On Numerical Invariants in Algebraic Complexity Theory

Dissertation

zur Erlangung des Doktorgrades
der Fakultät für Elektrotechnik, Informatik und Mathematik
der Universität Paderborn

vorgelegt von

Martin Lotz

Paderborn, den 17. Mai, 2005

Gutachter:	Prof. Dr. Peter Bürgisser
	Prof. Dr. Helmut Lenzing
	Prof. Dr. Felipe Cucker

Summary

A common theme in mathematics is the classification of mathematical objects by assigning numerical invariants to them. There are two ways in which such numerical invariants can appear in relation to computational complexity. On the one hand, mathematical invariants are used in the context of proving *lower complexity bounds*: they serve as obstructions to the existence of fast algorithms for solving certain problems. On the other hand, it is the computational complexity of actually computing such invariants that is of interest. The first part of this thesis is concerned with lower bounds for the problems of computing linear and bilinear maps. The invariants used, namely the *mean square volume*, *singular values*, and *rigidity*, belong to linear algebra. One of the main results is a tight lower bound of order $\Omega(n \log n)$ for the problem of multiplying two polynomials, in the model of bounded coefficient circuits. This lower bound is extended to circuits for which a limited number of unbounded scalar multiplications (help gates) are allowed. The second part is concerned with the complexity of actually computing numerical invariants. The objects of study are two of the most prominent invariants in algebraic geometry and topology: the *Euler characteristic* and the *Hilbert polynomial* of complex projective varieties. These problems are studied within the framework of counting complexity classes. It is shown that the problem of computing the Euler characteristic of a complex projective variety is on essentially the same level of difficulty as the problem of counting the number of solutions of a system of polynomial equations. A similar result is proved for the Hilbert polynomials, when the input variety is assumed to be smooth and equidimensional.

Danksagungen

An erster Stelle möchte ich meinem Betreuer Peter Bürgisser herzlichst danken: Für seine Unterstützung und Leitung, seine Geduld, und für alles was ich von ihm gelernt habe (mathematisch, und auch sonst). Estoy muy agradecido a Felipe Cucker por invitarme a Hong Kong, donde parte de este trabajo fue escrito, y por su ayuda en varios aspectos.

Darüber hinaus möchte ich mich bedanken bei:

- Joachim von zur Gathen, für das Bereitstellen eines Teils meiner Stelle, sein Interesse an meiner Arbeit, und für wichtige Literaturhinweise.
- Helmut Lenzing und dem Institut für Mathematik, für die hervorragenden Arbeitsbedingungen, und die Verlängerung meiner Stelle, was es mir ermöglicht hat die Arbeit hier zu beenden.
- Andreas Meyer and Peter Scheiblechner, für wertvolle Gespräche und Unterstützung in vielfacher Hinsicht.
- Die Teilnehmer der AG Geometrie. Einige der Dinge, die ich dort gelernt habe, konnten gewinnbringend in diese Arbeit einfliessen.
- Meinen Eltern, Evelina and Friedhelm, für das kritische Prüfen der Beweise ;-), und für sonstige Unterstützung.

Die vorliegende Arbeit wurde durch DFG Sachbeihilfe BU 1371 and PaSCo (Paderborn Institute for Scientific Computation) unterstützt.

Contents

Chapter 0

Introduction

A common theme in mathematics is the classification of mathematical objects by assigning numerical invariants to them. There are two ways in which such numerical invariants can appear in relation to computational complexity. On the one hand, mathematical invariants are used in the context of proving *lower complexity bounds*: they serve as obstructions to the existence of fast algorithms for solving certain problems. On the other hand, it is the computational complexity of actually computing such invariants that is of interest. The first part of this thesis is concerned with the use of invariants for proving lower complexity bounds. The problems under consideration are linear and bilinear maps, and the invariants used, namely the *mean square volume*, *singular values*, and *rigidity*, belong to linear algebra. The second part is concerned with the complexity of actually computing numerical invariants. The objects of study are two of the most prominent invariants in algebraic geometry and topology: the *Euler characteristic* and the *Hilbert polynomial* of complex projective varieties.

0.1 Lower Complexity Bounds

0.1.1 Linear Maps

Given an $m \times n$ matrix A over the complex numbers $\mathbb{C}$, how many arithmetic operations in $\mathbb{C}$ are necessary to compute the linear transformation $x \mapsto Ax$ for an input vector $x = (x_1, \dots, x_n) \in \mathbb{C}^n$? It is clear that this product can be computed with a budget of nm multiplications with scalars and $(n-1)m$ additions. On the other hand, there are obvious examples of matrices for which far less operations are needed. A less immediate example is the following:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \quad y = Ax = \begin{pmatrix} x_1 + x_2 + x_3 + x_4 \\ x_1 + ix_2 - x_3 - ix_4 \\ x_1 - x_2 + x_3 - x_4 \\ x_1 - ix_2 - x_3 + ix_4 \end{pmatrix}.$$

The vector $y = Ax$ can be computed from x using only 9 additions and scalar multiplications, as illustrated by the following sequence of instructions.

$$\begin{aligned}
g_1 &= x_1 + x_3\\
g_2 &= x_2 + x_4\\
g_3 &= x_1 - x_3\\
g_4 &= x_2 - x_4\\
g_5 &= i \cdot g_4\\
g_6 &= g_1 + g_2\\
g_7 &= g_3 + g_5\\
g_8 &= g_1 - g_2\\
g_9 &= g_3 - g_5
\end{aligned}$$

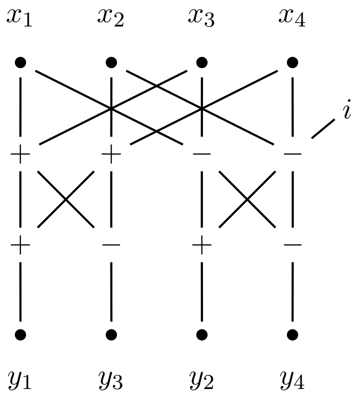


Figure 1: The Fast Fourier Transform

The above example is a special case of an important linear transformation called the *Discrete Fourier Transform* (DFT), while the algorithm presented in Figure (1) is known as the *Fast Fourier Transform* (FFT). In general, the $n \times n$ DFT matrix over $\mathbb{C}$ is the matrix $\mathrm{DFT}_n := \left(\omega^{ij}\right)_{0 \le i,j < n}$, where $\omega = e^{2\pi i/n}$ is an n-th root of unity in $\mathbb{C}$. The Fast Fourier Transform performs the linear transformation $x \mapsto \mathrm{DFT}_n x$ using $O(n \log n)$ arithmetic operations (a comprehensive exposition is found in [GG03, Chapter 8]). Is it possible to significantly improve this bound? Could there be a procedure that computes the DFT with a number of arithmetic operations that is *linear* in n? We don't know.

There is, however, a strong indication that the FFT algorithm is asymptotically optimal with respect to the number of arithmetic operations needed. The reason for this is a lower bound on the complexity of linear maps due to Jacques Morgenstern [Mor73]. For an $n \times n$ matrix A with entries in $\mathbb{C}$, let $\mathcal{C}(A)$ denote the minimal number of additions, subtractions, and scalar multiplications *with scalars of absolute value at most* 2, needed to compute the linear map $x \mapsto Ax$. Such a sequence of instructions is called *bounded coefficient circuit* (b.c. circuit for short) in the sequel. Morgenstern's bound states that

$$\mathcal{C}(A) \geq \log|\det A|. \tag{1}$$

In words, the absolute value of the determinant, that is, the volume of the parallelepiped spanned by the rows of A, provides a lower bound for the *size of a bounded coefficient circuit* computing the linear map $x \mapsto Ax$. It is known that the determinant of the DFT matrix is $n^{n/2}$, from which an $\frac{n}{2}\log n$ lower bound for the Discrete Fourier Transform follows.

In order to derive the Morgenstern's bound (1), assume $(g_1, \ldots, g_r)$ to be an optimal sequence of instructions computing Ax from $x = (x_1, \ldots, x_n)$.

For $0 \leq i \leq r$, let G_i be the $n \times (n+i)$ matrix whose columns consist of the vectors representing the linear forms $x_1, \dots, x_n, g_1, \dots, g_i$ (in particular, G_0 is the identity matrix). Let further $m_i := \mathrm{vol}_n(G_i)$ denote the maximum of the absolute values of all $n \times n$ subdeterminants of G_i. Every g_i is of the form $g_j + g_k$ or λg_j, with $j, k < i$ and $|\lambda| \leq 2$. From the multilinearity of the determinant it follows that m_i can *at most double* in each computation step. Since $m_0 = 1$, it follows that $|\det A| \leq m_r \leq 2^r$. Taking logarithms yields Morgenstern's bound.

One annoying drawback of this bound is the restriction to constants of bounded absolute value[1]. Leslie Valiant [Val76, Val77] analysed the problem of proving nonlinear lower bounds on the complexity of the Discrete Fourier Transform, and related linear problems, in the unrestricted model of arithmetic circuits. Despite many attempts, this problem is still open today. It should be noted, however, that many algorithms for arithmetic problems, like the Fast Fourier Transform and the fast algorithms based on it, use only small constants. Bernard Chazelle [Cha98] advocated the bounded coefficient model as a natural model of computation by arguing that the finite representation of numbers is essentially equivalent to bounded coefficients. In Section 0.1.3, the bounded coefficient property is relaxed by allowing a limited number of unbounded scalar multiplications ("help gates"), and it is shown that meaningful lower bounds are still possible in this setting.

0.1.2 Bilinear Maps

An important example of a bilinear map is *polynomial multiplication.* Given two univariate polynomials $f = \sum_{i=0}^{n-1} a_i X^i$ and $g = \sum_{j=0}^{n-1} b_j X^j$ in $\mathbb{C}[X]$, the problem consists of computing the product

$$f \cdot g = \sum_{k=0}^{2n-2} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

This map is readily interpreted as a bilinear map $\varphi\colon \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^{2n-1}$ on the coefficient vectors a and b. Polynomial multiplication can be reduced to the bilinear map of *cyclic convolution*, and vice versa:

$$f \star g = \sum_{k=0}^{n-1} c_k X^k, \quad c_k = \sum_{i+j \equiv k \bmod n} a_i b_j.$$

This corresponds to multiplication in the quotient ring $\mathbb{C}[X]/(X^n - 1)$. The cyclic convolution, in turn, can be computed using the Fast Fourier Transform (the procedure is described in detail in [GG03, Chapter 8]). The resulting circuit makes use of $O(n \log n)$ arithmetic operations. Again, the

[1] It is easy to see that the bound of 2 on the absolute value of the scalars can be replaced with any other constant c, with an increase in size of order $\log_2 c$.

question arises whether this is optimal. The main result of Part I (Theorem 2.4) consists of an $\Omega(n \log n)$ lower bound for the problem of computing the cyclic convolution, and thus also for polynomial multiplication, in the model of bounded coefficient circuits.

The proof is based on ideas by Ran Raz [Raz03] to establish a lower bound on the complexity of a bilinear map $(x, y) \mapsto \varphi(x, y)$ in terms of the complexity of the linear map $y \mapsto \varphi(a, y)$, obtained by specialising the first input to a (Lemma 1.4). Let A denote the matrix corresponding to $y \mapsto \varphi(a, y)$. A circuit for the computation of $y \mapsto Ay$ resulting from a hypothetical bounded coefficient circuit for φ has to be transformed into one with bounded coefficients with only a *small* increase in size. A lower bound s on $\mathcal{C}(A)$ thus leads to a lower bound on the complexity $\mathcal{C}(\varphi)$ of the original bilinear map:

$$\mathcal{C}(\varphi) \geq \rho\, \mathcal{C}(A) - R \geq \rho s - R, \tag{2}$$

where ρ and R depend on a and an optimal circuit for φ.

The existence of a suitable a is shown using the *probabilistic method*[2]: a vector a is chosen at random according to the standard normal distribution in a suitable linear subspace of $\mathbb{C}^n$ (Lemma 2.5). To obtain the bound (2), one has to show that this bound is satisfied with positive probability.

Raz applied this strategy to the bilinear map of matrix multiplication, and obtained an $\Omega(n^2 \log n)$ lower bound. His estimate of ρ and R, as well as his lower bound for the multiplication with a random matrix is based on his notion of geometric rigidity (see Equations (1.2) and (2.2)).

We apply a related approach to the problem of cyclic convolution. Let $\varphi\colon \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n$ denote the bilinear map of cyclic convolution. The matrix of the linear map $y \mapsto \varphi(a, y)$ resulting by specialising to $a \in \mathbb{C}^n$ is the *circulant matrix*

$$\mathrm{Circ}(a) = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}.$$

An estimate for the complexity of the multiplication with a random circulant matrix has to be found. An analysis reveals that, as in the case of matrix multiplication, such a bound does not seem attainable using only Morgenstern's bound. This problem is treated instead by extending Morgenstern's bound in a new way, which leads to the notion of the *r-Mean Square Volume* (MSV) of a complex matrix A, suggested by Bürgisser.

