Marie-Françoise Roy

Saugata Basu

Figure 1. Marie-Françoise in her office in Rennes (c.1997).

1. Brief Biography

Marie-Françoise Roy was born in Paris in 1950. She was educated at Lycée Condorcet, École Normale Supérieure de jeunes filles and Université Paris 7. Married to Michel Coste since 1971, she has two children Denis and Elise and two grandsons Pierre and Alexandre. She started teaching at University of Rennes in 1972 and continued at Université Paris Nord where she received her habilitation in 1980, supervised by Jean Bénabou. In 1981–1983 she spent two years at Abdou Moumouni University in Niger. In 1985 she became a professor of Mathematics at University of Rennes, where she is currently an emerita professor.

She was the president of Société Mathématique de France (SMF) from 2004 to 2007. In 2004, she received an Irène Joliot-Curie Prize and in 2009 she was made a Chevalier of the French Legion of Honour.

2. Mathematical Works

2.1. **Background.** The major part of Marie-Françoise's work has to do with various aspects of real algebraic geometry. So to put her work in the proper perspective it is good to start with a little bit of history. Historically, real algebraic geometry can be said to have two origins—both of which continues to play an important role as evidenced indeed by the works of Marie-Françoise herself.

Hilbert's 17th problem: Artin's theorem. The origin of real algebraic geometry can be arguably traced back to Artin's solution to Hilbert's 17th problem (in the famous list of 23 problems presented by Hilbert in the first International Congress of Mathematicians in Paris, in 1900 [12]). Hilbert's 17th problem concerns polynomials in $\mathbb{R}[X_1,\ldots,X_n]$ which take nonnegative values at each point in $\mathbb{R}^n$. Obviously any polynomial which is a sum of squares of polynomials has this property. But what about the converse? It is an easy exercise to verify that the converse is also true for polynomials in one variable, i.e., every nonnegative polynomial in $\mathbb{R}[X]$ is a sum of at most two squares (hint. use the "two squares" identity namely, $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$, and the fact that every polynomial in $\mathbb{R}[X]$ factors into linear and quadratic factors, where each quadratic factor is a sum of squares). It is also easy to check that any nonnegative polynomial of degree 2 in n variables is a sum of squares of at most n polynomials of degree one (hint. use Sylvester's inertia law). Hilbert also observed that the converse holds in one other case (degree 4 polynomials in two variables) but fails to hold in every other case. He asked nevertheless whether every nonnegative real polynomial is a sum of squares of *rational functions*. Artin [1] resolved this question in his seminal paper by proving Hilbert's statement. In the process he introduced the notion of a *real closed field*.

A real closed field R is an ordered field in which every positive element is a square and which satisfies the *intermediate value property* for polynomials (i.e., for each polynomial $P\in \mathrm{R}[X]$ and $a,b\in \mathrm{R}$ with $a<b$, $P(a)P(b)<0$ implies that there exists $c\in \mathrm{R}$ with $a<c<b$ and $P(c)=0$). The field of real numbers, $\mathbb{R}$, as well as well its subfield of real algebraic numbers are familiar examples of real closed fields. These fields satisfy the Archimedean property, but there exist non-Archimedean real closed fields such as the field $\mathrm{R}\langle\langle\varepsilon\rangle\rangle$ of *Puiseux series* in ε with coefficients in a real closed field R. Real closed fields admit a unique ordering (compatible with the field operations), and in this unique order the element $\varepsilon\in \mathrm{R}\langle\langle\varepsilon\rangle\rangle$ is positive but smaller than every positive element of R (ε is often referred to as an *infinitesimal*). The fields of such Puiseux series in one or more "infinitesimals" play an important role in algorithmic real algebraic geometry and they will be mentioned

Saugata Basu is a professor in the Department of Mathematics at Purdue University. His email address is sbasu@math.purdue.edu.

Communicated by Notices *Associate Editor Han-Bom Moon.*

DOI: https://doi.org/10.1090/noti2900

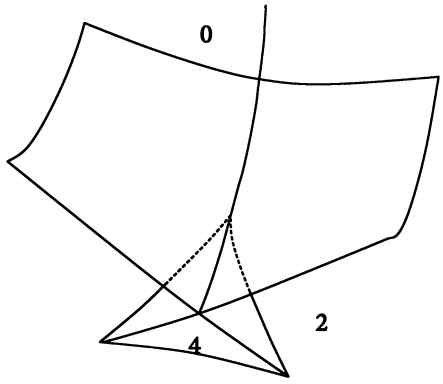


Figure 2. The discriminant hypersurface of the real quartic polynomial in one variable.

several times later in the article. In the rest of this article R will always denote a real closed field.

First order logic: Tarski's theorem. A second root of the subject originates in logic and the work of Tarski [22] who proved that the first order theory of the reals admits quantifier elimination and is decidable.

One usually meets an easy example of this theorem in middle school. The existentially quantified formula

$$(\exists X)X^2 + 2bX + c = 0$$

is equivalent modulo the first-order theory of the reals to the quantifier-free formula

$$b^2 - c \geq 0 \tag{1}$$

(we refrain from defining precisely what we mean by a formula but just say that a formula is built out of atoms of the form $P = 0, P > 0$ where P is a polynomial, logical connectives $\vee, \wedge, \neg$, and existential and universal quantifiers).

While the above example of quantifier elimination may indicate that quantifier elimination in the theory of the reals is a simple problem, this is misleading as one realizes if one tries to eliminate the existential quantifier from the formula

$$(\exists X)X^4 + aX^2 + bX + c = 0. \tag{2}$$

The real hypersurface in $\mathbb{R}^3$ (coordinatized by a, b, c) defined by the *discriminant* of the quartic polynomial $X^4 + aX^2 + bX + c$ is shown in Figure 2. The number of real zeros (counted with multiplicities) can be $0, 2$, or 4. The different connected components of the complement of the discriminant hypersurface in $\mathbb{R}^3$ correspond to real quartics with simple roots and having 0, 2, or 4 real roots, and these are labelled accordingly in Figure 2. A quantifier-free formula equivalent to (2) should describe the union of the closures of the connected components labelled by 2 and 4. Such a formula is considerably more complicated than the formula (1).[1]

Tarski-Seidenberg transfer principle. One important logical consequence of Tarski's theorem is that if ϕ is a sentence (i.e., a formula without free variables) whose atoms are polynomial inequalities with coefficients in a real closed field R, then ϕ is true in the structure R if and only if it is true over any real closed extension $\mathrm{R}' \supset \mathrm{R}$. This is usually referred to as the *Tarski-Seidenberg transfer principle*. As a special case we obtain that if a polynomial inequality $P < 0$ where $P \in \mathrm{R}[X_1, \ldots, X_n]$ has a solution in R'^n (i.e., the sentence $\exists X_1 \cdots \exists X_n \ P(X_1, \ldots, X_n) < 0$ is true over R′), where R′ is any real closed extension of R, then it already has a solution in R^n.

Complexity: Of algorithms and certificates. Tarski's proof of quantifier elimination in the theory of the reals is constructive and is based on (a parametrized version of a generalization of) Sturm's theorem for counting real roots of a polynomial.[2] The complexity of this procedure and the size of the quantifier-free formula that is output cannot be bounded by any fixed tower of exponents as a function of the size of the input formula (measured by the number of atomic formulas and the maximum degree of the polynomials appearing in them). However, because of its many applications in different areas of mathematics as well as in computer science, the question of understanding the true complexity of quantifier elimination has been considered a very important problem in real algebraic geometry—a topic on which Marie-Françoise has made significant contributions which we will discuss later.

There is a corresponding facet to Artin's proof as well. Artin's original proof used a delicate specialization argument (now referred to as the Artin-Lang homomorphism theorem [1], see also [3, Theorem 4.1.2]). Abraham Robinson [19, Chapter 6, Section 5] simplified Artin's proof by replacing the use of the Artin-Lang homomorphism theorem by an argument using the Tarski-Seidenberg transfer principle making Artin's proof quite simple to explain. We first sketch this simplified proof below.

