} 5** and **F^{S1} 6**), the number of positive zeros² of a generic real fewnomial system can be bounded only in terms of t and n , independently of the set A on which the system is supported. This showcases the radical difference in behaviour between real and complex zeros.

Example F^{S0} 1. Consider the polynomial $aX^d + b$. Its generic complex form has d non-zero complex roots, but its real generic form has at most one positive root. Δ

Example F^{S0} 2. Consider the fewnomial system with 4 exponent vectors

$$\begin{cases} \alpha_1 + \beta_1 X + \gamma_1 Y + \delta_1 XYZ^d = 0 \\ \alpha_2 + \beta_2 X + \gamma_2 Y + \delta_2 XYZ^d = 0 \\ \alpha_3 + \beta_3 X + \gamma_3 Y + \delta_3 XYZ^d = 0. \end{cases}$$

¹In what follows ‘generic’ just means that the statement is true for all systems whose tuple of coefficients lies outside the zero set of some polynomial in t variables. It can also be interpreted in the weaker sense of measure theory, where the statement is true outside a set of measure zero with respect to the Lebesgue measure.

²By a positive zero $x \in \mathbb{R}^n$, we will mean a zero in the positive orthant \mathbb{R}_+^n .

We observe that the set $A_d := \{0, e_1, e_2, (1, 1, d)^t\}$ on which this system is supported is a simplex of volume $d/6$ and which does not contain any other integer points in its convex hull. Despite not having integer points different from the vertices, the same phenomenon happens. The complex generic system has d complex zeros in $(\mathbb{C}^*)^3$, while the real generic system has at most one positive zero. \triangle

As of today, the following is the biggest open question in fewnomial theory. Recall that a *nondegenerate* zero of a system f is a zero x of f such that $\bar{D}_x f$ is invertible.

Open problem J (Kushnirenko's conjecture). [268]. Does the number of nondegenerate positive solutions of a real fewnomial system with t exponent vectors and n variables have a bound of the form $\text{poly}(t)^{\text{poly}(n)}$? In other words, can we bound the number of nondegenerate zeros of a real fewnomial system by a function that is polynomial in the number of exponent vectors t and exponential in the number of variables n ?

This appendix presents the work of the author in [93] together with Peter Bürgisser and Alperen A. Ergür: a positive answer to the Open Problem J for random real fewnomial systems (Theorems F^{S3}1 and F^{S3}5). This result can be considered as the first step in the creation of a real random fewnomial theory.

First, we present the history and state-of-the-art in fewnomial theory; second, we introduce random real algebraic geometry and we present the techniques that we will be using; third, we state, discuss and prove the main probabilistic bound (Theorem F^{S3}1), providing also a slightly better bound for a restricted univariate bound (Theorem F^{S3}5); and fourth and last, we provide a list of questions pointing into possible future directions of random fewnomial theory.

Remark F^{S0}1. We note that despite their theoretical appeal, fewnomial systems appear very often in applications where dense polynomials are rare. Examples of these applications are, among many others, chemical reaction networks [130, 227, 296, 309, 310, 189] (see [156] for a survey) and statistics [159, 314]. \P

F^{S1} A history of real fewnomial theory

In 1975, Kushnirenko [269, 271]³ proved the first theorem counting the number of complex zeros of a complex fewnomial system. The importance of this bound is that in general it is a lot better than the one obtained by Bézout's theorem.

Theorem F^{S1}1 (Kushnirenko's theorem). [378; Theorems 1.1] Let f be a complex fewnomial system supported on $A \subseteq \mathbb{Z}^n$. Then the number of non-degenerate complex zeros of f in $(\mathbb{C}^*)^n$ is at most $n! \text{vol}_n \text{conv}(A)$. Moreover, for a generic complex fewnomial system the number of complex zeros of f in $(\mathbb{C}^*)^n$ is exactly $n! \text{vol}_n \text{conv}(A)$. \square

The next year, in 1976, Bernstein [51] extended this result to the case in which each polynomial of the system is supported on a different set. Recall that the *mixed volume* of

³We note that a purely analytic proof can be found in [270]. This proof applies to the more general sums of exponentials. Although Kushnirenko planned to publish this paper in the journal *Inventiones mathematicae*, he was not allowed by USSR authorities to do so. After that he became “upset and never tried to publish that paper again at home or abroad” [268].

convex polytopes $K_1, \dots, K_n \subseteq \mathbb{R}^n$, $\text{mixvol}_n(K_1, \dots, K_n)$, is the coefficient of $X_1 \cdots X_n$ in the n -homogeneous polynomial

$$\text{vol}_n(X_1K_1 + \cdots + X_nK_n)$$

or, equivalently,

$$\text{mixvol}_n(K_1, \dots, K_n) := \frac{\partial^n}{\partial X_1 \cdots \partial X_n} \text{vol}_n(X_1K_1 + \cdots + X_nK_n).$$

Note that $n! \text{vol}_n(K) = \text{mixvol}_n(K, \dots, K)$.

Theorem F^{S1} 2 (Bernstein's theorem). [378; Theorem 1.2] Let f be a complex fewnomial system such that each f_i is supported on $A_i \subseteq \mathbb{Z}^n$. Then the number of non-degenerate complex zeros of f in $(\mathbb{C}^*)^n$ is at most $\text{mixvol}_n(\text{conv}(A_1), \dots, \text{conv}(A_n))$. Moreover, for a generic complex fewnomial system the number of complex zeros of f in $(\mathbb{C}^*)^n$ is exactly $\text{mixvol}_n(\text{conv}(A_1), \dots, \text{conv}(A_n))$. \square

Later that same year, Berstein, Kushnirenko and Khovanskii would provide further insight in the proof of this theorem [52]. Because of this, the above results are known collectively as the BKK theorem.

F^{S1}-1 A fuzzy idea of Kushnirenko

In this moment of history, at the zenith of complex fewnomial theory, during the Summer of 1977, Kushnirenko had a fuzzy idea while he was writing a paper for the journal *Квант* for high school students of the Soviet Union. This fuzzy idea, which we quoted at the beginning of this chapter, was as follows:

“We know that poly-nomials (много-члены) have a lot of (i.e. много) root, so probably few-nomials (мало-члены) have only a few (i.e. мало) roots”.

This idea is nothing more than a language game in Russian, where Kushnirenko substituted the Russian term ‘много’ which means ‘many’ by its Russian opposite term ‘мало’ which means ‘few’. This is also the way that the term ‘fewnomial’ was born, since Kushnirenko just applied the same linguistic logic to English, substituting ‘poly’, meaning ‘many’, by its opposite ‘few’.

After having this idea, Kushnirenko realized quickly that the number of roots is “nothing but a characteristic of [the] topological complexity” and that the number of terms is “a characteristic of [the] algebraic complexity” [268]. Based on this, Kushnirenko formulated three conjectures⁴ that would lead to the creation of real fewnomial theory: [268]

Kushnirenko Hypothesis I. The topological complexity of an object defined by real-valued polynomials can be controlled by the complexity of the description of these

⁴Although the term in English is ‘conjecture’, Russian-speaking mathematicians usually use the term ‘hypothesis’ which is just a literal translation of the Russian term ‘гипотеза’. Despite this literal translation, this term is the equivalent term to ‘conjecture’ in the Russian mathematical language.

polynomials⁵ (such as the number of non-zero terms or the size of a straight-line program computing the polynomial) rather than by the degree or some other characteristic of polytopes that the polynomials are supported on.

Kushnirenko Hypothesis II. The number of nondegenerate positive zeros of a real fewnomial system can be bounded from above by a function depending only on the number of variables n and the number of exponent vectors t of the system.

Kushnirenko Hypothesis III. Given a fewnomial system f in n variables such that each f_i has at most t_i terms, the number of nondegenerate positive zeros of f is at most $\prod_{i=1}^n (t_i - 1)$. In particular, a fewnomial system f in n variables with t exponent vectors has at most $(t - 1)^n$ nondegenerate positive real zeros.

F^{S1}-2 Towards Kushnirenko hypotheses

At the moment that Kushnirenko coined the term fewnomial and formulated his conjectures, he didn't have any evidence that this would effectively be the case beyond the so-called Descartes' rule of signs.

Theorem F^{S1}3. (*Descartes' rule of signs*) [151; p. 42] and [2]. Let

$$f = a_1 X^{\alpha_1} + \cdots + a_t X^{\alpha_t}$$

be a non-zero fewnomial where $\alpha_1 < \dots < \alpha_t$. Then the number of positive roots of f is bounded by the number of sign changes in the sequence (a_1, \dots, a_t) . In particular, f has at most $t - 1$ positive roots. \square

Because of this, when Kushnirenko talked to Arnold at the next day of coming up with his three conjectures, Arnold advised Kushnirenko to “try to state and prove some simple partial case” [268]. Kushnirenko would come up with the following simplest case of his conjectures.

Kushnirenko Hypothesis IV. Let $f \in \mathbb{R}[X, Y]$ be a fewnomial with at most t terms and $g \in \mathbb{R}[X, Y]$ a polynomial of degree at most D . Then the number of nondegenerate positive zeros of the system

$$\begin{cases} f(x, y) = 0 \\ g(x, y) = 0 \end{cases}$$

is at most $b(t, D)$ for some universal function b .

In the fall of 1977, during one of their regular discussions, Kushnirenko discussed the above conjectures with the then 22-years-old mathematician Konstantin A. Sevastyanov (Константин А. Севастьянов), who was a PhD student of Arnold. Half a year later, in the Winter of 1978, Sevastyanov was able to prove Kushnirenko Hypothesis IV and to disprove the Kushnirenko Hypothesis III.

Theorem F^{S1}4 (Sevastyanov's theorem). *Kushnirenko Hypothesis III is false, and IV is true.* \square

⁵When Kushnirenko formulated his conjectures, he meant not only polynomials with integer exponent vectors, but with arbitrary real exponent vectors.

This is the “first crucial step” in real fewnomial theory [268]. Unfortunately, a few years later, Sevastyanov died in a tragic car-pedestrian accident in which the driver left the scene unidentified [268]. Because of this, the original counterexample and proof of Sevastyanov are lost to history.

We should note that Open Problem **J** is a robust version of Kushnirenko Hypothesis III. This version has not been disproved yet. A counterexample to the original Kushnirenko Hypothesis III was found independently much time later by Haas [212], but it is not a counterexample to the robust version.

Motivated by the original work of Sevastyanov, Khovanskii [256] would prove Kushnirenko Hypothesis II with an explicit upper bound.

Theorem F^{S1} 5 (Khovanskii’s theorem). [257; §3.14, Corollary 4]. *Let f be a fewnomial system in n variables with t exponent vectors. Then the number of nondegenerate positive zeros of f is bounded by*

$$2^{\binom{t-1}{2}}(n+1)^{t-1}.$$

□

Continuing this line of results, Khovanskii proved several more results covering also Kushnirenko Hypothesis I, with a bound similar to the one above for the sum of Betti numbers. All these results came together in Khovanskii’s book *Fewnomials* [257] in 1991, which would be later translated to Russian [258].

At this moment the theory of real fewnomials was a consolidated and established theory. This theory had and still has two major challenges: the Open Problem **J** and developing a multivariate generalization of Descartes’ rule. These two problems have been and are the driving force of the real fewnomial theory.

F^{S1}–3 After Khovanskii’s *Fewnomials*

We will divide history here in three parts: the first one, for the work related to Open Problem **J**; the second one, for the work related to Sevastyanov’s theorem (known before as Kushnirenko Hypothesis IV); and the third and last one, for the multivariate generalization of Descartes’ rule of signs.

Approaching Kushnirenko Hypothesis III

In 2002, Haas [212] gave a counterexample to Kushnirenko Hypothesis III by providing a pair of bivariate trinomials⁶ whose system had 5 nondegenerate positive zeros. We note that Kusnirenko Hypothesis III’s bound is 4. A year later, in 2003, Li, Rojas and Wang [277] showed that 5 is a bound for the number of nondegenerate positive zeros of such a bivariate trinomial system.

Later work has focused mainly on fewnomial systems in n variables with $n+k$ exponent vectors, where k is assumed to be constant. In 2006, Bertrand, Bihan and Sottile [53] provided non-trivial bounds for a restricted class of fewnomial systems when $k = 2$. Next year, Bihan [56] obtained a tight bound for the general case of $k = 2$.

⁶A trinomial is a fewnomial with three terms.

However, the biggest result in this direction was an improvement of Khovanskii's bound (Theorem $\mathbf{F}^{\$1}$ 5) by Bihan and Sottile [63]. We observe that under the above assumption of $t = n + k$, for fixed k , the obtained bound is polynomial in n .

Theorem $\mathbf{F}^{\$1}$ 6 (Bihan-Sottile theorem). [63] *Let f be a fewnomial system in n variables with t exponent vectors. Then the number of nondegenerate positive zeros of f is bounded by*

$$\frac{e^2 + 3}{4} 2^{\binom{t-n-1}{2}} n^{t-n-1}.$$

□

In the late 2000s, Bihan, Rojas and Sottile [61] generalized this bound to the number of connected components of a fewnomial hypersurface, and, later, Bihan and Sottile [64] to the sum of Betti numbers of such a hypersurface. In the 2010s, Bihan and Sottile [65] further generalized and significantly improved their bound by restricting their attention to a special class of structured fewnomial systems. More concretely, the class that they considered is formed by fewnomials such that the only common exponent vector to all of them is the exponent vector of the constant term.

Phillipson and Rojas [313] further studied the existing lower bound on the maximum number of positive roots and considered generalizations to the p -adic case. The latter continues a long sequence of work in p -adic and local fields fewnomial theory by Lenstra [276], Poonen [319], [338], Rojas [339], Avendaño and Ibrahim [17, 18], and Avendaño and Krick [19].

Bihan [57] classified maximal fewnomial systems in n variables with $n + 2$ exponent vectors, where a maximally positive fewnomial system is a fewnomial system with maximum number of positive roots among the fewnomial systems with the number of exponent vectors. Based on this classification, Bihan [57] proposed a conjecture about maximally positive fewnomial systems.

Recently, in 2018, there has been some progress in obtaining new lower bounds by Bihan, Santos and Spaenlehauer [62], based on a version of a Viro's method originally used by Sturmfels [385], and by El Hilany [172] for bivariate fewnomial systems with five monomials.

All this shows that major progress has still to be done towards further improving the bounds of Khovanskii and of Bihan and Sottile.

Revisiting the forgotten Sevastyanov's theorem

In 2009, Avendaño [20] proved that the number of real intersections of a fewnomial planar curve with t terms and a straight line is at most $6t - 4$. This can be considered a particular explicit case of Sevastyanov's theorem when $D = 1$.

In general, an explicit bound for the general case of Sevastyanov's theorem was given by Koiran, Portier and Tavenas [263], based on previous work in [264]. The latter work was motivated by a discovery of a deep connection between a certain class of algebraic circuits that use fewnomials and complexity theory, the so-called real τ -conjecture, by Koiran [262].⁷

Theorem $\mathbf{F}^{\$1}$ 7 (Koiran-Portier-Tavenas theorem). [263; Theorem 15] *Let $f \in \mathbb{R}[X, Y]$ be a fewnomial with at most t terms and $g \in \mathbb{R}[X, Y]$ a polynomial of degree at most D .*

⁷For a proof in a restricted setting, see [197].

Then the number of connected components of the zero set of the system

$$\begin{cases} f(x, y) = 0 \\ g(x, y) = 0 \end{cases}$$

is at most $O(D^3 t + D^2 t^3)$. \square

The theorem above becomes open if the second polynomial is also a fewnomial.⁸ Furthermore, the above bound might not be tight, as it is the case for $D = 1$ due to Avendaño's bound [20]. Recently, Bihan and El-Hilany [60] improved the latter bound to the tight upper bound $6t - 7$.

All this shows that even in the low-dimensional cases, Open Problem **J** remains a challenging problem.

A multivariate version of Descartes' rule of signs?

In 1996, Itenberg and Roy [231] conjectured a multivariate generalization of Descarte's rule of signs. Unfortunately, in 1998, Li and Wang [278] found a counterexample to their conjecture.

After this, more than ten year passed by before seeing some progress. In 2010, Avenaño [16] proved the optimality of Descarte's rule of signs in some sense. However, another ten years had to pass until a partial multivariate generalizations of the Descartes' rule of signs appeared.

In 2016, Müller, Feliu, Regensburger, Conradi, Shiu and Dickenstein [296; Theorem 1.5] proposed the first multivariate partial generalization of Descartes' rule of signs, which can deal with at most one zero. Interestingly, this generalization was grounded in the application of real fewnomial theory to chemical reaction networks. Later, Bihan and Dickenstein [58] gave a generalization for fewnomial systems in n variable with at most $n+2$ exponent vectors, and this year, Bihan, Dickenstein and Forsgård [59] have proposed a tight generalization for the latter case.

The above generalizations show that there is still a long path until a satisfactory general multivariate generalization of Descartes' rule of signs is obtained, but that there is hope that a multivariate generalization of Descartes' rule of signs might be possible in the near future.

F^{S2} Random real algebraic geometry

A common technique in real algebraic geometry to make a problem easier is to substitute the problem of finding a worst-case bound of a phenomenon by the problem of finding a bound for the expectation of a random version of the phenomenon. On the one hand, the second bound can be more informative when we consider polynomials coming from a probability distribution in some applied context. On the other hand, it might give some insight in the original problem and on how good the proposed worst-case bound is.

In our case, the technique is standard in random real algebraic geometry. The expectation of the number of zeros of a random real polynomial system is a central topic in this area. The main techniques go back to the seminal work of Edelman and Kostlan [166].

⁸The case of the intersection of a trinomial and a fewnomial can be found in [264; Corollary 16].

However, one should take into account the previous works by Littlewood and Offord [279], Kac [239, 240], Erdős and Offord [174], Kostlan [265], Shub and Smale [367] and many others (see [54] for a survey on the topic regarding the univariate case).

In the fewnomial setting, the idea of using random objects is not new. Rojas [338] and Malajovich and Rojas [283] already considered random real fewnomial systems, and Shiffman and Zelditch [363, 364] random complex fewnomial systems. However, none of their bounds depend solely on the number of exponent vectors. A big motivation to apply the probabilistic approach to the Kushnirenko Hypothesis III was its successful application by Briquel and Bürgisser [76] to the real τ -conjecture of Koiran [262].

We introduce the main probabilistic result that we will be using to compute the number of zeros. First, we introduce an auxiliary formula from integral geometry; second, we present and prove an integral formula for the expected number of positive zeros of a random function in a very general sense.

$\mathbf{F}^{\mathbb{S}^2}-1$ An intersection formula for random maximal spheres

Poincaré's formula allows us to compute the expected volume of the intersection of randomly placed smooth submanifolds. Recall that every m -dimensional smooth submanifold \mathcal{M} of the p -dimensional sphere \mathbb{S}^p inherits naturally a Riemannian structure from \mathbb{S}^p . This Riemannian structure induces a volume form on \mathcal{M} and so we can talk about the volume of \mathcal{M} which we denote by $\text{vol}_m \mathcal{M}$. Note that vol_0 is the cardinal, $\#$, of the set.

Theorem $\mathbf{F}^{\mathbb{S}^2}1$ (Poincaré's formula). [87; Thm. A.55]. *Let $\mathcal{M}, \mathcal{N} \subseteq \mathbb{S}^p$ be smooth submanifolds of dimensions m and n , respectively, such that $m + n \geq p$ and $\mathbf{u} \in O(p+1)$ be uniformly distributed with respect to the Haar probability measure. Then almost surely $\mathcal{M} \cap \mathbf{u}\mathcal{N}$ is a smooth submanifold of dimension $m + n - p$, and*

$$\mathbb{E}_{\mathbf{u} \in O(p+1)} \text{vol}_{m+n-p}(\mathcal{M} \cap \mathbf{u}\mathcal{N}) = \frac{m+n-p+1}{(m+1)(n+1)} \frac{\omega_{m+n-p+1}}{\omega_{m+1}\omega_{n+1}} \text{vol}_m \mathcal{M} \text{vol}_n \mathcal{N}.$$

□

The above formula implies immediately the following easy corollary.

Corollary $\mathbf{F}^{\mathbb{S}^2}2$. *Let $\mathcal{M} \subseteq \mathbb{S}^p$ be a smooth submanifold of dimensions m and $\mathbf{u} \in O(p+1)$ be uniformly distributed with respect to the Haar probability measure. Then, almost surely, $\mathcal{M} \cap \mathbf{u}\mathbb{S}^{p-1}$ is a smooth submanifold of dimension $m-1$, and*

$$\mathbb{E}_{\mathbf{u} \in O(p+1)} \text{vol}_{m-1}(\mathcal{M} \cap \mathbf{u}\mathbb{S}^{p-1}) = \frac{m\omega_m}{(m+1)\omega_{m+1}} \text{vol}_m \mathcal{M}.$$

Proof. Just recall that $\text{vol}_{p-1} \mathbb{S}^{p-1} = p\omega_p$.

□

The above formula applied inductively gives the following nice formula which is the one we will be using.

Proposition $\mathbf{F}^{\mathbb{S}^2}3$. [93; Proposition 2.1]. *Let \mathcal{M} be an m -dimensional smooth submanifold of \mathbb{S}^p and $\mathbf{u}_1, \dots, \mathbf{u}_m \in O(p+1)$ be independent and uniformly distributed with respect to the Haar probability measure. Then we have*

$$\mathbb{E}_{\mathbf{u}_1, \dots, \mathbf{u}_m \in O(p+1)} \#(\mathcal{M} \cap \mathbf{u}_1 \mathbb{S}^{p-1} \cap \dots \cap \mathbf{u}_m \mathbb{S}^{p-1}) = c_m \text{vol}_m(\mathbb{S}^p),$$

where $c_m = \frac{2}{(m+1)\omega_{m+1}}$.

□

Remark F^{S2}1. Our main reason to write the constant in the right-hand side of the identity in Proposition F^{S2}3 is that this constant will be irrelevant to our proof technique. Because of this, we hide its value to show that it is not important. ¶

Remark F^{S2}2. There are further generalizations of Poincaré's formula in more general ambient spaces by Howard [228] and Bürgisser and Lerario [94; Cor. A.3]. ¶

F^{S2}-2 An integral formula for the expected number of zeros

Suppose we are given a smooth and semialgebraic function

$$\varphi : \mathbb{R}_+^n \rightarrow \mathbb{R}^t$$

without any zeros in \mathbb{R}_+^n . Associated to this function, we can consider the random function

$$\begin{aligned} \mathfrak{f} : \mathbb{R}_+^n &\rightarrow \mathbb{R}^n \\ x \mapsto [\mathfrak{c}_{ij}] \varphi(x) &= \begin{pmatrix} \sum_{j=1}^t \mathfrak{c}_{1,j} \varphi_j(x) \\ \vdots \\ \sum_{j=1}^t \mathfrak{c}_{n,j} \varphi_j(x) \end{pmatrix} \end{aligned}$$

where $[\mathfrak{c}_{ij}] \in \mathbb{R}^{n \times t}$ is a Gaussian matrix. Our goal is to study the expectation of the number of nondegenerate zeros of \mathfrak{f} .