While the determinant $\det A$ is the product $\lambda_1 \cdots \lambda_n$ of the eigenvalues of A, the r-mean square volume of $A \in \mathbb{C}^{n \times n}$ $(1 \leq r \leq n)$ can be defined as

[2] See [AS00].

the square root of the r-th elementary symmetric function in the $|\lambda_j|^2$:

$$\mathrm{msv}_r A = \left(\sum_{1 \le i_1 < \cdots < i_r \le n} |\lambda_{i_1}|^2 \cdots |\lambda_{i_r}|^2 \right)^{1/2} .$$

The square of $\mathrm{msv}_r A$ is, up to sign, the r-th coefficient of the characteristic polynomial of AA^*, where A^* denotes the complex transpose of A. From the definition given it is clear that the MSV is unitary invariant. Moreover, $\mathrm{msv}_r A \ge |\lambda_1| \cdots |\lambda_r| \ge |\lambda_r|^r$, where $|\lambda_1| \ge \cdots \ge |\lambda_n|$ is assumed. The case $r = n$ yields the absolute value of the determinant.

Based on a refinement of the proof of Morgenstern's bound due to Raz, the following MSV bound is obtained:

$$\mathcal{C}(A) \ge \log \mathrm{msv}_r A - n/2.$$

An immediate corollary is the eigenvalue bound

$$\mathcal{C}(A) \ge r \log |\lambda_r| - n/2. \tag{3}$$

This bound also follows from Chazelle's Spectral Lemma [Cha00, Lemma 6.1] and Raz's rigidity bound [Raz03], see also Equations (2.2) and (1.2).

The advantage of the mean square volume in our situation can be outlined as follows (details may be found in the proof of Lemma 2.6). Assume the vector $a \in \mathbb{C}^n$ is chosen at random, according to the standard normal distribution in some fixed r-dimensional subspace of $\mathbb{C}^n$. The eigenvalues of $\mathrm{Circ}(a)$ are given by $\lambda = \mathrm{DFT}_n a$. Since it is known that $n^{-1/2}\mathrm{DFT}_n$ is unitary, the vector $\alpha = n^{-1/2}\lambda$ is also standard normal distributed in an r-dimensional subspace $U \subseteq \mathbb{C}^n$. Unfortunately, the mean of the determinant $\det \mathrm{Circ}(a) = n^n \prod_{i=1}^n |\alpha_i|^2$ turns out to be too small to obtain useful lower bounds. The mean square volume, however, allows to select a "good" set of eigenvalues:

$$\mathrm{msv}_r(\mathrm{Circ}(a))^2 = n^r \sum_{|J|=r} \prod_{k \in J} |\alpha_k|^2 \ge n^r \prod_{k \in I} |\alpha_k|^2$$

for any $I \subseteq [n]$, $|I| = r$. Given an $n \times r$ matrix $B = (b_1, \ldots, b_r)$ whose columns are an orthonormal basis of U and $I \subseteq [n]$, with $|I| = r$, denote by B_I the matrix consisting of the rows of B indexed by I. Using the Covariance Lemma 2.7, it is shown that for any index set I, with probability at least 1/2 the following holds:

$$\prod_{k \in I} |\alpha_k|^2 \ge \delta^r |\det B_I|^2,$$

where δ is some positive constant.

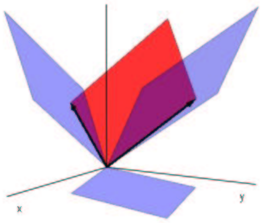


Figure 2: Volume contraction ratio

It is known (Binet-Cauchy formula) that the sum of the “volume contraction ratios” $|\det B_I|^2$ equals 1. Therefore, there exists an I such that $|\det B_I|^2 \geq \binom{n}{r}^{-1}$. Combining this with the MSV bound, we arrive at Lemma 2.6, which states that if a is standard normal distributed in an r-dimensional subspace of $\mathbb{C}^n$,

$$\mathcal{C}(\mathrm{Circ}(a)) \geq \frac{1}{2} r \log n - O(n) \tag{4}$$

holds with probability at least 1/2. The factor r plays a role in the determination of the parameters R and ρ, which bounds the increase in size of a circuit for φ after substituting a and transforming it into a b.c. circuit. The choice of $r = n/2$ leads to the lower bound on cyclic convolution

$$\mathcal{C}(\varphi) \geq \frac{1}{12} n \log n - O(n \log \log n).$$

Ran Raz (personal communication) pointed out a technically simpler proof for a variant of bound (4), which avoids the study of correlations. His proof is based on the eigenvalue (or rigidity) bound, combined with a lower bound for the sum of squares of the smallest r eigenvalues of a random circulant matrix. His proof is outlined in Section 2.3.

From the lower bound for the cyclic convolution, a nonlinear lower bound for polynomial multiplication, inversion of power series, and polynomial division with remainder is obtained by noting that the well-known reductions between these problems [BCS97] preserve the b.c. property. These lower bounds are again optimal up to order of magnitude.

0.1.3 Help Gates

It is possible to extend the eigenvalue bound (3) to circuits allowing up to $(1-\epsilon)n$ *help gates* $(0 < \epsilon \leq 1)$, corresponding to scalar multiplications with unbounded constants.

Assume a computation sequence $g_1, \ldots, g_r$ for computing the linear map $x \mapsto Ax$ is given, such that help gates are among the g_i, and the dimension of the space spanned by the linear forms computed at these help gates is $h < n$. Removing these help gates leads to a sequence computing a map $x \mapsto Bx$ for a matrix B that coincides with A on the orthogonal complement of the "help space", that is, the subspace spanned by the help gates. If $|\lambda_1| \geq \cdots \geq |\lambda_n|$ are absolute values of the eigenvalues of A, $|\widetilde{\lambda}_1| \geq \cdots \geq |\widetilde{\lambda}_n|$ those of B, then a classic result (see [GVL96, Theorem 8.1.7] or [CH31, I.§4.2]) states that

$$|\lambda_r| \geq |\widetilde{\lambda}_r| \geq |\lambda_{r+h}| \tag{5}$$

for $r + h \leq n$. Over $\mathbb{R}$, and assuming A to be symmetric, this can be seen geometrically by interpreting the absolute values of the eigenvalues as lengths of the principal axes of the ellipsoid $\{Ax \mid \|x\| = 1\}$. The eigenvalues of A restricted the complement of the help space are then the lengths of the principal axes of the intersection of this ellipsoid with this complement.

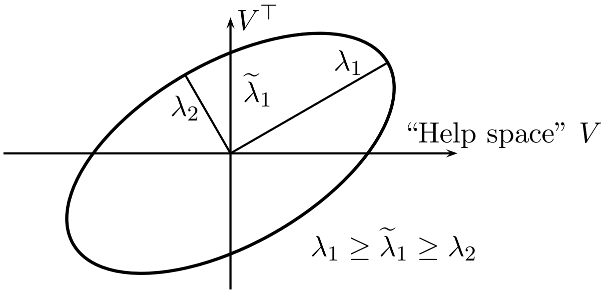


Figure 3: Interlacing property and help gates

Let $\mathcal{C}_h(A)$ denote the length of the shortest bounded coefficient sequence of instructions computing $x \mapsto Ax$ with at most h help gates. The MSV bound for B, the fact the number of instructions in the bounded coefficient sequence for B is at least h less than in the original sequence, and the "interlacing property" (5), give rise to the following lower bound:

$$\mathcal{C}_h(A) \geq r \log |\lambda_{r+h}| - n/2 + h.$$

This bound is derived in detail in Chapter 3. In the case of the Discrete Fourier Transform, this leads to an $\Omega(n \log n)$ lower bound in the presence of $(1 - \epsilon)n$ help gates, $0 < \epsilon \leq 1$.

In Part I, the ideas presented so far are developed in the more general context of $m \times n$ matrices, where *singular values* take over the role that the absolute values of the eigenvalues play for square matrices. It was shown by Bürgisser that the idea of allowing help gates carries over to the case of bilinear maps (Sections 3.2 and 3.3), although some subtleties have to be considered.

0.1.4 Related Work

A lower bound for the complexity of linear maps in terms of singular values was already given by Chazelle [Cha98, Cha00]. His applications are nonlinear lower bounds for range searching problems. His lower bound also works in the presence of up to $n/2$ help gates, which are allowed to compute *any* function on the intermediate results at unit cost. Thus his bound is weaker than ours with respect to the number of help gates allowed, but stronger with respect to the power of these help gates.

Several articles [NW95, Lok95, Pud98] studied b.c. arithmetic circuits. The concept of matrix rigidity, originally introduced in [Val77], hereby plays a vital role. A geometric variant of this concept (Euclidean metric instead of Hamming metric) is closely related to the singular value decomposition of a matrix and turns out to be an important tool, as worked out by Satyanarayana Lokam [Lok95]. Ran Raz [Raz02, Raz03] proved a nonlinear lower bound on the complexity of matrix multiplication in the b.c. model. This article and [NW95] seem to be the only ones which deal with the complexity of bilinear maps in the b.c. model of computation[3]. Recently, Maurice Jansen and Kenneth Regan [JR04] proved lower bounds on the complexity of linear and bilinear maps in a model of b.c. circuits that operate on orbits of the input vector under the action of a matrix group.

0.2 Complexity Theory in Geometry and Topology

Computational complexity theory is the study of the resources needed to solve problems algorithmically. The problems under consideration can be decision or computation problems, while the resources studied are usually space and time[4]. One of the central issues on the agenda of complexity theory, according to [Pap94], is to understand *why* some problems are inherently harder to solve than others. The standard approach chosen for this purpose is to group problem in *complexity classes* and to identify certain problems as *hardest* problems within each such class. It is this approach that we apply to the study of the algorithmic problems of computing the Euler characteristic and the Hilbert polynomial.

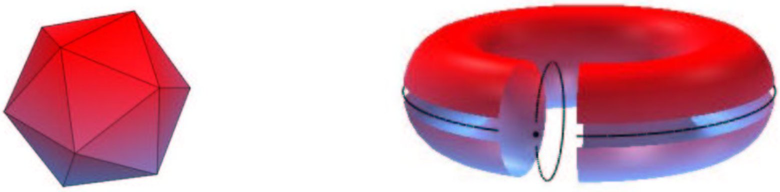
We begin by introducing these two objects and then proceed to discuss the philosophy of counting complexity theory.

[3] The proof of the $\Omega(n \log n)$ lower bound in [NW95](Cor. 3) is incorrect, as it assumes that the derivative inequality [BS83] carries over to the b.c. model. The counterexample $2^n \sum_{1 \leq i \leq n} X_i Y_i$, pointed out by Pavel Pudlák (personal communication), shows that this is not true.

[4] For precise definitions we refer to [Pap94]. Throughout this introduction, the reader may think of time complexity vaguely as the number of computation steps needed.

0.2.1 The Euler Characteristic

In its most simple incarnation, the Euler characteristic of a triangulated polyhedron counts the number of vertices minus the number of edges plus the number of faces[5]. In general, for spaces admitting a finite triangulation, it is the alternating sum of the number of i-simplices of the triangulation. The Euler characteristic of a topological space V is denoted by $\chi(V)$.



$\chi(S^2) = 12 - 30 + 20 = 2$ $\qquad$ $\chi(T) = 1 - 2 + 1 = 0$

Figure 4: Euler characteristic of polyhedra and cell complexes

The Euler characteristic does not depend on any specific triangulation of the object under consideration. In fact, it is a *topological invariant*, which means that it doesn't change under homeomorphism. Remarkably, the Euler characteristic appears in several different ways. It is the alternating sum of the Betti numbers $b_i(V)$ of a topological space V, that is, of the ranks of the homology groups $H_i(V;\mathbb{Z})$. For a finite cell complex, it is the alternating sum of the number of cells in each dimension (see Figure 4). For compact, differentiable manifolds, it can be characterised as the alternating sum over i of the number of critical points of index i of any Morse function $f\colon V \to \mathbb{R}$, or as the sum of the indices at the zeros of a vector field. Moreover, for a Riemannian manifold the Gauss-Bonnet theorem gives a characterisation of $\chi(V)$ in terms of Gaussian curvature. It is this diversity that makes the Euler characteristic fascinating from a purely mathematical, and accessible from a computational point of view.

A rich class of geometric objects are those defined as the zero sets of systems of polynomial equations over the complex numbers $\mathbb{C}$. These will be referred to as (complex affine) *varieties* throughout this introduction. Given a set of homogeneous multivariate polynomials over $\mathbb{C}$, their common zero set in complex projective n-space $\mathbb{P}^n$ is called a *projective variety.* An affine or projective variety is equipped with the Euclidean topology via the identification $\mathbb{C} \cong \mathbb{R}^2$. The computational problem we are interested in is the following.

ProjEuler$_{\mathbb{C}}$ (*Euler characteristic of projective varieties*). Given a finite

[5] See [Lak76] for a vivid account of the history of the Euler characteristic.

> set of complex homogeneous polynomials, compute the Euler characteristic of its projective zero set.

The model of computation in which this question is discussed is the *BSS machine* over $\mathbb{C}$, named after Lenore Blum, Mike Shub, and Steve Smale [BSS89, BCSS98]. Questions regarding the important issue on how the polynomials are encoded as inputs to such a machine are discussed in Section 4.4. In contrast to the lower bounds described in Part I, the complexity bounds for $\text{ProjEuler}_{\mathbb{C}}$ are not absolute. Instead, following the tradition of complexity theory, this problem is put in relation to another important computational problem, which in a sense captures the complexity of a large class of problems. This is the problem $\#\text{HN}_{\mathbb{C}}$ of counting the number of solutions of a system of polynomial equations. Informally, our main result about the Euler characteristic can be stated as follows:

> The problem $\text{ProjEuler}_{\mathbb{C}}$ is polynomial time equivalent to the problem $\#\text{HN}_{\mathbb{C}}$ of counting the number of solutions of a system of polynomial equations.