If $P \in \mathrm{R}[X_1, \ldots, X_n]$ is not a sum of squares in the field $\mathrm{R}(X_1, \ldots, X_n)$, then the field $\mathrm{R}(X_1, \ldots, X_n)$ admits an ordering $\prec$ (via Zorn's lemma) extending the order in R, in which the evaluation of P at $(X_1, \ldots, X_n) \in \mathrm{R}(X_1, \ldots, X_n)^n$ is negative (with respect to the order $\prec$). The Tarski-Seidenberg transfer principle applied to the *real closure* of the ordered field $(\mathrm{R}(X_1, \ldots, X_n), \prec)$ (i.e., the smallest real closed field containing $(\mathrm{R}(X_1, \ldots, X_n), \prec)$ as an ordered subfield), now implies there already exists $(x_1, \ldots, x_n) \in \mathrm{R}^n$ such that $P(x_1, \ldots, x_n) < 0$.

[1] *See Example 2.6.3 in* [2] *for such a description.*

[2] *A modern account of Tarski's proof appears in* [2, Chapter 2].

It is quite clear from the highly abbreviated sketch of (the simplified version of) Artin's proof given above that it is nonconstructive. Given a nonnegative polynomial P the proof gives no indication of how to write it as a sum of squares of rational functions. Indeed Artin mentions this in his paper [1, page 110].

> Dagegen sind unsere Beweise indirekt und liefern keine explizite Vorschrift für die Zerfallung. Man darf aber wohl erwarten, daß sich die Beweise nach dieser Richtung hin vervollständigen lassen...[3]

One should mention here that Hilbert also asked whether the coefficients appearing in the rational functions could be chosen to belong to the field generated by the coefficients of the given polynomial [12] and Artin's proof being nonconstructive does not answer this question. However, using model theoretic arguments Robinson [20, Theorem 5.1] proved this stronger version. Moreover, Robinson also proved [20, Theorem 8.2] the existence of a uniform bound on the degrees of the rational functions in Hilbert's 17th problem as a function of the degree and the number of variables in the given nonnegative polynomial. But this proof uses the compactness theorem from first-order logic, and thus is nonconstructive. In particular, it does not produce any explicit bound.

To find a constructive proof of Artin's theorem is thus a very natural question by itself. Kreisel provided such a proof (see [8]), with primitive recursive degree bounds. Finding better bounds for Hilbert's 17th problem has taken on added significance in recent times in view of developments in computer science (around sums-of-squares proof systems [11]) and mathematical optimization (semidefinite programming and what is now known as the *Lasserre hierarchy* [13]). These applications make it important to obtain explicit degree bounds on the polynomials appearing in the sum of squares decomposition. We will discuss Marie-Françoise's contribution to this topic later in the article.

Real étale topos and the real spectrum. The theorems of Artin and Tarski belong to the first half of the twentieth century. The subject of algebraic geometry underwent a revolutionary transformation in the second half of the twentieth century with the ideas introduced by Grothendieck (namely, that of schemes and Grothendieck topologies on them). It is in this milieu in Paris that Marie-Françoise started her research career. To describe her work one needs to describe some background.

Sites, sheaves and topos. The fundamental notion of *Grothendieck topology* or *sites* was introduced into algebraic geometry by Grothendieck in the sixties. A site on a category $\mathbf{C}$ is a generalization of the notion of topology on the category sets—where the role of open covers is replaced by collections of morphisms (sieves) satisfying certain axioms. Every topological space gives rise to a site but not vice versa. Moreover, the classical definition of sheaves on topological spaces can be extended to sites.

Another notion introduced by Grothendieck that plays an extremely important role is the notion of *schemes*. Given a finitely generated k-algebra A (for some field k), we denote by $\operatorname{Spec} A$ the set of prime ideals of A. The set $\operatorname{Spec} A$ is topologized by choosing as a basis of open sets the subsets of the form

$$D_a = \{\mathfrak{p} \in \operatorname{Spec} A \mid a \notin \mathfrak{p}\}, a \in A. \tag{3}$$

The corresponding site is referred to as the *Zariski site* and schemes of the form $\operatorname{Spec} A$ are called affine schemes. General schemes are built out of affine schemes by an algebraically defined glueing process.

A *topos* is a category satisfying certain axioms. A prototypical example is the category of sets, but the examples which are more relevant to algebraic geometry are the category of sheaves (of sets) on a topological space or the category of sets with a group action and more generally the category of sheaves on a site.

Topos and logic. Toposes carry an internal logic (which is *intuitionistic*) which makes it possible to interpret logical formulas in an arbitrary topos. This makes it possible to define models of so called *geometric axioms* (involving only conjunctions, disjunctions and existential quantifiers, without negations and universal quantifiers) in arbitrary toposes. A typical example of such axioms is the definition of a ring (commutative and with a unit element) or of a local ring which is a ring where for every element a, either a or $1+a$ is invertible. Thus, one obtains the notion of a ring object in a topos. A classical ring is a ring object in the topos of sets, while the ring object in the topos of sheaves on a topological space is just a sheaf of rings.

Definition of spectrum. Considering objects in arbitrary topos satisfying geometric axioms proves to be very useful in solving certain universal problems which do not admit solutions if restricted to the topos of sets only. Consider for any ring A the problem of finding a homomorphism f from A to a local ring $L(A)$ such that for all such homomorphisms $g : A \to B$, there is a unique local homomorphism $h : L(A) \to B$ such that $g = h \circ f$ (a homomorphism between local rings is local if it reflects invertibility). The solution to this problem unfortunately does not always exist since a ring can have several prime ideals. But now suppose we are allowed to change the topos while looking for the universal homomorphism to a local ring (object) now in a possibly larger topos. So now the universal problem becomes given a pair (A, E) where A is a ring object in a topos E find a pair $(\tilde{A}, \tilde{E})$ and a *geometric morphism*

[3] *This roughly translates "In contrast our proofs are indirect and provide no explicit instructions for the decomposition. One may however expect that the proof can be completed in this direction."*

$f : E \to \tilde{E}$ such that $\tilde{A} = f(A)$, and $\tilde{A}$ is a local ring object in $\tilde{E}$, and the morphism f has the obvious universal property. The pair $(\tilde{A}, \tilde{E})$ is then called the *spectrum* of the pair (A, E).

Zariski and étale spectra. In the case where $E = \mathbf{Sets}$, so that A is a classical ring, the spectrum of A happens to be the topos of sheaves on the Zariski topological space $\operatorname{Spec} A$ (i.e., $\tilde{E} = \operatorname{Sh}(\operatorname{Spec} A)$)), and the local ring object in $\tilde{E}$ is the structure sheaf $\tilde{A}$ defined on $\operatorname{Spec} A$—namely, which associates to each open set D_f the ring A_f (A localized at f). In this way one recovers the notion of the Zariski spectrum of a ring.

Another example of a spectrum is obtained by considering the axioms of local rings with a separably closed residue field. One obtains this way the topos of sheaves on étale sites on schemes as the étale spectrum of a local ring object. Étale sheaves and their cohomology play a central role in algebraic geometry. They were introduced by Grothendieck as a means to prove the Weil conjectures in number theory. One important point to note is that the étale site on a scheme is in general finer than the Zariski site (i.e., the site induced by the Zariski topology) and that the topos of sheaves on étale sites is not spatial (i.e., not equivalent to the topos of sheaves on some topological space). Indeed the étale spectrum of a field k of characteristic zero is the algebraic closure $\overline{k}$ of k equipped with the action of the Galois group $\operatorname{Gal}(\overline{k}/k)$.

