Counting Complexity Classes for Numeric Computations II: Algebraic and Semialgebraic Sets

Extended Abstract [*]

Peter Bürgisser[†]
Department of Mathematics
Paderborn University
D-33095 Paderborn, Germany
pbuerg@upb.de

Felipe Cucker[‡]
Department of Mathematics
City University of Hong Kong
83 Tat Chee Avenue, Kowloon, Hong Kong
macucker@math.cityu.edu.hk

ABSTRACT

We define counting classes $\#\mathrm{P}_{\mathbb{R}}$ and $\#\mathrm{P}_{\mathbb{C}}$ in the Blum-Shub-Smale setting of computations over the real or complex numbers, respectively. The problems of counting the number of solutions of systems of polynomial inequalities over $\mathbb{R}$, or of systems of polynomial equalities over $\mathbb{C}$, respectively, turn out to be natural complete problems in these classes. We investigate to what extent the new counting classes capture the complexity of computing basic topological invariants of semialgebraic sets (over $\mathbb{R}$) and algebraic sets (over $\mathbb{C}$). We prove that the problem to compute the (modified) Euler characteristic of semialgebraic sets is $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$-complete, and that the problem to compute the geometric degree of complex algebraic sets is $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$-complete. We also define new counting complexity classes GCR and GCC in the classical Turing model via taking Boolean parts of the classes above, and show that the problems to compute the Euler characteristic and the geometric degree of (semi)algebraic sets given by integer polynomials are complete in these classes. We complement the results in the Turing model by proving, for all $k \in \mathbb{N}$, the $\mathsf{FPSPACE}$-hardness of the problem of computing the kth Betti number of the set of real zeros of a given integer polynomial. This holds with respect to the singular homology as well as for the Borel-Moore homology.

Categories and Subject Descriptors

F.1.3 [**Computation by Abstract Devices**]: Complexity Measures and Classes—*Reducibility and completeness*; F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems; I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms

General Terms

Algorithms, Theory

Keywords

counting complexity classes, completeness, Euler characteristic, geometric degree, semialgebraic sets, Betti numbers

1. INTRODUCTION

The theory of computation introduced by Blum, Shub, and Smale in [9] allows for computations over an arbitrary ring R. Emphasis was put, however, on the cases $R = \mathbb{R}$ or $R = \mathbb{C}$. For these two cases, a major complexity result in [9] exhibited natural NP-complete problems, namely, the feasibility of semialgebraic or algebraic sets, respectively. Thus, the complexity of a basic problem in semialgebraic or algebraic geometry was precisely characterized in terms of completeness in complexity classes.

In contrast with discrete[1] complexity theory, these first completeness results were not followed by an avalanche of similar results. Also in contrast with discrete complexity theory, very little emphasis was put on functional problems. These attracted attention at the level of analysis of particular algorithms, but structural properties of classes of such problems have been hardly studied. So far, the most systematic approach to study the complexity of certain functional problems within a framework of computations over the reals is Valiant's theory of VNP-completeness [13, 54, 57]. However, the relationship of this theory to the more general BSS-setting is, as of today, poorly understood.

A recent departure from the situation above is the work focusing on complexity classes related with counting problems, i.e., functional problems, whose associated functions count the number of solutions of some decisional problem.

In classical complexity theory, counting classes were introduced by Valiant in his seminal papers [55, 56]. Valiant defined $\#\mathsf{P}$ as the class of functions which count the number of accepting paths of NP-machines and proved that the computation of the permanent is $\#\mathsf{P}$-complete. This exhibited

[*] A full version of this paper is available at `http://www.arxiv.org/abs/cs/cs.CC/0312007`

[†] Partially supported by DFG grant BU 1371.

[‡] Partially supported by City University SRG grant 7001558.

[1] All along this paper we use the words *discrete*, *classical* or *Boolean* to emphasize that we are refering to the theory of complexity over a finite alphabet as exposed in, e.g., [2, 46].

STOC'04, June 13–15, 2004, Chicago, Illinois, USA.
Copyright 2004 ACM 1-58113-852-0/04/0006 ...$5.00.

an unexpected difficulty for the computation of a function whose definition is only slightly different to that of the determinant, a well-known “easy” problem. This difficulty was highlighted by a result of Toda [53] proving that $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$, i.e., that $\#\mathsf{P}$ has at least the power of the polynomial hierarchy.

In the continuous setting, i.e., over the reals, counting classes were first defined by Meer in [41]. Here a real version $\#\mathrm{P}_\mathbb{R}$ of the class $\#\mathsf{P}$ was introduced, but the existence of complete problems for it was not studied[2]. Instead, the focus of Meer’s paper are some logical properties of this class (in terms of metafinite model theory). After that, in [15, 16], an in-depth study of the properties of counting classes over $(\mathbb{R}, +, -, \leq)$ was carried out. In this setting, real computations are restricted to those which do not perform multiplications and divisions. Main results in [15, 16] include both structural relationships between complexity classes and completeness results.

The goal of this paper is to further study $\#\mathrm{P}_\mathbb{R}$ (and its version over the complex numbers, $\#\mathrm{P}_\mathbb{C}$) following the lines of [15, 16]. A driving motivation is to capture the complexity to compute basic quantities of (real) algebraic geometry or algebraic topology in terms of complexity classes and completeness results. Examples for such quantities are: dimension, cardinality of 0-dimensional sets, geometric degree, multiplicities, number of connected or irreducible components, Betti numbers, rank of (sheaf) cohomology groups, Euler characteristic, etc. To our best knowledge, besides [15, 16], the only known non-trivial complexity lower bounds for some of these quantities are in [1, 47]. For other attempts to characterize the intrinsic complexity of problems of algebraic geometry, especially elimination, we refer to [40, 29].

1. Counting classes The class $\#\mathsf{P}$ is defined to be the class of functions $f\colon \{0,1\}^\infty \to \mathbb{N}$ for which there exists a polynomial time Turing machine M and a polynomial p with the property that for all $n \in \mathbb{N}$ and all $x \in \{0,1\}^n$, $f(x)$ counts the number of strings $y \in \{0,1\}^{p(n)}$ such that M accepts (x, y).

Replacing Turing machines by BSS-machines over $\mathbb{R}$ in the definition above, we get a class of functions $f\colon \mathbb{R}^\infty \to \mathbb{N} \cup \{\infty\}$, which we denote by $\#\mathrm{P}_\mathbb{R}$. Thus $f(x)$ counts the number of vectors $y \in \mathbb{R}^{p(n)}$ such that M accepts (x, y). Note that this number may be infinite, that is, $f(x) = \infty$. In a similar way, one defines $\#\mathrm{P}_\mathbb{C}$.

Feasibility of Boolean combinations of polynomial equalities and inequalities and of polynomial equations were proved to be $\mathrm{NP}_\mathbb{R}$-complete problems in [9]. These problems are denoted by $\mathrm{SAS}_\mathbb{R}$ and $\mathrm{F{\scriptsize EAS}}_\mathbb{R}$ respectively. As one may expect, their counting versions $\#\mathrm{SAS}_\mathbb{R}$ and $\#\mathrm{F{\scriptsize EAS}}_\mathbb{R}$, consisting of counting the number of solutions of systems as described above, turn out to be complete in $\#\mathrm{P}_\mathbb{R}$. Similarly, the problem $\#\mathrm{HN}_\mathbb{C}$ consisting of counting the number of complex solutions of systems of polynomial equations is complete in $\#\mathrm{P}_\mathbb{C}$. While we prove these results in §3, one of the goals of this paper is to show that other problems, of a basic geometric nature, are also complete in these counting classes.

2. Degree and Euler characteristic The study of the zero sets of systems of polynomial equations is the subject of algebraic geometry. Classically, these zero sets, called algebraic varieties, are considered in k^n for some algebraically closed field k. A central choice for k is $k = \mathbb{C}$. Given an algebraic variety Z, a number of quantities are attached to it, which describe several geometric features of Z. Examples of such quantities are dimension and degree. Roughly speaking, the degree measures how twisted Z is embedded in affine space by, more precisely, counting how many intersection points it has with generic affine subspaces of a certain well-chosen dimension. Not surprisingly, an algebraic variety has degree one if and only if it is an affine subspace of $\mathbb{C}^n$. The degree of an algebraic variety occurs in many results in algebraic geometry, the most celebrated of them being Bézout’s Theorem. It also occurs in the algorithmics of algebraic geometry [22, 28] and in lower bounds results [14, 51].

The birth of algebraic topology is entangled with more than one century of attempts to prove a statement of Euler asserting that in a polyhedron, the number of vertices plus the number of faces minus the number of edges equals 2 (see [39] for a vivid account of this history). A precise definition of a generalization of this sum is today known with the name of Euler or Euler-Poincaré characteristic.

The Euler characteristic of X, denoted by $\chi(X)$, is one of the most basic invariants in algebraic topology. Remarkably, it naturally occurs in many applications in other branches of geometry. For instance, in differential geometry, where it is proved that a compact, connected, differentiable manifold X has a non-vanishing vector field if and only if $\chi(X) = 0$ [50, p. 201]. Also, in algebraic geometry, a generalization of the Euler characteristic (w.r.t. sheaf cohomology) plays a key role in the Riemann-Roch Theorem for non-singular projective varieties [32]. The Euler characteristic has also played a role in complexity lower bounds results. For this purpose, Yao [58] introduced a minor variation of the Euler characteristic. This *modified Euler characteristic* has a desirable additivity property and coincides with the usual Euler characteristic in many cases, e.g., for compact semialgebraic sets and complex algebraic varieties.

