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

Peter Bürgisser*
Dept. of Mathematics
Paderborn University
D-33095 Paderborn
Germany
e-mail: pbuerg@upb.de

Felipe Cucker†
Dept. of Mathematics
City University of Hong Kong
83 Tat Chee Avenue, Kowloon
Hong Kong
e-mail: macucker@math.cityu.edu.hk

Abstract. We define counting classes $\#P_{\mathbb{R}}$ and $\#P_{\mathbb{C}}$ 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 of computing the Euler-Yao characteristic of semialgebraic sets is $FP_{\mathbb{R}}^{\#P_{\mathbb{R}}}$-complete, and that the problem of computing the geometric degree of complex algebraic sets is $FP_{\mathbb{C}}^{\#P_{\mathbb{C}}}$-complete. We also define new counting complexity classes 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 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.

AMS subject classifications. 68Q17, 68Q15, 14Q20, 14P99, 57R99

Key words. counting complexity, real complexity classes, geometric degree, Euler characteristic, Betti numbers

*Partially supported by DFG grant BU 1371 and Paderborn Institute for Scientific Computation.
†Partially supported by City University SRG grant 7001558.

1 Introduction

The theory of computation introduced by Blum, Shub, and Smale in [10] 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 [10] 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. One may say that, if NP-completeness exhibits a single problem with different dresses, the wardrobe of that problem in the real or complex settings seems to be definitely smaller than that in the discrete setting.

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 [15, 72, 75]. 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 [73, 74]. Valiant defined $\#\mathsf{P}$ as the class of functions which count the number of accepting paths of nondeterministic polynomial time Turing machines and proved that the computation of the permanent is $\#\mathsf{P}$-complete. This exhibited 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 [71] 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 [52]. 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 [18], 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 [18]

[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., [3, 60].

[2] To distinguish between classical and, say, real 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.

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 [18]. A driving motivation is to capture the complexity (in terms of completeness results) to compute basic quantities of 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 [18], the only known non-trivial complexity lower bounds for some of these quantities are in [2, 62]. For other attempts to characterize the intrinsic complexity of problems of algebraic geometry, especially elimination, we refer to [36, 50, 51].

Capturing the complexity of some of the above problems will help to reduce the contrasts we mentioned at the beginning of this introduction.

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 [10]. These problems are denoted by $\mathrm{SAS}_{\mathbb{R}}$ and $\mathrm{F}\textsc{eas}_{\mathbb{R}}$ respectively. As one may expect, their counting versions $\#\mathrm{SAS}_{\mathbb{R}}$ and $\#\mathrm{F}\textsc{eas}_{\mathbb{R}}$, 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 Section 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, Euler characteristic and Betti numbers 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. Maybe the most celebrated of them is Bézout's Theorem. It also occurs in the algorithmics of algebraic geometry [27, 35] and in lower bounds results [17, 68].

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 [49] for a vivid account of this history). A precise definition of a generalization of this sum is today (justly) known with the name of Euler characteristic or (justly as well) of 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 $\chi(X) = 0$ [67, 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 [40]. The Euler characteristic has also played a role in complexity lower bounds results. For this purpose, Yao [76] introduced a variation of the Euler characteristic. This *Euler-Yao characteristic*, denoted χ^*, 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. (For locally closed semialgebraic sets, the Euler-Yao characteristic can be equivalently characterized as the the Euler characteristic with respect to the Borel-Moore homology, or as the Euler characteristic with respect to the cohomology with compact supports.)

The Euler characteristic is invariant under homotopy equivalence and the Euler-Yao characteristic is invariant under homeomorphism. Thus, these quantities are used to prove that certain topological spaces are not homotopy equivalent or homeomorphic. Yet, there exist simple examples of pairs of non-equivalent spaces which have the same Euler characteristic. For instance the spheres S^1 and S^3 of dimensions 1 and 3, respectively, satisfy $\chi(S^1) = \chi(S^3) = 0$ and they are not homotopy equivalent. A more powerful object to distinguish non-equivalent spaces is the sequence of *Betti numbers*. This is a sequence of non-negative integers $b_k(X)$, $k \geq 0$, associated to a topological space X, invariant under homotopy equivalence, and satisfying that, if the dimension of X is d, then $b_k(X) = 0$ for all $k > d$. The quantity $b_0(X)$ has a very simple meaning: it is the number of connected components of X. Roughly speaking, for $k \geq 1$, $b_k(X)$ counts the number of k-dimensional holes of X. We have $b_0(S^1) = b_0(S^3) = 1$, $b_1(S^1) = 1$, $b_1(S^3) = b_2(S^3) = 0$, and $b_3(S^3) = 1$. This shows that S^1 and S^3 are not homotopically equivalent (as one could well expect). The Euler characteristic and the sequence of Betti numbers are not unrelated. One has $\chi(X) = \sum_{k\in\mathbb{N}}(-1)^k b_k(X)$.

For locally closed spaces X, a version of the Betti numbers was introduced by Borel and Moore [12]. These Borel-Moore Betti numbers $b_k^{\mathrm{BM}}(X)$ are invariant under homeomorphisms and are related to the Euler-Yao characteristic as follows: $\chi^*(X) = \sum_{k\in\mathbb{N}}(-1)^k b_k^{\mathrm{BM}}(X)$.

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 $\mathrm{EULER}^*_\mathbb{R}$ consisting of computing the Euler-Yao characteristic of a semialgebraic set is $\mathrm{FP}_\mathbb{R}^{\#\mathrm{P}_\mathbb{R}}$-complete. 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 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 of the main results 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.

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 [38] and was used also in [8], but the method itself was developed in [44, 46, 47] 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 [30, 31] 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 [4, 14, 69]. 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 cannot 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. This coincidence between the base field for the space of solutions and that for the ring of polynomials used to describe solution sets is not necessary. While one may think of several combinations breaking it, the one that stands out is the consideration of real (or complex) solutions of polynomial systems over the integers. In practice, the difference between considering real or integer coefficients in the input data is reflected in the difference between the numerical analysis of polynomial systems and their symbolic computation (computer algebra). Note that 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 a 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.

The complexity of computer algebra algorithms for, say, $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ is described using discrete models of computation (e.g., Turing machines). For instance, relatively recent results [27] show that $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}} \in \mathsf{PSPACE}$, and an even more recent result of Koiran [42] shows that, assuming the generalized Riemann hypothesis, $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ is in the Arthur-Merlin class AM. (The class AM was introduced in [1] and should be interpreted as a randomized version of NP that is "close" to 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, and that $\mathrm{EULER}_{\mathbb{R}}^{\mathbb{Z}}$, the problem of computing the (usual) Euler characteristic of a basic semialgebraic set, is complete in $\mathsf{FP}^{\mathsf{GCR}}$.

Canny [21] 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 [62, 63] stating the PSPACE-hardness of a generalized movers problem in robotics easily implies the $\mathsf{FPSPACE}$-hardness of the problem $\#\mathrm{CC}_{\mathbb{R}}^{\mathbb{Z}}$.

We give an alternative proof of the $\mathsf{FPSPACE}$-hardness of $\#\mathrm{CC}_{\mathbb{R}}^{\mathbb{Z}}$ following the lines of [18]. Extending this, we 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 also prove that the problem $\mathrm{BM\text{-}BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$ of computing the kth Borel-Moore Betti number of the set of real zeros of a given integer polynomial is FPSPACE-hard. Note that, for $k \geq 1$, the membership of $\text{BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$ and BM-$\text{BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$ to FPSPACE is, as of today, an open problem.

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 [4, 5]. In a recently published book [6, 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, $\text{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ is $\mathsf{FP}^{\mathsf{GCR}}$-complete, while $\text{BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$ is FPSPACE-hard. Thus the problem $\text{BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$ is not polynomial time equivalent to $\text{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ unless there is the collapse of complexity classes $\mathsf{FP}^{\mathsf{GCR}} = \mathsf{FPSPACE}$.

A similar observation for the Euler characteristic and the Betti numbers in the context of semi-linear sets and additive machines was made in [18, Corollary 5.23].

5. Organization of the paper We start in Section 2 by recalling basic facts about machines and complexity classes over $\mathbb{R}$ and $\mathbb{C}$ as well as about semialgebraic and algebraic sets. Then we define in Section 3 the counting complexity classes $\#\text{P}_{\mathbb{R}}$ and $\#\text{P}_{\mathbb{C}}$, introduce different notions of reduction, and prove some basic completeness results. The technique of generic quantifiers is described in Section 4 and then used in Section 5 to prove the completeness result for DEGREE. The proof of this result is preceded by the exposition of some basic facts about smoothness and transversality, which lead to a concise way of expressing the degree by a parameterized first order formula. We prove the completeness of $\text{EULER}_{\mathbb{R}}^{*}$ in Section 7 after recalling some basic facts from algebraic and differential topology in Section 6. Section 8 deals with complexity in the discrete setting. We define the classes GCC and GCR and, besides some basic completeness results, we prove the completeness of $\text{DEGREE}^{\mathbb{Z}}$ in GCC and of $\text{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ and $\text{EULER}_{\mathbb{R}}^{*\mathbb{Z}}$ in GCR. Finally, we prove the FPSPACE-hardness of the problems $\text{BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$ and BM-$\text{BETTI}(k)_{\mathbb{R}}^{\mathbb{Z}}$. We close the paper in Section 9 with a summary of problems and results, and with some selected open problems in Section 10.

6. Note added in proof For the setting of computations over the complex numbers, the results of this article have been extended in [19, 20].

Acknowledgment. We are thankful to Saugata Basu and Pascal Koiran for helpful discussions while writing this paper. We are specially indebted to Pascal Koiran since many of his results have been a great source of inspiration for us. We thank Maurice Rojas for informing us about a persistent typo in [42]. Thanks also go to Martin Lotz and Peter Scheiblechner for helpful conversations.

2 Preliminaries about real machines

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 $\text{size}(x)$. Contained in $\mathbb{R}^\infty$ is the set of bitstrings $\{0,1\}^\infty$ defined as the union of the sets $\{0,1\}^n$, for $n \in \mathbb{N}$.

In this paper we will consider BSS-machines over $\mathbb{R}$ as they are defined in [9, 10]. 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 $\{0,1\} \subset \mathbb{R}$.

We next introduce some central complexity classes.

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 $\mathrm{P}_\mathbb{R}$ 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 $\mathrm{FP}_\mathbb{R}$ as the set of functions which can be computed in polynomial time.

Definition 2.2 A set A belongs to $\mathrm{NP}_\mathbb{R}$ 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.

Remark 2.3 **(i)** In this model, the element y can be seen as the sequence of guesses used in the Turing machine model. However, we note that in this definition no nondeterministic machine is introduced as a computational model, and non-determinism appears here as a new acceptance definition for the deterministic machine. Also, we note that the length of y can be easily bounded by the time bound $p(\text{size}(x))$.

(ii) 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 $\mathrm{P}_\mathbb{C}$, $\mathrm{NP}_\mathbb{C}$, etc., are then naturally defined.

In [9, Chapter 18] models for parallel computation over $\mathbb{R}$ are defined. Using these models, one defines $\mathrm{PAR}_\mathbb{R}$ to be the class of subsets of $\mathbb{R}^\infty$, whose characteristic function can be computed in parallel polynomial time. Also, one defines $\mathrm{FPAR}_{\mathbb{R}}$ to be the class of functions computable in parallel polynomial time such that $\mathrm{size}(f(x))$ is bounded by a polynomial in $\mathrm{size}(x)$.

2.2 Algebraic and semialgebraic sets

Algebraic geometry is the study of zero sets of polynomials (or of objects which locally resemble these sets). Standard textbooks on algebraic geometry are [33, 56, 65]. For information about real algebraic geometry we refer to [7, 11].

We very briefly recall some definitions and facts from algebraic geometry, which will be needed later on.

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

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

of finitely many polynomials $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$. 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 $f_1, \ldots, f_r$. 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 $\mathbb{C}[X_0, X_1, \ldots, X_n]$, 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

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

where $g, f_1, \ldots, f_r$ are polynomials in $\mathbb{R}[X_1, \ldots, X_n]$. 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 $S = S_1 \cup \ldots \cup S_t$ of basic semialgebraic sets.[3]

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 assume, unless otherwise specified, that semialgebraic sets are given as unions of basic semialgebraic sets. So, properly speaking, the input data is not the set itself but a description of it. Also, we have to define how polynomials

[3] This respresentation is said to be in *Disjunctive Normal Form*. A representation in *Conjunctive Normal Form* is defined in the obvious manner.

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, cf. Remark 9.1.

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 coefficients u_e are given as real (or complex) numbers, while the exponent vector e is thought to be given by a bit vector of length at most $\mathcal{O}(n \log \deg f)$. Let $|I|$ be the total number of terms and $\delta := \max\{2, \deg f\}$. Then $\text{size}(f) := |I| n \log \delta$ is defined to be the sparse size of f. The sparse size of a set of polynomials $f_1, \ldots, f_r$ is defined as $\sum_{i=1}^{r} \text{size}(f_i)$. To fix ideas, we will always assume that polynomials are given by the sparse encoding. If we are dealing with integer polynomials f, we will also consider their sparse bit size, which is defined as the sparse size of f multiplied by the maximum bit size of the occuring integer coefficients.

We remark that another way of encoding polynomials is the *dense encoding.* Here, a polynomial of degree d in n variables is given by the list of its $\binom{n+d}{d}$ coefficients, which has therefore the size of this combinatorial number. Yet another way is to encode the polynomial by a *straight-line program* computing it, cf. [9, 17]. In this case, the size of the encoding of f is the length of the straight-line program.

2.3 Some known completeness results

We first recall the basic notions of reduction for classes of decision problems.[4]

Definition 2.4

1. Let $S, T \subseteq \mathbb{R}^\infty$. We say that $\varphi \colon \mathbb{R}^\infty \to \mathbb{R}^\infty$ is a (polynomial time many-one) *reduction* from S to T if φ can be computed in polynomial time and, for all $x \in \mathbb{R}^\infty$, $x \in S$ if and only if $\varphi(x) \in T$.
2. We say that S (polynomial time) *Turing reduces to* T if there exists an oracle machine which, with oracle T, decides S in polynomial time.
3. Let $\mathcal{C}$ be any class of subsets of $\mathbb{R}^\infty$. We say that a set T is *hard* for $\mathcal{C}$ if, for every $S \in \mathcal{C}$, there is a reduction from S to T. We say that T is $\mathcal{C}$*-complete* if, in addition, $T \in \mathcal{C}$.
4. The notions of *Turing-hardness* or *Turing-completeness* are defined similarly.

The extension of this definition to $\mathbb{C}$ is immediate.

The following problems describing variants of the basic feasibility problem over $\mathbb{R}$ and $\mathbb{C}$ were introduced and studied in [10].

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

[4] This definition is actually for a class $\mathcal{C}$ containing $\text{NP}_\mathbb{R} \cap \text{coNP}_\mathbb{R}$. To define $\text{P}_\mathbb{R}$-completeness, a stronger notion of reduction is necessary.

$\text{FEAS}_{\mathbb{R}}$ (*Polynomial feasibility*) Given a real multivariate polynomial, decide whether it has a real root.

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

In [10], the following fundamental completeness result was proved.

Theorem 2.5 *The problem* $\text{HN}_{\mathbb{C}}$ *is* $\text{NP}_{\mathbb{C}}$*-complete and the problems* $\text{FEAS}_{\mathbb{R}}$ *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.

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

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

We denote by $\text{DIM}_{\mathbb{C}}^{\mathbb{Z}}$ the restriction of the problem $\text{DIM}_{\mathbb{C}}$ 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 $\text{DIM}_{\mathbb{R}}^{\mathbb{Z}}$ and $\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$ are defined similarly.

Koiran [44, 47] significantly extended the list of known geometric $\text{NP}_{\mathbb{C}}$- or $\text{NP}_{\mathbb{R}}$-complete problems by showing the following.

Theorem 2.6 **(i)** $\text{DIM}_{\mathbb{C}}$ *is* $\text{NP}_{\mathbb{C}}$*-complete, and* $\text{DIM}_{\mathbb{C}}^{\mathbb{Z}}$ *is equivalent to* $\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$ *with respect to polynomial-time many-one reductions.*

(ii) $\text{DIM}_{\mathbb{R}}$ *is* $\text{NP}_{\mathbb{R}}$*-complete, and* $\text{DIM}_{\mathbb{R}}^{\mathbb{Z}}$ *is equivalent to* $\text{FEAS}_{\mathbb{R}}^{\mathbb{Z}}$ *with respect to polynomial-time many-one reductions.* □

3 Counting Complexity Classes

Definition 3.1 We say that a function $f\colon \mathbb{R}^\infty \to \mathbb{N} \cup \{\infty\}$ belongs to the class $\#\text{P}_{\mathbb{R}}$ if there exist a polynomial time machine M over $\mathbb{R}$ and a polynomial p such that, for all $x \in \mathbb{R}^n$,

$$f(x) = |\{y \in \mathbb{R}^{p(n)} \mid M \text{ accepts } (x, y)\}|.$$

The complexity class $\text{FP}_{\mathbb{R}}^{\#\text{P}_{\mathbb{R}}}$ consists of all functions $f\colon \mathbb{R}^\infty \to \mathbb{R}^\infty$, which can be computed in polynomial time using oracle calls to functions in $\#\text{P}_{\mathbb{R}}$.