Real spectrum. It is now very natural (from the point of view of real algebraic geometry) to consider the spectrum associated with the axioms of local rings with a real closed residue field (as opposed to being separably closed). The corresponding spectrum (now called the *real spectrum*) was investigated by Marie-Françoise and Michel Coste (in "Topologies for real algebraic geometry," appearing in the book *Topos theoretic methods in geometry*, Various Publications Series, Vol 30, 37-100, 1979).

Unlike the étale spectrum, the real spectrum turns out to be spatial (see Theorem 2 below)—and the underlying topological space is often referred to as the real spectrum. The role of the structure sheaf is now played by a sheaf of functions on this topological space, namely the sheaf of *Nash functions*. Since this marks the starting point of Marie-Françoise's work in real algebraic geometry, we start our description of her work by describing her work on the real spectrum.

2.2. The topos of real étale sheaves.

Let R be a real closed field and $V(\mathrm{R})$ denote the R-points of a variety V defined by a finite set of polynomial equations $P_1 = \cdots = P_m = 0$, where $P_i \in \mathrm{R}[X_1, \ldots, X_n]$.

Definition (Real étale site). [6] The real étale site on V is the site generated by collections of étale morphisms $(W_i \to W \subset V)_{i \in I}$ such that $(W_i(\mathrm{R}) \to W(\mathrm{R}))_{i \in I}$ is a surjective family.

There is another site defined on V (called the semi-algebraic topology [6]) whose coverings are generated by covers of $V(\mathrm{R})$ by open semi-algebraic subsets of $V(\mathrm{R})$ (i.e., finite unions of subsets of $V(\mathrm{R})$ defined by finite conjunctions of strict inequalities). Note that despite its name it is not really a classical topology—but only a Grothendieck topology.

With Michel Coste, Marie-Françoise proved the following two fundamental results clarifying the main properties of real étale sheaves thereby answering questions raised previously in the works of Brumfiel, Knebusch, and Delfs.

Theorem 1 ([6]). *The topos of sheaves with respect to the real étale site on V is isomorphic to the topos of sheaves with respect to the semi-algebraic topology site.*

Theorem 2. *The topos of sheaves with respect to the real étale site on V (and so using Theorem 1 also the topos of sheaves with respect to the semi-algebraic topology on V) is spatial (i.e., isomorphic to the topos of sheaves on a topological space).*

(Note that the underlying topological space of the spatial topos in Theorem 2 is the real spectrum of the ring $\mathrm{R}[V]$ described below.)

The algebraic definition of the real spectrum is as follows. Let A be a ring (commutative with a unit element). A subset $\alpha \subset A$ is called a *prime cone* if it satisfies the properties:

(i) $\alpha + \alpha \subset \alpha$,
(ii) $\alpha \cdot \alpha \subset \alpha$,
(iii) $A^2 \subset \alpha$,
(iv) $-1 \notin \alpha$, and
(v) $a \cdot b \in \alpha \Longrightarrow a \in \alpha$ or $-b \in \alpha$.

Definition (Real spectrum). The real spectrum, $\operatorname{Sper} A$, of A is the set of prime cones of A. The set $\operatorname{Sper} A$ is topologized by choosing as a basis of open sets the subsets

$$D_a = \{\mathfrak{p} \in \operatorname{Sper} A \mid a \notin \mathfrak{p}\}, a \in A \tag{4}$$

(compare with equation (3)).

Example. The real spectrum of a ring can be identified with its set of preorderings. The real spectrum of a field is the set of its total orderings. The real spectrum of the ring $A = \mathrm{R}[X]$ can be described as follows

$$\operatorname{Sper} A = \{\pm\infty\} \cup \{\alpha, \alpha_-, \alpha_+ \mid \alpha \in \mathrm{R}\},$$

where α (resp. α_-, α_+) is the cone of elements of A which are nonnegative at α (resp. immediately to the left of α, immediately to the right of α), and $-\infty$ (resp. $+\infty$) is the set of elements of A which are positive at negative (resp. positive) infinity.

The real spectrum $\operatorname{Sper} A$ shares some of the well-known properties of $\operatorname{Spec} A$ (for example, it is quasi-compact).

There is a canonical injection of $V(\mathrm{R})$ into $\operatorname{Sper} A$, and a bijection between open semi-algebraic subsets of $V(\mathrm{R})$

and the compact open subsets of Sper A. This last bijection gives a translation between geometric properties of V and algebraic properties of A. For example, the local (semi-algebraic) dimension of $V(\mathrm{R})$ at a point $x \in V(\mathrm{R})$ is equal to the maximal length of a chain of prime cones terminating at x. We refer the reader to the book [3, Chapter 7] for a detailed study of the real spectrum and its various applications.

The fact that the topos of sheaves on the real étale site of a real variety is spatial and isomorphic to the topos of sheaves on the real spectrum makes the study of these sheaves easier especially from the point of view of proving various kinds of comparison theorems between different cohomology theories on real varieties. This is exploited by Scheiderer in [21] who amongst other things gave an alternative proof of Theorem 2 (avoiding the use of categorical logic).

Like most other important notions in mathematics the notion of real spectrum arose independently from several directions such as in the work of Lou van den Dries in model theory. It is also interesting to note that one consequence of Theorems 1 and 2 is that abstract topos theory from which the idea of real spectrum originated perhaps becomes less relevant in real algebraic geometry—since the real spectrum and its constructible subsets can be studied using geometric tools without referring to Grothendieck topologies etc. Nevertheless, as we shall see next, topos theory (and intuitionistic logic that goes with it) seems to have influenced many of Marie-Françoise's works on topics that are a priori far from logic and topos theory.

2.3. Algorithms in real algebraic geometry.

A significant part of Marie-Françoise's work has been in the area of algorithms in real algebraic geometry. This switch from abstract topos theory to more algorithmic aspects of real algebraic geometry was probably inspired by new developments in the then-new and extremely active field of computer algebra in the late eighties. This is exemplified by the biannual conference MEGA (Effective Methods in Algebraic Geometry) which started in 1990, with Marie-Françoise in its initial committee and has continued from then.

The algorithmic problems addressed in Marie-Françoise's work include some of the fundamental algorithmic problems in real algebraic geometry.[4] The gamut of her work in this area extends from the decision problem and more generally quantifier elimination in the theory of the reals mentioned before, to problems with more topological flavor (deciding connectivity of semi-algebraic sets, computing higher Betti numbers and Euler-Poincaré characteristics, dimension etc.) These algorithmic problems arise in many applications—in discrete and computational geometry, mathematical optimization, theoretical computer science amongst others. Designing better algorithms for such problems is clearly of wide interest. A second (perhaps less well-known) aspect is that the mathematical results underlying the design of these algorithms and often their complexity analysis yield quantitative results in real algebraic geometry. Indeed, the fact that these two aspects are very intertwined is very explicit in Marie-Françoise's work. I mention some examples later.

Symbolic algorithms and their complexity. We first note that by the word "algorithm" in this section we mean algorithms which are exact, symbolic algorithms. This means that the algorithms take as input polynomials with coefficients in some ordered domain $\mathrm{D} \subset \mathrm{R}$, use only rational arithmetic and sign determinations on elements of D, and terminate after a finite number of steps with the correct output. By "complexity" of such an algorithm we mean the number of arithmetic operations and sign determinations. If $\mathrm{D} = \mathbb{Z}$, then the number of bit-operations is called the bit-complexity.

Algorithms come with upper bounds on their complexity. These upper bounds are in terms of the size of the input—and this is measured by the number of polynomials (denoted by s), an upper bound on the degrees of the input polynomials (denoted by d) and the number of variables k (and the bit-lengths of the coefficients of the input polynomials in case $\mathrm{D} = \mathbb{Z}$).