3. Completeness results A semialgebraic subset of $\mathbb{R}^n$ is defined by a Boolean combination of polynomial equalities and inequalities. Machines over $\mathbb{R}$ decide (in bounded time) sets which, when restricted to a fixed dimension n, are semialgebraic subsets of $\mathbb{R}^n$. Therefore, this kind of sets are also the natural input of geometric problems in this setting. We have already remarked that deciding emptyness of a semialgebraic set is $\mathrm{NP}_\mathbb{R}$-complete, and that counting the number of points of such a set is $\#\mathrm{P}_\mathbb{R}$-complete. One of the main results in this paper is that the problem $\mathrm{E{\scriptsize ULER}}^*_\mathbb{R}$ consisting of computing the modified Euler characteristic of a semialgebraic set is $\mathrm{FP}_\mathbb{R}^{\#\mathrm{P}_\mathbb{R}}$-complete (Theorem 7.1). The class $\mathrm{FP}_\mathbb{R}^{\#\mathrm{P}_\mathbb{R}}$ is an extension of $\#\mathrm{P}_\mathbb{R}$ in which we allow a polynomial time computation with an oracle (i.e., a black box) for a function f in $\#\mathrm{P}_\mathbb{R}$. This enhances the power of $\#\mathrm{P}_\mathbb{R}$ by allowing one to compute several values of f instead of only one.

Over the complex numbers, the situation is similar. Natural inputs for geometric problems are quasialgebraic sets, i.e., sets defined by a Boolean combination of polynomial equations. Of particular interest are algebraic varieties. We already remarked that deciding emptyness of an algebraic

[2] To distinguish between classical and, say, real complexity complexity classes, we use the subscript $\mathbb{R}$ to indicate the latter. Also, to further emphasize this distinction, we write the former in sans serif.

variety is $\mathrm{NP}_\mathbb{C}$-complete and that counting the number of points of such a set is $\#\mathrm{P}_\mathbb{C}$-complete. Another main result in this paper is that the problem Degree consisting of computing the degree of an algebraic variety is $\mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$-complete (Theorem 5.2).

The proofs of our completeness results rely on diverse tools drawn from algebraic geometry, algebraic topology, and complexity theory. Two of the techniques we use deserve, we believe, some highlight. The first one is the use of generic quantifiers, describing properties which hold for almost all values. A blend of reasonings in logic and geometry allows one to eliminate generic quantifiers in parameterized formulae. The basic idea behind this method appeared already in [31] and was used also in [7], but the method itself was developed in [35, 37, 38] to prove that the problem of computing the dimension of a semialgebraic (or complex algebraic) set is complete in $\mathrm{NP}_\mathbb{R}$ (resp. $\mathrm{NP}_\mathbb{C}$). We extend this method and use this in the completeness proofs of both the degree and the Euler characteristic problems.

The second technique we want to highlight is the application of Morse theory for the computation of the Euler characteristic. The use of Morse functions as an algorithmic tool in algebraic geometry goes back to [23, 24] where the "critical points method" was developed to decide quantified formulae. Several algorithms to compute the Euler characteristic of a semialgebraic set reduce first to the case of a smooth hypersurface and then apply the fundamental theorem of Morse theory [3, 12, 52]. We proceed similarly. It should be noted, however, that our reduction to the smooth hypersurface case is different from those in the references above since the latter can not be carried out within the allowed resources (polynomial time for real machines).

4. Completeness results in the Turing model In the discussion above we considered real solutions of systems of real polynomials and complex solutions of systems of complex polynomials. If one restricts the input polynomials for a problem to have integer coefficients, then the input data for this problem can be encoded in a finite alphabet and may be considered in the classical setting. To distinguish this discretized version from its continuous counterpart we will add the superscript $\mathbb{Z}$ in the problem's name. Thus, for instance, $\mathrm{HN}_\mathbb{C}^\mathbb{Z}$ is the problem of deciding the existence of complex solutions of a system of integer polynomial equations and $\#\mathrm{HN}_\mathbb{C}^\mathbb{Z}$ is the problem of counting the number of these solutions.

It is known that $\mathrm{HN}_\mathbb{C}^\mathbb{Z} \in \mathsf{PSPACE}$, and a more recent result of Koiran [34] shows that, assuming the generalized Riemann hypothesis, $\mathrm{HN}_\mathbb{C}^\mathbb{Z} \in \mathsf{RP}^{\mathsf{NP}}$. On the other hand, it is well-known (and rather trivial) that $\mathrm{HN}_\mathbb{C}^\mathbb{Z}$ is NP-hard. The complexity of problems like $\mathrm{Feas}_\mathbb{R}^\mathbb{Z}$ or $\mathrm{SAS}_\mathbb{R}^\mathbb{Z}$ is much less understood, the gap between their known lower NP and upper PSPACE bounds being much larger.

In this paper we introduce two new counting complexity classes in the discrete setting namely, GCC and GCR. These classes are closed under parsimonious reductions and located between $\#\mathsf{P}$ and $\mathsf{FPSPACE}$. The problem $\#\mathrm{HN}_\mathbb{C}^\mathbb{Z}$ is complete in GCC and the problems $\#\mathrm{SAS}_\mathbb{R}^\mathbb{Z}$ and $\#\mathrm{Feas}_\mathbb{R}^\mathbb{Z}$ are complete in GCR.

In addition, we also prove that $\mathrm{Degree}^\mathbb{Z}$ and $\mathrm{Euler}_\mathbb{R}^{*\mathbb{Z}}$ are complete in $\mathsf{FP}^{\mathsf{GCC}}$ and $\mathsf{FP}^{\mathsf{GCR}}$, respectively. (We can also show the corresponding statement for the computation of the nonmodified Euler characteristic.) It is interesting to compare this result on the complexity to compute the Euler characteristic with the problem to compute the number of connected components, or more generally, to compute Betti numbers.

Canny [17] showed that the problem $\#\mathrm{CC}_\mathbb{R}^\mathbb{Z}$ of counting the number of connected components of a semialgebraic set described by integer polynomials is in $\mathsf{FPSPACE}$. On the other hand, a result by Reif [47, 48] stating the PSPACE-hardness of a generalized movers problem in robotics easily implies the $\mathsf{FPSPACE}$-hardness of the problem $\#\mathrm{CC}_\mathbb{R}^\mathbb{Z}$.

Following the lines of [16], it is possible to give an alternative proof of the $\mathsf{FPSPACE}$-hardness of $\#\mathrm{CC}_\mathbb{R}^\mathbb{Z}$. Extending this, we can prove that the problem $\mathrm{Betti}(k)_\mathbb{R}^\mathbb{Z}$ of computing the kth Betti number of the real zero set of a given integer polynomial is $\mathsf{FPSPACE}$-hard, for fixed $k \in \mathbb{N}$. (We obtain a similar result for Borel-Moore Betti numbers.) It is open, whether Betti numbers can be computed in polynomial space. Due to lack of space we had to omit the hardness proofs for computing Betti numbers.

State-of-the-art algorithmics for computing the Euler characteristic or the number of connected components of a semialgebraic set suggests that the former is simpler than the latter [3, 4]. In a recently published book [5, page 547] it is explicitly observed that the Euler characteristic of real algebraic sets (which is the alternating sum of the Betti numbers) can be currently more efficiently computed than any of the individual Betti numbers.

Our results give some explanation for the observed higher complexity required for the computation of the number of connected components (or higher Betti numbers) compared to the computation of the Euler characteristic. Namely, $\mathrm{Euler}_\mathbb{R}^{*\mathbb{Z}}$ is $\mathsf{FP}^{\mathsf{GCR}}$-complete, while $\mathrm{Betti}(k)_\mathbb{R}^\mathbb{Z}$ is $\mathsf{FPSPACE}$-hard. Thus the problem $\mathrm{Betti}(k)_\mathbb{R}^\mathbb{Z}$ is not polynomial time equivalent to $\mathrm{Euler}_\mathbb{R}^{*\mathbb{Z}}$ unless there is the collapse of complexity classes $\mathsf{FP}^{\mathsf{GCR}} = \mathsf{FPSPACE}$.

Acknowledgment. We are thankful to Saugata Basu and Pascal Koiran for helpful discussions while writing this paper.

2. PRELIMINARIES

2.1 Machines and complexity classes

We denote by $\mathbb{R}^\infty$ the disjoint union $\mathbb{R}^\infty = \bigsqcup_{n \geq 0} \mathbb{R}^n$, where for $n \geq 0$, $\mathbb{R}^n$ is the standard n-dimensional space over $\mathbb{R}$. The space $\mathbb{R}^\infty$ is a natural one to represent problem instances of arbitrarily high dimension. For $x \in \mathbb{R}^n \subset \mathbb{R}^\infty$, we call n the *size* of x and we denote it by $\mathrm{size}(x)$.

In this paper we will consider BSS-machines over $\mathbb{R}$ as they are defined in [8, 9]. Roughly speaking, such a machine takes an input from $\mathbb{R}^\infty$, performs a number of arithmetic operations and comparisons following a finite list of instructions, and halts returning an element in $\mathbb{R}^\infty$ (or loops forever). For a given machine M, the function φ_M associating its output to a given input $x \in \mathbb{R}^\infty$ is called the *input-output function.* We shall say that a function $f : \mathbb{R}^\infty \to \mathbb{R}^k$, $k \leq \infty$, is *computable* when there is a machine M such that $f = \varphi_M$. Also, a set $A \subseteq \mathbb{R}^\infty$ is *decided* by a machine M if its characteristic function $\chi_A : \mathbb{R}^\infty \to \{0, 1\}$ coincides with φ_M. So, for decision problems we consider machines whose output space is $\{0, 1\} \subset \mathbb{R}$.