What this means is, roughly speaking, that any subroutine for one of these problems can be used to solve the other problem with a number of computation steps that is, up to the subroutine calls, polynomially bounded in the input size.

The mathematical aspects of the reduction of $\text{ProjEuler}_{\mathbb{C}}$ to $\#\text{HN}_{\mathbb{C}}$ are briefly outlined next. The reduction exploits an intimate relation of the Euler characteristic to the notion of *degree* of a complex projective variety. The degree d of a variety $V \subseteq \mathbb{P}^n$ counts the number of intersection points of V with a generic linear subspace of complementary dimension. For the zero set of a single irreducible polynomial f (called a hypersurface), the degree of this set is simply the degree of f.

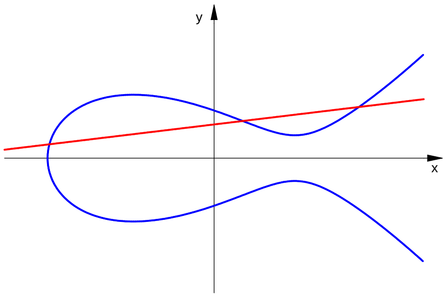


Figure 5: Degree of elliptic curve $y^2 = x^3 - x + 1/2$

For an irreducible, smooth hypersurface $V \subseteq \mathbb{P}^n$ of degree d, the relationship of Euler characteristic and degree is explicitly given by:

$$\chi(V) = \frac{1}{d}((1-d)^{n+1} - 1) + n + 1. \tag{6}$$

As an example, an irreducible degree 3 curve in $\mathbb{P}^2$ (elliptic curve) has Euler characteristic 0. In fact, such a curve is topologically a torus.

Assume now that an irreducible polynomial f is given, and that the resulting hypersurface V is smooth. A straight-forward approach for computing the Euler characteristic would be to intersect V with a random line $L \subseteq \mathbb{P}^n$, that is, add $n-1$ linear equations $g_1, \ldots, g_{n-1}$, and count the number of solutions to the system $f = 0, g_1 = 0, \ldots, g_{n-1} = 0$. The resulting number is with high probability the degree d, and Equation (6) thus yields the Euler characteristic. In order to turn this procedure into a deterministic polynomial time reduction, it has to be properly "derandomised".

The approach taken is to use the notion of *transversality*: if L meets V transversely, then the number of intersection point equals the degree. The point is now that it is possible to compute in polynomial time a sequence of lines $L_1, \ldots, L_r$, such that the majority of them meets V transversely. This was shown in [BC04a]. The reason for this to be possible is that the transversality condition can be expressed in a certain way as a first order formula over the reals, and moreover this formula is generically satisfied. It can be shown from this that a sequence of vectors called *partial witness sequence* can be constructed, such that the majority of them satisfies the first-order formula describing transversality. These ideas are discussed in Section 5.2.

A generalisation of Equation (6) to possibly singular hypersurfaces was found by Paolo Aluffi [Alu03] in terms of *projective degrees*. The sequence of projective degrees $d_0, \ldots, d_{n-1}$ is derived from the graph of the gradient map

$$\mathbb{P}^n \setminus \Sigma \to \mathbb{P}^n, \quad x = (x_0 \colon \cdots : x_n) \mapsto \left(\frac{\partial f}{\partial X_0}(x) \colon \cdots : \frac{\partial f}{\partial X_n}(x)\right),$$

where f is the polynomial defining the hypersurface and Σ is the common zero set of the partial derivatives $\partial f / \partial X_j$. Aluffi's formula states that

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

The d_i are arrived at by counting the points of the intersection of the closure of the graph Γ of the gradient map in $\mathbb{P}^n \times \mathbb{P}^n$ with a product of generic linear spaces. It is shown in Section 6.4 that such "generic" linear subspaces can be computed in polynomial time from f, using transversality arguments as in the case of the degree. The case of general varieties is reduced to the case of a hypersurface using the inclusion-exclusion principle (Lemma

4.5). Even though the resulting sum is exponential, it follows from an important principle in counting complexity, namely the closure of $\#\mathrm{P}_{\mathbb{C}}$ (and related classes) under exponential summation, that a single system of polynomial equations can be constructed such that the Euler characteristic can be deduced from the number of solutions of this system. The idea is best illustrated using a trivial example. Let $F(u,x)$ be a parametrised system of polynomial equations. For fixed $u \in \{0,1\}^m$, let $\varphi(u)$ denote the number of solutions of the system of equations $F(u,x)$ in x. Then the exponential sum $\sum_{u\in\{0,1\}^m} \varphi(u)$ equals the number of solutions of the single system of polynomial equations $F'(u,x)$ in (u,x), which arises from F by adding the equations $u_j^2 = u_j$, $1 \leq j \leq m$.

0.2.2 The Hilbert Polynomial

Let $V \subseteq \mathbb{C}^n$ be a complex projective variety of dimension m. The *Hilbert polynomial* $p_V(T)$ associated to V is a polynomial of degree m with rational coefficients, which encodes valuable geometric information about V: its leading coefficient is the degree of V, and the constant coefficient gives the *arithmetic genus* of V.

Our goal is to relate the complexity of computing the Hilbert polynomial to the problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting points. This goal is achieved for the case of smooth, equidimensional varieties. These are smooth varieties, in which each irreducible component has the same dimension. The main result of Chapter 7 can be roughly formulated as follows:

> The problem of computing the Hilbert polynomial of a smooth, equidimensional complex projective variety is at most as hard as the problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of solutions of a system of polynomial equations.

The reduction uses concepts from enumerative geometry and Schubert calculus, as well as the Hirzebruch-Riemann-Roch theorem, in order to express the coefficients of the Hilbert polynomial in terms of the degrees of certain *polar varieties*. An example of a plane curve $V \subseteq \mathbb{P}^2$, given by an irreducible polynomial f, should illustrate the case. The Hilbert polynomial of V is given by

$$p_V(T) = dT + (1-g),$$

where d is the degree of f and g the *genus* of the curve. The leading coefficient equals the number of intersection points of V with a generic line. Is there a way of interpreting $1-g$ in terms of the number of solutions to a polynomial system? For smooth V, given a point $y \in \mathbb{P}^2$, define the *polar variety* $P(y)$ to be the set of points in V whose tangents at V contain y:

$$P(y) := \{x \in V \mid y \in \mathbb{T}_x V\},$$

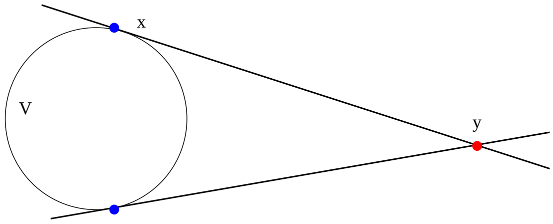


Figure 6: Polar variety

where $\mathbb{T}_x V$ denotes the tangent of V at x.

If V is smooth, then for *generic* $y \in \mathbb{P}^2$, the constant coefficient of the Hilbert polynomial is given by

$$1 - g = d - \frac{1}{2}|P(y)|.$$

This shows how the constant coefficient of the Hilbert polynomial can be computed by means of "counting points". In this simple example it is easy to see, using Bézout's Theorem, that $|P(y)| = d(d-1)$ holds for generic y. This is consistent with the well known formula $g = \frac{1}{2}(d-1)(d-2)$ for the genus. More on algebraic curves can be found in [BK81] or [Ful89]

For a general smooth, purely m-dimensional variety V, the projective tangent space $\mathbb{T}_x V$ at x lives in the *Grassmannian* $\mathbb{G}(m, n)$ of m-planes in $\mathbb{P}^n$. Associated to a partition $\lambda = (\lambda_1, \dots, \lambda_m)$ and a flag of subspaces $\underline{F}\colon F_0 \subseteq \cdots F_{n-1} \subseteq \mathbb{P}^n$, there are the Schubert varieties $\Omega_\lambda(\underline{F}) \subseteq \mathbb{G}(m, n)$. The *Gauss map* $\varphi\colon V \to \mathbb{G}(m, n)$ maps each $x \in V$ to its projective tangent space $\mathbb{T}_x V$, and the pullback

$$P_\lambda(\underline{F}) := \varphi^{-1}(\Omega_\lambda(\underline{F}))$$

is a generalised polar variety, called a degeneracy locus. The plane curve example arises as special case with $n = 2$, $m = 1$, and $\lambda = (1)$. It is known that there is an integer d_λ, such that for generic $\underline{F}$, $d_\lambda = \deg P_\lambda(\underline{F})$ holds. These integers will be called *projective characters*.

Just as in the case of a smooth curve, there is a relationship between the projective characters and the coefficients of the Hilbert polynomial of a smooth, purely m-dimensional variety $V \subseteq \mathbb{P}^n$. Let $p_k(V)$ denote the k-th coefficient of the Hilbert polynomial of V. Then for $0 \le k \le m$:

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

where the $\delta_\mu^{m,k}$ are combinatorial constants, easily describable in terms of m, k, and the partition μ. This formula is derived in Chapter 8 using the

Hirzebruch-Riemann-Roch theorem, which describes the coefficients of the Hilbert polynomial in terms of determinants in the Chern classes of the tangent bundle of V. These determinants, in turn, can be realised by the homology classes of degeneracy loci using a classic result of Schubert calculus (Kempf and Laksov [KL74], Fulton [Ful98]).

Again, the problem arises of how to compute a flag $\underline{F}$ such that $d_\lambda = \deg P_\lambda(\underline{F})$. As for the degree, such a flag can be computed by exploiting transversality. It is shown that whenever the Gauss map φ meets the Schubert variety transversely (in a sense described in Section 7.2), then the condition $d_\lambda = \deg P_\lambda(\underline{F})$ is satisfied. It is then shown in Section 7.4 that this transversality condition can be expressed as a logical formula in a way that allows to actually compute such a flag $\underline{F}$ in polynomial time, using the methods of Chapter 5. The fact that the formula for $p_k(V)$ consists of an exponential sum is treated by saying the magic formula "$\#\mathrm{P}_\mathbb{C}$ is closed under exponential summation", see the previous section and Chapter 5.

0.2.3 Counting Complexity Theory

As already seen in the previous sections, the computation of the Euler characteristic and the Hilbert polynomial is intimately related to a special kind of computation problem, called *counting problem*. While a decision problem usually asks for the existence of a solution to a problem instance, the corresponding counting problem asks for the *number of solutions*.

Counting problems abound in computer science and mathematics. A classic example from optimisation theory, well suited to illustrate the ideas of counting complexity theory, is the *assignment problem*: given a collection of n jobs and n persons, each of whom capable of performing one or more of the jobs, find an assignment such that each person gets to do a different job. Such an assignment is commonly referred to as a *perfect matching*[6] (see Figure 7). The corresponding counting problem asks for the number of possible perfect matchings.

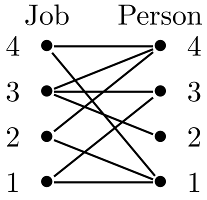
The problem of telling whether an assignment exists at all is easy from a computational complexity point of view. There are algorithms solving this problem in time $O(n^3)$ and better, see for example [Pap94, Chapter 1] and the references therein.

The number of perfect matchings is equal to the *permanent* of the adjacency matrix of the problem. The adjacency matrix is the $n \times n$-matrix M, whose (i, j)-th entry is 1 if person i is qualified for job j, and 0 else.

The *permanent* is then defined as

$$\mathrm{Per}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} m_{i,\sigma(i)},$$

[6] There are several variations to this theme. For example, each person may be differently skilled at each of the jobs, and the problem may consist in finding an optimal assignment.



$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\mathrm{Per}(M) = 2$$

Figure 7: There are 2 perfect matchings

where S_n is the symmetric group of permutations on n letters, and $m_{i,j}$ denotes the (i, j)-th entry of the matrix M. Multiplying each monomial in the sum with the sign of the corresponding permutation gives rise to the familiar definition of the *determinant* of the matrix. While the determinant can be computed with $O(n^3)$ arithmetic operations using Gaussian elimination, the permanent has pertinaciously resisted all attempts at finding an efficient algorithm. In fact, the best known methods for computing (deterministically and exact) the permanent require $O(2^n)$ arithmetic operations [Knu98, 4.6.4, Ex. 9-10][7].

In his seminal work [Val79a, Val79b], Leslie Valiant developed an elegant theory that, in a way, explains why the determinant is easier than the permanent. Roughly speaking, the class P consists of decision problems solvable in polynomial time, while NP consists of decision problems, such that each problem instance can be verified in polynomial time with the help of a *witness*. For example, the problem of deciding whether a bipartite graph has a perfect matching is in NP, since each graph with a perfect matching has this matching as witness. Valiant introduced the counting class $\#\mathsf{P}$, which consists of functions mapping problem instances in NP to the number of satisfying witnesses. He showed that the problem of computing the permanent of a $0-1$ matrix is *complete* in this class. This implies that the problem of computing the permanent is at least as hard as any other problem in $\#\mathsf{P}$, and hence, a deterministic, polynomial time algorithm for this problem would imply $\mathsf{P} = \mathsf{NP}$. It is generally believed that $\mathsf{P} \neq \mathsf{NP}$ holds, even though there is no proof for this yet.