Remark 3.2 **(i)** The class $\#\text{P}_{\mathbb{R}}$ is the one defined by Meer in [52].

(ii) The counting classes $\#\mathrm{P}_{\mathbb{C}}$ and $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$ are defined mutatis mutandis. Also, replacing $\mathbb{R}$ by $\mathbb{Z}_2$ in Definition 3.1 one obtains the classical $\#\mathsf{P}$.

We next define appropriate notions of reduction and completeness.

Definition 3.3 1. Let $f, g\colon \mathbb{R}^\infty \to \mathbb{N} \cup \{\infty\}$. We say that $\varphi\colon \mathbb{R}^\infty \to \mathbb{R}^\infty$ is a *parsimonious reduction* from f to g if φ can be computed in polynomial time and, for all $x \in \mathbb{R}^\infty$, $f(x) = g(\varphi(x))$.

2. We say that f *Turing reduces to* g if there exists an oracle machine which, with oracle g, computes f in polynomial time.

3. Let $\mathcal{C}$ be $\#\mathrm{P}_{\mathbb{R}}$ or $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$. We say that a function g is *hard* for $\mathcal{C}$ if, for every $f \in \mathcal{C}$, there is a parsimonious reduction from f to g. We say that g is $\mathcal{C}$*-complete* if, in addition, $g \in \mathcal{C}$.

4. The notions of *Turing-hardness* or *Turing-completeness* are defined similarly. The extension of this definition to $\mathbb{C}$ is immediate.

We define now the following counting versions of the basic feasibility problems $\mathrm{HN}_{\mathbb{C}}$, $\mathrm{F{\scriptsize EAS}}_{\mathbb{R}}$, and $\mathrm{SAS}_{\mathbb{R}}$.

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

$\#\mathrm{F{\scriptsize EAS}}_{\mathbb{R}}$ (*Real algebraic point counting*) Given a real multivariate 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. In the sequel, given $n \in \mathbb{N}$, we denote by $[n]$ the set $\{1, \ldots, n\}$.

Theorem 3.4 **(i)** *The problem* $\#\mathrm{HN}_{\mathbb{C}}$ *is* $\#\mathrm{P}_{\mathbb{C}}$*-complete (with respect to parsimonious reductions).*

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

PROOF. For part (i) simply check that the reductions given in the corresponding $\mathrm{NP}_{\mathbb{C}}$-completeness result by Blum, Shub and Smale [10] (see also [9]) are parsimonious.

The proof of part (ii) requires a more careful look at the reduction in [9]. In this proof, a machine M solving a given problem in $\mathrm{NP}_{\mathbb{R}}$ is considered and a reduction is established, which associates to every input $\omega \in \mathbb{R}^\infty$, a conjunctive normal form ψ_ω

$$\bigwedge_{i\in I}\left(g_i(x) = 0 \ \vee \ \bigvee_{j\in J_i} f_{ij}(x) > 0\right)$$

(the fact that there is only one equality in each clause is achieved by adding squares). An important point to remark here is that, while the cardinality of I is bounded by a polynomial in the size of ω, the cardinalities r_i of the sets J_i are independent of ω and depend only on M.

Now consider one of the clauses of ψ_ω

$$g_i(x) = 0 \ \vee \ \bigvee_{j\in J_i} f_{ij}(x) > 0. \tag{1}$$

Considering that g_i may be at a point x either $= 0$ or $\neq 0$, and that f_{ij} may be either < 0, $= 0$ or > 0 we have 2×3^{r_i} possibilities for the signs of $g_i, f_{i1}, \ldots, f_{ir_i}$ at a point x. From them, only $K_i = 2 \times 3^{r_i} - 2^{r_i}$ satisfy the clause (1). We conclude that we can rewrite this clause as an *exclusive* disjunction of K_i conjunctions of the form

$$g_i(x) \triangle_i 0 \ \wedge \ \bigwedge_{j\in J_i} f_{ij}(x) \square_{ij} 0 \tag{2}$$

where $\triangle_i \in \{=, \neq\}$ and $\square_{ij} \in \{<, =, >\}$. Now replace in (2) the occurrences

$$\begin{array}{lcl} g_i(x) \neq 0 & \text{by} & g_i(x) z_i - 1 = 0, \\ f_{ij}(x) > 0 & \text{by} & f_{ij}(x) y_{ij}^2 - 1 = 0, \\ f_{ij}(x) < 0 & \text{by} & f_{ij}(x) y_{ij}^2 + 1 = 0, \\ f_{ij}(x) = 0 & \text{by} & f_{ij}(x) = 0 \wedge y_{ij}^2 - 1 = 0. \end{array}$$

This yields a system of equalities which has, for every solution x of (2), exactly 2^{r_i} solutions in the variables x, y, z. Now, for $\ell \in [K_i]$, reduce the system in (2) corresponding to ℓ to a single equation $F_{i\ell}(x, y, z) = 0$ by adding squares and the clause (1) to an equation $F_i^*(x, y, z) = 0$ by taking $F_i^* = \prod_{\ell=1}^{K_i} F_{i\ell}$. Note that, for each solution x of ψ_ω there are exactly 2^r different solutions (x, y, z) of the polynomial

$$F := F_1^*(x, y, z)^2 + \cdots + F_m^*(x, y, z)^2$$

where m is the cardinality of I and $r = r_1 + \ldots + r_m$.

The $\#\mathrm{P}_{\mathbb{R}}$-Turing-hardness of $\mathrm{FEAS}_{\mathbb{R}}$ now follows. Finish the reduction above by querying $\mathrm{FEAS}_{\mathbb{R}}$ for the polynomial F and divide the result by 2^r. □

Remark 3.5 The proof of Theorem 3.4 shows that the version of $\mathrm{SAS}_{\mathbb{R}}$ with semialgebraic sets given in conjunctive normal form is $\#\mathrm{P}_{\mathbb{R}}$-complete with respect to parsimonious reductions.

Proposition 3.6 *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.*

Proof. To prove the statement note that, given $x \in \mathbb{R}^\infty$, there exist polynomials p, q such that the set of witnesses for x is a semialgebraic subset of $\mathbb{R}^{p(n)}$ defined by a union of at most $2^{q(n)}$ basic semialgebraic sets, each of them described by a system of at most $q(n)$ inequalities of polynomials in $p(n)$ variables with degree at most $2^{q(n)}$. If this set is finite, its cardinality coincides with the number of its connected components. Now use the bounds for the number of connected components of such basic semialgebraic sets (see e.g. [17, Thm. 11.1] or [9, Prop. 7, Chapt. 16]), which follow from the well-known Oleĭnik-Petrovski-Milnor-Thom bounds [54, 58, 59, 70]. □

We next locate the newly defined counting complexity classes within the landscape of known complexity classes.

Theorem 3.7 *We have $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}} \subseteq \mathrm{FPAR}_{\mathbb{R}}$. (To interpret this, represent ∞ by an element of $\mathbb{R} - \mathbb{N}$.)*

Proof. By Theorem 3.4(i), it is sufficient to prove that $\#\mathrm{SAS}_{\mathbb{R}}$ belongs to $\mathrm{FPAR}_{\mathbb{R}}$. By Theorem 2.6(ii), the problem of computing the dimension of a semialgebraic set is in $\mathrm{FP}_{\mathbb{R}}^{\mathrm{NP}_{\mathbb{R}}}$, and therefore, in $\mathrm{FPAR}_{\mathbb{R}}$. We use this to compute $\#\mathrm{SAS}_{\mathbb{R}}$ as follows. Given a semialgebraic set, we check whether it is zero dimensional. If yes, we return its number of connected components, otherwise we return ∞. This is in $\mathrm{FPAR}_{\mathbb{R}}$ due to the main result in [5, 32, 37]. □

Remark 3.8 Versions of Proposition 3.6 and of Theorem 3.7 hold over $\mathbb{C}$ as well, with proofs similar to those over $\mathbb{R}$.

The following lemma will be useful later on. It is an immediate consequence of the definition of the counting classes.

Lemma 3.9 *Let $f\colon \mathbb{R}^\infty \times \{0,1\}^\infty \to \mathbb{N}$ be a function in $\#\mathrm{P}_{\mathbb{R}}$. Assign to f and a polynomial p the following function $g\colon \mathbb{R}^\infty \to \mathbb{N}$ obtained by summation: for $x \in \mathbb{R}^n$,*

$$g(x) = \sum_{y \in \{0,1\}^{p(n)}} f(x, y).$$

Then g belongs to $\#\mathrm{P}_{\mathbb{R}}$. A similar statement holds over $\mathbb{C}$. □

4 Generic quantifiers

Our completeness results for DEGREE and $\text{EULER}^*_{\mathbb{R}}$ crucially depend on Koiran's method [44, 46, 47] 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 [44, 46, 47] is the introduction of the notion of a partial witness sequence (compared to the notion of a witness sequence from [44]).

4.1 Efficient quantifier elimination over the reals

For convenience of the reader, we recall a well-known result about efficient quantifier elimination over the reals from Renegar [64, Part III]. 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 real numbers. The subset of formulas with constant symbols for 0 and 1 only, is denoted by $\mathscr{F}^0_{\mathbb{R}}$.

Theorem 4.1 *Let F be a formula in $\mathscr{F}^0_{\mathbb{R}}$ in prenex form with k free variables, 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. That is, F has the form*

$$(Q_1 x^{(1)} \in \mathbb{R}^{n_1}) \dots (Q_w x^{(w)} \in \mathbb{R}^{n_w}) G(y, x^{(1)}, \dots, x^{(w)})$$

with alternating quantifiers $Q_i \in \{\exists, \forall\}$ and free variables $y = (y_1, \dots, y_k) \in \mathbb{R}^k$; the quantifier free formula G is a Boolean function of m atomic predicates

$$g_j(y, x^{(1)}, \dots, x^{(w)}) \Delta_j 0, \quad 1 \leq j \leq m,$$

where the g_j are integer polynomials of degree at most δ and with coefficients of bit-size at most ℓ. Hereby, Δ_j is any of the standard relations $\{\geq, >, =, \neq, \leq, <\}$.

Then F is equivalent to a quantifier-free formula F' in disjunctive normal form

$$\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (h_{ij} \Delta_{ij} 0),$$

where h_{ij} are integer polynomials with degree at most D and bit-size at most L, and such that

$$\log D \leq 2^{\mathcal{O}(w)} \Big(\prod_{i=1}^{w} n_i \Big) \log(m\delta), \quad \log L \leq 2^{\mathcal{O}(w)} \Big(\prod_{i=1}^{w} n_i \Big) \log(m\delta) + \log(k + \ell).$$

Moreover, the number $M := \sum_{i=1}^{I} J_i$ of atomic predicates satisfies the bound

$$\log M \leq 2^{\mathcal{O}(w)} k \Big(\prod_{i=1}^{w} n_i \Big) \log(m\delta).$$

4.2 Construction of generic points

Definition 4.2 Let $F \in \mathscr{F}_{\mathbb{R}}$ have free variables $a_1, \ldots, a_k$. 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 4.3 **(i)** 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) $\{a \in \mathbb{R}^k \mid F(a)\}$ is dense in $\mathbb{R}^k$ with respect to the Euclidean topology,

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

(c) $\forall a \in \mathbb{R}^k \big(\ a_1, \ldots, a_k$ algebraically independent over $K \implies F(a)\big)$.

Part (b) 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.

(ii) One can define the *generic existential quantifier* $\exists^*$ by

$$\exists^* a F(a) \equiv \neg \forall^* a \neg F(a).$$

Note that $\exists^* a F(a)$ iff the set of values $a \in \mathbb{R}^k$ satisfying $F(a)$ has dimension k. We may say that F is *Euclidean-generically true.*

(iii) For first order formulas over the language $\mathscr{F}_{\mathbb{C}}$ of the theory of fields with constant symbols for complex numbers, one can define $\forall^*$ and $\exists^*$ just as above. It is not difficult to see, however, that these two quantifiers coincide over $\mathbb{C}$. That is, Zariski genericity equals Euclidean genericity.

The following result was proved in Koiran [47, Cor. 1].

Proposition 4.4 **(i)** *Let $F \in \mathscr{F}^0_{\mathbb{R}}$ be in prenex form with k free variables, 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. If F is Zariski-generically true, then a point $\alpha \in \mathbb{Z}^k$ satisfying F can be computed by a division-free arithmetic straight-line program Γ of length $\mathcal{O}(kn^w \log(m\delta) + \log \ell)$ having 1 as its only constant and no inputs.*

(ii) *There exists a Turing machine which, with input $(k, n, w, m, \delta, \ell)$, computes Γ in time polynomial in the length of Γ. This machine does not depend on F.*

Since we will need the proof method behind this result later on, we recall the proof. A first ingredient is the following easy lemma, whose proof can be found for instance in [43].

Lemma 4.5 *For positive integers k, L, D recursively define*

$$\alpha_1 := 2^L, \ \alpha_j := 1 + \alpha_1 (D+1)^{j-1} \alpha_{j-1}^D \text{ for } 2 \le j \le k.$$

Then $h(\alpha_1, \ldots, \alpha_k) \neq 0$ for any nonzero integer polynomial h in k variables of degree at most D and coefficients of absolute value less than 2^L. □

The sequence $\alpha_1, \ldots, \alpha_k$ in Lemma 4.5 can be computed by a straight-line program Γ performing $\mathcal{O}(k \log D + \log L)$ arithmetic operations and which has 1 as its only constant.

Proof of Proposition 4.4. Put $S = \{a \in \mathbb{R}^k \mid F(a) \text{ holds}\}$. We use Theorem 4.1 to replace the formula F by an equivalent quantifier free formula $F' = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{ij} \Delta_{ij} 0$ and claim that

$$\bigcap_{i,j} \{a \in \mathbb{R}^k \mid h_{ij}(a) \neq 0\} \subseteq S.$$

Otherwise, there would be some $a \in \mathbb{R}^k - S$ such that $h_{ij}(a) \neq 0$ for all i, j. Since the sign of h_{ij} does not change in a small neighborhood of a, $\mathbb{R}^k - S$ would contain some ball around a. And this contradicts the assumption that S is dense in $\mathbb{R}^k$.

Let D and L be the upper bounds on the degree and bit-size of the polynomials occurring in F', given by Theorem 4.1. According to Lemma 4.5, we can compute a point $\alpha \in \mathbb{Z}^k$ satisfying $h_{ij}(\alpha) \neq 0$, for all i, j and thus $F(\alpha)$, by a straight-line program with $\mathcal{O}(k \log D + \log L)$ arithmetic operations. By plugging in the bounds on D and L the claim follows (use $(\prod_i n_i)^{1/w} \le n/w$). □

4.3 Partial witness sequences

Let $K \subseteq \mathbb{R}$ and $\alpha \in \mathbb{R}^k$ with components algebraically independent over K. By Remark 4.3(i)(c), 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 $\forall^* a\, F(a)$. (The adjective partial refers to the fact that we only have an implication and not an equivalence.)

Remark 4.6 The converse of the implication above, i.e., $F(\alpha) \Rightarrow (\forall^* a\, F(a))$ does not hold in general. Actually, a point $\alpha \in \mathbb{R}^k$ as above and such that $F(\alpha)$ is true only ensures Euclidean genericity: we have $F(\alpha) \Rightarrow (\exists^* a F(a))$.

Over $\mathbb{C}$, the equivalence $(\forall^* a F(a)) \Leftrightarrow F(\alpha)$ holds since Euclidean and Zariski genericity are equivalent. This leads to the stronger notion of *witness sequence.*

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. Recall that $[n]$ denotes the set $\{1, \ldots, n\}$.

Definition 4.7 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 $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_{2p+1}) \in (\mathbb{R}^k)^{(2p+1)}$ is called a *partial witness sequence* for F if

$$\forall u \in \mathbb{R}^p \left(\forall^* a \in \mathbb{R}^k \, F(u,a) \Longrightarrow |\{i \in [2p+1] \mid F(u, \boldsymbol{\alpha}_i)\}| > p \right). \tag{3}$$

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

Lemma 4.8 *$PW(F)$ is Zariski dense in $\mathbb{R}^{k(2p+1)}$.*

Proof. The proof is by a transcendence degree argument similar as in [44, Thm. 5.1]. Let K be the coefficient field of F. We interpret (3) as a first order formula in $\mathscr{F}_{\mathbb{R}}$ with free variables $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_{2p+1}$ and coefficient field K. Applying Remark 4.3(i)(c) to this formula, it is enough to show that $\boldsymbol{\alpha} \in PW(F)$ for any $\boldsymbol{\alpha} \in \mathbb{R}^{k(2p+1)}$ with components algebraically independent over K.