Definition 2.1 A machine M over $\mathbb{R}$ is said *to work in polynomial time* when there is a constant $c \in \mathbb{N}$ such that for every input $x \in \mathbb{R}^\infty$, M reaches its output node after at most $\text{size}(x)^c$ steps. The class $\text{P}_\mathbb{R}$ is then defined as the set of all subsets of $\mathbb{R}^\infty$ that can be accepted by a machine working in polynomial time, and the class $\text{FP}_\mathbb{R}$ as the set of functions which can be computed in polynomial time.

Definition 2.2 A set A belongs to $\text{NP}_\mathbb{R}$ if there is a machine M satisfying the following condition: for all $x \in \mathbb{R}^\infty$, $x \in A$ iff there exists $y \in \mathbb{R}^\infty$ such that M accepts the input (x, y) within time polynomial in $\text{size}(x)$. In this case, the element y is called a *witness* for x. (The length of y can be assumed to bounded by a polynomial in $\text{size}(x)$.)

Machines over $\mathbb{C}$ are defined as those over $\mathbb{R}$. Note, though, that branchings over $\mathbb{C}$ are done on tests of the form $z_0 = 0$. The classes $\text{P}_\mathbb{C}$, $\text{NP}_\mathbb{C}$, etc., are then naturally defined.

In [8, Chapter 18] models for parallel computation over $\mathbb{R}$ are defined. Using these models, one defines $\text{FPAR}_\mathbb{R}$ to be the class of functions computable in parallel polynomial time and such that $\text{size}(f(x))$ is bounded by a polynomial in $\text{size}(x)$.

2.2 Algebraic and semialgebraic sets

We very briefly recall some definitions and facts from algebraic geometry, which will be needed later on. Standard textbooks on algebraic geometry are [26, 44, 49]. For information about real algebraic geometry we refer to [6, 10].

An *algebraic set* (or *affine algebraic variety*) Z is defined as the zero set

$$Z = \mathcal{Z}(f_1, \dots, f_r) := \{x \in \mathbb{C}^n \mid f_1(x) = 0, \dots, f_r(x) = 0\}$$

of finitely many polynomials $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$. The *vanishing ideal* $\mathcal{I}(Z)$ of Z consists of all the polynomials vanishing on Z. Note that $\mathcal{I}(Z)$ might be strictly larger than the ideal I generated by $f_1, \dots, f_r$. Actually, by Hilbert's Nullstellensatz, $\mathcal{Z}(I)$ can be characterized as the so-called radical of the ideal I.

A usual compactification of the space $\mathbb{C}^n$ consists of embedding $\mathbb{C}^n$ into $\mathbb{P}^n(\mathbb{C})$, the *projective space* of dimension n over $\mathbb{C}$. Recall, this is the set of complex lines through the origin in $\mathbb{C}^{n+1}$ and $\mathbb{C}^n \hookrightarrow \mathbb{P}^n(\mathbb{C})$ maps a point $x \in \mathbb{C}^n$ to the line in $\mathbb{C}^{n+1}$ passing through the origin and through $(1, x)$. The notion of an affine algebraic variety extends to that of a *projective variety* by replacing polynomials by homogeneous polynomials in $\mathbb{C}[X_0, X_1, \dots, X_n]$, for which elements of $\mathbb{P}^n(\mathbb{C})$ are natural zeros. The embedding $\mathbb{C}^n \hookrightarrow \mathbb{P}^n(\mathbb{C})$ extends to the algebraic subsets of $\mathbb{C}^n$ by defining, for any such set Z, its *projective closure* $\overline{Z}$ as the smallest projective variety in $\mathbb{P}^n(\mathbb{C})$ containing Z.

A *basic semialgebraic set* $S \subseteq \mathbb{R}^n$ is defined to be a set of the form

$$S = \{x \in \mathbb{R}^n \mid g(x) = 0, f_1(x) > 0, \dots, f_r(x) > 0\},$$

where $g, f_1, \dots, f_r$ are polynomials in $\mathbb{R}[X_1, \dots, X_n]$. We say that $S \subseteq \mathbb{R}^n$ is a *semialgebraic set* when it is a Boolean combination of basic semialgebraic sets in $\mathbb{R}^n$. Every semialgebraic set S can be represented as a finite union $S = S_1 \cup \dots \cup S_t$ of basic semialgebraic sets.

We will consider algebraic or semialgebraic sets as input data for machines over $\mathbb{R}$ or $\mathbb{C}$. These sets are encoded by a family of polynomials describing the set as above. To fix ideas, we will unless otherwise specified assume that semialgebraic sets are given as unions of basic semialgebraic sets. So, properly speaking, the input data is not the set itself but the description of it. Also, we have to define how polynomials themselves are encoded as vectors of real (or complex) numbers. However, it will turn out that our results have little dependence on the choice of the representation of the semialgebraic set and on the encoding of the polynomials.

A polynomial $f = \sum_{e \in I} u_e \, x_1^{e_1} \cdots x_n^{e_n}$ is represented in the *sparse encoding* by a list of the pairs (u_e, e) for $e \in I$, where $I = \{e \in \mathbb{N}^n \mid u_e \neq 0\}$. The exponent vector e is thought to be given by a bit vector of length at most $\mathcal{O}(n \log \deg f)$. Depending on the model we are working in, the coefficients u_e are either given as real numbers, complex numbers, or by a bit vector when $u_e \in \mathbb{Z}$ and we are working in the Turing model. The sparse size of f is defined to be $|I|$ times the maximal size of (u_e, e) and the sparse size of a set of polynomials is defined as the sum of the sparse sizes of its elements. To fix ideas, we will always assume that polynomials are given by the sparse encoding.

2.3 Some known completeness results

The following problems describe variants of the basic feasibility problem over $\mathbb{R}$ and $\mathbb{C}$.

$\text{HN}_\mathbb{C}$ (*Hilbert's Nullstellensatz*) Given a finite set of complex polynomials, decide whether these polynomials have a common complex zero.

$\text{F}\small{\text{EAS}}_\mathbb{R}$ (*Polynomial feasibility*) Given a real polynomial, decide whether it has a root in $x \in \mathbb{R}^n$.

$\text{SAS}_\mathbb{R}$ (*Semialgebraic satisfiability*) Given a semialgebraic set S, decide whether it is nonempty.

(Polynomial time) many-one and Turing reductions for machines over $\mathbb{R}$ or $\mathbb{C}$, along with their induced notions of completeness and hardness, are defined as usual. Unless otherwise specified, completeness will refer to many-one completeness. In [9], the following fundamental completeness result was proved.

Theorem 2.3 *The problem* $\text{HN}_\mathbb{C}$ *is* $\text{NP}_\mathbb{C}$*-complete and the problems* $\text{F}\small{\text{EAS}}_\mathbb{R}$ *and* $\text{SAS}_\mathbb{R}$ *are* $\text{NP}_\mathbb{R}$*-complete,*

Consider the following decision problems related to the computation of the dimension of algebraic or semialgebraic sets.

$\text{D}\small{\text{IM}}_\mathbb{C}$ (*Algebraic dimension*) Given a finite set of complex polynomials with affine zero set Z and $d \in \mathbb{N}$, decide whether $\dim Z \geq d$.

$\text{D}\small{\text{IM}}_\mathbb{R}$ (*Semialgebraic dimension*) Given a semialgebraic set S and $d \in \mathbb{N}$, decide whether $\dim S \geq d$.

We denote by $\text{D}\small{\text{IM}}_\mathbb{C}^\mathbb{Z}$ the restriction of the problem $\text{D}\small{\text{IM}}_\mathbb{C}$ to input polynomials with integer coefficients. This problem can be encoded in a finite alphabet and may thus be studied in the classical Turing setting. The problems $\text{D}\small{\text{IM}}_\mathbb{R}^\mathbb{Z}$ and $\text{HN}_\mathbb{C}^\mathbb{Z}$ are defined similarly.

Koiran [35, 38] significantly extended the list of known geometric $\text{NP}_\mathbb{C}$- or $\text{NP}_\mathbb{R}$-complete problems by showing the following.

Theorem 2.4 **(i)** $\text{D}\small{\text{IM}}_\mathbb{C}$ *is* $\text{NP}_\mathbb{C}$*-complete, and* $\text{D}\small{\text{IM}}_\mathbb{C}^\mathbb{Z}$ *is equivalent to* $\text{HN}_\mathbb{C}^\mathbb{Z}$ *with respect to many-one reductions.*

(ii) $\textsc{Dim}_{\mathbb{R}}$ *is* $\mathrm{NP}_{\mathbb{R}}$*-complete, and* $\textsc{Dim}_{\mathbb{R}}^{\mathbb{Z}}$ *is equivalent to* $\textsc{Feas}_{\mathbb{R}}^{\mathbb{Z}}$ *with respect to many-one reductions.*

3. COUNTING COMPLEXITY CLASSES

We defined the classes $\#\mathrm{P}_{\mathbb{R}}$ and $\#\mathrm{P}_{\mathbb{C}}$ in the introduction. Parsimonious and Turing reductions, along with their induced notions of completeness and hardness, are defined as usual. We define now the following counting versions of the basic feasibility problems $\mathrm{HN}_{\mathbb{C}}$, $\textsc{Feas}_{\mathbb{R}}$, and $\mathrm{SAS}_{\mathbb{R}}$.

