The complexity of computing the Hilbert polynomial of smooth equidimensional complex projective varieties

Peter Bürgisser and Martin Lotz*

February 1, 2008

Abstract

We continue the study of counting complexity begun in [11, 14, 13] by proving upper and lower bounds on the complexity of computing the Hilbert polynomial of a homogeneous ideal. We show that the problem of computing the Hilbert polynomial of a smooth equidimensional complex projective variety can be reduced in polynomial time to the problem of counting the number of complex common zeros of a finite set of multivariate polynomials. Moreover, we prove that the more general problem of computing the Hilbert polynomial of a homogeneous ideal is polynomial space hard. This implies polynomial space lower bounds for both the problems of computing the rank and the Euler characteristic of cohomology groups of coherent sheaves on projective space, improving the #P-lower bound in Bach [1].

1 Introduction

Despite the impressive progress in the development of algebraic algorithms and computer algebra packages, the inherent computational complexity of even the most basic problems in algebraic geometry is still far from being understood. In [11] a systematic study of the inherent complexity for computing algebraic/topological quantities was launched with the goal of characterizing the complexity of various such problems by completeness results in a suitable hierarchy of complexity classes. In this article we continue this study by investigating the complexity of computing the Hilbert polynomial of a complex projective variety $V \subseteq \mathbb{P}^n$. This polynomial encodes important information about the variety V, like its dimension, degree and arithmetic genus.

Algorithms for computing Hilbert polynomials were described in [42, 7, 6]. Some of these algorithms have been implemented in computer algebra systems and work quite well in practice. These algorithms are based on the computation of Gröbner

*Institute of Mathematics, University of Paderborn, D-33095 Paderborn, Germany. E-mail: {pbuerg,lotzm}@upb.de. Partially supported by DFG grant BU 1371 and Paderborn Institute for Scientific Computation (PaSCo).

bases, which leads to bad upper complexity estimates. In fact, the problem of computing a Gröbner basis is exponential space complete [38]. Both the cardinality and the maximal degree of a Gröbner basis might be doubly exponential in the number of variables [39, 28]. It is generally believed that these bounds are quite pessimistic and that for problems with "nice" geometry, single exponential upper bounds should hold for Gröbner bases. Among the results that are known in this direction are [24, 18, 5, 38]. However, currently no upper bound better than exponential space is known for the computation of the Hilbert function or Hilbert polynomial of a homogeneous ideal.

Based on a lower bound on the homogeneous polynomial ideal membership problem in [38] we are able to show that the problem of computing the Hilbert polynomial is FPSPACE-hard, where FPSPACE denotes the complexity class of functions that can be computed in polynomial space by a Turing machine. As a corollary, we obtain an FPSPACE-lower bound for the problem of computing the rank of cohomology groups of coherent sheaves on projective space as well as for the problem of computing the corresponding Euler characteristic (Corollary 4.11), thus improving the #P-lower bound in Bach [1].

The bound on the Castelnuovo-Mumford regularity for the vanishing ideal of a smooth projective variety in [5, Thm. 3.12(b)] suggests that the computation of the Hilbert polynomial might actually be possible in polynomial space for *smooth* varieties. The main goal of this article is to prove a stronger result: we show that the problem $\textsc{Hilbert}_{\mathrm{sm}}$ of computing the Hilbert polynomial of a smooth equidimensional complex projective variety $V \subseteq \mathbb{P}^n$ can be reduced in polynomial time to the problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of complex common zeros of a finite set of complex multivariate polynomials. (The input specification for $\textsc{Hilbert}_{\mathrm{sm}}$ involves some subtleties, see §4.) Such reduction can be established in the Turing as well as in the Blum-Shub-Smale model of computation [9, 8]. In particular, in the Turing model we obtain an FPSPACE-upper bound for the discrete version of $\textsc{Hilbert}_{\mathrm{sm}}$, where the inputs are integer polynomials.

These results are interpreted in the framework of counting complexity. In [11] Valiant's counting complexity class #P [48, 49] was extended to the framework of computations over $\mathbb{C}$ in the sense of [8]. Thus $\#\mathrm{P}_{\mathbb{C}}$ is the class of functions from the space $\mathbb{C}^\infty$ of finite sequences of complex numbers to $\mathbb{N} \cup \{\infty\}$ which, roughly speaking, count the number of satisfying witnesses for an input of a problem in $\mathrm{NP}_{\mathbb{C}}$. The problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of complex common zeros of a given finite set of complex polynomials (returning ∞ if this number is not finite) turns out to be complete for the class $\#\mathrm{P}_{\mathbb{C}}$. The main results of [11, 13] state that both problems to compute the geometric degree and the topological Euler characteristic of complex varieties are polynomial time equivalent to $\#\mathrm{HN}_{\mathbb{C}}$ ([11] also contains a corresponding result for the computation of the Euler characteristic of semialgebraic sets). Hereby, "polynomial time equivalent" is meant in the sense of computations over $\mathbb{C}$. However, when restricting the inputs to integer coefficient polynomials, the

corresponding discrete problems are also equivalent in the Turing model of computation (for Turing reductions). The complexity of these discrete problems is captured by the Boolean part GCC of $\#\mathrm{P}_{\mathbb{C}}$, which is obtained by restricting the functions in $\#\mathrm{P}_{\mathbb{C}}$ to bit strings. Is is known that $\#\mathsf{P} \subseteq \mathsf{GCC} \subseteq \mathsf{FPSPACE}$ [11]. One can show along the lines of [11, §8.3] that the problem of computing the number of connected components of a complex affine algebraic variety (given by integer coefficients polynomials) is $\mathsf{FPSPACE}$-complete. This implies that the problem of computing the topological Euler characteristic is strictly easier than the problem of computing the number of connected components, unless GCC collapses with $\mathsf{FPSPACE}$, which we believe to be unlikely.

The class $\#\mathrm{P}_{\mathbb{C}}$ captures the complexity of counting the number of solutions to systems of polynomial equations. It is therefore not surprising that some of the ideas and tools of intersection theory, enumerative geometry, and Schubert calculus are salient for our purposes.

Our reduction from $\textsc{Hilbert}_{\mathrm{sm}}$ to $\#\mathrm{HN}_{\mathbb{C}}$ consists of the following three steps:

1. We interpret the value $p_V(d)$ of the Hilbert polynomial of $V \subseteq \mathbb{P}^n$ on $d \in \mathbb{Z}$ as the Euler characteristic $\chi(\mathcal{O}_V(d))$ of the twisted sheaf $\mathcal{O}_V(d)$.

2. The Hirzebruch-Riemann-Roch Theorem [27] gives an explicit combinatorial description of $\chi(\mathcal{O}_V(d))$ in terms of certain determinants $\Delta_\lambda(c)$ (related to Schur polynomials) in the Chern classes c_i of the tangent bundle of V.

3. The homology class corresponding to the cohomology class $\Delta_\lambda(c)$ can be realized up to sign by a degeneracy locus, which is defined as the pullback of a Schubert variety under the Gauss map (cf. Fulton [21, Ex. 14.3.3]). We call the geometric degree of such a degeneracy locus a projective character.

This allows to express (certain integer multiples of) the coefficients of the Hilbert polynomial as integer linear combinations of projective characters. We now use the fact that the computation of the geometric degree of varieties is possible in the complexity class $\textsc{Gap}^*_{\mathbb{C}}$, and that the class $\textsc{Gap}^*_{\mathbb{C}}$ is closed under exponential summation (Lemma 3.8). Here $\textsc{Gap}^*_{\mathbb{C}}$ is a class of functions slightly larger than $\#\mathrm{P}_{\mathbb{C}}$, which is closed under "generic parsimonious reductions" [13].

Organization of the article. In §2 we present all the necessary definitions and facts needed in order to state a formula for the coefficients of the Hilbert polynomial in terms of projective characters. While the formula is given in §2, the proof is postponed to §5. Section 3 contains background from (counting) complexity theory over $\mathbb{C}$. In §4 we present the main results of this article, the upper and lower bounds on the complexity of computing the coefficients of the Hilbert polynomial. Finally, §5 contains the derivation of the relationship between the Hilbert polynomial and degeneracy loci, using the Hirzebruch-Riemann-Roch theorem. In order to facilitate reading, the proofs of two technical lemmas from §2 and of a result used in §4 are postponed to the appendix.

Acknowledgment. We thank Felipe Cucker for discussions and inviting us to Hong Kong in Spring 2004, where the basis of this work was elaborated in the joint papers [14, 13].

2 Preliminaries from algebraic geometry

Throughout this article, unless otherwise stated, the term *variety* will mean a complex, projective, not necessarily irreducible variety. By a *subvariety* we will always understand a closed subvariety. We will say that a property holds *for almost all points in a variety*, if the set of points satisfying the given property is a dense subset with respect to the Zariski topology.

2.1 The Hilbert polynomial

Let $S := \mathbb{C}[X_0, \ldots, X_n]$ denote a polynomial ring and let M be a finitely generated, graded S-module. Denote by M_k the k-th graded part of M. The function $h_M \colon \mathbb{Z} \to \mathbb{N}$, defined by $h_M(k) = \dim_{\mathbb{C}} M_k$ is called the *Hilbert function* of M. A proof of the following theorem can be found in [26, I.7].

Theorem 2.1 (Hilbert-Serre) *Let M be a finitely generated, graded S-module. Then there exists a unique polynomial $p_M(T) \in \mathbb{Q}[T]$ such that $h_M(\ell) = p_M(\ell)$ for sufficiently large ℓ. Furthermore, the degree of p_M equals the dimension of the projective zero set of the annihilator $\{s \in S \mid sM = 0\}$ of M.*

The polynomial $p_M(T)$ is called the *Hilbert polynomial* of M. Of special interest is the case $M = S/I$, where $I \subseteq S$ is a homogeneous ideal. If $I = I(V)$ is the homogeneous ideal of a complex projective variety $V \subseteq \mathbb{P}^n$, then we write $p_V := p_{S/I}$ and call this the Hilbert polynomial of V. We thus have $\deg p_V = \dim V$.

Example 2.2

1. The Hilbert polynomial of $V = \mathbb{P}^n$ is $p_V(T) = \binom{T+n}{n}$.
2. Let $f \in \mathbb{C}[X_0, \ldots, X_n]$ be homogeneous and irreducible of degree d and let $V = \mathcal{Z}(f)$ be its projective zero set. Then $p_V(T) = \binom{T+n}{n} - \binom{T+n-d}{n}$.

Let $V \subseteq \mathbb{P}^n$ be an m-dimensional projective variety with Hilbert polynomial $p_V(T) = p_m T^m + \cdots + p_1 T + p_0$. The *geometric degree* $\deg V$ of V is defined as $\deg V := m!\, p_m$. The degree counts the number of intersection points of V with a generic linear subspace of complementary dimension [25, Lect. 18]. It is additive on the irreducible components of maximal dimension. The *arithmetic genus* of V is defined as $g_a(V) := (-1)^m(p_0 - 1)$. While the degree depends on the embedding in projective space, the arithmetic genus is a birational invariant (cf. [26, Ex. III.5.3]).

2.2 Projective characters

General references for the material presented in this section are [20, 37]. In the following we assume $0 \leq m \leq n$. The *Grassmann variety*

$$\mathbb{G}(m,n) := \{A \mid A \subseteq \mathbb{P}^n \text{ linear subspace of dimension } m\}$$

is an irreducible smooth projective variety of dimension $(m+1)(n-m)$ [25, Lect. 6].

The *flag variety* $\mathcal{F}$ is defined as the set of all complete flags $\underline{F}$ of linear subspaces $F_0 \subset \ldots \subset F_{n-1} \subset F_n = \mathbb{P}^n$, such that $\dim F_i = i$ for $0 \leq i \leq n$. It is an irreducible smooth projective variety [20, III.9.1].

For $A \in \mathbb{G}(m,n)$ and a flag $\underline{F} \in \mathcal{F}$ we consider the weakly increasing sequence of dimensions $(\dim(A \cap F_j))_{0 \leq j \leq n}$ and denote by $0 \leq \sigma_0 < \sigma_1 < \cdots < \sigma_m \leq n$ the positions where the "jumps" occur, that is, $\dim(A \cap F_j) = i$ for $\sigma_i \leq j < \sigma_{i+1}$ (using the conventions $\dim \emptyset = -1$ and $\sigma_{-1} := 0, \sigma_{m+1} := n$). The sequence (σ_i) can be encoded by the sequence of integers $n - m \geq \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_{m+1} \geq 0$ defined by $\lambda_{i+1} := n - m + i - \sigma_i$.

Generally, a *partition* $\lambda = (\lambda_1, \ldots, \lambda_r)$ is a weakly decreasing sequence of natural numbers. The length of λ is defined as the number of nonzero components of λ. The size of λ is defined as $|\lambda| := \lambda_1 + \cdots + \lambda_r$, and we call λ *a partition of* k, if $|\lambda| = k$. We say that a partition μ contains a partition λ, $\lambda \subseteq \mu$, if $\lambda_i \leq \mu_i$ for all i (we set $\lambda_i = 0$ for all i exceeding the length of λ).

To a partition λ of length at most $m+1$ with $\lambda_1 \leq n-m$ (in which case we call λ *admissible*) we associate a strictly increasing sequence $0 \leq \sigma_0 < \cdots < \sigma_m \leq n$ by setting $\sigma_i := n - m + i - \lambda_{i+1}$ for $0 \leq i \leq m$. The σ_i are used to select a subflag $F_{\sigma_0} \subset \ldots \subset F_{\sigma_m}$ with $\dim F_{\sigma_i} = \sigma_i$. For such a partition λ and a flag $\underline{F} \in \mathcal{F}$ the *Schubert variety* $\Omega_\lambda(\underline{F})$ is defined as follows:

$$\Omega_\lambda(\underline{F}) := \{A \in \mathbb{G}(m,n) \mid \dim(A \cap F_{\sigma_i}) \geq i \text{ for } 0 \leq i \leq m\}.$$

For $A \in \mathbb{G}(m,n)$ we always have $\dim(A \cap F_{\sigma_i}) \geq i - \lambda_{i+1}$, so that λ_{i+1} measures the excess in dimension of the intersection. It is known that $\Omega_\lambda(\underline{F})$ is an irreducible variety of codimension $|\lambda|$ in $\mathbb{G}(m,n)$ [20, III.9.4]. (Note that since λ is admissible, we have $|\lambda| \leq \dim \mathbb{G}(m,n)$.) In general, Schubert varieties are singular [37, §3.4].