Doubly vs. singly exponential. Several important problems in algorithmic real algebraic geometry can be solved using a technique called *cylindrical algebraic decomposition*. Given any semi-algebraic subset $S \subset \mathrm{R}^k$, a cylindrical algebraic decomposition of R^k adapted to S, is a partition of R^k into "cylindrical cells" (each semi-algebraically homeomorphic to $(0,1)^\ell, 0 \leq \ell \leq k$), such that for each cell C of the decomposition $C \cap S = C$ or empty. If S is closed and bounded such a cylindrical decomposition can be refined to a semi-algebraic triangulation of S. This technique was already familiar to geometers, in particular Lojasiewicz [14]. This was made algorithmic by Collins [5] using *subresultants* of pairs of polynomials and became a widely known algorithm. However, cylindrical algebraic decomposition is a big hammer. Having a cylindrical decomposition at hand allows one to solve all the algorithmic problems listed previously. However, since computation of a cylindrical decomposition involves iterated projection in which the degrees and the number of polynomials (roughly) square in each step—the size of a cylindrical decomposition (as well as complexity of computing it) is necessarily *doubly exponential* (of the form $(sd)^{2^{O(k)}}$).

Critical point method. A major focus of research in algorithmic real algebraic geometry has been in obtaining

[4] *A unified treatment of a major part of this work appears in the book* Algorithms in Real Algebraic Geometry [2] *(coauthored with Richard Pollack and the author).*

algorithms with *singly exponential* complexity. Even though singly exponential complexity might already seem very expensive from a practical point of view it should be remembered that each of the problems mentioned previously is conjecturally very hard from the computational complexity theory point of view (**NP**-hard or even **PSPACE**-hard), and that often the output itself has a singly exponential size in the worst case.

The key is to use more sophisticated ideas inspired by Morse theory (often called the critical point method), eliminating variables by blocks instead of eliminating variables one at a time. Even though the critical point method has been used by several researchers (in particular Grigoriev and Vorobjov), it is fair to say that Marie-Françoise is a pioneer in its application in a wide variety of settings achieving nearly optimal bounds in many cases.

Thom encoding. The key to the critical point method is to compute the set of critical points of a function restricted to certain real algebraic subsets of R^k. Using an initial deformation depending on one or more infinitesimals one ensures that the set of critical points is finite. But there still remains the problem of representing the coordinates of these points (which are algebraic over the ring generated by the coefficients of the input polynomials). A very elegant and also very general way of doing so is by using *Thom's lemma*—which was introduced to the area of symbolic computation by Marie-Françoise in joint work with Michel Coste ("Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets," *Journal of Symbolic Computation*, Vol 5, 121–129, 1988).

One consequence of Thom's lemma is that each real root $\alpha \in \mathrm{R}$ of a polynomial $f \in \mathrm{R}[T]$ is characterized by the signs of the various derivatives of f at α. (So the root $\sqrt{2}$ of the polynomial X^2-2 is distinguished from the root $-\sqrt{2}$ by the signs of the derivative $2X$ at these two roots.) The tuple

$$\left(\mathbf{sign}(f^{(i)}(\alpha))\right)_{1\leq i\leq \deg(f)} \in \{0,1,-1\}^{\deg(f)}$$

is now known as the *Thom encoding* of the root α of f. Moreover the sign determination algorithm, computing the realizable sign conditions on a finite set of polynomials at the roots of f (see for example [2]), can be used to determine the Thom encoding of the roots of f.

A point in R^k can be described by a k-tuple of rational functions

$$u = \left(\frac{g_1(T)}{g_0(T)}, \ldots, \frac{g_k(T)}{g_0(T)}\right)$$

evaluated at a real root α of another polynomial f specified by its Thom encoding σ. The tuple $(f, g_0, \ldots, g_k) \in \mathrm{R}[T]^{k+2}$ and the Thom encoding σ, specifies the point

$$\left(\frac{g_1(\alpha)}{g_0(\alpha)}, \ldots, \frac{g_k(\alpha)}{g_0(\alpha)}\right).$$

This method of representing real points, which works over arbitrary real closed fields (even non-Archimedean ones), is called *real univariate representation* in [2], and was introduced and used by Marie-Françoise in a series of papers. Parametrized versions of the same representations also play an important role in algorithmic real algebraic geometry in order to represent semi-algebraic curves (for example, in algorithms for computing *roadmaps* of semi-algebraic sets discussed below).

Sample points algorithm. The first application of the critical points method is in designing an algorithm that given a finite set $\mathcal{P}$ of polynomials in $\mathrm{R}[X_1, \ldots, X_k]$ as input, computes a finite set of "sample points" guaranteed to intersect every semi-algebraically connected component of the realizations of every realizable sign condition on $\mathcal{P}$. The coordinates of the points are represented by rational functions evaluated at a real root of a univariate polynomial—the real root specified by a Thom encoding. The main idea is computing these points as critical points of a function restricted to certain algebraic sets obtained by making infinitesimal perturbations of the polynomials in $\mathcal{P}$, and so technically they belong to some real closed extension of R (field of algebraic Puiseux series with coefficients in R). This algorithm which appears in the paper "On computing a set of points meeting every cell defined by a family of polynomials on a variety," *Journal of Complexity*, Vol 13, No. 1, 28–37, 1997 (coauthored with Richard Pollack and the author), and whose complexity is bounded by $s^{k+1}d^{O(k)}$, is a crucial ingredient in many subsequent papers. Moreover, the degrees of the (univariate) polynomials appearing in the output are bounded by $O(d)^k$ (independent of s).

Quantitative curve selection lemma. A refinement of the degree bound from the last paragraph has recently been exploited by Marie-Françoise and the author to prove quantitative upper bounds for the *curve selection lemma* in semi-algebraic geometry ("Quantitative curve selection lemma," *Mathematische Zeitschrift*, Vol 300, No. 3, 2349–2361, 2022). The curve selection lemma is a key result in semi-algebraic geometry which states the following: for every semi-algebraic set S and $x \in \overline{S}$ (the closure of S in the Euclidean topology) there exists a semi-algebraic curve $\varphi : [0,1) \to \overline{S}$, such that $\varphi(0) = x, \varphi((0,1)) \subset S$. A quantitative version of this lemma asks for a bound on the degree of the Zariski closure of the image of φ in terms of the parameters of the formula defining S.

In what follows it is useful to begin with the following definition.

Definition. Let $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$. We will call a quantifier-free first-order formula (in the theory of the reals) with atoms $P = 0, P > 0, P < 0, P \in \mathcal{P}$ to be a *$\mathcal{P}$-formula* and the set defined by it a $\mathcal{P}$-semi-algebraic set.

We denote by $\mathrm{R}[X_1,\ldots,X_k]_{\leq d}$ the subset of polynomials in $\mathrm{R}[X_1,\ldots,X_k]$ with degrees $\leq d$. The following result was proved by Marie-Françoise and the author.

Theorem 3 (Quantitative curve selection). *Let $\mathcal{P} \subset \mathrm{R}[X_1,\ldots,X_k]_{\leq d}$ be a finite set, S a $\mathcal{P}$-semi-algebraic set, and $x \in \overline{S}$. Then, there exist $t_0 \in \mathrm{R}, t_0 > 0$, a semi-algebraic path $\varphi : [0,t_0) \to \mathrm{R}^k$ with*

$$\varphi(0) = x,\ \varphi((0,t_0)) \subset S,$$

such that the degree of the Zariski closure of the image of φ is bounded by

$$(O(d))^{4k+3}.$$

Notice that the bound on the degree of the image of the curve φ in the above theorem has no combinatorial part, i.e., there is no dependence on the cardinality of $\mathcal{P}$.

The key ingredient in the proof of Theorem 3 is an accurate analysis of the degrees of the polynomials output in the sample points algorithm mentioned before, along with the identification of the field of algebraic Puiseux series with coefficients in R, with germs of semi-algebraic functions $(0,1) \to \mathrm{R}$. This is a good illustration how accurate complexity analysis of symbolic algorithms can lead to quantitative mathematical results.