Take such $\boldsymbol{\alpha}$ and let $u \in \mathbb{R}^p$ be such that $\forall^* a \in \mathbb{R}^k \, F(u,a)$. Let K' be the field extension of K generated by the components of u and let K'' be the field extension of K' generated by the components of $\boldsymbol{\alpha}$. Then the transcendence degree of K'' over K' is at least $k(2p+1) - p$. Let B be a transcendence basis of K'' over K' consisting of components of $\boldsymbol{\alpha}$. Then B can omit components of at most p of the $\boldsymbol{\alpha}_i$'s. The remaining $\boldsymbol{\alpha}_i$'s have algebraically independent components over K' and therefore $F(u, \boldsymbol{\alpha}_i)$ holds true for them. Thus $|\{i \in [2p+1] \mid F(u, \boldsymbol{\alpha}_i)\}| > p$. □

The next theorem is similar to [47, Thm. 3].

Theorem 4.9 **(i)** *Let $F(u,a) \in \mathscr{F}^0_{\mathbb{R}}$ 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 $\boldsymbol{\alpha} \in PW(F) \cap \mathbb{Z}^{k(2p+1)}$ 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.*

(ii) *There exists a Turing machine which, with input (p,k,n,w,m,δ,ℓ), computes Γ in time polynomial in the length of Γ. This machine does not depend on F.*

Proof. We first replace the formula F by a quantifier free formula F' according to Theorem 4.1. Let M be the number of atomic predicates of F', and D and L be the degree and the bit-size of the occuring polynomials, respectively. We have

$$\log D \leq \mathcal{O}(n^w \log(m\delta)), \quad \log L \leq \mathcal{O}(n^w \log(m\delta) + \log(p+k+\ell)),$$

and

$$\log M \leq \mathcal{O}(k n^w \log(m\delta)).$$

We replace the generic quantifier in formula (3) according to Remark 4.3(i)(b) and thus write the formula as

$$\forall u \, \forall \epsilon \, \forall a \, \exists a' \left(\epsilon \leq 0 \vee \left(F'(u,a') \wedge \|a - a'\| < \epsilon \right) \Longrightarrow \bigvee_I \bigwedge_{i \in I} F'(u, \boldsymbol{\alpha}_i) \right),$$

where I runs over all $p+1$-element subsets of $[2p+1]$. This formula, let us call it ψ, defines $PW(F)$ and is therefore Zariski-generically true by Lemma 4.8. We may therefore apply Proposition 4.4 to the prenex formula ψ. Note that ψ has $k(2p+1)$ free variables and $2k+p+1$ bounded variables, two quantifier blocks, and polynomials of degree at most D and bit-size at most L. The number of atomic predicates of ψ equals $(2p+2)M+2$. Proposition 4.4 therefore implies that we may compute an integer point in $PW(F)$ by a straight-line program with $\mathcal{O}(kp(k+p)^2 \log(MD) + \log L)$ arithmetic operations. The latter can be bounded by $(kp)^{\mathcal{O}(1)}\, n^w \log(m\delta) + \mathcal{O}(\log \ell)$. This shows part (i). Part (ii) follows from part (ii) in Proposition 4.4. □

Remark 4.10 **(i)** It follows from part (ii) of Theorem 4.9 that the element $\boldsymbol{\alpha}$ in part (i) of this theorem can be computed by a machine over $\mathbb{R}$ or $\mathbb{C}$, upon input (p,k,n,w,m,δ,ℓ), in time order of the length of Γ. Note, however, that this computation may not be possible within these time bounds in the classical setting since the bit-size of the components in $\boldsymbol{\alpha}$ grows exponentially fast.

(ii) We already remarked, over the field $\mathbb{C}$ one can define the stronger notion of *witness sequence*. For this we replace in formula (3) of Definition 4.7 the implication from left to right by an equivalence. The analogue of Lemma 4.8 is then true and therefore witness sequences can be computed by "short" straight-line programs as in Theorem 4.9. This approach was taken in Koiran [44] to devise a method to compute dimensions of algebraic sets in $\mathrm{NP}_{\mathbb{C}}$.

(iii) A different adaptation of the notion of witness sequences to the field of real numbers was introduced in [47] for showing that the problem $\mathrm{DIM}_{\mathbb{R}}$ is $\mathrm{NP}_{\mathbb{R}}$-complete (cf. Theorem 2.6).

5 Complexity of the geometric 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 [33, 56, 65]. 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.[5] The degree of the empty set is defined as 0.

[5]We note here that in algebraic complexity it is common to define the degree of a reducible variety as the sum of the degrees of *all* irreducible components (cf. [17]).

We are going to study the following problem in the computational model of machines over $\mathbb{C}$.

DEGREE (*Geometric degree*) Given a finite set of complex multivariate polynomials, compute the geometric degree of its affine zero set.

Here is the main result of this section.

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 $\#\mathrm{P}_{\mathbb{C}}$. The basic idea of our DEGREE algorithm is very simple. Let $f_1, \ldots, f_r$ be an instance for DEGREE and denote its zero set by Z. We first compute the dimension $d = \dim Z$ by calls to $\mathrm{HN}_{\mathbb{C}}$-oracles using Theorem 2.6. 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. This would yield a randomized algorithm for computing the degree. However, our goal is to choose A deterministically. We will do so using partial witness sequences for parametrized formulas as described in Section 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

$$\forall^* a \in \mathbb{C}^h \quad |Z \cap A_a| = \deg Z. \tag{4}$$

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 (4) in a more concise way. This will be achieved by using the notion of transversality (see Lemma 5.6). However, the translation of the transversality condition into a concise first order formula is a little subtle and will require some further ideas (see Lemma 5.9).

5.1 Smoothness and transversality

An important notion in algebraic geometry is that of a smooth point in a variety. To define smoothness we use Zariski tangent spaces.

Definition 5.3 Let $Z \subseteq \mathbb{C}^n$ be an algebraic set, $x \in Z$, and $f_1, \ldots, f_r$ be generators of the vanishing ideal $\mathcal{I}(Z)$ of Z. The *Zariski tangent space* $T_x Z$ of Z at x is defined by

$$T_x Z = \mathcal{Z}(d_x f_1, \ldots, d_x f_r)$$

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

Remark 5.4 Note that $T_x Z$ is easy to compute from a set of generators of $\mathcal{I}(Z)$, but it may not be so, if instead we only have at hand an arbitrary set of polynomials with zero set Z.

Definition 5.5 Let $Z \subseteq \mathbb{C}^n$ be an algebraic set of dimension d and $A \subseteq \mathbb{C}^n$ be an affine subspace of codimension d.

1. A is called *transversal to Z at $x \in Z \cap A$* iff x is a smooth point of Z and $T_x Z \oplus T_x A = \mathbb{C}^n$.
2. We say that A is *transversal* to Z when A is transversal to Z at all intersection points $x \in Z \cap A$ and if, 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.

In the following, we will 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 $g_1(x) = 0, \ldots, g_d(x) = 0$ with coefficient vector $a \in \mathbb{C}^h$, where $h = d(n+1) = \mathcal{O}(n^2)$. Note that $\dim A_a \geq n - d$ for all a and $\forall^* a \dim A_a = n - d$.

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 $\deg Z$.

Lemma 5.6 *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* $Z \Longrightarrow |Z \cap A_a| = \deg Z\big)$.

Proof. This lemma is proved in Mumford [56, §5A] for irreducible projective varieties Z. It remains to show that it extends to the case where Z is affine and reducible. Let $Z_1, \ldots, Z_t$ be the irreducible components of Z. A dimension argument shows that for a generic a, A_a does neither meet the components Z_i of dimension less than d, nor the intersections $Z_i \cap Z_j$ for $i < j$. Similarly, $\overline{A_a}$ does not meet $\overline{Z_i} - Z_i$ for generic a. Hence (i) follows from the corresponding statement for irreducible projective varieties.

For proving (ii) we assume that A_a is transversal to Z. Then $\mathrm{codim} A_a = d$ and each point $x \in Z \cap A_a$ is a smooth point of Z of local dimension d. Hence there is exactly one irreducible component of Z passing through x and this component has dimension d. We therefore have $|Z \cap A_a| = \sum_{i=1}^{s} |Z_i \cap A_a|$ where $Z_1, \ldots, Z_s$ denote the irreducible components of dimension d. Moreover, A_a is transversal to each of these Z_i, hence $|Z_i \cap A_a| = \deg Z_i$ by [56, §5A, Thm. 5.1]. Altogether, we obtain $|Z \cap A_a| = \sum_{i=1}^s \deg Z_i = \deg Z$ by the definition of the degree of reducible algebraic sets. □

5.2 Expressing smoothness and transversality

Lemma 5.6 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 generated by $f_1, \dots, f_r$ might be different from the radical ideal, and it is not clear how to compute generators of the radical 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.

To do so we will use the notion of intersection multiplicity, so we next recall some facts about it. For more on this, the book by Mumford [56] is an excellent reference fitting well our geometric viewpoint.[6]

Definition 5.7 Assume that $Z \subseteq \mathbb{C}^n$ is an irreducible variety of dimension d and let $A_a \subseteq \mathbb{C}^n$ be an affine subspace of codimension d as above. Suppose that x is an isolated point of $Z \cap A_a$. Then, by [56, Cor. 5.3], there exists a positive integer i satisfying that 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 $a' \in V$

$$A_{a'} \text{ is transversal to } Z \Rightarrow |Z \cap A_{a'} \cap U| = i. \tag{5}$$

We call i the *intersection multiplicity* of Z and A_a at x and we denote this number by $i(Z, A_a; x)$. The *multiplicity* $\mathrm{mult}_x(Z)$ of Z at x is defined as the minimum of $i(Z, A_a; x)$ over all affine linear subspaces A_a of codimension d such that x is an isolated point of $Z \cap A_a$ [56, Def. 5.9]. It is known that x is a smooth point of Z iff $\mathrm{mult}_x(Z) = 1$ [56, Cor. 5.15].

The following lemma is essential for the first order characterization we are seeking.

Lemma 5.8 *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.*

[6] Mumford considers projective varieties, but the following local considerations clearly hold in the affine setting as well.

(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.*

Proof. (a) $\Rightarrow$ (b). Assume that $\varphi_1(x') = 0, \ldots, \varphi_{n-d}(x') = 0$ are local equations of Z at x (i.e., they generate the vanishing ideal of Z in the localization at x). Let $g_1(a, x') = 0, \ldots, g_d(a, x') = 0$ be equations for A_a, parametrized by the coefficient vector $a \in \mathbb{C}^h$. The transversality of Z and A_a at x implies that the Jacobian matrix at x of the polynomial map

$$\mathbb{C}^n \to \mathbb{C}^n, x' \mapsto (\varphi_1(x'), \ldots, \varphi_{n-d}(x'), g_1(a, x'), \ldots, g_d(a, x'))$$

is invertible. The implicit function theorem tells us that there is a continuous map $s\colon V_0 \to U_0$ between Euclidean open neighborhoods V_0 of a and U_0 of x such that for all $a' \in V_0$, $s(a')$ is the unique solution in U_0 of the system of equations

$$\varphi_1(x') = 0, \ldots, \varphi_{n-d}(x') = 0, \; g_1(a, x') = 0, \ldots, g_d(a, x') = 0.$$

For any Euclidean neighborhood $U \subseteq U_0$ of x, the Euclidean neighborhood $V := s^{-1}(U)$ satisfies the statement of condition (b).

(b) $\Rightarrow$ (a). By contraposition, we assume that A_a is not transversal to Z at x and show that condition (b) is not satisfied by considering several cases.

Suppose first that $\dim_x Z < d$. Let U' denote the open neighborhood of x consisting of the set of points in $\mathbb{C}^n$, which do not lie in an irreducible component of Z of dimension d. Then $Z \cap A_{a'} \cap U' = \emptyset$ for Zariski almost all $a' \in \mathbb{C}^h$. If condition (b) were satisfied, there would exist sequences $x_i \to x$ and $a_i \to a$ such that $x_i \in Z \cap A_{a_i}$ and $Z \cap A_{a_i} \cap U' = \emptyset$ for all i. Hence $x_i \notin U'$ for all i, which contradicts the fact that x_i converges to x. Thus (b) is violated.

In the following we assume that $\dim_x Z = d$. We may assume that x is an isolated point of $Z \cap A_a$ since otherwise, (b) is clearly not satisfied. We will distinguish several cases and prove that condition (b) is violated by showing the following claim in each case:

> There are two sequences (x_i) and (x_i') in $\mathbb{C}^n$, both converging to x, and there is a sequence (a_i) in $\mathbb{C}^h$ converging to a such that $x_i, x_i' \in Z \cap A_{a_i}$ and $x_i \neq x_i'$ for all i. (6)

Let Z_1 be an irreducible component of Z passing through x such that $\dim Z_1 = d$. If x is a singular point of Z_1, then $i(Z_1, A_a; x) \geq \mathrm{mult}_x(Z_1) \geq 2$ and claim (6) follows by the characterization (5) of the multiplicity.

We may therefore assume that x is a smooth point of Z_1. If A_a is not transversal to Z_1 at x, then $T_x Z_1 \cap T_x A \neq \emptyset$ and therefore $T_x A$ contains a line ℓ tangent to Z_1 at x. There is a sequence of points $x_i \in Z_1$, $x_i \neq x$, converging to x in the Euclidean topology such that the secant s_i through x and x_i converges to ℓ. Take A_{a_i} to be the affine space of codimension d spanned by $\ell^\perp$ and s_i (here $\ell^\perp$ is the orthogonal complement of ℓ in A_a). Since $A_{a_i} \cap Z \supseteq \{x, x_i\}$, and we can achieve that $a_i \to a$ for a suitable choice of the parameter a_i, the claim (6) follows.

We are left with the case where A_a is transversal to Z_1 at x. Since A_a is not transversal to Z at x, there must be at least one further irreducible component Z_2 of Z passing through x. Consider a sequence of points $x_i \in Z_2 - Z_1$ converging to x and such that $x_i \neq x$. Consider also points $z_1, \ldots, z_{n-d}$ in A_a such that the vectors $z_1 - x, \ldots, z_{n-d} - x$ are linearly independent. Now let A_{a_i} be the affine space of codimension d passing through $x_i, z_1, \ldots, z_{n-d}$. We can achieve that $a_i \to a$.

On the other hand, since A_a is transversal to Z_1 at x, we may apply condition (b) to Z_1 and A_a. Passing over to a subsequence of (A_{a_i}), we obtain that there is a sequence $x_i' \in Z_1 \cap A_{a_i}$ converging to x. This shows the claim (6) and completes the proof of the lemma. □

In the following, we parametrize a system $f_1, \ldots, f_r$ of polynomials over $\mathbb{C}$ of degree at most $\delta \geq 2$ by its vector of non-zero coefficients $u \in \mathbb{C}^q$, and we denote the corresponding zero set by Z_u. (Hence we use the sparse encoding, cf. §2.2.) Recall that we parametrize affine subspaces $A_a \subseteq \mathbb{C}^n$ of codimension d by elements $a \in \mathbb{C}^h$.

Lemma 5.9 *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 $a \in \mathbb{C}^h$:*

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

PROOF. In what follows, we interpret all occuring formulas over $\mathbb{C}$ as first order formulas in $\mathscr{F}_\mathbb{R}$ by encoding a complex number by its real and imaginary part.

Suppose that A_a is of codimension d. Then property (b) in Lemma 5.8 expressing transversality of A_a to Z_u at x can be written as the following formula $\varphi(u, a, x)$:

$$\exists\, \epsilon_0 > 0\ \forall\, 0 < \epsilon < \epsilon_0\ \exists\, \mu > 0\ \forall a' \in \mathbb{C}^h\ \exists y \in \mathbb{C}^n\ \forall\, z \in \mathbb{C}^n\ \Big(\|a - a'\| < \mu \implies \Big(\|y - x\| < \epsilon\ \wedge\ y \in Z_u \cap A_{a'} \wedge\ (\|z - x\| < \epsilon\ \wedge\ z \in Z_u \cap A_{a'} \Rightarrow y = z) \Big)\Big).$$

The property that A_a is transversal to Z_u at all affine intersection points $x \in Z_u \cap A_a$ then reads as:

$$\forall x \in \mathbb{C}^n\ \big(x \in Z_u \cap A_a \Longrightarrow \varphi(u, a, x)\big).$$

The property that Z_u and A_a have no intersection points at infinity is expressed by

$$\forall x \in \mathbb{C}^{n+1} \big(x \in \overline{Z}_u \wedge x \in \overline{A}_a \Longrightarrow x_0 \neq 0\big),$$

where the bar denotes projective closure (we have now an additional homogenizing variable x_0). We express the predicate $x \in \overline{Z}_u$ in the form

$$\forall \epsilon > 0\ \exists x' \in \mathbb{C}^n\ \exists \lambda \in \mathbb{C} - \{0\}\ (x' \in Z_u \wedge \|x - \lambda(1, x')\| < \epsilon),$$

using the fact that the Zariski-closure of constructible sets equals the Euclidean closure.