$\#\mathrm{HN}_{\mathbb{C}}$ (*Algebraic point counting*) Given a finite set of complex polynomials, count the number of complex common zeros, returning ∞ if this number is not finite.

$\#\textsc{Feas}_{\mathbb{R}}$ (*Real algebraic point counting*) Given a real polynomial, count the number of its real roots, returning ∞ if this number is not finite.

$\#\mathrm{SAS}_{\mathbb{R}}$ (*Semialgebraic point counting*) Given a semialgebraic set S, compute its cardinality if S is finite, and return ∞ otherwise.

As was to be expected, these counting problems turn out to be complete in the classes $\#\mathrm{P}_{\mathbb{C}}$ and $\#\mathrm{P}_{\mathbb{R}}$, respectively.

Theorem 3.1 **(i)** *The problem* $\#\mathrm{HN}_{\mathbb{C}}$ *is* $\#\mathrm{P}_{\mathbb{C}}$*-complete with respect to parsimonious reductions.*

(ii) *The problems* $\#\textsc{Feas}_{\mathbb{R}}$ *and* $\#\mathrm{SAS}_{\mathbb{R}}$ *are* $\#\mathrm{P}_{\mathbb{R}}$*-complete with respect to Turing reductions.*

The following proposition, which holds over $\mathbb{C}$ as well, is proved using well-known bounds for the number of connected components of basic semialgebraic sets and the main result in [4, 25, 30].

Theorem 3.2 **(i)** *If* $f \in \#\mathrm{P}_{\mathbb{R}}$ *then, for all* $x \in \mathbb{R}^n$ *for which* $f(x)$ *is finite, the bit-size of* $f(x)$ *is bounded by a polynomial in the size of* x.

(ii) *We have* $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}} \subseteq \mathrm{FPAR}_{\mathbb{R}}$. *(To interpret this, represent* ∞ *by an element of* $\mathbb{R} - \mathbb{N}$.*)*

4. GENERIC QUANTIFIERS

Our completeness results for $\textsc{Degree}$ and $\textsc{Euler}_{\mathbb{R}}^{*}$ crucially depend on Koiran's method [35, 37, 38] to eliminate generic quantifiers in parameterized formulas. In this section, we further develop Koiran's method in order to adapt it to our purposes. The main difference to [35, 37, 38] is the introduction of the notion of a partial witness sequence (compared to the notion of a witness sequence from [35]).

In the sequel $\mathscr{F}_{\mathbb{R}}$ denotes the set of first order formulas over the language of the theory of ordered fields with constant symbols for 0 and 1. The set $\mathscr{F}_{\mathbb{C}}$ is defined similarly.

Definition 4.1 Let $F \in \mathscr{F}_{\mathbb{R}}$ have free variables $a_1, \dots, a_k$. We say that F is *Zariski-generically true* if the set of values $a \in \mathbb{R}^k$ not satisfying $F(a)$ has dimension strictly less than k. We express this fact by writing $\forall^* a\, F(a)$ using the *generic universal quantifier* $\forall^*$.

Remark 4.2 Let $F \in \mathscr{F}_{\mathbb{R}}$ have k free variables and coefficient field K, i.e., K is the field generated by the coefficients of all the polynomials occuring in F. Then $\forall^* a\, F(a)$ is equivalent to each of the following statements:

(a) $\forall \epsilon \in \mathbb{R}\, \forall a \in \mathbb{R}^k\, \exists a' \in \mathbb{R}^k\, \big(\epsilon > 0 \Rightarrow F(a') \wedge \|a - a'\| < \epsilon\big)$,

(b) $\forall a \in \mathbb{R}^k \big(a_1, \dots, a_k$ algebraically independent over $K \Longrightarrow F(a)\big)$.

Part (a) shows that $\forall^* a\, F(a)$ can be expressed by a first order formula. Hence by using the generic quantifier we still describe semialgebraic sets.

Let $K \subseteq \mathbb{R}$ and $\alpha \in \mathbb{R}^k$ with components algebraically independent over K. By Remark 4.2(i)(b), for any formula F with coefficient field contained in K, the implication $(\forall^* a\, F(a)) \Rightarrow F(\alpha)$ holds. Thus α may be interpreted as a *partial witness* for $\forall^* a\, F(a)$.

Given a formula $F(u, a)$ we are now interested in partial witnesses for its Zariski-genericity property which can be used for all values of the parameter u. This may not be attainable with a single partial witness, but it turns out to be doable by using short sequences of such witnesses and taking a majority vote. In the sequel $[n]$ denotes the set $\{1, \dots, n\}$.

Definition 4.3 Let $F(u, a) \in \mathscr{F}_{\mathbb{R}}$ with free variables $u \in \mathbb{R}^p$ and $a \in \mathbb{R}^k$. A sequence $\alpha = (\alpha_1, \dots, \alpha_{2p+1}) \in (\mathbb{R}^k)^{(2p+1)}$ is called a *partial witness sequence* for F if

$$\forall u \in \mathbb{R}^p \Big(\forall^* a \in \mathbb{R}^k\, F(u, a) \Rightarrow |\{i \in [2p{+}1] \mid F(u, \alpha_i)\}| > p\Big).$$

We denote the set of partial witnesses for F by $PW(F)$.

Lemma 4.4 $PW(F)$ *is Zariski dense in* $\mathbb{R}^{k(2p+1)}$.

The next theorem is similar to [38, Thm. 3].

Theorem 4.5 *Let* $F(u, a) \in \mathscr{F}_{\mathbb{R}}$ *be in prenex form with free variables* $u \in \mathbb{R}^p$ *and* $a \in \mathbb{R}^k$, n *bounded variables,* w *alternating quantifier blocks, and* m *atomic predicates given by polynomials of degree at most* $\delta \geq 2$ *with integer coefficients of bit-size at most* ℓ. *Then a point in* $\alpha \in PW(F) \subset \mathbb{Z}^{k(2p+1)}$ *can be computed by a division-free straight-line program* Γ *of length* $(kp)^{\mathcal{O}(1)}\, n^w \log(m\delta) + \mathcal{O}(\log \ell)$ *having* 1 *as its only constant and no inputs.*

Remark 4.6 There exists a Turing machine which, with input $(p, k, n, w, m, \delta, \ell)$, computes Γ in time polynomial in the length of Γ. (This machine does not depend on F.) Note that the computation of α cannot be executed by a Turing machine in polynomial time, since the bit-size of α grows exponentially fast. However, the computation can be executed by a machine over $\mathbb{R}$ or $\mathbb{C}$ in polynomial time.

5. COMPLEXITY OF THE DEGREE

The (geometric) degree $\deg Z$ of an algebraic variety Z embedded in affine or projective space can be interpreted as a measure for the degree of nonlinearity of Z. A detailed treatment of this notion can be found in standard textbooks on algebraic geometry [26, 44, 49]. In this section "dimension" always refers to complex dimension.

Definition 5.1 Let $Z \subseteq \mathbb{C}^n$ be an algebraic set of dimension $d \geq 0$. If Z is irreducible then its (geometric) *degree* $\deg Z$ is the number of intersection points of Z with a generic affine subspace of codimension d. If Z is reducible then its degree is the sum of the degrees of all irreducible components of Z of maximal dimension.The degree of the empty set is defined as 0.

One of the main results of this paper proves the completeness of the following problem over $\mathbb{C}$.
DEGREE(*Geometric degree*) Given a finite set of complex polynomials, compute the geometric degree of its affine zero set.

Theorem 5.2 *The problem* DEGREE *is* $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$*-complete for Turing reductions.*

The difficult part of the proof is the upper bound, i.e., the membership of DEGREE to $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$. To show this membership, we have to describe a polynomial time algorithm over $\mathbb{C}$, which computes the degree using oracle calls to $\#\mathrm{P}_{\mathbb{C}}$. Let $f_1, \dots, f_r$ be an instance for DEGREE and denote its zero set by Z. The basic idea of our algorithm is very simple: we first compute the dimension d of Z by calls to $\mathrm{HN}_{\mathbb{C}}$-oracles using Theorem 2.4. By definition, $\deg Z$ is the number of intersection points of Z with a generic affine subspace A of codimension d. If we could compute such an A, then the number of intersection points could be obtained by a call to $\#\mathrm{HN}_{\mathbb{C}}$.

The difficulty is how to compute a generic affine subspace. Of course, the obvious way to turn this idea into an algorithm would be to choose the subspace A at random. Our goal, however, is to choose A deterministically. We will do so using partial witness sequences for parametrized formulas as described in §4, for which we need to concisely express the degree. If A_a denotes an affine subspace of $\mathbb{C}^n$ of codimension d encoded by the parameter $a \in \mathbb{C}^h$, then we have by the definition of degree

$$\forall^* a \in \mathbb{C}^h \quad |Z \cap A_a| = \deg Z. \tag{1}$$

It is clear that the above statement can be expressed by a first-order formula over $\mathbb{C}$. However, the obvious way to do this leads to a formula with exponentially many variables since $\deg Z$ can be exponentially large.

Our goal is thus to express (1) in a concise way. This will be achieved by using the notion of transversality in §5.1. Expressing the transversality condition with a concise first order formula requires some further ideas shown in §5.2.