Example F^{S2}1. Let $\varphi : \mathbb{R}_+^n \rightarrow \mathbb{R}^t$ be the map given by

$$x \mapsto x^A := \begin{pmatrix} x^{A_1} \\ \vdots \\ x^{A_t} \end{pmatrix}, \quad (\mathbf{F.1})$$

where A_i is the i th row of A . Then \mathfrak{f} becomes a random polynomial and our problem reduces to estimate the number of zeros of a random polynomial. △

Consider the following random variable

$$N(\mathfrak{c}) := \#\{x \in \mathbb{R}_+^n \mid \mathfrak{f}(x) = 0, \det \bar{D}_x \mathfrak{f} \neq 0\}$$

taking values in $\mathbb{N} \cup \{\infty\}$, which counts the number of nondegenerate positive zeros of \mathfrak{f} . We now give a formula for its expectation that is the desired quantity.

Theorem F^{S2}4 (Edelman-Kostlan counting formula). [265; Thm. 3.3], [166; Theorem 7.1] and [93; Theorem 2.2]. In the above setting,

$$\mathbb{E}N = c_n \int_{\mathbb{R}_+^n} \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)} dx$$

where c_n is as in Proposition F^{S2}3 and $\psi : \mathbb{R}_+^n \rightarrow \mathbb{S}^{t-1}$ is the smooth map given by $\psi(x) = \frac{\varphi(x)}{\|\varphi(x)\|}$.

Proof. [93; Proof of Theorem 2.2]. We define the semialgebraic sets

$$V := \{x \in \mathbb{R}_+^n \mid \text{rank } \bar{D}_x \psi < n\} \text{ and } U := \{x \in \mathbb{R}_+^n \mid \text{rank } \bar{D}_x \psi = n\}.$$

Then we partition the open set V into the semialgebraic sets

$$U_k := \{x \in V \mid \#(\psi^{-1}(\psi(x)) \cap U) = k\},$$

for $k \in \mathbb{N} \cup \{\infty\}$. We associate with these semialgebraic sets the random variables

$$N_V(c) := \#\{x \in V \mid f(x) = 0, \det \bar{D}_x f \neq 0\}$$

and

$$N_k(c) := \#\{x \in U_k \mid f(x) = 0, \det \bar{D}_x f \neq 0\}.$$

Since $\{V, U_1, U_2, \dots, U_\infty\}$ form a partition of \mathbb{R}_+^n , it suffices to prove that

$$\mathbb{E} N_V = c_n \int_V \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)} dx, \quad (\mathbf{F. 2})$$

and that for all $k \in \mathbb{N} \cup \{\infty\}$,

$$\mathbb{E} N_k = c_n \int_{U_k} \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)} dx. \quad (\mathbf{F. 3})$$

The right-hand side of $(\mathbf{F. 2})$ is zero since $\text{rank}((\bar{D}_x \psi)^* \bar{D}_x \psi) = \text{rank } \bar{D}_x \psi < n$ for all $x \in V$. In order to prove $(\mathbf{F. 2})$, it is enough to show that $N_V = 0$, which means that every zero $x \in V$ of the system f is degenerate (i.e., $\bar{D}_x f$ is singular). By the definition of f , we have that $f(x) = [c_{ij}] \varphi(x)$ and so $\bar{D}_x f = [c_{ij}] \bar{D}_x \varphi$, for every $x \in \mathbb{R}_+^n$. By an explicit computation, we get

$$\bar{D}_x \psi = \frac{1}{\|\varphi(x)\|} \left(I - \psi(x) \psi(x)^* \right) \bar{D}_x \varphi. \quad (\mathbf{F. 4})$$

Suppose now that $x \in V$ satisfies $f(x) = 0$. By $(\mathbf{F. 4})$ and $\text{rank } \bar{D}_x \psi < n$, we either have $\text{rank } \bar{D}_x \varphi < n$, or there is some $v_x \in \mathbb{R}^n \setminus 0$ such that $\varphi(x) = \bar{D}_x \varphi v_x$. In the first case, $\bar{D}_x f = [c_{ij}] \bar{D}_x \varphi$ is singular. In the second case, $\bar{D}_x f v_x = [c_{ij}] \bar{D}_x \varphi v_x = [c_{ij}] \varphi(x) = f(x) = 0$, hence $v_x \in \ker \bar{D}_x f$ and $\bar{D}_x f$ is singular as well. We have thus shown that $(\mathbf{F. 2})$ holds.

For showing $(\mathbf{F. 3})$, let y_1, \dots, y_t be new variables. We associate to the functions $f_i := \sum_{j=1}^t c_{ij} \varphi_j(x)$ the linear forms $\ell_i := \sum_{j=1}^t c_{ij} y_j$ and denote by $Z(\ell_1, \dots, \ell_n)$ their zero set. So we have $f_i(x) = \ell_i(\varphi(x))$ for all x . By the definition of U_k , we have

$$\#\{x \in U_k \mid f(x) = 0\} = k \#(\psi(U_k) \cap Z(\ell_1, \dots, \ell_n)). \quad (\mathbf{F. 5})$$

We first consider the case where $\dim \psi(U_k) = n$ and $d \in \mathbb{N}$. Using the stratification of semialgebraic sets into manifolds (cf. [70; Chap. 9]), one shows that $\psi(U_k)$ contains a smooth n -dimensional submanifold M_k of \mathbb{S}^{t-1} such that $\dim(\psi(U_k) \setminus M_k) < n$. By Sard's Theorem (cf. [87; §A.2.4]), almost surely, the random hyperplanes $Z(\ell_1), \dots, Z(\ell_n)$ intersect the n -dimensional manifold M_k transversally,

$$\psi(U_k) \cap Z(\ell_1, \dots, \ell_n) = M_k \cap Z(\ell_1, \dots, \ell_n).$$

Moreover, all the zeros of $f(x) = 0$ in U_k are nondegenerate. With $(\mathbf{F. 5})$ we conclude that, for almost all ℓ_1, \dots, ℓ_n ,

$$N_k(c) = \#\{x \in U_k \mid f(x) = 0\} = k \#(\psi(U_k) \cap Z(\ell_1, \dots, \ell_n)) = k \#(M_k \cap Z(\ell_1, \dots, \ell_n)).$$

Therefore, applying Proposition F^{S2}3 to the manifold \mathcal{M}_k , we obtain

$$\mathbb{E} N_k = k \mathbb{E} \#(\mathcal{M}_k \cap Z(\ell_1, \dots, \ell_n)) = c_n k \text{vol}_n(\mathcal{M}_k).$$

Now we use that

$$\int_{U_k} \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)} dx = \int_{y \in \mathcal{M}_k} \#(\psi_k^{-1}(y) \cap U_k) d\mathcal{M}_k(y) = k \text{vol}_n(\mathcal{M}_k),$$

which follows from a slightly extended version of [87; Cor. 17.10]. (One can show that it does not matter that $\psi(U_k)$ may not be a manifold). This implies (F. 3).

In the case where $\dim \psi(U_k) < n$ and $d \in \mathbb{N}$, we write $\psi(U_k)$ as a union of smooth manifolds of dimension less than n . Then, using Sard's Theorem, we see that (F. 3) trivially holds in the form $0 = 0$.

To complete the proof, it suffices to show U_∞ is empty. By way of contradiction, assume that $x \in U_\infty$. By the Constant Rank Theorem [275; Theorem 4.12], the fiber $\psi^{-1}(\psi(x)) \cap U$ is a zero-dimensional subset of the open set U , since $\text{rank } D_p \psi = n$ for all $p \in U$. However, $\psi^{-1}(\psi(x)) \cap U$ is semialgebraic and hence finite, since any zero-dimensional semialgebraic set is finite. This contradicts $x \in U_\infty$, completing the proof. \square

Remark F^{S2}3. We note that our proof is different from the one in [265] and [166]. Our proof is more detailed than the one there and worked out in detail. \P

F^{S3} Probabilistic Kushnirenko Hypothesis III

We introduce the notion of random fewnomial system, which is the basis of our approach.

Definition F^{S3}1. Let $A \subseteq \mathbb{Z}^n$ be a subset and $\sigma: A \rightarrow \mathbb{R}_+$ be a map. The *random fewnomial system* with support A and system of variances σ is the random fewnomial system \mathfrak{f} given by

$$\begin{cases} \mathfrak{f}_1 := \sum_{\alpha \in A} \sigma(\alpha) c_{1,\alpha} X^\alpha \\ \vdots \\ \mathfrak{f}_m := \sum_{\alpha \in A} \sigma(\alpha) c_{1,\alpha} X^\alpha \end{cases}$$

where $c_{i,\alpha} \in \mathbb{R}$ are independent identically distributed (i.i.d.) Gaussian variables, i.e., $[x_{i,\alpha}]$ is a Gaussian matrix.

Remark F^{S3}1. The function $\sigma: A \rightarrow \mathbb{R}_+$ should be seen as assigning a different typical deviation to each one of the random coefficients of the system. In other words, the coefficients $\mathfrak{f}_{i,\alpha}$ of \mathfrak{f} are independent random variables such that $\mathfrak{f}_{i,\alpha} \sim N(0, \sigma(\alpha))$. Because of this, our probabilistic model for random fewnomial systems is very robust. \P

The following bound is the most important result of this appendix.

Theorem F^{S3}1. [93; Theorem 1.1]. Let $N(A, \sigma)$ be the random variable counting the number of nondegenerate positive zeros of the random fewnomial system \mathfrak{f} with support A and system of variances σ . Then

$$\mathbb{E} N(A, \sigma) \leq \frac{1}{2^{n-1}} \binom{t}{n},$$

for every $A \subseteq \mathbb{Z}^n$ of size $\leq t$ and every map $\sigma: A \rightarrow \mathbb{R}_+$. Further, if A affinely spans \mathbb{R}^n , then almost surely every positive zero of f is nondegenerate.

Remark F^{S3} 2. [93; Remark 1.2]. The above result holds for more general distributions. One only needs to assume that the random vectors

$$\mathbf{c}_i := (\mathbf{c}_{i,\alpha})_{\alpha \in A} \in \mathbb{R}^A$$

are independent and that for each one of them, $\mathbf{c}_i / \|\mathbf{c}_i\|$ is uniformly distributed on the unit sphere of \mathbb{R}^A . \blacksquare

Remark F^{S3} 3. We note that the obtained bound for the expectation in Theorem F^{S3} 1 is better than the bound of Kushnirenko Hypothesis III. Given the counterexample to this conjecture by Sevastyanov and Haas, we can jokingly say that “Kushnirenko Hypothesis III is generally true, although it will be sometimes false”. This is the reason behind the title of this section. \blacksquare

An important corollary of the above result is the following one. It shows that the usually studied fewnomial systems with $n + k$ exponent vectors have no zeros with very high probability, independently of the considered support and system of variances.

Corollary F^{S3} 2. [93; Remark 1.3]. Let k be a constant. Then

$$\lim_{n \rightarrow \infty} \sup_{\substack{A \subseteq \mathbb{Z}^n, \#A \leq n+k \\ \sigma: A \rightarrow \mathbb{R}_+}} \mathbb{E}N(A, \sigma) = 0.$$

In particular,

$$\lim_{n \rightarrow \infty} \sup_{\substack{A \subseteq \mathbb{Z}^n, \#A \leq n+k \\ \sigma: A \rightarrow \mathbb{R}_+}} \mathbb{P}(N(A, \sigma) = 0) = 1.$$

In other words, the probability that a random fewnomial system with $n + k$ exponent vectors has no positive nondegenerate zeros goes to one independently of the considered support and system of variance.

Proof. We just need to apply Theorem F^{S3} 1 and $\binom{n+k}{n} = \binom{n+k}{k}$. Since $\binom{n+k}{k}$ is a polynomial of degree k in n , it is clear that the right-hand side converges to zero as n goes to infinity. The last part follows from the fact that $N(A, \sigma)$ is a random variable with values in $\mathbb{N} \cup \{\infty\}$, and so

$$\mathbb{P}(N(A, \sigma) \geq 1) \leq \sum_{k=1}^{\infty} k \mathbb{P}(N(A, \sigma) = k) \leq \mathbb{E}N(A, \sigma),$$

which is a particular case of Markov’s inequality. \square

Remark F^{S3} 4. We note that both convergences are exponentially fast in n . Therefore, in fewnomial systems with only a few more exponent vectors than variables, positive zeros are rare. This shows that the fewnomial systems in n variables and with $n + k$ exponent vectors constructed by Bihan, Rojas and Sottile [61] and by Phillipson and Rojas [313] with at least $\lfloor 1 + \frac{n}{k-1} \rfloor^{k-1}$ roots for $n \geq k$ are probabilistically rare.

Moreover, let us note that $\mathbb{E}N(A, \sigma)$ is very small compared with the number of zeros of the explicit fewnomial systems with many zeros produced by Phillipson and Rojas [313]. This only points to the suspicion that the chosen probabilistic model might not be the best to produce fewnomial systems with many zeros. \blacksquare

We now turn our attention to the proof. First, we consider a special kind of systems that will be instrumental in the proof; and second, we give the proof of Theorem F^{S3}1. As a bonus, we show that the bound can be improved when $n = 1$ and when the system of variances is a constant map.

F^{S3}-1 Special systems with few terms

We prove a deterministic result (Lemma F^{S3}4) on the real zeros of a particular class of sparse systems that involve square roots and thus go slightly beyond our polynomial setting. This result will allow us to prove the following inequality of integrals that will be instrumental in the proof of Theorem F^{S3}1.

Proposition F^{S3}3. [93; Proposition 3.1]. Consider the function $g: \mathbb{R}_+^n \rightarrow \mathbb{R}_+$ defined by $g(x) := \left(\sum_{j=1}^m c_j^2 x^{2\beta_j} \right)^{\frac{1}{2}}$, where $\beta_1, \dots, \beta_m \in \mathbb{Z}^n$ and $c_1, \dots, c_m > 0$. Take $\alpha_1, \dots, \alpha_n \in \mathbb{Z}^n$ and $\sigma_1, \dots, \sigma_n > 0$, and define the functions $\varphi: \mathbb{R}_+^n \rightarrow \mathbb{R}_+^{n+1}$ and $\psi: \mathbb{R}_+^n \rightarrow \mathbb{S}^n$ by

$$\varphi(x) := \begin{pmatrix} \sigma_1 x^{\alpha_1} \\ \vdots \\ \sigma_n x^{\alpha_n} \\ g(x) \end{pmatrix} \text{ and } \psi(x) := \frac{\varphi(x)}{\|\varphi(x)\|}.$$

Then we have

$$c_n \int_{\mathbb{R}_+^n} \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)} dx \leq \frac{1}{2^{n-1}}$$

where c_n is as in Proposition F^{S2}3.

For proving Proposition F^{S3}3 we need the following lemma.

Lemma F^{S3}4. [93; Lemma 3.2]. Let $g(x)$ be the function from Proposition F^{S3}4, but with $\beta_1, \dots, \beta_m \in \mathbb{R}^n$. Moreover, let $\alpha_1, \dots, \alpha_n \in \mathbb{R}^n$. Then, for any non-singular $[\lambda_{ij}] \in \mathbb{R}^{n \times n}$, the system

$$\sum_{j=1}^n \lambda_{ij} x^{\alpha_j} = g(X), \quad (i \in [n]),$$

has at most two nondegenerate zeros in \mathbb{R}_+^n .

Proof of Proposition F^{S3}3. We begin with the following general observation: let v_1, \dots, v_n, w be independent Gaussian vectors in \mathbb{R}^n . Then

$$\sum_{\varepsilon \in \{-1, 1\}^n} \mathbb{P}(w \in \text{cone}(\varepsilon_1 v_1, \dots, \varepsilon_n v_n)) = \mathbb{P}(w \in \text{span}(v_1, \dots, v_n)) = 1.$$

By symmetry, the probabilities do not depend on ε , so that we get

$$\mathbb{P}(w \in \text{cone}(v_1, \dots, v_n)) = 2^{-n}. \tag{F . 6}$$

Suppose now that $[x_{ij}] \in \mathbb{R}^{n \times (n+1)}$ is a Gaussian matrix. If the random system

$$x_{i0} g(X) + \sum_{j=1}^n x_{ij} \sigma_j X^{\alpha_j} = 0, \quad (i \in [n]), \tag{F . 7}$$

has a positive solution, then $-\mathfrak{x}_0$ is a positive linear combination of $\mathfrak{x}_1, \dots, \mathfrak{x}_n$ and so

$$-\mathfrak{x}_0 \in \text{cone}(\mathfrak{x}_1, \dots, \mathfrak{x}_n).$$

The probability of the latter is at most 2^{-n} by (F . 6). Hence the probability that the random system (F . 7) has a positive root is bounded also by 2^{-n} .

By Lemma F^{S3} 4, the maximum number of positive nondegenerate zeros is at most two. Therefore, the expected number of nondegenerate solutions of (F . 7) is bounded by $2 \cdot 2^{-n}$. The assertion follows now by Theorem F^{S2} 4. \square

We recall the following fact about changing variables that we will use in the proof of the lemma. Suppose $A \in \mathbb{R}^{n \times n}$ is an invertible matrix. Then

$$\begin{aligned} \mathbb{R}_+^n &\rightarrow \mathbb{R}_+^n \\ x &\mapsto x^A, \end{aligned} \tag{F . 8}$$

where x^A was given in (F . 1), is a diffeomorphism. Indeed, via the group isomorphism $\mathbb{R}^n \rightarrow \mathbb{R}_+^n$, $y \mapsto \exp(y)$ and its inverse $\mathbb{R}_+^n \rightarrow \mathbb{R}^n$, $x \mapsto \ln x$, this turns (F . 8) into the linear isomorphism $y \mapsto Ay$.

Proof of Lemma F^{S3} 4. We divide into cases, depending on the rank k of the linear span of $\alpha_1, \dots, \alpha_n$.

In the case $k = n$, using the transformation in (F . 8), we can assume without loss of generality that $\alpha_1, \dots, \alpha_n$ is the standard basis of \mathbb{R}^n ; thus we study the positive zeros of a system

$$\sum_{j=1}^n \lambda_{ij} x_j = g(x), \quad (i \in [n]). \tag{F . 9}$$

Subtracting the n th equation from the others gives the system $\sum_{j=1}^n (\lambda_{ij} - \lambda_{nj}) x_j = 0$, ($i \in [n-1]$), which has a one-dimensional solution space $\mathbb{R}\xi$, for some nonzero $\xi \in \mathbb{R}^n$. We can assume that $\xi \in \mathbb{R}_+^n$ since otherwise the system (F . 9) has no solution in \mathbb{R}_+^n .

Plugging in $x = s\xi$ with unknown $s \in \mathbb{R}_+$ into (F . 9), we obtain by squaring the first equation

$$s^2 \left(\sum_{j=1}^m \lambda_{1j} \xi_j \right)^2 - \sum_{j=1}^m c_j^2 \xi^{2\beta_j} s^{2\gamma_j} = 0,$$

where γ_j denotes the sum of the components of β_j . We apply now Descartes' rule to this univariate polynomial in s (with possibly real exponents). Since the sequence of coefficients has at most two sign changes, there are at most two positive real zeros, provided the polynomial does not vanish altogether. In the latter case, all the γ_j equal 1 and we have $g(s\xi) = sg(\xi)$. The system (F . 9) then becomes the system $s \sum_j \lambda_{ij} \xi_j = sg(\xi)$ in s , for $i = 1, \dots, n$, whose solution set is either empty or all of \mathbb{R}_+ . But then all solutions of the original system (F . 9) are degenerate.

In the case $k < n$, using the transformation in (F . 8), we can assume without loss of generality that $\alpha_1, \dots, \alpha_n$ is contained in $\mathbb{R}^k \times 0^{n-k}$. Subtracting the n th equation of the original system from the others gives the system $\sum_{j=1}^n (\lambda_{ij} - \lambda_{nj}) X^{\alpha_j} = 0$, ($i \in [n-1]$). Since

x^{α_j} only depends on x_1, \dots, x_k , this is a system of $n - 1$ equations in k variables, having n exponent vectors.

If $k < n - 1$, this system only has degenerate solutions and we are done. If $k = n - 1$, we are faced with a system of $n - 1$ polynomials in $n - 1$ variables having n exponent vectors. This system can be put in the form

$$X^{\alpha_i} = a_i X^{\alpha_n}, \quad (i \in [n-1]),$$

after reordering the α_i ; if necessary, since $[\lambda_{ij} - \lambda_{nj}]$ has to contain a non-singular maximal minor, because $[\lambda_{ij}]$ is non-singular. The above system can be turned into

$$X^{\alpha_i - \alpha_n} = a_i, \quad (i \in [n-1]),$$

which has a unique nondegenerate positive solution if $\{\alpha_1 - \alpha_n, \dots, \alpha_{n-1} - \alpha_n\}$ has rank $n - 1$ or none otherwise. In the latter case, we are done; in the former case, let ξ be the unique nondegenerate positive real solution ξ of the system. Substituting $(\xi_1, \dots, \xi_{n-1}, x_n)$ with unknown x_n in the last equation, and using $\alpha_{j,n} = 0$, we obtain after squaring

$$\left(\sum_{j=1}^n \lambda_{1j} \xi_1^{\alpha_{j,1}} \cdots \xi_{n-1}^{\alpha_{j,n-1}} \right)^2 - \sum_{j=1}^m c_j^2 \xi_1^{2\beta_{j,1}} \cdots \xi_{n-1}^{2\beta_{j,n-1}} x_n^{2\beta_{j,n}} = 0.$$

By Descartes' rule, this polynomial in x_n (with possibly real exponents) has at most two positive zeros, unless it vanishes altogether, in which case all solutions of the original system are degenerate.

Summarizing, we have shown that in all cases, the system has at most two nondegenerate solutions. \square

Remark F^{S3} 5. The bound in Lemma F^{S3} 4 is optimal. The system

$$\begin{cases} X_1 = \sqrt{1 + \frac{1}{5} X_1^2 X_2^2} \\ X_2 = \sqrt{1 + \frac{1}{5} X_1^2 X_2^2} \end{cases}$$

has exactly two positive nondegenerate zeros. \P

F^{S3}-2 Proof of Theorem F^{S3} 1

We fix a support $A \subseteq \mathbb{Z}^n$ of cardinality t and a system of variances $\sigma: A \rightarrow \mathbb{R}_+$. Similarly to Example F^{S2} 1, we consider the map

$$\begin{aligned} \varphi_{A,\sigma}: \mathbb{R}_+^n &\rightarrow \mathbb{R}_+^A \\ x &\mapsto (\sigma(\alpha)x^\alpha)_{\alpha \in A}, \end{aligned} \tag{F . 10}$$

together with its scaled version

$$\begin{aligned} \psi_{A,\sigma}: \mathbb{R}_+^n &\rightarrow \mathbb{S}(\mathbb{R}^A) \\ x &\mapsto \frac{\varphi_{A,\sigma}(x)}{\|\varphi_{A,\sigma}(x)\|}, \end{aligned}$$

which takes values in the unit sphere.