Finally, we can express that $\mathrm{codim} A_a = d$ by requiring that there exists a linear subspace L with $\dim L \geq d$ and $A_a^{\mathrm{lin}} \cap L = 0$, where A_a^{lin} denotes the linear space associated with A_a.

Altogether, we see that the transversality condition can be expressed by a formula in $\mathcal{F}_{\mathbb{R}}$ of the required description size. □

Remark 5.10 **(i)** 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 $\mathbb{C}$.

(ii) Note that the projective closure $\overline{Z_u}$ is included in but may not be equal to the zero set of the homogenization of the polynomials defining 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, by Theorem 4.9 and Remark 4.10(i), a partial witness sequence $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{2p+1})$ for the formula $F_d(u, a)$ in Lemma 5.9 can be computed by a machine over $\mathbb{C}$, given input $(p, k, n, w, m, \delta, \ell)$, in time $(nq)^{\mathcal{O}(1)} \log \delta$. Note that this quantity is polynomially bounded in the sparse input size $\mathcal{O}(nq \log \delta)$.

We claim the correctness of the following algorithm for DEGREE.

> **input** $f_1, \ldots, f_r$ with coefficient vector u
> compute $d := \dim Z_u$ by oracle calls to $\mathrm{HN}_{\mathbb{C}}$ using Theorem 2.6
> compute a partial witness sequence $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{2p+1})$ of $F_d(u, a)$
> **for** $i = 1$ **to** $2p + 1$
>   compute $N_i := |Z_u \cap A_{\boldsymbol{\alpha}_i}|$ by an oracle call to $\#\mathrm{HN}_{\mathbb{C}}$
> compute the majority N of the numbers $N_1, \ldots, N_{2p+1}$
> **return** N

Put $I := \{i \in [2p + 1] \mid F_d(u, \boldsymbol{\alpha}_i) \text{ holds}\}$. Lemma 5.9 and Part (ii) of Lemma 5.6 imply that $N_i = \deg Z_u$ for all $i \in I$. Part (i) of Lemma 5.6 tells us that $\forall^* a\, F_d(u, a)$. Since $\boldsymbol{\alpha}$ is a partial witness sequence, this implies that $|I| > p$ (cf. Definition (4.7)). This proves the claim.

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

To prove the hardness, note that, by Theorem 3.4, $\#\mathrm{HN}_{\mathbb{C}}$ 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 2.6. 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 semialgebraic sets

It is well known that any compact semialgebraic set S can be triangulated [11, §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 §6.5. 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, [34] 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.

We note that each cell e^n_α has a *characteristic map* $\Phi_\alpha\colon D^n_\alpha \to X$ which extends the attaching map φ_α and is a homeomorphism from the interior of D^n_α onto e^n_α. Namely, we can take Φ_α to be the composition $D^n_\alpha \hookrightarrow X^{n-1} \sqcup_\alpha D^n_\alpha \to X^n \hookrightarrow X$, where the middle map is the quotient map defining X^n.

Example 1 **(i)** 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 $\varphi : S^{n-1} \to e^0$.

(ii) Real projective space $\mathbb{P}^n(\mathbb{R})$ is defined as the space of all lines through the origin in $\mathbb{R}^{n+1}$. This is equivalent to identify antipodal points in $S^n \subset \mathbb{R}^{n+1}$, a presentation which in addition yields a natural topology in $\mathbb{P}^n(\mathbb{R})$ —the quotient topology induced by the identification. Removing the southern hemisphere, this is yet equivalent to the space obtained by keeping the northern hemisphere and identifying antipodal points in the equator. Since the northern hemisphere (without the equator) is homeomorphic to e^n and the equator with identified antipodal points is just $\mathbb{P}^{n-1}(\mathbb{R})$, it follows that $\mathbb{P}^n(\mathbb{R})$ is obtained from the $n+1$ cells $e^0, e^1, \ldots, e^n$ by taking $X_0 = e^0$ and, inductively, obtaining $X_k = \mathbb{P}^k(\mathbb{R})$ from X_{k-1} by attaching e^k via the identification of antipodal points $\varphi_k : \partial D^k \to X^{k-1}$.

(iii) Complex projective space $\mathbb{P}^n(\mathbb{C})$ (already seen in §2.2) is the quotient of the unit sphere $S^{2n+1} \subset \mathbb{C}^{n+1}$ for the equivalence relation $v \equiv \lambda v$ for all $\lambda \in \mathbb{C}$ with $|\lambda| = 1$. A reasoning as the one above (taking into account that equivalence classes are now homeomorphic to S^1) shows that $\mathbb{P}^n(\mathbb{C})$ is obtained from the $n+1$ cells $e^0, e^2, \ldots, e^{2n}$ as above, now getting $X_{2k} = \mathbb{P}^k(\mathbb{C})$, for $k = 0, \ldots, n$.

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 (continued) For the spaces considered above we obtain, using their cell decompositions, that

$$\chi(S^n) = \begin{cases} 2 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases} \qquad \chi(\mathbb{P}^n(\mathbb{R})) = \begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

and $\chi(\mathbb{P}^n(\mathbb{C})) = n+1$.

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., [13, 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.

An example of a covering map with two sheets is the map $p\colon S^n \to \mathbb{P}^n(\mathbb{R})$, which identifies antipodal points. Note that $\chi(S^n) = 2\chi(\mathbb{P}^n(\mathbb{R}))$. This is no coincidence, as the following lemma shows.

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

For cell complexes, a proof of Lemma 6.1 can be found in [13, Prop. 13.5, p. 216]. For the more general case see for instance [66, p. 481].

6.2 Non-compact semialgebraic sets

There are several ways to extend the definition of χ to non-compact sets. The usual one uses singular homology and preserves the property of χ of being 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 *kth Betti number over* F $b_k(X;F)$ of X is defined as the dimension of $H_k(X;F)$. In case $F = \mathbb{Q}$ we write $b_k(X)$ and talk about the kth Betti number of X. The Euler characteristic of the space X is defined by

$$\chi(X) = \sum_{k\in\mathbb{N}} (-1)^k \dim_F H_k(X;F) \tag{7}$$

(if this sum is finite). The Betti numbers $b_k(X;F)$ depend on the field F as well as on X. Remarkably, their alternate sum, is independent of F. In addition, for cell complexes X, this alternate sum coincides with $\chi(X)$ as defined in §6.1. For a general reference to homology we refer to [34, 57].

More generally, one can assign to a pair $Y \subseteq X$ of topological spaces the *relative Euler characteristic* $\chi(X,Y) := \chi(X) - \chi(Y)$. It can also be characterized in terms of the *relative homology vector spaces* $H_k(X,Y;F)$ as $\chi(X,Y) = \sum_{k\in\mathbb{N}}(-1)^k \dim_F H_k(X,Y;F)$. Since $H_k(X,Y;F)$ depends only on the homotopy type of the pair (X,Y), the same holds for the relative Euler characteristic $\chi(X,Y)$. Note that $H_k(X,\emptyset;F) = H_k(X;F)$ and $\chi(X,\emptyset) = \chi(X)$.

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

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

PROOF. A fundamental duality principle going back to Poincaré and extended by Alexander and Lefschetz states that for an n-dimensional manifold Z and a compact subset K carrying the structure of a cell complex, the relative homology space $H_k(Z, Z-K;\mathbb{Z}_2)$ is isomorphic to the homology space[7] $H_{n-k}(K;\mathbb{Z}_2)$ for all k. See [34, Prop. 3.46, p. 256] or [13, Thm. 8.3, p. 351]. The assumptions in the statement allow us to use this result to obtain

$$\begin{aligned} \chi(Z) - \chi(Z-K) &= \chi(Z, Z-K) = \sum_k (-1)^k \dim H_k(Z, Z-K;\mathbb{Z}_2) \\ &= (-1)^n \sum_k (-1)^k \dim H_k(K;\mathbb{Z}_2) = (-1)^n \chi(K). \end{aligned}$$

This implies the claim in the case where n is even. When n is odd, we obtain that $\chi(Z-K) = \chi(K) + \chi(Z)$. On the other hand, applying the above formula for $K = Z$ yields $\chi(Z) = -\chi(Z)$ and thus $\chi(Z) = 0$. Hence $\chi(Z-K) = \chi(K)$. □

[7] Actually, one gets a natural isomorphism with the cohomology vector space $H^{n-k}(K;\mathbb{Z}_2)$ induced by the $\mathbb{Z}_2$-orientation of the manifold Z, but this is not important for our purposes.

6.3 The Euler-Yao characteristic

Let S be 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 a counterexample, consider the closed 3-dimensional unit ball D^3 decomposed into its interior e^3 and its boundary S^2.

Yao [76] defined the *Euler-Yao characteristic* χ^* of semi-algebraic sets, which satisfies an additivity property, and coincides with the usual Euler characteristic for compact semialgebraic sets. The following proposition from [76] 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 $\chi^*(S) = \sum_{i=1}^N \chi^*(S_i)$.*

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

(iii) *If there is a semialgebraic homeomorphism $S \to T$, then $\chi^*(S) = \chi^*(T)$.*

Proof. For the proof of existence, which relies on Hironaka's triangulation theorem [39] for bounded (not necessarily closed) semialgebraic sets, we refer to [76].

The proof of uniqueness shows that, in principle, the computation of χ^* can be reduced to computations of χ for compact semialgebraic sets. Since this is useful for calculating some examples, and to familiarize the reader with the notion of the Euler-Yao characteristic, we present the simple proof of uniqueness.

Any unbounded semialgebraic set $S \subseteq \mathbb{R}^n$ is semialgebraically homeomorphic to a bounded one. Namely, S is homeomorphic to its its image under the inverse of the stereographic projection $S^n - \{(0, \ldots, 0, 1)\} \to \mathbb{R}^n, x \mapsto y$ given by the equations $y_i = x_i/(1 - x_{n+1})$. Therefore, by property (iii), it suffices to show uniqueness for bounded semialgebraic sets S. We proceed by induction on the dimension of S. The case $\dim S \leq 0$ is clear. Consider the disjoint union $\overline{S} = S \cup R$, where $R := \overline{S} - S$. We have $\dim R \leq \dim \partial S < \dim S$ since R is contained in the boundary ∂S of S, cf. [11, Prop. 2.8.12]. Since $\overline{S}$ is compact we have $\chi^*(\overline{S}) = \chi(\overline{S})$ by property (ii). Property (i) implies that $\chi^*(S) = \chi(\overline{S}) - \chi^*(R)$, hence $\chi^*(S)$ is determined by $\chi^*(R)$, which in turn is uniquely determined by the induction hypothesis. □

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.

Corollary 6.4 *If $S_1, \ldots, S_N$ are semialgebraic subsets of $\mathbb{R}^n$, then we have*

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

where the summation is over all nonempty subsets I of $[N]$.

PROOF. This follows from the inclusion-exclusion principle taking into account that χ^* behaves additively with respect to disjoint unions. □

6.4 Locally closed spaces and Borel-Moore homology

A noncompact locally closed set S can be compactified by adding just one point. More specifically, there is a compact semi-algebraic set $\dot{S}$ and a continuous semi-algebraic map $\iota\colon S \to \dot{S}$, which is a homeomorphism onto its image, such that $\dot{S} - \iota(S)$ consists of just one point ∞, cf. [11, 2.5.9].

Let S be a locally closed semialgebraic set and F be a field. If S is not compact, then the *Borel-Moore homology vector spaces* of S over F are defined as the relative homology spaces of the pair $(\dot{S}, \infty)$, that is, $H_k^{\mathrm{BM}}(S; F) := H_k(\dot{S}, \infty; F)$, cf. [11, §11.4]. If S is compact, then we define $H_k^{\mathrm{BM}}(S; F) = H_k(S, F)$. Moreover, we define the kth *Borel-Moore Betti number* of S, denoted $b_k^{\mathrm{BM}}(S)$, as the dimension of $H_k^{\mathrm{BM}}(S; \mathbb{Q})$. Thus we have $b_k^{\mathrm{BM}}(S) = b_k(S)$ for compact S.

From the above, the following well-known characterization easily follows.

Proposition 6.5 *Let S be a locally closed semialgebraic set. Then*

$$\chi^*(S) = \sum_{k\in\mathbb{N}} (-1)^k b_k^{\mathrm{BM}}(S).$$

PROOF. If S is compact the result is trivial. Otherwise, we have $\chi^*(S) = \chi^*(\dot{S}) - \chi^*(\infty) = \chi(\dot{S}) - \chi(\infty) = \chi(\dot{S}, \infty)$. On the other hand

$$\chi(\dot{S}, \infty) = \sum_{k\in\mathbb{N}} (-1)^k \dim H_k(\dot{S}, \infty; \mathbb{Q}) = \sum_{k\in\mathbb{N}} (-1)^k \dim H_k^{\mathrm{BM}}(S; \mathbb{Q}),$$

which shows the assertion. □

Remark 6.6 **(i)** $\chi^*(S)$ can also be interpreted as the Euler characteristic of S with respect to the cohomology $H_c^*(S; \mathbb{Q})$ of S with compact supports, a notion naturally occuring in the Poincaré duality theorem for noncompact manifolds, cf. [34, §3.3, p. 242].

(ii) It is an important fact that for a complex algebraic variety W we have $\chi^*(W) = \chi(W)$. If W is smooth of complex dimension n, then this follows from the Poincaré duality $H_k(W) \simeq H_c^{2n-k}(W)$, using the interpretation of $\chi^*(W)$ as the Euler characteristic of the cohomology $H_c^*(W)$ with compact support. For the proof of the general case see [28, Exercise §4.5, p. 95 and Notes §4.13, p. 141].

(iii) Note that the Euler-Yao characteristic is defined for any semialgebraic set. It is thus a more general notion than the Euler characteristic in the sense of Borel-Moore, which is only defined for locally closed sets.

6.5 Morse Theory

We recall now some notions and facts from Morse theory. A general reference for this is [53].

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 if 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 if its Hessian is nondegenerate at x. The function φ is called a *Morse function* if all its critical points are nondegenerate.

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 $H_x\varphi$. Throughout the paper, we will use the convenient notation $\{\varphi \le r\} := \{x \in Z \mid \varphi(x) \le r\}$.

The main theorem of Morse theory [53, Thm. 3.5] states the following.

Theorem 6.7 *Assume that $\varphi\colon Z \to \mathbb{R}$ is a Morse function on a differentiable manifold Z with finitely many critical points. Moreover, assume that $\{\varphi \le r\}$ is compact for all $r \in \mathbb{R}$. Then Z has the homotopy type of a cell complex with one cell of dimension k for each critical point of φ of index k.* □

We will use the following consequence of this result, adapted to the semialgebraic setting.

Corollary 6.8 *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.*

Proof. **(i)** The first claim follows as in [53, §6] by using the semialgebraic Morse-Sard Theorem [11, Thm. 9.5.2].

