

Counting Complexity Classes for Numeric Computations.

III: Complex Projective Sets*

Peter Bürgisser[†]
Dept. of Mathematics
University of Paderborn
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

Martin Lotz[†]
Dept. of Mathematics
University of Paderborn
D-33095 Paderborn
Germany
e-mail: lotzm@upb.de

Abstract. In [8] counting complexity classes $\#P_{\mathbb{R}}$ and $\#P_{\mathbb{C}}$ in the Blum-Shub-Smale setting of computations over the real and complex numbers, respectively, were introduced. One of the main results of [8] is that the problem to compute the Euler characteristic of a semialgebraic set is complete in the class $FP_{\mathbb{R}}^{\#P_{\mathbb{R}}}$. In this paper, we prove that the corresponding result is true over \mathbb{C} , namely that the computation of the Euler characteristic of an affine or projective complex variety is complete in the class $FP_{\mathbb{C}}^{\#P_{\mathbb{C}}}$. We also obtain a corresponding completeness result for the Turing model.

1 Introduction

This paper provides a natural extension of one of the main results in [8] namely, that the computation of the modified¹ Euler characteristic of a semialgebraic set is

*The results of this work were announced in *Comptes rendus de l'Académie des sciences Paris*, Ser. I 339:37–376, 2004.

[†]Partially supported by DFG grant BU 1371 and Paderborn Institute for Scientific Computation (PaSCo).

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

¹The *modified Euler characteristic* was introduced by Yao [36]. It is a minor variation of the Euler characteristic, which has a desirable additivity property and coincides with the usual Euler

complete in the counting class $\text{FP}_{\mathbb{R}}^{\#\text{P}_{\mathbb{R}}}$. A main goal of this paper is to prove a similar result over \mathbb{C} , i.e., that the computation of the Euler characteristic of an algebraic variety (affine or projective) is complete in the class $\text{FP}_{\mathbb{C}}^{\#\text{P}_{\mathbb{C}}}$.

Here, we recall from [8], $\#\text{P}_{\mathbb{R}}$ denotes the class of functions from the space \mathbb{R}^{∞} of finite sequences of real numbers into $\mathbb{N} \cup \{\infty\}$ which, roughly speaking, count the number of satisfying witnesses for an input of a problem in $\text{NP}_{\mathbb{R}}$. This class of functions extends to the setting of computations over \mathbb{R} the class $\#\text{P}$ introduced by L. Valiant in his seminal papers [34, 35] where it was proved that the computation of the permanent is $\#\text{P}$ -complete. The extension to \mathbb{R} was done in [31] and the extension to \mathbb{C} (together with several completeness results over both \mathbb{R} and \mathbb{C}) was carried out in [8]. Also, the complexity class $\text{FP}_{\mathbb{R}}^{\#\text{P}_{\mathbb{R}}}$ consists of all functions $f: \mathbb{R}^{\infty} \rightarrow \mathbb{R}^{\infty}$, which can be computed in polynomial time using oracle calls to functions in $\#\text{P}_{\mathbb{R}}$. A similar definition applies over \mathbb{C} .

The Euler characteristic of Z , denoted by $\chi(Z)$, is one of the most basic invariants in algebraic topology. It naturally occurs in many applications in other branches of geometry. Remarkably, it can be characterized in several different ways. For instance, for spaces Z admitting a finite triangulation, it is the alternate sum of the number of i -simplices of the triangulation. In general, it is also the alternate sum of the Betti numbers $b_i(Z)$ of Z , that is, of the ranks of the homology groups $H_i(Z; \mathbb{Z})$. Also, for differentiable manifolds Z , $\chi(Z)$ can be characterized as the alternate sum over i of the number of critical points of index i of any Morse function $f: Z \rightarrow \mathbb{R}$. It is this last characterization, together with the elimination of generic quantifiers via partial witness sequences, that lies at the heart of the proof of completeness for the modified Euler characteristic given in [8]. Ultimately, this characterization reduces the problem of computing $\chi(Z)$ to that of counting points satisfying a certain property, and counting points is precisely what functions in $\#\text{P}_{\mathbb{R}}$ are able to do.

If Z is now a complex (affine or projective) variety and we want to compute $\chi(Z)$ with machines over \mathbb{C} , the use of Morse functions as described above is not possible. This is due to the fact that machines over \mathbb{C} can not compute signs or recognize elements in \mathbb{R} . Therefore, to extend the completeness result of [8] to complex varieties requires yet another characterization of $\chi(Z)$, for Z a complex variety, which would again reduce the computation of $\chi(Z)$ to counting points. Such a characterization was recently found by P. Aluffi [1]. A feature we want to highlight in this paper is the replacement of Morse theory (and hence the reliance on differential topology) by Aluffi's result (of a more algebraic-geometric nature).

To describe the main results in this paper, and to relate them with previous work, consider the following problems.

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

characteristic in many cases, e.g., for compact semialgebraic sets and complex algebraic varieties.

$\text{EULER}_{\mathbb{C}}$ (*Euler characteristic of affine varieties*) Given a finite set of complex multivariate polynomials, compute the Euler characteristic of its affine zero set.

$\text{PROJEULER}_{\mathbb{C}}$ (*Euler characteristic of projective varieties*) Given a finite set of complex homogeneous polynomials, compute the Euler characteristic of its projective zero set.

$\text{EULER}_{\mathbb{R}}$ (*Euler characteristic*) Given a semialgebraic set as a union of basic semi-algebraic sets, decide whether it is empty and if not, compute its modified Euler characteristic.

The main results of [8] can be summarized as follows.

Theorem 1.1 ([8]) *The problem DEGREE is $\text{FP}_{\mathbb{C}}^{\#\text{P}_{\mathbb{C}}}$ -complete and the problem $\text{EULER}_{\mathbb{R}}$ is $\text{FP}_{\mathbb{R}}^{\#\text{P}_{\mathbb{R}}}$ -complete, both for Turing reductions. \square*

The main result in this paper is the following.

Theorem 1.2 *Both problems $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$ are $\text{GAP}_{\mathbb{C}}^*$ -complete for Turing reductions.*

Here $\text{GAP}_{\mathbb{C}}^*$ is a class of functions lying in between $\#\text{P}_{\mathbb{C}}$ and $\text{FP}_{\mathbb{C}}^{\#\text{P}_{\mathbb{C}}}$. While complete problems in these two last classes are Turing equivalent (by definition), they are not equivalent for weaker reductions. One of the contributions of this paper is the introduction of a new kind of reduction, weaker than the Turing one but stronger than parsimonious, together with the classes $\#\text{P}_{\mathbb{C}}^*$ and $\text{GAP}_{\mathbb{C}}^*$, which are closed under this new reduction.

If the polynomials defining the variety Z are restricted to have integer coefficients, the problem of computing $\chi(Z)$ can be considered in the Turing model of computation. We denote by $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ and $\text{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$ these restricted problems. An easy consequence of Theorem 1.2 is the fact that these problems are complete in the discrete class FP^{GCC} . Here FP is the class of functions computed by Turing machines in polynomial time and GCC is a counting class of Boolean functions introduced in [8].

In his paper, Aluffi [1] presents an algorithm to compute the Euler characteristic (and related quantities) and describes an actual implementation by himself in `Macaulay2`. While the use of `Macaulay2` allows for a quick implementation, this algorithm has the theoretical drawback to rely on the computation of Gröbner bases. Algorithms based on Gröbner bases generally lead to bad complexity estimates (doubly exponential in the number of variables), with a few exceptions, where single exponential bounds have been established (e.g., in the zero dimensional case [12, 28]). The reduction presented in §6 yields an algorithm for computing the Euler characteristic with a running time that is essentially that of an algorithm counting the

number of points in a zero-dimensional variety. This latter problem is known to be in PSPACE (it is actually GCC-complete and $\text{GCC} \subseteq \text{PSPACE}$ [8]). This immediately yields PSPACE bounds for the computation of $\chi(Z)$. In addition, the completeness of $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ and $\text{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$ in FP^{GCC} ties any further improvement in the complexity of computing $\chi(Z)$ to improvements on the upper bounds for GCC.

The paper is organized as follows: after a preliminary section recalling some basic notions and facts from complexity theory and algebraic geometry, we give in §3 a short introduction to the quantities whose computational complexity we study. In particular, we recall there Aluffi’s result relating the Euler characteristic of a projective hypersurface with the projective degrees of its gradient map. In §4 we define generic parsimonious reductions and introduce the new complexity classes $\#\text{P}_{\mathbb{C}}^*$ and $\text{GAP}_{\mathbb{C}}^*$. These new classes are used in §5, where the main results are proved. Finally, we present in §6 corresponding completeness results in the Turing model, along with structural results of “transfer type” relating $\#\text{P}_{\mathbb{C}}$ with the corresponding counting complexity classes defined over algebraically closed fields of characteristic zero as well as with its restrictions to binary inputs.

2 Preliminaries

2.1 Machines and complexity classes

We denote by \mathbb{C}^{∞} the disjoint union $\mathbb{C}^{\infty} = \bigsqcup_{n \geq 0} \mathbb{C}^n$, where for $n \geq 0$, \mathbb{C}^n is the standard n -dimensional space over \mathbb{C} . The space \mathbb{C}^{∞} is a natural one to represent problem instances of arbitrarily high dimension. For $x \in \mathbb{C}^n \subset \mathbb{C}^{\infty}$, we call n the *size* of x and we denote it by $\text{size}(x)$. Contained in \mathbb{C}^{∞} 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{C} as they are defined in [3, 4]. Roughly speaking, such a machine takes an input from \mathbb{C}^{∞} , performs a number of arithmetic operations and tests for zero following a finite list of instructions, and halts returning an element in \mathbb{C}^{∞} (or loops forever). If the only machine constants occurring in a machine are 0 and 1 we say that the machine is *constant-free*. The computation of a machine on an input $x \in \mathbb{C}^{\infty}$ is well-defined and notions such as a function being computed by a machine or a subset of \mathbb{C}^{∞} being decided by a machine easily follow.

We next introduce some central complexity classes.

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

2.2 Affine and projective algebraic varieties

Algebraic geometry is the study of zero sets of polynomials (or of objects which locally resemble these sets). We very briefly recall some definitions and facts from algebraic geometry, which will be needed later on. For more exhaustive accounts, standard textbooks on algebraic geometry are [18, 19, 32, 33].

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

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

of finitely many polynomials $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$. The *vanishing ideal* $\mathcal{I}(Z)$ of Z consists of all the polynomials vanishing on Z . If f_1, \dots, f_r generate $\mathcal{I}(Z)$, then the *Zariski tangent space* $T_x Z$ of Z at a point $x \in Z$ is defined by $T_x Z = \mathcal{Z}(d_x f_1, \dots, d_x f_r)$, where the *differential* $d_x f: \mathbb{C}^n \rightarrow \mathbb{C}$ of f at x is the linear function $d_x f = \sum_{j=1}^n \partial_{X_j} f(x) X_j$. The point $x \in Z$ is called a *smooth point* of Z if the dimension of $T_x Z$ equals the local dimension of Z at x . Otherwise, x is called a *singular point* of Z .

The algebraic subsets of \mathbb{C}^n are the closed sets of a topology in \mathbb{C}^n , which is known as *Zariski topology*. Note that nonempty open sets in this topology are dense in \mathbb{C}^n . Locally closed sets in the Zariski topology are called *basic quasiaffine*. They can be described by a system $f_1 = \dots = f_r = 0, g \neq 0$. Finite unions of basic quasiaffine are called *quasiaffine*.

A usual compactification of the space \mathbb{C}^n consists of embedding \mathbb{C}^n into $\mathbb{P}^n = \mathbb{P}^n(\mathbb{C})$, 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 $\mathbb{C}^n \hookrightarrow \mathbb{P}^n$ maps a point $x \in \mathbb{C}^n$ to the only line in \mathbb{C}^{n+1} passing through the origin and through $(1, x)$. The notion of affine algebraic variety extends to that of *projective variety* by replacing polynomials by homogeneous polynomials in $\mathbb{C}[X_0, X_1, \dots, X_n]$, for which elements of \mathbb{P}^n are natural zeros. The embedding $\mathbb{C}^n \hookrightarrow \mathbb{P}^n$ extends to the algebraic subsets of \mathbb{C}^n by defining, for any such set Z , its *projective closure* \bar{Z} as the smallest projective variety in \mathbb{P}^n containing Z . It is customary to denote, for a point $(x_0, \dots, x_n) \in \mathbb{C}^{n+1}$, by $(x_0: \dots: x_n)$ the corresponding point in \mathbb{P}^n . We also note that the local notions of tangent space and smoothness extend to the projective setting in a straightforward way.

An important example of projective varieties are the Grassmannians. For $0 \leq k \leq n$ the *Grassmannian* $\mathbb{G}(k, n)$ is the set of all $k+1$ -dimensional vector subspaces of \mathbb{C}^{n+1} . The simplest example is $\mathbb{G}(0, n)$ which is isomorphic to \mathbb{P}^n . In general, $\mathbb{G}(k, n) \subseteq \mathbb{P}^{\binom{n+1}{k+1}-1}$ is an irreducible projective variety of dimension $\dim \mathbb{G}(k, n) = (k+1)(n-k)$, see [18, Lecture 6]. Elements in $\mathbb{G}(k, n)$ are in bijective correspondence with subspaces $\mathbb{P}^k \subseteq \mathbb{P}^n$. We will often write L^{n-k} for an element in $\mathbb{G}(k, n)$, the superscript emphasizing the codimension.

We will also consider varieties in products of projective spaces. It is a nontrivial fact that $\mathbb{P}^n \times \mathbb{P}^n$ has the structure of a projective variety. This follows from the

existence of an injective map (Segre embedding) $\mathbb{P}^n \times \mathbb{P}^n \hookrightarrow \mathbb{P}^{n(n+2)}$ whose image is a projective variety.

We will consider algebraic varieties as input data for machines over \mathbb{C} . We think of a variety Z as encoded by a family of polynomials of which Z is the zero set. Thus, we have to define how polynomials themselves are encoded as vectors of complex numbers. For simplicity we will assume that this is done using the *dense encoding*: a complex polynomial of degree d in n variables is given by the list of its $\binom{n+d}{d}$ coefficients. When working in the Turing model and dealing with integer polynomials, we will assume that the coefficients are given by a bit vector. We remark, however, that our results have little dependence on the choice of encoding and that they also hold for the so called sparse encoding, or even the straight-line program encoding, cf. [8, Remark 9.1].

2.3 Counting Complexity Classes

We now recall the definition of counting classes over \mathbb{C} in [8]. This definition follows the lines used in discrete complexity theory to define $\#P$.

Definition 2.2 We say that a function $\varphi: \mathbb{C}^\infty \rightarrow \mathbb{N} \cup \{\infty\}$ belongs to the class $\#P_{\mathbb{C}}$ if there exists a polynomial time machine M and a polynomial p such that, for all $x \in \mathbb{C}^n$,

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

The complexity class $FP_{\mathbb{C}}^{\#P_{\mathbb{C}}}$ consists of all functions $\varphi: \mathbb{C}^\infty \rightarrow \mathbb{C}^\infty$, which can be computed in polynomial time using oracle calls to functions in $\#P_{\mathbb{C}}$. (In principle, these oracle calls should be to a single function in $\#P_{\mathbb{C}}$ but the existence of complete problems in this class (cf. [8]) allows one to query different functions.)