As all the functions are semialgebraic, we can apply Theorem **F^{§2} 4**, which implies that

$$\mathbb{E} N(A, \sigma) = c_n \int_{\mathbb{R}_+^n} \sqrt{\det((\bar{D}_x \psi_{A,\sigma})^* \bar{D}_x \psi_{A,\sigma}))} dx.$$

We abbreviate $M(x) := \bar{D}_x \psi_{A,\sigma}$. For $I \subseteq A$ with $|I| = n$ we denote by $M_I(x)$ the square submatrix of $M(x)$ obtained by selecting the rows with index in I . The Cauchy-Binet formula [77; Part I, Ch. 4, §6], combined with the elementary inequality $\|u\|_2 \leq \|u\|_1$, gives

$$\sqrt{\det(M(x)^* M(x))} = \left(\sum_{|I|=n} (\det M_I(x))^2 \right)^{\frac{1}{2}} \leq \sum_{|I|=n} |\det M_I(x)|. \quad (\text{F . 11})$$

Therefore,

$$\mathbb{E} N(A, \sigma) \leq \sum_{|I|=n} c_n \int_{\mathbb{R}_+^n} |\det M_I(x)| dx.$$

It suffices to prove that

$$c_n \int_{\mathbb{R}_+^n} |\det M_I(x)| dx \leq \frac{1}{2^{n-1}}, \quad (\text{F . 12})$$

since there are $\binom{t}{n}$ summands.

For showing this, we put $I = \{\alpha_1, \dots, \alpha_n\}$ and $\sigma_i := \sigma(\alpha_i)$. We then apply Proposition **F^{§3} 3** to the function $\varphi: \mathbb{R}_+^n \rightarrow \mathbb{R}_+^{n+1}$ defined by

$$\varphi(x) := \begin{pmatrix} \sigma_1 x^{\alpha_1} \\ \vdots \\ \sigma_n x^{\alpha_n} \\ g(x) \end{pmatrix}, \text{ where } g(x) := \left(\sum_{\alpha \in A \setminus I} \sigma(\alpha)^2 x^{2\alpha} \right)^{\frac{1}{2}}.$$

Note that

$$\|\varphi(x)\|^2 = \sum_{i=1}^n \sigma_i^2 x^{2\alpha_i} + \sum_{\alpha \in A \setminus I} \sigma(\alpha)^2 x^{2\alpha} = \sum_{\alpha \in A} \sigma(\alpha)^2 x^{2\alpha} = \|\varphi_{A,\sigma}(x)\|^2.$$

Moreover, the i th component of the scaled function $\psi(x) := \varphi(x)/\|\varphi(x)\|$ satisfies for $1 \leq i \leq n$,

$$\psi_i(x) = \frac{\varphi_i(x)}{\|\varphi(x)\|} = \frac{\sigma_i x^{\alpha_i}}{\|\varphi_{A,\sigma}(x)\|},$$

which is the α_i th component of $\psi_{A,\sigma}(x)$. Therefore, $M_I(x) = [\partial_{x_j} \psi_i]_{i,j \leq n}$. The Cauchy-Binet formula implies that

$$|\det M_I(x)| \leq \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)}.$$

Proposition **F^{§3} 3** gives

$$c_n \int_{\mathbb{R}_+^n} \sqrt{\det((\bar{D}_x \psi)^* \bar{D}_x \psi)} dx \leq \frac{1}{2^{n-1}}.$$

Combining the above shows **(F . 12)** and completes the proof of Theorem **F^{§3} 1**. □

F^{S3-3} The case of one fewnomial

The case of a univariate polynomial is always of special interest. In this special case, we are able to provide a better bound for the case in which all typical deviations of the coefficients are the same.

Theorem F^{S3} 5. [93; Theorem 1.4]. *Let $A \subseteq \mathbb{Z}$ and $\mathbf{1} : A \rightarrow \mathbb{R}_+$ be the constant map taking the value 1. Then*

$$\mathbb{E} N(A, \mathbf{1}) \leq \frac{2}{\pi} \sqrt{t} \ln t.$$

Remark F^{S3} 6. The above bound looks like a mixture of the bound of Kac [239] and the bound of Kostlan [265]⁹. Both of these bounds are for $A = \{0, \dots, d\}$, i.e., the dense case, but Kac considered the constant system of variances $\mathbf{1}$ and Kostlan the map $a \mapsto \binom{d}{a}^{\frac{1}{2}}$. In Kac's case, the bound is $(\pi^{-1} + o(1)) \ln d$, and, in Kostlan's case, $\frac{1}{2} \sqrt{d}$. In this way, the above bound in Theorem F^{S3} 5 looks like the product of these two bounds. ¶

Proof. Note that $\mathbf{g} := \mathbf{f}(1/x)$ is a random Laurent polynomial with support $-A$, whose expected number of zeros in $(0, 1)$ is precisely the expected number of zeros of \mathbf{f} in $(1, \infty)$. Therefore, it is enough to bound the expected number of zeros $\mathbb{E} N_{(0,1)}(A, \mathbf{1})$ in the interval $(0, 1)$ by $\frac{1}{\pi} t^{1/2} \ln t$ for a random polynomial with arbitrary support A of size t . Moreover, since multiplying by x^k does not alter the number of zeros in $(0, 1)$ of a polynomial, we can assume without loss of generality that $0 \in A \subseteq \mathbb{N}$.

We observe that Theorem F^{S2} 4 holds for any open subset of \mathbb{R}_+^n with the same proof. Hence

$$\mathbb{E} N_{(0,1)}(A, \mathbf{1}) = \frac{1}{\pi} \int_0^1 \|\psi'(x)\| dx$$

where $\varphi(x) = (x^\alpha)_{\alpha \in A}$ and $\psi := \varphi/\|\varphi\|$. By (F . 4), $\psi'(x) = \|\varphi(x)\|^{-1} P_x \varphi'(x)$ where P_x is the orthogonal projection onto the orthogonal complement of $\psi(x)$, and so

$$\|\psi'(x)\| = \frac{\|P_x \varphi'(x)\|}{\|\varphi(x)\|} \leq \frac{\|\varphi'(x)\|}{\|\varphi(x)\|}.$$

Hence,

$$\|\psi'(x)\| \leq \sqrt{t} \frac{\|\varphi'(x)\|_1}{\|\varphi(x)\|_1} = \sqrt{t} (\ln \|\varphi(x)\|_1)', \quad (\text{F . 13})$$

using the standard inequalities between the 1-norm and 2-norm in \mathbb{R}^t . Finally, we obtain by integrating

$$\int_0^1 \|\psi'(x)\| dx \leq \sqrt{t} (\ln \|\varphi(1)\|_1 - \ln \|\varphi(0)\|_1) \leq \sqrt{t} \ln t,$$

since $0 \in A \subseteq \mathbb{N}$, which gives the desired result. □

⁹Although the bound in the univariate case is attributed to Shub and Smale [367], it was Kostlan in [265] who did the univariate case first. Shub and Smale proved the general multivariate case in [367].

F^{S4} A random real fewnomial theory?

As of today, Theorems **F^{S3}1** and **F^{S3}5** are the only existing results in what we may call random real fewnomial theory. However, these two results open more doors than what the number of doors they close. We now pose some conjectures, speculations and questions, which should be seen as an invitation to develop a random real fewnomial theory.

F^{S4}-1 Probabilistic Kushnirenko Hypothesis I

Kushnirenko Hypothesis I states that the topological complexity of the zero set $\mathcal{Z}_+(\mathbf{f})$ of a fewnomial system should be bounded by a function on the number of equations q , the number of variables n and the number of exponent vectors t . One can find precise bounds for this in the works of Khovanskii [257], Bihan, Rojas and Sottile [61], and Bihan and Sottile [64]. The latter bounds have an extra 2^n factor that do not appear in the zero-dimensional bound of Theorem **F^{S1}6**. Based on Theorem **F^{S3}1** and this extra factor we propose the following conjecture, where we just add the extra factor 2^n to the bound.

Hypothesis F . I. *Let \mathbf{f} be a random fewnomial polynomial in n variables with t exponent vectors. Then*

$$\mathbb{E}\beta_\Sigma(\mathcal{Z}_+(\mathbf{f})) \leq \binom{t}{n},$$

where β_Σ is the sum of the Betti numbers of $\mathcal{Z}_+(\mathbf{f}) := \{x \in \mathbb{R}_+^n \mid \mathbf{f}(x) = 0\}$.

Since we can see the n in 2^{n-1} as the codimension in the zero-dimensional case and we are conjecturing that this factor disappears when the codimension is one, we also make the following conjecture that generalizes the one above for arbitrary codimension q .

Hypothesis F . II. *Let \mathbf{f} be a random fewnomial system with q equations in n variables with t exponent vectors. Then*

$$\mathbb{E}\beta_\Sigma(\mathcal{Z}_+(\mathbf{f})) \leq \frac{1}{2^{q-1}} \binom{t}{n},$$

where β_Σ is the sum of the Betti numbers of $\mathcal{Z}_+(\mathbf{f}) := \{x \in \mathbb{R}_+^n \mid \mathbf{f}(x) = 0\}$.

An alternative generalization of Theorem **F^{S3}1** can be obtained if we substitute cardinality by volume when we pass to smaller codimensions. Unfortunately, we have to be careful, since a naive conjecture would trivially be false as shown by a random linear system. This is why we restrict the conjecture to the unit cube.

Hypothesis F . III. *Let \mathbf{f} be a random fewnomial system with q equations in n variables with t exponent vectors. Then*

$$\mathbb{E} \text{vol}_{n-q}(\mathcal{Z}_+(\mathbf{f}) \cap (0,1)^n) \leq \frac{1}{2^{q-1}} \binom{t}{n},$$

where vol_{n-q} is the $(n-q)$ -volume of $\mathcal{Z}_+(\mathbf{f}) := \{x \in \mathbb{R}_+^n \mid \mathbf{f}(x) = 0\}$.

Of course, the above conjectures might be false as stated. However, we expect the bounds to be polynomial in t . We state precise bounds as they are usually more motivating than finding a vague polynomial bound.

F^{S4}-2 How does $\mathbb{E}N(A, \sigma)$ depend on the support (A, σ) ?

The bound in Theorem F^{S3}1 is universal in the sense that it does neither depend on neither the support A nor on the system of variances σ . A natural question is how does the expectation depend on these parameters. Based on the experience with dense systems, we expect such a variation to occur.

Motivated by the fact that the number of non-zero complex roots grows when increasing the support, we conjecture the following.

Hypothesis F . IV. Let $A, B \subseteq \mathbb{Z}^n$ be such that $A \subseteq B$ and $\sigma : B \rightarrow \mathbb{R}_+$ be a map. Then

$$\mathbb{E}N(A, \sigma|_A) \leq \mathbb{E}N(B, \sigma).$$

In dense systems, the system of variances affects enormously how the zeros of a system are distributed. We expect a similar behaviour in fewnomial systems. Because of this, we propose the following conjecture regarding lower and upper bounds. They are motivated slightly by Kac's result [239].

Hypothesis F . V.

$$\inf_{\substack{A \subseteq \mathbb{Z}^n, \#A \leq t \\ \sigma : A \rightarrow \mathbb{R}_+}} \mathbb{E}N(A, \sigma) = \Theta\left(\frac{1}{2^{n-1}} \binom{\ln t}{n}\right)$$

and

$$\sup_{\substack{A \subseteq \mathbb{Z}^n, \#A \leq t \\ \sigma : A \rightarrow \mathbb{R}_+}} \mathbb{E}N(A, \sigma) = \Theta\left(\frac{1}{2^{n-1}} \binom{t}{n}\right),$$

where $f(t, n) = \Theta(g(t, n))$ means that there are universal constants $L, L' > 0$ such that $Lg(t, n) \leq f(t, n) \leq L'g(t, n)$.

A proof analysis of Theorem F^{S3}1 reveals that $\binom{t}{n}$ can be substituted by the cardinal of

$$\mathcal{B}_n(A) := \{X \subseteq A \mid \#X = n, \mathbb{R}^n = \text{span } X\},$$

which is the set of bases of \mathbb{R}^n contained in A . This might point to a connection between weighted matroids and random real fewnomial theory, since (\mathcal{A}, σ) can be seen as a linear representation of an integer linear matrix. This motivates the following question.

Open problem K. Can $\mathbb{E}N(A, \sigma)$ be related to a characteristic of the weighted matroid associated to (A, σ) ?

In Theorem F^{S3}5, we have shown that when the system of variances is constant we can improve the existing upper bound for the univariate case. This motivates us to formulate the following conjecture.

Hypothesis F . VI. Let $A \subseteq \mathbb{Z}^n$ and $\sigma : A \rightarrow \mathbb{R}_+$ a map. Then for some constant $C > 0$,

$$\mathbb{E}N(A, \sigma) \leq \left(C\sqrt{t} \ln t\right)^n.$$

F^{S4}-3 Bounds for more general fewnomial systems?

We note that the exponent vectors of a fewnomial system can be allowed to be real vectors and not just integer vectors. If one is able to drop the semialgebraic hypothesis from Theorem **F^{S2} 4**, the following should hold.

Hypothesis F. VII. Let $A \subseteq \mathbb{R}^n$ be such that $\#A \leq t$ and $\sigma : A \rightarrow \mathbb{R}_+$ be a map. Then

$$\mathbb{E}N(A, \sigma) \leq \frac{1}{2^{n-1}} \binom{t}{n}.$$

Further, the used techniques don't seem to rely too much on the fact that we are working with polynomials. Moreover, many results of Khovanskii [257] hold for a more general class of functions known as Pfaffian. Because of this, we propose the following conjecture.

Hypothesis F. VIII. Let $\varphi_1, \dots, \varphi_t : (0, 1)^n \rightarrow \mathbb{R}$ be Pfaffian functions such that the map

$$\varphi : x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_n(x) \end{pmatrix}$$

is a smooth submersion and has no zeros. Let \mathfrak{f} be the random system given by

$$\mathfrak{f} = [\mathfrak{c}_{ij}] \varphi$$

where $[\mathfrak{c}_{ij}] \in \mathbb{R}^{n \times t}$ is a Gaussian matrix. Then there is a constant $C > 0$ such that

$$\mathbb{E} \# (\mathcal{Z}(\mathfrak{f}) \cap (0, 1)^n) \leq \frac{C}{2^{n-1}} \binom{t}{n},$$

where $\mathcal{Z}(\mathfrak{f})$ is the zero set of \mathfrak{f} .

We conclude by noting that we have imposed the same support to all polynomials in our random fewnomial systems. There is a wider class of fewnomial systems where we allow a different supports for each one of the polynomials. Following the line of the Open Problem **K**, we propose the following conjecture.

Hypothesis F. IX. Let $A_1, \dots, A_n \subseteq \mathbb{R}^n$ and $\sigma_1 : A_1 \rightarrow \mathbb{R}_+, \dots, \sigma_n : A_n \rightarrow \mathbb{R}_+$. Consider the random \mathfrak{f} whose i th component is given by

$$\mathfrak{f}_i := \sum_{\alpha \in A_i} \sigma_i(\alpha) \mathfrak{c}_{i,\alpha}$$

where the $\mathfrak{c}_{i,\alpha}$ are i.i.d. Gaussian variables. Consider also the random variable

$$N(A_1, \dots, A_n, \sigma_1, \dots, \sigma_n)(\mathfrak{c}) := \{x \in \mathbb{R}_+^n \mid \mathfrak{f}(x) = 0, \text{rank } \bar{D}_x \mathfrak{f} = n\}$$

that counts the number of nondegenerate positive zeros of \mathfrak{f} . Then

$$\mathbb{E}N(A_1, \dots, A_n, \sigma_1, \dots, \sigma_n) \leq \frac{1}{2^{n-1}} \#\mathcal{B}_n(A_1, \dots, A_n)$$

where $\mathcal{B}_n(A_1, \dots, A_n)$ is the set of bases B of \mathbb{R}^n such that for each i , $A_i \cap B$ has exactly one element.

Further comments

Almost all of the statements and proofs here are taken literally from [93] with minimal changes. The main additions of this appendix to [93] are a better historical overview, which was clearly lacking in the original paper; and the final set of problems and questions that points to a possible future of random real fewnomial theory.

The core ideas regarding random real algebraic geometry can be found mainly in [166]. However, the main trick of the proof of Theorem **F^{S3}1** is an application of the Cauchy-Binet inequality which reduces a general bounding problem to a really specific family of systems. The combinatorial flavour of this technique can make one suspect that there is something deeper behind this proof.

When it was my turn, I got up and said, “I’m sorry; I hadn’t realized that the official language of the Brazilian Academy of Sciences was English, and therefore I did not prepare my talk in English. So please excuse me, but I’m going to have to give it in Portuguese.”

Richard P. Feynman, Surely You’re Joking, Mr. Feynman!



¿Cómo computar la “forma” de un conjunto semialgebraico?

En este apéndice, trataré de describir de una forma sencilla los resultados principales de esta tesis en castellano para un público no especialista. Por supuesto, es imposible hacer esto sin sacrificar detalles y precisión. Mi intención no es otra que transmitir una imagen gráfica de en qué ha consistido esta tesis. Los lectores no deben tratar de entender cada palabra o frase de este escrito, sino tratar de obtener una visión general.

El tema principal de esta tesis doctoral es el cálculo numérico de grupos de homología de conjuntos semialgebraicos. Hemos nombrado tres conceptos: cálculo numérico, grupos de homología y conjuntos semialgebraicos. El último es el objeto en el que estamos interesados, el segundo la propiedad qué nos interesa conocer y el tercero la acción que queremos ejercer. Por esto mismo, explicaré los términos en el orden inverso en el que están listados.

Por simplicidad explicaré como funciona todo en el plano, pero es importante notar que en matemáticas los objetos en el plano no son más que casos particulares de objetos n -dimensionales con n un número arbitrario. Mientras que en física se conforman con cuatro dimensiones o con las 10, 11 o 27 de la teoría de cuerdas, en matemáticas se considera un número arbitrario de dimensiones y se estudian las propiedades generales del espacio. Esto no es sólo interesante desde el punto de vista teórico, sino también desde el punto de vista práctico, porque si un modelo de las ciencias naturales tiene 13, 25 o 123 parámetros, muchas veces es útil considerar el modelo como un objeto dentro de un espacio con 13, 25 o 123 dimensiones.

M^{\$1} Conjuntos semialgebraicos

Los conjuntos semialgebraicos son una clase de conjuntos que se pueden describir con polinomios y las operaciones usuales de teoría de conjuntos. Para mostrar su generalidad, dejadme indicar que la image en la Figura M^{\$1}1 es un conjunto semialgebraico.

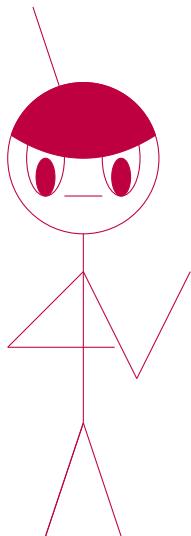


Figura **M\$1 1**: Un conjunto semialgebraico complicado

Recordemos que un polinomio no es más que una expresión que se puede obtener sumando y multiplicando números y variables, en nuestro caso X e Y. Consideraremos un polinomio en particular,

$$f := X^7 - 325X^2Y^5 + 1789XY - 4.$$

Para nosotros lo más importante de un polinomio es que es una regla que asigna valores numéricos a listas de números. Por ejemplo, podemos considerar el valor de f en $(0, 0)$, $(25, -12)$ y $(-7, 0)$, con lo que obtenemos

$$f(0, 0) = -4, f(25, -12) = 56646978921 \text{ y } f(-7, 0) = -823547.$$

Para nuestros conjuntos semialgebraicos, nos interesan los puntos segun el signo del polinomio, esto es, según el valor del polinomio en el punto sea cero, positivo o negativo.

De esta forma, los conjuntos semialgebraicos atómicos son conjuntos semialgebraicos que se pueden describir como

$$p = 0, p \neq 0, p \geq 0, p > 0, p \leq 0 \text{ o } p < 0$$

para algún polinomio p . Y los conjuntos semialgebraicos generales son los que se obtienen de estos mediante uniones, intersecciones y complementos. Así, es general describir estos conjuntos por fórmulas, como

$$(p_1 = 0) \vee (p_2 \leq 0 \wedge \neg(p_3 = 0))$$

donde \vee significa que tomamos una unión, \wedge que tomamos una intersección y \neg que tomamos un complemento. Para ilustrar esto, veamos como se construyen el conjunto semialgebraico dado por $((X^2 + Y^2 \leq 1) \vee (X + 3Y = 0)) \wedge (\neg(3Y - X^2 < 0))$ en la Figura **M\$1 2** y el dado por $((XY \leq 0) \wedge ((X^2 + Y^2 \leq 1) \vee (XY = 0))) \vee (X^2 + Y^2 = 1)$ en la Figura **M\$1 3**.

Para le lector con inclinaciones prácticas, debo indicar que los conjuntos semialgebraicos aparecen de forma natural al considerar el conjunto de configuraciones posibles de un brazo robótico. Para un ejemplo muy sencillo de cómo esto sucede, se puede mirar el Example **0\$2 1** en la introducción donde se muestra cómo este conjunto se describe para un brazo robótico determinado.