A counting complexity theory for algebraic and geometric problems over the real and complex numbers, based on the BSS model of computation, was initiated by Klaus Meer, Peter Bürgisser and Felipe Cucker [Mee00, BC04a, BC04b, BCL05]. The complexity class $\#\mathrm{P}_{\mathbb{C}}$ plays the role of $\#\mathsf{P}$ over the complex numbers, and the basic complete problem for this class is the prob-

[7] It should be noted, though, that there are randomised algorithms that *approximate* a permanent with non-negative entries in polynomial time, as shown by Jerrum, Sinclair, and Vigoda [JSV01]

lem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of solutions of a system of polynomial equations (the notation $\mathrm{HN}_{\mathbb{C}}$ stands for "Hilbert's Nullstellensatz over $\mathbb{C}$). It is then investigated how other geometric problems relate to $\#\mathrm{HN}_{\mathbb{C}}$ in terms of computational complexity.

When an enumerative geometer asks for the solution of a counting problems, like "how many lines in $\mathbb{P}^3$ intersect four given lines" [KL72], then it is assumed that the answer is the same for almost all (generic) lines. This assumption is based on what was called "Das Princip von der Erhaltung der Anzahl" by Hermann Schubert in 1879 [Sch79]. The same principle is implicit in the characterisation of the notion of degree as the number of intersection points of a variety with a "generic" linear space of complementary dimension. In a sense, the problem of computing the degree is a more natural representative for geometric counting problems than $\#\mathrm{HN}_{\mathbb{C}}$.

In terms of counting complexity theory, this state of affairs leads to the notions of *generic parsimonious reductions*, coined by Peter Bürgisser. In a very simplified way, the definition states that a function φ generically reduces to a counting function ψ in $\#\mathrm{P}_{\mathbb{C}}$, if $\varphi(x) = \psi(x, r)$ holds for all x and "almost all" parameters r. In practice, one would like to be able to actually compute such an r. Therefore, the definition involves a relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$, such that

1. $(x, r) \in R \Rightarrow \varphi(x) = \psi(x, r)$,
2. For all x, $R(x, r)$ is satisfied for almost all r.

Moreover, the relation is required to be expressible in a certain way, namely in the *constant free polynomial hierarchy over the reals.* It was shown in [BC04a, BCL05] (based on earlier work by Koiran [Koi97a]) that for such R, a satisfying parameter r can be computed in polynomial time by means of *partial witness sequences.* (A key step in the construction is closely related to the concept of correct test sequences from Heintz and Schnorr [HS82], and similar ideas also appear in the Witness Theorem [BCSS96, BCSS98].) All this is explained in Chapter 5.

Going back to geometry, it is well-known that a statement of the form

> A holds for almost all (generic) B

can very often be rephrased as saying

> A holds whenever B satisfies a certain transversality property,
> almost all (generic) B satisfy this transversality property.

This observation can be seen as a model for the definition of generic parsimonious reductions. In fact, it is this kind of situation that is encountered in the study of the Euler characteristic and the Hilbert polynomial in Chapters 6 and 7, where it is shown that suitable transversality conditions can be expressed in a way that leads to generic parsimonious reductions.

0.2.4 Related Work on Algorithms

There has been some recent work on the algorithmic problem of computing the Euler characteristic for real and complex varieties. The first single-exponential algorithm for computing the Euler characteristic of a semi-algebraic set was given by Saugata Basu [Bas99], see also [BPR03, Chapter 13]. The complexity of computing the Euler characteristic was studied in [BC04a], where using Morse theory, it was shown that this problem is polynomial time equivalent to the problem of counting points in semi-algebraic sets. Algorithms for computing the Euler characteristic of projective varieties where described by Uli Walther [Wal00, Wal02] and Paolo Aluffi [Alu03].

Several algorithms for computing the Hilbert function and Hilbert polynomial are known. To our knowledge, the first algorithms for the Hilbert function were described by Möller and Mora [MM83]. An important approach for computing Hilbert functions is based on a result of Macaulay [Mac27], which states that the Hilbert function of an ideal equals the Hilbert function of its initial ideal with respect to some monomial order, see also [Eis95, 15.10.2]. Therefore, the problem of computing the Hilbert function can be reduced to the case of monomial ideals via Gröbner bases [Buc65, Buc85], see also [CLO98, Eis95]. A polynomial space algorithm for computing the Hilbert function of a monomial ideal was described by Dave Bayer and Mike Stillman [BS92], see also [Eis95, Chapter 15] and [GP02, Chapter 5]. Moreover, Bayer and Stillman show that the problem of computing a Hilbert function is NP-hard. Other algorithms were described by Bigatti, Caboara, and Robbiano [BCR91, Big97] of the CoCoA Research Team. Some of these algorithms have been implemented in computer algebra systems, such as Macaulay2 [GS], Singular [GPS01], and CoCoA [CoC].

The algorithms considered so far all rely on the computation of Gröbner bases, which leads to bad worst-case complexity estimates. In fact, the problem of computing a Gröbner basis is exponential space hard [May97]. Both the cardinality and the maximal degree of a Gröbner basis can be double exponential in the number of variables [MM82, Huy86, BS88]. 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 [Giu84, DFGS91, BM93, May97]. 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. It is interesting to note that, while the Hilbert function is computed with the help of Gröbner bases, knowledge of the Hilbert function of an ideal can help speed up the Buchberger algorithm [Tra96] (see also [GP02, Remark 5.2.9]).

The problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of solutions of a system of polynomial equations has received some attention in the past. 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 [DFGS91, Lak91, LL91]. The number of solutions can then be determined using linear algebra techniques, as described for example in [CCS99, Chapter 2]. Another approach for counting the number of solutions is by using Bernstein's theorem, which interprets the number of solutions in $(\mathbb{C}^n)^*$ as mixed volume of the *Newton polytope* of the system of equations. However, this method assumes some regularity condition on the system of equations. For this and other approaches for solving $\#\mathrm{HN}_{\mathbb{C}}$ (such as resultants), a reference is [CLO98] (see also [Stu02]).

0.3 Outline

Chapter 1 contains a description of the model of computation, as well as basic definitions and results from linear algebra and probability theory. Chapter 2 contains the heart of Part I. Here, the mean square volume bound is introduced, and a lower bound for the bilinear problem of cyclic convolution is obtained. This bound is then used to obtain lower bounds for the problems of polynomial multiplication and division, and inversion of power series. Chapter 3 extends the lower bounds to a model of computation in which a limited number of help gates are allowed. This extension is carried out for linear and bilinear maps.

Chapter 4 recalls basic concepts from geometry, topology, and gives a short introduction to BSS complexity theory. In Chapter 5, a counting complexity theory in the BSS model of computation is explored. This chapter introduces the important notion of generic parsimonious reduction and the complexity classes related to this notion. The framework developed in Chapter 5 is used in Chapters 6 and 7, in order to study the complexity of the Euler characteristic and the Hilbert polynomial, respectively. Finally, Chapter 8 contains the derivation of a formula for the coefficients of the Hilbert polynomial in terms of the degrees of polar classes.

0.4 Credits

Most of the content of this thesis has been published as joint work with Peter Bürgisser and Felipe Cucker in [BL02, BL04, BCL04, BCL05, BL05]. The contribution of my co-authors, and that of the other persons mentioned below, is gratefully acknowledged.

Part I

The concept of the mean square volume as unitary invariant measure was proposed by Peter Bürgisser. The idea of studying help gates was inspired by the work of Bernard Chazelle [Cha98, Cha00] (even though our approach differs significantly), and the extension of help gates to the bilinear case (Section 3.3) was suggested by Satyanarayana Lokam and carried out by Bürgisser. The study of correlated standard normal vectors, specifically in Lemma 2.7 and in Section 3.2, has benefited from the expert advise of Mario Wschebor. The alternative proof of the lower bound on the complexity of random circulants in Section 2.3 has been worked out around an approach suggested by Ran Raz. Much of the content of Part I profits from Raz's article [Raz03], which was pointed out to us by Joachim von zur Gathen.

Part II

The study of counting complexity theory described in Chapter 5 was first started by Bürgisser and Cucker in [BC04a, BC04b], based on earlier ideas of Pascal Koiran [Koi97b, Koi99a], and further developed in [BCL05].

The main part of Chapter 6 is concerned with the application of Aluffi's formula (6.8) in order to obtain upper bounds on the complexity of the Euler characteristic. Aluffi's article [Alu03] was pointed out to us by Joachim von zur Gathen.

In Chapter 7, the idea of how to use the *testable input condition* (Equation (7.1)) instead of just assuming the input varieties to be smooth and equidimensional, was proposed by Bürgisser. The #P-hardness of the Hilbert polynomial of smooth varieties (Proposition 7.17) follows along the lines of the #P-hardness proof of Eric Bach for sheaf cohomology [Bac99], while the PSPACE lower bound for the Hilbert polynomials was pointed out by Bürgisser.

Part I

Lower Bounds on the Complexity of Bilinear Maps

Chapter 1

Preliminaries I

1.1 The Model of Computation

The underlying model of computation throughout Part I is the model of algebraic straight-line programs over $\mathbb{C}$, which are often called arithmetic circuits in the literature. Straight-line programs differ from the notion of circuit as introduced in Part II, in that no sign gates are allowed. For details on this model of computation, the reader may consult Chapter 4 of [BCS97]. By a result of Volker Strassen [Str73b], it is possible to exclude divisions without loss of generality.

Definition 1.1 A *straight-line program* Γ expecting inputs of length n is a sequence $(\Gamma_1, \ldots, \Gamma_r)$ of instructions $\Gamma_s = (\omega_s; i_s, j_s)$, $\omega_s \in \{\times, +, -\}$ or $\Gamma_s = (\omega_s; i_s)$, $\omega_s \in \mathbb{C}$, with integers i_s, j_s satisfying $-n < i_s, j_s < s$. A sequence of polynomials $b_{-n+1}, \ldots, b_r$ is called the *result sequence* of Γ on input variables $a_1, \ldots, a_n$, if for $-n < s \leq 0$, $b_s = a_{n+s}$, and for $1 \leq s \leq r$, $b_s = b_{i_s} \omega_s b_{j_s}$ if $\Gamma_s = (\omega_s; i_s, j_s)$ and $b_s = \omega_s b_{i_s}$ if $\Gamma_s = (\omega_s; i_s)$. Γ is said to *compute* a set of polynomials F on input $a_1, \ldots, a_n$, if the elements in F are among those of the result sequence of Γ on that input. The *size* $\mathcal{S}(\Gamma)$ of Γ is the number r of its instructions.

A straight-line program can be interpreted as directed graph with nodes (gates) corresponding to inputs, outputs, arithmetic operations, and scalar multiplications. In the sequel, such straight-line programs are briefly referred to as circuits. A circuit in which the scalar multiplication is restricted to scalars of absolute value at most 2 is called a *bounded coefficient circuit* (b.c. circuit for short). Any circuit can be transformed into a b.c. circuit by replacing a multiplication with a scalar λ with at most $\log|\lambda|$[1]. additions and a multiplication with a scalar of absolute value at most 2. By the same argument it follows that the bound of 2 could be replaced by any other fixed bound.

Next, restricted notions of circuits are introduced, which are designed for computing linear and bilinear maps.

[1] Unless otherwise stated, log always refers to logarithms to the base 2.

Definition 1.2 A circuit $\Gamma = (\Gamma_1, \ldots, \Gamma_r)$ expecting inputs $X_1, \ldots, X_n$ is called a *linear circuit*, if $\omega_s \in \{+, -\}$ for every instruction $\Gamma_s = (\omega_s; i_s, j_s)$, or $\omega_s \in \mathbb{C}$ if the instruction is of the form $(\omega_s; i_s)$. A circuit on inputs $X_1, \ldots, X_m, Y_1, \ldots, Y_n$ is called a *bilinear circuit*, if its sequence of instructions can be partitioned as $\Gamma = (\Gamma^{(1)}, \Gamma^{(2)}, \Gamma^{(3)}, \Gamma^{(4)})$, where $\Gamma^{(1)}$ is a linear circuit with the X_i as inputs, $\Gamma^{(2)}$ is a linear circuit with the Y_j as inputs, each instruction from $\Gamma^{(3)}$ has the form $(\times; i, j)$, with $\Gamma_i \in \Gamma^{(1)}$ and $\Gamma_j \in \Gamma^{(2)}$, and $\Gamma^{(4)}$ is a linear circuit with the previously computed results of $\Gamma^{(3)}$ as inputs. In other words, $\Gamma^{(1)}$ and $\Gamma^{(2)}$ compute linear functions $f_1, \ldots, f_k$ in the X_i and $g_1, \ldots, g_\ell$ in the Y_j. $\Gamma^{(3)}$ then multiplies the f_i with the g_j and $\Gamma^{(4)}$ computes linear combinations of the products $f_i g_j$.

It is clear that linear circuits compute linear maps and that bilinear circuits compute bilinear maps. On the other hand, it can be shown that any linear (bilinear) map can be computed by a linear (bilinear) circuit such that the size increases at most by a constant factor (see [BCS97, Theorem 13.1, Proposition 14.1]). This remains true when considering bounded coefficient circuits. From now on, only bounded coefficient circuits are considered.