For a flag $\underline{F} \in \mathcal{F}$ and an admissible partition λ the *Schubert cell* $e_\lambda(\underline{F})$ is defined as follows (put $F_{-1} = \emptyset$)

$$e_\lambda(\underline{F}) := \{A \in \Omega_\lambda(\underline{F}) \mid \dim(A \cap F_{\sigma_i - 1}) = i - 1 \text{ for } 0 \leq i \leq m\}. \tag{1}$$

Thus $e_\lambda(\underline{F})$ consists of those elements $A \in \Omega_\lambda(\underline{F})$ for which $\dim A \cap F_j$ increases at exactly the positions $j = \sigma_i$. The Grassmann variety $\mathbb{G}(m,n)$ is the disjoint union of the Schubert cells $e_\lambda(\underline{F})$ over all admissible partitions λ. Moreover, it is known that

$$\Omega_\lambda(\underline{F}) = \bigcup_{\lambda \subseteq \mu} e_\mu(\underline{F}), \tag{2}$$

where the union is over all admissible partitions μ containing λ, cf. [20, III.9.4, Ex. 13] or [37, §3.2]. The Schubert cell is a complex analytic submanifold of $\mathbb{G}(m,n)$ of codimension $|\lambda|$. It is open and dense in $\Omega_\lambda(\underline{F})$. Moreover, $e_\lambda(\underline{F})$ is contained in the smooth part of $\Omega_\lambda(\underline{F})$, cf. [37, §3.4].

Example 2.3 (i) In the case $\lambda = (k) = (k, 0, \ldots, 0)$ the degeneracy conditions reduce to the single condition $A \cap F_{\sigma_0} \neq \emptyset$ on $F_{\sigma_0} \in \mathbb{G}(n-m-k, n)$.

(ii) In the case $\lambda = (1^k) = (1, \ldots, 1, 0, \ldots, 0)$ the degeneracy conditions reduce to the single condition $\dim(A \cap F_{\sigma_{k-1}}) \geq k-1$ on $F_{\sigma_{k-1}} \in \mathbb{G}(n-m+k-2, n)$.

(iii) We have $\mathbb{P}^n = \mathbb{G}(0,n) = \Omega_0(\underline{F}) = \cup_{i=0}^n e_{(i)}$, where $e_{(i)} = F_i - F_{i-1} \cong \mathbb{C}^i$, which is just the usual decomposition of $\mathbb{P}^n$ as a disjoint union of affine spaces.

Let $V \subseteq \mathbb{P}^n$ be a smooth projective variety of pure dimension m. The *Gauss map* $\varphi\colon V \to \mathbb{G}(m,n)$ maps $x \in V$ to the projective tangent space $\mathbb{T}_x V \subseteq \mathbb{P}^n$ at x. For an admissible partition λ and a flag $\underline{F} \in \mathcal{F}$ we define the *generalized polar variety*

$$P_\lambda(\underline{F}) := \varphi^{-1}(\Omega_\lambda(\underline{F})) = \{x \in V \mid \dim(\mathbb{T}_x V \cap F_{\sigma_i}) \geq i \text{ for } 0 \leq i \leq m\} \qquad (3)$$

to be the preimage of the Schubert variety $\Omega_\lambda(\underline{F})$ under the Gauss map. The well-known *polar varieties*

$$P_k(\underline{F}) := P_{(1^k)}(\underline{F}) = \{x \in V \mid \dim(\mathbb{T}_x V \cap F_{n-m+k-2}) \geq k-1\}$$

correspond to the special case $\lambda = (1^k) = (1, \ldots, 1, 0, \ldots, 0)$, see [45, 10]. We remark that a different concept of generalized polar varieties has been previously used for algorithmic purposes, see [2, 3].

Note that the case where V is a linear space is degenerate: then $\dim \varphi(V) = 0$ and thus $P_\lambda(\underline{F})$ is empty for almost all $\underline{F} \in \mathcal{F}$, provided $|\lambda| > 0$. A result by Zak, cf. [23, §7], states that this is the only degenerate case. Namely, if $V \subseteq \mathbb{P}^n$ is a nonlinear irreducible smooth projective variety, then the Gauss map $\varphi\colon V \to \varphi(V)$ is finite. In particular, we have $\dim \varphi(V) = \dim V$ in this case.

We recall now the important notion of transversality. For $x \in V$ we denote by $T_x V$ the Zariski tangent space and by $d_x\varphi\colon T_x V \to T_{\varphi(x)}\mathbb{G}(m,n)$ the differential of φ at x, respectively. The Gauss map φ *meets* the Schubert cell $e_\lambda(\underline{F})$ *transversely at* $x \in \varphi^{-1}(e_\lambda(\underline{F}))$, written $\varphi \pitchfork_x e_\lambda(\underline{F})$, if

$$T_{\varphi(x)}\mathbb{G}(m,n) = d_x\varphi(T_x V) + T_{\varphi(x)} e_\lambda(\underline{F}).$$

Moreover, φ *meets* $e_\lambda(\underline{F})$ *transversely*, written $\varphi \pitchfork e_\lambda(\underline{F})$, if $\varphi \pitchfork_x e_\lambda(\underline{F})$ holds for all x in $\varphi^{-1}(e_\lambda(\underline{F}))$.

Remark 2.4 If $\varphi \pitchfork e_\lambda(\underline{F})$ then it is well known that $\varphi^{-1}(e_\lambda(\underline{F}))$ is a smooth complex submanifold of codimension $|\lambda|$ in V, unless it is empty. (Recall that $e_\lambda(\underline{F})$ has the codimension $|\lambda|$ in $\mathbb{G}(m,n)$.)

We can extend the notion of transversality to Schubert varieties in the following natural way, exploiting their stratification (2) by Schubert cells.

Definition 2.5 We say that φ *meets* $\Omega_\lambda(\underline{F})$ *transversely*, written $\varphi \pitchfork \Omega_\lambda(\underline{F})$, if for every admissible $\mu \supseteq \lambda$ we have $\varphi \pitchfork e_\mu(\underline{F})$.

The following lemma is proved in Appendix A.1.

Lemma 2.6 *Let $V \subseteq \mathbb{P}^n$ be a smooth projective variety of pure dimension m such that not all irreducible components of V are linear. Let $\varphi\colon V \to \mathbb{G}(m,n)$ be the Gauss map of V and λ be an admissible partition with $|\lambda| \leq m$. Then we have*

(i) *$\varphi \pitchfork \Omega_\lambda(\underline{F})$ for almost all flags $\underline{F} \in \mathcal{F}$,*

(ii) *if $\varphi \pitchfork \Omega_\lambda(\underline{F})$, then $\dim(\varphi(V) \cap e_\lambda(\underline{F})) = m - |\lambda|$ and $\operatorname{codim}_V P_\lambda(\underline{F}) = |\lambda|$,*

(iii) *there exists an integer d_λ, such that $\deg P_\lambda(\underline{F}) = d_\lambda$, provided $\varphi \pitchfork \Omega_\lambda(\underline{F})$.*

We call $\deg P_\lambda := d_\lambda$ the *projective character* of V corresponding to λ. These quantities were studied by Severi [46], see also [21, Ex. 14.3.3]. Note that the degree of V equals the projective character for $\lambda = 0$.

Example 2.7 Let $V \subseteq \mathbb{P}^2$ be a smooth curve. Then $\deg P_1$ counts the number of points on the curve whose tangents go through a generic point in $\mathbb{P}^2$. Bézout's theorem implies that this number equals $d(d-1)$, where d is the degree of the curve.

The following will be used later. Again, the proof is postponed to the Appendix.

Lemma 2.8 *Let W be a quasiprojective variety and let $\psi\colon W \to \mathbb{G}(m,n)$ be a morphism. Let λ be an admissible partition. For $\underline{F} \in \mathcal{F}$ set $R_\lambda(\underline{F}) := \psi^{-1}(\Omega_\lambda(\underline{F}))$. Then for almost all $\underline{F} \in \mathcal{F}$ we have $\dim R_\lambda(\underline{F}) \leq \dim W - |\lambda|$ if $|\lambda| \leq \dim W$, and $R_\lambda(\underline{F}) = \emptyset$ otherwise.*

2.3 Expressing the Hilbert polynomial by projective characters

Our goal is to express the coefficients of the Hilbert polynomial of V in terms of its projective characters. We first introduce some notation.

To any sequence $c = (c_i)_{i\in\mathbb{N}}$ of elements of a commutative ring such that $c_0 = 1$ and to a partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ we assign the ring element $\Delta_\lambda(c)$ as follows:

$$\begin{aligned}\Delta_\lambda(c) &:= \det\left((c_{\lambda_i - i + j})_{1\leq i,j\leq r}\right) \\ &= \det\begin{pmatrix} c_{\lambda_1} & c_{\lambda_1+1} & \cdots & c_{\lambda_1+r-1} \\ c_{\lambda_2-1} & c_{\lambda_2} & \cdots & c_{\lambda_2+r-2} \\ \cdots & \cdots & \cdots & \cdots \\ c_{\lambda_r-r+1} & c_{\lambda_r-r+2} & \cdots & c_{\lambda_r} \end{pmatrix}, \end{aligned} \tag{4}$$

using the convention $c_i = 0$ for $i < 0$. Note that the value of this determinant does not change if we extend the partition λ by zeros.

In the following let b be the coefficient sequence of the power series

$$\sum_{i\geq 0} b_i t^i := \frac{t}{1-e^{-t}} = 1 + \frac{t}{2} + \sum_{j\geq 1} (-1)^{j-1} \frac{B_j}{(2j)!}\, t^{2j}, \tag{5}$$

where the B_j are the *Bernoulli numbers*. E.g., $B_1 = \frac{1}{6}, B_2 = \frac{1}{30}, B_3 = \frac{1}{42}$.

Remark 2.9 It is known that $B_n = (-1)^{n-1} \sum_{k=1}^{2n} \frac{1}{k+1} \sum_{r=1}^{k} (-1)^r \binom{k}{r} r^n$ [51]. This implies that $(2n+1)!B_n$ is an integer, hence $i!(i+1)!b_i$ is an integer for all i. Taking into account that for a partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ of size M and length r we always have $\lambda_1 + r - 1 \leq M$, we conclude that $[(M+1)! \cdots (M-r+2)!]^2\, \Delta_\lambda(b)$ is an integer.

To a pair (λ, μ) of partitions of length at most m we assign the following determinant of binomial coefficients

$$d^m_{\lambda\mu} := \det\left(\binom{\lambda_i + m + 1 - i}{\mu_j + m + 1 - j}\right)_{1\leq i,j\leq m}.$$

Now let $0 \leq k \leq m$ and μ be a partition with $|\mu| \leq m - k$. To this data we assign the rational number

$$\delta^{m,k}_\mu := (-1)^{|\mu|} \sum_{\substack{\mu\subseteq\lambda \\ |\lambda|=m-k}} \Delta_\lambda(b) d^m_{\lambda\mu}, \tag{6}$$

where the sum is over all partitions λ of size $m - k$ that contain μ as subpartition.

The following crucial statement will be proved in §5.

Theorem 2.10 *Let $V \subseteq \mathbb{P}^n$ be a smooth complex projective variety of pure dimension m and $0 \leq k \leq m$. Then the k-th coefficient $p_k(V)$ of the Hilbert polynomial of V is given by*

$$p_k(V) = \frac{1}{k!} \sum_{\substack{|\mu|\leq m-k \\ \mu_1 \leq n-m}} \delta^{m,k}_\mu \deg P_\mu,$$

where $\deg P_\mu$ is the projective character introduced in §2.2. In particular, $[(m-k+1)! \cdots 2!1!]^2\, k!\, p_k(V)$ is an integer.

Example 2.11

1. The above formula yields $p_m(V) = \frac{1}{m!}\, \delta^{m,m}_0 \deg P_0 = \frac{1}{m!} \deg V$, as expected (check that $\Delta_0(b) = 1, d^m_{0,0} = 1$).

2. In the case where $V \subseteq \mathbb{P}^n$ is a smooth curve ($n \geq 2$), the above formula implies that $p_0 = \delta^{1,0}_0 \deg P_0 + \delta^{1,0}_1 \deg P_1 = \deg V - \frac{1}{2} \deg P_1$, where $\deg P_1 = \#\{x \in V \mid \mathbb{T}_x V \cap L \neq \emptyset\}$ for a generic linear subspace $L \subset \mathbb{P}^n$ of codimension 2.

3. In the special case of a smooth planar curve V (see Example 2.7), we have $p_0(V) = d - \frac{1}{2}d(d-1) = \frac{1}{2}d(3-d)$, which implies the well known formula $1 - p_0(V) = \frac{1}{2}(d-1)(d-2)$ for the arithmetic genus.

4. Consider the rational normal curve $V \subseteq \mathbb{P}^n$, which is defined as the projective closure of $\{(t, t^2, \ldots, t^n) \mid t \in \mathbb{C}\}$. The Hilbert polynomial of V satisfies $p_V(T) = nT + 1$. It is not too hard to verify directly that $\deg P_1 = 2(n-1)$.

3 Counting complexity over the complex numbers

We will consider BSS-machines over $\mathbb{C}$ as they are defined in [9, 8]. Roughly speaking, such a machine takes an input from $\mathbb{C}^\infty$, performs a number of arithmetic operations and tests for zero following a finite list of instructions, and halts returning an element in $\mathbb{C}^\infty$ (or loops forever). 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 $\mathbb{C}^\infty$ being decided by a machine easily follow. 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 $\mathrm{size}(x)^c$ steps. Hereby, we define $\mathrm{size}(x)$ to be the smallest $n \geq 0$ such that $x \in \mathbb{C}^n$. The complexity classes $\mathrm{P}_\mathbb{C}$ and $\mathrm{NP}_\mathbb{C}$ are defined as usual, as well as the notions of reduction and completeness. The class $\mathrm{coNP}_\mathbb{C}$ consists of all subsets of $\mathbb{C}^\infty$ whose complement lies in $\mathrm{NP}_\mathbb{C}$. In a completely analogous fashion we can also consider machines over $\mathbb{R}$ and corresponding classes $\mathrm{P}_\mathbb{R}$ and $\mathrm{NP}_\mathbb{R}$.

In [9] it was shown that the following fundamental problems is $\mathrm{NP}_\mathbb{C}$-complete.

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

For our convention on coding polynomials as elements of $\mathbb{C}^\infty$ we refer to §4, see also [32, 1.2] for a discussion.

3.1 Counting complexity classes

In classical complexity theory, Valiant [49] introduced the counting class $\#\mathsf{P}$ as the class of functions which count the number of accepting paths of nondeterministic polynomial time Turing machines. One of his main results [48] was that the problem of counting the number of perfect matchings in a bipartite graph, or equivalently, computing the permanent of its adjacency matrix, is $\#\mathsf{P}$-complete. For a comprehensive account to counting complexity we refer to [44, Chapter 18] and [19].

We now recall the definition of counting classes over $\mathbb{C}$ from [11, 13], which follows the lines used in discrete complexity theory to define $\#\mathsf{P}$ and GapP [19]. We denote by $\widehat{\mathbb{Z}} := \mathbb{Z} \cup \{-\infty, \infty, \mathrm{nil}\}$ the union of the set $\mathbb{Z}$ with three additional symbols $-\infty, \infty$, and nil (the latter standing for undefined). For the arithmetic in $\widehat{\mathbb{Z}}$, we refer to [13, §4.3].