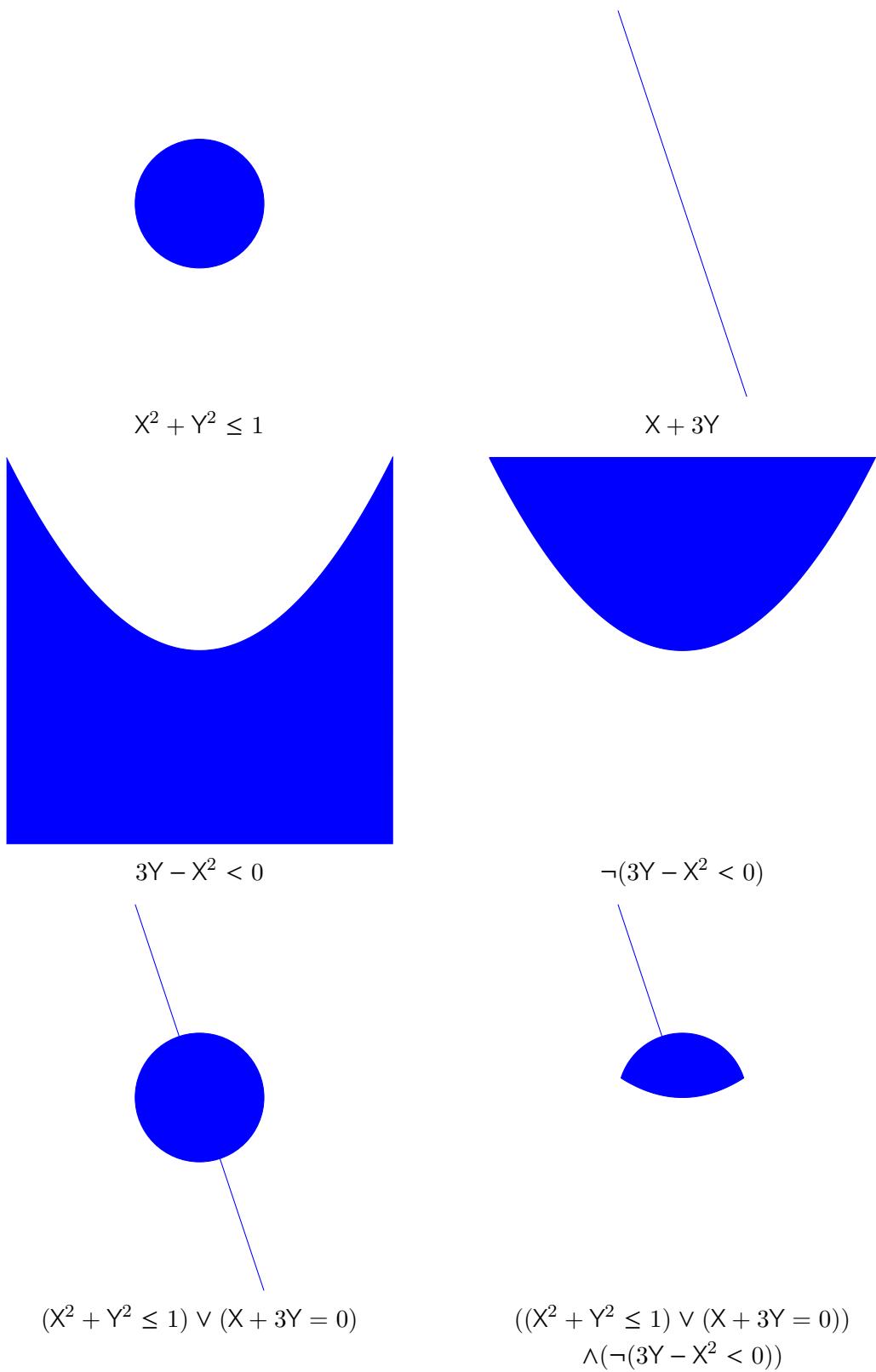


Figura **M^{S1}2**: Construcción de $((X^2 + Y^2 \leq 1) \vee (X + 3Y = 0)) \wedge (\neg(3Y - X^2 < 0))$

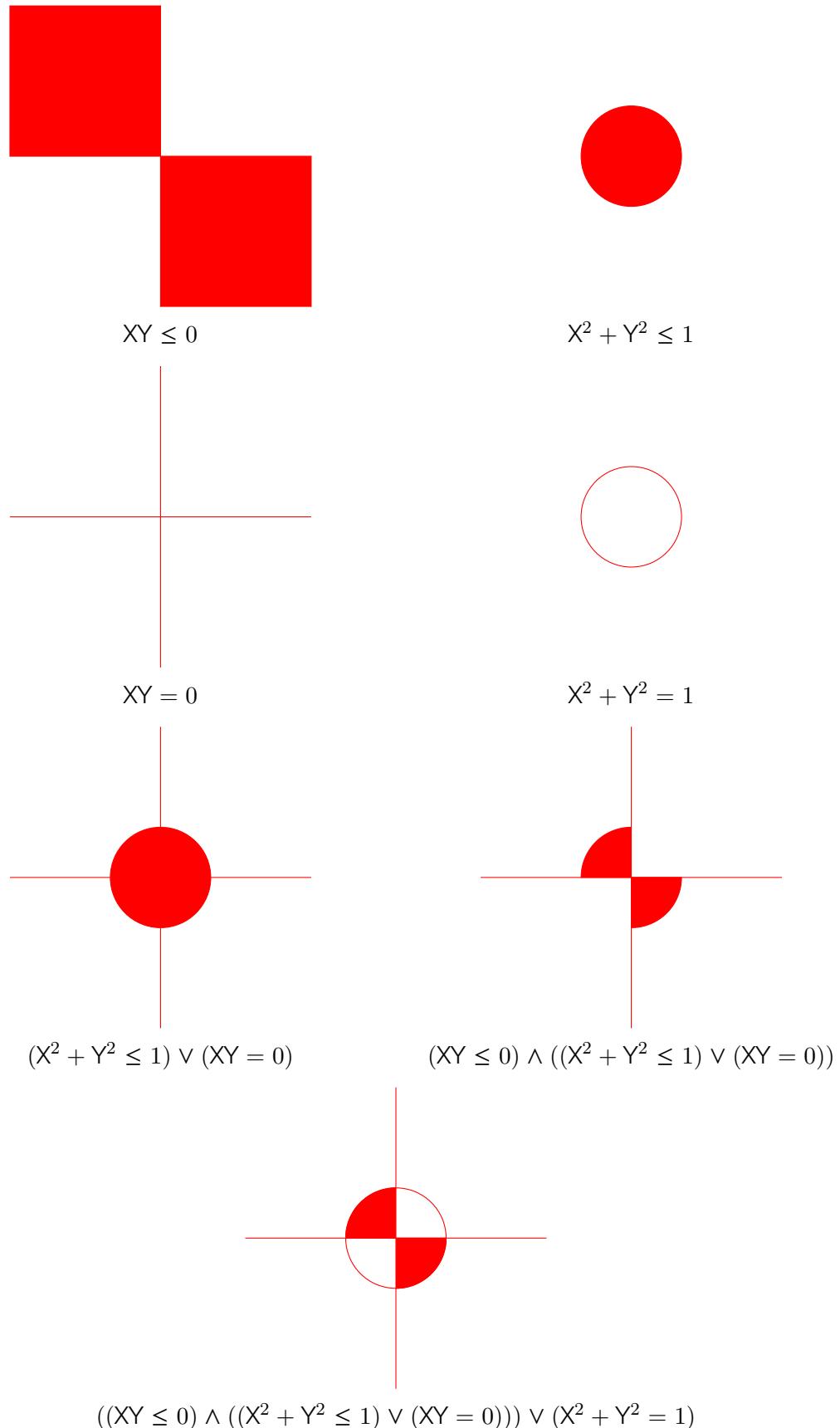


Figura **M\$1.3**: Construcción de $((XY \leq 0) \wedge ((X^2 + Y^2 \leq 1) \vee (XY = 0))) \vee (X^2 + Y^2 = 1)$

MS² Grupos de homología

El mayor problema a la hora de entender los conjuntos semialgebraicos, es que a priori no sabemos en qué puntos un polinomio es positivo, negativo o cero. Esto hace que las formas de un conjunto semialgebraico sean difíciles de entender. Y si ya son complicadas en el plano, en un espacio de dimensión arbitraria son excesivamente intrincadas. Por supuesto, queremos saber decir qué forma tiene un conjunto semialgebraico.

En este punto, los grupos de homología dan una aproximación a la pregunta de qué forma tiene un conjunto. En vez de centrarnos en toda clase de detalles geométricos, nos centramos en las partes de la forma que aun deformando el conjunto se preservan. En este intercambio, perdemos información sobre el conjunto, pero ganamos la habilidad de decir algo sobre la forma. En este sentido, los grupos de homología proporcionan información sobre la forma de un conjunto semialgebraico.

En general, el i -ésimo grupo de homología de un conjunto X , $H_i(X)$, “cuenta” la cantidad de agujeros topológicos del conjunto X . Entender el significado preciso de $H_i(X)$ y qué implica sobre la forma de un conjunto es difícil no sólo porque objetos de dimensión arbitraria entran en juego, sino porque el grupo de homología es una simplificación algebraica de la noción de agujero topológico, eso sí, una simplificación que se puede calcular.

Aunque no podemos ser más precisos en general, vamos a discutir sobre el significado de $H_0(X)$ y $H_1(X)$. Para ser más precisos, vamos a dar más bien el significado de los números de Betti $\beta_0(X)$ y $\beta_1(X)$ que miden, en cierto sentido, el tamaño de $H_0(X)$ y $H_1(X)$, respectivamente, y qué son más fáciles de entender. Es importante notar, que los números de Betti son números naturales, esto es, $0, 1, 2, \dots$ y que cuentan algo dentro del conjunto que estudiamos.

El ceroésimo número de Betti, $\beta_0(X)$, cuenta las componentes conexas de X . La componente conexa de X que contiene un punto x no es más que la región de aquellos puntos de X a los que podemos llegar desde x sin salir de X .

El primer número de Betti, $\beta_1(X)$, cuenta el número de caminos cerrados que no se pueden contraer a un punto en X hasta equivalencia. Hay ciertos matices que estamos ignorando, pero esos no son importantes para tener una intuición acerca del significado de β_1 . Para visualizar esto, imaginemos que caminamos en el espacio con una cuerda y que al terminar nuestro camino cerrado atamos los dos extremos de la cuerda creando un lazo. Si podemos recoger esta cuerda, entonces el camino se puede contraer a un punto; si no podemos, entonces tenemos un ciclo. En otras palabras, en este segundo caso, es como si hubiera una columna en el espacio donde nos estamos moviendo.

Para clarificar el significado con ejemplos concretos, miremos a los espacios de la Figura MS² 4. En esta, los espacios X_0 y X_1 , por un lado, y los espacios Y_0 e Y_1 , por otro lado, son topológicamente equivalentes. Esto quiere decir, que tienen la misma forma topológica, aunque claramente no tienen la misma forma geométrica. Si miramos al valor de β_0 , podemos ver que en todos los casos es igual a uno, porque podemos caminar de cualquier punto a cualquier otro punto. Si miramos al valor de β_1 , se puede ver que es cero en el caso de X_0 y X_1 y que es tres en el caso de Y_0 e Y_1 . En el primer caso, esto es obvio, dado que todo camino cerrado se puede contraer a un punto. En el segundo caso, la razón por la que

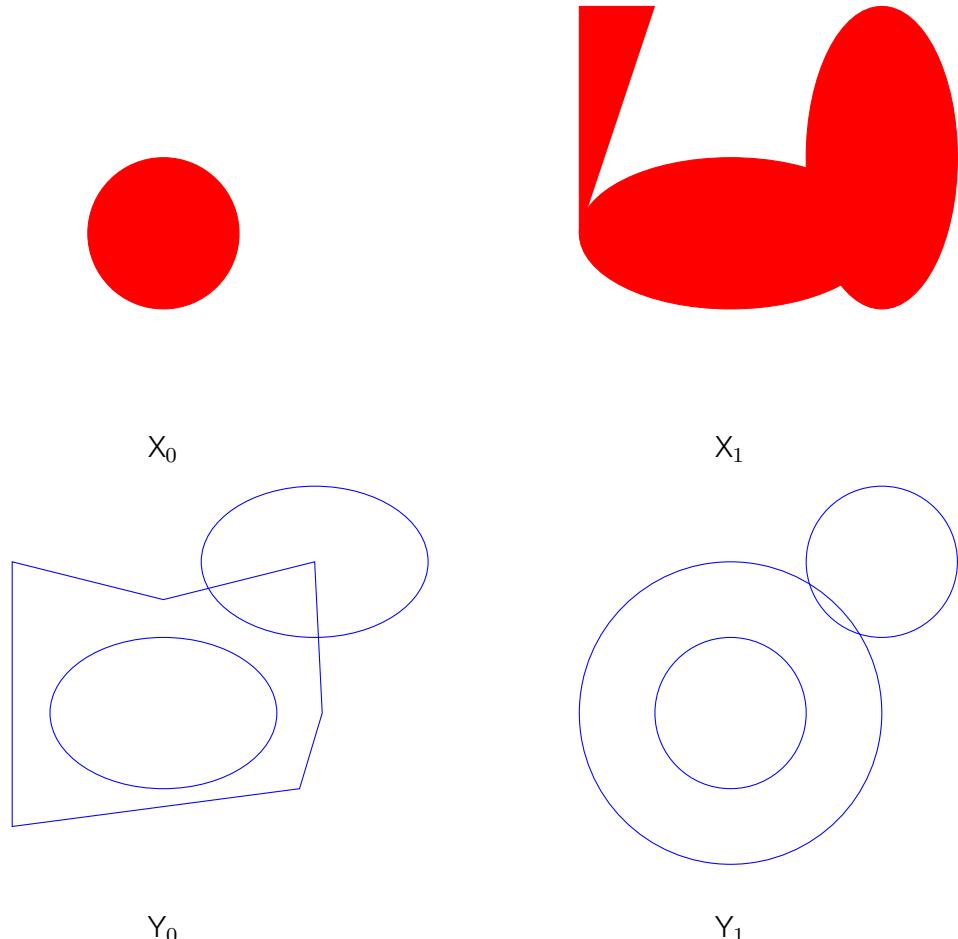


Figura **M\$2 4**: Dos pares de espacios (X_0, X_1) y (Y_0, Y_1)

el valor es tres, tiene que ver con que en cierto sentido todos los caminos cerrados que no se contraen a un punto se pueden obtener a partir de tres de ellos.

De esta forma, podemos ver la clase de información que proporcionan los grupos de homología dan información sobre la forma de un conjunto. Aunque haya información que se pierda, recordamos que esto se hace a cambio de ser capaces de obtener información fácilmente.

M\$3 Cálculo numérico

Una vez que sabemos qué queremos calcular, es importante entender cómo. El método que usamos es similar al que se usa en cualquier pantalla que muestra una imagen: aproximamos el conjunto por una nube de puntos a partir de la cuál se pueden computar los grupos de homología. La idea de este fundamento la representamos en la Figura **M\$3 5**, donde se muestra la manera de aproximar una curva por una nube de puntos: ponemos un retículo, tomamos los puntos del retículo que están suficientemente cerca y después los “engordamos”.

En la Figura **M\$3 5**, hay diversas cuestiones que están escondidas debajo de la alfombra:

1. ¿Cómo sabemos como de fino tiene que ser el retículo para capturar apropiadamente la forma del conjunto y no perder ninguna propiedad?

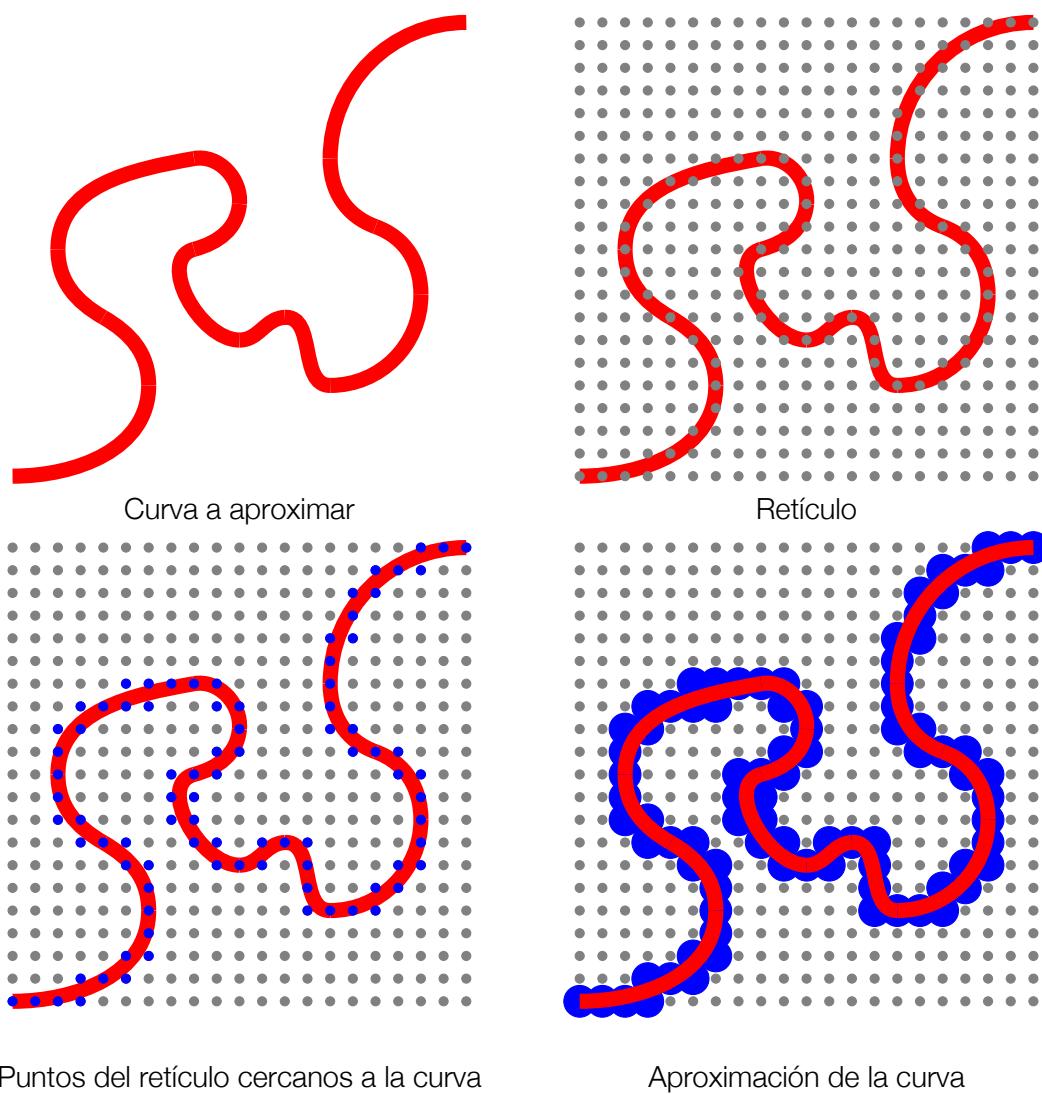


Figura **M^{S3} 5**: Ilustración del fundamento teórico del cálculo

2. ¿Cómo sabemos que puntos están cerca si no sabemos qué forma tiene y por dónde está el conjunto semialgebraico?
3. ¿Cómo sabemos cuánto hay qué “engordar” los puntos?

Justamente, estas son las preguntas a las qué responde esta tesis en general. Aunque no puedo dar esta respuesta en detalle aquí, voy a dar ahora las ideas intuitivas subyacentes:

1. Hay un parámetro, llamado condición, que se puede estimar evaluando los polinomios en los puntos del retículo. Si el retículo no es suficientemente fino, no se puede estimar el parámetro y hay que sustituirlo por otro más fino.
2. Evaluando un polinomio en un punto, podemos saber si el valor es “muy positivo”, “muy negativo” o si está “cerca” de cero. Usamos esto para seleccionar los puntos que satisfacen aproximadamente la descripción del conjunto semialgebraico considerado.
3. Cuánto hay que engordar las bolas depende explícitamente del número de condición y de cuán fino es el retículo.

Por supuesto, estas respuestas inducen más preguntas como las anteriores, pero esto es natural, dado que aquí no estamos haciendo un tratamiento técnico y nuestro lenguaje es más bien vago en el intento de hacerlo más comprensible.

Por último, ¿por qué cálculo numérico? La idea es que solamente podemos evaluar nuestros polinomios con precisión finita, va a haber errores. El término numérico hace referencia a que el método de cálculo desarrollado es robusto, es capaz de lidiar con errores. Por supuesto, esto tiene un coste, y hay conjuntos semialgebraicos para los que nuestro método no funciona, porque errores arbitrariamente pequeños en los coeficientes de los polinomios o el cómputo cambian la forma topológica radicalmente.

Index

Symbols			
1st Lipschitz property	35, 51	local	37
2nd Lipschitz property	36, 51	weak	51
		condition-based complexity	18
		counting problem	9
		covariance matrix	32
		critical points method	13
		Cylindrical Algebraic Decomposition	13
		CAD	13
A			
algebraic neighborhood of $S(f, t, \phi)$	61	D	
algebraic neighborhood of $\mathcal{Z}^S(f)$	60	dimension	
approximating cloud of \mathcal{G} -points	132	of a face	118
Attali-Lieutier-Salinas approximation		discriminant set	37
theorem	129	local	37
average framework	42	dobro random polynomial	172
		Durfee's theorem	81
B		E	
Betti number	3	Eclusion lemma	30
Boolean formula		Ehresmann's Lemma	66
atom	4	Euler's Gamma function	32
over (f, t)	61	Euler-Poincaré cahracteristic	17
over p	5	Euler-Yao cahracteristic	17
realization	5, 61		
size	4	F	
supported on $\{\alpha_1, \dots, \alpha_a\}$	4	Fisher-Snedecor distribution	176
boundary order	71	(f, λ) -lartition	76
		floating-point number system	161
		base	161
C		exponent range	161
Čech complex	122	overflow	162
Čech homology witness theorem	134	precision	161
Church-Turing thesis	2	range	162
strong	2	round-off unit	162
computational classification	201	rounding map	162
weak	202	underflow	162
concentration function	175	(f, λ) -partition	76
condition number	18	formula	
global condition number	34	disjunctive normal form	62
global intersection condition number			
50			
local condition number	33		
local intersection condition number	50		
condition number theorem			
global	38		

I	
lax	61
monotone	61
normal form	62
purely conjunctive	61
Frobenius	
inner product	29
norm	29
functorial nerve theorem (homological)	123
G	
Gabrielov-Vorobjov (δ, ε) -approximation	87
Gabrielov-Vorobjov (δ, ε) -block	87
Gabrielov-Vorobjov approximation theorem	87
Gaussian random matrix	32
Gaussian random vector	31
geodesic distance	
on \mathbb{S}^n	30
grid	
random $\tilde{\gamma}$ -grid with failure probability $\tilde{\gamma}^{-1}$	143
recursive $\tilde{\gamma}$ -grid	144
uniform grid	141
grid method	19
H	
Han's (f, \mathcal{O}) -property	191
Hausdorff distance	100
higher derivative estimate	39
homogenization map	53
homological inclusion-exclusion transfer	125
homology	
simplicial	119
singular	3
I	
ill-posed	18
J	
Jung's theorem	128
K	
k -boundary	119
k -chain	119
k -cycles	119
KSS random polynomial tuple	32
k th boundary operator	119
L	
ℓ -exponential random polynomial	173
Leray property	117
local feature size	103
local size bound	185
locally finite	67
M	
Mather-Thom theory	66
medial axis	102
N	
nearest-point retraction	101
nerve	117
nerve theorem	117
Newton vector field	59
discontinuous	64
Niyogi-Smale-Weinberger approximation	
theorem	107
normal distribution	31
standard	31
standard deviation	31
normal vector	106
P	
parallel algorithm	155
Plantinga-Vegter algorithm	179
pseudoinverse	34
Q	
quantitative Durfee's theorem	81
strong	82
quantitative Gabrielov-Vorobjov	
approximation theorem	89
R	
r -neighborhood	100
(Euclidean)	100
spherical	60
r -net	101
spherical	132
random variable	
anti-concentration property	172
centered	172
subgaussian	172
reach	103
local reach	103
local reach along u	104
μ -reach	109
weak reach	109

regularity inequality	34, 51	Whitney stratified set	67
round-off unit	162	Whitney's condition a	68
rounding map	162	Whitney's condition b	67
Rudelson-Vershynin concentration theorem	175	Whitney's umbrella	68
S			
sampling theorem	133		
saturated formula	71		
semialgebraic set	4		
Boolean description	5		
sign map	68		
sign vector	71		
simplicial complex			
(abstract)	117		
geometric	118		
singular homology	3		
Smale's gamma	39		
Smale's projective gamma	39		
Smith Normal Form	120		
smoothed framework	42		
space of d-homogeneous polynomial			
q-tuples	26		
spiral	68		
Spivak pronoun			
E	xiii		
Eir	xiii		
Em	xiii		
standard model of arithmetic	162		
stratified fiber bundle	69		
stratified homeomorphism	69		
strict formula	71		
submersion	69		
T			
Thom's first isotopy lemma	69		
torsion coefficients	3		
transversal	50, 69		
trivial fiber bundle	66		
trivial stratified set	68		
V			
Vietoris-Rips complex	128		
Vietoris-Rips graph	128		
Vietoris-Rips homology witness theorem			
134			
W			
Weyl random polynomial	173		
Whitney stratification	67		