5.1 Smoothness and transversality

Let $Z \subseteq \mathbb{C}^n$ be an algebraic set, $x \in Z$, and $f_1, \dots, f_r$ be generators of the vanishing ideal $\mathcal{I}(Z)$ of Z. The *Zariski tangent space* T_xZ of Z at x is defined by

$$T_xZ = \mathcal{Z}(d_xf_1, \dots, d_xf_r)$$

where the *differential of f at x*, $d_xf : \mathbb{C}^n \to \mathbb{C}$, is the linear function defined by $d_xfX = \sum_{j=1}^n \partial_{X_j} f(x)X_j$. We say that x is a *smooth point* of Z if the dimension of T_xZ equals the local dimension of Z at x. A point in Z which is not smooth is said to be a *singular point* of Z.

Definition 5.3 Let $Z \subseteq \mathbb{C}^n$ be an algebraic set and $A \subseteq \mathbb{C}^n$ be an affine subspace.

1. A is called *transversal to Z at $x \in Z \cap A$* iff x is a smooth point of Z and $T_xZ \oplus T_xA = \mathbb{C}^n$.
2. We say that A is *transversal* to Z iff A is transversal to Z at all intersection points $x \in Z \cap A$ and, additionally, there are no intersection points of Z and A at infinity. No intersection points at infinity means that $\overline{Z} \cap \overline{A} \subseteq \mathbb{C}^n$, where $\overline{Z}$ and $\overline{A}$ are the projective closures in $\mathbb{P}^n(\mathbb{C})$ of Z and A.

We remark that $\dim Z = \mathrm{codim} A$ if A is transversal to Z and $Z \cap A \neq \emptyset$.

In the following, we parametrize affine subspaces of codimension d as follows. We denote by $A_a \subseteq \mathbb{C}^n$ the affine subspace of $\mathbb{C}^n$ described by the system of linear equations $g_1(x) = 0, \dots, g_d(x) = 0$ with coefficient vector $a \in \mathbb{C}^h$, where $h = d(n+1) = \mathcal{O}(n^2)$. Note that $\forall^* a \dim A_a = n-d$.

The following lemma shows that the transversality of A to Z can be used to certify that the number of intersection points of Z and A equals $\deg Z$. The proof is based on [44, §5A, Thm. 5.1].

Lemma 5.4 *If $Z \subseteq \mathbb{C}^n$ is an algebraic set of dimension d and $h = d(n+1)$, then we have:*

(i) $\forall^* a \in \mathbb{C}^h$ *A_a is transversal to Z*

(ii) $\forall a \in \mathbb{C}^h$ $\big($*A_a is transversal to Z* $\Rightarrow |Z \cap A_a| = \deg Z\big)$.

5.2 Expressing smoothness and transversality

Lemma 5.4 suggests to use transversality to concisely express degree. But, in turn, to express transversality a difficulty may arise. When we try to describe the Zariski tangent space of Z at a point x, the given equations $f_1 = 0, \dots, f_r = 0$ for Z might not generate the vanishing ideal of Z, since multiplicities might occur. In other words, the ideal I generated by $f_1, \dots, f_r$ might not be radical, and it is not clear how to compute generators of the radical $\sqrt{I}$ within the resources allowed. As a way out, we will express the tangent space and the transversality condition at x by a first order formula, in which all information regarding Z is given by a unary predicate expressing membership of points to Z.

The following lemma is essential for the first order characterization we are seeking. Its proof uses the notion of intersection multiplicity (see the book by Mumford [44] for an exposition of this concept).

Lemma 5.5 *Let $Z \subseteq \mathbb{C}^n$ be an algebraic set of dimension d and $A_a \subseteq \mathbb{C}^n$ be an affine subspace of codimension d, parametrized as above. For $x \in Z \cap A_a$ the following two conditions are equivalent:*

(a) *A_a is transversal to Z at x.*

(b) *For every sufficiently small Euclidean neighborhood $U \subseteq \mathbb{C}^n$ of x there is a Euclidean neighborhood $V \subseteq \mathbb{C}^h$ of a such that for all $a' \in V$ the intersection $Z \cap A_{a'} \cap U$ contains exactly one point.*

Remark 5.6 It is not clear whether transversality can be expressed by short first order formulas over $\mathbb{C}$ since the Euclidean topology is involved. We will circumvent this difficulty by working with the first order theory over the reals. The next lemma provides a concise first order (over the reals) characterization of transversality. However, it is important to keep in mind that we will resort to the reals only as a way of reasoning. All computations in the proof of Theorem 5.2 will be done by machines over $\mathbb{C}$.

In the following, we parametrize a system $f_1, \dots, f_r$ of polynomials over $\mathbb{C}$ by its vector of non-zero coefficients $u \in \mathbb{C}^q$, and we denote the corresponding zero set by Z_u. (Recall, we use the sparse encoding, cf. §2.2.) The following result is proved using Lemma 5.5.

Lemma 5.7 *For all $0 \leq d \leq n$ there is a first order formula $F_d(u, a)$ in $\mathscr{F}_{\mathbb{R}}$ in prenex form with seven quantifier blocks, $\mathcal{O}(n^2)$ bounded variables, and with $\mathcal{O}(q + n)$ atomic predicates given by integer polynomials of degree at most δ and bit-size $\mathcal{O}(1)$, such that for all $u \in \mathbb{C}^q \simeq \mathbb{R}^{2q}$ with $\dim_{\mathbb{C}} Z_u = d$ and all $a \in \mathbb{C}^h$:*

$$F_d(u, a) \text{ is true} \iff A_a \text{ is transversal to } Z_u.$$

5.3 Proof of Theorem 5.2

We begin with the membership of Degree to $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$. Let $p = 2q$. Then, Theorem 4.5 implies that a partial witness sequence $\alpha = (\alpha_1, \dots, \alpha_{2p+1})$ for the formula $F_d(u, a)$ in Lemma 5.7 can be computed (uniformly) by a division-free straight-line program with $(nq)^{\mathcal{O}(1)} \log \delta$ arithmetic operations, using 1 as the only constant. Note that this quantity is polynomially bounded in the sparse input size $\mathcal{O}(nq \log \delta)$.

We claim that the following algorithm solves Degree.

```
input $f_1, \dots, f_r$ with coefficient vector $u$
compute $d := \dim Z_u$ querying $\mathrm{HN}_{\mathbb{C}}$ (use Theorem 2.4)
compute a partial witness sequence
    $\alpha = (\alpha_1, \dots, \alpha_{2p+1})$ for $F_d(u, a)$
for $i = 1$ to $2p + 1$
    compute $N_i := |Z_u \cap A_{\alpha_i}|$ by an oracle call to $\#\mathrm{HN}_{\mathbb{C}}$
compute the majority $N$ of the numbers $N_1, \dots, N_{2p+1}$
return $N$
```

Put $I := \{i \in [2p + 1] \mid F_d(u, \alpha_i) \text{ holds}\}$. Lemma 5.7 and Part (ii) of Lemma 5.4 imply that $N_i = \deg Z_u$ for all $i \in I$. Part (i) of Lemma 5.4 tells us that $\forall^* a\, F_d(u, a)$. Since α is a partial witness sequence, this implies that $|I| > p$ (cf. Definition 4.3). This proves the claim.

It is obvious that the above algorithm can be implemented as a polynomial time oracle machine over $\mathbb{C}$. This shows the membership.

To prove the hardness, note that, by Theorem 3.1, $\#\mathrm{HN}_{\mathbb{C}}$ is $\#\mathrm{P}_{\mathbb{C}}$-complete. It is therefore sufficient to Turing reduce $\#\mathrm{HN}_{\mathbb{C}}$ to Degree. The following reduction does so. For a given system of equations first decide whether its solution set Z is zero-dimensional by a call to $\mathrm{HN}_{\mathbb{C}}$ using Theorem 2.4. This call to $\mathrm{HN}_{\mathbb{C}}$ can be replaced by a call to Degree since $\mathrm{HN}_{\mathbb{C}}$ reduces to Degree (recall $Z = \emptyset$ iff $\deg Z = 0$). If $\dim Z = 0$, then compute $N := \deg Z$ by a call to Degree and return N, otherwise return ∞.

6. PRELIMINARIES FROM ALGEBRAIC AND DIFFERENTIAL TOPOLOGY

6.1 Euler characteristic of compact sets

It is well known that any compact semialgebraic set S can be triangulated [10, § 9.2]. Instead of working with triangulations, we will use the more general notion of finite cell complexes, since this is necessary for the application of Morse theory in §6.4. Compact semialgebraic sets are homeomorphic to finite cell complexes and their topology can be studied through the combinatorics of cell complexes.

We briefly recall the definition of a finite cell complex (also called finite CW-complex), see, for instance, [27] for more details. We denote by D^n the closed unit ball in $\mathbb{R}^n$, and by $S^{n-1} = \partial D^n$ its boundary, the $(n-1)$-dimensional unit sphere. An *n-disk* is a space homemorphic to D^n. By an *open n-cell* we understand a space e^n homeomorphic to the open unit ball $D^n - \partial D^n$. A (finite) *cell complex* X is obtained by the following inductive procedure.

We start with a finite discrete set X^0, whose points are regarded as 0-cells. Inductively, we form the *n-skeleton* X^n from X^{n-1} by attaching a finite number of open n-cells e^n_α via continuous maps $\varphi_\alpha \colon S^{n-1} \to X^{n-1}$. This means that X^n is the quotient space of the disjoint union $X^{n-1} \sqcup_\alpha D^n_\alpha$ of X^{n-1} with a finite collection of n-disks D^n_α under the identifications $x \equiv \varphi_\alpha(x)$ for $x \in \partial D^n_\alpha = S^{n-1}$. Thus as a set, $X^n = X^{n-1} \sqcup_\alpha e^n_\alpha$, where each e^n_α is an open n-cell. We stop this procedure after finitely many steps obtaining the compact space $X = X^d$ of dimension d.