Definition 3.1 (i) A function $\varphi\colon \mathbb{C}^\infty \to \mathbb{N} \cup \{\infty\}$ belongs to the class $\#\mathrm{P}_\mathbb{C}$ if there exists a polynomial time machine M and a polynomial p such that $\varphi(x) = |\{y \in \mathbb{C}^{p(n)} \mid M \text{ accepts } (x, y)\}|$ holds for all $x \in \mathbb{C}^n$ and all $n \in \mathbb{N}$.

(ii) The class $\mathrm{GAP}_\mathbb{C}$ consists of all functions $\gamma\colon \mathbb{C}^\infty \to \widehat{\mathbb{Z}}$ of the form $\gamma = \varphi - \psi$ for $\varphi, \psi \in \#\mathrm{P}_\mathbb{C}$.

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

Definition 3.2 1. Let $\varphi, \psi\colon \mathbb{C}^\infty \to \widehat{\mathbb{Z}}$. We say that $\pi\colon \mathbb{C}^\infty \to \mathbb{C}^\infty$ is a *parsimonious reduction* from φ to ψ if π can be computed in polynomial time and, for all $x \in \mathbb{C}^\infty$, $\varphi(x) = \psi(\pi(x))$.

2. Let $\varphi, \psi\colon \mathbb{C}^\infty \to \mathbb{C}^\infty$. We say that φ *Turing reduces to* ψ if there exists an oracle machine which, with oracle ψ, computes φ in polynomial time.

Let $\mathcal{C}$ be either $\#\mathrm{P}_\mathbb{C}$, or $\mathrm{GAP}_\mathbb{C}$. 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 $\psi \in \mathcal{C}$. The notions of *Turing-hardness* and *Turing-completeness* are defined similarly.

In [11] it was shown that the following basic problem is $\#\mathrm{P}_\mathbb{C}$-complete with respect to parsimonious reductions.

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

In an analogous fashion, the problem $\Delta\mathrm{HN}_\mathbb{C}$ (as introduced in [13, §4.3]), which counts the difference in the the number of solutions of two given systems of polynomial equations, is seen to be complete for the class $\mathrm{GAP}_\mathbb{C}$.

There are algorithms solving $\#\mathrm{HN}_\mathbb{C}$ in single exponential time (or even parallel polynomial time). A key point for showing this is the fact that a Gröbner basis of a zero-dimensional ideal can be computed in single exponential time [18, 34, 35]. The number of solutions can then be determined using linear algebra techniques, as described for example in [16, Chapter 2].

We remark that a corresponding counting class $\#\mathrm{P}_\mathbb{R}$ over the reals has been introduced by Meer [40] and was further explored in [11].

3.2 Polynomial hierarchy over the reals

The constant-free polynomial hierarchy over the reals will be needed in the next section for extending the notion of a parsimonious reduction. It is important to work over the reals since the polynomial hierarchy over the complex numbers has not enough expressive power for our purposes.

For what follows, we call a machine (over $\mathbb{R}$ or $\mathbb{C}$) *constant-free*, if its only machine constants are 0 and 1. The following definition is from [8, Chapter 21].

Definition 3.3 A relation $R \subseteq \mathbb{R}^\infty$ 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 M over $\mathbb{R}$, and polynomials $p_1, \ldots, p_k$, such that for $x \in \mathbb{R}^n$:

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

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

We next observe that the dimension and local dimension of semialgebraic sets can be expressed in $\mathrm{PH}_{\mathbb{R}}^0$. We study this in the general situation of a family of semialgebraic sets S_u depending on a parameter $u \in \mathbb{R}^\infty$ such that the property $x \in S_u$ is expressible in $\mathrm{PH}_{\mathbb{R}}^0$. We denote by $\dim_x S_u$ the local dimension of S_u at $x \in S_u$ (defined to be -1 if $x \notin S_u$).

Lemma 3.4 *Let $R \subseteq \mathbb{R}^\infty \times \mathbb{R}^\infty$ be a relation in $\mathrm{PH}_{\mathbb{R}}^0$, p be a polynomial, and consider for $u \in \mathbb{R}^n$ the semialgebraic set $S_u := \{x \in \mathbb{R}^{p(n)} \mid (u, x) \in R\}$. Then both decision problems $\{(u, d) \in \mathbb{R}^\infty \times \mathbb{N} \mid \dim S_u \geq d\}$ and $\{(u, x, d) \in \mathbb{R}^\infty \times \mathbb{R}^\infty \times \mathbb{N} \mid \dim_x S_u \geq d\}$ are in $\mathrm{PH}_{\mathbb{R}}^0$.*

Proof. We have $\dim S_u \geq d$ if and only if there exists a d-dimensional coordinate subspace such that the projection of S_u on this subspace has a nonempty interior. Writing this condition as a first order formula over $\mathbb{R}$ yields the claim for the dimension. (For a more economic description, see [33].)

Let $B_\epsilon(x)$ denote the open ball with radius ϵ centered at x. We have $\dim_x S_u \geq d$ if and only if $\dim(S_u \cap B_\epsilon(x)) \geq d$ for sufficiently small $\epsilon > 0$, cf. [4]. Writing this as a first order formula over $\mathbb{R}$ implies the claim about the local dimension. □

3.3 Generic parsimonious reductions

The concept of generic parsimonious reduction, as introduced in [13] and implicit in [11], 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 $\mathrm{HN}_{\mathbb{C}}$ 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" (see the notion of partial witness sequences introduced in [11]). This can be achieved by only requiring the genericity condition to be describable in terms of the constant-free polynomial hierarchy over the reals.

In the following, we are concerned with relations $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$. It makes sense to say that such a relation is in $\mathrm{PH}_{\mathbb{R}}^0$ by representing points in $\mathbb{C}^n$ as points in $\mathbb{R}^{2n}$ in the obvious way.

We call a relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ *balanced* if there is a polynomial p such that $R(u, a)$ implies $\mathrm{size}(a) \leq p(\mathrm{size}(u))$ for all $(u, a) \in \mathbb{C}^\infty \times \mathbb{C}^\infty$. In this case we say

that p is associated to R. Moreover, we will write $\forall^* a \in \mathbb{C}^n\, R(a)$ in order to express that Zariski almost all points $a \in \mathbb{C}^n$ satisfy a relation R.

Definition 3.5 Let $\varphi, \psi \colon \mathbb{C}^\infty \to \widehat{\mathbb{Z}}$. A *generic parsimonious reduction* from φ to ψ consists of a pair (π, R), where $\pi \colon \mathbb{C}^\infty \times \mathbb{C}^\infty \to \mathbb{C}^\infty$ is computable in polynomial time over $\mathbb{C}$ by a constant-free machine, and $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ is a balanced relation (with associated polynomial p) in $\mathrm{PH}^0_{\mathbb{R}}$ such that for all $m \in \mathbb{N}$ the following holds:

(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 exists a generic parsimonious reduction from φ to ψ. In [13] it was shown that this is a transitive relation. The following important fact is shown in [13, Theorem 4.4].

Theorem 3.6 *Let $\varphi, \psi \colon \mathbb{C}^\infty \to \widehat{\mathbb{Z}}$. If $\varphi \preceq_* \psi$ then φ Turing reduces to ψ .*

The closures of $\#\mathrm{P}_{\mathbb{C}}$ and $\mathrm{GAP}_{\mathbb{C}}$ with respect to generic parsimonious reductions defined below seem to capture more accurately the kind of counting problems encountered in algebraic geometry.

Definition 3.7 (i) The class $\#\mathrm{P}^*_{\mathbb{C}}$ consists of all functions $\varphi \colon \mathbb{C}^\infty \to \mathbb{N} \cup \{\infty\}$ such that there exists $\psi \in \#\mathrm{P}_{\mathbb{C}}$ with $\varphi \preceq_* \psi$.

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

The functions in $\mathrm{GAP}^*_{\mathbb{C}}$ can also be characterized as the differences of two functions in $\#\mathrm{P}^*_{\mathbb{C}}$.

Similar as GapP (cf. [19]), the class $\mathrm{GAP}^*_{\mathbb{C}}$ is closed under exponential summation.

Lemma 3.8 *Let $\varphi \colon \mathbb{C}^\infty \times \{0,1\}^\infty \to \mathbb{Z}$ be a function in $\mathrm{GAP}^*_{\mathbb{C}}$, q be a polynomial, and $g \colon \{0,1\}^\infty \to \mathbb{Z}$ be in GapP. Define $\widetilde{\varphi} \colon \mathbb{C}^\infty \to \mathbb{Z}$ by setting for $u \in \mathbb{C}^m$*

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

Then $\widetilde{\varphi}$ belongs to $\mathrm{GAP}^*_{\mathbb{C}}$. A similar statement holds for $\mathrm{GAP}_{\mathbb{C}}$.

Proof. The function $\mathbb{C}^\infty \times \{0,1\}^\infty \to \mathbb{Z}, (u,y) \mapsto g(y)\varphi(u,y)$ is in $\mathrm{GAP}^*_{\mathbb{C}}$ since the product of two finite valued functions in $\mathrm{GAP}^*_{\mathbb{C}}$ is in $\mathrm{GAP}^*_{\mathbb{C}}$ [13, Lemma 4.9]. The claim now follows from the fact that $\mathrm{GAP}^*_{\mathbb{C}}$ is closed under exponential summation [13, Lemma 4.10]. □

In [11] the problem of computing the geometric degree of the zero set $Z \subseteq \mathbb{C}^n$ of given complex polynomials was Turing reduced to $\mathrm{HN}_{\mathbb{C}}$. An analysis of the proof reveals that this reduction is generic parsimonious except for the computation of the dimension of Z at the beginning. Therefore, the following slight modification of the degree problem is in $\#\mathrm{P}_{\mathbb{C}}^*$: given Z as above and $d \in \mathbb{N}$ such that $\dim Z \leq d$, compute the geometric degree of the d-dimensional part of Z.

We can even extend this to the situation, where $Z_u \subseteq \mathbb{C}^n$ is a constructible set depending on a complex parameter vector u and membership of x in Z_u can be decided by a polynomial time machine. (By the degree of a constructible set we understand the sum of the degrees of its components of maximal dimension.)

Lemma 3.9 *Let M be a polynomial time machine over $\mathbb{C}$, $p\colon \mathbb{N} \to \mathbb{N}$ be a polynomial and consider for $u \in \mathbb{C}^n$ the constructible set*

$$Z_u := \{x \in \mathbb{C}^{p(n)} \mid M \text{ accepts } (u, x)\}.$$

Then there is a function φ in $\#\mathrm{P}_{\mathbb{C}}^*$ such that for all $u \in \mathbb{C}^\infty, d \in \mathbb{N}$ the value $\varphi(u, d)$ equals the degree of the d-dimensional part of Z_u, provided $\dim Z_u \leq d$.

Proof. The proof is completely analogous to the case where Z_u is given as the zero set of polynomials [11], see also [12, Theorem 7.2]. □

Example 3.10 Let F be a matrix with entries in $\mathbb{C}[X_1, \ldots, X_n]$, $k, d \in \mathbb{N}$ such that $Z := \{x \in \mathbb{C}^n \mid \operatorname{rank} F(x) \leq k\}$ has dimension at most d. Then, by Lemma 3.9, the degree of Z can be computed in $\#\mathrm{P}_{\mathbb{C}}^*$. This follows since the rank condition can be tested in polynomial time using linear algebra. (However, writing down the rank condition in terms of non-vanishing of minors would lead to a representation of exponential size.)

3.4 Boolean parts

If L is one of the computational problems studied in this paper, we denote by $L^{\mathbb{Z}}$ its restriction to input polynomials with integer coefficients. These discrete problems will be studied in the Turing model of computation. For doing so, we introduce the notion of the Boolean part of a complexity class over $\mathbb{C}$. For more details on the following we refer to [11, 13].

Let $\mathcal{C}$ be a class of functions $\mathbb{C}^\infty \to \widehat{\mathbb{Z}}$. We define its *Boolean part* $\mathrm{BP}(\mathcal{C})$ as the class of functions $\{0,1\}^\infty \to \widehat{\mathbb{Z}}$ obtained from functions in $\mathcal{C}$ by restriction to $\{0,1\}^\infty$. In [11], the class GCC of *geometric counting complex problems* was defined as the Boolean part of $\#\mathrm{P}_{\mathbb{C}}$. The discrete version $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ of the problem $\#\mathrm{HN}_{\mathbb{C}}$ is GCC-complete [11]. Both GCC and the Boolean part $\mathrm{BP}(\textsc{Gap}_{\mathbb{C}}^*)$ are closed under parsimonious reductions and (cf. [13])

$$\#\mathsf{P} \subseteq \mathsf{GCC} \subseteq \mathrm{BP}(\textsc{Gap}_{\mathbb{C}}^*) \subseteq \mathsf{FPSPACE}.$$

The class $\mathrm{BP}(\mathrm{GAP}^*_{\mathbb{C}})$ is closely related to GCC in the sense that any $\varphi \in \mathrm{BP}(\mathrm{GAP}^*_{\mathbb{C}})$ can be parsimoniously reduced to $\Delta\mathrm{HN}_{\mathbb{C}}$ in a randomized sense, cf. [13, Remark 6.7]. It is a challenging open problem to characterize GCC and $\mathrm{BP}(\mathrm{GAP}^*_{\mathbb{C}})$ in terms of previously studied classical complexity classes.

4 Complexity of computing the Hilbert polynomial

Our goal is to show that the problem of computing the Hilbert polynomial of a smooth equidimensional projective variety lies in the class $\mathrm{GAP}^*_{\mathbb{C}}$. When trying to formally define the problem under consideration, the question arises whether the smoothness condition can be tested at all within these resources. The obvious idea of checking the Jacobian criterion at all points in the variety V (which is possible in $\mathrm{coNP}_{\mathbb{C}}$) will fail if the given polynomials $f_1, \ldots, f_r$ describing the variety V do not generate a radical ideal and thus differ from the vanishing ideal $I(V)$ of V. Indeed, it is not known whether a set of generators of $I(V)$ can be computed from $f_1, \ldots, f_r$ in parallel polynomial time or even weaker, in single exponential time.

We overcome these difficulties by requiring an input specification, which, on the one hand, can be checked in $\mathrm{coNP}_{\mathbb{C}}$, and on the other hand guarantees that the highest dimensional part of the variety is smooth. The goal is then to compute the Hilbert polynomial of the highest dimensional part.

Thus in the following, we will assume that the projective variety $V' \subseteq \mathbb{P}^n$ is given as the zero set of a family $f_1, \ldots, f_r$ of homogeneous polynomials in $\mathbb{C}[X_0, \ldots, X_n]$ satisfying the following *input condition*:

$$\forall x \in \mathcal{Z}(f_1, \ldots, f_r) - \{0\} \ \dim\{z \in \mathbb{C}^{n+1} \mid d_x f_1(z) = 0, \ldots, d_x f_r(z) = 0\} \leq m+1 \quad (7)$$

for some $m \in \mathbb{N}$. Here and in the following, we assume that the given polynomials f are encoded as strings in $\mathbb{C}^\infty$ using the *sparse encoding*. Thus $f = \sum_{e \in I} a_e X_0^{e_0} \cdots X_n^{e_n}$ is represented by a list of pairs (a_e, e), where the coefficients a_e are given as complex numbers, while the exponent vector e is given by a bit vector of length at most $\mathcal{O}(n \log \deg f)$.