List of algorithms

1	SIMPLICIALBETTI	121
2	SIMPLICIALHOMOLOGY	121
3	$\bar{\kappa}$ -ESTIMATE	146
4	SPHERICALHOMOLOGY	148
5	SPHERICALLAXHOMOLOGY	149
6	AFFINEHOMOLOGY	151
7	PARMULTIPLICATION	155
8	$\bar{\kappa}$ -PARESTIMATE	156
9	PARHOMOLOGYWITNESS	158
10	PVSUBDIVISION	180
11	CUBICALHANCOVERING	191
12	SPHERICALHANCOVERING	194
13	$\bar{\kappa}$ -FASTESTIMATE	197

List of figures

FP	Peter Bürgisser (right) and Felipe Cucker (left) drawn by Jorge Chan	vii
2^{S¹}1	Discontinuous Newton vector field for a convex cone	66
2^{S²}2	$\Pi_{f,\lambda}$ with $f = (XY)$ and $\lambda = (0, \sqrt{3}/4)$	78
2^{S²}3	An example of $\Pi_{f,\lambda}$ (locally) on \mathbb{S}^2 with $q = 2$ and $m = 2$	78
2^{S⁴}4	The Gabrielov-Vorobjov construction for two open half-lines	88
2^{S⁴}5	The Gabrielov-Vorobjov construction for the positive quadrant	89
2^{S⁴}6	The Gabrielov-Vorobjov construction for an ill-posed system	89
3^{S¹}1	X, in red, and part of its medial axis, Δ_X , in blue.	102
3^{S¹}2	Sets with reach zero, in red, and their medial axis in blue	104
3^{S¹}3	Diagram of the proof of Theorem 3 ^{S¹} 8	109
3^{S²}4	X, in red, and Y, in blue, from Remark 3 ^{S²} 1	112
3^{S²}5	A semialgebraic set with reach equal to zero	116
3^{S³}6	Natural map of Mayer-Vietoris sequences in the proof of Theorem 3 ^{S³} 8.	126
5^{S²}1	PV Algorithm applied to the polynomial $f = X^4 - 6X^3 + 2X^2Y^2 - 6X^2Y - 34X^2 - 6XY^2 - 320XY + 376X + Y^4 - 6Y^3 - 34Y^2 + 376Y + 3128$ in $[-10, 10]^2$	182
M^{S¹}1	Un conjunto semialgebraico complicado	228
M^{S¹}2	Construcción de $((X^2 + Y^2 \leq 1) \vee (X + 3Y = 0)) \wedge (\neg(3Y - X^2 < 0))$	229
M^{S¹}3	Construcción de $((XY \leq 0) \wedge ((X^2 + Y^2 \leq 1) \vee (XY = 0))) \vee (X^2 + Y^2 = 1)$	230
M^{S²}4	Dos pares de espacios (X_0, X_1) y (Y_0, Y_1)	232
M^{S³}5	Ilustración del fundamento teórico del cálculo	233

Bibliography

- [1] E. Aamari, J. Kim, F. Chazal, B. Michel, A. Rinaldo, and L. Wasserman. Estimating the reach of a manifold. *Electron. J. Stat.*, 13(1):1359–1399, 2019.
- [2] A. A. Albert. An inductive proof of Descartes’ rule of signs. *Amer. Math. Monthly*, 50:178–180, 1943.
- [3] L. Alberti, B. Mourrain, and J.-P. Técourt. Isotopic triangulation of a real algebraic surface. *J. Symbolic Comput.*, 44(9):1291–1310, 2009.
- [4] J. G. Alcázar and J. R. Sendra. Computation of the topology of real algebraic space curves. *J. Symbolic Comput.*, 39(6):719–744, 2005.
- [5] P. S. Alexandrov. Über den allgemeinen Dimensionsbegriff und seine Beziehungen zur elementaren geometrischen Anschauung (German) [About the general concept of dimension and its relations to elementary geometrical intuition]. *Math. Ann.*, 98(1):617–635, 1928.
- [6] D. Amelunxen and M. Lotz. Average-case complexity without the black swans. *J. Complexity*, 41:82–101, 2017.
- [7] V. I. Arnold. Distribution of ovals of the real plane of algebraic curves, of involutions of four-dimensional smooth manifolds, and the arithmetic of integer-valued quadratic forms. *Functional Analysis and Its Applications*, 5(3):169–176, 1971. Transl. from В. И. Арнольд, О расположении овалов вещественных плоских алгебраических кривых, инволюциях четырехмерных гладких многообразий и арифметике целочисленных квадратичных форм (Russian), *Функц. анализ и его прил.*, 5(3):1–9, 1971.
- [8] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition. I. The basic algorithm. *SIAM J. Comput.*, 13(4):865–877, 1984.
- [9] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition. II. An adjacency algorithm for the plane. *SIAM J. Comput.*, 13(4):878–889, 1984.
- [10] D. S. Arnon and S. McCallum. A polynomial-time algorithm for the topological type of a real algebraic curve—extended abstract. *Rocky Mountain J. Math.*, 14(4):847–850, 1984. Ordered fields and real algebraic geometry (Boulder, Colo., 1983).
- [11] D. S. Arnon and S. McCallum. A polynomial-time algorithm for the topological type of a real algebraic curve. *J. Symbolic Comput.*, 5(1-2):213–236, 1988.

- [12] S. Arora and B. Barak. *Computational Complexity: A modern approach*. Cambridge University Press, Cambridge, 2009.
- [13] E. Artin and O. Schreier. Algebraische Konstruktion reeller Körper (German) [Algebraic construction of real fields]. *Abh. Math. Sem. Univ. Hamburg*, 5(1):85–99, 1927.
- [14] D. Attali, A. Lieutier, and D. Salinas. Vietoris-Rips complexes also provide topologically correct reconstructions of sampled shapes (extended abstract). In *Computational geometry (SCG'11)*, pages 491–500. ACM, New York, 2011.
- [15] D. Attali, A. Lieutier, and D. Salinas. Vietoris-Rips complexes also provide topologically correct reconstructions of sampled shapes. *Comput. Geom.*, 46(4):448–465, 2013.
- [16] M. Avendaño. Descartes’ rule of signs is exact! *J. Algebra*, 324(10):2884–2892, 2010.
- [17] M. Avendaño and A. Ibrahim. Ultrametric root counting. *Houston J. Math.*, 36(4):1011–1022, 2010.
- [18] M. Avendaño and A. Ibrahim. Multivariate ultrametric root counting. In *Randomization, relaxation, and complexity in polynomial equation solving*, volume 556 of *Contemp. Math.*, pages 1–23. Amer. Math. Soc., Providence, RI, 2011.
- [19] M. Avendaño and T. Krick. Sharp bounds for the number of roots of univariate fewnomials. *J. Number Theory*, 131(7):1209–1228, 2011.
- [20] M. Avendaño. The number of roots of a lacunary bivariate polynomial on a line. *Journal of Symbolic Computation*, 44(9):1280–1284, 2009.
- [21] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 408–417. ACM, New York, 1996.
- [22] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. *Discrete Comput. Geom.*, 22(1):1–18, 1999.
- [23] S. Basu. Computing the first few Betti numbers of semi-algebraic sets in single exponential time. *J. Symbolic Comput.*, 41(10):1125–1154, 2006.
- [24] S. Basu. A complex analogue of Toda’s theorem. *Found. Comput. Math.*, 12(3):327–362, 2012.
- [25] S. Basu. Algorithms in real algebraic geometry: a survey. In *Real algebraic geometry*, volume 51 of *Panor. Synthèses*, pages 107–153. Soc. Math. France, Paris, 2017.
- [26] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 632–641. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

- [27] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets (extended abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 168–173. ACM, New York, 1996.
- [28] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, 1996.
- [29] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety (extended abstract). In *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 1–15. Springer, Berlin, 1997.
- [30] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *J. Amer. Math. Soc.*, 13(1):55–82, 2000.
- [31] S. Basu, R. Pollack, and M.-F. Roy. Computing the dimension of a semi-algebraic set. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 316(Teor. Slozhn. Vychisl. 9):42–54, 225, 2004.
- [32] S. Basu, R. Pollack, and M.-F. Roy. Betti number bounds, applications and algorithms. In *Combinatorial and computational geometry*, volume 52 of *Math. Sci. Res. Inst. Publ.*, pages 87–96. Cambridge Univ. Press, Cambridge, 2005.
- [33] S. Basu, R. Pollack, and M.-F. Roy. Computing the first Betti number and the connected components of semi-algebraic sets. In *STOC’05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 304–312. ACM, New York, 2005.
- [34] S. Basu, R. Pollack, and M. F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.
- [35] S. Basu, R. Pollack, and M.-F. Roy. Computing the first Betti number of a semi-algebraic set. *Found. Comput. Math.*, 8(1):97–136, 2008.
- [36] S. Basu and C. Riener. Efficient algorithms for computing the Euler-Poincaré characteristic of symmetric semi-algebraic sets. In *Ordered algebraic structures and related topics*, volume 697 of *Contemp. Math.*, pages 51–79. Amer. Math. Soc., Providence, RI, 2017.
- [37] S. Basu and C. Riener. On the equivariant Betti numbers of symmetric definable sets: vanishing, bounds and algorithms. *Selecta Math. (N.S.)*, 24(4):3241–3281, 2018.
- [38] S. Basu and C. Riener. Vandermonde varieties, mirrored spaces, and the cohomology of symmetric semi-algebraic sets, December 2018. (arXiv:1812.10994v2).
- [39] S. Basu and M.-F. Roy. Divide and conquer roadmap for algebraic sets. *Discrete Comput. Geom.*, 52(2):278–343, 2014.
- [40] S. Basu, M.-F. Roy, M. Safey El Din, and E. Schost. A baby step–giant step roadmap algorithm for general algebraic sets. *Found. Comput. Math.*, 14(6):1117–1172, 2014.

- [41] S. Basu and N. Vorobjov. On the number of homotopy types of fibres of a definable map. *J. Lond. Math. Soc.* (2), 76(3):757–776, 2007.
- [42] S. Basu and T. Zell. Polynomial hierarchy, Betti numbers and a real analogue of Toda’s theorem. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2009*, pages 73–82. IEEE Computer Soc., Los Alamitos, CA, 2009.
- [43] S. Basu and T. Zell. Polynomial hierarchy, Betti numbers, and a real analogue of Toda’s theorem. *Found. Comput. Math.*, 10(4):429–454, 2010.
- [44] U. Bauer. Ripser: efficient computation of vietoris-rips persistence barcodes, August 2019. (arXiv:1908.02518). See also <http://ripser.org>.
- [45] C. Beltrán and L. Pardo. Smale’s 17th problem: average polynomial time to compute affine and projective solutions. *J. Amer. Math. Soc.*, 22(2):363–385, 2009.
- [46] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. *J. Comput. System Sci.*, 32(2):251–264, 1986. 16th annual ACM-SIGACT symposium on the theory of computing (Washington, D.C., 1984).
- [47] R. Benedetti and J.-J. Risler. *Real algebraic and semi-algebraic sets*. Actualités Mathématiques. [Current Mathematical Topics]. Hermann, Paris, 1990.
- [48] M. Benedikt, G. Dong, L. Libkin, and L. Wong. Relational expressive power of constraint query languages. *J. ACM*, 45(1):1–34, 1998.
- [49] S. J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inf. Process. Lett.*, 18(3):147–150, Mar. 1984.
- [50] D. Bernoulli. Exposition of a new theory on the measurement of risk. *Econometrica*, 22(1):23–36, 1954. Trans. by L. Sommer from D. Bernoulli. Specimen Theoriae Novae de Mensura Sortis. In volume V of *Commentarii Academiae Scientiarum Imperialis Petropolitanae* [Latin] (Papers of the Imperial Academy of Sciences in Petersburg), pages 175–192, 1738.
- [51] D. N. Bernshtein. The number of roots of a system of equations. *Functional Analysis and Its Applications*, 9(3):183–185, 1975. Transl. from Д. Н. Бернштейн. Число корней системы уравнений (Russian). *Функц. анализ и его прил.*, 9(3):1–4, 1975.
- [52] D. N. Bernstein (Д. Н. Бернштейн), A. G. Kushnirenko (А. Г. Кушниренко), and A. G. Khovanskii (А. Г. Хованский). Многогранники Ньютона (Russian) [Newton polyhedra]. *УМН*, 31(3(189)):201–202, 1976.
- [53] B. Bertrand, F. Bihan, and F. Sottile. Polynomial systems with few real zeroes. *Math. Z.*, 253(2):361–385, 2006.
- [54] A. T. Bharucha-Reid and M. Sambandham. *Random polynomials*. Probability and Mathematical Statistics. Academic Press, Inc., Orlando, FL, 1986.

- [55] F. Bihan. Une quintique numérique réelle dont le premier nombre de Betti est maximal (French) [A real numerical quintic surface whose first Betti number is maximal]. *C. R. Acad. Sci. Paris Sér. I Math.*, 329(2):135–140, 1999.
- [56] F. Bihan. Polynomial systems supported on circuits and dessins d’enfants. *J. Lond. Math. Soc. (2)*, 75(1):116–132, 2007.
- [57] F. Bihan. Maximally positive polynomial systems supported on circuits. *J. Symbolic Comput.*, 68(part 2):61–74, 2015.
- [58] F. Bihan and A. Dickenstein. Descartes’ rule of signs for polynomial systems supported on circuits. *Int. Math. Res. Not. IMRN*, 22:6867–6893, 2017.
- [59] F. Bihan, A. Dickenstein, and J. Forsgård. Optimal descartes’ rule of signs for systems supported on circuits, 2019. Manuscript.
- [60] F. Bihan and B. El-Hilany. A sharp bound on the number of real intersection points of a sparse plane curve with a line. *Journal of Symbolic Computation*, 81:88–96, 2017.
- [61] F. Bihan, J. M. Rojas, and F. Sottile. On the sharpness of fewnomial bounds and the number of components of fewnomial hypersurfaces. In *Algorithms in algebraic geometry*, volume 146 of *IMA Vol. Math. Appl.*, pages 15–20. Springer, New York, 2008.
- [62] F. Bihan, F. Santos, and P.-J. Spaenlehauer. A polyhedral method for sparse systems with many positive solutions. *SIAM J. Appl. Algebra Geom.*, 2(4):620–645, 2018.
- [63] F. Bihan and F. Sottile. New fewnomial upper bounds from Gale dual polynomial systems. *Mosc. Math. J.*, 7(3):387–407, 573, 2007.
- [64] F. Bihan and F. Sottile. Betti number bounds for fewnomial hypersurfaces via stratified Morse theory. *Proc. Amer. Math. Soc.*, 137(9):2825–2833, 2009.
- [65] F. Bihan and F. Sottile. Fewnomial bounds for completely mixed polynomial systems. *Adv. Geom.*, 11(3):541–556, 2011.
- [66] G. Blekherman, P. A. Parrilo, and R. R. Thomas, editors. *Semidefinite optimization and convex algebraic geometry*, volume 13 of *MOS-SIAM Series on Optimization*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA; Mathematical Optimization Society, Philadelphia, PA, 2013.
- [67] G. E. Blelloch and B. M. Maggs. Parallel algorithms. In *Algorithms and theory of computation handbook*, pages 47–1–47–44. CRC, Boca Raton, FL, 1999.
- [68] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998. With a foreword by R. M. Karp.
- [69] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21(1):1–46, 1989.

- [70] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated and revised from J. Bochnak, M. Coste and M.-F. Roy, *Géométrie algébrique réelle*, volume 12 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1987.
- [71] J.-D. Boissonnat, D. Cohen-Steiner, B. Mourrain, G. Rote, and G. Vegter. Meshing of Surfaces. In J.-D. Boissonnat and M. Teillaud, editors, *Effective Computational Geometry for Curves and Surfaces*, pages 181–229. Springer Berlin Heidelberg, 2006.
- [72] J.-D. Boissonnat, D. Cohen-Steiner, and G. Vegter. Isotopic implicit surface meshing. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, pages 301–309. ACM, New York, 2004.
- [73] J.-D. Boissonnat, D. Cohen-Steiner, and G. Vegter. Isotopic implicit surface meshing. *Discrete Comput. Geom.*, 39(1-3):138–157, 2008.
- [74] J.-D. Boissonnat and S. Oudot. Provably good sampling and meshing of Lipschitz surfaces. In *Computational geometry (SCG'06)*, pages 337–346. ACM, New York, 2006.
- [75] H. Bosse, M. Grötschel, and M. Henk. Polynomial inequalities representing polyhedra. *Math. Program.*, 103(1, Ser. A):35–44, 2005.
- [76] I. Briquel and P. Bürgisser. The real tau-conjecture is true on average, June 2018. (arXiv:1806.00417).
- [77] J. G. Broida and S. G. Williamson. *A comprehensive introduction to linear algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.
- [78] C. W. Brown. Constructing cylindrical algebraic decomposition of the plane quickly. Available at: <https://www.usna.edu/Users/cs/wcbrown/research/MOTS2002.1.ps.gz> [29/07/2019], 2002.
- [79] C. W. Brown and J. H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, ISSAC '07, pages 54–60. ACM, New York, 2007.
- [80] E. Brugallé. Real plane algebraic curves with asymptotically maximal number of even ovals. *Duke Math. J.*, 131(3):575–587, 2006.
- [81] V. Bunimov and M. Schimmler. Efficient parallel multiplication algorithm for large integers. In H. Kosch, L. Böszörnyi, and H. Hellwagner, editors, *Euro-Par 2003 Parallel Processing*, pages 923–928, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
- [82] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1997.

- [83] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations. I. Semilinear sets. *SIAM J. Comput.*, 33(1):227–260, 2003.
- [84] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations. II. Algebraic and semialgebraic sets. *J. Complexity*, 22(2):147–191, 2006.
- [85] P. Bürgisser and F. Cucker. Exotic quantifiers, complexity classes, and complete problems. *Found. Comput. Math.*, 9(2):135–170, 2009.
- [86] P. Bürgisser and F. Cucker. On a problem posed by Steve Smale. *Annals of Mathematics*, 174:1785–1836, 2011.
- [87] P. Bürgisser and F. Cucker. *Condition: The geometry of numerical algorithms*, volume 349 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2013.
- [88] P. Bürgisser, F. Cucker, and P. Lairez. Computing the homology of basic semialgebraic sets in weak exponential time. *J. ACM*, 66(1):5:1–5:30, Dec. 2018.
- [89] P. Bürgisser, F. Cucker, and M. Lotz. Counting complexity classes for numeric computations. III. Complex projective sets. *Found. Comput. Math.*, 5(4):351–387, 2005.
- [90] P. Bürgisser, F. Cucker, and M. Lotz. The probability that a slightly perturbed numerical analysis problem is difficult. *Math. Comp.*, 77(263):1559–1583, 2008.
- [91] P. Bürgisser, F. Cucker, and J. Tonelli-Cueto. Computing the Homology of Semialgebraic Sets. I: Lax Formulas. *Foundations of Computational Mathematics*, May 2019. (arXiv:1807.06435v3).
- [92] P. Bürgisser, F. Cucker, and J. Tonelli-Cueto. Computing the Homology of Semialgebraic Sets. II: General formulas, March 2019. (arXiv:1903.10710).
- [93] P. Bürgisser, A. A. Ergür, and J. Tonelli-Cueto. On the Number of Real Zeros of Random Fewnomials, April 2019. To appear at SIAM Journal on Applied Algebra and Geometry (SIAGA). (arXiv:1811.09425v3).
- [94] P. Bürgisser and A. Lerario. Probabilistic Schubert calculus. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2018. To appear.
- [95] P. Bürgisser and P. Scheiblechner. On the complexity of counting components of algebraic varieties. *J. Symbolic Comput.*, 44(9):1114–1136, 2009.
- [96] P. Bürgisser and P. Scheiblechner. Counting irreducible components of complex algebraic varieties. *Comput. Complexity*, 19(1):1–35, 2010.
- [97] M. A. Burr. Continuous amortization and extensions: with applications to bisection-based root isolation. *J. Symbolic Comput.*, 77:78–126, 2016.

- [98] M. A. Burr, S. Gao, and E. P. Tsigaridas. The complexity of an adaptive subdivision method for approximating real curves. In *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation*, pages 61–68. ACM, New York, 2017.
- [99] M. A. Burr, S. Gao, and E. P. Tsigaridas. The complexity of subdivision for diameter-distance tests, January 2018. (arXiv:1801.05864).
- [100] M. A. Burr, F. Krahmer, and C. K. Yap. Continuous amortization: A non-probabilistic adaptive analysis technique. *Electronic Colloquium on Computational Complexity*, Report. No. 136, 2009.
- [101] J. Canny. *The complexity of robot motion planning*, volume 1987 of *ACM Doctoral Dissertation Awards*. MIT Press, Cambridge, MA, 1988.
- [102] J. Canny. Constructing roadmaps of semi-algebraic sets. I. Completeness. *Artificial Intelligence*, 37(1-3):203–222, 1988. Geometric reasoning (Oxford, 1986).
- [103] J. Canny. Some Algebraic and Geometric Computations in PSPACE. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 460–467. ACM, New York, 1988.
- [104] J. Canny. Computing roadmaps of general semi-algebraic sets. *Comput. J.*, 36(5):504–514, 1993.
- [105] J. Canny. Improved algorithms for sign determination and existential quantifier elimination. *Comput. J.*, 36(5):409–418, 1993.
- [106] J. Canny, D. Y. Grigoriev, and N. N. Vorobjov. Finding connected components of a semialgebraic set in subexponential time. *Appl. Algebra Engrg. Comm. Comput.*, 2(4):217–238, 1992.
- [107] J. F. Canny. Computing roadmaps of general semi-algebraic sets. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 94–107. Springer, Berlin, 1991.
- [108] B. F. Caviness and J. R. J.son, editors. *Quantifier elimination and cylindrical algebraic decomposition*, Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1998.
- [109] F. Chazal, D. Cohen-Steiner, and A. Lieutier. A sampling theory for compact sets in euclidean space. *Discrete & Computational Geometry*, 41(3):461–479, 2009.
- [110] F. Chazal and A. Lieutier. The “ λ -medial axis”. *Graphical Models*, 67(4):304 – 331, 2005.
- [111] F. Chazal and A. Lieutier. Weak feature size and persistant homology: computing homology of solids in \mathbb{R}^n from noisy data samples. In *Computational geometry (SCG'05)*, pages 255–262. ACM, New York, 2005.