(ii) It is easy to see that the set of critical points of L_a is semialgebraic. Moreover, critical points are isolated. Since semialgebraic sets have finitely many components, it follows that there are only finitely many critical points. Note that $Z \cap \{x \in \mathbb{R}^n \mid L_a(x) \le r\}$ is compact for all $r \in \mathbb{R}$. Hence we can apply Theorem 6.7 and the claim follows from the definition of χ. □

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

$$\forall x \in \mathbb{R}^n \ (f(x) = 0 \Rightarrow \operatorname{grad} f(x) \neq 0). \tag{8}$$

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

Consider $f \in \mathscr{H}$ and $Z = \mathcal{Z}(f)$. Then $x \in Z$ is a critical point of L_a if and only if $\sum_k \partial_{X_k} f(x)(x_k - a_k) = 0$. Let x be a critical point of L_a such that (w.l.o.g.) $\partial_{X_n} f(x) \neq 0$. By the implicit function theorem, locally around x, Z is the graph of a function $(t_1, \ldots, t_{n-1}) \mapsto y(t_1, \ldots, t_{n-1})$ which defines a local coordinate system around x,

$$(t_1, \ldots, t_{n-1}) \mapsto x(t) := (t_1, \ldots, t_{n-1}, y(t_1, \ldots, t_{n-1})).$$

Lemma 6.9 *The Hessian $(H_{ij}) = (\partial_{t_i}\partial_{t_j} L_a(x(t)))$ of the distance function L_a at x in terms of the local coordinates t_i is given by*

$$\frac{1}{2}(\partial_{X_n} f)^2 H_{ij} =$$
$$(\partial_{X_n} f)^2 \delta_{ij} + (\partial_{X_i} f)(\partial_{X_j} f) + (x_n - a_n)((\partial_{X_i} f)(\partial_{X_j}\partial_{X_n} f) - (\partial_{X_i}\partial_{X_j} f)(\partial_{X_n} f)).$$

Proof. By differentiating $L_a(x) = \sum_k (x_k - a_k)^2$ with respect to t_i we obtain

$$\partial_{t_i} L_a = 2\sum_{k=1}^{n} (x_k - a_k)\, \partial_{t_i} x_k = 2(t_i - a_i + (y - a_n)\partial_{t_i} y).$$

Differentiating again with respect to t_j yields

$$H_{ij} = \partial_{t_i}\partial_{t_j} L_a = 2(\delta_{ij} + (\partial_{t_i} y)(\partial_{t_j} y) + (y - a_n)\, \partial_{t_i}\partial_{t_j} y).$$

From $f(t_1, \ldots, t_{n-1}, y(t_1, \ldots, t_{n-1})) = 0$ we get $\partial_{t_i} y = -\frac{\partial_{X_i} f}{\partial_{X_n} f}$ by differentiating. Differentiating this again with respect to t_j we obtain

$$\partial_{t_i}\partial_{t_j} y = \frac{-(\partial_{t_j}\partial_{X_i} f)(\partial_{X_n} f) + (\partial_{X_i} f)(\partial_{t_j}\partial_{X_n} f)}{(\partial_{X_n} f)^2}.$$

By plugging these expressions for the partial derivatives of y into the above formula for H_{ij} and taking into account that $t_i = x_i$ for $i < n$ we obtain the asserted formula.

□

As in Section 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 $\text{Euler}^*_{\mathbb{R}}$ as the certificate for transversality for the completeness proof of Degree, which was provided in Lemma 5.9.

Lemma 6.10 *There is a first order formula $F(u, a)$ in $\mathscr{F}^0_{\mathbb{R}}$ 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 $a \in \mathbb{R}^n$, the following holds:*

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

PROOF. The fact that $L_a\colon Z_u \to \mathbb{R}$ is a Morse function can be expressed by the following formula

$$\forall x \in \mathbb{R}^n \left(f(x) = 0 \wedge \sum_{k=1}^{n} \partial_{X_k} f(x)(x_k - a_k) = 0 \Longrightarrow \bigvee_{k=1}^{n} \big(\partial_{X_k} f(x) \neq 0 \wedge \det H_x L_a \neq 0 \big) \right)$$

where, we recall, $H_x L_a$ denotes the Hessian of L_a at x. We now replace $H_x L_a$ by the explicit expression for it given in Lemma 6.9, after making the appropriate changes due to the fact that we require the kth partial derivative of f to be nonvanishing at x instead of the nth derivative. The assertion follows now easily by inspecting the above formula. □

7 Complexity of the Euler characteristic

Another main result of this paper proves the completeness in $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$ of the following problem over $\mathbb{R}$.

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

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

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

Theorem 7.1 *The problem* $\mathrm{EULER}_{\mathbb{R}}^{*}$ *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: in Section 7.1 we reduce the basic semialgebraic case to the case of a smooth hypersurface. This case is then treated in Section 7.2 based on Morse theory and the concept of partial witness sequence developed in Section 4.3. Finally, we combine these two ingredients in Section 7.3 to treat the case of arbitrary semialgebraic sets, using the inclusion-exclusion principle, which is possible due to the additivity property of the Euler-Yao characteristic.

7.1 Basic semialgebraic, projective and affine varieties

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* $1 \le i \le r$

$$g_i := X_{n+i}^2 f_i - 1,\ G_i := X_0^{\delta+3} g_i(X_1/X_0, \ldots, X_{n+r}/X_0),\ H := \sum_{i=0}^{r} G_i^2.$$

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

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

PROOF. Note that, for $i = 1, \ldots, r$, $G_i \in \mathbb{R}[X_0, \ldots, X_{n+r}]$ is homogeneous and $g_i \in \mathbb{R}[X_1, \ldots, X_{n+r}]$. Define the affine variety Y_a and the projective variety Y_p by

$$Y_a := \mathcal{Z}(g_0, \ldots, g_r) \subseteq \mathbb{R}^{n+r}, \ Y_p := \mathcal{Z}(G_0, \ldots, G_r) = \mathcal{Z}(H) \subseteq \mathbb{P}^{n+r}(\mathbb{R}).$$

For $\epsilon \in \{-1, 1\}^r$ consider the open subsets $Y_\epsilon := Y_a \cap (\cap_{i=1}^r \{\mathrm{sgn}(X_{n+i}) = \epsilon_i\})$ of Y_a. Clearly, each Y_ϵ is semialgebraically homeomorphic to S. Moreover, Y_a is the disjoint union of the Y_ϵ. Hence

$$2^r \chi^*(S) = \sum_\epsilon \chi^*(Y_\epsilon) = \chi^*(Y_a). \tag{9}$$

Consider the open subset $V := Y_p \cap \{X_0 \neq 0\}$ of Y_p, which is semialgebraically homeomorphic to Y_a. Since we homogenized with exponent $\delta + 3$, which is one higher than the maximum degree $\delta + 2$ of the g_i, we have $Y_p - V = \mathcal{Z}_{\mathbb{P}^{n+r}(\mathbb{R})}(X_0) \simeq \mathbb{P}^{n+r-1}(\mathbb{R})$. By additivity of χ^* we have $\chi(Y_p) = \chi(\mathbb{P}^{n+r-1}(\mathbb{R})) + \chi^*(V)$, hence

$$\chi^*(Y_a) = \chi^*(V) = \begin{cases} \chi(Y_p) & \text{if } n + r \text{ is even,} \\ \chi(Y_p) - 1 & \text{if } n + r \text{ is odd.} \end{cases} \tag{10}$$

Note that 1 is a regular value of H, since $H = (\deg H)^{-1} \sum_i X_i \partial_{X_i} H$ by the homogeneity of H. Hence the "Milnor fibre"

$$\Phi := \{x \in \mathbb{R}^{n+r+1} \mid H(x) = 1\}$$

is a smooth affine hypersurface. Put $U := \{x \in \mathbb{P}^{n+r}(\mathbb{R}) \mid H(x) \neq 0\}$. We claim that the canonical map

$$\pi \colon \Phi \to U, \ (x_0, \ldots, x_{n+r}) \mapsto (x_0 : \cdots : x_{n+r})$$

is a covering map with two sheets. Indeed, $\pi^{-1}(U \cap \{X_i \neq 0\}) = (\Phi \cap \{X_i > 0\}) \cup (\Phi \cap \{X_i < 0\})$, and π induces homeomorphisms from both $\Phi \cap \{X_i > 0\}$ and $\Phi \cap \{X_i < 0\}$ to $U \cap \{X_i \neq 0\}$, respectively.

By Lemma 6.1 we have $\chi(\Phi) = 2\chi(U)$. On the other hand, by Lemma 6.2 and Example 1, we get $\chi(U) = 1 - \chi(Y_p)$ if $n + r$ is even and $\chi(U) = \chi(Y_p)$ if $n + r$ is odd. Altogether, we obtain

$$\chi(Y_p) = \begin{cases} 1 - \frac{1}{2}\chi(\Phi) & \text{if } n + r \text{ is even,} \\ \frac{1}{2}\chi(\Phi) & \text{if } n + r \text{ is odd.} \end{cases} \tag{11}$$

Combining Equations (9), (10), and (11) the assertion follows. □

7.2 The case of a smooth real hypersurface

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 do not consider the Euler-Yao characteristic here.

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

Proof. Let u encode a real polynomial f in n variables, write $Z_u = \mathcal{Z}(f)$ as before, and let $a \in \mathbb{R}^n$. We denote by $\chi_+(u,a)$ the number of $x \in Z_u$ such that x is a critical point of the function $L_a \colon Z_u \to \mathbb{R}$ and the determinant of the Hessian $H_x L_a$ is positive. Similarly, $\chi_-(u,a)$ counts the number of critical points $x \in Z_u$ such that $\det H_x L_a < 0$.

Assume that L_a is a Morse function on Z_u. Let $x \in Z_u$ be a critical point of the function $L_a \colon Z_u \to \mathbb{R}$. Then $\det H_x L_a > 0$ iff L_a is nondegenerate at x and the index of L_a at x is even. Hence, by Corollary 6.8(ii), we have

$$\chi(Z_u) = \chi_+(u,a) - \chi_-(u,a) \text{ if } L_a \text{ is a Morse function on } Z_u. \tag{12}$$

By explicitly expressing the Hessian $H_x L_a$ in terms of the first and second order partial derivatives of f, we see that it can be computed in polynomial time given u, a, x. Moreover, determinants can be by computed in polynomial time. Hence 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 $\#\mathrm{P}_{\mathbb{R}}$.

Lemma 6.10 and Theorem 4.9 imply that a partial witness sequence α for the first order formula $F(u,a)$ certifying that $L_a \colon Z_u \to \mathbb{R}$ is a Morse function can be computed (uniformly) by a division-free straight-line program with $(np)^{\mathcal{O}(1)} \log \delta$ arithmetic operations, using 1 as the only constant.

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

> **input** $f \in \mathscr{H}$ encoded by its coefficient vector u
> compute a partial witness sequence $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{2p+1})$ of $F(u,a)$
> **for** $\ell = 1$ **to** $2p+1$
>   compute $\chi(u, \boldsymbol{\alpha}_\ell) := \chi_+(u, \boldsymbol{\alpha}_\ell) - \chi_-(u, \boldsymbol{\alpha}_\ell)$
> compute the majority $\chi(u)$ of the numbers $\chi(u, \boldsymbol{\alpha}_1), \ldots, \chi(u, \boldsymbol{\alpha}_{2p+1})$
> **return** $\chi(u)$

In order to show that this algorithm actually computes the Euler characteristic of its input, put $\Lambda := \{\ell \in [2p+1] \mid F(u, \boldsymbol{\alpha}_\ell) \text{ holds}\}$. By definition of F we know that $L_{\boldsymbol{\alpha}_\ell}$ is a Morse function on Z_u for all $\ell \in \Lambda$. Hence, by (12), $\chi(Z_u) = \chi(u, \boldsymbol{\alpha}_\ell)$ for all $\ell \in \Lambda$. On the other hand, by Proposition 6.8(i) we have $\forall^* a\, F(u,a)$. Since $\boldsymbol{\alpha}$ is a partial witness sequence, this implies that $|\Lambda| > p$ (cf. Definition (4.7)). Therefore, the algorithm indeed computes the Euler characteristic of Z_u. □

7.3 Arbitrary semialgebraic sets

Proposition 7.4 *The problem* $\text{EULER}^*_{\mathbb{R}}$ *is contained in* $\text{FP}_{\mathbb{R}}^{\#\text{P}_{\mathbb{R}}}$.

PROOF. Consider an instance $S = \cup_{i=1}^t S_i$ of the problem $\text{EULER}^*_{\mathbb{R}}$, where $t \geq 1$ and $S_i = \{x \in \mathbb{R}^n \mid g_i(x) = 0, f_{i1}(x) > 0, \ldots, f_{ir_i}(x) > 0\}$. Emptyness of S can be easily decided in $\text{FP}_{\mathbb{R}}^{\#\text{P}_{\mathbb{R}}}$.

Assume $S \neq \emptyset$. By adding dummy inequalities $1 > 0$, we may assume that $r_i = r$ for all i. Corollary 6.4 tells us that

$$\chi^*(S) = \textstyle\sum_{I \neq \emptyset} (-1)^{|I|-1} \chi^*(S_I), \tag{13}$$

where for $I \subseteq [t]$, the basic semialgebraic set $S_I \subseteq \mathbb{R}^n$ is defined by

$$S_I := \bigcap_{i \in I} S_i = \Big\{ x \in \mathbb{R}^n \mid \sum_{i \in I} g_i(x)^2 = 0,\ f_{ij}(x) > 0 \text{ for } i \in I, j \in [r] \Big\}.$$

We will assume that each S_I is described by exactly rt inequalities, which can be achieved by adding further dummy inequalities

According to Lemma 7.2, we can assign to each nonempty index set $I \subseteq [t]$ a homogeneous polynomial $H_I \in \mathbb{R}[X_0, \ldots, X_{n+rt}]$, such that $\chi^*(S_I)$ can be expressed by the Euler characteristic of the smooth affine hypersurface $\Phi_I := \mathcal{Z}(H_I - 1)$ in $\mathbb{R}^{n+1+rt}$ as follows

$$\chi^*(S_I) = \frac{(-1)^{n+rt}}{2^{rt+1}} (2 - \chi(\Phi_I)). \tag{14}$$

Plugging (14) into (13) and using that $\sum_I (-1)^{|I|} = 0$ we obtain

$$\chi^*(S) = \frac{(-1)^{n+rt}}{2^{rt+1}} \Big(2 + \sum_{I \neq \emptyset} (-1)^{|I|} \chi(\Phi_I) \Big). \tag{15}$$

We proceed now similarly as in the proof of Proposition 7.3. Let p be the number of real parameters of all the polynomials g_i, f_{ij} involved in the above description of the set S. To emphasize the dependence on u, we will write $\Phi_{I,u}$ instead of Φ_I. For a projection point $a \in \mathbb{R}^{n+1+rt}$ and a parameter $u \in \mathbb{R}^p$ we consider the distance function $L_a \colon \Phi_{I,u} \to \mathbb{R}, x \mapsto \|x - a\|^2$.

Similarly as in the proof of Proposition 7.3, we assign to $u \in \mathbb{R}^p, a \in \mathbb{R}^{n+1+rt}$, and $I \subseteq [t]$ two values $\chi_{+,I}(u,a), \chi_{-,I}(u,a) \in \mathbb{N}$ such that (cf. (12))

$$\chi(\Phi_{I,u}) = \chi_{+,I}(u,a) - \chi_{-,I}(u,a) \text{ if } L_a \text{ is a Morse function on } \Phi_{I,u}. \tag{16}$$

Namely, $\chi_{+,I}(u,a)$ is defined as the number of critical points $x \in \mathbb{R}^{n+1+rt}$ of the function $L_a \colon \Phi_{I,u} \to \mathbb{R}$ such that $\det H_x L_a > 0$. Similarly, one defines $\chi_{-,I}(u,a)$ by requiring a negative sign. As in the proof of Proposition 7.3, one shows that the functions $\{0,1\}^\infty \times \mathbb{R}^\infty \times \mathbb{R}^\infty \to \mathbb{N} \cup \{\infty\}$ mapping (I,u,a) to $\chi_{+,I}(u,a)$ and $\chi_{-,I}(u,a)$, respectively, are in $\#\text{P}_{\mathbb{R}}$.

Assume now that u, a are chosen such that L_a is a Morse function on $\Phi_{I,u}$ for all nonempty subsets I of $[t]$. Plugging (16) into (15) we obtain

$$
\begin{aligned}
(-1)^{n+rt}\, 2^{rt+1}\, \chi^*(S) &= 2 + \sum_{I\neq\emptyset} (-1)^{|I|} \big(\chi_{+,I}(u,a) - \chi_{-,I}(u,a)\big) \\
&= 2 + \chi_+(u,a) - \chi_-(u,a),
\end{aligned}
$$

where we have put

$$
\chi_+(u,a) := \sum_{I\neq\emptyset, |I| \text{ even}} \chi_{+,I}(u,a), \quad \chi_-(u,a) := \sum_{I\neq\emptyset, |I| \text{ odd}} \chi_{-,I}(u,a).
$$

According to Lemma 3.9, the functions $(u,a) \mapsto \chi_+(u,a)$ and $(u,a) \mapsto \chi_-(u,a)$ are in $\#\mathrm{P}_{\mathbb{R}}$.

Consider the first order formula $G_I(u,a)$ in $\mathscr{F}^0_{\mathbb{R}}$ provided by Lemma 6.10, which expresses the fact that $L_a \colon \Phi_{I,u} \to \mathbb{R}$ is a Morse function. Define the first order formula $G(u,a) := \wedge_{I\neq\emptyset} G_I(u,a)$, which certifies that, for all nonempty index sets $I \subseteq [t]$, $L_a \colon \Phi_{I,u} \to \mathbb{R}$ is a Morse function. Theorem 4.9 and Remark 4.10 imply that a partial witness sequence $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{2p+1})$ for the formula $G(u,a)$ can be computed in time polynomial in the input size of S. (Note that it does not harm that the number of atomic predicates of $G(u,a)$ is exponential in the input size of S.)