The power of counting can be located between known complexity classes. Recall that $NP_{\mathbb{C}}$ is the class of sets decidable in nondeterministic polynomial time over \mathbb{C} [4] and that $FPar_{\mathbb{C}}$ denotes the class of functions computable in parallel polynomial time such that $\text{size}(f(x)) = (\text{size}(x))^{\mathcal{O}(1)}$ for every $x \in \mathbb{C}^\infty$ [3, §18].

Proposition 2.3 ([8]) We have $FP_{\mathbb{C}}^{NP_{\mathbb{C}}} \subseteq FP_{\mathbb{C}}^{\#P_{\mathbb{C}}} \subseteq FPar_{\mathbb{C}}$. □

We next define notions of reduction and completeness appropriate for counting classes.

Definition 2.4 1. Let $\varphi, \psi: \mathbb{C}^\infty \rightarrow \mathbb{N} \cup \{\infty\}$. We say that $\pi: \mathbb{C}^\infty \rightarrow \mathbb{C}^\infty$ is a *parsimonious reduction* from φ to ψ if π can be computed in polynomial time and, for all $x \in \mathbb{C}^\infty$, $\varphi(x) = \psi(\pi(x))$. If such a reduction exists we write $\varphi \preceq \psi$.

2. We say that φ *Turing reduces* to ψ , and we write $\varphi \preceq_T \psi$, if there exists an oracle machine which, with oracle ψ , computes φ in polynomial time.

3. Let \mathcal{C} be any of $\#P_{\mathbb{C}}$, or $FP_{\mathbb{C}}^{\#P_{\mathbb{C}}}$. We say that a function ψ is *hard* for \mathcal{C} if, for every $\varphi \in \mathcal{C}$, there is a parsimonious reduction from φ to ψ . We say that ψ is *\mathcal{C} -complete* if, in addition, $\psi \in \mathcal{C}$.

4. The notions of *Turing-hardness* or *Turing-completeness* are defined similarly.

We remark that $\#P_{\mathbb{C}}$ is closed under parsimonious reductions, that is, $\varphi \preceq \psi$ and $\psi \in \#P_{\mathbb{C}}$ implies $\varphi \in \#P_{\mathbb{C}}$.

The following counting problems are the basic complete problems in $\#P_{\mathbb{C}}$.

$\#HN_{\mathbb{C}}$ (*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.

$\#QAS_{\mathbb{C}}$ (*Quasialgebraic point counting*) Given a quasialgebraic set $S \subseteq \mathbb{C}^n$ count the number of points in S , returning ∞ if this number is not finite.

Theorem 2.5 ([8]) *The problems $\#HN_{\mathbb{C}}$ and $\#QAS_{\mathbb{C}}$ are $\#P_{\mathbb{C}}$ -complete with respect to parsimonious reductions. \square*

3 Projective degrees and Euler characteristic

In this section we give a short introduction to the quantities whose computational complexity we shall study. Two of these quantities are the *degree* of the embedding of a projective variety and the *projective degrees* of a rational map; these are commonly occurring invariants in algebraic geometry. Another is the *Euler characteristic*, one of the most fundamental invariants in algebraic topology.

As it turns out, these quantities are more closely related than it may appear at first sight. On the one hand, the algebraic-geometric degree of an embedding can be characterized topologically. On the other hand, in many cases (smooth hypersurfaces, complete intersections) there are formulas for the Euler characteristic in terms of degrees. For not necessarily smooth hypersurfaces, a formula for the Euler characteristic in terms of the projective degrees of the rational morphism associated to the gradient of the defining polynomial follows from a formula due to Aluffi [1].

It is this relationship between projective degrees and Euler characteristic that we will exploit in order to relate the computational complexity of these problems.

3.1 Degree and projective degrees

We start by defining the notion of degree of an algebraic variety embedded in projective space \mathbb{P}^n . Recall that a variety is called *irreducible* if it cannot be written as the union of two proper subvarieties. It is well known that every variety Z can

be written as a non-redundant finite union of irreducible varieties. The latter are called the *irreducible components* of Z .

A notion that will be used all along this paper (and which is at the heart of the definition of degree) is that of a property holding “for almost all” points (or for a *generic* point) in an irreducible variety Z . By this we mean that the set of points in Z satisfying the given property contains a nonempty open (and thus dense) set in the Zariski topology. In most of the cases, we will use this notion with Z being either a Grassmannian or a product of Grassmannians.

Definition 3.1 (i) The *degree* $\deg Z$ of an irreducible projective variety $Z \subseteq \mathbb{P}^n$ is the number of intersection points of Z with a generic linear subspace $L \subseteq \mathbb{P}^n$ of complementary dimension.

(ii) The *degree* $\deg Z$ of a reducible projective variety $Z \subseteq \mathbb{P}^n$ is the sum of the degrees of all irreducible components of maximal dimension.

A similar definition applies to the affine case (see, e.g., [8]). This is a well-defined notion, as shown in any standard text on algebraic geometry [18, 19, 32, 33].

Remark 3.2 The degree as defined above is sometimes called *geometric degree* in contrast with the so called *cumulative degree* which is the sum of the degrees of *all* the irreducible components of Z . While the former is of more common use in algebraic geometry, the latter has been extensively used in algebraic complexity, see [7].

An extension of the notion of degree of a projective variety is the sequence of projective degrees of a rational morphism. We next briefly explain how this is defined.

Let $f_0, \dots, f_n \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous nonzero polynomials of the same degree d and let $\Sigma := \mathcal{Z}_{\mathbb{P}^n}(f_0, \dots, f_n)$ denote their projective zero set. Then these polynomials define a *regular morphism*

$$\varphi: U \rightarrow \mathbb{P}^n, (x_0 : \dots : x_n) \mapsto (f_0(x) : \dots : f_n(x))$$

on the domain of definition $U := \mathbb{P}^n \setminus \Sigma$, which is open and dense in the Zariski topology. We will call such φ a *rational morphism* and sometimes write shortly $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$. Let $\Gamma_U \subseteq \mathbb{P}^n \times \mathbb{P}^n$ denote the graph of φ and let Γ denote the closure of Γ_U in the Zariski topology. It is easy to see that $\Gamma = \Gamma_U \cup \Gamma_\Sigma$, where Γ_Σ is the inverse image of Σ under the projection $\pi_1: \Gamma \rightarrow \mathbb{P}^n$ onto the first factor. Note that $\dim \Gamma_\Sigma < n = \dim \Gamma$.

Consider $L^i \in \mathbb{G}(n-i, n)$ and $L^{n-i} \in \mathbb{G}(i, n)$ in the Grassmannians. Since $\dim \Gamma = n$, the intersection $\Gamma \cap (L^i \times L^{n-i})$ is finite for generic (L^i, L^{n-i}) . We may wonder under which conditions the number of points in this intersection does not depend on (L^i, L^{n-i}) . The next proposition gives an answer and leads to the concept of projective degrees. To state this proposition, we have to give a definition first.

Definition 3.3 Let $Z \subseteq M$ be a subvariety of a smooth variety M , $L \subseteq M$ be a smooth subvariety and $p \in Z \cap L$. We say that Z is *transverse* to L at p , and we write $Z \pitchfork_p L$, if Z is smooth at p and $T_p Z \oplus T_p L = T_p M$, where T_p denotes the tangent space at a point p . We say that Z is *transverse* to L , and we write $Z \pitchfork L$, if $Z \pitchfork_p L$ for all $p \in Z \cap L$.

The following result should be well known. For lack of a suitable reference, we provide a proof in the Appendix.

Proposition 3.4 Let $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ be a rational morphism defined on U and let Γ be the closure of the graph of φ .

(i) For $0 \leq i < n$ there exists a nonnegative integer d_i such that, if

$$\Gamma_U \pitchfork (L^i \times L^{n-i}) \quad \text{and} \quad \Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$$

then

$$|\Gamma_U \cap (L^i \times L^{n-i})| = |L^i \cap \varphi^{-1}(L^{n-i})| = d_i.$$

(ii) The above conditions are satisfied for generic $(L^i, L^{n-i}) \in \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$.

Definition 3.5 We call the integers d_0, \dots, d_{n-1} the *projective degrees* of the rational morphism φ (compare [18, Chapter 19]).

Example 1 Consider $f_0 = X_1 X_2$, $f_1 = X_0 X_2$, $f_2 = X_0 X_1$ in the case $n = 2$. Then $\Sigma = \mathcal{Z}_{\mathbb{P}^2}(f_0, f_1, f_2) = \{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)\}$. It is easy to see that $d_1 = 2$. We claim that $d_0 = 1$. Indeed, take $L^2 = \mathcal{Z}_{\mathbb{P}^2}(a_0 Y_0 + a_1 Y_1 + a_2 Y_2, b_0 Y_0 + b_1 Y_1 + b_2 Y_2)$ and note that

$$\varphi^{-1}(L^2) = \mathcal{Z}_{\mathbb{P}^2}(a_0/X_0 + a_1/X_1 + a_2/X_2, b_0/X_0 + b_1/X_1 + b_2/X_2, X_0 X_1 X_2 \neq 0)$$

consists of exactly one point in \mathbb{P}^2 for generic coefficients a_i, b_i .

In general, if the image of $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ is dense, then d_0 is the cardinality of the generic fibre of φ .

The following proposition is just stated for illustrating the notion of projective degrees and will not be needed in the rest of this paper.

Proposition 3.6 Let $f_0, \dots, f_n \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous nonzero polynomials of the same degree d and let r be the codimension of $\Sigma := \mathcal{Z}_{\mathbb{P}^n}(f_0, \dots, f_n)$ in \mathbb{P}^n . Then the projective degrees d_i of the corresponding rational map φ satisfy $d_{n-i} = d^i$ for $1 \leq i < r$ and $d_{n-r} = d^r - \deg(\Sigma)$.

PROOF. For a generic L^r we may write $\varphi^{-1}(L^r) = \mathcal{Z}_{\mathbb{P}^n}(g_1, \dots, g_r) \setminus \Sigma$, where g_1, \dots, g_r form a generic linear combination of f_0, \dots, f_n . It is well known [30] that (g_1, \dots, g_r) is a regular sequence. Let C_1, \dots, C_s be the irreducible components of $Z := \mathcal{Z}_{\mathbb{P}^n}(g_1, \dots, g_r)$. Then all C_j have codimension r and we have $\deg Z = \sum_{j=1}^s \deg C_j = d^r$, see [19]. Suppose that C_1, \dots, C_k are the irreducible components of Z that are contained in Σ . Then these are the irreducible components of Σ of maximal dimension and hence $\deg \Sigma = \sum_{j=1}^k \deg C_j$. Therefore, we obtain for generic L^{n-r} ,

$$d_{n-r} = |L^{n-r} \cap \varphi^{-1}(L^r)| = |L^{n-r} \cap (Z \setminus \Sigma)| = \sum_{j=k+1}^r \deg C_j = d^r - \deg \Sigma.$$

The proof that $d_{n-i} = d^i$ for $i < r$ is similar. \square

3.2 Euler characteristic

The Euler characteristic is one of the oldest and most important topological invariants. There are many ways to characterize it; some are very general, others assume restrictions on the topological space Z . The most intuitive one is perhaps using a finite triangulation. In this situation, which requires Z to be finitely triangulable (and therefore, compact), the Euler characteristic is the alternating sum $\chi(Z) = \sum_{i=0}^d (-1)^i N_i$, where N_i denotes the number of i -simplices in the triangulation and d is the dimension of Z . It is a fundamental fact that this definition does not depend on the particular triangulation chosen. As an example, for the tetrahedron T , we have $\chi(T) = 4 - 6 + 4 = 2$, and therefore for the 2-sphere $\chi(S^2) = 2$. More generally, for the n -sphere S^n we have $\chi(S^n) = 1 + (-1)^n$.

For possibly more general topological spaces, we define the Euler characteristic via *singular homology*. We next briefly describe how. Good general references for this material are [5] and [20].

To a topological space Z one can associate the singular homology groups $H_i(Z)$ with coefficients in \mathbb{Z} . These are abelian groups that are homotopy invariant, meaning that if Z is homotopy equivalent to Z' , then $H_i(Z) \cong H_i(Z')$ for all $i \in \mathbb{N}$. If Z is finite dimensional then $H_i(Z) = 0$ for all $i > \dim Z$.

Definition 3.7 The *Euler characteristic* $\chi(Z)$ of a topological space Z is defined as the alternating sum $\chi(Z) = \sum_{k \in \mathbb{N}} (-1)^k \text{rank } H_k(Z)$, provided this sum is finite.

If $Z \subseteq \mathbb{P}^n$ is an k -dimensional complex algebraic variety, then it can be seen as a $2k$ -dimensional real algebraic variety and therefore $H_j(Z) = 0$ for $j > 2k$.

In [8], the complexity of computing the modified Euler characteristic $\chi^*(S)$ of a semialgebraic set S was studied. The latter is a minor variation of the Euler characteristic, which is additive with respect to disjoint unions and coincides with the usual Euler characteristic for compact semialgebraic sets.

The following proposition expresses that for complex quasialgebraic sets, the modified Euler characteristic coincides with the Euler characteristic. A proof can be found in [15, Exercise §4.5, p. 95 and Notes §4.13, p. 141].

Proposition 3.8 *If $Z = \bigsqcup_{i=1}^N Z_i$ is a disjoint union of complex quasialgebraic sets, then $\chi(Z) = \sum_{i=1}^N \chi(Z_i)$. \square*

The Euler characteristic satisfies the following principle of inclusion and exclusion. (Note that, compared with the usual application of this principle, the roles of \cup and \cap are interchanged.)

In the sequel, $[r]$ denotes the set $\{1, \dots, r\}$.

Lemma 3.9 *Let Z_1, \dots, Z_r be complex quasialgebraic sets. Write $Z_I := \cup_{i \in I} Z_i$ for an index set $I \subseteq [r]$. Then we have*

$$\chi(Z_1 \cap \dots \cap Z_r) = \sum_{\emptyset \neq I \subseteq [r]} (-1)^{|I|-1} \chi(Z_I).$$

PROOF. This follows easily from Proposition 3.8 and [8, Corollary 6.4] by passing over to the complement. \square

3.3 Expressing the Euler characteristic by degrees

Let $Z = \mathcal{Z}(f) \subset \mathbb{P}^n$ be a smooth, irreducible hypersurface. Then, a known formula [13, §5] expresses the Euler characteristic in terms of the degree d of Z :

$$\chi(Z) = \frac{1}{d}((1-d)^{n+1} - 1) + n + 1. \quad (1)$$

Example 2 (i) Taking $\mathbb{P}^n = \mathcal{Z}(X_0) \subset \mathbb{P}^{n+1}$ we get $\chi(\mathbb{P}^n) = n + 1$.

(ii) For a smooth planar curve $Z \subset \mathbb{P}^2$ of degree d , Equation (1) implies the well-known formula $\chi(Z) = \frac{1}{d}((1-d)^3 - 1) + 3 = d(3-d) = 2(1-g(Z))$, where $g(Z)$ is the arithmetic genus of Z , cf. [19]

A generalization of Equation (1) to the case of possibly singular hypersurfaces follows from a formula of Aluffi [1] for Chern-Schwartz-MacPherson classes for arbitrary hypersurfaces. Our statement below follows from Theorem 2.1 and the remark at the end of §2.6 in [1].