Definition 1.3 The *b.c. complexity* $\mathcal{C}(\varphi)$ of a bilinear map $\varphi\colon \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^p$ is the size of a smallest b.c. bilinear circuit computing φ. The *b.c. complexity* $\mathcal{C}(\varphi^A)$ of a linear map $\varphi^A\colon \mathbb{C}^n \to \mathbb{C}^m$ (or of the corresponding matrix $A \in \mathbb{C}^{m \times n}$), is the size of a smallest b.c. linear circuit computing φ^A.

By abuse of notation, $\mathcal{C}(F)$ also stands for the smallest size of a b.c. circuit computing a set F of polynomials from the variables.

Let $\varphi\colon \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^p$ be a bilinear map described by $\varphi_\ell(X, Y) = \sum_{i,j} a_{ij\ell} X_i Y_j$ for $1 \leq \ell \leq p$. Assuming $|a_{ij\ell}| \leq 2$, it is clear that $\mathcal{C}(\varphi) \leq 3mnp$.

The complexity of a bilinear map φ can be related to the complexity of the associated linear map $\varphi(a, -)$, where $a \in \mathbb{C}^m$. The following lemma is from [Raz03].

Lemma 1.4 *Let $\varphi\colon \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^p$ be a bilinear map and Γ be a b.c. bilinear circuit computing φ. If $f_1, \ldots, f_k$ are the linear maps computed by the circuit on the first set of inputs, then for all $a \in \mathbb{C}^m$:*

$$\mathcal{C}(\varphi(a, -)) \leq \mathcal{S}(\Gamma) + p \log (\max_j |f_j(a)|).$$

Proof. Let $a \in \mathbb{C}^m$ be chosen and set $\gamma = \max_j |f_j(a)|$. Transform the circuit Γ into a linear circuit Γ' by the following steps:

1. replace the first argument x of the input by a,

2. replace each multiplication by $f_i(a)$ with a multiplication by $2\gamma^{-1} f_i(a)$,

3. multiply each output by $\gamma/2$, simulating this with at most $\log(\gamma/2)$ additions and one multiplication with a scalar of absolute value at most 2.

This is a b.c. linear circuit computing the map $\varphi(a, -)\colon \mathbb{C}^n \to \mathbb{C}^p$. Since there are p outputs, the size increases by at most $p \log \gamma$. □

1.2 Singular Values and Matrix Rigidity

The *Singular Value Decomposition* (SVD) is an important matrix decompositions in numerical analysis. Lately, it has also come to play a prominent role in proving lower bounds for linear circuits [Lok95, Cha98, Raz03]. In this section, some basic facts about singular values are presented, and it is shown how they relate to notions of matrix rigidity. For a more detailed account on the SVD, the reader may consult [GVL96]. The classic [CH31, Chapt. 1, Sect. 4] also turns out to be a useful reference.

The *singular values* of $A \in \mathbb{C}^{m\times n}$, $\sigma_1 \geq \ldots \geq \sigma_{\min\{m,n\}}$, can be defined as the square roots of the eigenvalues of the Hermitian $m \times m$-matrix AA^*, where A^* denotes the complex transpose of A. Alternatively, the singular values can be characterised as follows:

$$\sigma_{r+1} = \min\{\|A - B\|_2 \mid B \in \mathbb{C}^{m\times n}, \mathrm{rk}(B) \leq r\},$$

where $\|\cdot\|_2$ denotes the matrix 2-norm, that is, $\|A\|_2 := \max_{\|x\|_2=1} \|Ax\|_2$. A geometric version of the above characterisation is the Courant-Fischer min-max theorem stating

$$\sigma_{r+1} \;=\; \min_{\mathrm{codim} V = r} \;\; \max_{x \in V - \{0\}} \frac{\|Ax\|_2}{\|x\|_2},$$

where the minimum is taken over all linear subspace $V \subseteq \mathbb{C}^n$ of codimension r in $\mathbb{C}^n$. This description implies the following useful fact from matrix perturbation theory:

$$\sigma_{r+h}(A) \leq \sigma_r(A + E) \tag{1.1}$$

if the matrix E has rank at most h.

More generally, for a metric d on $\mathbb{C}^{m\times n}$ (or $\mathbb{R}^{m\times n}$) and $1 \leq r \leq \min\{m, n\}$, the *r-rigidity* of a matrix A can be defined to be the distance of A to the set of all matrices of rank at most r with respect to this metric:

$$\mathrm{rig}_{\mathrm{d},r}(A) = \min\{\mathrm{d}(A, B) \mid B \in \mathbb{C}^{m\times n}, \mathrm{rk}(B) \leq r\}.$$

Using the Hamming metric, we obtain the usual matrix rigidity as introduced in [Val77]. On the other hand, using the metric induced by the 1, 2-norm $\|A\|_{1,2} := \max_{\|x\|_1=1} \|Ax\|_2$, we obtain the following *geometric* notion of *rigidity*, as introduced in [Raz03]:

$$\mathrm{rig}_r(A) \;=\; \min_{\dim V = r} \;\; \max_{1 \leq i \leq n} \mathrm{dist}(a_i, V).$$

Here, the a_i are the column vectors of $A \in \mathbb{C}^{m\times n}$ and dist denotes the usual Euclidean distance, that is, $\mathrm{dist}(a_i, V) := \min_{b\in V} \|a_i - b\|_2$. Note that in Equation (1.2), the minimum is taken over subspaces of *dimension* r.

Example 1.5 Let $A \in \mathbb{R}^{3\times 3}$. Then $\mathrm{rig}_0(A)$ is the radius of the smallest ball centred at the origin enclosing the column vectors of A, $\mathrm{rig}_1(A)$ the radius of the smallest cylinder through the origin containing these vectors, and $\mathrm{rig}_2(A)$ has a similar interpretation in terms of plates.

Notions of rigidity can be related to one another the same way the underlying norms can. In particular, the following relationship between the geometric rigidity and the singular values holds:

$$\frac{1}{\sqrt{n}}\,\sigma_{r+1}(A) \leq \mathrm{rig}_r(A) \leq \sigma_{r+1}(A). \tag{1.2}$$

The proofs of these inequalities are based on well known inequalities for matrix norms. To be precise, note that if B is a matrix of rank at most r with columns b_i, then

$$\|A-B\|_{1,2}^2 = \max_i \|a_i - b_i\|_2^2 \geq \frac{1}{n}\sum_{i=1}^{n}\|a_i - b_i\|_2^2 \geq \frac{1}{n}\|A-B\|_2^2 \geq \frac{1}{n}\sigma_{r+1}^2,$$

which shows the left inequality. The other inequality follows from the fact that $\|A\|_{1,2} \leq \|A\|_2$, which is a consequence of $\|x\|_2 \leq \|x\|_1$ for $x \in \mathbb{C}^n$.

1.3 Complex Gaussian Vectors

A random vector $X = (X_1, \ldots, X_n)$ in $\mathbb{R}^n$ is called *standard Gaussian* if its components X_i are i.i.d. standard normal distributed. An orthogonal transformation of such a random vector is again standard Gaussian.

We will mainly consider random vectors Z assuming values in $\mathbb{C}^n$. By identifying $\mathbb{C}^n$ with $\mathbb{R}^{2n}$, Z can be thought of as a $2n$-dimensional real random vector. In particular, it makes sense to say that such Z is (standard) Gaussian in $\mathbb{C}^n$.

Let U be an r-dimensional linear subspace of $\mathbb{C}^n$. A random vector Z with values in U is *standard Gaussian in* U if for some orthonormal basis $b_1, \ldots, b_r$ of U this vector can be written as $Z = \sum_j \zeta_j b_j$, where the random vector (ζ_j) of the components is standard Gaussian in $\mathbb{C}^r$. This description does not depend on the choice of the orthonormal basis. In fact, the transformation of a standard Gaussian vector with a unitary matrix is again standard Gaussian, since a unitary transformation $\mathbb{C}^r \to \mathbb{C}^r$ induces an orthogonal transformation $\mathbb{R}^{2r} \to \mathbb{R}^{2r}$.

The following lemma is a direct consequence of known facts about the normal distribution. For completeness, a proof is outlined.

Lemma 1.6 *Let $(Z_1, \ldots, Z_n)$ be standard Gaussian in $\mathbb{C}^n$. Consider a complex linear combination $S = f_1 Z_1 + \ldots + f_n Z_n$ with $f = (f_1, \ldots, f_n) \in \mathbb{C}^n$. Then the real and imaginary parts of S are independent and normal distributed, each with mean 0 and variance $\|f\|_2^2$. Moreover, $T := |S|^2/2\|f\|_2^2$ is exponentially distributed with parameter 1. That is, the density function is e^{-t} for $t \geq 0$ and the mean and the variance of T are both equal to 1.*

Proof. If $X_1, \ldots, X_n$ are standard Gaussian in $\mathbb{R}$ and $a = (a_1, \ldots, a_n) \in \mathbb{R}^n$, then $\sum_{j=1}^n a_j X_j$ is again Gaussian, with mean 0 and variance $\|a\|_2^2$. Note also that if $Z = X + iY$ with independent standard Gaussian X, Y in $\mathbb{R}$, and $f \in \mathbb{C}$, then the real and imaginary parts of fZ are again independent, with mean 0 and variance $|f|^2$. This follows from the fact that complex multiplication corresponds to a rotation and scaling. These observations imply the first statement of the lemma. In particular, $\|f\|_2^{-1} S = X + iY$ with independent standard Gaussian X, Y in $\mathbb{R}$. It is well known that in this case, $\frac{1}{2}(X^2 + Y^2)$ is exponentially distributed with parameter 1, see [Fel71, II.2-3] for details □

1.4 Bounding Large Deviations

The theory of large deviations is concerned with the rate of convergence of the strong law of large numbers. For a proof of the following theorem, references are [DZ98] or [Bau02, Section 12].

Theorem 1.7 (Cramér, Chernoff) *Let $S_n = X_1 + \cdots + X_n$ be the sum of i.i.d. random variables, each with mean η. Then for any $\epsilon \geq 0$*

$$\mathrm{P}\left[S_n \geq (\eta + \epsilon)n\right] \leq e^{-\mathrm{I}(\eta+\epsilon)n}$$

where

$$\mathrm{I}(\lambda) := \sup_{t\in\mathbb{R}} \{t\lambda - \ln \mathrm{E}[e^{tX_1}]\}$$

is called the rate function (or Cramér transform) of the distribution of X_1.

This theorem will be needed in the case of exponentially distributed variables. For X exponentially distributed with parameter 1 and $t < 1$,

$$\mathrm{E}[e^{tX}] = \int_0^\infty e^{tx} e^{-x} dx = \frac{1}{1-t}.$$

In this case, the rate function takes the form

$$\mathrm{I}(\lambda) = \sup_{t<1} \{\lambda t + \ln(1-t)\},$$

and a simple calculation shows that for $\lambda > 0$ the supremum takes the value $(\lambda - 1) - \ln \lambda$.

If Z is standard normal distributed in $\mathbb{C}^n$, then $\|Z\|^2/2$ is the sum of n independent exponentially distributed variables (cf. Section 1.3) and it follows that

$$\mathrm{P}\left[\|Z\|^2/2 \geq (1+\epsilon)n\right] \leq ((1+\epsilon)e^{-\epsilon})^n \tag{1.3}$$

for $\epsilon \geq 0$.

A useful consequence, which is used only in Section 2.3, is the estimate

$$\mathrm{P}\left[\|Z\|^2 \leq n\right] \leq \left(\sqrt{e}/2\right)^n. \tag{1.4}$$

To see this, let $\|Z\|^2/2 = \sum_{i=1}^n X_i$, with exponentially distributed X_i, and set $Y_i = 1 - X_i$, $T_n = \sum_{i=1}^n Y_i$. Then $\mathrm{P}\left[\|Z\|^2/2 \leq n/2\right] = \mathrm{P}\left[T_n \geq n/2\right]$. A straight-forward calculation shows that the rate function of Y_1 at $\lambda = 1/2$ is given by $\mathrm{I}(1/2) = \ln(2) - 1/2$, and the claim follows from Theorem 1.7.