After all these preparations, we see that the Euler-Yao characteristic of S can be computed by essentially the same algorithm as in the proof of Proposition 7.3. The modifications are as follows: replace the formula F by G, reinterpret the quantities $\chi_+(u,a), \chi_-(u,a)$ in the above way, and return $(-1)^{n+rt} 2^{-rt-1}(2 + \chi(u))$ where, again, $\chi(u)$ is obtained by taking a majority vote on the $\chi_+(u,\boldsymbol{\alpha}_i) - \chi_-(u,\boldsymbol{\alpha}_i)$. This algorithm can be implemented as a polynomial time oracle Turing machine accessing oracles in $\#\mathrm{P}_{\mathbb{R}}$. The proof of correctness is identical as for the proof of Proposition 7.3. □

Proof of Theorem 7.1. The membership of $\mathrm{EULER}^*_{\mathbb{R}}$ to $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$ is the content of Proposition 7.4. By Theorem 3.4, $\#\mathrm{FEAS}_{\mathbb{R}}$ is $\#\mathrm{P}_{\mathbb{R}}$-complete. To prove the Turing-hardness of $\mathrm{EULER}^*_{\mathbb{R}}$ for $\#\mathrm{P}_{\mathbb{R}}$, it is therefore sufficient to Turing reduce $\#\mathrm{FEAS}_{\mathbb{R}}$ to $\mathrm{EULER}^*_{\mathbb{R}}$. The following reduction does so. For a given real polynomial first decide whether its solution set Z is zero-dimensional by a call to $\mathrm{FEAS}_{\mathbb{R}}$ using Theorem 2.6. This call to $\mathrm{FEAS}_{\mathbb{R}}$ can be replaced by a call to $\mathrm{EULER}^*_{\mathbb{R}}$ since $\mathrm{FEAS}_{\mathbb{R}}$ reduces to $\mathrm{EULER}^*_{\mathbb{R}}$ (this follows from the case distinction in the definition of the problem $\mathrm{EULER}^*_{\mathbb{R}}$). If $\dim Z = 0$, then compute $N := \chi^*(Z)$ by a call to $\mathrm{EULER}^*_{\mathbb{R}}$ and return N, otherwise return ∞. □

Remark 7.5 In the papers [14, 69], 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 [26]. Although Morse theory is not explicitly mentioned in [14, 69], the main idea behind these papers is an application of this theory as exposed in [55]. The single exponential time algorithm in [4] for computing the Euler characteristic uses Morse theory explicitly and in a crucial way. However, we note that the reduction in [4] from the case of an arbitrary semialgebraic set to the case of a smooth hypersurface, as well as the reductions in [14, 69], 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, we have expressed 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 Completeness results in the Turing model

It is common to restrict the input polynomials in the problems considered so far to polynomials with integer coefficients. The resulting problems can be encoded in a finite alphabet and studied in the classical Turing setting. In general, if L denotes a problem defined over $\mathbb{R}$ or $\mathbb{C}$, 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.

We are going to show next that all the above problems are (Turing-) complete in certain discrete complexity classes. These classes are obtained from real or complex complexity classes by the operation of taking the Boolean part.

8.1 Basic complete problems in Boolean parts

A problem that has attracted much attention in real (or complex) complexity is the computation of Boolean parts [16, 23, 24, 25, 41, 45]. Roughly speaking, this 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.

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

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

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 [18, 25, 41]. In contrast, much less is known in the setting of unrestricted machines. Two of the most significant results state that $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}) \subseteq \mathsf{P}^{\mathsf{RP}}$ [24] and $\mathrm{BP}(\mathrm{PAR}_{\mathbb{R}}) = \mathsf{PSPACE}/_{\mathsf{poly}}$ [23], and a third one is discussed in Proposition 8.3 below. For stating it, we briefly recall the *Arthur-Merlin class* AM [1], which can be seen as a natural and robust randomized extension of NP.

Let $p_1(n), p_2(n)$ be polynomials and R be a polynomial time decidable predicate such that, for all n and all $x \in \{0,1\}^n$, the probability

$$\pi(x) := \mathrm{Prob}\{r \in \{0,1\}^{p_1(n)} \mid \exists y \in \{0,1\}^{p_2(n)}\ R(x,r,y)\}$$

satisfies either $\pi(x) \geq 2/3$ or $\pi(x) \leq 1/3$. Let the language L consist of all x such that $\pi(x) \geq 2/3$. Then L is in AM, and all languages in AM can be characterized this way.

The Arthur-Merlin class AM satisfies $\mathsf{NP} \subseteq \mathsf{AM} \subseteq \Pi_2$, where Π_2 denotes a class in the second level of the polynomial hierarchy. Moreover, the nonuniform versions of AM and NP coincide, i.e., $\mathsf{AM}/\mathsf{poly} = \mathsf{NP}/\mathsf{poly}$. A prominent problem in AM, which is not known to be in NP, is the graph non-isomorphism problem. (Proofs of the above claims can be found in [1].)

The following upper bound for $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ was obtained by Koiran [42].

Theorem 8.2 *The problem* $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ *belongs to* AM *under the generalized Riemann hypothesis GRH.* □

A natural restriction for real or complex machines (considered e.g. in [25, 41, 45]) 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 indicated by a superscript 0 as in $\mathrm{P}_{\mathbb{R}}^0$, $\mathrm{NP}_{\mathbb{R}}^0$, etc.

Theorem 8.2 provides an upper bound for $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$. On the other hand, the clear NP-hardness of $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ provides a lower bound. Yet there is a gap between NP and AM and the problem of how to close it (with regard to $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$) is, as of today, an open question. A disturbing —but not for that more unlikely— possibility is that $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ is not complete in any of the two classes above but in some intermediate class. The following result elaborates on that question.

Proposition 8.3 **(i)** $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ *and* $\mathrm{DIM}_{\mathbb{C}}^{\mathbb{Z}}$ *are* $\mathrm{BP}(\mathrm{NP}_{\mathbb{C}}^0)$*-complete.*

(ii) *Assuming GRH, we have* $\mathsf{NP} \subseteq \mathrm{BP}(\mathrm{NP}_{\mathbb{C}}^0) \subseteq \mathsf{AM}$.

Proof. The completeness of $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ in part (i) follows from the following fact. The $\mathrm{FP}_{\mathbb{C}}$-reduction from an arbitrary $\mathrm{NP}_{\mathbb{C}}$-problem to $\mathrm{HN}_{\mathbb{C}}$ exhibited in [9], when applied to a problem L in $\mathrm{NP}_{\mathbb{C}}^0$, yields a FP-reduction from $L^{\mathbb{Z}}$ to $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$. This shows that $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ is $\mathrm{BP}(\mathrm{NP}_{\mathbb{C}}^0)$-complete. The completeness of $\mathrm{DIM}_{\mathbb{C}}^{\mathbb{Z}}$ follows from Theorem 2.6(i).

For the reasoning above to hold it is essential that we only consider problems defined by $\mathrm{NP}_{\mathbb{C}}$-machines that do not use complex constants. Otherwise, these constants would appear as coefficients in the constructed polynomial system.

The second inclusion in part (ii) follows from part (i) and Theorem 8.2. The first inclusion is trivial. □

The rest of this section is devoted to completeness results in Boolean parts in the spirit of Proposition 8.3. Before stating our result, we 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.

Definition 8.4 The class GCC of *geometric counting complex problems* and the class GCR of *geometric counting real problems* are defined as follows:

$$\mathsf{GCC} := \mathrm{BP}(\#\mathrm{P}^0_{\mathbb{C}}), \quad \mathsf{GCR} := \mathrm{BP}(\#\mathrm{P}^0_{\mathbb{R}}).$$

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

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

where the rightmost inclusion follows from Theorem 3.7 and [23].

Proposition 8.5 **(i)** $\mathrm{FEAS}^{\mathbb{Z}}_{\mathbb{R}}$, $\mathrm{SAS}^{\mathbb{Z}}_{\mathbb{R}}$, *and* $\mathrm{DIM}^{\mathbb{Z}}_{\mathbb{R}}$ *are* $\mathrm{BP}(\mathrm{NP}^0_{\mathbb{R}})$*-complete.*

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

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

PROOF. For the hardness in part (i) we use the argument in the proof of Proposition 8.3(i), namely, that the reductions from an arbitrary $\mathrm{NP}_{\mathbb{R}}$-problem to $\mathrm{FEAS}_{\mathbb{R}}$ or $\mathrm{SAS}_{\mathbb{R}}$ yield reductions from problems in $\mathrm{BP}(\mathrm{NP}^0_{\mathbb{R}})$ to $\mathrm{FEAS}^{\mathbb{Z}}_{\mathbb{R}}$ or $\mathrm{SAS}^{\mathbb{Z}}_{\mathbb{R}}$, respectively. For the hardness in parts (ii) and (iii) one uses the reductions in the proof of Theorem 3.4. The memberships in all statements are clear except for $\mathrm{DIM}^{\mathbb{Z}}_{\mathbb{R}}$, for which the claim follows from Theorem 2.6(ii). □

Remark 8.6 One can show that $\mathrm{BP}(\mathrm{NP}^0_{\mathbb{C}}) = \mathrm{BP}(\mathrm{NP}_{\mathbb{C}})$ and $\mathsf{GCC} = \mathrm{BP}(\#\mathrm{P}^0_{\mathbb{C}}) = \mathrm{BP}(\#\mathrm{P}_{\mathbb{C}})$. Hence it is immaterial whether we allow the use of complex machine constants in the definition of these classes or not.

We can give some evidence that counting over $\mathbb{C}$ is indeed harder than deciding feasibility over $\mathbb{C}$.

Corollary 8.7 *If* $\#\mathrm{P}_{\mathbb{C}} \subseteq \mathrm{FP}^{\mathrm{NP}_{\mathbb{C}}}_{\mathbb{C}}$*, then the classical polynomial hierarchy collapses at the fourth level, assuming GRH.*

PROOF. (Sketch) Recall that BPP denotes the classical complexity class of problems decidable by randomized machines in polynomial time. Its subclass RP is obtained by requiring one-sided error (if the instance is not in the language then the machine always answers correctly). The class coRP denotes the complement of RP.

We have $\mathsf{coRP} \subseteq \mathsf{BPP}$. The well-known proof of $\mathsf{BPP} \subseteq \Sigma_2 \cap \Pi_2$ (cf. [60, p. 429]) easily extends to show that $\mathsf{BPP}^{\mathsf{NP}} \subseteq \Sigma_3 \cap \Pi_3$.

Extending Proposition 8.3(ii), one can prove that $\mathrm{BP}(\mathrm{FP}_{\mathbb{C}}^{\mathrm{NP}_{\mathbb{C}}}) \subseteq (\mathsf{coRP})^{\mathsf{NP}}$, assuming GRH. The proof relies on the possibility to eliminate complex constants using witness sequences, as developed in [8, 43, 46], and combines this with the proof of Theorem 8.2 from [42]. (Note that there is a typo in [42] confusing RP and coRP.) Details are omitted for lack of space.

Assuming $\#\mathrm{P}_{\mathbb{C}} \subseteq \mathrm{FP}_{\mathbb{C}}^{\mathrm{NP}_{\mathbb{C}}}$ and taking Boolean parts, we thus obtain

$$\#\mathsf{P} \subseteq \mathrm{BP}(\#\mathrm{P}_{\mathbb{C}}) \subseteq \mathrm{BP}(\mathrm{FP}_{\mathbb{C}}^{\mathrm{NP}_{\mathbb{C}}}) \subseteq (\mathsf{coRP})^{\mathsf{NP}} \subseteq (\mathsf{BPP})^{\mathsf{NP}} \subseteq \Sigma_3.$$

Toda's theorem [71] states that $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$. Hence we conclude from the above that

$$\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{P}^{\Sigma_3} = \Delta_4$$

which means that the polynomial hierachy collapses at the fourth level. □

8.2 Degree and Euler characteristic in the Turing model

We can now easily deduce completeness results for the discrete versions of the problems to compute the degree or the Euler-Yao characteristic.

Theorem 8.8 **(i)** $\textsc{Degree}^{\mathbb{Z}}$ *is* $\mathsf{FP}^{\mathsf{GCC}}$*-complete with respect to Turing reductions.*

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

Proof. (i) The proof given in Section 5 for the membership of $\textsc{Degree}^{\mathbb{Z}}$ to $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$ applies in our case with only one modification. The algorithm in the proof of Theorem 5.2 computes the partial witness sequence $\boldsymbol{\alpha}$ (this is done in $\mathrm{FP}_{\mathbb{C}}$) and then performs $2p+1$ oracle calls to $\#\mathrm{P}_{\mathbb{C}}$ to obtain the numbers N_i for $i \in [2p+1]$. While it is clear that the computation of $\boldsymbol{\alpha}$ is in $\mathrm{BP}(\mathrm{FP}_{\mathbb{C}})$, it is equally clear that it is not in FP due to the exponential coefficient growth caused by repeated powering (cf. Lemma 4.5). A way to solve this is to "move" the computation of $\boldsymbol{\alpha}$ 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 $\boldsymbol{\alpha}$ 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 2.6(i) instead of the first.

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

Remark 8.9 **(i)** The algorithms for $\textsc{Degree}^{\mathbb{Z}}$ and $\textsc{Euler}_{\mathbb{R}}^{*\mathbb{Z}}$ above can be further simplified. Since we can bound the description size of the formula $F(u, a)$ or $G(u, a)$ by taking into account a bound on the bit-size of the components of the given $u \in \mathbb{Z}^p$, the input vector u does not need to be considered as a parameter any more. Therefore, we may take $p = 0$. The partial witness sequence then consists of a single vector $\alpha \in \mathbb{Z}^k$ and only one oracle call to $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ (or two oracle calls to $\#\mathrm{FEAS}_{\mathbb{R}}^{\mathbb{Z}}$) are needed.

(ii) Alternatively, the algorithm in the proof of Theorem 5.2 (or Theorem 7.1) could be modified as follows. By part (i) we may assume that $p = 0$. The straight-line computation for the partial witness $\alpha \in \mathbb{Z}^k$ of F cannot be executed in the bit model because of the exponential coefficient growth. However, we can easily remedy this by describing the construction of the partial witness sequence by existentially quantifying over additional variables $\beta_1, \dots, \beta_q$ along the recursive description in Lemma 4.5. We then query $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ for the system of equations in the variables x, α_i and $\beta_1, \dots, \beta_q$ expressing the recursive construction of α_i and the fact that $x \in Z_u \cap L_\alpha$.

In the Turing model we can also prove a completeness result for the computation of the (usual) Euler characteristic: consider the problem

$\mathrm{EULER}_{\mathbb{R}}$ (*Euler characteristic for basic semialgebraic sets*) Given a basic semialgebraic set $S = \{x \in \mathbb{R}^n \mid g(x) = 0, f_1(x) > 0, \dots, f_r(x) > 0\}$, decide whether S is empty and if not, compute $\chi(S)$.

Theorem 8.10 $\mathrm{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ *is* $\mathsf{FP}^{\mathsf{GCR}}$*-complete with respect to Turing reductions.*

To prepare for the proof, recall that a closed semialgebraic set $S \subseteq \mathbb{R}^n$ has a conic structure at infinity [6, Prop. 5.50], which implies that there exists $r > 0$ such that for all $r' \geq r$ there is a semialgebraic deformation retraction from S to $S_{r'} := S \cap \{x \in \mathbb{R}^n \mid \|x\| \leq r'\}$. We will call r a *cone radius of S at infinity.* Clearly, we have $\chi(S) = \chi(S_r) = \chi^*(S_r)$.

Lemma 8.11 *Let $p \in \mathbb{Z}[X_1, \dots, X_n]$ be of degree at most δ with coefficients of bit-size at most ℓ. Then, there exists $m = (n\delta\ell)^{\mathcal{O}(1)}$ such that 2^{2^m} is a cone radius of $\mathcal{Z}(p)$ at infinity.*

Proof. (Sketch) In [29] it is shown that there is a first order formula $\Phi(r)$ in $\mathscr{F}_{\mathbb{R}}^0$ in prenex form with the free variable r such that there exists $r_0 > 0$ with

$$[r_0, \infty[\subseteq \{r \in \mathbb{R} \mid \Phi(r) \text{ true}\} \subseteq \{r \in \mathbb{R} \mid r \text{ is a cone radius of } \mathcal{Z}(f) \text{ at infinity}\}.$$

By an inspection of the constructions in [29, 61] one can show that the formula $\Phi(r)$ has a bounded number of quantifier blocks, $n^{\mathcal{O}(1)}$ bounded variables, and m atomic predicates given by integer polynomials of degree at most d and bit-size at most ℓ' such that $\log(dm\ell') \leq (n\delta\ell)^{\mathcal{O}(1)}$. The tedious details of verifying this statement about the desription size of $\Phi(r)$ are omitted for lack of space and left to the reader.