We remark that the input condition (7) can be tested in $\mathrm{coNP}_{\mathbb{C}}$.

Lemma 4.1 *Assume that the input condition (7) is satisfied. Then $V' = V \cup W$ is a disjoint union of a smooth variety $V \subseteq \mathbb{P}^n$ of pure dimension m (possibly empty) and a subvariety $W \subseteq \mathbb{P}^n$ with $\dim W < m$. In particular, the irreducible components of the m-dimensional part V of V' are pairwise disjoint. A point $x \in V'$ is in V if and only if $\dim_x V' = m$. Moreover, $n - m \leq r$ and for all $x \in V$ the Jacobian matrix $(\frac{\partial f_s}{\partial X_i}(x))$ has rank $n - m$.*

Proof. For all $x \in V'$ we have $\mathbb{T}_x V' \subseteq \mathbb{P}(\cap_{i=1}^r \ker d_x f_i)$, where $\mathbb{T}_x V'$ is the projective tangent space of V' at x. The input condition implies that for all $x \in V'$, $\dim_x V' \leq \dim \mathbb{T}_x V' \leq m$ holds. Therefore, all points $x \in V'$ of local dimension m are smooth.

The first claim follows since there is exactly one irreducible component passing through a smooth point. The remaining claims are clear. □

We give now a formal definition of our main problem under investigation. In order to make sure that the output is an integer, we require to compute a certain multiple of the k-th coefficient of the Hilbert polynomial.

HILBERT$_{\mathrm{sm}}$ (*Hilbert polynomial of smooth equidimensional varieties*) Given integers $0 \leq k \leq m \leq n$ and a family $f_1, \ldots, f_r$ of homogeneous polynomials in $\mathbb{C}[X_0, \ldots, X_n]$ satisfying the input condition for m, compute the integer multiple $N(k,m)\, p_k(V)$ of the k-th coefficient $p_k(V)$ of the Hilbert polynomial of the m-dimensional part V of V', where $N(k,m) := [(m-k+1)! \cdots 2!1!]^2$.

Here is the main result of this article.

Theorem 4.2 *The problem* HILBERT$_{\mathrm{sm}}$ *is in* GAP$^*_{\mathbb{C}}$. *In particular, the problem* HILBERT$_{\mathrm{sm}}$ *Turing reduces (over* $\mathbb{C}$*) to* HN$_{\mathbb{C}}$.

This theorem immediately implies the following corollary, cf. Section 3.4. Recall that HILBERT$^{\mathbb{Z}}_{\mathrm{sm}}$ denotes the restriction of HILBERT$_{\mathrm{sm}}$ to input polynomials with integer coefficients.

Corollary 4.3 *The problem* HILBERT$^{\mathbb{Z}}_{\mathrm{sm}}$ *is in* BP(GAP$^*_{\mathbb{C}}$). *In particular, the problem* HILBERT$^{\mathbb{Z}}_{\mathrm{sm}}$ *Turing reduces to* HN$^{\mathbb{Z}}_{\mathbb{C}}$ *(in the sense of classical Turing machines).*

4.1 Upper bounds

The upper bound on HILBERT$_{\mathrm{sm}}$ is based on Theorem 2.10. We therefore first study the problem to compute projective characters (recall Lemma 2.6 for their definition).

PROJCHAR (*Projective characters*) Given $0 \leq m \leq n$, homogeneous polynomials $f_1, \ldots, f_r$ in $\mathbb{C}[X_0, \ldots, X_n]$ satisfying the input condition for m and a partition λ such that $\lambda_1 \leq n-m$ and $|\lambda| \leq m$, compute the projective character $\deg P_\lambda$ of the m-dimensional part V of $V' = \mathcal{Z}(f_1, \ldots, f_r)$.

Proposition 4.4 *The problem* PROJCHAR *is in* #P$^*_{\mathbb{C}}$.

Using this proposition, we can immediately proceed to prove the main Theorem 4.2.

Proof of Theorem 4.2. Put $N(k,m) := [(m-k+1)! \cdots 2!1!]^2$. Consider the function $g\colon \{0,1\}^\infty \to \mathbb{Z}$ mapping (m,k,μ) to $N(k,m)\delta_\mu^{m,k}$, where $m,k \in \mathbb{N}$, μ a partition with $|\mu| \leq m-k$, $\mu_1 \leq n-m$ and $\delta_\mu^{m,k}$ is defined in Equation (6), i.e., $\delta_\mu^{m,k} := (-1)^{|\mu|} \sum_{\mu \subseteq \lambda, |\lambda| = m-k} \Delta_\lambda(b) d^m_{\lambda\mu}$. By Remark 2.9, the values of g are integers. The functions mapping (m,k,μ,λ) to $\Delta_\lambda(b)d^m_{\lambda\mu}$ and to $N(k,m)$, respectively, are

clearly polynomial time computable, if we think of (m, k, μ) as being encoded in unary. It then follows from elementary properties of GapP (closure under exponential summation and product, cf. [19]) that g is in GapP. Let $\varphi\colon \mathbb{C}^\infty \times \{0,1\}^\infty \to \mathbb{Z} \cup \{-\infty, \infty\}$ be the function corresponding to the problem ProjChar, where the first argument contains the description of the polynomials and the second argument the partition λ. According to Proposition 4.4, $\varphi \in \#\mathrm{P}^*_{\mathbb{C}}$, so we can apply the Summation Lemma 3.8 to the main formula in Theorem 2.10 to conclude that $\textsc{Hilbert}_{\mathrm{sm}} \in \textsc{Gap}^*_{\mathbb{C}}$. □

We prove Proposition 4.4 using a generic parsimonious reduction from ProjChar to a certain auxiliary problem, which we describe next. Consider an instance of ProjChar. Write $\psi(x) := \mathbb{P}\big(\bigcap_{i=1}^r \ker d_x f_i\big)$ for $x \in V'$ and define for a flag $\underline{F} \in \mathcal{F}$ the following constructible set (recall that $\sigma_i = n - m + i - \lambda_{i+1}$)

$$Q_\lambda(\underline{F}) := \{x \in V' \mid \dim(\psi(x) \cap F_{\sigma_i}) \geq i \text{ for } 0 \leq i \leq m\}. \tag{8}$$

We will represent a flag $\underline{F} \in \mathcal{F}$ by a matrix $a \in \mathbb{C}^{n\times(n+1)}$ such that F_{σ_i} is the projective zero set of the linear forms corresponding to the first $\delta_i := n - \sigma_i = m - i + \lambda_{i+1}$ rows of a, for $0 \leq i < m$.

Lemma 4.5 *There is a function Φ in $\#\mathrm{P}^*_{\mathbb{C}}$ which takes as input an instance of* ProjChar *and a flag $\underline{F} \in \mathcal{F}$ and outputs the degree of the $(m - |\lambda|)$-dimensional part of $Q_\lambda(\underline{F})$, provided* $\dim Q_\lambda(\underline{F}) \leq m - |\lambda|$.

Proof. Suppose we have an instance of ProjChar and a flag $\underline{F} \in \mathcal{F}$ given by the matrix $a \in \mathbb{C}^{n\times(n+1)}$. Let $M_i(x, a) \in \mathbb{C}^{(\delta_i+r)\times(n+1)}$ denote the matrix obtained by taking the submatrix of a consisting of the first δ_i rows of a and adding the Jacobian matrix $(\partial f_s/\partial X_j(x))_{1\leq s\leq r, 0\leq j\leq n}$ at the bottom. Then we have for all x

$$\dim(\psi(x) \cap F_{\sigma_i}) \geq i \Longleftrightarrow \mathrm{rank} M_i(x, a) \leq n - i.$$

This condition can be tested in $\mathrm{P}_{\mathbb{C}}$, since the rank of a matrix can be computed in polynomial time, e.g., using Gaussian elimination (compare Example 3.10). The claim follows now from Lemma 3.9. □

Proof of Proposition 4.4. Suppose we are given an instance of ProjChar. Let $\psi(x) = \mathbb{P}\big(\bigcap_{i=1}^r \ker d_x f_i\big)$ and $Q_\lambda(\underline{F})$ be defined for a flag $\underline{F} \in \mathcal{F}$ as in (8). By the input condition (7), $\psi(x)$ is a linear subspace of $\mathbb{P}^n$ of dimension at most m for every $x \in V'$. Let $V' = V \cup W$ be as in Lemma 4.1, so that V is smooth of dimension m and $\dim W < m$. We then have $\psi(x) = \mathbb{T}_x V$ for all $x \in V$, so that the restriction $\varphi := \psi|_V$ determines the Gauss map $\varphi\colon V \to \mathbb{G}(m, n)$. Note that $\psi(x)$ may be different from the projective tangent space at points $x \in W$.

Set $P_\lambda(\underline{F}) := Q_\lambda(\underline{F}) \cap V$ and $R_\lambda(\underline{F}) := Q_\lambda(\underline{F}) \cap W$. Then $P_\lambda(\underline{F})$ is the generalized polar variety introduced in (3) and we have $Q_\lambda(\underline{F}) = P_\lambda(\underline{F}) \cup R_\lambda(\underline{F})$.

Consider the following property of an instance I of ProjChar and a flag $\underline{F} \in \mathcal{F}$:

$$\varphi \pitchfork \Omega_\lambda(\underline{F}) \text{ and } \dim R_\lambda(\underline{F}) < m - |\lambda|. \tag{Π}$$

According to Lemma 2.6, the condition $\varphi \pitchfork \Omega_\lambda(\underline{F})$ implies that $\dim P_\lambda(\underline{F}) = m-|\lambda|$ and $\deg P_\lambda(\underline{F}) = \deg P_\lambda$, under the assumption that not all components of V are linear, or $\lambda = 0$. (If the latter assumption is violated, then $P_\lambda(\underline{F}) = \emptyset$.) We therefore get

$$\Pi \text{ is satisfied } \implies \deg P_\lambda = \deg P_\lambda(\underline{F}) = \Phi(I, \underline{F}),$$

where Φ is the function from Lemma 4.5, i.e., the degree of the $(m-|\lambda|)$-dimensional part of $Q_\lambda(\underline{F})$. This establishes a generic parsimonious reduction from ProjChar to the function $\Phi \in \#\mathrm{P}^*_{\mathbb{C}}$, once we have shown that Π is definable in the constant-free polynomial hierarchy over $\mathbb{R}$ and that for any fixed instance I of ProjChar, property Π is satisfied by almost all $\underline{F} \in \mathcal{F}$ (cf. Definition 3.5).

Lemma 2.6 tells us that $\varphi \pitchfork \Omega_\lambda(\underline{F})$ is satisfied for almost all $\underline{F} \in \mathcal{F}$. In order to show that $\dim R_\lambda(\underline{F}) < m-|\lambda|$ for almost all $\underline{F}$, we apply Lemma 2.8 to the quasiprojective set $W_j := \{x \in W \mid \dim \psi(x) = j\}$ and the map $\psi_j \colon W_j \to \mathbb{G}(j,n), x \mapsto \psi(x)$, for $0 \le j \le m$. It is not hard to identify the set

$$R_{j,\lambda}(\underline{F}) := \{x \in W_j \mid \dim(\psi(x) \cap F_{\sigma_i}) \ge i \text{ for } 0 \le i \le m\}$$

as the preimage of the Schubert variety corresponding to the flag $\underline{F}$ and to a partition $\mu^{(j)}$ satisfying $|\mu^{(j)}| \ge |\lambda|$. Thus $R_{j,\lambda}(\underline{F})$ has dimension $\dim W_j - |\mu| \le \dim W_j - |\lambda|$ for almost all $\underline{F}$. Since $W = W_0 \cup \cdots \cup W_m$ and $\dim W < m$ we have $R_\lambda(\underline{F}) = R_{0,\lambda}(\underline{F}) \cup \cdots \cup R_{m,\lambda}(\underline{F})$, and conclude that indeed $\dim R_\lambda(\underline{F}) < m - |\lambda|$.

It remains to be seen that Π can be defined in $\mathrm{PH}^0_{\mathbb{R}}$. According to Definition 2.5, $\varphi \pitchfork \Omega_\lambda(\underline{F})$ can be expressed as follows:

$$\forall \mu \; (\mu \supseteq \lambda \wedge \mu \text{ admissible } \implies \varphi \pitchfork e_\mu(\underline{F})), \tag{9}$$

where the transversality condition $\varphi \pitchfork e_\mu(\underline{F})$ means that

$$\forall x \; (x \in V \wedge \varphi(x) \in e_\mu(\underline{F}) \implies \varphi \pitchfork_x e_\mu(\underline{F})).$$

Lemma A.3 in Appendix A.2 says that the local transversality condition in the parenthesis is decidable in $\mathrm{P}^0_{\mathbb{C}}$. This implies that condition (9) is expressible in $\mathrm{coNP}^0_{\mathbb{C}}$ and thus in $\mathrm{PH}^0_{\mathbb{R}}$.

In order to express $\dim R_\lambda(\underline{F}) < m - |\lambda|$, we recall that the points $x \in W$ can be characterized among the points of V' as those having local dimension smaller than m, cf. Lemma 4.1. The local dimension of (semi)algebraic sets is expressible in the constant-free polynomial hierarchy over the reals (compare Lemma 3.4). We can thus express membership to $R_\lambda(\underline{F})$ in $\mathrm{PH}^0_{\mathbb{R}}$. Finally, using Lemma 3.4 again, we conclude that the condition $\dim R_\lambda(\underline{F}) < m - |\lambda|$ is expressible in $\mathrm{PH}^0_{\mathbb{R}}$. □

4.2 Lower bounds

We first complement the upper bound in Corollary 4.3 by a lower bound.

Proposition 4.6 *The problem* $\textsc{Hilbert}_{\mathrm{sm}}^{\mathbb{Z}}$ *is* #P*-hard.*

Proof. We proceed as in [1]. Let φ be a Boolean formula in the variables $X_1, \ldots, X_n$ in conjunctive normal form. It is well known that the problem #SAT to count the number of satisfying assignments of such formulas is #P-complete [49, 48].

For each literal λ put $g_\lambda := 1 - X_i$ if $\lambda = X_i$ and $g_\lambda := X_i$ if λ is the negation of X_i. For each clause $\kappa = \lambda_1 \vee \cdots \vee \lambda_k$ put $g_\kappa := \prod_{i=1}^{k} g_{\lambda_i}$. Let f_κ denote the homogenization of g_κ with respect to the variable X_0.