Quantifier elimination algorithm. The critical point method can be used to eliminate whole blocks of quantifiers at the same time, leading to improvement in complexity. The following theorem, proved by Marie-Françoise with Richard Pollack and the author has been applied in many contexts ("On the combinatorial and algebraic complexity of quantifier elimination," *Journal of the ACM*, vol 43, No. 6, 1002–1045, 1996).

Theorem 4. *Let $\mathcal{P} \subset \mathrm{R}[X_{[1]},\ldots,X_{[\omega]},Y]_{\leq d}$ be a finite set of s polynomials, where $X_{[i]}$ is a block of k_i variables, and Y is a block of ℓ variables. Let*

$$\Phi(Y) = (Q_1 X_{[1]}) \cdots (Q_\omega X_{[\omega]}) \Psi(X_{[1]},\ldots,X_{[\omega]},Y)$$

be a quantified-formula, with $Q_i \in \{\exists,\forall\}$ and Ψ a quantifier-free formulas with atoms $P = 0, P > 0, P < 0, P \in \mathcal{P}$.

Then there exists a quantifier-free formula

$$\Psi(Y) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} \Big(\bigvee_{n=1}^{N_{ij}} \mathbf{sign}(P_{ijn}(Y)) = \sigma_{ijn}\Big),$$

where $P_{ijn}(Y)$ are polynomials in the variables Y, $\sigma_{ijn} \in \{0,1,-1\}$,

$$\begin{aligned} I &\leq s^{(k_\omega+1)\cdots(k_1+1)(\ell+1)} d^{O(k_\omega)\cdots O(k_1)O(\ell)}, \\ J_i &\leq s^{(k_\omega+1)\cdots(k_1+1)} d^{O(k_\omega)\cdots O(k_1)}, \\ N_{ij} &\leq d^{O(k_\omega)\cdots O(k_1)}, \end{aligned}$$

equivalent to Φ, and the degrees of the polynomials P_{ijk} are bounded by $d^{O(k_\omega)\cdots O(k_1)}$.

The proof of Theorem 4 is effective, in that an algorithm is described to obtain the quantifier-free formula Ψ given the formula Φ as input, whose proof of correctness and complexity analysis yield Theorem 4. The bounds on the size of the quantifier-free formula Ψ in Theorem 4 and on the degrees of the polynomials appearing in Ψ, are doubly exponential in ω which is the number of alternations in the blocks of quantifier (this is unavoidable) but is singly exponential if ω is fixed. The improvement comes from the critical point method. Several quantifier elimination algorithms with doubly exponential complexity in the number of blocks exist [10, 18], but Theorem 4 is more precise by treating differently the number of polynomials and their degrees.

Combinatorial vs. algebraic complexity. Notice the different roles played by the "combinatorial" parameter $s = \mathrm{card}(\mathcal{P})$ and the "algebraic" parameter d (a bound on the degrees of the polynomials in $\mathcal{P}$). This separation of the "combinatorial part" from the "algebraic part" in the complexity upper bounds in algorithms as well as in other quantitative bounds in real algebraic geometry is an important distinguishing feature in many of Marie-Françoise's papers on quantitative and algorithmic aspects of real algebraic geometry. For example, the fact that the degrees of the polynomials in the quantifier-free formula Ψ in Theorem 4 can be bounded only in terms of the algebraic parameter d (independent of s) has many applications (for example, it plays a key role in several results in discrete and computational geometry).

Algorithmic vs. proof complexity. The critical point method produces a "better" algorithm than that using cylindrical algebraic decomposition in the sense of algorithmic complexity—singly exponential as opposed to doubly exponential. However, the proof of the correctness of this algorithm is much more complicated since it depends on connectivity results. Thus, if one is interested in converting an instance of a run of this algorithm into a formal mathematical proof (starting from the axioms of real closed fields) of the equivalence of the output and the input formula—then an algorithm using the critical point method is less suitable. In recent work (joint with Daniel Perrucci) Marie-Françoise has given an algorithm with elementary recursive (fixed tower of exponents) complexity algorithm for quantifier-elimination ("Elementary recursive quantifier elimination based on Thom encoding and sign determination," *Annals of Pure and Applied Logic*, Vol 168, No. 8, 1588–1604, 2017). Though from the point of view of algorithmic complexity this might seem much worse than the algorithm in Theorem 4, or even than the cylindrical algebraic decomposition algorithm, it is better from the point of view of *proof theory*, since its proof of correctness is purely algebraic (and does not require

arguments involving connectivity which can be quite complicated from the point of view of formal logic).

An algebraic proof of the fundamental theorem of algebra. This is a natural place to mention the paper "Quantitative fundamental theorem of algebra," *The Quarterly Journal of Mathematics*, Vol 70, No. 3, 1099–1037, 2019, (with the same coauthor) which gives a new algebraic proof of one of the oldest theorems of algebra—namely, the fundamental theorem of algebra which states that the field $\mathrm{R}[i]$ is algebraically closed (assuming that R is real closed). The proof is based on a previous proof the same theorem by Michael Eisermann [9] which uses an algebraic definition of the winding number. The important new property of the proof in the paper under discussion is that in order to prove that every polynomial in $\mathrm{R}[i][T]$ of degree d has a root in $\mathrm{R}[i]$, the intermediate value property for polynomials in $\mathrm{R}[T]$ is needed only for polynomials of degree at most d^2, using subresultant polynomials which makes remainder sequences more efficient (subresultants are ubiquitous in Marie-Françoise's work). The classical proof due to Laplace that one meets in many textbooks of abstract algebra requires the use of the intermediate value property for real polynomials of exponential degree.

Roadmaps and connectivity. There is another class of algorithmic problems in real algebraic geometry that goes beyond the logical realm—namely, computing topological invariants of semi-algebraic sets. While initially motivated by problems of motion planning in robotics in the pioneering works of Jack Schwartz and Micha Sharir as well as John Canny, it has developed into a very active area of research in which Marie-Françoise has left an indelible mark. One of the first problems to be investigated in this area was the problem of counting the number of (semi-algebraically) connected components of a given semi-algebraic set. An important construction—namely, a semi-algebraic subset of a given semi-algebraic set of dimension at most one (also called a roadmap) was introduced by Canny in [4] to solve this problem within a singly exponential complexity bound. Once a roadmap of a semi-algebraic set has been computed, the problem of counting the number of connected components simplifies to a combinatorial problem of counting the number of connected components of a graph for which efficient algorithms are known. The history of the development of algorithms for computing roadmaps is quite long with several key contributions along the way (including contributions due to Marie-Françoise as well as Canny, Gournay, Grigoriev, Heintz, Pollack, Risler, Solerno, and Vorobjov amongst others.

We mention here two fundamental contributions due to Marie-Françoise. In the paper "Computing roadmaps of semi-algebraic sets on a variety," *Journal of the American Mathematical Society*, Vol 13, No. 1, 55–82, 2000, Marie-Françoise (with Richard Pollack and the author) gave a deterministic algorithm for computing the roadmap of a semi-algebraic set contained in a variety of dimension k' whose complexity is bounded by $s^{k'+1}d^{O(k^2)}$.

The underlying geometric idea behind algorithms for computing roadmaps has stayed the same over the years. This is roughly as follows. Suppose the goal is to compute the roadmap of a closed and bounded algebraic hypersurface $V \subset \mathrm{R}^k$. One first computes descriptions of two semi-algebraic subsets $V^0, V^1 \subset V$, where $V^1 = \pi^{-1}(M) \cap V$, where $\pi : \mathrm{R}^k \to \mathrm{R}^\ell$ is a linear projection map and $M \subset \mathrm{R}^\ell$ is a certain well-chosen finite subset, and V^0 is a certain polar subvariety of V of dimension ℓ. Then, $\dim(V^0) = \ell$, and $\dim V^1 = k - \ell - 1$. One then proves that $V^0 \cup V^1$ has a good connectivity property with respect to V—namely, that the intersection of $V^0 \cup V^1$ with each semi-algebraically connected component of V is non-empty and semi-algebraically connected. The algorithm then makes recursive calls on V^0 and V^1 taking advantage of the fact that the dimensions of V^0, V^1 are strictly smaller than $\dim V$.