The *Euler characteristic* of a cell complex X is defined as $\chi(X) = \sum_{k=0}^{d} (-1)^k N_k$, where N_k is the number of k-cells of the complex. It is a well-known fact that $\chi(X)$ depends only on the topological space X and not on the cellular decomposition. That is, if two cell complexes are homeomorphic, then their Euler characteristics are the same. Actually χ is even a homotopy invariant.

Example 1 The n-sphere S^n can be realized as a cell complex with two cells, of dimension 0 and n, respectively. The cell e^n is attached to e^0 by the constant map $\varphi : S^{n-1} \to e^0$. We have $\chi(S^n) = 2$ if n is even and $\chi(S^n) = 2$ if n is odd.

A continuous map $p \colon X \to Y$ between topological spaces is called a *covering map* if there exists an open cover $\{U_\alpha\}$ of Y such that for each α, $p^{-1}(U_\alpha)$ is a disjoint union of open sets in X, each of which is mapped by p homeomorphically onto U_α (see e.g., [11, III.3]). If the cardinality of the fibre $p^{-1}(y)$ is constant for $y \in Y$, then this cardinality is called the *number of sheets* of the covering map. This condition is satisfied when Y is connected.

Lemma 6.1 *If $X \to Y$ is a covering map with m sheets (m finite) and Y is defined, then $\chi(X) = m\chi(Y)$.*

6.2 Non-compact semialgebraic sets

There are several ways to extend the definition of χ to non-compact sets. The usual one is using singular homology, which preserves the property of χ of being a homotopy invariant. In §6.3 we will see another way which does not, but instead has a useful additivity property.

In algebraic topology one assigns to a topological space X and a field F the singular *homology vector spaces* $H_k(X; F)$ for $k \in \mathbb{N}$, which depend only on the homotopy type of X and F. The Euler characteristic of X is defined by

$$\chi(X) = \sum_{k \in \mathbb{N}} (-1)^k \dim_F H_k(X; F). \tag{2}$$

It is well known that for cell complexes X, this is consistent with the previous definition. (Note that $\dim_F H_k(X; F) = 0$ if k is greater than the dimension of X.) Consequently, the left-hand side of (2) is independent of the field F. For a general reference to homology we refer to [27, 45].

The following is proved using a relative version of Poincaré-Alexander-Lefschetz duality, cf. [11, Thm. 8.3, p. 351].

Lemma 6.2 *Let Z be a compact n-dimensional real algebraic manifold and $K \subseteq Z$ be a compact semialgebraic subset. Then*

$$\chi(Z-K) = \begin{cases} \chi(Z)-\chi(K) & \text{if } n \text{ is even,}\\ \chi(K) & \text{if } n \text{ is odd.}\end{cases}$$

6.3 Modified Euler characteristic

Assume that S is the disjoint union of two semialgebraic sets S_1 and S_2. In general, it is not true that $\chi(S) = \chi(S_1) + \chi(S_2)$ (for instance, consider the closed 2-dimensional unit ball D^2 decomposed into its interior and its boundary S^2). Yao [58] defined the *modified Euler characteristic* χ' of semialgebraic sets, which satisfies a nice additivity property, and coincides with the usual Euler characteristic for compact semialgebraic sets. The following proposition from [58] characterizes this notion.

Proposition 6.3 *There is a unique function χ' mapping semialgebraic sets to integers, which satisfies the following properties:*

(i) *If $S = \bigsqcup_{i=1}^N S_i$ is a disjoint union of semialgebraic sets, then $\chi'(S) = \sum_{i=1}^N \chi'(S)$.*

(ii) *We have $\chi'(S) = \chi(S)$ for compact semialgebraic sets.*

(iii) *If there is a semialgebraic homeomorphism $S \to T$, then $\chi'(S) = \chi'(T)$.*

Example 2 The inverse image of $\mathbb{R}^n$ under the stereographic projection is S^n minus a point, hence $\chi'(\mathbb{R}^n) = \chi(S^n) - 1 = (-1)^n$. Note that, in contrast with χ, χ' is not invariant under homotopies.

The inclusion-exclusion principle implies that

$$\chi'\Big(\bigcup_{i=1}^N S_i\Big) = \sum_{I\neq\emptyset} (-1)^{|I|-1} \chi'\Big(\bigcap_{i\in I} S_i\Big), \tag{3}$$

where $S_1, \ldots, S_N$ are semialgebraic subsets of $\mathbb{R}^n$ and the summation is over all nonempty subsets I of $[N]$.

6.4 Morse Theory

We recall now some notions and facts from Morse theory. A general reference for this is [42].

Let Z be a differentiable manifold and $\varphi\colon Z \to \mathbb{R}$ be differentiable. A point $x \in Z$ is a *critical point* of φ iff the differential $d_x\varphi\colon T_xZ \to \mathbb{R}$ vanishes. In this case, one may consider the *Hessian* $H_x\varphi\colon T_xZ \times T_xZ \to \mathbb{R}$ of φ at x, which is a symmetric bilinear form (defined by the second order derivatives of φ in local coordinates). The function φ is called *nondegenerate* at the critical point x iff its Hessian is nondegenerate at x. We call the number of negative eigenvalues of a symmetric matrix or of a symmetric bilinear form its *index*. The *index* of φ at x is defined as the index of $H_x\varphi$. The function φ is called a *Morse function* if all its critical points are nondegenerate. Throughout the paper, we will use the convenient notation $\{\varphi \le r\} := \{x \in Z \mid \varphi(x) \le r\}$.

The following result follows from the main theorem of Morse theory [42, Thm. 3.5] and the semialgebraic Morse-Sard Theorem [10, Thm. 9.5.2].

Proposition 6.4 *Let $Z \subseteq \mathbb{R}^n$ be a real algebraic manifold. Then,*

(i) *The Euclidean distance function $L_a\colon Z \to \mathbb{R}$, $x \mapsto \|x-a\|^2$ is a Morse function for Zariski almost all $a \in \mathbb{R}^n$.*

(ii) *Suppose that L_a is a Morse function on Z. Then the number N_k of critical points of L_a with index k is finite for all $0 \le k \le n$ and $\sum_{k=0}^n (-1)^k N_k$ equals the Euler characteristic $\chi(Z)$ of Z.*

Let $\mathscr{H}$ be the set of polynomials $f \in \mathbb{R}[X_1, \ldots, X_n]$ satisfying that $\mathcal{Z}(f) \neq \emptyset$ along with the regularity condition

$$\forall x \in \mathbb{R}^n \ \ (f(x) = 0 \Rightarrow \operatorname{grad} f(x) \neq 0). \tag{4}$$

Note that $\mathcal{Z}(f)$ is a smooth hypersurface for $f \in \mathscr{H}$.

As in §5, we denote by $u \in \mathbb{R}^p$ the vector of non-zero coefficients of the polyomial $f = f_u$ of degree δ in $X_1, \ldots, X_n$, and write $Z_u := \mathcal{Z}(f_u)$ for its zero set in $\mathbb{R}^n$.

The following lemma gives a certificate for L_a to be a Morse function on Z_u in form of a parametrized first order formula. It plays a similar role for the completeness proof of $\textsc{Euler}^*_{\mathbb{R}}$ as the certificate for transversality for the completeness proof of $\textsc{Degree}$ provided in Lemma 5.7.

Lemma 6.5 *There exists $F(u,a)$ in $\mathscr{F}_{\mathbb{R}}$ in prenex form with one quantifier block, n bounded variables, and with $\mathcal{O}(n)$ atomic predicates given by integer polynomials of degree at most $\mathcal{O}(n\delta)$ and bit-size $\mathcal{O}(n\log(np))$ such that, for all $u \in \mathbb{R}^p$ such that $f_u \in \mathscr{H}$ and all $a \in \mathbb{R}^n$,*

$$F(u,a) \text{ holds} \Leftrightarrow L_a\colon Z_u \to \mathbb{R} \text{ is a Morse function.}$$

7. COMPLEXITY OF THE EULER CHARACTERISTIC

Another main result of this paper proves the completeness of the following problem over $\mathbb{R}$.

$\textsc{Euler}^*_{\mathbb{R}}$ (*Modified Euler characteristic*) Given a semialgebraic set $S \subseteq \mathbb{R}^n$ as a union of basic semialgebraic sets

$$S = \textstyle\bigcup_{i=1}^t \{x \in \mathbb{R}^n \mid g_i(x) = 0, f_{i1}(x) > 0, \ldots, f_{ir_i}(x) > 0\},$$

decide whether S is empty and if not, compute $\chi'(S)$.

Theorem 7.1 *The problem $\textsc{Euler}^*_{\mathbb{R}}$ is $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$-complete with respect to Turing reductions.*

The upper bound in Theorem 7.1 is proved in several steps: we first reduce the basic semialgebraic case to the case of a smooth hypersurface by the following lemma, whose proof relies on Lemmas 6.1 and 6.2.