According to Theorem 4.1, the formula $\neg\Phi(r)$ is equivalent to a quantifier-free formula in disjunctive normal form $\vee_{i=1}^{I} \wedge_{j=1}^{J_i} (h_{ij}(r)\Delta_{ij}0)$, containing integer polynomials $h_{ij}(r)$ of bit-size at most L such that $\log L \leq (n\delta\ell)^{\mathcal{O}(1)}$.

Let $\rho \in \mathbb{R}$ be the maximum of the real roots of the nonzero h_{ij}. We have $\rho \leq 1+\|h\|_\infty \leq 1+2^L$. Note that the sign of $h_{ij}(x)$ is constant for $x > \rho$. Therefore, since the set $\{r > 0 \mid \neg\Phi(r)\}$ is bounded, we have $\{r > 0 \mid \neg\Phi(r)\} \subseteq]0, \rho]$. Hence $2 + 2^L$ is a cone radius of $\mathcal{Z}(f)$ at infinity, which proves the claim. □

Proof of Theorem 8.10. The hardness of $\text{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ follows as in the proof of Theorem 7.1. We prove now that $\text{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ belongs to $\mathsf{FP}^{\mathsf{GCR}}$. For given $S = \{x \in \mathbb{R}^n \mid g(x) = 0, f_1(x) > 0, \dots, f_r(x) > 0\}$, compute the polynomial

$$p(X,Y) := g(X)^2 + \sum_{i=1}^{r} (Y_i^2 f_i(X) - 1)^2$$

in the variables $X_1, \dots, X_n, Y_1, \dots, Y_r$. As in the proof of Lemma 7.2 we see that $\chi(S) = 2^{-r}\chi(\mathcal{Z}(p))$. Let $\rho = 2^{2^m}$ be a cone radius of $\mathcal{Z}(p)$ at infinity as in Lemma 8.11. Note that m is polynomially bounded in the input size of S (given by the sparse bit size of the family of polynomials describing S). Consider the semialgebraic set $T \subseteq \mathbb{R}^{n+r+m+1}$ defined by

$$p(x,y) = 0, z_0 = 2, z_1 - z_0^2 = 0, \dots, z_m - z_{m-1}^2 = 0, \|x\|^2 + \|y\|^2 \leq z_m^2.$$

Clearly, T is homeomorphic to $\mathcal{Z}(p)_\rho = \mathcal{Z}(p) \cap \{\|x\|^2 + \|y\|^2 \leq \rho^2\}$. Therefore, since ρ is a cone radius, we have $\chi(\mathcal{Z}(p)) = \chi(\mathcal{Z}(p)_\rho) = \chi^*(\mathcal{Z}(T))$. By Theorem 7.1 we can compute $\chi^*(\mathcal{Z}(T))$ in $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$. This implies that $\chi(S)$ may be computed within the same resources. □

Remark 8.12 Theorem 8.10 easily extends to the case where we also allow inequalities $h(x) \geq 0$ in the definition of the basic semialgebraic set. For instance, for $S = \{x \in \mathbb{R}^n \mid p(x) = 0, h(x) \geq 0\}$ consider

$$Z := \{(x,y) \in \mathbb{R}^{n+1} \mid p(x) = 0, h(x) - y^2 = 0\}.$$

The sets $Z_+ := Z \cap \{y \geq 0\}$ and $Z_- := Z \cap \{y \leq 0\}$ are closed semialgebraic sets both homeomorphic to S and $Z = Z_+ \cup Z_-$. The formula $\chi(Z_+ \cup Z_-) + \chi(Z_+ \cap Z_-) = \chi(Z_+) + \chi(Z_-)$ then allows to compute $\chi(S)$ from the Euler characteristic of real algebraic varieties.

8.3 Connected components and Betti numbers

We are going to study here the following problems:

$\#\mathrm{CC}_{\mathbb{R}}$ (*Counting connected components*) Given a semialgebraic set S, compute the number of its connected components.

$\mathrm{BETTI}(k)_{\mathbb{R}}$ (kth *Betti number of a real algebraic set*) Given a real multivariate polynomial, compute the kth Betti number of its real zero set.

$\mathrm{BM\text{-}BETTI}(k)_{\mathbb{R}}$ (kth *Borel-Moore Betti number of a real algebraic set*) Given a real multivariate polynomial, compute the kth Borel-Moore Betti number of its real zero set.

For the problems related to Betti numbers, we restrict the input to be a real algebraic set. Since we will only prove lower bounds for these problems, this restriction makes our results stronger. Note that $\mathrm{BETTI}(0)_{\mathbb{R}}$ is just the restriction of $\#\mathrm{CC}_{\mathbb{R}}$ to real algebraic sets.

We will focus here on the discretized versions of the above problems, where the input polynomials have integer coefficients, and study these problems in the Turing model.

The following upper bound was first shown by Canny [21].

Theorem 8.13 *The problem* $\#\mathrm{CC}_{\mathbb{R}}^{\mathbb{Z}}$ *is in* FPSPACE.

From a result by Reif [62, 63] on the PSPACE-hardness of a generalized movers problem in robotics, it follows easily that the problem $\#\mathrm{CC}_{\mathbb{R}}^{\mathbb{Z}}$ is in fact FPSPACE-complete. We will give an alternative proof of the FPSPACE-hardness of this problem following the lines of [18]. This will also allow us to sharpen the lower bound by showing that $\#\mathrm{CC}_{\mathbb{R}}^{\mathbb{Z}}$ remains FPSPACE-hard when restricted to compact real algebraic sets. Based on this, we will prove the FPSPACE-hardness of the problems $\mathrm{BETTI}(k)_{\mathbb{R}}$ and $\mathrm{BM\text{-}BETTI}(k)_{\mathbb{R}}$.

The following lemma follows by inspecting the usual $\mathrm{NP}_{\mathbb{R}}$-completeness proof of $\mathrm{FEAS}_{\mathbb{R}}$ [10], see also [22].

Lemma 8.14 *For $A \in \mathrm{P}_{\mathbb{R}}^{0}$ there is a polynomial p and a polynomial time, division-free Turing machine computing on input $n \in \mathbb{N}$ a quantifier free first order formula $\Phi_n \in \mathscr{F}_{\mathbb{R}}^{0}$ in the free variables $x_1, \dots, x_{p(n)}$ such that the projection*

$$\{x \in \mathbb{R}^{p(n)} \mid \Phi_n(x) \text{ holds } \} \longrightarrow A \cap \mathbb{R}^n,\ (x_1, \dots, x_{p(n)}) \mapsto (x_1, \dots, x_n)$$

is a homeomorphism. The machine can be chosen such that the inverse image of an integer point $x \in A \cap \mathbb{Z}^n$ is again integer and can be computed in polynomial time.

Lemma 8.15 *There is a polynomial time Turing machine computing from a quantifier free formula $\Phi \in \mathscr{F}_{\mathbb{R}}^{0}$ in the free variables $X_1, \dots, X_m$ a polynomial f_Φ in $\mathbb{Z}[X_1, \dots, X_m, Y_1, \dots, Y_{q(m)}]$ such that the projection $\pi\colon \mathbb{R}^{m+q(m)} \to \mathbb{R}^m, (x, y) \mapsto x$ induces for all $\epsilon \in \{-1, 1\}^{q(m)}$ a homeomorphism*

$$\mathcal{Z}(f_\Phi) \cap \{\epsilon_1 y_1 \geq 0, \dots, \epsilon_{q(m)} y_{q(m)} \geq 0\} \longrightarrow \{x \in \mathbb{R}^m \mid \Phi(x) \text{ holds } \}.$$

Proof. As in the $\mathrm{NP}_{\mathbb{R}}$-completeness proof of $\mathrm{FEAS}_{\mathbb{R}}$ [10] the machine M performs the following (see also [22]). For each atomic formula of Φ containing an inequality choose a new variable Y and replace

$$
\begin{array}{lll}
p(X) \geq 0 & \text{by} & p(X) - Y^2 = 0 \\
p(X) > 0 & \text{by} & p(X)Y^2 - 1 = 0.
\end{array}
$$

In the resulting formula iteratively eliminate the connectives as follows: replace

$$\bigvee_{i=1}^{s} p_i = 0 \text{ by } \prod_{i=1}^{s} p_i = 0, \text{ and } \bigwedge_{i=1}^{t} p_i = 0 \text{ by } \sum_{i=1}^{t} p_i^2 = 0.$$

We end up with a single polynomial equation $f_\Phi = 0$, which is easily seen to satisfy the claim of the lemma. □

Consider the following auxiliary problem:

$\mathrm{REACH}_{\mathbb{R}}$ (*Reachability*) Given real polynomials f, g, h, decide whether there exist points $p \in \mathcal{Z}_{\mathbb{R}^n}(f,g)$ and $q \in \mathcal{Z}_{\mathbb{R}^n}(f,h)$ which lie in the same connected component of $\mathcal{Z}_{\mathbb{R}^n}(f)$.

Proposition 8.16 *The problem* $\mathrm{REACH}_{\mathbb{R}}^{\mathbb{Z}}$ *is* PSPACE*-hard.*

Proof. Assume $L \in \mathsf{PSPACE}$. In the proof of [18, Proposition 5.9] the configuration graph of a symmetric Turing machine deciding membership of $w \in \{0,1\}^n$ to L was embedded in a certain way in Euclidean space as a compact one-dimensional semi-linear set S_n. More specifically, a polynomial time computable function mapping $w \in \{0,1\}^n$ to $(\mathscr{C}_n, u_n(w), v_n)$ was constructed, where $\mathscr{C}_n$ is a constant free additive circuit describing membership to $S_n \subseteq \mathbb{R}^{c(n)}$, c is a polynomial, and $u_n(w), v_n \in \{0,1\}^{c(n)}$ such that $w \in L$ iff $u_n(w)$ and v_n are connected in S_n. Note that, in particular, the set $A := \{(w,x) \in \{0,1\}^n \times \mathbb{R}^{c(n)} \mid n \in \mathbb{N}, x \in S_n\}$ is contained in $\mathrm{P}^0_{\mathrm{add}}$ and hence in $\mathrm{P}^0_{\mathbb{R}}$.

We apply Lemma 8.14 to the set A. Let $\Phi_n \in \mathscr{F}^0_{\mathbb{R}}$ be the formula in the free variables $X_1, \ldots, X_{p(n)}$ corresponding to the input size $n + c(n)$ and let $f_n \in \mathbb{Z}[X_1, \ldots, X_{p(n)}, Y_1, \ldots, Y_{q(n)}]$ be the integer polynomial corresponding to Φ_n according to Lemma 8.15. We know that f_n can be computed from n in polynomial time. For $w \in \{0,1\}^n$ let $\mu_w, \nu_w \in \mathbb{Z}^{p(n)}$ be the inverse images of $(w, u_n(w)), (w, v_n)$, respectively, under the projection homeomorphism

$$T_n := \{x \in \mathbb{R}^{p(n)} \mid \Phi_n(x) \text{ holds }\} \longrightarrow A \cap \mathbb{R}^{n+c(n)}, (x_1, \ldots, x_{p(n)}) \mapsto (x_1, \ldots, x_{n+c(n)}).$$

Note that μ_w and ν_w are connected in T_n iff $u_n(w)$ and v_n are connected in S_n, which is the case iff $w \in L$.

According to Lemma 8.15, for any $\epsilon \in \{-1,1\}^{q(n)}$, the projection $(x,y) \mapsto x$ induces a homeomorphism

$$\mathcal{Z}(f_n) \cap \{\epsilon_1 y_1 \geq 0, \ldots, \epsilon_{q(n)} y_{q(n)} \geq 0\} \longrightarrow T_n.$$

This implies that there exist points $(\mu_w, \eta), (\nu_w, \eta') \in \mathcal{Z}(f_n)$ that are connected in $\mathcal{Z}(f_n)$ iff μ_w and ν_w are connected in T_n. Define the integer polynomials $g_w := f_n(\mu_w, Y), h_w := f_n(\nu_w, Y)$. Then $w \in L$ iff the instance f_n, g_w, h_w of the problem $\text{REACH}_{\mathbb{R}}^{\mathbb{Z}}$ has a solution. Moreover, f_n, g_w, h_w can be computed in polynomial time from w. $\square$

Remark 8.17 The proof of Proposition 8.16 shows that $\text{REACH}_{\mathbb{R}}^{\mathbb{Z}}$ remains PSPACE-hard when restricted to one-dimensional compact real algebraic sets.

Lemma 8.18 *For a compact $Z \subseteq \mathbb{R}^n$ let $\Sigma(Z) \subseteq \mathbb{R}^{n+1}$ be the one-point compactification of $Z \times \mathbb{R}$. Then we have $b_{\ell+1}(\Sigma(Z)) = b_\ell(Z)$ for all $\ell \in \mathbb{N}$. (This is also true for $Z = \emptyset$ with the convention that $\Sigma(\emptyset)$ is a one point space.)*

PROOF. The *suspension* $S(Z)$ of a nonempty topological space Z is defined as the space obtained from the cylinder $Z \times [0,1]$ over Z by identifying the points in each of the sets $Z \times \{0\}$ and $Z \times \{1\}$ obtaining the points v_0 and v_1. Essentially, this is a double cone with basis Z and vertices v_0, v_1. It is well known that the Betti numbers of $S(Z)$ and Z are related as follows (cf. [34, 57]):

$$b_{\ell+1}(S(Z)) = \begin{cases} b_\ell(Z) & \text{if } \ell > 0 \\ b_0(Z) - 1 & \text{if } \ell = 0. \end{cases} \tag{17}$$

Assume, without loss of generality, that Z is nonempty. Since Z is compact, the one-point compactification $\Sigma(Z)$ of $Z \times \mathbb{R}$ is homeomorphic to the space arising from the suspension $S(Z)$ by identifying the two vertices v_0 and v_1 of the double cone. This space is homotopy equivalent to the space obtained from $S(Z)$ by connecting the vertices v_0 and v_1 with a one-dimensional cell. This space, in turn, is homotopy equivalent to the space obtained from $S(Z)$ by attaching a circle S^1 at a point. Since this amounts to attach to $S(Z)$ only a cell e^1 we conclude that

$$b_{\ell+1}(\Sigma(Z)) = \begin{cases} b_{\ell+1}(S(Z)) & \text{if } \ell > 0 \\ b_1(S(Z)) + 1 & \text{if } \ell = 0. \end{cases}$$

Combining this with (17), the claim $b_{\ell+1}(\Sigma(Z)) = b_\ell(Z)$ follows, for any $\ell \in \mathbb{N}$. $\square$

The one point compactification of a non-compact real algebraic set can be realized as a real algebraic set by a simple construction [11, p. 68]. For $\xi \in \mathbb{R}^n$ consider the homeomorphism ι_ξ (inversion with respect to the unit sphere with center ξ) defined by

$$\iota_\xi \colon \mathbb{R}^n - \{\xi\} \longrightarrow \mathbb{R}^n - \{\xi\}, \quad x \mapsto \xi + \frac{x - \xi}{\|x - \xi\|^2}.$$

Let f be a real polynomial of degree d with zero set $Z \subseteq \mathbb{R}^n$ and assume that $\xi \notin Z$. Consider the polynomial $f^\xi := \|X - \xi\|^{2d} f(\xi + \|X - \xi\|^{-2}(X - \xi))$ with zero set $Z^\xi \subseteq \mathbb{R}^n$. If Z is unbounded then $Z^\xi = \iota_\xi(Z) \cup \{\xi\}$ is homeomorphic to the one-point compactification of Z. Note that if Z is empty, then Z^ξ consists just of the point ξ.

Theorem 8.19 *For any $k \in \mathbb{N}$ both problems* $\mathrm{BETTI}(k)^{\mathbb{Z}}_{\mathbb{R}}$ *and* $\mathrm{BM\text{-}BETTI}(k)^{\mathbb{Z}}_{\mathbb{R}}$ *are* $\mathsf{FPSPACE}$*-hard with respect to Turing reductions.*

PROOF. Note first that the Borel-Moore and the usual Betti numbers coincide for compact sets. We denote by $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(k)$ and $\mathrm{CREACH}^{\mathbb{Z}}_{\mathbb{R}}$ the restrictions of the problems $\mathrm{BETTI}(k)^{\mathbb{Z}}_{\mathbb{R}}$ and $\mathrm{REACH}^{\mathbb{Z}}_{\mathbb{R}}$ to compact real algebraic sets. We know by Proposition 8.16 and Remark 8.17 that $\mathrm{CREACH}^{\mathbb{Z}}_{\mathbb{R}}$ is $\mathsf{FPSPACE}$-hard. To prove the theorem, it is thus sufficient to establish a Turing reduction from $\mathrm{CREACH}^{\mathbb{Z}}_{\mathbb{R}}$ to $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(k)$. Our proof is similar to the one of [18, Lemma 5.20].