We assign to the Boolean formula $\varphi = \kappa_1 \wedge \cdots \wedge \kappa_s$ the system of homogeneous equations

$$X_1^2 - X_1X_0, \ldots, X_n^2 - X_nX_0, f_{\kappa_1}, \ldots, f_{\kappa_s}.$$

Clearly, the zero set V' of this system in $\mathbb{P}^n$ corresponds bijectively to the satisfying assignments of φ (there are no solutions at infinity). Moreover, looking at the first n equations we see that the input condition (7) is satisfied with $m = 0$. The Hilbert polynomial of V' is constant and equals the number of satisfying assignments of φ. This provides a polynomial time reduction from #SAT to $\textsc{Hilbert}_{\mathrm{sm}}^{\mathbb{Z}}$. □

Remark 4.7 Due to the input condition (7) it is not clear whether $\textsc{Hilbert}_{\mathrm{sm}}$ and $\textsc{Hilbert}_{\mathrm{sm}}^{\mathbb{Z}}$ are $\#\mathrm{P}_{\mathbb{C}}$-hard and GCC-hard, respectively.

Corollary 4.3 states that the problem $\textsc{Hilbert}_{\mathrm{sm}}^{\mathbb{Z}}$ to compute the Hilbert polynomial of smooth varieties is in $\mathrm{BP}(\textsc{Gap}_{\mathbb{C}}^{*})$. We next show that the general problem to compute the Hilbert polynomial of a homogeneous ideal is presumably more difficult, namely FPSPACE-hard. Consider the following problems:

HIM (*Homogeneous ideal membership problem*) Given non-constant homogeneous polynomials $f_1, \ldots, f_r, g \in \mathbb{C}[X_0, \ldots, X_n]$, decide whether g lies in the ideal generated by $f_1, \ldots, f_r$.

Hilbert (*Hilbert polynomial*) Given a family of non-constant homogeneous polynomials $f_1, \ldots, f_r$ in $\mathbb{C}[X_0, \ldots, X_n]$ and $0 \leq k \leq n$, compute the k-th coefficient of the Hilbert polynomial of the homogeneous ideal generated by $f_1, \ldots, f_r$.

We will use the following simple and well-known lemma to establish a Turing reduction from $\mathrm{HIM}^{\mathbb{Z}}$ to $\textsc{Hilbert}^{\mathbb{Z}}$, and then invoke a result in Mayr [38, Thm. 17], which states that $\mathrm{HIM}^{\mathbb{Z}}$ is PSPACE-complete.

Lemma 4.8 *Let I be a homogeneous ideal such that some X_i is not a zero-divisor of $\mathbb{C}[X_0, \ldots, X_n]/I$. Let g be a non-constant homogeneous polynomial. Then $g \in I$ if and only if I and $I + (g)$ have the same Hilbert polynomial.*

Proof. Assume X_i is not a zero-divisor of $\mathbb{C}[X_0,\ldots,X_n]/I$. Let I, g be such that $J := I + (g)$ and I have the same Hilbert polynomial. This means that $J^{(d)} = I^{(d)}$ for sufficiently large degree d. Hence, we have $X_i^d g \in I$ for sufficiently large d, and thus $g \in I$. □

By introducing a further variable Y we can achieve that Y is not a zero-divisor of $\mathbb{C}[X_0,\ldots,X_n,Y]/\overline{I}$, where $\overline{I} = \mathbb{C}[X_0,\ldots,X_n,Y]I$. Hence we obtain the following lower bound.

Theorem 4.9 *The problem* HILBERT$^{\mathbb{Z}}$ *is* FPSPACE*-hard.*

Based on this theorem, we can now improve the #P-lower bound in [1] for the problem to compute the ranks of cohomology groups of coherent sheaves on projective space. The lower bound is also true for the problem to compute the corresponding Euler characteristic.

For an introduction to sheaf cohomology we refer to [26, 29]. We encode the input to our problems as in [1]. Thus we specify a coherent sheaf on $\mathbb{P}^n$ by giving a *graded matrix*. This is a matrix $(p_{ij})_{1\le i\le s, 1\le j\le r}$ of homogeneous polynomials in $S := \mathbb{C}[X_0,\ldots,X_n]$ together with two arrays of integers $(d_1,\ldots,d_s)$ and $(e_1,\ldots,e_r)$ such that $\deg p_{ij} = d_i - e_j$ whenever $p_{ij} \neq 0$. A graded matrix defines a degree-preserving morphism

$$\gamma\colon \bigoplus_{j=1}^{r} S(e_j) \to \bigoplus_{i=1}^{s} S(d_i)$$

of graded S-modules. (As usual, $S(d)$ denotes S with degrees shifted by d to the left, so that $S(d)_0 = S_d$.) The cokernel M of γ is a finitely generated, graded S-module and thus determines a coherent sheaf $\widetilde{M}$ on $\mathbb{P}^n$ (cf. [26, p. 116]). We study the task to compute the dimensions of the cohomology $\mathbb{C}$-vector spaces $H^i(\mathbb{P}^n, \widetilde{M})$ for $i = 0,\ldots,n$. (It is known that these vector spaces vanish for $i > n$ [26, III.2.7].) The Euler characteristic of the sheaf $\widetilde{M}$ is defined as

$$\chi(\widetilde{M}) := \sum_{i=0}^{n} (-1)^i \dim H^i(\mathbb{P}^n, \widetilde{M}). \tag{10}$$

The link to the Hilbert polynomial is given by the following proposition, a proof of which can be found in [29, Section 7.6], see also [26, Ex. III.5.2].

Proposition 4.10 *Let $I \subseteq S := \mathbb{C}[X_0,\ldots,X_n]$ be a homogeneous ideal, $M = S/I$ and $p_M(T) \in \mathbb{Q}[T]$ the corresponding Hilbert polynomial. Then $p_M(d) = \chi(\widetilde{M}(d))$ for all $d \in \mathbb{Z}$.*

We now consider the following problems.

RANKSHEAF (*Rank of sheaf cohomology*) Given a morphism γ by a graded matrix as above and given $i \in \mathbb{N}$, compute $\dim H^i(\mathbb{P}^n, \widetilde{M})$ for $M = \mathrm{coker}\gamma$.

EULERSHEAF (*Euler characteristic of sheaf cohomology*) Given a morphism γ by a graded matrix as above, compute $\chi(\widetilde{M})$ for $M = \mathrm{coker}\gamma$.

The following result improves the #P-lower bound in [1].

Corollary 4.11 *The problems* RANKSHEAF$^{\mathbb{Z}}$ *and* EULERSHEAF$^{\mathbb{Z}}$ *are* FPSPACE*-hard.*

Proof. Clearly, EULERSHEAF$^{\mathbb{Z}}$ can be Turing reduced to RANKSHEAF$^{\mathbb{Z}}$. Theorem 4.9 tells us that HILBERT$^{\mathbb{Z}}$ is FPSPACE-hard. It is therefore sufficient to establish a Turing reduction from HILBERT$^{\mathbb{Z}}$ to EULERSHEAF$^{\mathbb{Z}}$.

An instance of HILBERT$^{\mathbb{Z}}$ is a family of non-constant homogeneous polynomials $f_1, \ldots, f_r$ in $\mathbb{Z}[X_0, \ldots, X_n]$. Let I denote the corresponding homogeneous ideal in $\mathbb{C}[X_0, \ldots, X_n]$. Consider the graded morphism $\gamma\colon \oplus_{j=1}^{r} S(e_j) \to S$ given by $f_1, \ldots, f_r$, where $e_j := -\deg f_j$. The cokernel M of γ equals S/I.

By Proposition 4.10 we have $p_M(d) = \chi(\widetilde{M}(d))$ for all $d \in \mathbb{Z}$. We can therefore obtain the values $p_M(d)$ for $d = 0, \ldots, n$ by $n+1$ calls to EULERSHEAF$^{\mathbb{Z}}$ and then compute the coefficients of p_M by interpolation. □

Remark 4.12 The algorithm in [6] combined with the upper bounds in [38] implies that HILBERT$^{\mathbb{Z}}$ is in FEXPSPACE. We do not know of any better upper bound on this problem. The known algorithms for sheaf cohomology (cf. [50, Chapter 8], [17]) suggest that RANKSHEAF$^{\mathbb{Z}}$ is in FEXPSPACE.

5 Hilbert polynomial and degeneracy loci

This section is devoted to the proof of Theorem 2.10.

5.1 Chern classes and Riemann-Roch

References for the material presented here are [15, 27, 41]. See also [21] for the algebraic geometry perspective. Let V be a variety (recall the conventions made for varieties at the beginning of §2). Chern classes are characteristic cohomology classes $c_i(E) \in H^{2i}(V)$ associated to a complex vector bundle $p\colon E \to V$. Chern classes are characterized axiomatically as follows:

1. $c_i(E) \in H^{2i}(V)$, $c_0(E) = 1$ and $c_1(\mathscr{L})$ generates $H^2(\mathbb{P}^n)$, where $\mathscr{L}$ is the canonical line bundle on $\mathbb{P}^n$.
2. Let $f\colon W \to V$ be a morphism of projective varieties. Then $c_i(f^*(E)) = f^*(c_i(E))$, where $f^*(E)$ denotes the pull-back bundle with respect to f.
3. (Whitney formula.) An exact sequence of bundles $0 \to E' \to E \to E'' \to 0$, implies $c_k(E) = \sum_i c_i(E') \smile c_{k-i}(E'')$, where $\smile$ denotes the cup-product.

The total Chern class is the sum $c(E) = \sum_{i\geq 0} c_i(E) \in H^*(V)$ of all the Chern classes. If V is smooth and irreducible of dimension m, then the top Chern class $c_m(TV)$ of the tangent bundle evaluated at the fundamental class yields the topological Euler characteristic of V:

$$\chi(V) = \deg(c_m(TV) \frown [V]),$$

see [41, page 170]. Here $\frown$ denotes the cap-product and $\deg\colon H_0(V) \to \mathbb{Z}$ is defined by $\deg(\sum_p n_p\,[p]) = \sum_p n_p$.

We now introduce the necessary terminology needed to state the Hirzebruch-Riemann-Roch theorem, which relates the Chern classes to the Hilbert polynomial.

Let $f(t) = \frac{t}{1-e^{-t}} \in \mathbb{Q}[[t]]$ be the formal power series (5) and $t_1, \ldots, t_n$ different variables. Consider the product

$$f(t_1)\cdots f(t_n) = \sum_{i=0}^{\infty} g_i(t_1, \ldots, t_n),$$

where the g_i are the i-th graded parts. The g_i are symmetric polynomials in the t_i, so there is an expression $g_n(t_1, \ldots, t_n) = T_n(\sigma_1, \ldots, \sigma_n)$, where σ_i is the i-th elementary symmetric function in the t_i. The $T_n \in \mathbb{Q}[X_1, \ldots, X_n]$ are called *Todd polynomials*. Note that T_n is homogeneous of weight n, when we define the weight of a monomial $X_1^{i_1}\cdots X_n^{i_n}$ to be the sum $\sum_{k=1}^n k i_k$. For example, the first three Todd polynomials are: $T_1 = \frac{1}{2}X_1,\ T_2 = \frac{1}{12}(X_1^2 + X_2),\ T_3 = \frac{1}{24}X_1X_2$.

If $c(TV)$ is the total Chern polynomial of the tangent bundle of a smooth variety V of dimension m, then we define the Todd class of V to be

$$\mathrm{td}(V) := 1 + \sum_{i=1}^{m} T_i(c_1, \ldots, c_i),$$

where here (and later) we write c_i as shorthand for $c_i(TV)$.

Consider the sum $\sum_{i=1}^n e^{t_i} = n + \sum_{i\geq 1} p_i(t_1, \ldots, t_n)$. Again, the p_i are symmetric, so there is a polynomial $K_n(X_1, \ldots, X_n)$ which evaluated at the elementary symmetric functions in the t_i yields p_n. If $c_i(E)$ are the Chern classes of a vector bundle E on a variety V, then the class

$$\mathrm{ch}(E) := 1 + \sum_{i\geq 1} K_i(c_1(E), \ldots, c_i(E))$$

is called the *Chern character* of E.

To a variety $V \subseteq \mathbb{P}^n$ and $d \in \mathbb{Z}$ one can assign the twisted sheaf $\mathcal{O}_V(d)$. The Chern character of the sheaf $\mathcal{O}_V(d)$ is particularly easy to describe. Since $\mathcal{O}_V(d)$ corresponds to a line bundle, we have only a first Chern class, which is $c_1(\mathcal{O}_V(d)) = dc_1(\mathscr{L}_V)$. Here, and in what follows, $\mathscr{L}_V$ denotes the line bundle corresponding to

the sheaf $\mathcal{O}_V(1)$ and $\mathscr{L}_V^\vee$ its dual, i.e., the canonical line bundle on V. For the Chern character we get

$$\mathrm{ch}(\mathcal{O}_V(d)) = e^{c_1(\mathcal{O}_V(d))} = \sum_{i\geq 0} \frac{d^i}{i!} c_1(\mathscr{L}_V)^i. \tag{11}$$

To a vector bundle E on a variety V there corresponds a locally free sheaf $\mathscr{E}$, see [47, VI.1.3] or [26, Ex. II.5.18]. Thus we can define the Euler characteristic $\chi(E)$ of E to be the Euler characteristic $\chi(\mathscr{E}) = \sum_i (-1)^i \dim H^i(V, \mathscr{E})$ of $\mathscr{E}$ with respect to sheaf cohomology, cf. Equation (10).

Lemma 5.1 *Let $V \subseteq \mathbb{P}^n$ be a variety and $d \in \mathbb{Z}$. Then the Euler characteristic of the line bundle $\mathcal{O}_V(d)$ equals the Hilbert polynomial of V evaluated at d, that is, $\chi(\mathcal{O}_V(d)) = p_V(d)$.*

Proof. Let $i\colon V \to \mathbb{P}^n$ be the inclusion and $\mathscr{F}$ be a coherent sheaf on V. Then $H^i(V, \mathscr{F}) = H^i(\mathbb{P}^n, i_*\mathscr{F})$ for all i, cf. [26, Lemma III.2.10]. If $M = S/I$ denotes the homogeneous coordinate ring of V, then $i_*\mathcal{O}_V(d) = \widetilde{M}(d)$, so by Proposition 4.10 we have $\chi(\mathcal{O}_V(d)) = p_V(d)$. □

With all these notions introduced, we can formulate the Hirzebruch-Riemann-Roch theorem.

Theorem 5.2 (Hirzebruch-Riemann-Roch, [27]) *Let E be a vector bundle on an irreducible smooth variety V of dimension m. Then*

$$\chi(E) = \deg\left((\mathrm{ch}(E) \smile \mathrm{td}(V))_m \frown [V]\right).$$

Theorem 5.2 combined with Lemma 5.1 and Equation (11) immediately yields the following.

Corollary 5.3 *Let $V \subseteq \mathbb{P}^n$ be an irreducible, smooth variety of dimension m. Then the k-th coefficient of the Hilbert polynomial of V is given by*

$$p_k(V) = \frac{1}{k!} \deg(c_1(\mathscr{L}_V)^k \smile T_{m-k}(c_1, \ldots, c_{m-k}) \frown [V]),$$

where $c_1, \ldots, c_m$ are the Chern classes of the tangent bundle TV.