- [112] J. Cheng, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of planar algebraic curves. In *Proceedings of the Twenty-fifth Annual Symposium on Computational Geometry*, SCG '09, pages 361–370. ACM, New York, 2009.
- [113] J.-S. Cheng, X.-S. Gao, and M. Li. Determining the topology of real algebraic surfaces. In R. Martin, H. Bez, and M. Sabin, editors, *Mathematics of Surfaces XI*, pages 121–146. Springer Berlin Heidelberg, 2005.
- [114] J.-S. Cheng, K. Jin, and D. Lazard. Certified rational parametric approximation of real algebraic space curves with local generic position method. *J. Symbolic Comput.*, 58:18–40, 2013.
- [115] S.-W. Cheng, T. K. Dey, E. A. Ramos, and T. Ray. Sampling and meshing a surface with guaranteed topology and geometry. *SIAM J. Comput.*, 37(4):1199–1227, 2007.
- [116] D. Cheung and F. Cucker. A new condition number for linear programming. *Math. Program.*, 91(1, Ser. A):163–174, 2001.
- [117] D. Cheung and F. Cucker. Solving linear programs with finite precision. I. Condition numbers and random programs. *Math. Program.*, 99(1, Ser. A):175–196, 2004.
- [118] D. Cheung and F. Cucker. Solving linear programs with finite precision. II. Algorithms. *J. Complexity*, 22(3):305–335, 2006.
- [119] H. Y. Cheung, T. C. Kwok, and L. C. Lau. Fast matrix rank algorithms and applications. *J. ACM*, 60(5):Art. 31, 25, 2013.
- [120] B. Chevallier. Four m-curves of degree 8. *Functional Analysis and Its Applications*, 36(1):76–78, 2002. Transl. from Б. Шевалье (B. Chevallier), Четыре М-кривые степени 8. *Функциональный анализ и его приложения*, 36(10):90–93, 2002.
- [121] A. L. Chistov and D. Y. Grigoriev. Polynomial-time factoring of multivariate polynomials over a global field, 1982. Preprint LOMI E-5-82, Leningrad. (Non-available).
- [122] A. L. Chistov and D. Y. Grigoriev. Subexponential-time solving of systems of algebraic equations. i, 1982. Preprint LOMI E-9-83, Leningrad. (Non-available).
- [123] A. L. Chistov and D. Y. Grigoriev. Subexponential-time solving of systems of algebraic equations. ii, 1982. Preprint LOMI E-10-83, Leningrad. (Non-available).
- [124] A. L. Chistov and D. Y. Grigoriev. Complexity of quantifier elimination in the theory of algebraically closed fields. In *Mathematical foundations of computer science, 1984 (Prague, 1984)*, volume 176 of *Lecture Notes in Comput. Sci.*, pages 17–31. Springer, Berlin, 1984.
- [125] A. L. Chistov (А. Л. Чистов). Алгоритм полиномиальной сложности для разложения многочленов и нахождение компонент многообразия в субэкспоненциальное время (Russian) [Polynomial-time factoring of polynomials and finding the compounds of a variety within the subexponential time]. *Теория сложности вычислений. II*, 137:124–188, 2009.

- [126] A. Church. A Note on the Entscheidungsproblem. *J. Symbolic Logic*, 1(1):40–41, 03 1936.
- [127] A. Church. An Unsolvable Problem of Elementary Number Theory. *Amer. J. Math.*, 58(2):345–363, 1936.
- [128] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, pages 134–183. Volume 33 of Lecture Notes in Comput. Sci. Springer, 1975.
- [129] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *J. Symbolic Comput.*, 12(3):299–328, 1991.
- [130] C. Conradi, A. Iosif, and T. Kahle. Multistationarity in the Space of Total Concentrations for Systems that Admit a Monomial Parametrization. *Bulletin of Mathematical Biology*, July 2019.
- [131] M. Coste and M.-F. Roy. Thom’s lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. *J. Symbolic Comput.*, 5(1-2):121–129, 1988.
- [132] T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2006.
- [133] F. Cucker. Approximate zeros and condition numbers. *J. Complexity*, 15(2):214–226, 1999.
- [134] F. Cucker. Grid methods in computational real algebraic (and semialgebraic) geometry. *Chin. Ann. Math. Ser. B*, 39(2):373–396, 2018.
- [135] F. Cucker. Recent advances in the computation of the homology of semialgebraic sets. In F. Manea, B. Martin, D. Paulusma, and G. Primiero, editors, *Computing with Foresight and Industry*, pages 1–12, Cham, 2019. Springer International Publishing.
- [136] F. Cucker, A. A. Ergür, and J. Tonelli-Cueto. Plantinga-Vegter Algorithm Takes Average Polynomial Time. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, ISSAC ’19, pages 114–121. ACM, New York, 2019. (arXiv:1901.09234v2).
- [137] F. Cucker, A. A. Ergür, and J. Tonelli-Cueto. Functional norms, condition numbers and numerical algorithms in algebraic geometry [Working title], 2020. In progress.
- [138] F. Cucker, L. González-Vega, and F. Rossello. On algorithms for real algebraic plane curves. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 63–87. Birkhäuser Boston, Boston, MA, 1991.
- [139] F. Cucker, T. Krick, G. Malajovich, and M. Wschebor. A numerical algorithm for zero counting. I: Complexity and accuracy. *J. Complexity*, 24:582–605, 2008.

- [140] F. Cucker, T. Krick, G. Malajovich, and M. Wschebor. A numerical algorithm for zero counting. II: Distance to ill-posedness and smoothed analysis. *J. Fixed Point Theory Appl.*, 6:285–294, 2009.
- [141] F. Cucker, T. Krick, G. Malajovich, and M. Wschebor. A numerical algorithm for zero counting. III: Randomization and condition. *Adv. Applied Math.*, 48:215–248, 2012.
- [142] F. Cucker, T. Krick, and M. Shub. Computing the homology of real projective sets. *Found. Comput. Math.*, 18:929–970, 2018.
- [143] F. Cucker and S. Smale. Complexity estimates depending on condition and round-off error. In *Algorithms—ESA ’98 (Venice)*, volume 1461 of *Lecture Notes in Comput. Sci.*, pages 115–126. Springer, Berlin, 1998.
- [144] F. Cucker and S. Smale. Complexity estimates depending on condition and round-off error. *J. ACM*, 46(1):113–184, 1999.
- [145] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *J. Symbolic Comput.*, 5(1-2):29–35, 1988.
- [146] V. de Silva and R. Ghrist. Coverage in sensor networks via persistent homology. *Algebr. Geom. Topol.*, 7:339–358, 2007.
- [147] J.-P. Dedieu. *Points fixes, zéros et la méthode de Newton (French) [Fixed points, zeroes and the Newton method]*, volume 54 of *Mathématiques & Applications (Berlin) [Mathematics & Applications]*. Springer, Berlin, 2006.
- [148] A. I. Degtyarev and V. M. Kharlamov. Topological properties of real algebraic varieties: du côté de chez Rokhlin. *Russian Mathematical Surveys*, 55(4):735–814, 2000. Transl. from A. И. Дегтярев and В. М. Харламов, Топологические свойства вещественных алгебраических многообразий: du côté de chez Rokhlin (Russian), УМН, 55(4), 129–212, 2000.
- [149] J. W. Demmel. On condition numbers and the distance to the nearest ill-posed problem. *Numer. Math.*, 51(3):251–289, 1987.
- [150] J. W. Demmel. The probability that a numerical analysis problem is difficult. *Math. Comp.*, 50:449–480, 1988.
- [151] R. Descartes. *La Géométrie*. Librairie Scientifique A. Hermann, 1886. Digital reproduction of 2008 by Project Gutenberg (Ebook number: 26400).
- [152] D. N. Diatta, S. Diatta, F. Rouillier, M. F. Roy, and M. Sagraloff. Bounds for polynomials on algebraic numbers and application to curve topology, July 2018. (arXiv:1807.10622).
- [153] D. N. Diatta and A. Lerario. Low degree approximation of random polynomials, December 2018. (arXiv:1812.10137).

- [154] D. N. Diatta, F. Rouillier, and M. F. Roy. On the computation of the topology of plane curves. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 130–137. ACM, New York, 2014.
- [155] N. D. Diatta, B. Mourrain, and O. Ruatta. On the computation of the topology of a non-reduced implicit space curve. In *Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation*, ISSAC '08, pages 47–54. ACM, New York, 2008.
- [156] A. Dickenstein. Biochemical reaction networks: an invitation for algebraic geometers. In *Mathematical Congress of the Americas*, volume 656 of *Contemp. Math.*, pages 65–83. Amer. Math. Soc., Providence, RI, 2016.
- [157] J. Dieudonné. The historical development of algebraic geometry. *Amer. Math. Monthly*, 79:827–866, 1972.
- [158] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *J. Symbolic Comput.*, 44(7):818–835, 2009.
- [159] M. Drton, B. Sturmfels, and S. Sullivant. *Lectures on algebraic statistics*, volume 39 of *Oberwolfach Seminars*. Birkhäuser Verlag, Basel, 2009.
- [160] J.-G. Dumas, F. Heckenbach, D. Saunders, and V. Welker. Computing simplicial homology based on efficient smith normal form algorithms. In M. Joswig and N. Takayama, editors, *Algebra, Geometry and Software Systems*, pages 177–206, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
- [161] J.-G. Dumas, B. D. Saunders, and G. Villard. On efficient sparse integer matrix Smith normal form computations. *J. Symbolic Comput.*, 32(1-2):71–99, 2001. Article presented at Computer algebra and mechanized reasoning (St. Andrews, 2000).
- [162] J.-G. Dumas and G. Villard. Computing the Rank of Large Sparse Matrices over Finite Fields. In *Computer Algebra in Scientific Computing (CASC) 2002*, Proceedings of the fifth International Workshop on Computer Algebra in Scientific Computing, Yalta, Ukraine, pages 47–62. Victor G. Ganzha, Ernst W. Mayr, Evgenii V. Vorozhtsov, 2002.
- [163] A. H. Durfee. Neighborhoods of algebraic sets. *Trans. Amer. Math. Soc.*, 276(2):517–530, 1983.
- [164] R. Durrett. *Probability—theory and examples*, volume 49 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, fifth edition, 2019.
- [165] W. Eberly, M. Giesbrecht, and G. Villard. On computing the determinant and Smith form of an integer matrix. In *41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)*, pages 675–685. IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

- [166] A. Edelman and E. Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc. (N.S.)*, 32(1):1–37, 1995.
- [167] H. Edelsbrunner and J. L. Harer. *Computational topology: An introduction*. American Mathematical Society, Providence, RI, 2010.
- [168] H. Edelsbrunner, D. Letscher, and A. Zomorodian. Topological persistence and simplification. In *41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)*, pages 454–463. IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.
- [169] H. Edelsbrunner and S. Parsa. On the computational complexity of Betti numbers: reductions from matrix rank. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 152–160. ACM, New York, 2014.
- [170] R. H. Eggermont, E. Horobet, and K. Kubjas. Algebraic boundary of matrices of non-negative rank at most three. *Linear Algebra Appl.*, 508:62–80, 2016.
- [171] A. Eigenwillig, M. Kerber, and N. Wolpert. Fast and exact geometric analysis of real algebraic plane curves. In *Proceedings of the 2007 on International Symposium on Symbolic and Algebraic Computation*, ISSAC ’07, pages 151–158. ACM, New York, 2007.
- [172] B. El Hilany. Constructing polynomial systems with many positive solutions using tropical geometry. *Rev. Mat. Complut.*, 31(2):525–544, 2018.
- [173] M. El Kahoui. Topology of real algebraic space curves. *J. Symbolic Comput.*, 43(4):235–258, 2008.
- [174] P. Erdős and A. C. Offord. On the number of real roots of a random algebraic equation. *Proceedings of the London Mathematical Society*, 3(1):139–160, 1956.
- [175] A. A. Ergür, G. Paouris, and J. M. Rojas. Probabilistic Condition Number Estimates for Real Polynomial Systems I: A Broader Family of Distributions. *Found. Comput. Math.*, 2018.
- [176] A. A. Ergür, G. Paouris, and J. M. Rojas. Probabilistic Condition Number Estimates for Real Polynomial Systems II: Structure and Smoothed Analysis, September 2018. (arXiv:1809.03626).
- [177] H. Federer. Curvature measures. *Trans. Amer. Math. Soc.*, 93:418–491, 1959.
- [178] H. H. Feng. *Decomposition and computation of the topology of plane real algebraic curves*. PhD thesis, KTH Royal Institute of Technology, Stockholm, 1992.
- [179] T. Fidler. New congruences in the topology of real plane algebraic curves. *Dokl. Akad. Nauk SSSR*, 270(1):56–58, 1983.
- [180] A. F. Filippov. *Introducción a la Teoría de Ecuaciones Diferenciales* (Spanish) [*Introduction to the Theory of Differential Equations*]. Editorial URSS, 2007. Transl. (by J. E. Palomino Pérez and C. D. Nvarro Hernández) from А. Ф. Филиппов. *Введение в теорию дифференциальных уравнений* (Russian). Издательство “КомКнига”, 2007.

- [181] M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic. In *Complexity of computation (Proc. SIAM-AMS Sympos., New York, 1973)*, pages 27–41. Volume VII of SIAM–AMS Proc. AMS, Providence, R.I., 1974.
- [182] E. Fortuna, P. Gianni, and D. Luminati. Algorithmical determination of the topology of a real algebraic surface. *J. Symbolic Comput.*, 38(6):1551–1567, 2004.
- [183] E. Fortuna, P. Gianni, D. Luminati, and P. Parenti. The adjacency graph of a real algebraic surface. *Appl. Algebra Engrg. Comm. Comput.*, 16(5):271–292, 2005.
- [184] E. Fortuna, P. Gianni, P. Parenti, and C. Traverso. Algorithms to compute the topology of orientable real algebraic surfaces. *J. Symbolic Comput.*, 36(3-4):343–364, 2003. International Symposium on Symbolic and Algebraic Computation (ISSAC’2002) (Lille).
- [185] A. Gabrielov and N. Vorobjov. Betti numbers of semialgebraic sets defined by quantifier-free formulae. *Discrete Comput. Geom.*, 33(3):395–401, 2005.
- [186] A. Gabrielov and N. Vorobjov. Approximation of definable sets by compact families, and upper bounds on homotopy and homology. *J. Lond. Math. Soc. (2)*, 80(1):35–54, 2009.
- [187] G. Gatellier, A. Labrouzy, B. Mourrain, and J. P. Técourt. Computing the topology of three-dimensional algebraic curves. In *Computational methods for algebraic spline surfaces*, pages 27–43. Springer, Berlin, 2005.
- [188] P. Gianni and C. Traverso. Shape determination for real curves and surfaces. *Ann. Univ. Ferrara Sez. VII (N.S.)*, 29:87–109 (1984), 1983.
- [189] M. Giaroli, F. Bihan, and A. Dickenstein. Regions of multistationarity in cascades of Goldbeter-Koshland loops. *J. Math. Biol.*, 78(4):1115–1145, 2019.
- [190] C. Gibson, K. Wirthmüller, A. du Plessis, and E. Looijenga. *Topological stability of smooth mappings*. Lecture Notes in Mathematics, Vol. 552. Springer-Verlag, Berlin-New York, 1976.
- [191] M. Giesbrecht. Fast computation of the Smith form of a sparse integer matrix. *Comput. Complexity*, 10(1):41–69, 2001.
- [192] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I (German) [On formally undecidable propositions of Principia Mathematica and related systems. I]. *Monatsh. Math. Phys.*, 38(1):173–198, 1931.
- [193] J.-L. Goffin. The relaxation method for solving systems of linear inequalities. *Math. Oper. Res.*, 5(3):388–414, 1980.
- [194] H. H. Goldstine and J. von Neumann. Numerical inverting of matrices of high order. II. *Proc. Amer. Math. Soc.*, 2:188–202, 1951.

- [195] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. Complexity*, 12(4):527–544, 1996. Special issue for the Foundations of Computational Mathematics Conference (Rio de Janeiro, 1997).
- [196] L. Gonzalez-Vega and I. Necula. Efficient topology determination of implicitly defined algebraic plane curves. *Comput. Aided Geom. Design*, 19(9):719–743, 2002.
- [197] B. Grenet, P. Koiran, N. Portier, and Y. Strozecki. The limited power of powering: polynomial identity testing and a depth-four lower bound for the permanent. In *31st International Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 13 of *LIPICS. Leibniz Int. Proc. Inform.*, pages 127–139. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2011.
- [198] D. Y. Grigor’ev. Factorization of polynomials over a finite field and the solution of systems of algebraic equations. *Journal of Soviet Mathematics*, 34(4):1762–1803, 1986. Transl. from Д. Ю. Григорьев, Разложение многочленов над конечным полем и решение систем алгебраических уравнений. In *Теория сложности вычислений. II*, volume 137 of Zap. Nauchn. Sem. LOMI, pages 20–79, Изд-во «Наука», Ленинград. отд., 1984.
- [199] D. Y. Grigor’ev. The complexity of the decision problem for the first order theory of algebraically closed fields. *Mathematics of the USSR-Izvestiya*, 29(2):459–475, 1987. Transl. from Д. Ю. Григорьев, Сложность разрешения теории первого порядка алгебраически замкнутых полей, *Изв. АН СССР. Сер. матем.*, 50(5):1106–1120, 1986.
- [200] D. Y. Grigor’ev. Complexity of deciding the first-order theory of real closed fields. *Journal of Soviet Mathematics*, 55(2):1553–1587, 1991. Transl. from Д. Ю. Григорьев, Сложность разрешения теории первого порядка вещественно замкнутых полей. In *Теория сложности вычислений. 3*, volume 174 of Зап. научн. сем. ЛОМИ, pages 53–100, Изд-во «Наука», Ленинград. отд., 1988.
- [201] D. Grigoriev, J. Heintz, M.-F. Roy, P. Solernó, and N. N. Vorobjov. Comptage des composantes connexes d’un ensemble semi-algébrique en temps simplement exponentiel (French) [Counting connected components of a semi-algebraic set in single exponential time]. *C. R. Acad. Sci. Paris Sér. I Math.*, 311(13):879–882, 1990.
- [202] D. Y. Grigoriev. Complexity of deciding Tarski algebra. *J. Symbolic Comput.*, 5(1-2):65–108, 1988.
- [203] D. Y. Grigoriev and N. N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5(1-2):37–64, 1988.
- [204] D. Y. Grigoriev and N. N. Vorobjov. Counting connected components of a semialgebraic set in subexponential time. *Comput. Complexity*, 2(2):133–186, 1992.

- [205] D. Y. Grigor'ev (Д. Ю. Григорьев) and A. L. Chistov (А. Л. Чистов). Быстрое разложение многочленов на неприводимые и решение систем алгебраических уравнений (Russian) [Fast factorization of polynomials into irreducible ones and the solution of systems of algebraic equations]. *Докл. АН СССР*, 275(6):1302–1306, 1984.
- [206] D. A. Gudkov. The topology of real projective algebraic varieties. *Russian Mathematical Surveys*, 29(4):1–79, 1974. Transl. from Д. А. Гудков, Топология вещественных проективных алгебраических многообразий (Russian), УМН, 29(4):3–79, 1974.
- [207] D. A. Gudkov and G. A. Utkin. *Nine papers on Hilbert's 16th problem*, volume 112 of *American Mathematical Society Translations, Series 2*. American Mathematical Society, Providence, R.I., 1978. Transl. (by M. A. Dostal and M. D. Tretkoff) from Russian.
- [208] D. A. Gudkov (Д. А. Гудков). О расположении овалов кривой шестого порядка (Russian) [The arrangement of the ovals of a sixth order curve]. *Докл. АН СССР*, 185:260–263, 1969.
- [209] D. A. Gudkov (Д. А. Гудков). Построение новой серии М-кривых (Russian) [Construction of a new series of M-curves]. *Докл. АН СССР*, 200:1269–1272, 1971.
- [210] D. A. Gudkov (Д. А. Гудков). Построение кривой 6-го порядка типа $\frac{5}{1}$ (Russian) [Construction of a sixth order curve of type $\frac{5}{1}$]. *Изв. вузов. Матем.*, pages 28–36, 1973.
- [211] D. A. Gudkov (Д. А. Гудков) and A. D. Krakhnov (А. Д. Крахнов). О периодичности эйлеровой характеристики вещественных алгебраических $(M - 1)$ -многообразий (Russian) [Periodicity of Euler characteristic of real algebraic $(M - 1)$ -manifolds]. *Функционализ и его прил.*, 7:15–19, 1973.
- [212] B. Haas. A simple counterexample to Kouchnirenko's conjecture. *Beiträge Algebra Geom.*, 43(1):1–8, 2002.
- [213] J. Han. An Adaptive Grid Algorithm for Computing the Homology Group of Semialgebraic Set. Master's thesis, Université Paris Sud, 2018.
- [214] J. Han. An Adaptive Grid Algorithm for Computing the Homology Group of Semialgebraic Set, March 2019. (arXiv:1903.02388).
- [215] A. Harnack. Ueber die Vieltheiligkeit der ebenen algebraischen Curven (German) [On the many parts of level algebraic curves]. *Math. Ann.*, 10(2):189–198, 1876.
- [216] A. Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002.
- [217] J. Heinonen. *Lectures on Lipschitz analysis*, volume 100 of *Report. University of Jyväskylä Department of Mathematics and Statistics*. University of Jyväskylä, Jyväskylä, 2005.