The algorithm mentioned above (and in fact in all prior algorithms for computing roadmaps) used $\ell = 1$ in the definition of V^0 and V^1, and in this case the quadratic dependence on k in the exponent of the complexity is unavoidable (there are too many recursive calls). For a decade afterwards, this remained the algorithm with the best complexity bound for the problem and it was thought that the quadratic dependence on k was unavoidable. In a series of two papers ("A baby step–giant step roadmap algorithm for general algebraic sets," *Foundations of Computational Mathematics*, Vol 14, No. 6, 1117–1172, 2014, with Mohab Safey-el-Din, Éric Schost, and the author, and "Divide and conquer roadmap for algebraic sets," *Discrete & Computational Geometry*, Vol 52, No. 2, 278–343, 2014, with the author), Marie-Françoise improved the exponent (in the case of algebraic sets) to $O(k^{3/2})$ and then to $\tilde{O}(k)$ (suppressing poly-log factors). The latter is the best exponent currently known for the complexity of computing roadmaps at the moment. The mathematical results that make the advances in the above mentioned papers possible are new connectivity results similar to a result proved in an earlier paper by Safey-el-Din and Schost. The distinguishing feature of the new connectivity results as opposed to that in the prior work of Safey-el-Din and Schost is that no assumptions (such as genericity) are needed on V.

In another direction, it is natural to ask about the complexity of computing the higher Betti numbers of semi-algebraic sets (the number of connected components being the zeroth Betti number). Another contribution of Marie-Françoise (with Richard Pollack and the author) is the first singly exponential complexity algorithm for computing the first Betti number ("Computing the first Betti

number of a semi-algebraic set," *Foundations of Computational Mathematics*, Vol 8, No. 1, 97–136, 2008). The key new ingredient is an algorithm with a singly exponential complexity for computing covers of semi-algebraic sets by closed contractible semi-algebraic subsets. This construction which is also based on the roadmap algorithm is a fundamental ingredient for more recent works on computing higher Betti numbers of semi-algebraic sets.

2.4. **Quantitative real algebraic geometry.** Real algebraic geometry has important connections with the field of discrete geometry which has blossomed in recent years—partly because of the injection of algebraic methods into incidence combinatorics due to Larry Guth and Nets Katz. Marie-Françoise was an early pioneer. It is in this work that she started her long collaboration with Richard Pollack which led to many of the works mentioned above (I was fortunate to be a part of some of them). A basic ingredient from real algebraic geometry is in proving upper bounds on the number of combinatorially distinct geometric configurations of various kinds—for example, the maximum number of *order types* that can be realized by n distinct points in $\mathbb{R}^k$ (the order type of a set S of n points in $\mathbb{R}^k$ is an element of $\{0,1,-1\}^{\binom{S}{k+1}}$, recording the orientation of each $(k+1)$-tuple of points of S). Questions of this type often reduce to bounding the number of realized sign conditions of certain finite sets of real polynomials restricted to some real variety. Such an upper bound follows from a bound on the number of connected components (the zeroth Betti number) of the realizations of every realizable sign condition of the set of polynomials.

The problem of proving upper bounds on the Betti numbers of real varieties has a long history. An upper bound on the sum of the Betti numbers of a real variety $V \subset \mathrm{R}^k$ defined by polynomials of degrees bounded by d was proved by Petrovskiĭ and Oleĭnik and later rediscovered by Milnor and Thom. They proved:

Theorem.

$$\sum_i b_i(V) \leq d(2d-1)^{k-1}.$$

An asymptotically tight upper bound on the number of connected components (the zeroth Betti number) of the realizations of all realizable sign conditions for finite sets of polynomials in $\mathrm{R}[X_1,\ldots,X_k]_{\leq d}$ was proved by Marie-Françoise in a joint paper with Richard Pollack in ("On the number of cells defined by a set of polynomials," *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, Vol 316, No. 6, 573–577, 1993) and extended to sign conditions restricted to varieties in ("On the number of cells defined by a family of polynomials on a variety," *Mathematika*, Vol 43, No. 1, 1201–26, 1996, with Richard Pollack and the author). It is in these papers that the formal techniques of introducing infinitesimals, extending the given real closed fields to the field of algebraic Puiseux series in certain infinitesimals, and considering neighborhoods of various algebraic sets using different infinitesimals, were introduced, and these have proved to be the standard techniques in quantitative study of real algebraic geometry. A culmination of this line of work is the following theorem due to Marie-Françoise (with Richard Pollack and the author) which gives a bound on the sum of the Betti numbers (in any fixed dimension not just 0) of the realizations of all realizable sign conditions of a finite set of polynomials of bounded degree restricted to a variety ("On the Betti numbers of sign conditions," *Proceedings of the American Mathematical Society*, Vol 133, No. 4, 965–974, 2005). An extra topological ingredient needed in this semi-algebraic situation (compared to the Petrovskiĭ-Oleĭnik upper bound) is certain inequalities coming from the Mayer-Vietoris exact sequence.

Theorem 5. *The sum of the i-th Betti numbers of the realizations of all realizable sign conditions of a set of s polynomials in* $\mathrm{R}[X_1,\ldots,X_k]_{\leq d}$ *restricted to a variety* $V \subset \mathrm{R}^k$ *of dimension* $\leq k'$ *defined by polynomials of degree at* d *is bounded by:*

$$\sum_{1\leq j\leq k'-i} \binom{s}{j} 4^j d(2d-1)^{k-1}.$$

This theorem recovers prior bounds on the number of connected components of sign conditions by substituting i by 0.

It is to be noted that the techniques introduced in the paper mentioned above have had an impact beyond real algebraic geometry. They are crucial ingredients in quantitative results on Betti numbers in more general structures—such as in o-minimal geometry and even in the theory of algebraically closed valued fields of arbitrary characteristics.

2.5. **Constructive Positivstellensatz.**

The language of "certificates" and analogy with Hilbert's Nullstellensatz. One suggestive way of viewing Artin's theorem is that it produces an *algebraic certificate* for the nonnegativity of a real polynomial $P \in \mathbb{R}[X_1,\ldots,X_n]$ (or equivalently the unrealizability of the formula $P < 0$). A generalization of this theorem which produces an algebraic certificate for the unrealizability of more general formulas of the form

$$\bigwedge_{i\in I}(P_i \neq 0) \wedge \bigwedge_{j\in J}(Q_j \geq 0) \wedge \bigwedge_{k\in K}(R_k = 0) \qquad (5)$$

was proved by Krivine and independently by Stengle. The following formulation is due to Stengle.

Theorem. *The formula in equation* (5) *is unrealizable in* R^n *if and only if there exists P belonging to the monoid generated by the polynomials* P_i^2*, Q belonging to the nonnegative cone generated by the polynomials* Q_j*, and R belonging to the ideal*

generated by the polynomials R_k, such that

$$P + Q + R = 0. \tag{6}$$

The equality (6) is called an *algebraic certificate* of the unrealizability of the formula in (5).

This is known as the *Positivstellensatz* in analogy with the case of algebraically closed fields where, as is well known, Hilbert's Nullstellensatz produces such an algebraic certificate for the unrealizability of polynomial equations—namely, the emptiness of an algebraic set defined by polynomial equations $P_1 = \cdots = P_s = 0$ in C^n where C is an algebraically closed field, can always be certified by polynomials $Q_1, \ldots, Q_s$ satisfying

$$1 = P_1Q_1 + \cdots P_sQ_s. \tag{7}$$

Moreover, due to the work of Brownawell, Kollár, and Jelonek, very tight (singly exponential) upper bounds are known on the maximum degrees of the polynomials necessary in such a certificate in terms of the maximum degrees of the polynomials P_i. The following theorem proved by Marie-Françoise, in joint work with Henri Lombardi and Daniel Perrucci [16] provides the first elementary recursive upper bound on the algebraic certificate in Hilbert's seventeenth problem.