5.2 Generalities on symmetric functions

We gather some results from the theory of symmetric functions that will be used later. Reference for this material are [36, 37], [22, Appendix A] and [21, Appendix A.9].

For a partition λ, we denote by λ' its conjugate partition. Recall the definition of $\Delta_\lambda(c)$ in Equation (4). Claims 1 and 2 of the following lemma are easy to verify, a proof of the third one is given in [21, Lemma A.9.2].

Lemma 5.4 *Let λ be a partition and $c = \{c_i\}_{i\in\mathbb{N}}$ be a sequence of elements of a commutative ring such that $c_0 = 1$.*

1. *The polynomial $\Delta_\lambda(c)$ is homogeneous of weight $|\lambda|$ in the c_i, when c_i has weight i.*
2. *Let $c^\vee = \{(-1)^i c_i\}_{i\in\mathbb{N}}$. Then $\Delta_\lambda(c^\vee) = (-1)^{|\lambda|}\Delta_\lambda(c)$.*
3. *Let $c^{-1} = \{c'_i\}_{i\in\mathbb{N}}$, where the c'_i are the coefficients of the inverse power series $(\sum_{i\geq 0} c_i t^i)^{-1}$. Then $\Delta_\lambda(c^{-1}) = \Delta_{\lambda'}(c^\vee)$.*

Example 5.5 We verify claims 2 and 3 of the previous lemma for the special case $\lambda = (1^k)$. For the partition (k) we have $\Delta_{(k)}(c) = c_k$. For the partition (1^k) we have $\Delta_{(1^k)}(c) = \det M_k(c)$, where $M_k(c)$ is the Toeplitz matrix

$$M_k(c) = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{k-1} & c_k \\ 1 & c_1 & c_2 & \cdots & c_{k-2} & c_{k-1} \\ 0 & 1 & c_1 & \cdots & c_{k-3} & c_{k-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & c_1 \end{pmatrix},$$

We can expand the determinant as

$$\det M_k(c) = -\sum_{i=1}^{k} (-1)^i c_i \det M_{k-i}(c).$$

This equation coincides with the recursive formula for the coefficients c'_j of the inverse power series $(\sum_{i\geq 0}(-1)^i c_i)^{-1}$. In particular, we obtain $\Delta_{(1^k)}(c) = \det M_k(c) = c'_k = \Delta_{(k)}\left(c^{-1}\right)$.

Let $\gamma = (\gamma_1, \ldots, \gamma_m)$ be variables and λ be a partition such that $|\lambda| \leq m$. Define the Schur polynomial associated to λ as

$$s_\lambda(\gamma) := s_\lambda(\gamma_1, \ldots, \gamma_m) = \frac{\det(\gamma_i^{\lambda_j + m - j})_{1\leq i,j\leq m}}{\det(\gamma_i^{m-j})_{1\leq i,j\leq m}}. \tag{12}$$

The polynomial $s_\lambda(\gamma)$ is symmetric and homogeneous of degree $|\lambda|$. Note that s_λ depends not only on the partition λ but also on m.

A proof of the following lemma can be found in [36, I.3] and [22, Appendix A].

Lemma 5.6 (Giambelli's formula) *Let λ be a partition with $|\lambda| \leq m$ and $c = \{c_i\}_{i\in\mathbb{N}}$ be given such that*

$$c_0 + c_1 t + \cdots + c_m t^m = \prod_{i=1}^{m} (1 + \gamma_i t),$$

i.e., the c_i are elementary symmetric functions in the γ_j. Then $\Delta_\lambda(c) = s_{\lambda'}(\gamma)$.

Example 5.7 If $\lambda = (k)$, then $s_\lambda(\gamma)$ is the k-th complete symmetric polynomial in the γ_i. This is the sum of all distinct monomials of degree k in the γ_i. If $\lambda = (1^k)$, then $s_\lambda(\gamma)$ is the k-th elementary symmetric function in the γ_i.

We will further need a formula expanding the Schur polynomial of a sum of variables. The following lemma follows from [21, Example A.9.1] (see also [36, Example I.3.10]).

Lemma 5.8 *Let λ be a partition with $|\lambda| \leq m$. Then*

$$s_\lambda(\gamma_1 + \beta, \ldots, \gamma_{m+1} + \beta) = \sum_{\mu \subseteq \lambda} d^m_{\lambda\mu} \beta^{|\lambda|-|\mu|} s_\mu(\gamma_1, \ldots, \gamma_{m+1}),$$

where

$$d^m_{\lambda\mu} = \det \binom{\lambda_i + m + 1 - i}{\mu_j + m + 1 - j}_{1 \leq i,j \leq m}$$

Example 5.9 Let $\lambda = (1^k)$. Then any subpartition $\mu \subseteq \lambda$ is of the form (1^j) for some $j \leq k$ and $d^m_{\lambda\mu} = \binom{m-j+1}{m-k+1}$. This follows from looking at the coefficients of the expansion of $s_{(1^k)}(\gamma_1 + \beta, \ldots, \gamma_{m+1} + \beta)$, using the fact that $s_{(1^k)}$ is an elementary symmetric function (see Example 5.7).

5.3 Proof of Theorem 2.10

In this section we derive Theorem 2.10 from Corollary 5.3 in a series of reductions. We start by observing a determinantal formula for the Todd polynomials. For what follows, we will often write $T_m(c)$ as shorthand for $T_m(c_1, \ldots, c_m)$.

Lemma 5.10 *Let $b = \{b_i\}_{i \in \mathbb{N}}$ be the sequence of rational numbers from Equation (5), $c_0 = 1$ and let $c_1, \ldots, c_m$ be variables. Then the m-th Todd polynomial is given by*

$$T_m(c) = \sum_{|\lambda| = m} \Delta_{\lambda'}(b) \Delta_\lambda(c),$$

where $\lambda = (\lambda_1, \ldots, \lambda_m)$ runs over all partitions of m.

Proof. Consider the (formal) factorizations

$$1 + \sum_{i=1}^m c_i = \prod_{j=1}^m (1 + \gamma_j), \quad 1 + \sum_{i=1}^m b_i = \prod_{j=1}^m (1 + \beta_j).$$

This amounts to writing the c_i and b_i as elementary symmetric functions in the γ_j and β_j, respectively. For a partition λ of m, let $m_\lambda(\gamma)$ be the sum of all different monomials arising from $\gamma_1^{\lambda_1} \cdots \gamma_m^{\lambda_m}$ by permutation of the γ_i (for example,

$m_{(1^m)}(\gamma) = \gamma_1 \cdots \gamma_m$). Also, let $\sigma_\lambda = \sigma_{\lambda_1} \cdots \sigma_{\lambda_m}$ denote the product of the elementary symmetric functions indexed by the partition. By definition, $T_m(c)$ is the m-th graded component of $f(\gamma_1) \cdots f(\gamma_m)$, where $f(\gamma_i) = \sum_{j \geq 0} b_j \gamma_i^j$. It follows that

$$\begin{aligned} T_m(c) &= \sum_{i_1 + \cdots + i_m = m} b_{i_1} \cdots b_{i_m} \gamma_1^{i_1} \cdots \gamma_m^{i_m} \\ &= \sum_{|\lambda| = m} b_{\lambda_1} \cdots b_{\lambda_m} m_\lambda(\gamma) = \sum_{|\lambda| = m} \sigma_\lambda(\beta) m_\lambda(\gamma). \end{aligned}$$

By [36, I.4(4.2'-3')] we have

$$\sum_{|\lambda| \leq m} \sigma_\lambda(\beta) m_\lambda(\gamma) = \prod_{1 \leq i,j \leq m} (1 + \beta_j \gamma_i) = \sum_{|\lambda| \leq m} s_{\lambda'}(\beta) s_\lambda(\gamma), \tag{13}$$

where s_λ is the Schur polynomial of the partition λ. Giambelli's formula (Lemma 5.6) expresses the Schur polynomials as determinants:

$$s_\lambda(\gamma) = \Delta_{\lambda'}(c).$$

Noting that $\deg s_\lambda(\gamma) = \deg m_\lambda(\gamma) = |\lambda|$ and taking the degree m parts in (13) completes the proof. □

What makes this formula useful is the fact that if c denotes the total Chern class of the tangent bundle of a smooth variety, the cohomology classes $\Delta_\lambda(c)$ can be put in relation to homology classes $[P_\lambda]$ of the generalized polar varieties.

To a smooth variety $V \subseteq \mathbb{P}^n$ of dimension m we can associate a vector bundle $\widetilde{T}V$ of rank $m+1$ such that for all $x \in V$, $\mathbb{T}_x V = \mathbb{P}(\widetilde{T}_x V)$.

The proof of the following proposition uses a result of Kempf and Laksov [30, Theorem 10], see also [21, Theorem 14.3].

Proposition 5.11 *Let $V \subseteq \mathbb{P}^n$ be an irreducible, smooth variety of dimension m and let λ be a partition with $|\lambda| \leq m$. Then*

$$\Delta_{\lambda'}(c(\widetilde{T}V)) \frown [V] = \begin{cases} (-1)^{|\lambda|}[P_\lambda] & \text{if } \lambda_1 \leq n - m \\ 0 & \text{else.} \end{cases}$$

Proof. Let E be the trivial $(n+1)$-bundle on V, $\widetilde{N}V := E/\widetilde{T}V$ and $\pi \colon E \to \widetilde{N}V$ be the projection map. Let λ be a partition with $|\lambda| \leq m$ and $\lambda_1 \leq n-m$. A flag $\underline{F} \in \mathcal{F}$ determines a partial flag $\underline{A}$ of trivial subbundles of E with A_i corresponding to $F_{\sigma_{i-1}}$ for $1 \leq i \leq m$. Thus $\operatorname{rank}(A_i) = \sigma_{i-1} + 1 = n - m + i - \lambda_i$. The determinantal locus

$$\Omega_\lambda(\underline{A}; \pi) = \{x \in V \mid \dim(\ker \pi(x) \cap A_i(x)) \geq i,\ 1 \leq i \leq m\}$$

studied in [21, Chapter 14] coincides with the generalized polar variety $P_\lambda(\underline{F})$. Here, by $\dim(\ker \pi(x) \cap A_i(x))$ we mean the affine dimension. The statement of [21, Theorem 14.3] implies that

$$\Delta_\lambda(c(\widetilde{N}V)) \frown [V] = [\Omega_\lambda(\underline{A}; \pi)] = [P_\lambda(\underline{F})],$$

provided $\Omega_\lambda(\underline{A}; \pi)$ is of pure codimension $|\lambda|$. For justifying this, note that in [21], $\Omega_\lambda(\underline{A}; \pi)$ is interpreted as a subscheme of V and its class is an element of the Chow group $A_*(\Omega_\lambda(\underline{A}; \pi))$. However, for generic $\underline{F} \in \mathcal{F}$, the scheme $\Omega_\lambda(\underline{A}; \pi)$ is multiplicity-free and of the right codimension, cf. Lemma 2.6. Moreover, there is a cycle map $A_*(\Omega_\lambda(\underline{A}; \pi)) \to H_*(\Omega_\lambda(\underline{A}; \sigma))$ [21, Chapter 19], which is compatible with the action of Chern classes.

Let $s(\widetilde{T}V) := 1/c(\widetilde{T}V)$ and $\widetilde{T}V^\vee$ denote the dual bundle. We have $c(\widetilde{N}V) = s(\widetilde{T}V)$ and $c_i(\widetilde{T}V^\vee) = (-1)^i c_i(\widetilde{T}V)$ [21]. Using Lemma 5.4, we thus get

$$\Delta_\lambda(c(\widetilde{N}V)) = \Delta_\lambda(s(\widetilde{T}V)) = \Delta_{\lambda'}(c(\widetilde{T}V^\vee)) = (-1)^{|\lambda|}\Delta_{\lambda'}(c(\widetilde{T}V)).$$

This shows the assertion in the case $\lambda_1 \leq n - m$. If $\lambda_1 > n - m$, then since $\widetilde{N}V$ is an $(n-m)$-bundle, we have $c_j(\widetilde{N}V) = 0$ for $j \geq \lambda_1$, which in turn implies $\Delta_\lambda(c(\widetilde{N}V)) = 0$. This completes the proof. □

We now turn attention to the tangent bundle TV.

Lemma 5.12 *Let $V \subseteq \mathbb{P}^n$ be an irreducible, smooth variety of dimension m and let λ be a partition with $|\lambda| \leq m$. For the tangent bundle TV we have*

$$\Delta_{\lambda'}(c(TV)) \frown [V] = \sum_{\substack{\mu \subseteq \lambda \\ \mu_1 \leq n-m}} (-1)^{|\mu|} d^m_{\lambda\mu} c_1(\mathscr{L}_V)^{|\lambda|-|\mu|} \frown [P_\mu],$$

where $d^m_{\lambda\mu}$ is defined as in Lemma 5.8.

Proof. It is well known (compare [25, Chapter 16]) that the tangent bundle TV of a smooth variety is given by $TV \cong \operatorname{Hom}\left(\mathscr{L}_V^\vee, \widetilde{T}V/\mathscr{L}_V^\vee\right)$. Taking the direct sum with the trivial bundle $E = \operatorname{Hom}(\mathscr{L}_V^\vee, \mathscr{L}_V^\vee)$ we get

$$TV \oplus E \cong \operatorname{Hom}\left(\mathscr{L}_V^\vee, \widetilde{T}V/\mathscr{L}_V^\vee\right) \oplus E \cong \operatorname{Hom}(\mathscr{L}_V^\vee, \widetilde{T}V) \cong \mathscr{L}_V \otimes \widetilde{T}V.$$

By the Whitney product formula (see §5.1) and the fact that $c(E) = 1$ we obtain

$$c(TV) = c(TV \oplus E) = c(\mathscr{L}_V \otimes \widetilde{T}V).$$

Let $c(\widetilde{T}V) = \prod_{i=1}^{m+1}(1 + \gamma_i)$ be the formal factorization and set $\beta := c_1(\mathscr{L}_V)$. By Giambelli's formula (Lemma 5.6) we have for a partition μ with $|\mu| \leq m$

$$\Delta_{\mu'}(c(\widetilde{T}V)) = s_\mu(\gamma_1, \ldots, \gamma_{m+1}). \tag{14}$$

On the other hand, it is known that (see [21, Remark 3.2.3b])

$$c(\mathscr{L}_V \otimes \widetilde{T}V) = \prod_{i=1}^{m+1}(1+\gamma_i+\beta).$$

Using Lemma 5.6 again, we get for any partition λ with $|\lambda| \leq m$

$$\Delta_{\lambda'}(c(TV)) = \Delta_{\lambda'}(c(\mathscr{L}_V \otimes \widetilde{T}V)) = s_\lambda(\gamma_1+\beta,\ldots,\gamma_{m+1}+\beta).$$

By Lemma 5.8 we have

$$s_\lambda(\gamma_1+\beta,\ldots,\gamma_{m+1}+\beta) = \sum_{\mu\subseteq\lambda} d^m_{\lambda\mu}\beta^{|\lambda|-|\mu|}s_\mu(\gamma_1,\ldots,\gamma_{m+1}).$$

Proposition 5.11 and (14) now imply for a partition μ with $|\mu| \leq m$:

$$s_\mu(\gamma)\frown[V] = \Delta_{\mu'}(c(\widetilde{T}V))\frown[V] = \begin{cases}(-1)^{|\mu|}[P_\mu] & \text{for } \mu_1 \leq n-m\\ 0 & \text{else.}\end{cases}$$

This finishes the proof. □

Example 5.13 Let $\lambda = (1^k)$. Then $\Delta_{\lambda'}(c) = c_k(TV)$, the k-th Chern class of the tangent bundle. By Example 5.9 we have $d^m_{\lambda\mu} = \binom{m-j+1}{m-k+1}$, where $\mu = (1^j)$. Plugging this into the formula of Lemma 5.12, we get

$$c_k(TV)\frown[V] = \sum_{j=0}^{k}(-1)^j\binom{m-j+1}{m-k+1}c_1(\mathscr{L}_V)^{k-j}\frown[P_j],$$

where the $[P_j]$ are the homology classes of the polar varieties. This formula is just the known expression for Chern classes in terms of polar classes, see for example [45, 10].