Lemma 7.2 *Let $g, f_1, \ldots, f_r \in \mathbb{R}[X_1, \ldots, X_n]$ be of degree at most δ and $S := \{x \in \mathbb{R}^n \mid g(x) = 0, f_1(x) > 0, \ldots, f_r(x) > 0\}$. Put $g_0 := g$ and define for $1 \le i \le r$*

$$g_i := X_{n+i}^2 f_i - 1, \ G_i := X_0^{\delta+3} g_i(X_1/X_0, \ldots, X_{n+r}/X_0),$$

$$\text{and} \quad H := \sum_{i=0}^r G_i^2.$$

Then, $\Phi := \mathcal{Z}(H-1) \subset \mathbb{R}^{n+r+1}$ is a smooth affine hypersurface and

$$\chi'(S) = \frac{(-1)^{n+r}}{2^{r+1}}(2 - \chi(\Phi)).$$

The case of a smooth hypersurface is dealt with in Proposition 7.3, using Morse theory and partial witness sequences. Consider the function $\chi_{\mathscr{H}} : \mathscr{H} \to \mathbb{Z},\ f \mapsto \chi(\mathcal{Z}(f))$ computing the Euler characteristic of the smooth hypersurface $\mathcal{Z}(f)$ given by $f \in \mathscr{H}$. Note that we don't consider the modified Euler characteristic here.

Proposition 7.3 *The function $\chi_{\mathscr{H}}$ belongs to $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$.*

Sketch of the proof. Let INDEX be the following decision problem. An input to INDEX is a tuple (u, a, x, k, J), where u encodes a real polynomial f in n variables, $a, x \in \mathbb{R}^n$, $k \in \mathbb{N}$ and $J \subseteq [n]$ is nonempty. The question is to decide whether x is a critical point of index k of the function $L_a \colon Z_u \to \mathbb{R}$ satisfying $\partial_{X_j} f(x) \neq 0$ for all $j \in J$. Using efficient algorithms for the characteristic polynomial and Sturm's algorithm, one can show that INDEX is in $\mathrm{P}_{\mathbb{R}}$.

Given (u, a), let $\chi_+(u, a)$ denote the number of (x, k, J) such that $(u, a, x, k, J) \in$ INDEX and $k + |J|$ is odd. Similarly, we define $\chi_-(u, a)$ by requiring that $k + |J|$ is even. Since INDEX $\in \mathrm{P}_{\mathbb{R}}$, the functions $\mathbb{R}^\infty \times \mathbb{R}^\infty \to \mathbb{N} \cup \{\infty\}$ mapping (u, a) to $\chi_+(u, a)$ and $\chi_-(u, a)$, respectively, are in $\#\mathrm{P}_{\mathbb{R}}$.

Using Proposition 6.4 one proves that, if L_a is a Morse function on Z_u then $\chi(Z_u) = \chi_+(u, a) - \chi_-(u, a)$.

Lemma 6.5 and Theorem 4.5 imply that a partial witness sequence α for the formula $F(u, a)$ certifying that $L_a \colon Z_u \to \mathbb{R}$ is a Morse function can be computed (uniformly) by a machine over $\mathbb{R}$ in time $(np)^{\mathcal{O}(1)} \log(\delta)$.

The following algorithm computing $\chi_{\mathscr{H}}$ can be implemented as a polynomial time oracle Turing machine accessing oracles in $\#\mathrm{P}_{\mathbb{R}}$.

```
input $f \in \mathscr{H}$ encoded by its coefficient vector $u$
compute a partial witness sequence
  $\alpha = (\alpha_1, \dots, \alpha_{2p+1})$ for $F(u, a)$
for $\ell = 1$ to $2p + 1$
    compute $\chi(u, \alpha_\ell) := \chi_+(u, \alpha_\ell) - \chi_-(u, \alpha_\ell)$
compute the majority $\chi(u)$ of the numbers
  $\chi(u, \alpha_1), \dots, \chi(u, \alpha_{2p+1})$
return $\chi(u)$
```

In order to show that this algorithm actually computes the Euler characteristic of its input, put $\Lambda := \{\ell \in [2p + 1] \mid F(u, \alpha_\ell) \text{ holds}\}$. By definition of F we know that L_{α_ℓ} is a Morse function on Z_u for all $\ell \in \Lambda$. Hence, $\chi(Z_u) = \chi(u, \alpha_\ell)$ for all $\ell \in \Lambda$. On the other hand, by Proposition 6.4(i) we have $\forall^* a\, F(u, a)$. Since α is a partial witness sequence, this implies that $|\Lambda| > p$ (cf. Def. 4.3). Therefore, the algorithm indeed computes the Euler characteristic of Z_u. □

The proof of the upper bound in Theorem 7.1 is obtained by using (3) and generalizing the proofs of Lemma 7.2 and Proposition 7.3. The proof of hardness is similar as in the proof of Theorem 5.2.

Remark 7.4 In the papers [12, 52], the Euler characteristic of a real algebraic variety is expressed by the index of an associated gradient vector field at zero, which can be algebraically computed according to [21]. Although Morse theory is not explicitly mentioned in [12, 52], the main idea behind these papers is an application of this theory as exposed in [43]. The single exponential time algorithm in [3] for computing the Euler characteristic uses Morse theory explicitly and in a crucial way. However, we note that the reduction in [3] from the case of an arbitrary semialgebraic set to the case of a smooth hypersurface, as well as the reductions in [12, 52], cannot be used in our context, since it is not clear how to compute the deformation parameter or the sufficiently small radius of the intersecting sphere within the allowed resources (polynomial time for *real* machines). Instead, in the proof of Lemma 7.2 we express the Euler characteristic of a real projective variety by the Euler characteristic of its complement, which in turn can be expressed as the Euler characteristic of a "Milnor fibre", which is a smooth hypersurface.

8. RESULTS IN THE TURING MODEL

We recall that if L denotes a problem defined over $\mathbb{R}$ or $\mathbb{C}$, then we denote its restriction to integer inputs by $L^{\mathbb{Z}}$. This way, the discrete problems $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$, $\mathrm{Dim}_{\mathbb{C}}^{\mathbb{Z}}$, $\mathrm{Degree}^{\mathbb{Z}}$, $\mathrm{Euler}_{\mathbb{R}}^{*\mathbb{Z}}$, etc. are well defined and can be studied in the classical Turing setting. We are going to show that all these problems are (Turing-) complete in certain discrete complexity classes, which are obtained from real or complex complexity classes by the operation of taking the Boolean part.

A natural restriction for real or complex machines (considered e.g. in [20, 33, 36]) is the requirement that no constants other than 0 and 1 appear in the machine program. Complexity classes arising by considering such constant-free machines are denoted by a superscript 0 as in $\mathrm{P}_{\mathbb{R}}^0$, $\mathrm{NP}_{\mathbb{R}}^0$, etc.

Definition 8.1 Let $\mathcal{C}$ be a complexity class over $\mathbb{R}$ or $\mathbb{C}$. Its *Boolean part* is the classical complexity class

$$\mathrm{BP}(\mathcal{C}) := \{S \cap \{0,1\}^\infty \mid S \in \mathcal{C}\}.$$

Determining the Boolean part amounts to characterize, in terms of classical complexity classes, the power of resource bounded machines over $\mathbb{R}$ or $\mathbb{C}$ when their inputs are restricted to be binary. The study of Boolean parts has been successful in the setting of additive machines, where practically all natural complexity classes have had their Boolean parts characterized [15, 16, 20, 33]. In contrast, less is known in the setting of unrestricted machines. Two of the most significant results state that $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}) \subseteq \mathsf{P}^{\mathsf{RP}}$ [19] and $\mathrm{BP}(\mathrm{PAR}_{\mathbb{R}}) = \mathsf{PSPACE}/\mathsf{poly}$ [18]. A third one follows from [34] and states that $\mathsf{NP} \subseteq \mathrm{BP}(\mathrm{NP}_{\mathbb{C}}^0) \subseteq \mathsf{RP}^{\mathsf{NP}}$, assuming GRH.

Note that the definition of the Boolean part can be extended to classes such as $\#\mathrm{P}_{\mathbb{C}}$ or $\#\mathrm{P}_{\mathbb{R}}$ in an obvious way. We define the class of *geometric counting complex problems* as $\mathsf{GCC} := \mathrm{BP}(\#\mathrm{P}_{\mathbb{C}}^0)$ and the class of *geometric counting real problems* $\mathsf{GCR} := \mathrm{BP}(\#\mathrm{P}_{\mathbb{R}}^0)$. These are classes of discrete counting problems, closed under parsimonius reductions, which can be located in a small region in the general landscape of classical complexity classes. Namely, we have

$$\#\mathsf{P} \subseteq \mathsf{GCC} \subseteq \mathsf{GCR} \subseteq \mathsf{FPSPACE},$$

the rightmost inclusion following from Theorem 3.2 and [18].

Corollary 8.2

(i) $\mathrm{Feas}_{\mathbb{R}}^{\mathbb{Z}}$, $\mathrm{SAS}_{\mathbb{R}}^{\mathbb{Z}}$, *and* $\mathrm{Dim}_{\mathbb{R}}^{\mathbb{Z}}$ *are* $\mathrm{BP}(\mathrm{NP}_{\mathbb{R}}^0)$*-Turing-complete.*

(ii) $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ *and* $\mathrm{Dim}_{\mathbb{C}}^{\mathbb{Z}}$ *are* $\mathrm{BP}(\mathrm{NP}_{\mathbb{C}}^0)$*-Turing-complete.*

(iii) $\#\mathrm{SAS}_{\mathbb{R}}^{\mathbb{Z}}$ *and* $\#\mathrm{Feas}_{\mathbb{R}}^{\mathbb{Z}}$ *are* GCR*-Turing-complete.*

(iv) $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ *is* GCC*-Turing-complete.*

This follows by direct inspection of the completeness proofs in the model over $\mathbb{R}$ or $\mathbb{C}$, except for the dimension problems, where the claims follow from Theorem 2.4.