1.5 Two Useful Inequalities

The inequalities presented in this section are only needed in the proof of Lemma 2.7. Let X, Y be i.i.d. standard normal random variables and set $\gamma := 1 - \mathrm{E}[\log X^2]$ and $\theta := \mathrm{E}[\log^2(X^2+Y^2)]$. Evaluating the corresponding integrals yields[2]

$$\begin{aligned} \gamma &= 1 - \frac{1}{\sqrt{2\pi}}\int_0^\infty t^{-1/2}e^{-t/2}\log t\,dt \approx 2.83 \\ \theta &= \frac{1}{2}\int_0^\infty e^{-t/2}\log^2 t\,dt \approx 3.45. \end{aligned}$$

Lemma 1.8 *Let Z be a centred Gaussian variable with complex values. Then*

$$0 \leq \log \mathrm{E}[|Z|^2] - \mathrm{E}[\log |Z|^2] \leq \gamma, \ \mathrm{Var}(\log |Z|^2) \leq \theta.$$

Proof. By a principal axis transformation, it can be assumed that $Z = \lambda_1 X + i\lambda_2 Y$ with independent standard normal X, Y and $\lambda_1, \lambda_2 \geq 0$. The difference $\Delta := \log \mathrm{E}[|Z|^2] - \mathrm{E}[\log |Z|^2]$ is nonnegative, since log is concave (Jensen's inequality). By linearity of the mean, Δ as well as $\mathrm{Var}(\log |Z|^2)$ are invariant under multiplication of Z with scalars. We may therefore w.l.o.g. assume that $1 = \lambda_1 \geq \lambda_2$. From this it follows that

$$\begin{aligned} \log \mathrm{E}[|Z|^2] &= \log \mathrm{E}[X^2 + \lambda_2^2 Y^2] \leq \log \mathrm{E}[X^2 + Y^2] = 1 \\ \mathrm{E}[\log |Z|^2] &= \mathrm{E}[\log (X^2 + \lambda_2^2 Y^2)] \geq \mathrm{E}[\log X^2] = 1 - \gamma, \end{aligned}$$

which implies the first claim. The estimates

$$\mathrm{Var}(\log |Z|^2) \leq \mathrm{E}[\log^2 |Z|^2] \leq \mathrm{E}[\log^2(X^2+Y^2)] = \theta$$

prove the second claim. □

[2] The sum of n squares of standard normal random variables is χ^2-distributed with n degrees of freedom, cf. [Fel71, II.2-3] for background and the corresponding densities.

Chapter 2

Lower Bounds for Linear and Bilinear Maps

Morgenstern's bound [Mor73] states that $\mathcal{C}(A) \geq \log|\det(A)|$ for a square matrix A, see also [BCS97, Chapter 13] for details. In this chapter, several generalisations of this bound are presented.

2.1 The Mean Square Volume Bound

Let $A \in \mathbb{C}^{m\times n}$ be a matrix. For an r-subset $I \subseteq [m] := \{1,\dots,m\}$ let A_I denote the sub-matrix of A consisting of the rows indexed by I. Over $\mathbb{R}$, the Gramian determinant $\det A_I A_I^*$ can be interpreted as the square of the volume of the parallelepiped spanned by the rows of A_I.

Raz [Raz03] defined the *r-volume* of A by

$$\mathrm{vol}_r(A) := \max_{|I|=r} (\det A_I A_I^*)^{1/2}$$

and observed that the proof of Morgenstern's bound extends to the following *r-volume bound*:

$$\mathcal{C}(A) \geq \log \mathrm{vol}_r(A). \tag{2.1}$$

Moreover, Raz related this quantity to the geometric rigidity as follows:

$$\mathrm{vol}_r(A) \geq (\mathrm{rig}_r(A))^r,$$

which implies the *rigidity bound*,

$$\mathcal{C}(A) \geq r \log \mathrm{rig}_r(A). \tag{2.2}$$

It will be convenient to work with a variant of the r-volume that is completely invariant under unitary transformations. Instead of taking the maximum of the volumes $(\det A_I A_I^*)^{1/2}$, the sum of the squares is used. The *r-mean square volume* $\mathrm{msv}_r(A)$ of $A \in \mathbb{C}^{m\times n}$ is defined by

$$\mathrm{msv}_r(A) := \left(\sum_{|I|=r} \det A_I A_I^*\right)^{1/2} = \left(\sum_{|I|=|J|=r} |\det A_{I,J}|^2\right)^{1/2}.$$

Hereby, $A_{I,J}$ denotes the $r \times r$ sub-matrix consisting of the rows indexed by I and columns indexed by J. The second equality is a consequence of the Binet-Cauchy formula $\det A_I A_I^* = \sum_{|J|=r} |\det A_{I,J}|^2$, see [Bel97, Chapter 4]. The choice of the L_2-norm instead of the maximum norm results in the following inequality

$$\operatorname{vol}_r(A) \leq \operatorname{msv}_r(A) \leq \sqrt{\binom{m}{r}} \operatorname{vol}_r(A). \tag{2.3}$$

The mean square volume has some nice properties.

Lemma 2.1 *Let $A \in \mathbb{C}^{m \times n}$. Then*

$$\operatorname{msv}_r(A) = \operatorname{msv}_r(A^*), \ \operatorname{msv}_r(\lambda A) = \ |\lambda|^r \operatorname{msv}_r(A), \ \operatorname{msv}_r(A) = \operatorname{msv}_r(UAV),$$

where $\lambda \in \mathbb{C}$ and U and V are unitary matrices of the correct format.

Proof. The first two properties are straightforward to verify. As for unitary invariance, let $A = (a_1, \ldots, a_m)^\top$, where a_i denotes the i-th column of A, $1 \leq i \leq m$. Then for $I \subseteq [m]$ with $|I| = r$ we have $A_I A_I^* = (\langle a_j, a_k \rangle)_{j,k \in I}$, where $\langle \cdot, \cdot \rangle$ denotes the complex scalar product. From the unitary invariance of this scalar product, we get $\operatorname{msv}_r(AV) = \operatorname{msv}_r(A)$ for a unitary matrix V of the correct format. Unitary invariance on the right follows now from the invariance under complex conjugation. □

Remark 2.2 The r-volume can be seen as the 1, 2-norm of the map $\Lambda^r A$ induced by A between the exterior algebras $\Lambda^r \mathbb{C}^n$ and $\Lambda^r \mathbb{C}^m$.[1] Similarly, the mean square volume can be interpreted as the Frobenius norm of $\Lambda^r A$. The unitary invariance of the mean square volume also follows from the fact that Λ^r is equivariant with respect to unitary transformations and that the Frobenius norm is invariant under such.

Note also that $\operatorname{msv}_n(A) = |\det A|$ for $A \in \mathbb{C}^{n \times n}$. The unitary invariance allows to express the mean square volume of A in terms of the singular values $\sigma_1 \geq \ldots \geq \sigma_p$ of A, $p := \min\{m, n\}$, as follows.

It is well known [GVL96] that there are unitary matrices $U \in \mathbb{C}^{m \times m}$ and $V \in \mathbb{C}^{n \times n}$ such that $U^* AV = \operatorname{diag}(\sigma_1, \ldots, \sigma_p)$.[2] Hence

$$\operatorname{msv}_r^2(A) = \operatorname{msv}_r^2(\operatorname{diag}(\sigma_1, \ldots, \sigma_p)) = \sum_{|I|=r} \prod_{i \in I} \sigma_i^2 \ \geq \ \sigma_1^2 \sigma_2^2 \cdots \sigma_r^2, \tag{2.4}$$

where I runs over all r-subsets of $[p]$. It follows that the square of the r-mean square volume of a matrix is the r-th elementary symmetric polynomial in the squares of its singular values.

[1] See e.g.., [Bou70] for background on multilinear algebra.

[2] In fact, this is how the SVD is defined in [GVL96].

Combining the r-volume bound (2.1) with (2.3) we obtain the following *mean square volume bound.*

Proposition 2.3 *For* $A \in \mathbb{C}^{m\times n}$ *and* $r \in \mathbb{N}$ *with* $1 \le r \le \min\{m,n\}$

$$\mathcal{C}(A) \ge \log \mathrm{msv}_r(A) - \frac{m}{2}. \tag{2.5}$$

2.2 A Lower Bound on Cyclic Convolution

In this section, the mean square volume bound (2.5) is used in order to prove a lower bound on the bilinear map of the cyclic convolution.

Let $f = \sum_{i=0}^{n-1} a_i X^i$ and $g = \sum_{i=0}^{n-1} b_i X^i$ be polynomials in $\mathbb{C}[X]$. The cyclic convolution of f and g is the polynomial $h = \sum_{i=0}^{n-1} c_i X^i$, which is given by the product of f and g in the quotient ring $\mathbb{C}[X]/(X^n-1)$. Explicitly:

$$c_k = \sum_{i+j\equiv k \bmod n} a_i b_j, \quad 0 \le k < n.$$

Cyclic convolution is a bilinear map on the coefficients. For a fixed polynomial with coefficient vector $a = (a_0,\dots,a_{n-1})$, this map turns into a linear transformation with the circulant matrix

$$\mathrm{Circ}(a) = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}.$$

Let $\mathrm{DFT}_n = (\omega^{jk})_{0\le j,k<n}$ be the matrix of the Discrete Fourier Transform, with $\omega = e^{2\pi i/n}$. It is well known [GVL96, Sect. 4.7.7] that

$$\mathrm{Circ}(a) = \big(\frac{1}{\sqrt{n}}\mathrm{DFT}_n\big)^{-1}\mathrm{diag}(\lambda_0,\dots,\lambda_{n-1})\frac{1}{\sqrt{n}}\mathrm{DFT}_n,$$

where the eigenvalues λ_k of $\mathrm{Circ}(a)$ are given by

$$(\lambda_0,\dots,\lambda_{n-1})^\top = \mathrm{DFT}_n(a_0,\dots,a_{n-1})^\top. \tag{2.6}$$

Hence the singular values of $\mathrm{Circ}(a)$ are $|\lambda_0|,\dots,|\lambda_{n-1}|$ (in some order). Note that $n^{-1/2}\mathrm{DFT}_n$ is unitary.

The Fast Fourier Transform provides a b.c. bilinear circuit of size $O(n\log n)$ that computes the n-dimensional cyclic convolution, see [GG03, 8.2]. The main result of this chapter is the asymptotic optimality of this algorithm in the b.c. model.

Theorem 2.4 *The bounded coefficient complexity of the n-dimensional cyclic convolution* conv_n *satisfies* $\mathcal{C}(\mathrm{conv}_n) \ge \frac{1}{12} n\log n - O(n\log\log n)$.

In fact, the proof of the theorem shows that the constant factor 1/12 can be replaced by the slightly larger value 0.086. The theorem is stated with 1/12 for simplicity of exposition.

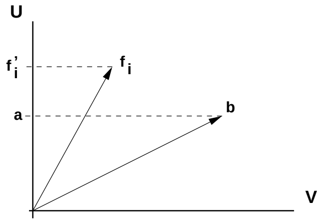
2.2.1 Bounding the Absolute Values of Linear Forms

To prepare for the proof, some lemmas are needed. The idea behind the following lemma is already present in [Raz03]. Linear forms on $\mathbb{C}^n$ are identified with vectors in $\mathbb{C}^n$.

Lemma 2.5 *Let $f_1, \ldots, f_k \in \mathbb{C}^n$ be linear forms and let $1 \leq r < n$. Then there exists a complex subspace $U \subseteq \mathbb{C}^n$ of dimension r such that for a standard normal distributed complex random vector a with values in U, we have*

$$\mathrm{P}\left[\max_i |f_i(a)| \leq 2\sqrt{\ln(4k)}\ \mathrm{rig}_{n-r}(f_1, \ldots, f_k)\right] \geq \frac{1}{2}.$$

Proof. Set $R = \mathrm{rig}_{n-r}(f_1, \ldots, f_k)$. Then there exists a linear subspace $V \subseteq \mathbb{C}^n$ of dimension $n-r$ such that $\mathrm{dist}(f_i, V) \leq R$ for all $1 \leq i \leq k$. Let f_i' be the projection of f_i along V onto the orthogonal complement $U := V^\perp$ of V. By the choice of the subspace V we have $\|f_i'\| \leq R$.



Let $(b_1, \ldots, b_n)$ be standard normal distributed in $\mathbb{C}^n$ and a be the orthogonal projection of b onto U along V. Then a is standard normal distributed with values in U. Moreover, we have $f_i'(b) = f_i(a)$. By Lemma 1.6, the random variable $T = |f_i'(b)|^2/(2\|f_i'\|^2)$ is exponentially distributed with parameter 1. For any $\lambda > 1$, and using Equation (1.3) with $n = 1$, we get

$$\mathrm{P}\left[T \geq \lambda\right] = \mathrm{P}\left[|f_i'(b)|^2 \geq 2\lambda\|f_i'\|^2\right] \leq \lambda e^{-(\lambda-1)}.$$

By the union bound, and using the fact that $\|f_i'\| \leq R$, we obtain

$$\mathrm{P}\left[\max_i |f_i(a)| \geq \sqrt{2\lambda}\, R\right] \leq k\lambda e^{-(\lambda-1)}.$$

Setting $\lambda = 2\ln(4k)$ completes the proof. □

2.2.2 Proof of the Main Result

In the next lemma, a lower bound on the b.c. linear complexity of a circulant $\mathrm{Circ}(a)$ with standard Gaussian parameter vector a in a subspace of $\mathbb{C}^n$ is stated.

Lemma 2.6 *Let $U \subseteq \mathbb{C}^n$ be a subspace of dimension r. For a standard Gaussian vector a in U,*

$$\mathrm{P}\left[\mathcal{C}(\mathrm{Circ}(a)) \geq \frac{1}{2} r \log n - cn\right] > \frac{1}{2},$$

where $c = \frac{1}{2}(2 + \gamma + \sqrt{2\theta}) \approx 3.73$, and γ, θ are the constants introduced in Section 1.5.

We postpone the proof of this lemma and proceed with the proof of the main theorem.