Theorem 3.10 (Aluffi [1]) *Let $f \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous and nonconstant. The Euler characteristic of the projective hypersurface $Z = \mathcal{Z}(f)$ is given by*

$$\chi(Z) = n + \sum_{i=1}^n (-1)^{i-1} d_{n-i},$$

where d_0, \dots, d_{n-1} are the projective degrees of the gradient morphism

$$\mathbb{P}^n \setminus \Sigma \rightarrow \mathbb{P}^n, \quad x = (x_0 : \dots : x_n) \mapsto (\partial_0 f(x) : \dots : \partial_n f(x))$$

and $\Sigma := \mathcal{Z}(\partial_0 f, \dots, \partial_n f)$. □

Example 3 (i) Consider the factorization of $f = \prod_{i=1}^s (\alpha_i X_0 + \beta_i X_1)^{e_i}$. Then $\mathcal{Z}(f) \subseteq \mathbb{P}^1$ consists of exactly s points. Theorem 3.10 says $\chi(\mathcal{Z}(f)) = 1 + d_0$. On the other hand, a straightforward calculation shows that indeed $d_0 = s - 1$. (This example illustrates that Theorem 3.10 works for reducible f .)

(ii) Proposition 3.6 implies that $d_{n-i} = (d - 1)^i$ for $1 \leq i < \text{codim}_{\mathbb{P}^n} \Sigma$. In the special case of a smooth irreducible hypersurface we have $\Sigma = \emptyset$ and therefore $d_{n-i} = (d - 1)^i$ for $1 \leq i \leq n$. Plugging this into the formula in Theorem 3.10, we retrieve Equation (1).

(iii) Consider $f = X_0 X_1 X_2$ with zero set Z in \mathbb{P}^2 . Note that Z is a singular hypersurface. In Example 1 we showed that $d_0 = 1, d_1 = 2$. Theorem 3.10 therefore gives $\chi(Z) = 2 + d_1 - d_0 = 3$. This can be easily verified using the principle of inclusion and exclusion: put $V_i := \mathcal{Z}(X_i) \simeq \mathbb{P}^1$. Then, for $i < j$, each $V_i \cap V_j$ consists of one point only and

$$\chi(Z) = \chi(V_0) + \chi(V_1) + \chi(V_2) - \chi(V_0 \cap V_1) - \chi(V_0 \cap V_2) - \chi(V_1 \cap V_2) = 3.$$

(iv) One can generalize the last example by considering the zero set $Z \subset \mathbb{P}^n$ of $f = X_0 X_1 \cdots X_n$. Note that the hypersurface Z is highly non-smooth. Its singular locus $\Sigma = \cup_{i < j} \mathcal{Z}_{\mathbb{P}^n}(X_i, X_j)$ is a subspace arrangement with an interesting combinatorial structure. The projective degrees of Z thus contain information about Σ which does not follow from $\deg Z$. It is an instructive exercise to prove that $d_i = \binom{n}{i}$ for $0 \leq i < n$ and to check the formula in Theorem 3.10. To compute $\chi(Z)$, note that $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ is homotopy equivalent to the circle S^1 and $(\mathbb{C}^*)^n \rightarrow \mathbb{P}^n \setminus Z, (x_1, \dots, x_n) \mapsto (1 : x_1 : \dots : x_n)$ is an isomorphism, hence $\chi(Z) = \chi(\mathbb{P}^n) - \chi((\mathbb{C}^*)^n) = n + 1$ since $\chi(S^1) = 0$.

3.4 Degree and homology

For readers familiar with algebraic topology we outline a characterization of the concepts of degree and projective degree in terms of homology. Details can be found in [18]. The contents of this subsection will not be used in the rest of this paper.

Recall first that for $0 \leq k \leq n$, the even homology groups $H_{2k}(\mathbb{P}^n)$ of the projective space \mathbb{P}^n are isomorphic to \mathbb{Z} and generated by the class $[L^{n-k}]$ of subspaces $L^{n-k} \in \mathbb{G}(k, n)$.

For any irreducible, k -dimensional, projective variety Z , the top homology class $H_{2k}(Z)$ is isomorphic to \mathbb{Z} and generated by the so called *fundamental class* μ_Z of Z .

Assume that Z is embedded in \mathbb{P}^n via $i: Z \rightarrow \mathbb{P}^n$. We denote by $[Z]$ the image of the fundamental class μ_Z under the push-forward $i_*: H_{2k}(Z) \rightarrow H_{2k}(\mathbb{P}^n)$. Then the degree of Z in \mathbb{P}^n can be characterized as the uniquely determined integer d such that $[Z] = d[L^{n-k}]$.

The projective degrees can be characterized similarly. From Künneth's formula [5, VI.1] it follows that $H_{2n}(\mathbb{P}^n \times \mathbb{P}^n)$ is torsion-free and generated by the classes $[L^{n-i} \times L^i]$. Let $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ be a rational map with closed graph Γ . The inclusion $i: \Gamma \hookrightarrow \mathbb{P}^n \times \mathbb{P}^n$ gives rise to a presentation $i_*(\mu_\Gamma) = \sum_{i=0}^n d_i [L^{n-i} \times L^i]$ and it turns out that d_0, \dots, d_{n-1} are the projective degrees of φ .

The preceding discussion can also be made in the context of algebraic geometry, using divisors and Chow groups instead of homology, see [16].

4 Generic quantifiers and generic reductions

Our goal here is to develop a formal complexity framework for the analysis of general position arguments related to counting problems in (semi)algebraic geometry. Implicitly, these ideas appear already in [8]. The key concept is that of a *generic parsimonious reduction*, which allows to make general position arguments as part of a reduction algorithm. A paradigmatic example is that of reducing the problem of computing the geometric degree of a variety V to $\text{HN}_{\mathbb{C}}$ by intersecting V with a generic linear subspace of complementary dimension. We are interested in problems where it is possible to compute in polynomial time a list of candidates for generic parameters, among which the majority is in fact “generic”. The latter list can be formalized by the notion of partial witness sequences, introduced in [8]. In order to achieve this, we require the genericity condition to be describable in terms of the constant-free polynomial hierarchy *over the reals*. Even though the focus here is on computational problems defined over \mathbb{C} , it is essential to allow the descriptive power of formulas over \mathbb{R} , as the polynomial hierarchy over the complex numbers has not enough expressive power for our purposes.

4.1 Generic parsimonious reductions

Let $S \subseteq \mathbb{R}^m$ be a semialgebraic subset. Using the generic universal quantifier \forall^* we will write $\forall^* a \in \mathbb{R}^m (a \in S)$ for expressing that S is dense in \mathbb{R}^m with respect to the Euclidean topology. This is equivalent to $\dim(\mathbb{R}^m - S) < m$.

The following definition is from [3, Chapter 21].

Definition 4.1 A subset $R \subseteq \mathbb{R}^\infty$ is said to be in Σ_k^0 for $k \in \mathbb{N}$, if there exists a relation $A \subseteq (\mathbb{R}^\infty)^{k+1}$, decidable in polynomial time by a constant-free machine over \mathbb{R} , and polynomials p_1, \dots, p_k , such that for $x \in \mathbb{R}^n$:

$$x \in R \Leftrightarrow Q_1 x_1 \in \mathbb{R}^{p_1(n)} \dots Q_k x_k \in \mathbb{R}^{p_k(n)} (x_1, \dots, x_k, x) \in A$$

where $Q_1 = \exists$ and the quantifiers $Q_i \in \{\exists, \forall\}$ alternate. We define the *constant-free polynomial hierarchy* $\text{PH}_{\mathbb{R}}^0$ to be the union $\text{PH}_{\mathbb{R}}^0 = \cup_k \Sigma_k^0$.

We call a relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ *balanced* if there is a polynomial p such that

$$R_m := R \cap (\mathbb{C}^m \times \mathbb{C}^\infty) \subseteq \mathbb{C}^m \times \mathbb{C}^{p(m)},$$

for all $m \in \mathbb{N}$. We say that the polynomial p is *associated* to R . Instead of $(u, a) \in R$ we will write shortly $R(u, a)$. In what follows we will identify \mathbb{C}^m with \mathbb{R}^{2m} and thus \mathbb{C}^∞ with \mathbb{R}^∞ in the obvious way. It therefore makes sense to say that a relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ is in $\text{PH}_{\mathbb{R}}^0$.

We define now generic parsimonious reductions, which extend the notion of parsimonious reductions. Hereby, we confine ourselves to the situation over \mathbb{C} , but we remark that a corresponding reduction can also be introduced over \mathbb{R} . This would lead to conceptual simplifications in some of the proofs of [8].

We denote by $\widehat{\mathbb{Z}} := \mathbb{Z} \cup \{-\infty, \infty, \text{nil}\}$ the union of the set \mathbb{Z} of integers with three additional symbols $-\infty, \infty$, and nil (the latter standing for undefined), cf. §4.3.

Definition 4.2 Let $\varphi, \psi: \mathbb{C}^\infty \rightarrow \widehat{\mathbb{Z}}$. A *generic parsimonious reduction* from φ to ψ consists of a pair (π, R) where $\pi: \mathbb{C}^\infty \times \mathbb{C}^\infty \rightarrow \mathbb{C}^\infty$ is computable in polynomial time by a constant-free machine over \mathbb{C} , and $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ is a balanced relation in $\text{PH}_{\mathbb{R}}^0$ such that, for all $m \in \mathbb{N}$, the following holds (where p is associated to R):

- (i) $\forall u \in \mathbb{C}^m \forall a \in \mathbb{C}^{p(m)} (R(u, a) \Rightarrow \varphi(u) = \psi(\pi(u, a))),$
- (ii) $\forall u \in \mathbb{C}^m \forall^* a \in \mathbb{C}^{p(m)} R(u, a).$

We write $\varphi \preceq_* \psi$ if there is a generic parsimonious reduction from φ to ψ .

Note that the definition above requires π to be computable by a machine over \mathbb{C} (and therefore, computable without the use of inequality testing) but allows the relation R to be definable in $\text{PH}_{\mathbb{R}}^0$ (where inequalities are allowed). The points $u \in \mathbb{C}^m$ and $a \in \mathbb{C}^{p(m)}$ are represented by points in \mathbb{R}^{2m} and $\mathbb{R}^{2p(m)}$ in the obvious way. This is a subtle point since, as will be apparent in what follows, the definability of R over \mathbb{R} is not an obstacle to our computability results over \mathbb{C} .

Lemma 4.3 *The generic parsimonious reduction \preceq_* is transitive.*

PROOF. Assume that $\varphi \preceq_* \psi$ via the reduction given by (π, R) and $\psi \preceq_* \chi$ via the reduction given by (ρ, S) . Define the function σ by $\sigma(u, a, b) := \rho(\pi(u, a), b)$ and the relation T by setting $T(u, a, b) \equiv R(u, a) \wedge S(\pi(u, a), b)$. We claim that (σ, T) provides a generic parsimonious reduction $\varphi \preceq_* \chi$.

Let p and q be the polynomials associated to R and S , respectively, and r be a polynomial such that $\pi(u, a) \in \mathbb{C}^{r(m)}$ for $u \in \mathbb{C}^m, a \in \mathbb{C}^{p(m)}$. It is easy to see that T is a balanced relation in $\text{PH}_{\mathbb{R}}^0$. Moreover, we have

$$\forall u \in \mathbb{C}^m \forall a \in \mathbb{C}^{p(m)} \forall b \in \mathbb{C}^{q(r(m))} (T(u, a, b) \Rightarrow \varphi(u) = \chi(\sigma(u, a, b))),$$

which gives Condition (i) in Definition 4.2. Finally,

$$(\forall u \in \mathbb{C}^m \forall^* a \in \mathbb{C}^{p(m)} R(u, a)) \wedge (\forall u \in \mathbb{C}^m \forall a \in \mathbb{C}^{p(m)} \forall^* b \in \mathbb{C}^{q(r(m))} S(\pi(u, a), b)),$$

which implies that

$$\forall u \in \mathbb{C}^m \forall^* a \in \mathbb{C}^{p(m)} \forall^* b \in \mathbb{C}^{q(r(m))} T(u, a, b),$$

hence Condition (ii) in Definition 4.2 is also satisfied. \square

4.2 Relation to Turing reduction

We are going to show that Turing reductions are stronger than generic parsimonious reductions. (The possibility to prove this is the main reason for allowing R to be in $\text{PH}_{\mathbb{R}}^0$ in the definition of generic parsimonious reductions.)

Theorem 4.4 *Let $\varphi, \psi: \mathbb{C}^\infty \rightarrow \widehat{\mathbb{Z}}$. If $\varphi \preceq_* \psi$, then φ Turing reduces to ψ .*

The proof relies on the elimination of generic quantifiers in parameterized formulas due to Koiran [24, 26], as well as its extension developed in [8]. We recall the definition of partial witness sequences from [8].

Definition 4.5 Let $R_m \subseteq \mathbb{R}^{2m} \times \mathbb{R}^k$ be a semialgebraic subset. A *partial witness sequence* for R_m is a sequence $(\alpha^{(1)}, \dots, \alpha^{(4m+1)})$ of points in \mathbb{R}^k such that

$$\forall u \in \mathbb{R}^{2m} \left((\forall^* a \in \mathbb{R}^k R_m(u, a)) \implies |\{i \in [4m+1] \mid R_m(u, \alpha^{(i)})\}| > 2m \right).$$

The next result, Theorem 4.6 below, is a consequence of [8, Theorem 4.9 and Remark 4.10].

Theorem 4.6 *Let $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ be a balanced relation in $\text{PH}_{\mathbb{R}}^0$. Then there is a constant-free machine over \mathbb{C} , which computes upon input $m \in \mathbb{N}$ a partial witness sequence α_m for $R_m(u, a)$ in time polynomial in m . \square*

Remark 4.7 The partial witness sequence α_m constructed in the proof of Theorem 4.6 is a sequence of integers obtained by repeated squaring, cf. [8, Theorem 4.9 and Remark 4.10]. Since some components of α_m have bit-size exponential in m , it follows that the computation of α_m is not possible in time polynomial in m in the classical setting of Turing machines. It follows, however, from the examination of the proof, that a system of equations $S_m(y, \alpha)$ with integer coefficients can be obtained by a Turing machine in time polynomial in m such that there exists a unique solution $(\bar{y}, \bar{\alpha})$ of $S_m(y, \alpha)$ with $\bar{\alpha} = \alpha_m$.

PROOF OF THEOREM 4.4. Let (π, R) provide a generic parsimonious reduction from φ to ψ . By Theorem 4.6, a partial witness sequence α_m for R_m can be computed by a machine over \mathbb{C} in time polynomial in m . Hence the following algorithm can be implemented as a polynomial time oracle Turing machine over \mathbb{C} :

```

input  $u \in \mathbb{C}^m$ 
compute a partial witness sequence  $(\alpha_m^{(1)}, \dots, \alpha_m^{(4m+1)})$  for  $R_m$ 
for  $i = 1$  to  $4m + 1$  do
  compute  $\pi(u, \alpha_m^{(i)})$ 
  get  $N_i := \psi(\pi(u, \alpha_m^{(i)}))$  by an oracle call to  $\psi$ 
compute the majority  $N$  of the numbers  $N_1, \dots, N_{4m+1}$ 
return  $N$ .