Proof of Theorem 2.10. Assume first that V is irreducible and write $c = c(TV)$. We express the Poincaré dual of the Todd polynomials in terms of the degeneracy loci, using Lemma 5.10 and Lemma 5.12:

$$\begin{aligned}T_{m-k}(c)\frown[V] &= \sum_{|\lambda|=m-k}\Delta_\lambda(b)\Delta_{\lambda'}(c)\frown[V]\\ &= \sum_{|\lambda|=m-k}\Delta_\lambda(b)\sum_{\substack{\mu\subseteq\lambda\\ \mu_1\leq n-m}}(-1)^{|\mu|}d^m_{\lambda\mu}c_1(\mathscr{L}_V)^{m-k-|\mu|}\frown[P_\mu]\\ &= \sum_{\substack{|\mu|\leq m-k\\ \mu_1\leq n-m}}\underbrace{(-1)^{|\mu|}\left(\sum_{\substack{\mu\subseteq\lambda\\ |\lambda|=m-k}}\Delta_\lambda(b)d^m_{\lambda\mu}\right)}_{=:\delta^{m,k}_\mu}c_1(\mathscr{L}_V)^{m-k-|\mu|}\frown[P_\mu]\end{aligned}$$

(Recall the definition of $\delta_\mu^{m,k}$ in Equation (6).) By Corollary 5.3 we obtain for the k-th coefficient $p_k(V)$ of the Hilbert polynomial of V

$$\begin{aligned} p_k(V) &= \frac{1}{k!} \deg \left(c_1(\mathscr{L}_V)^k \smile T_{m-k}(c) \frown [V] \right) \\ &= \sum_{\substack{|\mu| \le m-k \\ \mu_1 \le n-m}} \delta_\mu^{m,k} \deg \left(c_1(\mathscr{L}_V)^{m-|\mu|} \frown [P_\mu] \right). \end{aligned}$$

Since capping with $c_1(\mathscr{L}_V)^{m-|\mu|}$ corresponds to an intersection with a generic linear subspace of codimension $|\mu|$ in V, we have $\deg \left(c_1(\mathscr{L}_V)^{m-|\mu|} \frown [P_\mu] \right) = \deg P_\mu$. This proves the claim for irreducible V.

Now let $V = V_1 \cup \cdots \cup V_s$ be the decomposition of V into irreducible components of the same dimension. Let P_μ^i denote the degeneracy locus of V_i corresponding to μ and a generic flag $\underline{F}$. Since V is smooth, the V_i are pairwise disjoint and $P_\mu = P_\mu^1 \cup \cdots \cup P_\mu^s$, from which $\deg P_\mu = \sum_i \deg P_\mu^i$ follows. On the other hand, the Hilbert polynomial is additive on the V_i, which finishes the proof. □

Appendix

A.1 Proofs of Lemmas 2.6 and 2.8

For Lemma 2.6 we need the following result of Kleiman [31], see also [26, III.10].

Lemma A.1 *Let $\varphi\colon V \to Y$ be a morphism of smooth irreducible varieties and let $X \subseteq Y$ be a quasiprojective smooth subvariety. Assume that Y is a homogeneous space, with a connected algebraic group G acting transitively on it. Then for almost all $g \in G$, φ meets gX transversely. Moreover, if $\delta := \dim \varphi(V) + \dim X - \dim Y \ge 0$, then $\varphi(V) \cap gX$ is of pure dimension δ, for almost all $g \in G$.*

Recall that a partition λ was named admissible if $\lambda_1 \le n - m$ and $|\lambda| \le m + 1$.

Corollary A.2 *Let $Z \subseteq \mathbb{G}(m, n)$ be a quasiprojective irreducible subvariety and λ be an admissible partition. Then, for almost all $\underline{F} \in \mathcal{F}$, the intersection $Z \cap \Omega_\lambda(\underline{F})$ has codimension $|\lambda|$ in Z if $|\lambda| \le \dim Z$, and it is empty otherwise.*

Proof. Recall from (2) the cell decomposition $\Omega_\lambda(\underline{F}) = \cup_{\lambda \subseteq \mu} e_\mu(\underline{F})$. The Grassmannian $\mathbb{G}(m, n)$ is a homogeneous space with respect to the natural action of the linear group $G := \mathrm{GL}(n+1, \mathbb{C})$. The group G also acts transitively on the flag variety $\mathcal{F}$ (in fact, we can define $\mathcal{F}$ as a quotient of G, cf. [37, §3.6]) and we have $g e_\lambda(\underline{F}) = e_\lambda(g\underline{F})$. Decompose Z as finite disjoint union of smooth irreducible quasiprojective varieties Z_j. We can then apply Lemma A.1 to the inclusion of Z_j in $\mathbb{G}(m, n)$ and to a Schubert cell $X := e_\mu(\underline{F})$ in order to obtain that, for almost all $\underline{F}$, the intersection $Z_j \cap e_\mu(\underline{F})$ has the expected dimension (namely $\dim Z_j - |\mu|$ if this is nonnegative, otherwise the intersection is empty). This implies the assertion. □

Proof of Lemma 2.6. Without lack of generality we may assume that V is irreducible and not linear. (Note that for linear V, $\varphi(V)$ consists of one point only and thus the transversality condition $\varphi \pitchfork \Omega_\lambda(\underline{F})$ is equivalent to $\varphi(V) \cap \Omega_\lambda(\underline{F}) = \emptyset$, except for the trivial case $\lambda = (0)$. We may thus safely ignore linear components and restrict attention to a single nonlinear component.)

In this case, a result of Zak [23, §7] says that the Gauss map $\varphi\colon V \to \mathbb{G}(m,n)$ is finite, hence $\dim \varphi(V) = \dim V = m$. Since we are dealing with projective varieties, we have $\dim(\varphi(V) \cap \Omega_\lambda(\underline{F})) \geq \dim \varphi(V) + \dim \Omega_\lambda(\underline{F}) - \dim \mathbb{G}(m,n) = m - |\lambda|$ for any partition λ with $|\lambda| \leq m$ by a standard dimension argument, cf. [25, Thm.17.24].

(i) Let $\mu \supseteq \lambda$ be an admissible partition. Lemma A.1 implies that for almost all flags $\underline{F} \in \mathcal{F}$, φ meets $e_\mu(\underline{F})$ transversely. Looking at the cell decomposition (2) of $\Omega_\lambda(\underline{F})$, the claim follows (recall Definition 2.5).

(ii) We proceed by induction on the size of λ. Assume that the claim is true for all partitions μ such that $|\lambda| < |\mu| \leq m$. Suppose $\varphi \pitchfork \Omega_\lambda(\underline{F})$. The cell decomposition (2) of $\Omega_\lambda(\underline{F})$ implies that

$$\varphi(V) \cap \Omega_\lambda(\underline{F}) = \bigcup_{\mu \supseteq \lambda} \varphi(V) \cap e_\mu(\underline{F}).$$

We are going to show that $\varphi(V)$ intersects the cell $e_\lambda(\underline{F})$. If this were not the case, we had $\dim(\varphi(V) \cap \Omega_\lambda(\underline{F})) = \max_{\mu \supset \lambda}(m - |\mu|) < m - |\lambda|$, since we have $\dim(\varphi(V) \cap e_\mu(\underline{F})) = m - |\mu|$ by induction hypothesis. However, this contradicts the fact that $\dim(\varphi(V) \cap \Omega_\lambda(\underline{F})) \geq m - |\lambda|$.

Now note that $P_\lambda(\underline{F}) = \cup_{\mu \supseteq \lambda} \varphi^{-1}(e_\lambda(\underline{F}))$. By Remark 2.4, $\varphi^{-1}(e_\mu(\underline{F}))$ is either empty or of codimension $m - |\mu|$ in V. Moreover, we just showed that $\varphi^{-1}(e_\lambda(\underline{F}))$ is nonempty. This show the induction claim. The induction start where $|\lambda| = m$ is proved similarly.

(iii) We fix a flag $\underline{F}_0 \in \mathcal{F}$ and set $\Omega := \Omega_\lambda(\underline{F}_0)$, $e := e_\lambda(\underline{F}_0)$, $\partial e := \Omega - e$. Consider the map

$$\delta\colon G \to \mathbb{N},\ g \mapsto \deg \varphi^{-1}(g\Omega).$$

It is easy to see that the fibers of δ are constructible. Since G is irreducible, there exists a unique integer d_λ such that $\delta(g) = d_\lambda$ for almost all $g \in G$. We have to show that

$$\forall g \in G\ (\varphi \pitchfork g\Omega \Longrightarrow \delta(g) = d_\lambda).$$

Fix $g' \in G$ such that $\varphi \pitchfork g'\Omega$ holds and write $N := \delta(g')$. By (ii) we know that $\varphi^{-1}(g'\Omega)$ is of codimension $|\lambda|$ in V. It is sufficient to show that the function δ is constant in a *Euclidean* neighborhood of g'.

Let $A \subseteq \mathbb{P}^n$ be a linear subspace of dimension $k := n - m + |\lambda|$ such that

$$A \cap \varphi^{-1}(g'\partial e) = \emptyset \ \text{ and } A \pitchfork \varphi^{-1}(g'e). \tag{15}$$

Then the intersection $A \cap \varphi^{-1}(g'\Omega)$ consists of exactly N elements, say $x_1, \ldots, x_N$, cf. [43, §5A]. It is therefore sufficient to show that for all g in some neighborhood of g' condition (15) holds with g instead of g' and $|A \cap \varphi^{-1}(g\Omega)| = N$.

Fix a point x_i. Since $\varphi^{-1}(g'e)$ is smooth and of codimension k in $\mathbb{P}^n$, it can be defined locally around x_i by k equations $h_1(x,g'),\ldots,h_k(x,g')$. Moreover, these equations can be chosen such that $h_1,\ldots,h_{n-m}$ are local equations for V around x_i (not depending on g') and $h_{n-m+1},\ldots,h_k$ are obtained by pulling back local equations for $g'e$ at the smooth point $\varphi(x)$. Note that these last $|\lambda|$ equations are polynomials in x as well as in the parameter g'. Suppose that A is the zero set of linear forms $a_1,\ldots,a_{n-k}$. The transversality condition $A \pitchfork_{x_i} \varphi^{-1}(g'e)$ implies that $d_x h_1(x_i,g'),\ldots,d_x h_k(x_i,g'),a_1,\ldots,a_{n-k}$ are linearly independent. We are thus in the situation of the implicit function theorem: there is a Euclidean neighborhood U of g' and a Euclidean neighborhood V_i of x_i such that for each $g \in U$ the set $A \cap \varphi^{-1}(g\Omega) \cap V_i$ consists of exactly one point $x_i(g)$.

It remains to be seen that for g sufficiently close to g', the set $A \cap \varphi^{-1}(g\Omega)$ cannot have more than N elements. Suppose by contradiction that there is a sequence g_ν in G converging to g' such that for all ν, $A \cap \varphi^{-1}(g_\nu\Omega)$ contains a point y_ν different from $x_1(g_\nu),\ldots,x_N(g_\nu)$. Since V is compact, by passing to a subsequence, we may assume that y_ν converges to a point $y \in V$. By continuity, $y \in A \cap \varphi^{-1}(g'\Omega)$, hence $y = x_i$ for some i. We conclude that $y_\nu = x_i(g_\nu)$ for ν sufficiently large, contradicting our assumption. □

Proof of Lemma 2.8. We may assume without loss of generality that W is irreducible and that $\dim \psi^{-1}(\psi(x))$ is constant for $x \in W$, say equal to δ. (Decompose W into the locally closed subsets $W_i := \{x \in W \mid \dim \psi^{-1}(\psi(x)) = i\}$ and apply the assertion to the irreducible components of W_i.) By [47, §I.6.3 Thm. 7] (see also [25, Thm. 11.12]) we have

$$\dim W = \dim Z + \delta, \quad \dim R_\lambda(\underline{F}) \leq \dim \psi(R_\lambda(\underline{F})) + \delta,$$

where we have set $Z := \psi(W)$. Assume first that $|\lambda| \leq \dim Z$. By Corollary A.2, we have $\dim(Z \cap \Omega_\lambda(\underline{F})) = \dim Z - |\lambda|$ for almost all $\underline{F} \in \mathcal{F}$. Since $\psi(R_\lambda(\underline{F})) = Z \cap \Omega_\lambda(\underline{F})$, we obtain for almost all $\underline{F}$

$$\dim R_\lambda(\underline{F}) \leq \dim \psi(R_\lambda(\underline{F})) + \delta = \dim Z - |\lambda| + \delta = \dim W - |\lambda|.$$

If $|\lambda| > \dim Z$ we have $Z \cap \Omega_\lambda(\underline{F}) = \emptyset$ and therefore $R_\lambda(\underline{F}) = \emptyset$ for almost all $\underline{F}$. The inequality $\dim R_\lambda(\underline{F}) \geq \dim W - |\lambda|$ follows from [25, Thm. 17.24]. □

A.2 Expressing transversality

In this section we conclude the proof of Proposition 4.4. We consider input data of the form $(f,n,m,\mu,\underline{F},x)$ where $f = (f_1,\ldots,f_r)$ is a sequence of homogeneous polynomials in $\mathbb{C}[X_0,\ldots,X_n]$ satisfying the input condition (7) for $m \in \mathbb{N}$ and x is in the projective zero set V' of these polynomials. Moreover, $\underline{F}$ is a flag in $\mathcal{F}$ encoded by a matrix $a \in \mathbb{C}^{n\times(n+1)}$ and $\mu = (\mu_1,\ldots,\mu_{m+1})$ is an admissible partition with

respect to n and m. Recall from Lemma 4.1 the decomposition $V' = V \cup W$, where V is smooth of pure dimension m and $\dim W < m$.