Proof. (of Theorem 2.4) Let Γ be a b.c. bilinear circuit for conv_n, which computes the linear forms $f_1, \ldots, f_k$ on the first set of inputs. Fix $1 \leq r < n$, to be specified later, and set $R = \mathrm{rig}_{n-r}(f_1, \ldots, f_k)$. By Lemma 2.5 and Lemma 2.6 there exists an $a \in \mathbb{C}^n$, such that the following conditions hold:

1. $\max_{1 \leq i \leq k} |f_i(a)| \leq 2\sqrt{\ln(4k)}\, R$,
2. $\mathcal{C}(\mathrm{Circ}(a)) \geq \frac{1}{2} r \log n - cn$.

By Lemma 1.4 and the fact that $k \leq 3n^3$ (see Section 1.1), we get

$$\mathcal{S}(\Gamma) + n \log(2\sqrt{\ln(12n^3)}\, R) \geq \mathcal{C}(\mathrm{Circ}(a)). \tag{2.7}$$

On the other hand, the rigidity bound (2.2) implies the following upper bound on R in terms of $\mathcal{S}(\Gamma)$:

$$\mathcal{S}(\Gamma) \geq \mathcal{C}(f_1, \ldots, f_k) \geq (n - r) \log R.$$

By combining this with (2.7) and using the second condition above, we obtain

$$\left(1 + \frac{n}{n-r}\right)\mathcal{S}(\Gamma) \geq \frac{r}{2} \log n - O(n \log\log n).$$

Setting $\epsilon = r/n$ yields

$$\mathcal{S}(\Gamma) \geq \frac{\epsilon(1-\epsilon)}{2(2-\epsilon)} n \log n - O(n \log\log n).$$

A simple calculation shows that the coefficient of the $n \log n$ term attains the maximum 0.086 for $\epsilon \approx 0.58$. Choosing $\epsilon = 1/2$ for simplicity of exposition finishes the proof. □

Before going into the proof of Lemma 2.6, a lemma on bounding the deviations of products of correlated normal random variables is stated.

Lemma 2.7 *Let $Z = (Z_1, \ldots, Z_r)$ be a centred Gaussian vector in $\mathbb{C}^r$. Define the complex covariance matrix of Z by $\Sigma_r := (\mathrm{E}(Z_j \overline{Z}_k))_{j,k}$ and put $\delta := 2^{-(\gamma + \sqrt{2\theta})} \approx 0.02$. Then $\mathrm{E}(|Z_1|^2 \cdots |Z_r|^2) \geq \det \Sigma_r$ and*

$$\mathrm{P}\left[|Z_1|^2 \cdots |Z_r|^2 \geq \delta^r \det \Sigma_r\right] > \frac{1}{2}.$$

Proof. For proving the bound on the expectation decompose $Z_r = \xi + \eta$ into a component ξ in the span of $Z_1, \ldots, Z_{r-1}$ plus a component η orthogonal to this span in the Hilbert space of quadratic integrable random variables with respect to the inner product defined by the joint probability density of Z. Therefore, $|Z_r|^2 = |\xi|^2 + \xi\overline{\eta} + \overline{\xi}\eta + |\eta|^2$, hence by independence

$$\begin{aligned} \mathrm{E}(|Z_1|^2 \cdots |Z_{r-1}|^2 |Z_r|^2) &= \mathrm{E}(|Z_1|^2 \cdots |Z_{r-1}|^2 |\xi|^2) + \mathrm{E}(|Z_1|^2 \cdots |Z_{r-1}|^2)\,\mathrm{E}(|\eta|^2) \\ &\geq \mathrm{E}(|Z_1|^2 \cdots |Z_{r-1}|^2)\,\mathrm{E}(|\eta|^2). \end{aligned}$$

Let $\xi = \sum_{i<r} \lambda_i Z_i$. Then the complex covariance matrix Σ_r' of the vector $(Z_1, \ldots, Z_{r-1}, \eta)$ arises from Σ_r by subtracting the $\overline{\lambda}_i$-th multiple of the i-th column from the r-th column, and by subtracting the λ_j-th multiple of the j-th row from the r-th row, for all $i, j < r$. Therefore, using $\mathrm{E}(Z_i\overline{\eta}) = 0$, we obtain

$$\det \Sigma_r = \det \Sigma_r' = \mathrm{E}(|\eta|^2) \det \Sigma_{r-1}.$$

The desired bound on the expectation $\mathrm{E}(|Z_1|^2 \cdots |Z_r|^2) \geq \det \Sigma_r$ thus follows by induction on r. Noting that $\mathrm{E}(|Z_r|^2) \geq \mathrm{E}(|\eta|^2)$, we also conclude from the above equation that

$$\mathrm{E}(|Z_1|^2) \cdots \mathrm{E}(|Z_r|^2) \geq \det \Sigma_r. \tag{2.8}$$

In order to prove the probability estimate for the product $|Z_1|^2 \cdots |Z_r|^2$, we first transform the product into a sum by taking logarithms. For every $\epsilon > 0$ Chebychev's inequality yields the bound

$$\mathrm{P}\Big[\frac{1}{r}\Big|\sum_{j=1}^{r}(\log|Z_j|^2 - \mathrm{E}[\log|Z_j|^2])\Big| \geq \epsilon\Big] \leq \frac{\mathrm{Var}(\sum_{j=1}^{r}\log|Z_j|^2)}{\epsilon^2 r^2}. \tag{2.9}$$

For the variance we have by Lemma 1.8

$$\begin{aligned} \mathrm{Var}(\sum_{j=1}^{r}\log|Z_j|^2) &= \sum_{j,k}\mathrm{Cov}(\log|Z_j|^2, \log|Z_k|^2) \\ &\leq \sum_{j,k}\sqrt{\mathrm{Var}(\log|Z_j|^2)\mathrm{Var}(\log|Z_k|^2)} \leq r^2\theta. \end{aligned}$$

Setting $\epsilon^2 = 2\theta$ in this equation and after exponentiating in (2.9) we obtain

$$\mathrm{P}\left[|Z_1|^2 \cdots |Z_r|^2 \leq 2^{-\epsilon r + \sum_{j=1}^{r}\mathrm{E}[\log|Z_j|^2]}\right] \leq \frac{1}{2}. \tag{2.10}$$

By combining the bound (2.8) with Lemma 1.8 we get

$$\log\det\Sigma_r \leq \sum_{i=1}^{r}\log\mathrm{E}[|Z_i|^2] \leq \gamma r + \sum_{i=1}^{r}\mathrm{E}[\log|Z_i|^2].$$

Hence we conclude from (2.10) that

$$\mathrm{P}\left[|Z_1|^2 \cdots |Z_r|^2 \leq 2^{-(\epsilon+\gamma)r}\det\Sigma_r\right] \leq \frac{1}{2},$$

from which the lemma follows. □

Proof. (of Lemma 2.6) By Equation (2.6) we have $\lambda = \mathrm{DFT}_n a$ and the singular values of the circulant $\mathrm{Circ}(a)$ are given by the absolute values of the components of λ. Setting

$$\alpha = n^{-1/2}\lambda = n^{-1/2}\mathrm{DFT}_n a,$$

we obtain for the r-mean square volume by (2.4)

$$\mathrm{msv}_r^2(\mathrm{Circ}(a)) = n^r \sum_{|I|=r} \prod_{i\in I} |\alpha_i|^2. \tag{2.11}$$

Now let a be a standard Gaussian vector in the subspace U of dimension r. Let W be the image of U under the unitary transformation $n^{-1/2}\mathrm{DFT}_n$. As a unitary transformation of a, α is standard Gaussian in the subspace W (cf. Section 1.3). This means that there is an orthonormal basis $b_1, \ldots, b_r$ of W such that

$$\alpha = \beta_1 b_1 + \cdots + \beta_r b_r,$$

where (β_i) is standard Gaussian in $\mathbb{C}^r$. Let $B \in \mathbb{C}^{n\times r}$ denote the matrix with the columns $b_1, \ldots, b_r$ and let B_I be the sub-matrix of B consisting of the rows indexed by I, for $I \subseteq [n]$ with $|I| = r$. Setting $\alpha_I = (\alpha_i)_{i\in I}$ we have $\alpha_I = B_I\beta$. The complex covariance matrix of α_I is given by $\Sigma := E[\alpha_I\alpha_I^*] = B_I B_I^*$, hence

$$\det\Sigma = |\det B_I|^2.$$

Note that $|\det B_I|^2$ can be interpreted as the volume contraction ratio of the projection $\mathbb{C}^n \to \mathbb{C}^I, \alpha \mapsto \alpha_I$ restricted to W. For later purposes we also note that $\mathrm{E}(|\alpha_i|^2) = \sum_j |B_{ij}|^2 \leq 1$.

By the Binet-Cauchy formula and the orthogonality of the basis (b_i) we get

$$\sum_{|I|=r} |\det B_I|^2 = \det\left(\langle b_i, b_j\rangle\right)_{1\leq i,j\leq r} = 1.$$

Therefore, an index set I can be chosen such that

$$|\det B_I|^2 \geq \binom{n}{r}^{-1} \geq 2^{-n}.$$

By applying Lemma 2.7 to the random vector α_I and using (2.11), we get that with probability at least 1/2,

$$\mathrm{msv}_r^2(\mathrm{Circ}(a)) \geq n^r\delta^r \det\Sigma \geq n^r\delta^r 2^{-n}, \tag{2.12}$$

where $\delta = 2^{-(\gamma+\sqrt{2\theta})}$. The mean square volume bound (2.5) implies that

$$\mathcal{C}(\mathrm{Circ}(a)) \geq \log \mathrm{msv}_r(\mathrm{Circ}(a)) - \frac{n}{2} \geq \frac{1}{2} r\log n - \frac{1}{2}(2 + \log\delta^{-1})n,$$

with probability at least 1/2. This proves the lemma. □

2.3 An Alternative to Lemma 2.6 (after Raz)

The purpose of this section is to prove a variation of Lemma 2.6, using a method suggested by Ran Raz (personal communication). The proof depends crucially on a sharp tail estimate for the sum of independent exponentially distributed random variables, as given in Equation (1.4). Also, the parameter r has to be carefully chosen.

Lemma 2.8 *Let $U \subseteq \mathbb{C}^n$ be a subspace of dimension $r > (26/50)n$. For a standard Gaussian vector a in U and sufficiently large n,*

$$\mathrm{P}\left[\mathcal{C}(\mathrm{Circ}(a)) \geq \frac{1}{50} n \log n - O(n)\right] > \frac{1}{2}.$$

Proof. Let $U \subseteq \mathbb{C}^n$ be a fixed subspace of dimension $r = \epsilon n$, with some $\epsilon > 26/50$ fixed. Let b be a complex normal distributed vector in $\mathbb{C}^n$ and let $a = b - c$ be the orthogonal projection of b to U. Write $A = \mathrm{Circ}(a)$, $B = \mathrm{Circ}(b)$ and $C = B - A = \mathrm{Circ}(c)$. Set $d = \delta n$ for some $0 < \delta < 1$. The mean square volume bound (2.5) implies

$$\mathcal{C}(A) \geq \log \mathrm{msv}_d(A) - O(n) \geq d \log \sigma_d(A) - O(n),$$

where σ_d denotes the d-th largest singular value of A. (The second inequality is basically the rigidity bound.) Let D be a matrix of rank at most $d-1$ such that $\sigma_d(A) = \|A - D\|_2$ (cf. Section 1.2). Then

$$\sqrt{n}\sigma_d(A) \geq \|A - D\|_F \geq \|B - D\|_F - \|C\|_F, \tag{2.13}$$

where $\|\cdot\|_F$ denotes the Frobenius norm[3]. We would like to show that for large n, the right-hand side of Equation (2.13) is of order $\Omega(n)$ with probability greater than 1/2. We do this by proving (a) a lower bound on $\|B - D\|_F^2$ and (b) an upper bound on $\|C\|_F^2$.

(a) The term $\|B-D\|_F^2$ can be bounded from below by the squares of the $n - d$ smallest singular values of B, using the Hoffman-Wielandt inequality [GVL96, 8.1.2]:

$$\|B - D\|_F^2 \geq \sum_{j=1}^{n} (\sigma_j(B) - \sigma_j(D))^2 \geq \sum_{j=d+1}^{n} \sigma_j^2(B),$$

where the last inequality follows from the fact that the last $n-d+1$ singular values of D vanish, since D has rank at most $d-1$.

Let $\beta = n^{-1/2}\mathrm{DFT}_n b$, so that the vector of eigenvalues of B is given by $\sqrt{n}\beta$, see Equation (2.6). Since $n^{-1/2}\mathrm{DFT}_n$ is unitary, β is again complex standard normal distributed in $\mathbb{C}^n$, and thus each $\frac{1}{2}|\beta_i|^2$ is exponentially

[3] The Frobenius norm of a matrix $M = (m_{ij})$ is given by $\|M\|_F^2 = \sum_{i,j} m_{ij}^2$.

distributed with parameter 1. For $I \subset [n]$ with $|I| = n - d$ set $S_I = \sum_{j \in I} |\beta_j|^2$, and set $S_{\min} := \min_{|I|=n-d} S_I$. From Bound (1.4) it follows that for each such I, $\mathrm{P}\left[S_I \le n - d\right] \le (\sqrt{e}/2)^{n-d}$, and by the union bound we get

$$\mathrm{P}\left[S_{\min} \le n - d\right] \le \binom{n}{d} \left(\frac{\sqrt{e}}{2}\right)^{n-d}. \tag{2.14}$$

The binomial coefficient can be estimated using the entropy bound[4]

$$\binom{n}{d} \le 2^{nH(\delta)},$$

where $H(\delta) = -\delta \log(\delta) - (1 - \delta)\log(1 - \delta)$ is the entropy function (recall that $\delta = d/n$). We would like the right-hand side in Equation 2.14 to be smaller than 1/2 for large n. Taking logarithms, it follows that this is the case whenever

$$H(\delta) + (1 - \delta) \log \frac{\sqrt{e}}{2} < 0.$$

This equation is satisfied for $\delta = 1/25$. Using the fact that $\sum_{j=d+1}^{n} \sigma_j^2(B) = nS_{\min}$, we obtain

$$\sum_{j=d+1}^{n} \sigma_j^2(B) \ge \frac{24}{25} n^2$$

with probability greater than 1/2.