```

We now show that this algorithm indeed outputs $\varphi(u)$ on input $u \in \mathbb{C}^m$. Condition (ii) of Definition 4.2 states that $\forall^* a \in \mathbb{C}^{p(m)} R_m(u, a)$. Hence, since α_m is a partial witness sequence, $R_m(u, \alpha_m^{(i)})$ holds for the majority of the indices $i \in [4m + 1]$. On the other hand, by Condition (i) of Definition 4.2, we have for all $i \in [4m + 1]$,

$$R_m(u, \alpha_m^{(i)}) \Rightarrow \varphi(u) = \psi(\pi(u, \alpha_m^{(i)})).$$

Therefore, we have $\varphi(u) = \psi(\pi(u, \alpha^{(i)}))$ for the majority of the indices $i \in [4m + 1]$ as claimed. \square

4.3 Two generic counting complexity classes

In what follows we extend our definition of the class $\#P_{\mathbb{C}}$ to create new classes in between $\#P_{\mathbb{C}}$ and $\text{FP}_{\mathbb{C}}^{\#P_{\mathbb{C}}}$, which capture enough functions and yet retain a basic feature of $\#P_{\mathbb{C}}$ (see Lemma 4.11 below).

Recall the extended set $\widehat{\mathbb{Z}} := \mathbb{Z} \cup \{-\infty, \infty, \text{nil}\}$ of integers (nil standing for undefined). We extend the addition and multiplication of integers to maps $\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}} \rightarrow \widehat{\mathbb{Z}}$ by setting

$$\infty + (-\infty) := \text{nil}, \quad (-\infty) + \infty := \text{nil}, \quad 0 \cdot (\pm\infty) := 0, \quad (\pm\infty) \cdot 0 := 0,$$

and $a + b := \text{nil}$, $a \cdot b := \text{nil}$ if a or b equals nil. In all other cases, we define $a + b$ and $a \cdot b$ in the usual, intuitive way. It is straightforward to check that the addition and the product are both associative on $\widehat{\mathbb{Z}}$. The distributivity law may be violated: for instance $\infty = \infty \cdot (2 + (-1)) \neq \infty \cdot 2 + \infty \cdot (-1) = \text{nil}$. However, we have $a \cdot (b + c) = a \cdot b + a \cdot c$ for $a \in \mathbb{Z} \setminus \{0\}$, $b, c \in \widehat{\mathbb{Z}}$. We define the subtraction by $a - b := a + (-1) \cdot b$ for $a, b \in \widehat{\mathbb{Z}}$. The sum, the difference, and the product of two functions $\mathbb{C}^{\infty} \rightarrow \widehat{\mathbb{Z}}$ is defined pointwise.

The following definition is motivated by the class GapP , which is studied in classical complexity theory, see [14].

Definition 4.8 The class $\text{GAP}_{\mathbb{C}}$ consists of all functions $\gamma: \mathbb{C}^{\infty} \rightarrow \widehat{\mathbb{Z}}$ of the form $\gamma = \varphi - \psi$ for $\varphi, \psi \in \#\text{P}_{\mathbb{C}}$.

It is easy to see that the class $\text{GAP}_{\mathbb{C}}^*$ just consists of the difference of functions in $\#\text{P}_{\mathbb{C}}^*$. Moreover, it is obvious that the following natural problem is $\text{GAP}_{\mathbb{C}}$ -complete with respect to parsimonious reductions:

$\Delta\text{HN}_{\mathbb{C}}$ Given two finite families F_1, F_2 of complex multivariate polynomials, compute $|\mathcal{Z}(F_1)| - |\mathcal{Z}(F_2)|$.

We define now the closures of $\#\text{P}_{\mathbb{C}}$ and $\text{GAP}_{\mathbb{C}}$ with respect to generic parsimonious reductions. The resulting *generic counting complexity classes* $\#\text{P}_{\mathbb{C}}^*$ and $\text{GAP}_{\mathbb{C}}^*$ seem to capture more accurately the kind of counting problems encountered in algebraic geometry.

Definition 4.9 (i) The class $\#\text{P}_{\mathbb{C}}^*$ consists of all functions $\varphi: \mathbb{C}^{\infty} \rightarrow \mathbb{N} \cup \{\infty\}$ such that there exists $\psi \in \#\text{P}_{\mathbb{C}}$ with $\varphi \preceq_* \psi$.

(ii) The class $\text{GAP}_{\mathbb{C}}^*$ consists of all functions $\varphi: \mathbb{C}^{\infty} \rightarrow \widehat{\mathbb{Z}}$ such that there exists $\psi \in \text{GAP}_{\mathbb{C}}$ with $\varphi \preceq_* \psi$.

The following lemma lists some basic properties of the above defined classes.

Lemma 4.10 (i) *The class $\text{GAP}_{\mathbb{C}}$ is closed under parsimonious reductions.*

(ii) *The sum and the difference of two functions in $\text{GAP}_{\mathbb{C}}$ is in $\text{GAP}_{\mathbb{C}}$. The product of two finite valued functions in $\text{GAP}_{\mathbb{C}}$ is also in $\text{GAP}_{\mathbb{C}}$.*

(iii) *Both classes $\#\text{P}_{\mathbb{C}}^*$ and $\text{GAP}_{\mathbb{C}}^*$ are closed under generic parsimonious reductions.*

(iv) *The sum and the difference of two functions in $\text{GAP}_{\mathbb{C}}^*$ is in $\text{GAP}_{\mathbb{C}}^*$. The product of two finite valued functions in $\text{GAP}_{\mathbb{C}}^*$ is also in $\text{GAP}_{\mathbb{C}}^*$.*

(v) *We have the inclusions $\#\text{P}_{\mathbb{C}} \subseteq \#\text{P}_{\mathbb{C}}^*$ and $\#\text{P}_{\mathbb{C}} \subseteq \text{GAP}_{\mathbb{C}} \subseteq \text{GAP}_{\mathbb{C}}^* \subseteq \text{FP}_{\mathbb{C}}^{\#\text{P}_{\mathbb{C}}}$.*

(vi) *If φ is $\#\text{P}_{\mathbb{C}}$ -complete with respect to parsimonious reductions, then φ is $\#\text{P}_{\mathbb{C}}^*$ -complete with respect to generic parsimonious reductions.*

PROOF. (i) This follows immediately from the definition and the fact that $\#\text{P}_{\mathbb{C}}$ is closed under parsimonious reductions.

(ii) Let $\varphi, \psi \in \#\text{P}_{\mathbb{C}}$ and let M_{φ}, M_{ψ} and p, q be the polynomial time machines and polynomial bounds in Definition 2.2. Then, for all $u \in \mathbb{C}^m$,

$$(\varphi + \psi)(u) = \left| \left\{ (b, y, z) \in \mathbb{C}^{1+p(m)+q(m)} \mid (b = 0 \wedge y = 0 \wedge M_{\psi} \text{ accepts } (u, z)) \right. \right. \\ \left. \left. \vee (b = 1 \wedge z = 0 \wedge M_{\varphi} \text{ accepts } (u, y)) \right\} \right|,$$

$$(\varphi\psi)(u) = \left| \left\{ (y, z) \in \mathbb{C}^{p(m)+q(m)} \mid (M_{\psi} \text{ accepts } z \wedge M_{\varphi} \text{ accepts } y) \right\} \right|.$$

This shows that $\varphi + \psi$ and $\varphi\psi$ are in $\#P_{\mathbb{C}}$ and therefore, $\#P_{\mathbb{C}}$ is closed under taking sums and products. The claim about the product of functions is now obvious. Moreover, using the associativity of $+$ and the fact that $(-1) \cdot (b+c) = (-1) \cdot b + (-1) \cdot c$ for $b, c \in \widehat{\mathbb{Z}}$, it is straightforward to verify that $\text{GAP}_{\mathbb{C}}$ is closed under sums and differences. (The fact that the distributivity law does not hold generally is the reason to impose the finiteness restriction.)

(iii) This is an immediate consequence of the definition and Lemma 4.3.

(iv) We just prove the claim for the addition of functions. For the difference and the product one can argue similarly.

Let $\varphi, \psi \in \text{GAP}_{\mathbb{C}}^*$ and $\chi_1, \chi_2 \in \text{GAP}_{\mathbb{C}}$ such that $\varphi \preceq_* \chi_1$ and $\psi \preceq_* \chi_2$ with respect to the generic parsimonious reductions given by (π, R) and (ρ, S) , respectively. Let p, q be the polynomials associated to R and S . Then, for all $u \in \mathbb{C}^m$

$$\begin{aligned} \forall a \in \mathbb{C}^{p(m)} \quad & (R_m(u, a) \Rightarrow \varphi(u) = \chi_1(\pi(u, a))), \\ \forall b \in \mathbb{C}^{q(m)} \quad & (S_m(u, b) \Rightarrow \psi(u) = \chi_2(\rho(u, b))). \end{aligned}$$

Moreover, $\forall^* a \in \mathbb{C}^{p(m)} R_m(u, a)$ and $\forall^* b \in \mathbb{C}^{q(m)} S_m(u, b)$. By part (ii), the function χ defined by $\chi(u, v) := \chi_1(u) + \chi_2(v)$ is in $\text{GAP}_{\mathbb{C}}$. If we define the polynomial time function σ by $\sigma(u, a, b) := (\pi(u, a), \rho(u, b))$, then we have for all $u \in \mathbb{C}^m$

$$\forall a \in \mathbb{C}^{p(m)} \forall b \in \mathbb{C}^{q(m)} (R_m(u, a) \wedge S_m(u, b) \Rightarrow \varphi(u) + \psi(u) = \chi(\sigma(u, a, b))).$$

Moreover, $\forall^* a \in \mathbb{C}^{p(m)} \forall^* b \in \mathbb{C}^{q(m)} R_m(u, a) \wedge S_m(u, b)$. This shows the assertion (iv).

(v) This follows from Theorem 4.4.

(vi) This follows from Lemma 4.3. \square

One of the main features of $\text{GAP}_{\mathbb{C}}^*$ is that [8, Lemma 3.9] can be extended from $\#P_{\mathbb{C}}$ to this class. This result does not seem to hold instead for $\text{FP}_{\mathbb{C}}^{\#P_{\mathbb{C}}}$.

Lemma 4.11 *Let $\varphi: \mathbb{C}^\infty \times \{0, 1\}^\infty \rightarrow \widehat{\mathbb{Z}}$ be a function in $\text{GAP}_{\mathbb{C}}^*$ and q be a polynomial. Define the function $\tilde{\varphi}: \mathbb{C}^\infty \rightarrow \widehat{\mathbb{Z}}$ by setting for $u \in \mathbb{C}^m$*

$$\tilde{\varphi}(u) = \sum_{y \in \{0, 1\}^{q(m)}} \varphi(u, y)$$

Then $\tilde{\varphi}$ belongs to $\text{GAP}_{\mathbb{C}}^$. A similar statement holds for $\#P_{\mathbb{C}}^*$.*

PROOF. We first note that [8, Lemma 3.9] contains an analogous statement for functions in the class $\#P_{\mathbb{C}}$. From this, the corresponding statement immediately follows for functions in the class $\text{GAP}_{\mathbb{C}}$.

Let now $\varphi \in \text{GAP}_{\mathbb{C}}^*$ and $\psi \in \text{GAP}_{\mathbb{C}}$ such that $\varphi \preceq_* \psi$ via the reduction given by (π, R) . Let p be the polynomial associated to R . Then, for all $m \in \mathbb{N}$,

$$\forall u \in \mathbb{C}^m \forall y \in \{0, 1\}^{q(m)} \forall a \in \mathbb{C}^{p(m+q(m))} \left(R(u, y, a) \Rightarrow \varphi(u, y) = \psi(\pi(u, y, a)) \right)$$

and $\forall u \in \mathbb{C}^m \forall y \in \{0, 1\}^{q(m)} \forall^* a \in \mathbb{C}^{p(m+q(m))} R(u, y, a)$. The above formula implies

$$\forall u \in \mathbb{C}^m \forall a \in \mathbb{C}^{p(m+q(m))} \left(\bigwedge_{y \in \{0, 1\}^{q(m)}} R(u, y, a) \Rightarrow \tilde{\varphi}(u) = \tilde{\psi}(u, a) \right),$$

where the function $\tilde{\psi}$ is defined by $\tilde{\psi}(u, a) = \sum_{y \in \{0, 1\}^{q(m)}} \psi(\pi(u, y, a))$. It is now easy to see that $\tilde{\varphi} \preceq_* \tilde{\psi}$. On the other hand, the map

$$\mathbb{C}^\infty \times \{0, 1\}^\infty \times \mathbb{C}^\infty \rightarrow \widehat{\mathbb{Z}}, \quad (u, y, a) \mapsto \psi(\pi(u, y, a))$$

is in $\text{GAP}_{\mathbb{C}}$, since $\text{GAP}_{\mathbb{C}}$ is closed under parsimonious reductions (see Lemma 4.10). Since we already noted that the assertion of the lemma is true for the class $\text{GAP}_{\mathbb{C}}$, we obtain that $\tilde{\psi}$ belongs to $\text{GAP}_{\mathbb{C}}$ and hence, that $\tilde{\varphi} \in \text{GAP}_{\mathbb{C}}^*$. \square

5 Proofs of the main results

In this section we determine the complexity of the problems $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$, which were defined in the introduction. To do so, we will also deal with the following auxiliary problems:

PROJDEGREE $_{\mathbb{C}}$ (*Projective degrees*) Given homogeneous polynomials f_0, \dots, f_n in $\mathbb{C}[X_0, \dots, X_n]$ of the same degree and $i \in \mathbb{N}$, $0 \leq i < n$, compute the i th projective degree d_i of the rational map $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ defined by them.

#PROJQAS $_{\mathbb{C}}$ (*Counting points in projective quasialgebraic sets*) Given a quasialgebraic set $S \subseteq \mathbb{P}^n$, count the number of points in S , returning ∞ if this number is not finite.

#BIPROJQAS $_{\mathbb{C}}$ (*Counting points in biprojective quasialgebraic sets*) Given a quasialgebraic set $S \subseteq \mathbb{P}^n \times \mathbb{P}^n$, count the number of points in S , returning ∞ if this number is not finite.

Our main results show that $\text{PROJDEGREE}_{\mathbb{C}}$ is in $\#\text{P}_{\mathbb{C}}^*$ and that $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$ are $\text{GAP}_{\mathbb{C}}^*$ -complete with respect to Turing reductions. To prove them, we will need the following auxiliary result.