Let $u \in \mathbb{C}^\infty$ be an encoding of (f, n, m, μ), let $a \in \mathbb{C}^\infty$ be an encoding of $\underline{F}$ and define the relation $\texttt{trans} \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty \times \mathbb{C}^\infty$ by

$$\texttt{trans}(u, a, x) :\Longleftrightarrow \big(x \in V \wedge \varphi(x) \in e_\mu(\underline{F}) \Longrightarrow \varphi \pitchfork_x e_\mu(\underline{F})\big),$$

where φ is the Gauss map of V.

Lemma A.3 *The relation* `trans` *is decidable in polynomial time by a constant-free machine over* $\mathbb{C}$.

Before going into the proof, we recall some facts concerning the manifold structure and cell decomposition of Grassmannians. For a comprehensive account, we refer to [20, III.9] and [37].

Dual to our usual encoding $a \in \mathbb{C}^{n\times(n+1)}$ of a flag $\underline{F} \in \mathcal{F}$ (where the F_i are zero sets of row forms of a), we can represent the flag $\underline{F}$ by a basis $\ell = (\ell_0, \ldots, \ell_n)$ of $\mathbb{C}^{n+1}$ such that F_i is spanned by $(\ell_0, \ldots, \ell_i)$ for $0 \le i \le n$. Clearly, this basis is uniquely determined by $\underline{F}$ up to scaling and can be computed from a in polynomial time.

Let μ be an admissible partition and let σ denote the associated sequence $0 \le \sigma_0 < \cdots < \sigma_m \le n$ defined by $\sigma_i := n - m + i - \mu_{i+1}$. To a fixed basis ℓ and μ we assign the Schubert cell $e_\mu := e_\mu(\ell) := e_\mu(\underline{F})$ according to (1). (To ease notation, we will usually drop the dependence on ℓ.) It is not hard to see that every subspace A in e_μ has a unique basis, that can be represented with respect to the basis ℓ by the rows of an $(m+1)\times(n+1)$ row echelon matrix, which has a 1 at the intersection of the i-th row with the σ_i-th column, and zeros in the i-th row to the right of this position as well as zeros in the σ_i-th column below this position, for all $0 \le i \le m$. In the case $m = 3, n = 7$, $\mu = (3, 1, 0)$, $\sigma = (1, 4, 6, 7)$ such an echelon matrix looks as follows:

$$\begin{pmatrix} * & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & 0 & * & * & 1 & 0 & 0 & 0 \\ * & 0 & * & * & 0 & * & 1 & 0 \\ * & 0 & * & * & 0 & * & 0 & 1 \end{pmatrix}. \tag{16}$$

In order to describe a covering of $\mathbb{G}(m, n)$ in terms of affine charts, consider for fixed ℓ the subspaces L_μ and $\overline{L}_\mu$ of $\mathbb{C}^{n+1}$ spanned by $\ell_{\sigma_0}, \ldots, \ell_{\sigma_m}$ and $\{\ell_j \mid j \notin \{\sigma_0, \ldots, \sigma_m\}\}$, respectively. We define $U_\mu := U_\mu(\ell) \subseteq \mathbb{G}(m, n)$ as the set of $(m+1)$-dimensional subspaces $A \subseteq \mathbb{C}^{n+1}$ whose projection to the subspace L_μ along $\overline{L}_\mu$ is an isomorphism. The open sets U_μ form an open cover of $\mathbb{G}(m, n)$. By identifying $A \in U_\mu$ with the graph of a linear map from L_μ to $\overline{L}_\mu$, we get an isomorphism

$$\alpha_\mu \colon U_\mu \xrightarrow{\sim} \mathrm{Hom}(L_\mu, \overline{L}_\mu) \xrightarrow{\sim} \mathbb{C}^{(n-m)\times(m+1)}, \tag{17}$$

where the last isomorphism maps an element of $\mathrm{Hom}(L_\mu, \overline{L}_\mu)$ to its matrix representation with respect to the bases defined by ℓ. The matrix $\alpha_\mu(A)$ is obtained

from the echelon matrix in (16) by removing all the σ_i-columns (thus removing a unit matrix of size $m+1$) and transposing. Taking this into account, we see that $e_\mu \subset U_\mu$ and that the image of e_μ under α_μ can be described as follows:

$$\alpha_\mu(e_\mu) = \{(a_{ij}) \in \mathbb{C}^{(n-m)\times(m+1)} \mid \ a_{ij} = 0 \text{ for } j \geq \sigma_i - i, 0 \leq i \leq m, 0 \leq j < n-m\}. \tag{18}$$

In particular, $\alpha_\mu(e_\mu)$ is a linear subspace of $\mathbb{C}^{(n-m)\times(m+1)}$.

Proof of Lemma A.3. Assume that $x \in V$ and $\varphi(x) \in e_\mu(\ell)$. The claim is that the transversality condition

$$T_{\varphi(x)}\mathbb{G}(m,n) = d_x\varphi(T_xV) + T_{\varphi(x)}e_\mu(\ell). \tag{19}$$

can be checked in constant-free polynomial time over $\mathbb{C}$.

In order to simplify notation, we will identify V with its affine cone $\widehat{V}$, x with an affine representative $\widehat{x}$, and the Gauss map φ with the corresponding morphism $\widehat{\varphi}\colon \widehat{V} - \{0\} \to \mathbb{G}(m,n)$. This causes no problem, since $d_x\varphi(T_xV) = d_{\widehat{x}}\widehat{\varphi}(T_{\widehat{x}}\widehat{V})$.

Given a basis ℓ and a partition μ, we represent $e_\mu = e_\mu(\ell)$ and the tangent spaces $T_A\mathbb{G}(m,n)$ and T_Ae_μ for $A \in e_\mu$ by means of the chart α_μ defined in (17). Around x we extend the Gauss map φ into the chart considering

$$\varphi_\mu\colon V \cap \varphi^{-1}(U_\mu) \xrightarrow{\varphi} U_\mu \xrightarrow{\alpha_\mu} \mathbb{C}^{(n-m)\times(m+1)}$$

In this light, Equation (19) translates into

$$\mathbb{C}^{(n-m)\times(m+1)} = d_x\varphi_\mu(T_xV) + \alpha_\mu(e_\mu).$$

Equation (18) gives an explicit and simple description of $\alpha_\mu(e_\mu)$. It remains to find a suitable description of $d_x\varphi_\mu(T_xV)$.

After a linear coordinate transformation, we may assume that $L_\mu = \mathbb{C}^{m+1} \times 0$ and $\overline{L}_\mu = 0 \times \mathbb{C}^{n-m}$. Thus without loss of generality, we assume that $X_0, \ldots, X_n$ are coordinates adapted to the decomposition $\mathbb{C}^{n+1} = L_\mu \oplus \overline{L}_\mu$.

Locally around the point x, the variety $V \subseteq \mathbb{C}^{n+1}$ is given as the zero set of the polynomials $f_1, \ldots, f_r$. Our assumption $\varphi(x) \in e_\mu$ means that T_xV lies in e_μ and thus in U_μ. This implies that the matrix $(\frac{\partial f_s}{\partial X_t}(x)))_{1\leq s\leq r, m<t\leq n}$ has rank $n-m$. After a permutation, we may assume that $(\frac{\partial f_s}{\partial X_t}(x)))_{1\leq s\leq n-m, m<t\leq n}$ is invertible. It will be convenient to use the abbreviations $X' := (X_0, \ldots, X_m)$ and $X'' := (X_{m+1}, \ldots, X_n)$.

By the implicit function theorem there are analytic functions $h_1, \ldots, h_{n-m}$ in X' such that in a neighborhood of x, the variety V is the graph of the analytic function $h := (h_1, \ldots, h_{n-m})$ defined on a neighborhood of x'. In particular, $x = (x', h(x'))$. From this we obtain the following description of the Gauss map:

$$\varphi_\mu(X', h(X')) = \Big(\frac{\partial h_s}{\partial X_i}(X')\Big)_{1\leq s\leq n-m, 0\leq i\leq m} \in \mathbb{C}^{(n-m)\times(m+1)}.$$

Hence the vector space $d_x\varphi_\mu(T_xV)$ is spanned by the matrices

$$\Big(\frac{\partial^2 h_s}{\partial X_i \partial X_j}(x')\Big)_{1\le s\le n-m, 0\le i\le m}$$

for $0 \le j \le m$. It remains to show that these matrices can be computed in constant-free polynomial time over $\mathbb{C}$. We remark that in the case of a hypersurface ($m = n-1$), this matrix just describes the second fundamental form of V at x.

By taking the derivative with respect to X_i of $f_s(X', h(X')) = 0$, we obtain

$$\frac{\partial f_s}{\partial X_i}(X', h(X')) + \sum_{t=m+1}^{n} \frac{\partial f_s}{\partial X_t}(X', h(X'))\frac{\partial h_t}{\partial X_i}(X') = 0 \tag{20}$$

for $1 \le s \le n-m, 0 \le i \le m$. From this, $\frac{\partial h_t}{\partial X_i}(x')$ can be computed by inverting the matrix $(\frac{\partial f_s}{\partial X_t}(x))$. By taking the derivative of Equation (20) with respect to X_j for $0 \le j \le m$ we get

$$\frac{\partial^2 f_s}{\partial X_i \partial X_j} + 2\sum_{t>m} \frac{\partial^2 f_s}{\partial X_t \partial X_j}\frac{\partial h_t}{\partial X_i} + \sum_{t,k>m} \frac{\partial^2 f_s}{\partial X_t \partial X_k}\frac{\partial h_t}{\partial X_i}\frac{\partial h_k}{\partial X_j} + \sum_{t>m} \frac{\partial f_s}{\partial X_t}\frac{\partial^2 h_t}{\partial X_i \partial X_j} = 0.$$

From this, the desired second order derivatives $\frac{\partial^2 h_t}{\partial X_i \partial X_j}(x')$ can be computed by inverting the matrix $(\frac{\partial f_s}{\partial X_t}(x))$. This finishes the proof. □

References

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

[2] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.

[3] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties: Geometry and algorithms. 2004. Preprint.

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

[5] D. Bayer and D. Mumford. What can be computed in algebraic geometry? In *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, Sympos. Math., XXXIV, pages 1–48. Cambridge Univ. Press, Cambridge, 1993.

[6] D. Bayer and M. Stillman. Computation of Hilbert functions. *J. Symb. Comp.*, 14:31–50, 1992.

[7] A.M. Bigatti, M. Caboara, and L. Robbiano. On the computation of Hilbert-Poincaré series. *Appl. Algebra Engrg. Comm. Comput.*, 2(1):21–33, 1991.

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

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

[10] J.P. Brasselet. From Chern classes to Milnor classes—a history of characteristic classes for singular varieties. In *Singularities—Sapporo 1998*, volume 29 of *Adv. Stud. Pure Math.*, pages 31–52. Kinokuniya, Tokyo, 2000.

[11] 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`.

[12] P. Bürgisser and F. Cucker. Variations by complexity theorists on three themes of Euler, Bézout, Betti, and Poincaré. In Jan Krajicek, editor, *Complexity of computations and proofs*, Quaderni di Matematica. 2004. To appear.

[13] P. Bürgisser, F. Cucker, and M. Lotz. Counting complexity classes for numeric computations III: Complex projective sets. *Foundations of Computational Mathematics*. Accepted.

[14] P. Bürgisser, F. Cucker, and M. Lotz. The complexity to compute the Euler characteristic of complex varieties. *C.R. Acad. Sc. Paris*, Ser I 339:371–376, 2004.

[15] S-S. Chern. Characteristic classes of Hermitian manifolds. *Annals of Mathematics (2)*, 47:85–121, 1946.

[16] A. M. Cohen, H. Cuypers, and H. Sterk. *Some tapas of computer algebra*, volume 4 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1999.

[17] W. Decker and D. Eisenbud. Sheaf algorithms using the exterior algebra. In *Computations in algebraic geometry with Macaulay 2*, volume 8 of *Algorithms Comput. Math.*, pages 215–249. Springer, Berlin, 2002.

[18] 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.

[19] L. Fortnow. Counting complexity. In *Complexity theory retrospective, II*, pages 81–107. Springer, New York, 1997.

[20] W. Fulton. *Young tableaux*, volume 35 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1997.

[21] W. Fulton. *Intersection Theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 1998.

[22] W. Fulton and J. Harris. *Representation Theory*. Number 129 in GTM. Springer Verlag, 1991.

[23] W. Fulton and R. Lazarsfeld. Connectivity and its applications in algebraic geometry. In *Algebraic geometry (Chicago, Ill., 1980)*, volume 862 of *Lecture Notes in Math.*, pages 26–92. Springer, Berlin, 1981.

[24] M. Giusti. Some effectivity problems in polynomial ideal theory. In *EUROSAM 84 (Cambridge, 1984)*, volume 174 of *Lecture Notes in Comput. Sci.*, pages 159–171. Springer, Berlin, 1984.

[25] J. Harris. *Algebraic Geometry: A First Course*. GTM. Springer Verlag, New York, 1992.

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

[27] F. Hirzebruch. *New Topological Methods in Algebraic Geometry*. Die Grundlehren der Mathematischen Wissenschaften, Band 131. Springer Verlag, 1966.

[28] D.T. Huyn. A superexponential lower bound for Gröbner bases and Church-rosser commutative Thue systems. *Information and Control*, 68:196–206, 1986.

[29] S. Iitaka. *Algebraic geometry*, volume 76 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[30] G. Kempf and D. Laksov. The determinantal formula of Schubert calculus. *Acta Math.*, 132:153–162, 1974.

[31] S. L. Kleiman. The transversality of a general translate. *Compositio Math.*, 28:287–297, 1974.

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

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

[34] Y. N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 227–234. Birkhäuser Boston, Boston, MA, 1991.

[35] Y. N. Lakshman and D. Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 217–225. Birkhäuser Boston, Boston, MA, 1991.

[36] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1995.

[37] L. Manivel. *Symmetric functions, Schubert polynomials and degeneracy loci*, volume 6 of *SMF/AMS Texts and Monographs*. American Mathematical Society, Providence, RI, 2001.

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

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

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

[41] J. Milnor and J.D. Stasheff. *Characteristic classes*. Princeton University Press, Princeton, N. J., 1974.

[42] F. Mora and H.M. Möller. The computation of the Hilbert function. In *EUROCAL*, number 162 in LNCS, pages 157–167. Springer Verlag, 1983.

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

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

[45] R. Piene. Polar classes of singular varieties. *Ann. Sci. École Norm. Sup. (4)*, 11(2):247–276, 1978.

[46] F. Severi. Sulle intersezioni delle varieta algebriche e sopra i loro caratteri e singolarita proiettive. *Mem. Accad. Sci. Torino*, 52(2):61–118, 1902.

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

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

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

[50] W.V. Vasconcelos. *Computational methods in commutative algebra and algebraic geometry*, volume 2 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998.

[51] E. W. Weisstein. Bernoulli number. Mathworld, Wolfram Research, Inc., http://mathworld.wolfram.com/BernoulliNumber.html.