- [218] J. Heintz, T. Krick, M.-F. Roy, and P. Solernó. Geometric problems solvable in single exponential time. In *Applied algebra, algebraic algorithms and error-correcting codes (Tokyo, 1990)*, volume 508 of *Lecture Notes in Comput. Sci.*, pages 11–23. Springer, Berlin, 1991.
- [219] J. Heintz, M.-F. Roy, and P. Solernó. Sur la complexité du principe de Tarski-Seidenberg. *Bull. Soc. Math. France*, 118(1):101–126, 1990.
- [220] J. Heintz, M.-F. Roy, and P. Solernó. Description of the connected components of a semialgebraic set in single exponential time. *Discrete Comput. Geom.*, 11(2):121–140, 1994.
- [221] N. J. Higham. *Accuracy and stability of numerical algorithms*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, second edition, 2002.
- [222] D. Hilbert. Ueber die reellen Züge algebraischer Curven (German) [On the real features of algebraic curves]. *Math. Ann.*, 38(1):115–138, 1891.
- [223] D. Hilbert. Mathematische Probleme (German) [Mathematical Problems]. In *Archiv der Mathematik und Physik*, volume 1 of *3rd series*, pages 213–237, Berlin and Leipzig, Germany, 1901. B. G. Teubner Verlag.
- [224] D. Hilbert. Mathematical problems. *Bull. Amer. Math. Soc.*, 8(10):437–479, 1902. Transl. from D. Hilbert, Mathematische Probleme (German), *Göttinger Nachrichten*, 253–297, 1900. and D. Hilbert, Mathematische Probleme (German). In *Archiv der Mathematik und Physik*, volume 1 of *3rd series*, pages 213–237, B.G. Teubner Verlag, Germany, 1901.
- [225] H. Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC ’90, pages 261–264. ACM, New York, 1990.
- [226] H. Hong. Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination. In *Papers from the International Symposium on Symbolic and Algebraic Computation*, ISSAC ’92, pages 177–188. ACM, New York, 1992.
- [227] F. Horn and R. Jackson. General mass action kinetics. *Arch. Rational Mech. Anal.*, 47:81–116, 1972.
- [228] R. Howard. The kinematic formula in Riemannian homogeneous spaces. *Mem. Amer. Math. Soc.*, 106(509):vi+69, 1993.
- [229] I. Itenberg. Contre-exemples à la conjecture de Ragsdale (French) [Counterexamples to Ragsdale’s conjecture]. *C. R. Acad. Sci. Paris Sér. I Math.*, 317(3):277–282, 1993.
- [230] I. Itenberg. Counter-examples to Ragsdale conjecture and T-curves. In *Real algebraic geometry and topology (East Lansing, MI, 1993)*, volume 182 of *Contemp. Math.*, pages 55–72. Amer. Math. Soc., Providence, RI, 1995.

- [231] I. Itenberg and M.-F. Roy. Multivariate Descartes' rule. *Beiträge Algebra Geom.*, 37(2):337–346, 1996.
- [232] I. Itenberg and O. Viro. Patchworking algebraic curves disproves the Ragsdale conjecture. *Math. Intelligencer*, 18(4):19–28, 1996.
- [233] G. Jäger. Parallel algorithms for computing the smith normal form of large matrices. In J. Dongarra, D. Laforenza, and S. Orlando, editors, *Recent Advances in Parallel Virtual Machine and Message Passing Interface*, pages 170–179, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
- [234] G. Jäger and C. Wagner. Efficient parallelization of Hermite and Smith normal form algorithms. *Parallel Comput.*, 35(6):345–357, 2009.
- [235] G. Jeronimo and D. Perrucci. A probabilistic symbolic algorithm to find the minimum of a polynomial function on a basic closed semialgebraic set. *Discrete Comput. Geom.*, 52(2):260–277, 2014.
- [236] G. Jeronimo, D. Perrucci, and E. Tsigaridas. On the minimum of a polynomial function on a basic closed semialgebraic set and applications. *SIAM J. Optim.*, 23(1):241–255, 2013.
- [237] K. Jin and J.-S. Cheng. Isotopic epsilon-meshing of real algebraic space curves. In *Proceedings of the 2014 Symposium on Symbolic-Numeric Computation*, SNC '14, pages 118–127. ACM, New York, 2014.
- [238] K. Jin and J.-S. Cheng. On the Complexity of Computing the Topology of Real Algebraic Space Curves, January 2019. (arXiv:1901.10317).
- [239] M. Kac. On the average number of real roots of a random algebraic equation. *Bull. Amer. Math. Soc.*, 49:314–320, 1943.
- [240] M. Kac. On the average number of real roots of a random algebraic equation. II. *Proc. London Math. Soc.* (2), 50:390–408, 1949.
- [241] N. Kaihnsa, M. Kummer, D. Plaumann, M. S. Namin, and B. Sturmfels. Sixty-Four Curves of Degree Six. *Exp. Math.*, 28(2):132–150, 2019.
- [242] R. Kannan and A. Bachem. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *Siam Journal on Computing*, 8(4):499–507, 1979.
- [243] M. Kerber. *Geometric algorithms for algebraic curves and surfaces*. PhD thesis, Max-Planck-Institut für Informatik, Saarbrücken, 2009.
- [244] M. Kerber and M. Sagraloff. A worst-case bound for topology computation of algebraic curves. *J. Symbolic Comput.*, 47(3):239–258, 2012.
- [245] V. Kharlamov and O. Y. Viro. Easy reading on topology of real plane algebraic curves. Available at: <http://www.math.stonybrook.edu/~0./easymath/introMSRI/introMSRI.html> [29/07/2019].

- [246] V. M. Kharlamov. The maximal number of components of a fourth degree surface in \mathbb{RP}^3 . *Functional Analysis and Its Applications*, 6(4):345–346, 1972. Transl. from B. M. Харламов, Максимальное число компонент поверхности 4-й степени в \mathbb{RP}^3 (Russian), *Функц. анализ и его прил.*, 6(4):101, 1972.
- [247] V. M. Kharlamov. New relations for the euler characteristic of real algebraic manifolds. *Functional Analysis and Its Applications*, 7(2):147–150, 1973. Transl. from B. M. Харламов, Новые сравнения для эйлеровой характеристики вещественных алгебраических многообразий (Russian), *Функц. анализ и его прил.*, 7(2):74–78, 1973.
- [248] V. M. Kharlamov. A generalized petrovskii inequality. *Functional Analysis and Its Applications*, 8(2):132–137, 1974. Transl. from B. M. Харламов, Обобщенное неравенство Петровского (Russian), *Функц. анализ и его прил.*, 8(2):50–56, 1974.
- [249] V. M. Kharlamov. Additional congruences for the euler characteristic of real algebraic manifolds of even dimensions. *Functional Analysis and Its Applications*, 9(2):134–141, 1975. Transl. from B. M. Харламов, Дополнительные сравнения для эйлеровой характеристики четномерных вещественных алгебраических многообразий (Russian), *Функц. анализ и его прил.*, 9(2):51–60, 1975.
- [250] V. M. Kharlamov. A generalized petrovskii inequality. ii. *Functional Analysis and Its Applications*, 9(3):266–268, 1975. Transl. from B. M. Харламов, Обобщенное неравенство Петровского. II (Russian), *Функц. анализ и его прил.*, 9(3):93–94, 1975.
- [251] V. M. Kharlamov. The topological type of nonsingular surfaces in \mathbb{RP}^3 of degree four. *Functional Analysis and Its Applications*, 10(4):295–305, 1976. Transl. from B. M. Харламов, Топологические типы неособых поверхностей степени 4 в \mathbb{RP}^3 (Russian), *Функц. анализ и его прил.*, 10(4):55–68, 1976.
- [252] V. M. Kharlamov. Isotopic types of nonsingular surfaces in \mathbb{RP}^3 of degree four. *Functional Analysis and Its Applications*, 12(1):68–69, 1978. Transl. from B. M. Харламов, Изотопические типы неособых поверхностей степени 4 в \mathbb{RP}^3 (Russian), *Функц. анализ и его прил.*, 12(1):86–87, 1978.
- [253] V. M. Kharlamov. Rigid isotopic classification of real planar curves of degree 5. *Functional Analysis and Its Applications*, 15(1):73–74, 1981. Transl. from B. M. Харламов, Жесткая изотопическая классификация вещественных плоских кривых степени 5 (Russian), *Функц. анализ и его прил.*, 15(1):88–89, 1981.
- [254] V. M. Kharlamov. Classification of nonsingular surfaces of degree 4 in \mathbb{RP}^3 with respect to rigid isotopies. *Functional Analysis and Its Applications*, 18(1):39–45, 1984. Transl. from B. M. Харламов, К классификации неособых поверхностей степени 4 в \mathbb{RP}^3 относительно жестких изотопии (Russian), *Функц. анализ и его прил.*, 18(1):49–56, 1984.
- [255] V. M. Kharlamov and I. Itenberg. Towards the maximal number of components of a nonsingular surface of degree 5 in \mathbb{RP}^3 . In *Topology of real algebraic varieties and*

- related topics*, volume 173 of *Amer. Math. Soc. Transl. Ser. 2*, pages 111–118. Amer. Math. Soc., Providence, RI, 1996.
- [256] A. G. Khovanskii. A class of systems of transcendental equations. *Dokl. Akad. Nauk SSSR*, 255(4):804–807, 1980.
- [257] A. G. Khovanskii. *Fewnomials*, volume 88 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1991.
- [258] A. G. Khovanskii (А. Г. Хованский). *Малочлены (Russian)*, volume 2 of *Библиотека Математика*. фазис, Moscow, 1996. Transl. from A. G. Khovanski, *Fewnomials*, volume 88 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1991.
- [259] F. Klein. Ueber Flächen dritter Ordnung (german) [on surfaces of degree three]. *Math. Ann.*, 6(4):551–581, 1873.
- [260] F. Klein. Ueber eine neue Art von Riemann’schen Flächen (german) [on a new kind of riemann surfaces]. *Math. Ann.*, 10(3):398–416, 1876.
- [261] A. Kobel and M. Sagraloff. On the complexity of computing with planar algebraic curves. *J. Complexity*, 31(2):206–236, 2015.
- [262] P. Koiran. Shallow circuits with high-powered inputs. *Proc. Second Symposium on Innovations in Computer Science, ICS*, 2011.
- [263] P. Koiran, N. Portier, and S. Tavenas. On the intersection of a sparse curve and a low-degree curve: a polynomial version of the lost theorem. *Discrete Comput. Geom.*, 53(1):48–63, 2015.
- [264] P. Koiran, N. Portier, and S. Tavenas. A Wronskian approach to the real τ -conjecture. *J. Symbolic Comput.*, 68(part 2):195–214, 2015.
- [265] E. Kostlan. On the distribution of roots of random polynomials. In *From Topology to Computation: Proceedings of the Smalefest*, pages 419–431. Springer, 1993.
- [266] R. Krone and K. Kubjas. Nonnegative rank four boundaries, February 2019. (arXiv:1902.02868).
- [267] K. Kubjas, E. Robeva, and R. Z. Robinson. Positive semidefinite rank and nested spectrahedra. *Linear Multilinear Algebra*, 66(10):1952–1974, 2018.
- [268] A. G. Kushnirenko. Letter to Professor Sottile (February 26, 2008). Available at: <https://www.math.tamu.edu/~sottile/research/pdf/Kushnirenko.pdf> [29/07/2019].
- [269] A. G. Kushnirenko. Newton polyhedron and milnor numbers. *Functional Analysis and Its Applications*, 9(1):71–72, 1975. Transl. from А. Г. Кушниренко. Многогранник Ньютона и числа Милнора (Russian). *Функц. анализ и его прил.*, 9(1):74–75, 1975.

- [270] A. G. Kushnirenko. How to guess the number of roots of a system of polynomial equations with fixed Newton polyhedron, 1976. Never published. Attachment to Kushnirenko's Letter to Professor Ottlie.
- [271] A. G. Kushnirenko. Newton polytopes and the bezout theorem. *Functional Analysis and Its Applications*, 10(3):233–235, 1976. Transl. from A. Г. Кушниренко. Многогранники Ньютона и теорема Безу (Russian). *Функц. анализ и его прил.*, 10(3):82–83, 1976.
- [272] P. Lairez. A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time. *Found. Comput. Math.*, 17(5):1265–1292, 2017.
- [273] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [274] J.-C. Latombe. Motion planning: A journey of robots, molecules, digital actors, and other artifacts. *The International Journal of Robotics Research*, 18(11):1119–1128, 1999.
- [275] J. M. Lee. *Introduction to smooth manifolds*, volume 218 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2013.
- [276] H. W. Lenstra, Jr. On the factorization of lacunary polynomials. In *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, pages 277–291. de Gruyter, Berlin, 1999.
- [277] T.-Y. Li, J. M. Rojas, and X. Wang. Counting real connected components of trinomial curve intersections and m -nomial hypersurfaces. *Discrete & Computational Geometry*, 30(3):379–414, 2003.
- [278] T. Y. Li and X. Wang. On multivariate Descartes' rule—a counterexample. *Beiträge Algebra Geom.*, 39(1):1–5, 1998.
- [279] J. E. Littlewood and A. C. Offord. On the number of real roots of a random algebraic equation. II. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 35, pages 133–148. Cambridge University Press, 1939.
- [280] G. Livshyts, G. Paouris, and P. Pivovarov. On sharp bounds for marginal densities of product measures. *Israel Journal of Mathematics*, 216(2):877–889, 2016.
- [281] M. Lotz. On the volume of tubular neighborhoods of real algebraic varieties. *Proc. Amer. Math. Soc.*, 143(5):1875–1889, 2015.
- [282] M. Lotz and V. Noferini. Wilkinson's bus: Weak condition numbers, with an application to singular polynomial eigenproblems, May 2019. (arXiv:1905.05466).
- [283] G. Malajovich and J. M. Rojas. High probability analysis of the condition number of sparse polynomial systems. *Theoretical computer science*, 315(2-3):525–555, 2004.

- [284] A. Marin. Quelques remarques sur les courbes algébriques planes réelles (French) [Some remarks on real plane algebraic curves]. In *Seminar on Real Algebraic Geometry (Paris, 1977/1978 and Paris, 1978/1979)*, volume 9 of *Publ. Math. Univ. Paris VII*, pages 51–68. Univ. Paris VII, Paris, 1980.
- [285] J. Mather. Notes on topological stability. *Bull. Amer. Math. Soc. (N.S.)*, 49(4):475–506, 2012. Reprint of lectures notes of a course given in the spring of 1970 at Harvard University.
- [286] C. C. McGeoch. Computer Science Sampler: Parallel Addition. *Amer. Math. Monthly*, 100(9):867–871, 1993.
- [287] K. Meer. Counting problems over the reals. In *Mathematical foundations of computer science 1997 (Bratislava)*, volume 1295 of *Lecture Notes in Comput. Sci.*, pages 398–407. Springer, Berlin, 1997.
- [288] K. Meer. Counting problems over the reals. *Theoret. Comput. Sci.*, 242(1-2):41–58, 2000.
- [289] K. Mehlhorn, M. Sagraloff, and P. Wang. From approximate factorization to root isolation. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC ’13, pages 283–290. ACM, New York, 2013.
- [290] K. Mehlhorn, M. Sagraloff, and P. Wang. From approximate factorization to root isolation with application to cylindrical algebraic decomposition. *J. Symbolic Comput.*, 66:34–69, 2015.
- [291] G. Mikhalkin. The complex separation of real surfaces and extensions of Rokhlin congruence. *Invent. Math.*, 118(2):197–222, 1994.
- [292] J. Milnor. On the Betti numbers of real varieties. *Proc. Amer. Math. Soc.*, 15:275–280, 1964.
- [293] B. Mourrain and J.-P. Técourt. Isotopic meshing of a real algebraic surface. Research Report RR-5508, INRIA, 2006.
- [294] A. Mucherino, C. Lavor, L. Liberti, and N. Maculan, editors. *Distance geometry: Theory, methods, and applications*. Springer, New York, 2013.
- [295] M. R. Muldoon, R. S. MacKay, J. P. Huke, and D. S. Broomhead. Topology from time series. *Phys. D*, 65(1-2):1–16, 1993.
- [296] S. Müller, E. Feliu, G. Regensburger, C. Conradi, A. Shiu, and A. Dickenstein. Sign conditions for injectivity of generalized polynomial maps with applications to chemical reaction networks and real algebraic geometry. *Found. Comput. Math.*, 16(1):69–97, 2016.
- [297] J. v. Neumann and H. Goldstine. Numerical inverting matrices of high order. *Bull. Amer. Math. Soc.*, 53:1021–1099, 1947.

- [298] V. V. Nikulin. Integral symmetric bilinear forms and some of their applications. *Mathematics of the USSR-Izvestiya*, 14(1):103–167, 1980. Transl. from B. B. Никулин, Целочисленные симметрические билинейные формы и некоторые их геометрические приложения (Russian), *Изв. АН СССР. Сер. матем.*, 43(1):111–177, 1979.
- [299] V. V. Nikulin. Involutions of integral quadratic forms and their applications to real algebraic geometry. *Mathematics of the USSR-Izvestiya*, 22(1):99–172, 1984. Transl. from B. B. Никулин, Инволюции целочисленных квадратичных форм и их приложения к вещественной алгебраической геометрии (Russian), *Изв. АН СССР. Сер. матем.*, 47(1):109–188, 1983.
- [300] P. Niyogi, S. Smale, and S. Weinberger. Finding the homology of submanifolds with high confidence from random samples. *Discrete Comput. Geom.*, 39(1-3):419–441, 2008.
- [301] P. Niyogi, S. Smale, and S. Weinberger. A topological view of unsupervised learning from noisy data. *SIAM J. Comput.*, 40(3):646–663, 2011.
- [302] V. Noferini and A. Townsend. Numerical instability of resultant methods for multidimensional rootfinding. *SIAM J. Numer. Anal.*, 54(2):719–743, 2016.
- [303] O. A. Oleinik (О. А. Олейник). О топологии действительных алгебраических кривых на алгебраической поверхности (Russian) [On the topology of real algebraic curves on algebraic surfaces]. *Матем. сб.*, 29(71):133–156, 1951.
- [304] O. A. Oleinik (О. А. Олейник). Оценки чисел Бетти действительных алгебраических гиперповерхностей (russian) [estimates of the Betti numbers of real algebraic hypersurfaces]. *Матем. сб.*, 28(70):635–640, 1951.
- [305] S. Y. Orevkov. Real quintic surface with 23 components. *C. R. Acad. Sci. Paris Sér. I Math.*, 333(2):115–118, 2001.
- [306] S. Y. Orevkov. Classification of flexible M-curves of degree 8 up to isotopy. *Geom. Funct. Anal.*, 12(4):723–755, 2002.
- [307] S. Y. Orevkov and V. M. Kharlamov. Asymptotic growth of the number of classes of real plane algebraic curves as the degree grows. *Journal of Mathematical Sciences*, 113(5):666–674, 2003. Transl. from С. Ю. Оревков and В. М. Харламов, Порядок роста числа классов вещественных плоских алгебраических кривых при возрастании степени (Russian). In *Теория представлений, динамические системы, комбинаторные и алгоритмические методы. V*, volume 266 of Зап. научн. сем. ПОМИ, pages 218–233, St. Petersburg, Russia. ПОМИ.
- [308] C. H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.
- [309] M. Pérez Millán and A. Dickenstein. The structure of MESSI biological systems. *SIAM J. Appl. Dyn. Syst.*, 17(2):1650–1682, 2018.

- [310] M. Pérez Millán, A. Dickenstein, A. Shiu, and C. Conradi. Chemical reaction systems with toric steady states. *Bull. Math. Biol.*, 74(5):1027–1065, 2012.
- [311] I. Petrovskii. On the topology of real plane algebraic curves. *Ann. of Math. (2)*, 39(1):189–209, 1938.
- [312] I. G. Petrovskii (И. Г. Петровский) and O. A. Oleĭnik (О. А. Олейник). О топологии действительных алгебраических поверхностей (russian) [on the topology of real algebraic surfaces]. *Изв. АН СССР. Сер. матем.*, 13:389–402, 1949.
- [313] K. Phillipson and J. M. Rojas. Fewnomial systems with many roots, and an adelic tau conjecture. In *Proceedings of Bellairs workshop on tropical and non-Archimedean geometry (May 6–13, 2011, Barbados)*, *Contemporary Mathematics*, volume 605, pages 45–71, 2014.
- [314] G. Pistone, E. Riccomagno, and H. P. Wynn. *Algebraic statistics*, volume 89 of *Monographs on Statistics and Applied Probability*. Chapman & Hall/CRC, Boca Raton, FL, 2001. Computational commutative algebra in statistics.
- [315] S. Plantinga and G. Vegter. Isotopic approximation of implicit curves and surfaces. In *Proceedings of the 2004 Eurographics/ACM SIGGRAPH Symposium on Geometry Processing*, SGP ’04, pages 245–254. ACM, New York, 2004.
- [316] G. M. Polotovskii. An algorithm for determining the topological type of a structurally stable plane algebraic curve of even degree. In *Качественные методы теории дифференциальных уравнений и их приложения (Russian)* [Qualitative methods of the theory of differential equations and their applications], Gor'kov. Gos. Univ. Učen. Zap., pages 143–187. Gor'kov. Gosudarstv. Univ., Gorki, 1973.
- [317] G. M. Polotovskii. On the classification of non-singular curves of degree 8. In O. Y. Viro and A. M. Vershik, editors, *Topology and Geometry – Rohlin Seminar*, pages 455–485. Springer Berlin Heidelberg, Berlin, Heidelberg, 1988.
- [318] G. M. Polotovskii (Г. М. Полотовский). В. В. Морозов, Д. А. Гудков и первая часть 16-й проблемы Гильберта (Russian) [V. V. Morozov, D. A. Gudkov and the first part of the 16th Hilbert problem]. Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки, 154(2):31–43, 2012.
- [319] B. Poonen. Zeros of sparse polynomials over local fields of characteristic p . *Math. Res. Lett.*, 5(3):273–279, 1998.
- [320] V. Ragsdale. On the Arrangement of the Real Branches of Plane Algebraic Curves. *Amer. J. Math.*, 28(4):377–404, 1906.
- [321] H. Ratschek and J. Rokne. *Computer methods for the range of functions*. Ellis Horwood Series: Mathematics and its Applications. Ellis Horwood Ltd., Chichester; Halsted Press [J. Wiley & Sons, Inc.], New York, 1984.

- [322] J. H. Reif. Complexity of the Mover's Problem and Generalizations. In *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, SFCS '79, pages 421–427, Washington, DC, USA, 1979. IEEE Computer Society.
- [323] J. H. Reif. Complexity of the Generalized Mover's Problem. Technical report, Harvard University, Aiken Computation Lab, 1985.
- [324] A. Renaudineau and K. Shaw. Bounding the Betti numbers of real hypersurfaces near the tropical limit, May 2018. (arXiv:1805.02030).
- [325] J. Renegar. Recent progress on the complexity of the decision problem for the reals. In *Discrete and computational geometry (New Brunswick, NJ, 1989/1990)*, volume 6 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 287–308. Amer. Math. Soc., Providence, RI, 1991.
- [326] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. I. Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals. *J. Symbolic Comput.*, 13(3):255–299, 1992.
- [327] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. II. The general decision problem. Preliminaries for quantifier elimination. *J. Symbolic Comput.*, 13(3):301–327, 1992.
- [328] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. III. Quantifier elimination. *J. Symbolic Comput.*, 13(3):329–352, 1992.
- [329] J. Renegar. Some perturbation theory for linear programming. *Math. Programming*, 65(1, Ser. A):73–91, 1994.
- [330] J. Renegar. Incorporating condition measures into the complexity theory of linear programming. *SIAM J. Optim.*, 5(3):506–524, 1995.
- [331] J. Renegar. Linear programming, complexity theory and elementary functional analysis. *Math. Programming*, 70(3, Ser. A):279–351, 1995.
- [332] J. Richter-Gebert. *Realization spaces of polytopes*, volume 1643 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.
- [333] V. Robins. Towards computing homology from finite approximations. In *Proceedings of the 14th Summer Conference on General Topology and its Applications (Brookville, NY, 1999)*, volume 24, pages 503–532 (2001), 1999.
- [334] V. Robins, J. D. Meiss, and E. Bradley. Computing connectedness: an exercise in computational topology. *Nonlinearity*, 11(4):913–922, 1998.
- [335] V. Robins, J. D. Meiss, and E. Bradley. Computing connectedness: disconnectedness and discreteness. *Phys. D*, 139(3-4):276–300, 2000.