Lemma 5.1 *The problems #PROJQAS $_{\mathbb{C}}$ and #BIPROJQAS $_{\mathbb{C}}$ are in #P $_{\mathbb{C}}$.*

PROOF. The projective space \mathbb{P}^n can be partitioned as $\mathbb{P}^n = \bigsqcup_{i=0}^n \mathbb{E}_i$, where

$$\mathbb{E}_i = \{x \in \mathbb{P}^n \mid x_0 = \dots = x_{i-1} = 0, x_i \neq 0\} \simeq \mathbb{C}^{n-i}.$$

Let $\varphi(x_0, \dots, x_n)$ be the system of homogeneous polynomials describing $S \subseteq \mathbb{P}^n$. The above partition of \mathbb{P}^n induces a partition of S as a disjoint union of the quasialgebraic subsets of \mathbb{C}^{n+1} defined by the systems $\varphi_i := \varphi(0, \dots, 0, 1, x_{i+1}, \dots, x_n)$ of

(non homogeneous) polynomials. It follows that the number of points of S is equal to the number of points of the quasiagebraic subset of \mathbb{C}^{n+1} described by $\bigvee_{i=0}^n \varphi_i$. This reduces $\#\text{PROJQAS}_{\mathbb{C}}$ to $\#\text{QAS}_{\mathbb{C}}$ and thus shows that $\#\text{PROJQAS}_{\mathbb{C}} \in \#\text{P}_{\mathbb{C}}$. The proof for $\#\text{BIPROJQAS}_{\mathbb{C}}$ is similar. \square

5.1 Computing projective degrees

In this section we will prove the following result.

Proposition 5.2 *The problem $\text{PROJDEGREE}_{\mathbb{C}}$ is in $\#\text{P}_{\mathbb{C}}^*$.*

The proof will be based on the technical Lemma 5.3 stated below, whose proof is deferred to §5.3. In order to state this lemma, we need to introduce some notation.

Let $u \in \mathbb{C}^m$ be a vector parameterizing the homogeneous polynomials f_0, \dots, f_n and let $\Gamma^u = \Gamma_U^u \cup \Gamma_{\Sigma}^u \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be the graph associated to f_0, \dots, f_n as described in §3.1. Also, to a point $a \in \mathbb{C}^{i(n+1)}$ (seen as a matrix with i rows and $n+1$ columns), we associate the linear space L_a^i defined by $ax = 0$. Note that, for generic a , $\dim L_a^i = n+1-i$, i.e., $L_a \in \mathbb{G}(n-i, n)$. So, we will write L_a^i for an element in $\mathbb{G}(n-i, n)$ parameterized by a , even though for a thin subset of $\mathbb{C}^{i(n+1)}$, one has $L_a^i \notin \mathbb{G}(n-i, n)$. Similarly for $b \in \mathbb{C}^{(n-i)(n+1)}$ and L_b^{n-i} .

We define the following transversality relation for $m \in \mathbb{N}$ and $0 \leq i < n$:

$$\text{transv}_{m,n,i} := \left\{ (u, a, b) \in \mathbb{C}^{m+n(n+1)} \mid \Gamma_{\Sigma}^u \cap (L_a^i \times L_b^{n-i}) = \emptyset \wedge \Gamma_U^u \pitchfork (L_a^i \times L_b^{n-i}) \right\}$$

and write $\text{transv} := \bigcup_{m,n,i} \text{transv}_{m,n,i}$.

Lemma 5.3 *The relation transv is in $\text{PH}_{\mathbb{R}}^0$.*

PROOF OF PROPOSITION 5.2. We construct a generic parsimonious reduction (π, R) from $\text{PROJDEGREE}_{\mathbb{C}}$ to $\#\text{BIPROJQAS}_{\mathbb{C}}$. Let $0 \leq i < n$, $f_0, \dots, f_n \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous given by a parameter $u \in \mathbb{C}^m$ and let (L_a^i, L_b^{n-i}) be given by a parameter $(a, b) \in \mathbb{C}^{n(n+1)}$. The following formula expresses that $(p, q) \in L_a^i \times L_b^{n-i}$:

$$\text{memb}_L(p, q, a, b) := \bigwedge_{k=1}^i \left(\sum_{j=0}^n a_{k,j} p_j = 0 \right) \wedge \bigwedge_{\ell=1}^{n-i} \left(\sum_{j=0}^n b_{\ell,j} q_j = 0 \right).$$

Consider the bihomogeneous polynomial $F_{r,s} := Y_r f_s(X_0, \dots, X_n) - Y_s f_r(X_0, \dots, X_n)$ in the variables X_0, \dots, X_n and Y_0, \dots, Y_n . Then $(p, q) \in \Gamma_U^u$ can be described by the following formula:

$$\text{memb}_U(p, q, u) := \bigwedge_{0 \leq r < s \leq n} (F_{r,s}(p, q) = 0) \wedge \bigvee_{r=0}^n (f_r(p) \neq 0). \quad (2)$$

It follows that a description of the set $\Gamma_U^u \cap (L_a^i \times L_b^{n-i})$ can be computed in polynomial time from i, a, b and f_0, \dots, f_n by a constant-free machine. We define π as the function mapping (u, a, b) to the above description of the set $\Gamma_U^u \cap (L_a^i \times L_b^{n-i})$ and let $R := \text{transv}$ be the above defined relation, which, according to Lemma 5.3, is in $\text{PH}_{\mathbb{R}}^0$.

Part (i) of Proposition 3.4 shows that the number of solutions of $\pi(u, (a, b))$ is the i th projective degree of (f_0, \dots, f_n) , provided $R(u, a, b)$ holds. Part (ii) of Proposition 3.4 says that $\forall u \in \mathbb{C}^m \forall^*(a, b) \in \mathbb{C}^{n(n+1)} R(u, a, b)$. Therefore, (π, R) is a generic parsimonious reduction from $\text{PROJDEGREE}_{\mathbb{C}}$ to $\#\text{BIPROJQAS}_{\mathbb{C}}$ and the statement follows from Lemma 5.1. \square

5.2 The complexity of computing the Euler characteristic

We now prove Theorem 1.2, i.e., we prove that $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$ are $\text{GAP}_{\mathbb{C}}^*$ -complete for Turing reductions.

The next lemma proves the upper bounds in Theorem 1.2. To state it, we define the following auxiliary problem:

PHSEULER_ℂ (*Euler characteristic of projective hypersurfaces*) Given a nonconstant complex homogeneous polynomial, compute the Euler characteristic of its projective zero set.

Proposition 5.4 (i) $\text{PHSEULER}_{\mathbb{C}} \in \text{GAP}_{\mathbb{C}}^*$,

(ii) $\text{PROJEULER}_{\mathbb{C}} \in \text{GAP}_{\mathbb{C}}^*$,

(iii) $\text{EULER}_{\mathbb{C}} \in \text{GAP}_{\mathbb{C}}^*$.

PROOF. (i) Let $f \in \mathbb{C}[X_0, \dots, X_n]$ be an instance of $\text{PHSEULER}_{\mathbb{C}}$, that is, a nonconstant homogeneous polynomial. Put $d := \deg f$ and let $Z \subset \mathbb{P}^n$ denote the projective zero set of f . Let d_0, \dots, d_{n-1} be the projective degrees of the rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^n$ defined by the gradient $(\partial_0 f, \dots, \partial_n f)$ of f . Theorem 3.10 states that

$$\chi(Z) = \sum_{i=1}^n ((-1)^{i-1} d_{n-i} + 1).$$

Now consider the function

$$\varphi: \mathbb{C}^\infty \times \{0, 1\}^\infty \rightarrow \mathbb{Z}, \quad (Z, i) \mapsto \begin{cases} (-1)^{i-1} d_{n-i} + 1 & \text{if } 0 \leq i < n \\ 0 & \text{otherwise.} \end{cases}$$

By Proposition 5.2, the problem $\text{PROJDEGREE}_{\mathbb{C}}$ belongs to $\#\text{P}_{\mathbb{C}}^*$. Using Lemma 4.10, it follows that $\varphi \in \text{GAP}_{\mathbb{C}}^*$. Using now Lemma 4.11, we conclude that $\text{PHSEULER}_{\mathbb{C}}$ belongs to $\text{GAP}_{\mathbb{C}}^*$.

(ii) Let $f_1, \dots, f_r \in \mathbb{C}[X_0, \dots, X_n]$ be an instance of $\text{PROJEULER}_{\mathbb{C}}$. For an index set $I \subseteq [r]$ write Z_I for the projective zero set of the product $f_I := \prod_{i \in I} f_i$. Lemma 3.9 implies that $\chi(\mathcal{Z}_{\mathbb{P}^n}(f_1, \dots, f_r)) = \chi_+(f_1, \dots, f_r) - \chi_-(f_1, \dots, f_r)$, where

$$\chi_+ := \sum_{|I| \text{ odd}} \chi(Z_I), \quad \chi_- := \sum_{|I| > 0 \text{ even}} \chi(Z_I).$$

By part (i), $\text{PHSEULER}_{\mathbb{C}}$ belongs to $\text{GAP}_{\mathbb{C}}^*$. Therefore, Lemma 4.11 implies that both functions χ_+ and χ_- belong to $\text{GAP}_{\mathbb{C}}^*$ as well. This proves that $\text{PROJEULER}_{\mathbb{C}}$ belongs to $\text{GAP}_{\mathbb{C}}^*$.

(iii) Let $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$ be an instance of $\text{EULER}_{\mathbb{C}}$ and d be an upper bound on the degrees of these polynomials. Define the homogeneous polynomials F_i of degree $d+1$ by $F_i := X_0^{d+1} f_i(X_1/X_0, \dots, X_n/X_0)$ and put $Z := \mathcal{Z}_{\mathbb{P}^n}(F_1, \dots, F_r)$ and $U := Z \cap \{X_0 \neq 0\}$. The set U is homeomorphic to the affine zero set $\mathcal{Z}_{\mathbb{C}^n}(f_1, \dots, f_r)$. Moreover, by construction, we have $Z - U = \mathcal{Z}_{\mathbb{P}^n}(X_0) \simeq \mathbb{P}^{n-1}$. Proposition 3.8 implies that $\chi(U) = \chi(Z) - \chi(\mathbb{P}^{n-1}) = \chi(Z) - n$. The assertion (iii) therefore follows from (ii). \square

The next lemma gives the lower bounds in Theorem 1.2.

Lemma 5.5 *Both problems $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$ are $\#\text{P}_{\mathbb{C}}$ -hard for Turing reductions.*

PROOF. In the proof of part (iii) of Proposition 5.4 we already established a Turing reduction from $\text{EULER}_{\mathbb{C}}$ to $\text{PROJEULER}_{\mathbb{C}}$. To prove the hardness, we establish a Turing reduction from DEGREE to $\text{EULER}_{\mathbb{C}}$.

As usual, we parameterize an instance $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$ of DEGREE by its coefficient vector u . Let $Z_u \subseteq \mathbb{C}^n$ denote the affine zero set of these polynomials. Let $a \in \mathbb{C}^{n(n+1)}$ parameterize in the usual way a sequence of affine subspaces A_0, A_1, \dots, A_n of \mathbb{C}^n such that $\dim A_i = i$. Note that if Z_u is nonempty of codimension k , then for generic a , we have $A_i \cap Z_u = \emptyset$ for $i < k$, $A_k \cap Z_u \neq \emptyset$, $A_k \pitchfork Z_u$, and $\chi(A_k \cap Z_u) = |A_k \cap Z_u| = \deg Z_u$. Consider the set

$$R_{m,n} := \left\{ (u, a) \in \mathbb{C}^{m+n(n+1)} \mid \right. \\ \left. (Z_u = \emptyset) \vee \bigvee_{k=0}^n \bigwedge_{i < k} (A_i \cap Z_u = \emptyset \wedge A_k \cap Z_u \neq \emptyset \wedge A_k \pitchfork Z_u) \right\}. \quad (3)$$

According to [8, Lemma 5.9], the set $R := \bigcup_{m,n} R_{m,n}$ is expressible in $\text{PH}_{\mathbb{R}}^0$. Moreover, for fixed $u \in \mathbb{C}^m$, we have $\forall^* a \in \mathbb{C}^{n(n+1)} R_{m,n}(u, a)$.

We define now $\delta(u, a)$ to be the first nonzero element of the sequence

$$(\chi(Z_u \cap A_0), \dots, \chi(Z_u \cap A_n)),$$

if this is not the zero sequence; otherwise we put $\delta(u, a) := 0$. Note that $\delta(u, a)$ can be computed by a polynomial time machine making oracle calls to $\text{EULER}_{\mathbb{C}}$. By the previous reasonings we have that, for all u, a ,

$$R(u, a) \text{ holds} \Rightarrow \delta(u, a) = \deg Z_u.$$

As in the proof of Theorem 4.4 we can prove that the following algorithm computes the degree of Z_u .

```

input  $u \in \mathbb{C}^m$ 
compute a partial witness sequence  $\alpha_m = (\alpha_m^{(1)}, \dots, \alpha_m^{(4m+1)})$  for  $R_{m,n}(u, a)$ 
for  $i = 1$  to  $4m + 1$  do
  compute  $N_i := \delta(u, \alpha_m^{(i)})$  by making oracle calls to  $\text{EULER}_{\mathbb{C}}$ 
compute the majority  $N$  of the numbers  $N_1, \dots, N_{4m+1}$ 
return  $N$ 

```

Clearly, the algorithm can be implemented as a polynomial time Turing machine over \mathbb{C} making oracle calls to $\text{EULER}_{\mathbb{C}}$. \square

5.3 Expressing transversality in the polynomial hierarchy

The goal of this section is to prove Lemma 5.3.

For an irreducible variety $Z \subseteq \mathbb{P}^n \times \mathbb{P}^n$ given as the zero set of bihomogeneous polynomials f_1, \dots, f_r , we will write \widehat{Z} for the zero set of these polynomials in $\mathbb{C}^{n+1} \times \mathbb{C}^{n+1}$. Let $(p, q) \in Z$ and $\widehat{p}, \widehat{q} \in \mathbb{C}^{n+1}$ be affine representatives of p, q , respectively. From the homogeneity of the defining equations it follows that the tangent space of \widehat{Z} at $(\widehat{p}, \widehat{q})$ does not depend on the particular \widehat{p}, \widehat{q} chosen, and we may therefore write $T_{(p,q)}\widehat{Z}$.

Consider the canonical map $\pi: \widehat{Z} \setminus \{0\} \rightarrow Z$. At a point $(p, q) \in Z$, π induces a surjective map $d_{(p,q)}\pi: T_{(p,q)}\widehat{Z} \rightarrow T_{(p,q)}Z$ of the tangent spaces with kernel $p \times q$, which allows us to identify the tangent space $T_{(p,q)}Z$ with $T_{(p,q)}\widehat{Z}/(p \times q)$ in a natural way. Here $p \times q$ is the product of p and q as one-dimensional subspaces of \mathbb{C}^{n+1} .

For a projective linear subspace $L \subseteq \mathbb{P}^n$ we will write \widehat{L} for the corresponding linear subspace of \mathbb{C}^{n+1} .