We first describe a Turing reduction from $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(0)$ to $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(k)$, for fixed $k > 0$. Let the compact $Z = \mathcal{Z}(f) \subseteq \mathbb{R}^n$ be given by $f \in \mathbb{Z}[X_1, \ldots, X_n]$. Set $f_0 := f^2 + X_{n+1}^2$, $\xi_0 := (0, \ldots, 0, 1) \in \mathbb{R}^{n+1}$ and note that $\xi_0 \notin \mathcal{Z}(f_0) = \mathcal{Z}(f) \times \{0\}$.

We recursively compute the sequence of polynomials $f_1, \ldots, f_k$ as follows. Let $1 \le i \le k$ and assume that $f_{i-1} \in \mathbb{R}[X_1, \ldots, X_{n+i}]$ has already been computed such that $\xi_{i-1} := (0, \ldots, 0, 1, \ldots, 1) \in \mathbb{R}^{n+i}$ (n zeros, i ones) is not contained in $\mathcal{Z}(f_{i-1})$. Let $\widetilde{f}_{i-1}$ denote the polynomial f_{i-1} interpreted as a polynomial in $X_1, \ldots, X_{n+i+1}$, where X_{n+i+1} is a new variable and $\widetilde{\xi}_{i-1} := (\xi_{i-1}, 0) \in \mathbb{R}^{n+i+1}$. Note that $\mathcal{Z}(\widetilde{f}_{i-1}) = \mathcal{Z}(f_{i-1}) \times \mathbb{R}$. We define now the polynomial $f_i := (\widetilde{f}_{i-1})^{\widetilde{\xi}_{i-1}}$, which results from $\widetilde{f}_{i-1}$ by transformation with the inversion $\iota_{\widetilde{\xi}_{i-1}}$ w.r.t. the unit sphere with center $\widetilde{\xi}_{i-1}$ (see the comments before Theorem 8.19). Note that $\xi_i = \iota_{\widetilde{\xi}_{i-1}}(\xi_i) \notin \mathcal{Z}(f_i)$ since $\|\xi_i - \widetilde{\xi}_{i-1}\| = 1$ and $\widetilde{\xi}_{i-1} \notin \mathcal{Z}(\widetilde{f}_{i-1})$. Then we have $\mathcal{Z}(f_i) = \Sigma(\mathcal{Z}(f_{i-1}))$ and Lemma 8.18 implies that $b_0(Z) = b_k(\mathcal{Z}(f_k))$. This gives the desired reduction from $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(0)$ to $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(k)$.

In order to show that $\mathrm{CREACH}^{\mathbb{Z}}_{\mathbb{R}}$ reduces to $\mathrm{CBETTI}^{\mathbb{Z}}_{\mathbb{R}}(0)$ we first discuss an auxiliary construction. Assume we are given real polynomials f, g such that $\mathcal{Z}(f) \subseteq \mathbb{R}^n$ is compact and $\mathcal{Z}(f, g)$ is nonempty. Consider the one-point compactification $Z_{f;g} \subseteq \mathbb{R}^{n+1}$ of the space $\mathcal{Z}(f) \cup (\mathcal{Z}(f, g) \times \mathbb{R})$. Topologically, this space is obtained from $\mathcal{Z}(f)$ by attaching a double cone with base $\mathcal{Z}(f, g)$ and identifying the two vertices of this cone. What is important is that all the points of $Z(f, g)$ are connected in the new space. This is illustrated in Figure 1 below where $\mathcal{Z}(f)$ is the three closed curves, $\mathcal{Z}(g)$ is the dotted curve and, consequently, $\mathcal{Z}(f, g)$ is the four intersecting points.

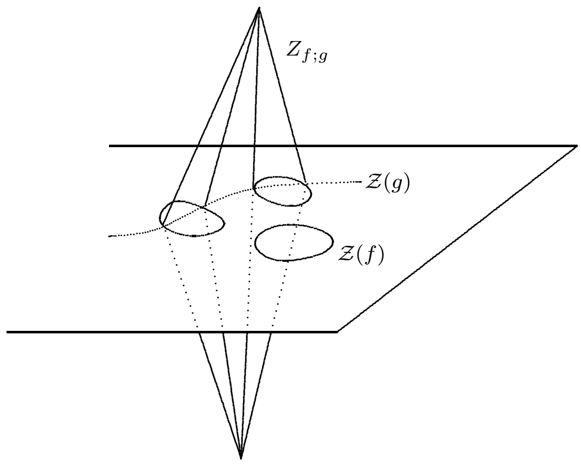

Figure 1: An auxiliary construction.

Using inversions as above, an equation of an algebraic set homeomorphic to $Z_{f;g}$ can be easily computed from f, g. Let h by a further polynomial such that $\mathcal{Z}(f,h) \neq \emptyset$. By attaching a double cone with basis $\mathcal{Z}(f,h)$ to $Z_{f;g}$, we get a real algebraic variety $Z_{f;g,h}$, where all the points of $\mathcal{Z}(f,g)$ and $\mathcal{Z}(f,h)$, respectively, are connected.

We describe now the Turing reduction from $\text{CReach}_{\mathbb{R}}^{\mathbb{Z}}$ to $\text{CBetti}_{\mathbb{R}}^{\mathbb{Z}}(0)$. For a given instance $f, g, h \in \mathbb{Z}[X_1, \ldots, X_n]$ of $\text{CReach}_{\mathbb{R}}^{\mathbb{Z}}$ we first check whether $\mathcal{Z}(f,g)$ or $\mathcal{Z}(f,h)$ is empty by two oracle calls. If this is the case, the corresponding reachability problem has no solution. Otherwise, we know that both $\mathcal{Z}(f,g)$ and $\mathcal{Z}(f,h)$ are nonempty. We compute now equations for the spaces $Z_{f;g,h}$ and $Z_{f;gh}$ (note that in the latter, all points of $\mathcal{Z}(f,g) \cup \mathcal{Z}(f,h)$ have been connected). The spaces $Z_{f;g,h}$ and $Z_{f;gh}$ have the same number of connected components iff there exist points $p \in \mathcal{Z}(f,g)$ and $q \in \mathcal{Z}(f,h)$ which lie in the same connected component of $\mathcal{Z}(f)$. Hence we get the desired reduction using two more oracle calls, one for $Z_{f;g,h}$ and one for $Z_{f;gh}$. □

Remark 8.20 The Betti numbers modulo a prime p are defined similarly as the Betti numbers, but replacing the coefficient field $\mathbb{Q}$ by the finite field $\mathbb{F}_p$. It is easy to check that the proof of Theorem 8.19 also gives the FPSPACE-hardness of the computation of the kth Betti number mod$p$, and similarly for the Borel-Moore Betti numbers.

9 Summary and final remarks

We have summarized the results of this paper in Figure 2 which contains three diagrams showing results in the Turing model, over $\mathbb{C}$, and over $\mathbb{R}$. In this figure, an arrow denotes an inclusion, problems in square brackets are Turing-complete for the class at their left, problems in curly brackets are many-one-complete for that class, and problems in angle brackets are hard for that class. The problems appearing in the figure are defined in the list below. Recall that if L denotes a problem defined over $\mathbb{R}$ or $\mathbb{C}$, we denote its restriction to integer inputs by $L^{\mathbb{Z}}$.

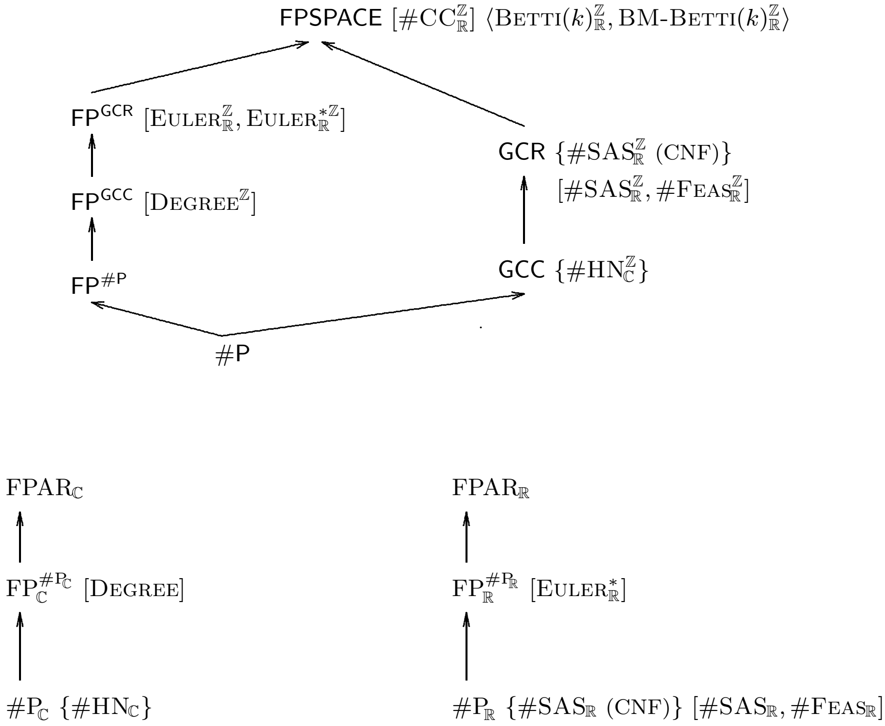

Figure 2: Survey of main results.

$\#\textsc{Feas}_{\mathbb{R}}$ (*Real algebraic point counting*) Given a real multivariate 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.

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

$\textsc{Euler}_{\mathbb{R}}$ (*Euler characteristic for basic semialgebraic sets*) Given a basic semialgebraic set S, decide whether S is empty and if not, compute $\chi(S)$.

$\textsc{Euler}_{\mathbb{R}}^{*}$ (*Euler-Yao characteristic*) Given a semialgebraic set S, decide whether it is empty and if not, compute its Euler-Yao characteristic.

$\#\mathrm{CC}_{\mathbb{R}}$ (*Counting connected components*) Given a semialgebraic set S, compute the number of its connected components.

$\text{BETTI}(k)_{\mathbb{R}}$ (kth *Betti number of a real algebraic set*) Given a real multivariate polynomial, compute the kth Betti number of its real zero set.

$\text{BM-BETTI}(k)_{\mathbb{R}}$ (kth *Borel-Moore Betti number of a real algebraic set*) Given a real multivariate polynomial, compute the kth Borel-Moore Betti number of its real zero set.

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

DEGREE (*Geometric degree*) Given a finite set of complex multivariate polynomials, compute the geometric degree of its affine zero set.

Other problems which appeared in this paper are listed below. The first three are $\text{NP}_{\mathbb{R}}$-complete, the other two, $\text{NP}_{\mathbb{C}}$-complete.

$\text{FEAS}_{\mathbb{R}}$ (*Polynomial feasibility*) Given a real multivariate polynomial, decide whether it has a real root.

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

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

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

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

Remark 9.1 **(i)** To fix ideas, we assumed in the definition of the above problems that the input polynomials are given in sparse representation. However, note that choosing the dense encoding leads to polynomial time equivalent problems. In order to see this, one just has to introduce additional variables that help to represent monomials of high degree by "repeated squaring". The solution set of the new system of polynomial (in)equalities is homeomorphic to the original one. A similar remark applies for the encoding of polynomials by division free straight-line programs.

(ii) Instead of restricting inputs to integer polynomials, one could allow also algebraic (or real algebraic) coefficients with their standard binary encoding. The results in this paper would then hold as well and our proofs would only need some extra algorithmics, common in symbolic computation.

10 Open problems

We believe that the developments in this paper open up a variety of meaningful new questions. To finish this paper we list some of them.

Problem 1 Can one decide $\text{FEAS}_{\mathbb{R}}$ in polynomial time with a black box for the Euler characteristic?

Problem 2 It is known that the problem to count the number of connected components of a semialgebraic set is in $\text{FPAR}_{\mathbb{R}}$. Is it hard in this class? We know that the corresponding result is true in the additive setting [18].

Problem 3 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?

Problem 4 Can Betti numbers of semialgebraic sets be computed in $\text{FPAR}_{\mathbb{R}}$? We know that, in the additive setting, the computation of Betti numbers of semi-linear sets is FPAR_{add}-complete [18].

Problem 5 What is the complexity to compute the multiplicity $\text{mult}_x(Z)$ of a point x in an algebraic variety Z? And how about the computation of intersection multiplicities $i(Z, A; x)$?

Problem 6 Can one characterize GCR and GCC in terms of known classical complexity classes?

Problem 7 Toda's theorem [71] states that $\mathsf{PH} \subseteq \mathsf{FP}^{\#\mathsf{P}}$. Is there an analogue of this over $\mathbb{R}$ or over $\mathbb{C}$?

References

[1] L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Comput. System Sci.*, 36(2): 254–276, 1988.

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

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

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

[5] 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.

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

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

[8] 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.

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

[10] 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.

[11] 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.

[12] A. Borel and J.C. Moore. Homology theory for locally compact spaces. *Michigan Math. J.*, 7:137–159, 1960.

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

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

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

[16] P. Bürgisser. Cook's versus Valiant's hypothesis. *Theoret. Comp. Sci.*, 235:71–88, 2000.

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

[18] P. Bürgisser and F. Cucker. Counting Complexity Classes for Numeric Computations I: Semilinear Sets. *SIAM J. Comp.*, 33:227–260, 2003.

[19] P. Bürgisser and F. Cucker and M. Lotz. Counting Complexity Classes for Numeric Computations III: Complex Projective Sets. *Found. Comput. Math.*, to appear.

[20] P. Bürgisser and M. Lotz. The complexity of computing the Hilbert polynomial of smooth equidimensional complex projective varieties. *Found. Comput. Math.*, to appear.

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

[22] F. Cucker. On the Complexity of Quantifier Elimination: the Structural Approach. *The Computer Journal*, 36:399–408, 1993.

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

[24] 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.

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

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

[27] 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.

[28] W. Fulton. *Introduction to Toric Varieties*. Annals of Math. Studies. Princeton University Press, 1993.

[29] F. Geerts. Expressing the cone radius in the relational calculus with real polynomial constraints. *Discrete Comput. Geom.*, 30(4):607–622, 2003.

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

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

[32] D.Yu. Grigoriev and N. Vorobjov. Counting connected components of a semialgebraic set in subexponential time. *Comp. Compl.*, 2(2):133–186, 1992.

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

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

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

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

[37] 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.

[38] 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.

[39] H. Hironaka. Triangulation of algebraic sets. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974)*, volume 29 of *Proceedings of Symposia in Pure Mathematics*, pages 165–185. Amer. Math. Soc., 1975.

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

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

[42] P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Compl.*, 12:273–286, 1996. Additional information is contained in the DIMACS Technical Report 96-27, July 1996.

[43] P. Koiran. Elimination of constants from machines over algebraically closed fields. *J. Compl.*, 13:65–82, 1997.

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

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

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

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

[48] G.M. Kuper, J. Paredaens, and L. Libkin. *Constraint Databases.* Springer-Verlag, 2000.

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

[50] E.W. Mayr. Some Complexity Results for Polynomial Ideals. *J. Compl.*, 13:303–325, 1997.

[51] 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.

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

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

[54] J. Milnor. On the Betti numbers of real varieties. In *Proc. AMS*, volume 15, pages 275–280, 1964.

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

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

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

[58] O.A. Oleĭnik. Estimates of the Betti numbers of real algebraic hypersurfaces. *Math. Sb. (N.S.)*, 28 (70):635–640, 1951.

[59] O.A. Oleĭnik and I.B. Petrovskii. On the topology of real algebraic surfaces. *Izv. Akad. Nauk SSSR*, 13:389–402, 1949.

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

[61] E. Rannou. The complexity of stratification computation. *Discrete Comput. Geom.*, 19:47–78, 1998.

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

[63] 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.

[64] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. part I, II, III. *J. Symb. Comp.*, 13(3):255–352, 1992.

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

[66] E. Spanier. *Algebraic Topology.* MacGraw-Hill, 1966.

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

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

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

[70] R. Thom. Sur l'homologie des variétés algébriques réelles. In S.S. Cairns, editor, *Differential and Combinatorial Topology*, pages 255–265. Princeton Univ. Press, 1965.

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

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

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

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

[75] 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.

[76] A.C. Yao. Algebraic decision trees and Euler characteristic. Theoret. Comput. Sci., 141:133–150, 1995.