Theorem 6. *Let $P \subset \mathrm{R}[X_1, \ldots, X_k]_{\leq d}$ be a nonnegative polynomial. Then P can be written as a sum of squares of rational functions, and the degrees of the numerators and denominators of these rational functions are bounded by*

$$2^{2^{2^{d^{4^k}}}}.$$

A similar bound (tower of five exponents) is also proved for the algebraic certificate for the Positivstellensatz in the same paper [16, Theorem 1.3.2].

We explain below some of the ideas that go into the proof of Theorem 6.

Constructive proofs of Postivstellensatz. In joint work with Henri Lombardi and Michel Coste [7], Marie-Francoise introduced a very general method for producing constructive proofs of theorems that guarantee the existence of algebraic certificates (for example, Nullstellensatz for algebraically closed fields, Positivstellensatz for real closed fields, and even a Positivstellensatz for algebraically closed valued fields).

We restrict to the case of real closed fields in the following.

One starts with an algorithm for quantifier elimination in the theory of the reals. Such an algorithm with input the formula in (5) preceded by a block of existential quantifiers will produce the output 'FALSE' if and only if the semi-algebraic set defined by the formula in [16] is empty. The steps taken by the algorithm can be thought of as a tree with branchings depending on the signs of certain elements of R computed by the algorithm.

This tree can be converted into a formal mathematical "proof" having a special shape (referred to as a dynamical proof in [7]). (It is interesting to mention here that the dynamical theories and proofs have very close connections with Grothendieck toposes as explained in [7, Section 1.1].)

As an illustration, at a certain step of the proof one might want to infer the conclusion $P(u) > 0 \vee P(u) < 0$ from the hypothesis $P(u) \neq 0$ (where u is a tuple of indeterminates and $P \in \mathrm{R}[u]$). More generally, such an inference will be usually needed in a "context" where the signs of some other polynomials in $v = (u, u')$ are fixed.

A key notion defined first in a paper by Lombardi [15] is *weak inference* and more generally *weak existence*.

Definition (Weak existence, weak inference). We follow the same notation introduced above. A weak existence

$$(\exists t_0)\mathcal{F}(u, t_0) \vdash (\exists t_1)\mathcal{F}_1(u, t_1) \vee \cdots \vee (\exists t_m)\mathcal{F}_m(u, t_m)$$

is a construction which produces, given sign condition $\mathcal{H}(u, u') = (\mathcal{H}_{\neq 0}, \mathcal{H}_{\geq 0}, \mathcal{H}_{=0})$ and algebraic certificates for the unrealizability of $\mathcal{F}_i \wedge \mathcal{H}$, $i = 1, \ldots, m$ (these are called *initial incompatibilities* in [16]), an algebraic certificate for the unrealizability of $\mathcal{F} \wedge \mathcal{H}$ (called the *final incompatibility*).

A weak inference is defined similarly but without the existential quantifiers.

Since the final incompatibility is given by an explicit construction taking as input the initial incompatibilities, the degrees of the polynomials in the final incompatibility can be bounded explicitly in terms of the degrees of the initial incompatibilities.

Going back to the preceding illustrative example, the weak inference version says the following. We consider a context given by sign conditions $\mathcal{H} = (\mathcal{H}_{\neq 0}, \mathcal{H}_{\geq 0}, \mathcal{H}_{\geq 0})$ and start from the two initial incompatibilities,

$$P_1 + Q_1 + R_1 = 0,$$

$$P_2 + Q_2 + R_2 = 0,$$

where P_1, P_2 belong to the monoid generated by the polynomials $H_{\neq 0} \cup \{P^2\}$, Q_1 is in the cone generated by $H_{\neq 0} \cup \{P\}$ (resp. Q_2 is in the cone generated by $H_{\geq 0} \cup \{-P\}$ and R_1, R_2 are in the ideal generated by $H_{=0}$.

The final incompatibility is constructed as follows: multiply both sides of

$$P_1 = -Q_1 - R_1,$$

$$P_2 = -Q_2 - R_2,$$

to obtain

$$P_1P_2 = -Q_3 - R_3,$$

where P_1P_2 belongs to the monoid generated by the polynomials $H_{\neq 0} \cup \{P^2\}$, Q_3 is in the cone generated by $H_{\geq 0}$ and

R_3 is in the ideal generated by $H_{=0}$. Thus, we obtain the final incompatibility

$$P_1P_2 + Q_3 + R_3 = 0.$$

The construction described above is quite simple and the bounds on the degrees easy to obtain.

Here is a more complicated weak inference that is one of the many (!) key steps in the proof of Theorem 6.

Weak inference version of the intermediate value theorem.

Theorem 7. [16, Theorem 3.1.3] *Let* $P = \sum_{0\leq h\leq p} C_h \cdot y^h \in \mathrm{R}[u][y]$. *Then,*

$$\exists(t_1, t_2)[C_p \neq 0 \wedge P(t_1)P(t_2) \leq 0] \vdash \exists t P(t = 0).$$

The degree of the monoid part of the final incompatibility is bounded by a function which is doubly exponential in the degree p *of* P *in* y *(see* [16] *for a much more precise statement).*

The proof of Theorem 7 (including the estimate on the degree) is not straightforward and is based an inductive argument on the degree of P, and is an adaptation of the proof by Artin [1] that if a field is real (i.e., in which -1 is not a sum of squares), then its extension by an irreducible polynomial of odd degree is also real.

In summary, the idea behind the proof of Theorem 6 is the following. Start from a quantifier elimination algorithm applied to the given sign condition (with empty realization). Convert the steps of the algorithm into a proof each of whose steps are logical deductions of a certain type. Prove weak inference/existence versions of these steps and make a careful accounting of how the degrees are growing in each step. As one can imagine this is a formidable task and includes as substeps giving new constructive proofs of very classical theorems—like the Laplace's algebraic proof of the fundamental theorem of algebra, Hermite's theorem for counting real roots using signatures of quadratic forms, the intermediate value theorem amongst others—all the time keeping track of the degrees appearing in the algebraic certificates.

2.6. **Works not covered.** I hope that in this article I have been able to give a snapshot of Marie-Françoise's work and some of the beautiful mathematics behind them. Unfortunately, because of its breadth and large volume, as well as constraints on the length of this article, it was not possible to discuss many very important aspects of her work. In particular, just to mention a *few*, I have not discussed her work with Diatta, Diatta, Rouillier, and Sagraloff on efficient algorithms for computing topology of curves, with Aviva Szpirglas on Sylvester double sums, with Dima Pasechnik and the author on the topology of semi-algebraic sets defined by "partly" quadratic polynomials, with Fatima Boudaoud and Fabrizio Caruso on certificates of positivity using the Bernstein basis, with Thomas Lickteig on Sylvester-Habicht sequences and fast Cauchy index computation, and with Nicolai Vorobjov on complexification and degree of semi-algebraic sets.

Figure 3. Louis Mahé, Marie-Françoise Roy and Michel Coste in Rennes, 2011.

2.7. **Impact.** While the topic of real algebraic geometry is now firmly rooted as a subdiscipline of mathematics worthy of study—it was certainly not the case when Marie-Françoise began her career. Indeed it is fair to say that the book *Géométrie algébrique réelle* (with Jacek Bochnak and Michel Coste) [3] published in 1987, and the once-a-decade series of conferences in Rennes (1981, 1991, 2001, and 2011) with published proceedings played a major role in establishing the topic as an important area of research in mathematics (one with many connections to both pure and applied aspects of mathematics).