Lemma 5.6 *Let Γ_U be the graph of a rational morphism $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ defined by polynomials f_0, \dots, f_n of the same degree. Let $0 \leq i < n$, $(L^i, L^{n-i}) \in \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$, and $(p, q) \in \Gamma_U \cap (L^i \times L^{n-i})$. Then $\Gamma_U \pitchfork_{(p,q)} (L^i \times L^{n-i})$ if and only if*

$$T_{(p,q)}\widehat{\Gamma}_U \cap (\widehat{L}^i \times \widehat{L}^{n-i}) = p \times q.$$

PROOF. Since the spaces Γ_U and $L^i \times L^{n-i}$ have complementary dimension in $\mathbb{P}^n \times \mathbb{P}^n$, we have $\Gamma_U \pitchfork_{(p,q)} (L^i \times L^{n-i})$ if and only if

$$T_{(p,q)}\Gamma_U \cap T_{(p,q)}(L^i \times L^{n-i}) = 0.$$

This is equivalent to $T_{(p,q)}\widehat{\Gamma}_U/(p \times q) \cap (\widehat{L}^i \times \widehat{L}^{n-i})/(p \times q) = 0$, which shows the assertion. \square

PROOF OF LEMMA 5.3. Denote by \mathbb{C}_*^{n+1} the set $\mathbb{C}^{n+1} \setminus \{0\}$ and write $\Gamma_U := \Gamma_U^u$. By Lemma 5.6, $\Gamma_U \pitchfork (L_a^i \times L_b^{n-i})$ if and only if

$$\begin{aligned} \forall p, q \in \mathbb{C}_*^{n+1} \quad & [((p, q) \in \widehat{\Gamma}_U \cap (\widehat{L}_a^i \times \widehat{L}_b^{n-i})) \Rightarrow (T_{(p,q)}\widehat{\Gamma}_U \cap (\widehat{L}_a^i \times \widehat{L}_b^{n-i}) = p \times q)] \\ & \wedge \dim L_a^i = n - i \wedge \dim L_b^{n-i} = i. \end{aligned}$$

The condition $(p, q) \in \widehat{\Gamma}_U \cap (\widehat{L}_a^i \times \widehat{L}_b^{n-i})$ is expressed by the formula $\text{memb}_U(p, q, u) \wedge \text{memb}_L(p, q, a, b)$ (see the proof of Proposition 5.2) and can thus be checked in polynomial time. Also, the last two statements concerning dimension can be checked in polynomial time.

Let $(p, q) \in \widehat{\Gamma}_U$ and $\xi, \eta \in \mathbb{C}^{n+1}$. Since locally at (p, q) the vanishing ideal of $\widehat{\Gamma}_U$ is given by the polynomials $F_{r,s}(X, Y)$ (cf. (2)), we have $(\xi, \eta) \in T_{(p,q)}\widehat{\Gamma}_U$ if and only if

$$\bigwedge_{0 \leq r < s \leq n} \left(\sum_{j=0}^n \xi_j \frac{\partial F_{r,s}}{\partial X_j}(p, q) + \sum_{k=0}^n \eta_k \frac{\partial F_{r,s}}{\partial Y_k}(p, q) = 0 \right).$$

More explicitly, this can be expressed by the following formula $\text{memb}_T(\xi, \eta, p, q, u)$:

$$\bigwedge_{0 \leq r < s \leq n} \left(\eta_r f_s(p) - \eta_s f_r(p) + \sum_{j=0}^n (\xi_j q_r \frac{\partial f_s}{\partial X_j}(p) - \xi_j q_s \frac{\partial f_r}{\partial X_j}(p)) = 0 \right).$$

Hence, $T_{(p,q)}\widehat{\Gamma}_U \cap (\widehat{L}_a^i \times \widehat{L}_b^{n-i}) = p \times q$ can be expressed as follows:

$$\forall \xi, \eta \in \mathbb{C}^{n+1} \quad \left((\xi, \eta) \in p \times q \iff \text{memb}_T(\xi, \eta, p, q, u) \wedge \text{memb}_L(\xi, \eta, a, b) \right).$$

This is a $\text{coNP}_{\mathbb{C}}^0$ -statement, in particular, it is expressible in $\text{PH}_{\mathbb{R}}^0$.

We next deal with the property $\Gamma_{\Sigma}^u \cap (L_a^i \times L_b^{n-i}) = \emptyset$. This property is equivalent to $\Gamma \cap (L_a^i \times L_b^{n-i}) \subseteq \Gamma_U$, which means that

$$\forall p, q \in \mathbb{C}_*^{n+1} \quad ((p, q) \in \overline{\Gamma}_U \cap (L_a^i \times L_b^{n-i}) \Rightarrow (p, q) \in \Gamma_U), \quad (4)$$

since Γ is the Zariski closure of Γ_U . To express this condition we use the fact [32] that Γ is also the closure of Γ_U with respect to the Euclidean topology. This topology can be defined by a metric in projective space as follows. Define, for $p, q \in \mathbb{C}_*^{n+1}$,

$$d_{\mathbb{P}^n}(p, q) = \arccos(|\langle p, q \rangle| / (\|p\| \cdot \|q\|)),$$

which is the angle between the vectors p and q . It is straightforward to check that this is well defined when considering p and q as elements in \mathbb{P}^n , that the usual properties of a metric are satisfied, and that the metric induced on the affine charts is equivalent to the Euclidean metric.

We note that “ $d_{\mathbb{P}^n}(p, q) < \varepsilon$ for sufficiently small $\varepsilon > 0$ ” is equivalent to “ $|\langle p, q \rangle| / (\|p\| \cdot \|q\|) \geq 1 - \delta$ for sufficiently small δ ” and thus can be expressed by a first order formula over \mathbb{R} . (It is not clear how to express condition (4) by a formula over \mathbb{C} .)

Condition (4) can now be expressed in $\text{PH}_{\mathbb{R}}^0$ as follows:

$$\forall p, q \in \mathbb{C}_*^{n+1} \forall \varepsilon > 0 \exists p', q' \in \mathbb{C}_*^{n+1} [\text{memb}_U(p', q', u) \wedge \text{memb}_L(p, q, a, b) \wedge d_{\mathbb{P}^n}(p, p') < \varepsilon \wedge d_{\mathbb{P}^n}(q, q') < \varepsilon \Rightarrow \text{memb}_U(p, q, u)].$$

The completes the proof. □

6 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{C} , we denote its restriction to integer inputs by $L^{\mathbb{Z}}$. This way, the discrete problems $\#\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$, $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$, etc. are well defined.

We present here completeness results for some of these problems in the Turing model. Also, we prove structural results of “transfer type” relating $\#\text{P}_{\mathbb{C}}$ with the corresponding counting complexity classes defined over algebraically closed fields of characteristic zero, as well as with its restrictions to binary inputs.

6.1 Boolean part of counting complexity classes

Determining Boolean parts 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 [6, 9, 10, 11, 22, 25]. The formal definition is the following.

Definition 6.1 Let \mathcal{C} be a complexity class over \mathbb{C} .

- (i) If \mathcal{C} is a class of counting functions $\mathbb{C}^{\infty} \rightarrow \widehat{\mathbb{Z}}$, then the class of functions $\{0, 1\}^{\infty} \rightarrow \widehat{\mathbb{Z}}$ obtained by restricting functions in \mathcal{C} to $\{0, 1\}^{\infty}$ is called the *Boolean part* $\text{BP}(\mathcal{C})$ of \mathcal{C} .
- (ii) If \mathcal{C} is a class of functions $\mathbb{C}^{\infty} \rightarrow \mathbb{C}^{\infty}$, then its *Boolean part* $\text{BP}(\mathcal{C})$ is defined as the class of functions $\{0, 1\}^{\infty} \rightarrow \{0, 1\}^{\infty}$, which can be obtained from functions in the class \mathcal{C} by restricting inputs to $\{0, 1\}^{\infty}$. Note that not all functions in \mathcal{C} yield functions in $\text{BP}(\mathcal{C})$ by restricting their inputs to $\{0, 1\}^{\infty}$.
- (iii) We denote by \mathcal{C}^0 the subclass of \mathcal{C} obtained by requiring all the considered machines over \mathbb{C} to be constant-free.
- (iv) The *constant-free Boolean part* of \mathcal{C} is defined as $\text{BP}^0(\mathcal{C}) := \text{BP}(\mathcal{C}^0)$.

In [8], the class of *geometric counting complex problems* GCC was defined as the constant-free Boolean part of $\#P_{\mathbb{C}}$. This is a class of Boolean counting problems, closed under parsimonious reductions, which can be located in a small region in the general landscape of Boolean complexity classes, namely,

$$\#P \subseteq \text{GCC} \subseteq \text{FPSPACE}.$$

We next show that GCC may be alternatively defined as the Boolean part of $\#P_{\mathbb{C}}$. That is, the restriction to constant-free machines is not necessary. (This was already claimed in [8, Remark 8.5].)

Lemma 6.2 *We have $\text{BP}(\#P_{\mathbb{C}}) = \text{GCC}$.*

For the proof we need the following lemma from [23].

Lemma 6.3 *For positive integers k, ℓ, d compute*

$$\alpha_1 := 2^\ell, \alpha_j := 1 + \alpha_1(d+1)^{j-1}\alpha_{j-1}^d \text{ for } 2 \leq j \leq k$$

from 1 by a straight-line program with $\mathcal{O}(k \log d + \log \ell)$ arithmetic operations. Then $h(\alpha_1, \dots, \alpha_k) \neq 0$ for any integer polynomial h in k variables of degree at most d and coefficients of absolute value less than 2^ℓ .

PROOF OF LEMMA 6.2. Let $\varphi: \{0, 1\}^\infty \rightarrow \mathbb{N} \cup \{\infty\}$ be in $\text{BP}(\#P_{\mathbb{C}})$. Then there is a polynomial p and a polynomial time machine M over \mathbb{C} such that, for all $x \in \{0, 1\}^n$, $\varphi(x) = |\{y \in \mathbb{C}^{p(n)} \mid M \text{ accepts } (x, y)\}|$. Without loss of generality [3, §7], we may assume that the machine constants $a_1, \dots, a_k \in \mathbb{C}$ are algebraically independent over \mathbb{Q} and that M does not perform divisions.

For $x \in \{0, 1\}^n$ let $g_x \in \mathbb{Z}[a_1, \dots, a_k]$ be the product of the (non-zero) test polynomials occurring along the computation path on input x . Moreover, define g_n to be the product of the g_x over all $x \in \{0, 1\}^n$. It is easy to see that both the degree and the bit size of the coefficients of g_n are bounded by $2^{n^{\mathcal{O}(1)}}$.

The following constant-free machine computes φ : On input $x \in \{0, 1\}^n$ compute a test vector $\alpha := (\alpha_1, \dots, \alpha_k) \in \mathbb{Z}^n$ satisfying $g_n(\alpha) \neq 0$. This can be done by a machine over \mathbb{C} in time polynomial in n by Lemma 6.3. Then simulate the computation of M by replacing the constants a_i by α_i . Note that the resulting machine has the same branching behavior as M . \square

We strengthen now the previous lemma by showing that, as far as Boolean parts are concerned, the generic class $\#P_{\mathbb{C}}^*$ does not introduce more power than $\#P_{\mathbb{C}}$ when considering Turing reductions.

Proposition 6.4 (i) $\text{BP}(P_{\mathbb{C}}^{\#P_{\mathbb{C}}^*}) = \text{BP}(P_{\mathbb{C}}^{\#P_{\mathbb{C}}}) = \text{PGCC}$.

(ii) $\text{BP}(\text{FP}_{\mathbb{C}}^{\#P_{\mathbb{C}}^*}) = \text{BP}(\text{FP}_{\mathbb{C}}^{\#P_{\mathbb{C}}}) = \text{FP}^{\text{GCC}}$.

The proof needs some preparations. In the following, the polynomial ring $R := \mathbb{Z}[a_1, \dots, a_k]$ in the indeterminates a_1, \dots, a_k will serve as a coefficient ring. For a polynomial $f \in R[X_1, \dots, X_n]$ and $\alpha \in \mathbb{C}^k$, we will write $f^\alpha \in \mathbb{Z}[X_1, \dots, X_n]$ for the polynomial obtained from f by specializing the vector of indeterminates (a_1, \dots, a_k) to α .

Lemma 6.5 *Let f_1, \dots, f_r be polynomials in $\mathbb{Z}[a_1, \dots, a_k, X_1, \dots, X_n]$ of total degree at most d and having coefficients of bit size at most ℓ . We suppose that the zero set of f_1, \dots, f_r over the algebraic closure K of the field of fractions of the ring $R := \mathbb{Z}[a_1, \dots, a_k]$ is finite. Then there is a polynomial $h \in \mathbb{Z}[a_1, \dots, a_k]$ with degree and bit size bounded by $(r\ell d^n)^{\mathcal{O}(1)}$ satisfying the following property: For all $\alpha \in \mathbb{C}^k$ such that $h(\alpha) \neq 0$, the system $f_1^\alpha = 0, \dots, f_r^\alpha = 0$ has the same number of solutions as the system $f_1 = 0, \dots, f_r = 0$.*

For proving this lemma, we require the following auxiliary result, which follows from [17, §3.4.7].

Lemma 6.6 *We assume the situation of Lemma 6.5. Then there exist integers $\gamma_1, \dots, \gamma_n$ and an irreducible univariate polynomial $g \in R[Y]$ such that*

$$\varphi: \mathcal{Z}_{K^n}(f_1, \dots, f_r) \rightarrow \mathcal{Z}_K(g), (x_1, \dots, x_n) \mapsto \gamma_1 x_1 + \dots + \gamma_n x_n$$

is a bijective map, whose inverse ψ is given by $y \mapsto \theta^{-1}(r_1(y), \dots, r_n(y))$ for some $\theta \in R \setminus 0$ and $r_1, \dots, r_n \in R[Y]$. The total degree and the bit size of the r_i , g , and θ can be bounded by $(r\ell d^n)^{\mathcal{O}(1)}$. (The bit size of γ_i can be bounded by $\mathcal{O}(n \log d + \log r)$.)

PROOF OF LEMMA 6.5. Let $h_1 \in R$ denote the product of θ , the discriminant of g , and of the leading coefficient of g . We are going to show that there exists a polynomial $h_2 \in R$ of the required size such that if $h_1(\alpha)h_2(\alpha) \neq 0$, then the map

$$\varphi^\alpha: \mathcal{Z}_{\mathbb{C}^n}(f_1^\alpha, \dots, f_r^\alpha) \rightarrow \mathcal{Z}_{\mathbb{C}}(g^\alpha), (x_1, \dots, x_n) \mapsto \gamma_1 x_1 + \dots + \gamma_n x_n$$

is bijective and its inverse ψ^α is given by $y \mapsto (\theta(\alpha)^{-1}r_1^\alpha(y), \dots, \theta(\alpha)^{-1}r_n^\alpha(y))$. This implies the desired assertion since g^α is square free and $\deg g = \deg g^\alpha$.

The polynomials $P_0 := g(\gamma_1 X_1 + \dots + \gamma_n X_n)$ and $P_k := r_k(\gamma_1 X_1 + \dots + \gamma_n X_n) - \theta X_k$ ($1 \leq k \leq n$) vanish on $Z := \mathcal{Z}_{K^n}(f_1, \dots, f_r)$. In fact, note that $(P_1(x), \dots, P_n(x)) = \theta(\psi(\varphi(x)) - x)$ for $x \in Z$. By the effective arithmetic Nullstellensatz (cf. [27]), there are representations

$$\rho_k P_k^{e_k} = u_{k,1} f_1 + \dots + u_{k,r} f_r, \quad 0 \leq k \leq n, \quad (5)$$

with positive integers e_k , polynomials $u_{k,j}$ over R , and nonzero $\rho_k \in R$ such that the degree and the bit size of ρ_k is bounded by $(\ell d^n)^{\mathcal{O}(1)}$. We define $h_2 := \rho_0 \dots \rho_n$ and put $h := h_1 h_2$. Then the degree and the bit size of h are bounded by $(r\ell d^n)^{\mathcal{O}(1)}$.