Theorem 8.3 **(i)** $\textsc{Degree}^{\mathbb{Z}}$ *is* $\mathsf{FP}^{\mathsf{GCC}}$*-complete with respect to Turing reductions.*

(ii) $\textsc{Euler}^{*\mathbb{Z}}_{\mathbb{R}}$ *is* $\mathsf{FP}^{\mathsf{GCR}}$*-complete with respect to Turing reductions.*

Proof. (i) The proof of Theorem 5.2 for the membership of $\textsc{Degree}$ to $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$ applies here with only one modification. The partial witness sequence α cannot be computed in $\mathrm{BP}(\mathrm{FP}_{\mathbb{C}})$, due to the exponential coefficient growth (cf. Remark 4.6). A way to solve this is to "move" the computation of α to the query. That is, one considers the problem of computing N_i with input (u, i). Clearly, this problem is in $\mathrm{BP}(\#\mathrm{P}_{\mathbb{C}})$: one first computes α in $\mathrm{FP}_{\mathbb{C}}$ and then N_i in $\#\mathrm{P}_{\mathbb{C}}$. The hardness of $\textsc{Degree}^{\mathbb{Z}}$ follows as in Theorem 5.2 using the second statement in Theorem 2.4(i) instead of the first.

(ii) The proof for $\textsc{Euler}^{*\mathbb{Z}}_{\mathbb{R}}$ is a modification of the proof of Theorem 7.1, similar as for part (i) □

9. OPEN PROBLEMS

Problem 1 Can one characterize GCR or GCC in terms of known classical complexity classes?

Problem 2 Toda's theorem [53] states that $\mathsf{PH} \subseteq \mathsf{FP}^{\#\mathsf{P}}$. Is there an analogue of this over $\mathbb{R}$ or over $\mathbb{C}$?

Problem 3 It is known that the problem to count the number of connected components of a semialgebraic set is in $\mathrm{FPAR}_{\mathbb{R}}$. Is it hard in this class? We know that the corresponding result is true in the additive setting [16].

Problem 4 Can Betti numbers of semialgebraic sets be computed in $\mathrm{FPAR}_{\mathbb{R}}$? We know that, in the additive setting, the computation of Betti numbers of semi-linear sets is $\mathrm{FPAR}_{\mathrm{add}}$-complete [16].

Problem 5 What is the complexity to check irreducibility of algebraic varieties over $\mathbb{C}$? And what is the complexity of counting the number of irreducible components of algebraic varieties?

10. REFERENCES

[1] E. Bach. Sheaf cohomology is #P-hard. *J. Symbolic Comput.*, 27(4):429–433, 1999.

[2] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Springer Verlag, 1988.

[3] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. *Discrete Comput. Geom.*, 22(1):1–18, 1999.

[4] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *J. Amer. Math. Soc.*, 13:55–82, 1999.

[5] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics.* Springer Verlag, 2003.

[6] R. Benedetti and J.-J. Risler. *Real Algebraic and Semi-Algebraic Sets.* Hermann, 1990.

[7] L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic Settings for the Problem "$P \neq NP$?". In *The mathematics of numerical analysis*, number 32 in Lectures in Applied Mathematics, pages 125–144. Amer. Math. Soc., 1996.

[8] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer, 1998.

[9] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers. *Bull. Amer. Math. Soc.*, 21:1–46, 1989.

[10] J. Bochnak, M. Coste, and M.F. Roy. *Géometrie algébrique réelle*, volume 12 of *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge.* Springer Verlag, 1987.

[11] G.E. Bredon. *Topology and Geometry.* Number 139 in GTM. Springer Verlag, 1993.

[12] J.W. Bruce. Euler characteristics of real varieties. *Bull. London Math. Soc.*, 22:547–552, 1990.

[13] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and Computation in Mathematics.* Springer Verlag, 2000.

[14] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften.* Springer Verlag, 1997.

[15] P. Bürgisser and F. Cucker. Counting complexity classes over the reals I: The additive case. In *Proc. 14th ISAAC 2003*, number 2906 in LNCS, pages 625–634, 2003.

[16] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations I: Semilinear sets. *SIAM J. Comp.*, 2004. To appear.

[17] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th Ann. ACM STOC*, pages 460–467, 1988.

[18] F. Cucker and D.Yu. Grigoriev. On the power of real Turing machines over binary inputs. *SIAM J. Comp.*, 26:243–254, 1997.

[19] F. Cucker, M. Karpinski, P. Koiran, T. Lickteig, and K. Werther. On real Turing machines that toss coins. In *Proc. 27th ACM STOC, Las Vegas*, pages 335–342, 1995.

[20] F. Cucker and P. Koiran. Computing over the reals with addition and order: Higher complexity classes. *J. Compl.*, 11:358–376, 1995.

[21] D. Eisenbud and H. Levine. An algebraic formula for the degree of a C^∞ map-germ. *Ann. of Math.*, 106:19–38, 1977.

[22] N. Fitchas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *J. Pure Appl. Alg.*, 67:1–14, 1990.

[23] D.Yu. Grigoriev. Complexity of deciding Tarski algebra. *J. Symb. Comp.*, 5:65–108, 1988.

[24] D.Yu. Grigoriev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *J. Symb. Comp.*, 5:37–64, 1988.

[25] D.Yu. Grigoriev and N. Vorobjov. Counting connected components of a semialgebraic set in subexponential

time. *Comp. Compl.*, 2(2):133–186, 1992.

[26] R. Hartshorne. *Algebraic Geometry.* GTM. Springer Verlag, 1977.

[27] A. Hatcher. *Algebraic Topology.* Cambridge University Press, Cambridge, 2002.

[28] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comp. Sci.*, 24:239–277, 1983.

[29] J. Heintz and J. Morgenstern. On the intrinsic complexity of elimination theory. *Journal of Complexity*, 9:471–498, 1993.

[30] 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.

[31] J. Heintz and C.P. Schnorr. Testing polynomials which are hard to compute. In *Logic and Algorithmic: An international Symposium held in honor of Ernst Specker*, pages 237–254. Monogr. No. 30 de l'Enseign. Math., 1982.

[32] F. Hirzebruch. *New Topological Methods in Algebraic Geometry.* Springer Verlag, 1965.

[33] P. Koiran. Computing over the reals with addition and order. *Theoret. Comp. Sci.*, 133:35–47, 1994.

[34] P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Compl.*, 12:273–286, 1996.

[35] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th FOCS*, pages 36–45, 1997.

[36] P. Koiran. A weak version of the Blum, Shub & Smale model. *J. Comp. Syst. Sci.*, 54:177–189, 1997.

[37] P. Koiran. Elimination of parameters in the polynomial hierarchy. *Theoret. Comp. Sci.*, 215:289–304, 1999.

[38] P. Koiran. The real dimension problem is $\mathrm{NP}_{\mathbf{R}}$-complete. *J. Compl.*, 15(2):227–238, 1999.

[39] I. Lakatos. *Proofs and refutations: the logic of mathematical discovery.* Cambridge University Press, 1976.

[40] E.W. Mayr and A.R. Meyer. The complexity of the word problem for commutative semigroups and polynomial ideals. *Adv. Math.*, 46:305–329, 1982.

[41] K. Meer. Counting problems over the reals. *Theoret. Comp. Sci.*, 242:41–58, 2000.

[42] J. Milnor. *Morse theory.* Number 51 in Annals of Math. Studies. Princeton University Press, 1963.

[43] J. Milnor. *Singular points of complex hypersurfaces.* Number 61 in Annals of Math. Studies. Princeton University Press, 1968.

[44] D. Mumford. *Algebraic Geometry I: Complex Projective Varieties.* Springer Verlag, 1976.

[45] James R. Munkres. *Elements of algebraic topology.* Addison-Wesley Publishing Company, Menlo Park, CA, 1984.

[46] C.H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[47] J.H. Reif. Complexity of the mover's problem and generalizations. In *Proc. 20th FOCS*, pages 421–427, 1979.

[48] J.H. Reif. Complexity of the generalized mover's problem. In J.T. Schwartz, M. Sharir, and J. Hopcroft, editors, *Planning, Geometry and Complexity of Robot Motion*, pages 267–281. Ablex Publishing Corporation, 1987.

[49] I.R. Shafarevich. *Basic Algebraic Geometry.* Springer Verlag, 1974.

[50] N. Steenrod. *Topology of Fibre Bundles.* Princeton University Press, 1965.

[51] V. Strassen. Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten. *Num. Math.*, 20:238–251, 1973.

[52] Z. Szafraniec. On the Euler characteristic of analytic and algebraic sets. *Topology*, 25:411–414, 1986.

[53] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comp.*, 21(2):865–877, 1991.

[54] L.G. Valiant. Completeness classes in algebra. In *Proc. 11th ACM STOC*, pages 249–261, 1979.

[55] L.G. Valiant. The complexity of computing the permanent. *Theoret. Comp. Sci.*, 8:189–201, 1979.

[56] L.G. Valiant. The complexity of enumeration and reliability problems. *SIAM J. Comp.*, 8:410–421, 1979.

[57] L.G. Valiant. Reducibility by algebraic projections. In *Logic and Algorithmic: an International Symposium held in honor of Ernst Specker*, volume 30, pages 365–380. Monogr. No. 30 de l'Enseign. Math., 1982.

[58] A.C. Yao. Algebraic decision trees and Euler characteristic. In *Proc. 33rd FOCS*, 1992.