Within the community of real algebraic geometry (as I hope it is clear from this article) Marie-Françoise has been involved in a very wide spectrum of research—from the very abstract, to constructive and computational. She has had an unusually large number of collaborators some of whom are from outside the area of real algebraic geometry. I think what made this possible is Marie-Françoise's rather rare ability to grasp and communicate key ideas very lucidly—even to mathematicians not versed in real algebra. This led to building bridges between different areas—such as between real algebraic geometry and discrete and computational geometry as well as to the area of symbolic computation. Indeed it was such a collaboration (with my Phd advisor Richard Pollack) that brought me into contact with her for which I am grateful. From her I learned that one does not really understand a proof (even one's own) unless one is able to "see" it and the vital importance of proper notation in writing and communicating mathematics. Many ideas that have been mentioned above (use of infinitesimals in algorithms, dynamical proofs, subresultants etc.) existed prior to Marie-Françoise's work.

However, it is Marie-Françoise (in collaboration with various coauthors) who clarified and sharpened these ideas leading to new advances. I would be remiss if I don't mention one other quality. Some of Marie-Françoise's projects have taken a long time to bring to fruition. This is indicative of a particularly obstinate trait in her character—of not giving up even when the technical obstacles to carrying through a particular program might seem impossible to overcome. In this she is a role model for all young mathematicians.

Over her career Marie-Françoise has mentored many mathematicians from many parts of the world (including the author) and she (along with Michel Coste and Louis Mahé) made Rennes a leading center of research in real algebraic geometry with a constant stream of visitors and weekly seminars.

3. Women in Mathematics

Marie-Françoise has been very active in promoting the cause of women in mathematics in various national and international forums. Marie-Françoise was one of the founders of European Women in Mathematics (EWM), and was the convenor of EWM between 2009 and 2013. In 1987 she cofounded the French organization for women in mathematics, Femmes et Mathématiques, and became the organization's first president and was one of the founding members of the African Women in Mathematics Association (founded in 2013). She was the first chair of the IMU Committee for Women in Mathematics (CWM) between 2015 and 2022 and led the "Gender gap in science"[5] project (funded by the International Science Council [ISC] in cooperation with IUPAC). A book[6] as well as a booklet[7] containing the summary of the results of the project and a full list of its recommendations in several languages have been published.

4. Work in Africa and Niger

Marie-Françoise spent two years of her professional career (1981–1983) at Abdou Moumouni University in Niger. She has continued to be very deeply involved in mathematical and social projects in Africa and in particular in Niger. She was the scientific officer for Sub-Saharan Africa in Centre International de Mathématiques Pures et Appliquées, CIMPA] (2007–2013) and is the president of Association d'Echanges Culturels Cesson Dankassari (Tarbiyya-Tatali), an organization working to support the sustainable development of the commune of Dankassari in Niger through the solidarity of the French commune Cesson-Sévigné where she lives. Her book [17] (coauthored with Nicole Moulin, Boubé Namaiwa, and Bori Zamo) is a sociopolitical work describing the history of a village called Lougou in Niger and of its queen Saraouniya, its encounter with colonialism and its aftermath.

[5] https://gender-gap-in-science.org

[6] https://zenodo.org/record/3882609

[7] https://gender-gap-in-science.org/promotional-materials

References

[1] Emil Artin, *Über die Zerlegung definiter Funktionen in Quadrate* (German), Abh. Math. Sem. Univ. Hamburg **5** (1927), no. 1, 100–115, DOI 10.1007/BF02952513. MR3069468

[2] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2006 (second edition). Revised version of the second edition online at http://perso.univ-rennes1.fr/marie-francoise.roy/. MR1998147 (2004g:14064)

[3] J. Bochnak, M. Coste, and M.-F. Roy, *Géométrie algébrique réelle* (French), Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 12, Springer-Verlag, Berlin, 1987. MR949442

[4] John Canny, *The complexity of robot motion planning*, ACM Doctoral Dissertation Awards, vol. 1987, MIT Press, Cambridge, MA, 1988. MR952555

[5] George E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), Lecture Notes in Comput. Sci., Vol. 33, Springer, Berlin-New York, 1975, pp. 134–183. MR403962

[6] Michel Coste and Marie-Françoise Coste-Roy, *Le topos étale réel d'un anneau* (French), Cahiers Topologie Géom. Différentielle **22** (1981), no. 1, 19–24. Third Colloquium on Categories (Amiens, 1980), Part II. MR609155

[7] Michel Coste, Henri Lombardi, and Marie-Françoise Roy, *Dynamical method in algebra: effective Nullstellensätze*, Ann. Pure Appl. Logic **111** (2001), no. 3, 203–256, DOI 10.1016/S0168-0072(01)00026-4. MR1848137

[8] Charles N. Delzell, *Kreisel's unwinding of Artin's proof*, Kreiseliana, A K Peters, Wellesley, MA, 1996, pp. 113–246. MR1435764

[9] Michael Eisermann, *The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains*, Amer. Math. Monthly **119** (2012), no. 9, 715–752, DOI 10.4169/amer.math.monthly.119.09.715. MR2990932

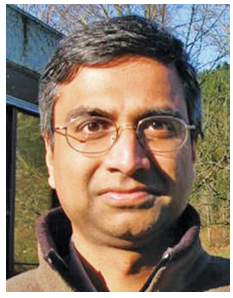
[10] D. Yu. Grigor'ev, *Complexity of deciding Tarski algebra*, J. Symbolic Comput. **5** (1988), no. 1-2, 65–108, DOI 10.1016/S0747-7171(88)80006-3. MR949113

[11] D. Grigoriev, *Complexity of Positivstellensatz proofs for the knapsack*, Comput. Complexity **10** (2001), no. 2, 139–154, DOI 10.1007/s00037-001-8192-0. MR1880908

[12] David Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. (N.S.) **37** (2000), no. 4, 407–436, DOI 10.1090/S0273-0979-00-00881-8. Reprinted from Bull. Amer. Math. Soc. **8** (1902), 437–479. MR1779412

[13] Jean B. Lasserre, *The moment-SOS hierarchy*, Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. IV. Invited lectures, World Sci. Publ., Hackensack, NJ, 2018, pp. 3773–3794. MR3966551

[14] S. Lojasiewicz, *Triangulation of semi-analytic sets*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (3) **18** (1964), 449–474. MR173265
[15] Henri Lombardi, *Effective real Nullstellensatz and variants*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 263–288. MR1106428
[16] Henri Lombardi, Daniel Perrucci, and Marie-Françoise Roy, *An elementary recursive bound for effective Positivstellensatz and Hilbert's 17th problem*, Mem. Amer. Math. Soc. **263** (2020), no. 1277, v+125, DOI 10.1090/memo/1277. MR4071235
[17] Nicole Moulin, Boubé Namaiwa, Marie-Françoise Roy, and Bori Zamo, *Lougou et saraouniya*, 2ème édition, Coedition L'Harmattan - Tarbiyya-Tatali, 2017.
[18] James 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** (1992), no. 3, 255–299, DOI 10.1016/S0747-7171(10)80003-3. MR1156882
[19] Abraham Robinson, *Introduction to model theory and to the metamathematics of algebra*, North-Holland Publishing Co., Amsterdam, 1963. MR153570
[20] Abraham Robinson, *Model theory as a framework for algebra*, Studies in model theory, MAA Stud. Math., Vol. 8, Math. Assoc. America, Buffalo, NY, 1973, pp. 134–157. MR337596
[21] Claus Scheiderer, *Real and étale cohomology*, Lecture Notes in Mathematics, vol. 1588, Springer-Verlag, Berlin, 1994. MR1321819
[22] Alfred Tarski, *A decision method for elementary algebra and geometry*, University of California Press, Berkeley-Los Angeles, Calif., 1951. 2nd ed. MR44472



Saugata Basu

Credits

Figures 1 and 3 are courtesy of Marie-Françoise Roy.
Figure 2 is courtesy of Saugata Basu.
Photo of Saugata Basu is courtesy of Mathematisches Forschungsinstitut Oberwolfach, CC-BY-SA 2.