Assume that $h(\alpha) \neq 0$ and $x \in \mathcal{Z}_{\mathbb{C}^n}(f_1, \dots, f_r)$. Specializing a_j to α_j in Equation (5), we get $P_k^\alpha(x) = 0$ for all k , since $\rho_k(\alpha) \neq 0$. In particular, $P_0^\alpha(x) = 0$, which implies that the map φ^α is well defined.

The polynomials $Q_i := \theta^d f_i(\theta^{-1}r_1(Y), \dots, \theta^{-1}r_n(Y))$ and $Q_0 := \gamma_1 r_1(Y) + \dots + \gamma_n r_n(Y) - \theta Y$ vanish on $\mathcal{Z}_K(g)$. In fact, note that $Q_0(y) = \theta(\varphi(\psi(y)) - y)$ for $y \in \mathcal{Z}_K(g)$. Therefore, the irreducible polynomial g divides the Q_i in $R[Y]$. It follows that the map ψ^α is well defined. Moreover, the maps φ^α and ψ^α are inverse to each other. \square

PROOF OF PROPOSITION 6.4. (i) It is sufficient to show that $\text{BP}(\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}}) \subseteq \text{P}^{\text{GCC}}$. Namely, the reverse inclusion is straightforward and $\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}^*} = \mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}}$ by Lemma 4.10(v).

Claim 1. $\text{BP}(\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}}) \subseteq \text{BP}^0(\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}})$.

In order to prove this, let $S \subseteq \{0, 1\}^\infty$ be a set in $\text{BP}(\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}})$. Then, there exists a machine M deciding S in polynomial time with oracle $\#\text{HN}_{\mathbb{C}}$. Again, we may assume that the machine constants $a_1, \dots, a_k \in \mathbb{C}$ of M are algebraically independent over \mathbb{Q} and that M does not perform divisions.

Fix $c > 0$ and let $\alpha_1, \dots, \alpha_k$ be the integers of Lemma 6.3 for $\ell = d = 2^{n^c}$. We denote by M' the constant-free machine over \mathbb{C} , which first computes the α_i in polynomial time and then simulates M with the constants a_i replaced by α_i . From Lemma 6.5 and Lemma 6.3 we can deduce that the machine M' will still decide S on all inputs $x \in \{0, 1\}^\infty$, provided $c > 0$ is sufficiently large. This shows that $S \in \text{BP}^0(\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}})$ and shows Claim 1.

Claim 2. $\text{BP}^0(\mathbb{P}_{\mathbb{C}}^{\#\mathbb{P}_{\mathbb{C}}}) \subseteq \text{P}^{\text{GCC}}$.

In order to prove this, let M be a constant-free machine over \mathbb{C} deciding $S \subseteq \{0, 1\}^\infty$ in polynomial time with oracle $\#\text{HN}_{\mathbb{C}}$. As before, we may assume that M does not perform divisions.

At any moment of the computation of M with input $x \in \{0, 1\}^n$, the value z of any intermediately computed quantity can be described by a division-free straight-line program ζ with n input variables, and length polynomial in n , in the sense that $z = \zeta(x)$.

To such a ζ we can associate in polynomial time a system of equations $\varphi_\zeta(x, y)$ in x and new variables y_1, \dots, y_m such that, for all $x^* \in \{0, 1\}^n$, $\varphi_\zeta(x, y)$ has a unique solution (x^*, y^*) and $y_m^* = \zeta(x^*)$. Therefore, for all $x \in \{0, 1\}^n$, the system $\{\varphi_\zeta(x, y), y_m = 0\}$ has either one solution or none at all and

$$\zeta(x) = 0 \iff |\{y \in \mathbb{C}^m \mid \varphi_\zeta(x, y), y_m = 0\}| = 1.$$

We use this construction in the following Turing machine deciding S .

input $x \in \{0, 1\}^\infty$
 simulate the computation of M instead of actually performing arithmetic
 (by keeping straight-line program representations of intermediate results)
 when reaching a test node
 if the tested value is z query $\#\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$ with input
 $\{\varphi_{\zeta}(x, y), y_m = 0\}$
 when reaching a query node
 if the input to the query is a system of equations $f_1 = 0, \dots, f_r = 0$
 whose coefficients are z_1, \dots, z_s
 query $\#\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$ with input $\{f_1^y = 0, \dots, f_r^y = 0, \varphi_{\zeta_1}(x, y^{(1)}), \dots, \varphi_{\zeta_s}(x, y^{(s)})\}$
 (where f_{ρ}^y is obtained from f_{ρ} by replacing z_j by $y_{m_j}^{(j)}$, $j = 1, \dots, s$)

This machine runs in polynomial time and queries $\#\text{HN}_{\mathbb{C}}^{\mathbb{Z}} \in \text{GCC}$. This shows $\text{BP}(\text{P}_{\mathbb{C}}^{\#\text{P}_{\mathbb{C}}}) \subseteq \text{PGCC}$.

(ii) The assertion about functional classes follows by applying part (i) to the components of any function in $\text{BP}(\text{FP}_{\mathbb{C}}^{\#\text{P}_{\mathbb{C}}})$. \square

Remark 6.7 Let $\varphi, \psi: \{0, 1\}^\infty \rightarrow \widehat{\mathbb{Z}}$. It is natural to define a notion of *randomized parsimonious reduction* from φ to ψ as a pair (π, R) where $\pi: \{0, 1\}^\infty \times \{0, 1\}^\infty \rightarrow \{0, 1\}^\infty$ is computable in polynomial time by a Turing machine, and $R \subseteq \{0, 1\}^\infty \times \{0, 1\}^\infty$ is a balanced relation such that, for all $m \in \mathbb{N}$, the following holds (where p, q are polynomials and p is associated to R):

- (i) $\forall u \in \{0, 1\}^m \forall a \in \{0, 1\}^{p(m)} (R(u, a) \Rightarrow \varphi(u) = \psi(\pi(u, a)))$,
- (ii) $\forall u \in \{0, 1\}^m \text{Prob}\{a \in \{0, 1\}^{p(m)} \mid \neg R(u, a)\} \leq 2^{-q(m)}$.

As in the proof of Proposition 6.4 one may show that for any φ in $\text{BP}(\#\text{P}_{\mathbb{C}}^*)$ there exists a randomized parsimonious reduction from φ to $\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$. Recall from the proof that the intermediate results of the computation are integers represented by straight-line programs. The point is now that testing those for zero can be done in coRP [21]. We leave the verification of the details to the reader. Similarly, for any φ in $\text{BP}(\text{GAP}_{\mathbb{C}}^*)$ there exists a randomized parsimonious reduction from φ to $\Delta\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$.

6.2 Completeness of Euler characteristic in the Turing model

Recall that the problems $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ and $\text{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$ are defined by restricting the input polynomials in the corresponding problems over \mathbb{C} to have integer coefficients.

Theorem 6.8 *Both problems $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ and $\text{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$ are in $\text{BP}(\text{GAP}_{\mathbb{C}}^*) \subseteq \text{FP}^{\text{GCC}}$. They are both FP^{GCC} -complete with respect to Turing reductions.*

Remark 6.9 By Remark 6.7 there are randomized parsimonious reductions from both problems $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ and $\text{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$ to the problem $\Delta\text{HN}_{\mathbb{C}}^{\mathbb{Z}}$. In other words, given a family F of polynomials with integer coefficients, it is possible to compute from this in randomized polynomial time two further families G_1, G_2 of such polynomials such that the Euler characteristic of $\mathcal{Z}(F)$ equals $|\mathcal{Z}(G_1)| - |\mathcal{Z}(G_2)|$.

PROOF OF THEOREM 6.8. The upper bounds follow directly from Proposition 5.4. Note that $\text{BP}(\text{GAP}_{\mathbb{C}}^*) \subseteq \text{FP}^{\text{GCC}}$ is a consequence of Proposition 6.4.

For the hardness, note that the Turing reduction from $\text{EULER}_{\mathbb{C}}$ to $\text{PROJEULER}_{\mathbb{C}}$ described in Proposition 5.4(iii) yields a classical Turing reduction from $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ to $\text{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$.

In the following, we argue that after some little modification, the Turing reduction from DEGREE to $\text{EULER}_{\mathbb{C}}$ given in Lemma 5.5 yields a classical Turing reduction from $\text{DEGREE}^{\mathbb{Z}}$ to $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$. Together with the completeness of $\text{DEGREE}^{\mathbb{Z}}$ in FP^{GCC} [8, Theorem 8.7(i)], the assertion will then follow.

Since we are now considering integer polynomials f_1, \dots, f_r , we can bound size of the formula describing the semialgebraic set $R_{m,n}$ introduced in Equation (3) by taking into account a bound on the bit-size of the components of the given f_i . Therefore, the coefficient vector u does not need to be considered as a parameter any more and we may take $m = 0$. The partial witness sequence for $R_{m,n}$ then consists of a single vector $\alpha \in \mathbb{Z}^{n(n+1)}$. Recall that $a \in \mathbb{C}^{n(n+1)}$ parameterizes a sequence of affine subspaces A_0, A_1, \dots, A_n of \mathbb{C}^n such that $\dim A_i = i$.

The straight-line computation for α 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 along the recursive description in Lemma 6.3. More specifically, we can compute in polynomial time a system of polynomial equations $S_n(a, y)$ in $a \in \mathbb{C}^{n(n+1)}$ and new variables $y_1, \dots, y_{q(n)}$ such that $S_n(a, y)$ is solvable if and only if $a = \alpha$. In the latter case, y is uniquely determined. Note that

$$\{(x, a, y) \in \mathbb{C}^n \times \mathbb{C}^{n(n+1)} \times \mathbb{C}^{q(n)} \mid (x \in Z_u \cap A_i) \wedge S_n(a, y)\} \rightarrow Z_u \cap A_i, (x, a, y) \mapsto x$$

is a homeomorphism for each i .

The following algorithm provides a classical Turing reduction from $\text{DEGREE}^{\mathbb{Z}}$ to $\text{EULER}_{\mathbb{C}}^{\mathbb{Z}}$. Given integer polynomials f_1, \dots, f_r , for $0 \leq i \leq n$, query $\text{EULER}_{\mathbb{R}}^{\mathbb{Z}}$ for the systems of equations in x, a, y expressing that $(x \in Z_u \cap A_i) \wedge S_n(a, y)$ and return the first nonzero element of the sequence $(\chi(Z_u \cap A_0), \dots, \chi(Z_u \cap A_n))$, if this is not the zero sequence; otherwise return 0. \square

We remark that instead of using Proposition 6.4, one could give more direct proofs of the membership in Theorem 6.8 by directly inspecting the corresponding membership proofs for the problems over \mathbb{C} .

6.3 A transfer result for counting classes

Although emphasis was put on the cases $R = \mathbb{R}$ and $R = \mathbb{C}$, the complexity theory developed in [4] was over an arbitrary ring R . An immediate question arising from this framework was whether, for instance, the problems $\text{P}_K \stackrel{?}{=} \text{NP}_K$ and $\text{P}_{\mathbb{C}} \stackrel{?}{=} \text{NP}_{\mathbb{C}}$ have the same answer when K is an algebraically closed field of characteristic zero. In [2] (see also [3, §7]) it was shown that this is actually the case. The next proposition extends this transfer result to the setting of counting classes (the classes therein being defined in the obvious way). The proof is a simple extension of the one in [2] so we only sketch it.

Proposition 6.10 *Let $K \subseteq L$ be an extension of algebraically closed fields of characteristic zero. Then $\#P_K \subseteq \text{FP}_K$ if and only if $\#P_L \subseteq \text{FP}_L$.*

PROOF. We denote by $\#\text{HN}_K$ and $\#\text{HN}_L$ the versions of the algebraic point counting problem over K and L , respectively. The proof of [8, Theorem 3.4] carries over to show that these problems are complete in $\#P_K$ and $\#P_L$, respectively.

(\Rightarrow) If $\#P_K \subseteq \text{FP}_K$ then $\#\text{HN}_K \in \text{FP}_K$. Let M be a machine over K solving $\#\text{HN}_K$ in polynomial time. We claim that M , considered as a machine over L , solves $\#\text{HN}_L$ (also in polynomial time). The proof of this claim follows exactly the same lines as the proof of the main result in [3, §7.8] which we now briefly recall.

For given $n, r \geq 1$ and $d = (d_1, \dots, d_r) \in \mathbb{N}^r$, let $N := \sum_{i=1}^r \binom{n+d_i}{n}$ and parameterize a system of polynomials $f_1^u, \dots, f_r^u \in \Omega[X_1, \dots, X_n]$ with $\deg f_i = d_i$ over a field Ω by the vector $u \in \Omega^N$ of the coefficients of the f_i . For all $k \geq 0$, there exists a first order formula $\varphi_{(n,r,d)}^k(U)$ in the language of fields with constants for 0 and 1 and with N free variables U_1, \dots, U_N and such that, for all for all fields Ω and all $u \in \Omega^N$,

$\varphi_{(n,r,d)}^k(u)$ expresses that the system $f_1^u = 0, \dots, f_r^u = 0$ has at least k different solutions in Ω^n .

Also, for all $k \geq 0$, there exists a formula $\mu_{(n,r,d)}^k(U)$, with N free variables and possibly with constants from K , such that

$\mu_{(n,r,d)}^k(u)$ expresses that the machine M with input u returns k .

Since M solves $\#\text{HN}_K$, for every $k \geq 0$ the field K satisfies the sentence

$$\forall u_1 \dots \forall u_N [(\varphi_{(n,r,d)}^k(u) \wedge \neg \varphi_{(n,r,d)}^{k+1}(u)) \iff \mu_{(n,r,d)}^k(u)].$$

By the model completeness of the theory of algebraically closed fields [29] it follows that L also satisfies these sentences. But this implies that, for all $k \geq 0$ and all systems $f_1, \dots, f_r \in L[X_1, \dots, X_n]$, the system has k solutions if and only if M returns k with input the coefficient vector u of f . Since the only other possible output of M is ∞ we deduce that M returns ∞ if and only if the system has infinitely

many solutions. This proves the claim and, with it, it shows that $\#\text{HN}_L \in \text{FP}_L$ and therefore $\#\text{P}_L \subseteq \text{FP}_L$.

(\Leftarrow) Proposition 9 in [3, §7] states that if a machine M computes a function $\varphi: L^\infty \rightarrow \{0, 1\}$ then there exists a machine M' over K computing the restriction $\varphi|_K$ whose running time is bounded by a polynomial in the running time of M . By coding $\mathbb{N} \cup \{\infty\}$ as $\{0, 1\}^\infty$ and taking components, it follows that the same result holds for functions $\varphi: L^\infty \rightarrow \mathbb{N} \cup \{\infty\}$.

Assume that $\#\text{P}_L \subseteq \text{FP}_L$. Then $\#\text{HN}_L \in \text{FP}_L$ and, by the previous remark, the restriction of $\#\text{HN}_L$ to K can be solved in FP_K . It thus only remains to be seen that this restriction is precisely $\#\text{HN}_K$. But this follows similarly as before from the model completeness of the theory of algebraically closed fields. \square

Appendix

The goal is to give a proof of Proposition 3.4. We start with a definition of the concepts of regular points and regular values, tailored to our situation of not necessarily smooth varieties.