- [336] D. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.
- [337] K. Rohn. Die Maximalzahl und Anordnung der Ovale bei der ebenen Kurve 6. Ordnung und bei der Fläche 4. Ordnung (german) [the maximal number and arrangement of ovals of a level curve of degree 6 and of a surface of degree 4]. *Math. Ann.*, 73(2):177–229, 1913.
- [338] J. M. Rojas. On the average number of real roots of certain random sparse polynomial systems. *Lectures in Applied Mathematics*, 32:689–700, 1996.
- [339] J. M. Rojas. Arithmetic multivariate Descartes’ rule. *Amer. J. Math.*, 126(1):1–30, 2004.
- [340] V. A. Rokhlin. Congruences modulo 16 in Hilbert’s sixtieth problem. *Functional Analysis and Its Applications*, 6(4):301–306, 1972. Transl. from B. A. Рохлин, Сравнения по модулю 16 в шестнадцатой проблеме Гильберта (Russian), *Функц. анализ и его прил.*, 6(4):58–64, 1972.
- [341] V. A. Rokhlin. Proof of Gudkov’s hypothesis. *Functional Analysis and Its Applications*, 6(2):136–138, 1972. Transl. from B. A. Рохлин, Доказательство гипотезы Гудкова (Russian), *Функц. анализ и его прил.*, 6(2):62–64, 1972.
- [342] V. A. Rokhlin. Congruence modulo 16 in Hilbert’s sixteenth problem. ii. *Functional Analysis and Its Applications*, 7(2):163–164, 1973. Transl. from B. A. Рохлин, Сравнения по модулю 16 в шестнадцатой проблеме Гильберта. II (Russian), *Функц. анализ и его прил.*, 7(2):91–92, 1973.
- [343] V. A. Rokhlin. Complex orientations of real algebraic curves. *Functional Analysis and Its Applications*, 8(4):331–334, 1974. В. А. Рохлин, Комплексные ориентации вещественных алгебраических кривых (Russian), *Функц. анализ и его прил.*, 8(4):71–75, 1974.
- [344] V. A. Rokhlin. Complex topological characteristics of real algebraic curves. *Russian Mathematical Surveys*, 33(5):85–98, 1978. Transl. from B. A. Рохлин, Комплексные топологические характеристики вещественных алгебраических кривых (Russian), УМН, 33(5):77–89, 1978.
- [345] V. A. Rokhlin. New inequalities in the topology of real planar algebraic curves. *Functional Analysis and Its Applications*, 14(1):29–33, 1980. Transl. from B. A. Рохлин, Новые неравенства в топологии вещественных плоских алгебраических кривых (Russian), *Функц. анализ и его прил.*, 14(1):37–43, 1980.
- [346] J. J. Rotman. *An introduction to algebraic topology*, volume 119 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988.
- [347] J. J. Rotman. *An introduction to homological algebra*. Universitext. Springer, New York, second edition, 2009.

- [348] M.-F. Roy. Computation of the topology of a real curve. *Astérisque*, 192:17–33, 1990. Algorithmique, topologie et géométrie algébriques (Seville, 1987 and Toulouse, 1988).
- [349] M.-F. Roy. The role of Hilbert problems in real algebraic geometry. In *European women in mathematics (Loccum, 1999)*, pages 189–200. Hindawi Publ. Corp., Cairo, 2000.
- [350] M.-F. Roy and A. Szpirglas. Complexity of the computation of cylindrical decomposition and topology of real algebraic curves using thom’s lemma. In M. Galbiati and A. Tognoli, editors, *Real Analytic and Algebraic Geometry*, pages 223–236, Berlin, Heidelberg, 1990. Springer Berlin Heidelberg.
- [351] M. Rudelson and R. Vershynin. Small ball probabilities for linear images of high-dimensional distributions. *Int. Math. Res. Not. IMRN*, 19:9594–9617, 2015.
- [352] M. Safey el Din and E. Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete Comput. Geom.*, 45(1):181–220, 2011.
- [353] M. Safey El Din and E. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6):48:1–48:37, Jan. 2017.
- [354] P. Scheiblechner. *On the Complexity of Counting Irreducible Components and Computing Betti Numbers of Algebraic Varieties*. PhD thesis, Universität Paderborn, 2007.
- [355] P. Scheiblechner. On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety. *J. Complexity*, 23(3):359–379, 2007.
- [356] P. Scheiblechner. *Complexity of Counting Components of Algebraic Varieties – Irreducible and Connected Components, Betti Numbers*. VDM Verlag Dr. Müller, 2008.
- [357] P. Scheiblechner. Castelnuovo-Mumford regularity and computing the de Rham cohomology of smooth projective varieties. *Found. Comput. Math.*, 12(5):541–571, 2012.
- [358] L. Schläfli. On the distribution of surfaces of the third order into species, in reference to the absence or presence of singular points, and the reality of their lines. *Phil. Trans. Roy. Soc. London*, 153:193–241, 1863.
- [359] J. T. Schwartz and M. Sharir. A survey of motion planning and related geometric algorithms. *Artificial Intelligence*, 37(1-3):157–169, 1988. Geometric reasoning (Oxford, 1986).
- [360] M. O. Searcoid. *Metric spaces*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 2007.
- [361] S. M. Sedjelmaci. Two fast parallel gcd algorithms of many integers. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC ’17, pages 397–404. ACM, New York, 2017.

- [362] A. Seidenberg. A new decision method for elementary algebra. *Ann. of Math.* (2), 60:365–374, 1954.
- [363] B. Shiffman and S. Zelditch. Random polynomials with prescribed Newton polytope. *Journal of the American Mathematical Society*, 17(1):49–108, 2004.
- [364] B. Shiffman and S. Zelditch. Random complex fewnomials, I. In *Notions of positivity and the geometry of polynomials*, Trends Math., pages 375–400. Birkhäuser/Springer Basel AG, Basel, 2011.
- [365] M. Shub. Complexity of Bezout’s theorem. VI. Geodesics in the condition (number) metric. *Found. Comput. Math.*, 9(2):171–178, 2009.
- [366] M. Shub and S. Smale. Complexity of Bézout’s Theorem I: geometric aspects. *Journal of the Amer. Math. Soc.*, 6:459–501, 1993.
- [367] M. Shub and S. Smale. Complexity of Bézout’s Theorem II: volumes and probabilities. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 267–285. Birkhäuser, 1993.
- [368] M. Shub and S. Smale. Complexity of Bézout’s Theorem III: condition number and packing. *Journal of Complexity*, 9:4–14, 1993.
- [369] M. Shub and S. Smale. Complexity of Bézout’s Theorem V: polynomial time. *Theoret. Comp. Sci.*, 133:141–164, 1994.
- [370] M. Shub and S. Smale. Complexity of Bézout’s Theorem IV: probability of success; extensions. *SIAM J. of Numer. Anal.*, 33:128–148, 1996.
- [371] E. I. Shustin. Counterexamples to a conjecture of Rokhlin. *Functional Analysis and Its Applications*, 19(2):162–163, 1985. Transl. from Е. И. Шустин, Контрпримеры к гипотезе Рохлина. *Функц. анализ и его прил.*, 19(2):94–95, 1985.
- [372] E. I. Shustin. A new m -curve of degree 8. *Mathematical notes of the Academy of Sciences of the USSR*, 42(2):606–610, 1987. Transl. from Е. И. Шустин, Новая M -кривая 8-й степени. *Матем. заметки*, 42(2):180–186, 1987.
- [373] E. I. Shustin. New restrictions on the topology of real curves of degree a multiple of 8. *Mathematics of the USSR-Izvestiya*, 37(2):421–443, 1991. Transl. from Е. И. Шустин, Новые ограничения на топологию вещественных кривых степени, кратной 8. *Изв. АН СССР. Сер. матем.*, 54(5):1069–1089, 1990.
- [374] S. Smale. Complexity theory and numerical analysis. In A. Iserles, editor, *Acta Numerica*, pages 523–551. Cambridge University Press, 1997.
- [375] S. Smale. Mathematical problems for the next century. *Mathematical Intelligencer*, 20:7–15, 1998.
- [376] J. M. Snyder. *Generative modeling for computer graphics and CAD: Symbolic shape design using interval analysis*. Academic Press, Inc., Boston, MA, 1992.

- [377] J. M. Snyder. Interval analysis for computer graphics. *SIGGRAPH Comput. Graph.*, 26(2):121–130, 1992.
- [378] F. Sottile. *Real solutions to equations from geometry*, volume 57 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2011.
- [379] E. Spanier. *Algebraic Topology*. McGraw-Hill, New York, 1966.
- [380] D. A. Spielman and S.-H. Teng. Smoothed analysis of algorithms. In *Proceedings of the International Congress of Mathematicians*, volume I, pages 597–606, 2002.
- [381] M. Spivak. *A comprehensive introduction to differential geometry. Vol. I*. Publish or Perish Inc., Wilmington, Del., 2nd edition, 1979.
- [382] B. T. Stander and J. C. Hart. Guaranteeing the topology of an implicit surface polygonization for interactive modeling. In *ACM SIGGRAPH 2005 Courses*, SIGGRAPH ’05. ACM, New York, 2005.
- [383] A. Storjohann. Near optimal algorithms for computing smith normal forms of integer matrices. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, ISSAC ’96, pages 267–274. ACM, New York, 1996.
- [384] V. Strassen. Gaussian elimination is not optimal. *Numer. Math.*, 13:354–356, 1969.
- [385] B. Sturmfels. On the number of real roots of a sparse polynomial system. In *HAMILTONIAN AND GRADIENT FLOWS, ALGORITHMS AND CONTROL*, volume 3 of *Fields Inst. Commun.*, pages 137–143. Amer. Math. Soc., Providence, RI, 1994.
- [386] A. Tarski. *A decision method for elementary algebra and geometry*. University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.
- [387] R. Thom. Sur l’homologie des variétés algébriques réelles (French) [On the homology of real algebraic varieties]. In *Differential and Combinatorial Topology (A Symposium in Honor of Marston Morse)*, pages 255–265. Princeton Univ. Press, Princeton, N.J., 1965.
- [388] R. Thom. Ensembles et morphismes stratifiés (French) [Stratified sets and morphisms]. *Bull. Amer. Math. Soc.*, 75:240–284, 1969.
- [389] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991.
- [390] J. Tonelli-Cueto. Norms and numerical algorithms adapted to the cube. I: Hypersurfaces [Working title], 2020. In progress.
- [391] J. Tonelli-Cueto. The Miranda algorithm of Xu and Yap takes average polynomial time [Working title], 2020. In progress.
- [392] L. N. Trefethen and D. Bau, III. *Numerical linear algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1997.

- [393] A. Turing. Rounding-off errors in matrix processes. *Quart. J. Mech. Appl. Math.*, 1:287–308, 1948.
- [394] A. M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proc. London Math. Soc. (2)*, 42(3):230–265, 1936.
- [395] G. A. Utkin. Construction of an m -surface of fourth order in \mathbb{RP}^3 . *Functional Analysis and Its Applications*, 8(2):179–181, 1974. Transl. from Г. А. Уткин, Построение одной М-поверхности четвертого порядка в \mathbb{RP}^3 (Russian), *Функц. анализ и его прил.*, 8(2):91–92, 1974.
- [396] G. A. Utkin (Г. А. Уткин). О топологической классификации неособых поверхностей четвертого порядка (russian) [topological classification of non-singular fourth-order surfaces]. *Докл. АН СССР*, 175(1):40–43, 1967.
- [397] G. A. Utkin (Г. А. Уткин). Построение поверхности четвертого порядка, состоящей из десяти компонент (russian) [construction of a fourth order surface that consists of ten components]. *Изв. вузов. Матем.*, pages 116–117, 1977.
- [398] R. Vershynin. Introduction to the non-asymptotic analysis of random matrices. In *Compressed sensing*, pages 210–268. Cambridge Univ. Press, Cambridge, 2012.
- [399] R. Vershynin. *High-dimensional probability: An introduction with applications in data science*, volume 47 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, 2018.
- [400] G. Villard. Fast parallel computation of the smith normal form of polynomial matrices. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC ’94, pages 312–317. ACM, New York, 1994.
- [401] O. Viro. Construction of M-surfaces. *Functional Analysis and Its Applications*, 13(3):212–213, Jul 1979. Transl. from О. Я. Виро, Построение М-поверхностей. *Функц. анализ и его прил.*, 13(3):71–72, 1979.
- [402] O. Viro. Encomplexing the writhe. In *Topology, ergodic theory, real algebraic geometry*, volume 202 of *Amer. Math. Soc. Transl. Ser. 2*, pages 241–256. Amer. Math. Soc., Providence, RI, 2001.
- [403] O. Viro and Y. Drobotukhina. Configurations of skew-lines. *Leningrad Mathematical J.*, 1(4):1027–1050, 1990. Transl. from О. Я. Виро and Ю. В. Дроботухина, Конфигурации скрещивающихся прямых. *Алгебра и анализ*, 1(4):222–246, 1989.
- [404] O. Y. Viro. Introduction to topology of real algebraic varieties. Available at: <http://www.math.stonybrook.edu/~0./easymath/es/es.html> [29/07/2019].
- [405] O. Y. Viro. Gluing of plane real algebraic curves and constructions of curves of degrees 6 and 7. In *Topology (Leningrad, 1982)*, volume 1060 of *Lecture Notes in Math.*, pages 187–200. Springer, Berlin, 1984.

- [406] O. Y. Viro. Real plane curves of degrees 7 and 8: new prohibitions. *Mathematics of the USSR-Izvestiya*, 23(2):409–422, 1984. Transl. from О. Я. Виро, Плоские вещественные кривые степеней 7 и 8: новые запреты (Russian), *Изв. АН СССР. Сер. матем.*, 47(5):1135–1150, 1983.
- [407] O. Y. Viro. Real plane algebraic curves: constructions with controlled topology. *Leningrad Math. J.*, 1(5):1059–1134, 1990. Transl. from О. Я. Виро, Плоские вещественные алгебраические кривые: построения с контролируемой топологией (Russian), *Алгебра и анализ*, 1(5):1–73, 1989.
- [408] O. Y. Viro. From the sixteenth Hilbert problem to tropical geometry. *Jpn. J. Math.*, 3(2):185–214, 2008.
- [409] O. Y. Viro and S. Y. Orevkov. Congruence mod 8 for real algebraic curves of degree 9. *Russian Mathematical Surveys*, 56(4):770–771, 2001. Transl. from О. Я. Виро and С. Ю. Оревков, Сравнение по модулю 8 для вещественных алгебраических кривых степени 9, *УМН*, 56(4):137–138, 2001.
- [410] O. Viro (О. Я. Виро). Топологические задачи о прямых и точках трехмерного пространства (Russian) [Topological problems on lines and points of three-dimensional space]. *Докл. АН СССР*, 284(5):1049–1052, 1985.
- [411] O. Y. Viro (О. Я. Виро). Кривые степени 7, кривые степени 8 и гипотеза Рэгсдейл (russian) [curves of degree 7, curves of degree 8, and the ragsdale conjecture]. *Докл. АН СССР*, 254:1306–1310, 1980.
- [412] N. N. Vorob'ev and D. Y. Grigor'ev. Finding connected components of a semialgebraic set in subexponential time. *Journal of Mathematical Sciences*, 70(4):1847–1872, 1994. Transl. from Н. Н. Воробьев (мл.) and Д. Ю. Григорьев, Нахождение компонент связности полуалгебраического множества в субэкспоненциальное время. In *Теория сложности вычислений*. 5, volume 192 of Зап. научн. сем. ЛОМИ, pages 3–46, Наука, 1991.
- [413] N. N. Vorobjov and D. Y. Grigor'ev. Solving systems of polynomial inequalities over a real closed field in subexponential time. *Journal of Soviet Mathematics*, 55(2):1519–1540, 1991. Transl. from Н. Н. Воробьев (мл.) and Д. Ю. Григорьев, Решение систем полиномиальных неравенств над вещественно замкнутым полем в субэкспоненциальное время, *Теория сложности вычислений*. 3, 174:3–36, 1988.
- [414] N. N. Vorobjov (Н. Н. Воробьев) and D. Y. Grigor'ev (Д. Ю. Григорьев). Нахождение вещественных решений систем алгебраических неравенств в субэкспоненциальное время (Russian) [Finding real solutions of systems of algebraic inequalities in subexponential time]. *Докл. АН СССР*, 283(6):1294–1299, 1985.
- [415] Z. Wan. Computing the Smith forms of integer matrices and solving related problems. PhD thesis, University of Delaware, 2005.

- [416] G. Wang and Z. Xu. A Survey of Computations of Homotopy Groups of Spheres and Cobordism. Available at: <http://math.mit.edu/~guozhen/homotopygroups.pdf> [03/08/2019], 2010.
- [417] V. Weispfenning. The complexity of linear problems in fields. *J. Symbolic Comput.*, 5(1-2):3–27, 1988.
- [418] J. H. Wilkinson. Some comments from a numerical analyst. *J. Assoc. Comput. Mach.*, 18:137–147, 1971.
- [419] H. Wüthrich. Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper. In E. Specker and V. Strassen, editors, *Komplexität von Entscheidungsproblemen*, volume 43 of *Lect. Notes in Comp. Sci.*, pages 138–162. Springer-Verlag, 1976.
- [420] J. Xu and C. Yap. Effective subdivision algorithm for isolating zeros of real systems of equations, with complexity analysis. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, ISSAC ’19, pages 355–362. ACM, New York, 2019.
- [421] C. Yap. Towards soft exact computation (invited talk). In M. England, W. Koepf, T. M. Sadykov, W. M. Seiler, and E. V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing*, pages 12–36, Cham, 2019. Springer International Publishing.
- [422] C. K. Yap. In praise of numerical computation. In S. Albers, H. Alt, and S. Näher, editors, *Efficient Algorithms: Essays Dedicated to K. Mehlhorn on the Occasion of His 60th Birthday*, pages 380–407. Springer, 2009.
- [423] H. G. Zeuthen. Études géométriques de quelques-unes des propriétés de deux surfaces dont les points se correspondent un-à-un (French) [Geometric studies of some of the properties of two surfaces whose points correspond one-to-one]. *Math. Ann.*, 4(1):21–49, 1871.
- [424] G. M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics. Springer New York, 2012.
- [425] A. Zomorodian. Fast construction of the Vietoris-Rips complex. *Computers & Graphics*, 34(3):263 – 271, 2010. Shape Modelling International (SMI) Conference 2010.

References for used quotes in chapter heads and rhetorics

- [Q1] E. Bishop. *Foundations of Constructive Analysis*. McGraw-Hill Book Co., 1967.
- [Q2] E. Bishop. Schizophrenia in contemporary mathematics. In *Errett Bishop: reflections on him and his research (San Diego, Calif., 1983)*, volume 39 of *Contemp. Math.*, pages 1–32. Amer. Math. Soc., Providence, RI, 1985.
- [Q3] X. Deng. *Selected Works of Deng Xiaoping – Volume I (1938-1965)*. Foreign Language Press, Beijing, 2nd edition, 1995. Transl. from 邓小平, 邓小平文选/第一卷 (Chinese). 人民出版社, Beijing, 2nd edition, 1994.
- [Q4] X. Deng (邓小平). 邓小平文选/第一卷. (Chinese) [Selected Works of Deng Xiaoping/Volume I]. 人民出版社 [People's Publishing House], Beijing, 2nd edition, 1994.
- [Q5] J. Fenby. *The Penguin history of modern China: The fall and rise of a great power, 1850-2009*. Penguin Books, London, 2008.
- [Q6] P. Feyerabend. *Wissenschaft als Kunst. (German) [Science as Art]*. Suhrkamp Verlag, Frankfurt am Main, 1984.
- [Q7] R. P. Feynman and R. Leighton. *Surely You're Joking, Mr. Feynman!* WW. Norton Company, Inc, New York, 1985.
- [Q8] D. Hilbert. *Gesammelte Abhandlungen III (German) [Collected writings III]*. Verlag von Julius Springer, Berlin, 1935.
- [Q9] A. G. Kushnirenko. Letter to Professor Sottile (February 26, 2008). Available at: <https://www.math.tamu.edu/~sottile/research/pdf/Kushnirenko.pdf> [29/07/2019].
- [Q10] R. F. Lyon. A brief history of 'pixel'. In *Digital Photography II*, volume 6069, page 606901. International Society for Optics and Photonics, 2006.
- [Q11] G. Orwell. *Animal Farm: A Fairy Story*. Houghton Mifflin Harcourt, Boston, 2009.
- [Q12] G. Peano. Sur une courbe, qui remplit toute une aire plane (French) [On a curve, which fills a whole flat area]. *Math. Ann.*, 36(1):157–160, 1890.
- [Q13] M. C. Salaman. *The Old Engravers of England in Their Relation to Contemporary Life and Art (1540-1800)*. Cassell and Company, 1906.

- [Q14] P. Signac. *D'Eugène Delacroix au néo-impressionnisme*. H. Flourey, Libraire-Éditeur, Paris, 1911.
- [Q15] J. T. Smith. David Hilbert's Radio Address. *Loci: Convergence*, 11, February 2014.
- [Q16] M. Spivak. *The Joy of \TeX : A Gourmet Guide to Typesetting with the $\text{\textit{AMS-}\TeX}$ Macro Package*. American Mathematical Society, Boston, MA, USA, 1st edition, 1997.

Used auxiliary resources for \LaTeX

- [L1] \TeX ample.net. <http://www.texample.net/>.
- [L2] CTAN. The Comprehensive \TeX Archive Network. <https://www.ctan.org/>.
- [L3] Detexify. <http://detexify.kirelabs.org/>.
- [L4] \TeX - \LaTeX Stack Exchange. <http://tex.stackexchange.com/>.
- [L5] \LaTeX . Wikibooks, The Free Textbook Project. <https://en.wikibooks.org/wiki/\LaTeX>.

After giving You our life, Mathematics,
which theorem will You reveal to us?
Long after we are not longer remembered,
will our names still inhabit Your world?
Once humanity becomes extinct in the universe,
will You still be there?
Or will You go away with all these other abstractions of the naked monkeys?

lasafro Maesman