Definition A.1 Let $\varphi: X \rightarrow Y$ be a surjective morphism of irreducible complex projective varieties of the same dimension. We call a point $p \in X$ a *regular point* of φ if p is a smooth point of X and $d_p\varphi: T_pX \rightarrow T_{\varphi(p)}Y$ is an isomorphism (and hence $\varphi(p)$ is smooth in Y). We call a point $q \in Y$ a *regular value* of φ if all $p \in \varphi^{-1}(q)$ are regular points of φ .

Lemma A.2 Let $\varphi: X \rightarrow Y$ be a surjective morphism of irreducible complex projective varieties of the same dimension. Then all fibres of regular values of φ have the same finite cardinality.

PROOF. In [32, Cor. 4.16] it is proved that any nonempty Zariski open subset of an irreducible complex projective variety is connected in the Euclidean topology. Sard's lemma [32, 3.7] implies that the set R of regular values of φ is a nonempty Zariski open subset of Y . Therefore, R is connected. It is thus sufficient to prove that the function $\psi: R \rightarrow \mathbb{N}, y \mapsto |\varphi^{-1}(y)|$ is well defined and locally constant.

Let $y \in R$. The inverse function theorem implies that $\varphi^{-1}(y)$ is discrete. Since it is also compact, it must be finite. So, ψ is well defined. Let $\varphi^{-1}(y) = \{x_1, \dots, x_k\}$. By the inverse function theorem there exists an open neighbourhood $\Omega \subseteq Y$ of y and pairwise disjoint open neighbourhoods V_1, \dots, V_k of x_1, \dots, x_k , respectively, such that $\varphi^{-1}(\Omega) = V_1 \cup \dots \cup V_k$ and $\varphi|_{V_j}: V_j \rightarrow \Omega$ is an isomorphism for all i . Since $|\varphi^{-1}(y')| = k$ for all $y' \in \Omega$, it follows that ψ is locally constant. \square

Recall that the Grassmannian $\mathbb{G}(k, n)$ is an irreducible smooth projective variety of dimension $\dim \mathbb{G}(k, n) = (k+1)(n-k)$, cf. [18].

Lemma A.3 Let $\Gamma \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be an irreducible projective variety of dimension n and $0 \leq i \leq n$. Define the closed subvariety

$$\Phi := \{(p, q, L^i, L^{n-i}) \mid (p, q) \in \Gamma \cap (L^i \times L^{n-i})\} \subseteq \Gamma \times \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$$

and let $\pi_2: \Phi \rightarrow \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$ be the projection on the second factor.

- (i) The incidence relation Φ is an irreducible projective variety of dimension $\dim \Phi = \dim(\mathbb{G}(n-i, n) \times \mathbb{G}(i, n)) = 2i(n-i) + n$.
- (ii) Let (p, q) be a smooth point of Γ and $(L^i, L^{n-i}) \in \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$. Then $\Gamma \pitchfork_{(p,q)} (L^i \times L^{n-i})$ holds if and only if (p, q, L^i, L^{n-i}) is a regular point of the projection π_2 .

PROOF. (i) Consider the projection $\pi_1: \Phi \rightarrow \Gamma$ onto the first factor. For any $(p, q) \in \Gamma$, we have the following isomorphism of varieties

$$\begin{aligned} \pi_1^{-1}(p, q) &\simeq \{L^i \in \mathbb{G}(n-i, n) \mid p \in L^i\} \times \{L^{n-i} \in \mathbb{G}(i, n) \mid q \in L^{n-i}\} \\ &\simeq \mathbb{G}(n-i-1, n-1) \times \mathbb{G}(i-1, n-1). \end{aligned}$$

This is an irreducible variety of dimension $\dim \pi_1^{-1}(p, q) = 2i(n-i)$ (we use the convention $\mathbb{G}(-1, m) := \emptyset$). Using [18, Theorem 11.14], it follows that Φ is irreducible and

$$\dim \Phi = \dim \Gamma + \dim \pi_1^{-1}(p, q) = n + 2i(n-i) = \dim(\mathbb{G}(n-i, n) \times \mathbb{G}(i, n)).$$

(ii) We may assume without loss of generality that $p = q = (1: 0: \dots: 0)$, $L^i = \mathcal{Z}_{\mathbb{P}^n}(X_{n-i+1}, \dots, X_n)$, and $L^{n-i} = \mathcal{Z}_{\mathbb{P}^n}(Y_{i+1}, \dots, Y_n)$. Moreover, since the assertion is local, we may work with the affine neighborhoods $\{X_0 \neq 0\} \simeq \mathbb{C}^n$ and $\{Y_0 \neq 0\} \simeq \mathbb{C}^n$ of p and q in \mathbb{P}^n , respectively. Let $\tilde{\Gamma} \subseteq \mathbb{C}^n \times \mathbb{C}^n$ be the subvariety thus corresponding to Γ .

For a matrix $a \in \mathbb{C}^{i \times (n+1-i)}$ let $L_a^i \subseteq \mathbb{C}^n$ be the zero set of the affine polynomials

$$\begin{aligned} g_1 &:= a_{1,0} + a_{1,1}X_1 + \dots + a_{1,n-i}X_{n-i} - X_{n-i+1}, \\ &\vdots \\ g_i &:= a_{i,0} + a_{i,1}X_1 + \dots + a_{i,n-i}X_{n-i} - X_n. \end{aligned}$$

(Note that this notation L_a^i slightly differs from the one used in §5.) It is well known that [18, Lecture 6]

$$\mathbb{C}^{i \times (n+1-i)} \rightarrow \mathbb{G}(n-i, n), \quad a \mapsto L_a^i$$

gives local isomorphisms of sufficiently small neighborhoods of 0 to neighborhoods of $L^i = L_0^i$ in $\mathbb{G}(n-i, n)$. An analogous statement holds for

$$\mathbb{C}^{(n-i) \times (i+1)} \rightarrow \mathbb{G}(i, n), \quad b \mapsto L_b^{n-i},$$

where the affine space L_b^{n-i} is defined as the zero set of the affine polynomials

$$\begin{aligned} g_{i+1} &:= b_{1,0} + b_{1,1}Y_1 + \cdots + b_{1,i}Y_i - Y_{i+1}, \\ &\vdots \\ g_n &:= b_{n-i,0} + b_{n-i,1}Y_1 + \cdots + b_{n-i,i}Y_i - Y_n. \end{aligned}$$

This induces the following local isomorphism φ around the origin:

$$\begin{aligned} \varphi: \mathbb{C}^n \times \mathbb{C}^n \times \mathbb{C}^{i \times (n+1-i)} \times \mathbb{C}^{(n-i) \times (i+1)} &\rightarrow \mathbb{P}^n \times \mathbb{P}^n \times \mathbb{G}(n-i, n) \times \mathbb{G}(i, n), \\ (x, y, a, b) &\mapsto ((1: x_1: \cdots: x_n), (1: y_1: \cdots: y_n), L_a^{n-i}, L_b^i). \end{aligned}$$

Assume now that (p, q) is a smooth point of Γ . Let f_1, \dots, f_n be polynomials in $X_1, \dots, X_n, Y_1, \dots, Y_n$ having the zero set $\tilde{\Gamma} \subseteq \mathbb{C}^n \times \mathbb{C}^n$ locally around $(0, 0)$ such that the differentials df_1, \dots, df_n at $(0, 0)$ are linearly independent (this is possible, see [32]). Let $\tilde{\Phi}$ denote the zero set of $f_1, \dots, f_n, g_1, \dots, g_n$ in $\mathbb{C}^n \times \mathbb{C}^n \times \mathbb{C}^{i \times (n+1-i)} \times \mathbb{C}^{(n-i) \times (i+1)}$. Then the map φ gives a local isomorphism of $\tilde{\Phi}$ to Φ around the origin.

The differentials of the g_i at the origin satisfy

$$\begin{aligned} d_0g_1 &= d_0a_{1,0} - d_0X_{n-i+1}, \dots, d_0g_i = d_0a_{i,0} - d_0X_n, \\ d_0g_{i+1} &= d_0b_{1,0} - d_0Y_{i+1}, \dots, d_0g_n = d_0b_{n-i,0} - d_0Y_n. \end{aligned}$$

Clearly, these differentials are linearly independent of d_0f_1, \dots, d_0f_n . Therefore, the tangent space of $\tilde{\Phi}$ at 0 is given by the zero set of $d_0f_1, \dots, d_0f_n, d_0g_1, \dots, d_0g_n$. In particular, we get $\dim T_0\tilde{\Phi} = \dim \tilde{\Phi}$ and hence 0 is a smooth point of $\tilde{\Phi}$.

Let $\tilde{\pi}_2: \tilde{\Phi} \rightarrow \mathbb{C}^{i \times (n+1-i)} \times \mathbb{C}^{(n-i) \times (i+1)}$ denote the projection onto the second factor. Then the above description of the differentials shows that the kernel of

$$d_0\tilde{\pi}_2: T_0\tilde{\Phi} \rightarrow \mathbb{C}^{i \times (n+1-i)} \times \mathbb{C}^{(n-i) \times (i+1)}, (\xi, \eta, \alpha, \beta) \mapsto (\alpha, \beta)$$

is isomorphic to $T_{(0,0)}\tilde{\Gamma} \cap (L_0^i \times L_0^{n-i})$. Hence 0 is a regular point of $\tilde{\pi}_2$ if and only if $\tilde{\Gamma}$ and $L_0^i \times L_0^{n-i}$ intersect transversally at 0, which was to be shown. \square

PROOF OF PROPOSITION 3.4. Let $\Gamma \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be the closure of the graph of a rational map $\varphi: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$. Fix $0 \leq i < n$ and consider the incidence relation

$$\Phi := \{(p, q, L^i, L^{n-i}) \mid (p, q) \in \Gamma \cap (L^i \times L^{n-i})\} \subseteq \Gamma \times \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$$

introduced in Lemma A.3. Then the projection $\pi_2: \Phi \rightarrow \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$ satisfies all the assumptions of Lemma A.2. Hence there is an integer d_i such that all fibres of π_2 at regular values (L^i, L^{n-i}) have cardinality d_i .

(i) If $\Gamma_U \cap (L^i \times L^{n-i})$ and $\Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$, then all $(p, q) \in \pi_2^{-1}(L^i, L^{n-i})$ are in Γ_U and thus smooth points of Γ . Hence (p, q, L^i, L^{n-i}) is a regular value of π_2 by Lemma A.3. Therefore,

$$d_i = |\pi_2^{-1}(L^i, L^{n-i})| = |\Gamma_U \cap (L^i \times L^{n-i})|$$

which shows claim (i).

For part (ii), note first that the property $\Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$ holds for generic (L^i, L^{n-i}) since $\dim \Gamma_\Sigma < n$. Moreover, if $\Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$ holds, then Lemma A.3 implies that $\Gamma_U \pitchfork (L^i \times L^{n-i})$ if and only if (L^i, L^{n-i}) is a regular value of π_2 . Hence the claim (ii) follows from Sard's lemma [32, 3.7]. \square

Acknowledgments. We are grateful to Joachim von zur Gathen for pointing out to us Aluffi's article [1].

References

- [1] P. Aluffi. Computing characteristic classes of projective schemes. *J. Symbolic Comput.*, 35(1):3–19, 2003.
- [2] 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.
- [3] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer, 1998.
- [4] 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.
- [5] G. E. Bredon. *Topology and Geometry*, volume 139 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1997.
- [6] P. Bürgisser. Cook's versus Valiant's hypothesis. *Theoret. Comp. Sci.*, 235:71–88, 2000.
- [7] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer Verlag, 1997.
- [8] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets. In *Proc. 36th Ann. ACM STOC*, pages 475–485, 2004. Full version at <http://www.arxiv.org/abs/cs/cs.CC/0312007>.
- [9] F. Cucker and D.Yu. Grigoriev. On the power of real Turing machines over binary inputs. *SIAM J. Comp.*, 26:243–254, 1997.
- [10] 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.
- [11] F. Cucker and P. Koiran. Computing over the reals with addition and order: Higher complexity classes. *J. Compl.*, 11:358–376, 1995.
- [12] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Appl. Math.*, 33(1-3):73–94, 1991.
- [13] A. Dimca. *Singularities and Topology of Hypersurfaces*. Universitext. Springer Verlag, 1992.
- [14] L. Fortnow. Counting complexity. In *Complexity theory retrospective, II*, pages 81–107. Springer, New York, 1997.

- [15] W. Fulton. *Introduction to Toric Varieties*. Annals of Math. Studies. Princeton University Press, 1993.
- [16] W. Fulton. *Intersection Theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 1998.
- [17] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In D. Eisenbud and L. Robbiano, editors, *Proc. Cortona Conference on Computational Algebraic Geometry and Commutative Algebra*. Cambridge University Press, 1993.
- [18] J. Harris. *Algebraic Geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
- [19] R. Hartshorne. *Algebraic Geometry*. GTM. Springer Verlag, 1977.
- [20] A. Hatcher. *Algebraic Topology*. Cambridge University Press, Cambridge, 2002.
- [21] O.H. Ibarra and S. Moran. Equivalence of straight-line programs. *J. ACM*, 30:217–228, 1983.
- [22] P. Koiran. Computing over the reals with addition and order. *Theoret. Comp. Sci.*, 133:35–47, 1994.
- [23] P. Koiran. Elimination of constants from machines over algebraically closed fields. *J. Compl.*, 13:65–82, 1997.
- [24] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th FOCS*, pages 36–45, 1997.
- [25] P. Koiran. A weak version of the Blum, Shub & Smale model. *J. Comp. Syst. Sci.*, 54:177–189, 1997.
- [26] P. Koiran. Elimination of parameters in the polynomial hierarchy. *Theoret. Comp. Sci.*, 215:289–304, 1999.
- [27] T. Krick and L.M. Pardo. Une approche informatique pour l'approximation diophantienne. *C.R. Acad. Sc. Paris*, 318:407–412, 1994.
- [28] Y. N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective methods in algebraic geometry (Castiglione, 1990)*, volume 94 of *Progr. Math.*, pages 227–234. Birkhäuser Boston, Boston, MA, 1991.
- [29] A. Macintyre. Model completeness. In J. Barwise, editor, *Handbook of Mathematical Logic*, pages 139–180. North-Holland, 1977.
- [30] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1986.
- [31] K. Meer. Counting problems over the reals. *Theoret. Comp. Sci.*, 242:41–58, 2000.
- [32] D. Mumford. *Algebraic Geometry I: Complex Projective Varieties*. Springer Verlag, 1976.
- [33] I.R. Shafarevich. *Basic Algebraic Geometry*. Springer Verlag, 1974.
- [34] L.G. Valiant. The complexity of computing the permanent. *Theoret. Comp. Sci.*, 8:189–201, 1979.

- [35] L.G. Valiant. The complexity of enumeration and reliability problems. *SIAM J. Comp.*, 8:410–421, 1979.
- [36] A.C. Yao. Algebraic decision trees and Euler characteristic. In *Proc. 33rd FOCS*, 1992.