(b) Next, we derive an upper bound on $\|C\|_F^2$. It is known [GVL96, 2.5.3] that the square of the Frobenius norm is the sum of the squares of all singular values of a matrix. The singular values of C are given by $\sqrt{n}|\gamma_i|$, where $\gamma = n^{-1/2}\mathrm{DFT}_n c$. It follows from this that $\|C\|_F^2 = n \sum_j |\gamma_j|^2$. Since γ is standard normal distributed in a subspace of dimension $n - r$, the sum $\sum_j |\gamma_j|^2$ is χ^2-distributed with $2(n-r)$ degrees of freedom, and the expected value of $\|C\|_F^2$ equals $2n(n - r) = 2(1 - \epsilon)n^2$. The sum $\sum_j |\gamma_j|^2/2$ can be seen as the sum of $n - r$ independent, exponentially distributed random variables. Therefore, Bound (1.3) implies that

$$\mathrm{P}\left[\|C\|_F^2 \le 2(1 + \lambda)(1 - \epsilon)n^2\right] \ge 1 - ((1 + \lambda)e^{-\lambda})^{n-r}$$

holds for any $\lambda \ge 0$ (note that the ϵ of Bound (1.3) is called λ here). For the right-hand side of Equation (2.13) to be positive, λ has to be adjusted such that $2(1 + \lambda)(1 - \epsilon) < 24/25$. Clearly, as long as $\epsilon > 26/50$, a solution $\lambda > 0$ can be found.

Summarising, for $\epsilon > 26/50$ and sufficiently large n (the bigger ϵ, the smaller n may be), Equation (2.13) implies that with probability at least 1/2,

$$\sigma_d(A) \ge \Omega(\sqrt{n}),$$

[4] See [vL99, (1.4.5)] for a derivation.

where $d = n/25$. Inserting this into the the singular value bound, the claim follows. □

2.4 Multiplication and Division of Polynomials

By reducing the cyclic convolution to several other important computational problems, lower bounds of order $n \log n$ for these problems are proved. These bounds are optimal up to a constant factor.

2.4.1 Polynomial Multiplication

Let $f = \sum_{i=0}^{n-1} a_i x^i$, $g = \sum_{i=0}^{n-1} b_i x^i$ be polynomials in $\mathbb{C}[X]$ and $fg = \sum_{i=0}^{2n-2} c_i x^i$. Clearly, the coefficients of the cyclic convolution of f and g can be obtained by adding c_k to c_{k+n} for $0 \leq k < n$. This observation and Theorem 2.4 immediately imply the following corollary.

Corollary 2.9 *The bounded coefficient complexity of the multiplication of polynomials of degree less than n is at least $\frac{1}{12} n \log n - O(n \log\log n)$.*

2.4.2 Division with Remainder

First, a lower bound on the inversion of power series mod X^{n+1} is derived, and then this is used to get a lower bound for the division of polynomials.

Let $\mathbb{C}[[X]]$ denote the ring of formal power series in the variable X. We will study the problem to compute the first n coefficients $b_1, , \ldots, b_n$ of the inverse in $\mathbb{C}[[X]]$

$$f^{-1} = 1 + \sum_{k=1}^{\infty} b_k X^k$$

of the polynomial $f = 1 - \sum_{i=1}^{n} a_i X^i$ given by the coefficients a_i. Note that the b_k are polynomials in the a_i, which are recursively given by

$$b_0 := 1, \quad b_k = \sum_{i=0}^{k-1} a_{k-i} b_i.$$

It should be noted that the problem to invert power series is not bilinear. [Sie72] and [Kun74] designed a b.c. circuit of size $O(n \log n)$ solving this problem.

We now prove a corresponding lower bound on the b.c. complexity of this problem by reducing polynomial multiplication to the problem to invert power series.

Theorem 2.10 *The map assigning to $a_1, \ldots, a_n$ the first n coefficients $b_1, \ldots, b_n$ of the inverse of $f = 1 - \sum_{i=1}^{n} a_i X^i$ in the ring of formal power series has bounded coefficient complexity greater than $\frac{1}{324} n \log n - O(n \log\log n)$.*

Proof. Put $g = \sum_{i=1}^n a_i X^i$. The equation

$$1 + \sum_{k=1}^{\infty} b_k X^k = \frac{1}{1-g} = \sum_{k=0}^{\infty} g^k.$$

shows that g^2 is the homogeneous quadratic part of $\sum_{k=1}^{\infty} b_k X^k$ in the variables a_i.

Let Γ be an optimal b.c. circuit computing $b_1, \ldots, b_n$. According to the proof in [BCS97, Theorem 7.1], there is a b.c. circuit of size at most $9\,\mathcal{S}(\Gamma)$ computing the homogeneous quadratic parts of the $b_1, \ldots, b_n$ with respect to the variables a_i. This leads to a b.c. circuit of size at most $9\,\mathcal{S}(\Gamma)$ computing the coefficients of the squared polynomial g^2.

Now let $m := \lfloor n/3 \rfloor$, and assume that $g = g_1 + X^{2m} g_2$ with g_1, g_2 of degree smaller than m. Then

$$g^2 = g_1^2 + 2 g_1 g_2 X^{2m} + g_2^2 X^{4m},$$

By the assumption on the degrees we have no "carries" and we can therefore find the coefficients of the product polynomial $g_1 g_2$ among the middle terms of g^2. Thus we obtain a b.c. circuit for the multiplication of polynomials of degree $m-1$. The theorem now follows from Corollary 2.9. □

We now show how to reduce the inversion of power series to the problem of dividing polynomials with remainder. The reduction in the proof of the following corollary is from [Str73a], see also [BCS97, Section 2.5].

Corollary 2.11 *Let f, g be polynomials with $n = \deg f \geq m = \deg g$ and g be monic. Let q be the quotient and r be the remainder of f divided by g, so that $f = qg + r$ and $\deg r < \deg g$. The map assigning to the coefficients of f and g the coefficients of the quotient q and the remainder r has bounded coefficient complexity at least $\frac{1}{324} n \log n - O(n \log\log n)$.*

Proof. Dividing $f = X^{2n}$ by $g = \sum_{i=0}^n a_i X^{n-i}$, where $a_0 = 1$, we obtain:

$$X^{2n} = \Big(\sum_{i=0}^{n} q_i X^i\Big)\Big(\sum_{i=0}^{n} a_i X^{n-i}\Big) + \sum_{i=0}^{n-1} r_i X^i.$$

By substituting X with $1/X$ in the above equation and multiplying with X^{2n}, we get

$$1 = \Big(\sum_{i=0}^{n} q_i X^{n-i}\Big)\Big(\sum_{i=0}^{n} a_i X^{i}\Big) + \sum_{i=0}^{n-1} r_i X^{2n-i}.$$

Since the remainder is now a multiple of X^{n+1}, we get

$$\Big(\sum_{i=0}^{n} a_i X^{i}\Big)^{-1} \equiv \Big(\sum_{i=0}^{n} q_i X^{n-i}\Big) \bmod X^{n+1}.$$

From this it follows that the coefficients of the quotient are precisely the coefficients of the inverse mod X^{n+1} of $\sum_{i=0}^{n} a_i X^i$ in the ring of formal power series, and the proof is finished. □

Chapter 3

Unbounded Scalar Multiplications

The model of bounded coefficient circuits can be extended by allowing some instructions corresponding to scalar multiplications with constants of absolute value greater than two, briefly called *help gates* in the sequel. If there are at most h help gates allowed, then the corresponding bounded coefficient complexity is denoted by the symbol $\mathcal{C}_h$.

It turns out that the proof techniques from the previous chapters are robust in the sense that they still allow to prove $n \log n$ lower bounds if the number of help gates is restricted to $(1-\epsilon)n$ for some fixed $\epsilon > 0$.

3.1 Extension of the Mean Square Volume Bound

As a first step the mean square volume bound (2.4) and (2.5) is extended for dealing with help gates.

Proposition 3.1 *Assume $A \in \mathbb{C}^{m \times n}$ has the singular values $\sigma_1 \geq \ldots \geq \sigma_p$, where $p := \min\{m, n\}$. Then for all integers s, h with $1 \leq s \leq p - h$,*

$$\mathcal{C}_h(A) \geq \sum_{i=h+1}^{h+s} \log \sigma_i - \frac{m}{2} + h \geq s \log \sigma_{h+s} - \frac{m}{2} + h.$$

Proof. Let Γ be a b.c. circuit with at most h help gates, which computes the linear map corresponding to A. Without loss of generality, it may be assumed that Γ has exactly h help gates. Let g_i, $i \in I$, be the linear forms computed at the help gates of Γ. We transform the circuit Γ into a b.c. circuit Γ' by replacing each help gate with a multiplication by zero. This new circuit is obviously a b.c. circuit of size $\mathcal{S}(\Gamma') = \mathcal{S}(\Gamma) - h$, computing a linear map corresponding to a matrix $B \in \mathbb{C}^{m \times n}$. The linear maps corresponding to A and B coincide on the orthogonal complement of $\operatorname{span}\{g_i \mid i \in I\}$ in $\mathbb{C}^n$, therefore $B = A + E$ for a matrix E of rank at most h. From the perturbation inequality (1.1) it follows that

$$\sigma_i(B) \geq \sigma_{i+h}(A) \quad \text{for } i \leq p - h.$$

By (2.4) this implies for $s \leq p - h$ that

$$\mathrm{msv}_s^2(B) \geq \sum_{0<i_1<\cdots<i_s\leq p-h} \sigma_{i_1}^2(B)\cdots\sigma_{i_s}^2(B) \geq \sum_{h<i_1<\cdots<i_s\leq p} \sigma_{i_1}^2(A)\cdots\sigma_{i_s}^2(A).$$

On the other hand, the mean square volume bound (2.5) implies

$$\mathcal{S}(\Gamma) - h = \mathcal{S}(\Gamma') \geq \log \mathrm{msv}_s(B) - \frac{m}{2}.$$

Combining the last two estimates completes the proof. □

Remark 3.2 1. Proposition 3.1 implies $\mathcal{C}_{(1-\epsilon)n}(\mathrm{DFT}_n) \geq \epsilon(\frac{1}{2}n\log n - n)$ for the Discrete Fourier Transform DFT_n, provided $0 < \epsilon \leq 1$.

2. The number h of help gates may be replaced by the dimension of the subspace spanned by the linear functions computed at the help gates.

3. Proposition 3.1 can be seen as a variant of the spectral lemma in [Cha98]. Using entropy considerations, Chazelle obtained the slightly worse lower bound $\Omega((r-2h)\log\sigma_r)$ for the b.c. complexity of a matrix $A \in \mathbb{R}^{n\times n}$ with at most h help gates. While this allows to handle at most $n/2$ help gates, Chazelle's result is stronger in the sense that it involves a more general notion of help gates, which are allowed to compute *any* function of the previous intermediate results.

3.2 Extremal Values of Gaussian Random Vectors

In this section an auxiliary result about the distribution of the maximal absolute value of the components of a Gaussian random vector is derived. This result is needed in order to extend the the lower bound on cyclic convolution by accommodating help gates.

Lemma 3.3 *1. A centred Gaussian random vector $X = (X_1, \ldots, X_n)$ in $\mathbb{R}^n$ with $\max_i \mathrm{E}(X_i^2) \leq 1$ satisfies for any $\epsilon > 0$*

$$\lim_{n\to\infty} \mathrm{P}\left[\max_i |X_i| > \sqrt{2\ln n} + \epsilon\right] = 0.$$

2. A centred Gaussian random vector $Z = (Z_1, \ldots, Z_n)$ in $\mathbb{C}^n$ such that $\max_i \mathrm{E}(|Z_i|^2) \leq 1$ satisfies for any $\epsilon > 0$

$$\lim_{n\to\infty} \mathrm{P}\left[\max_i |Z_i| > 2\sqrt{\ln(2n)} + \epsilon\right] = 0.$$

Proof. 1. Since X is centred we have for any $u \in \mathbb{R}$

$$\mathrm{P}\left[\max_i |X_i| \geq u\right] \leq \mathrm{P}\left[\max_i X_i \geq u\right] + \mathrm{P}\left[\max_i (-X_i) \geq u\right] \leq 2\mathrm{P}\left[\max_i X_i \geq u\right].$$

For proving the first assertion it is therefore sufficient to show that for any $\epsilon > 0$

$$\lim_{n\to\infty} \mathrm{P}\left[\max_i X_i > \sqrt{2\ln n} + \epsilon\right] = 0. \tag{3.1}$$

For this we may assume that the components of X are uncorrelated. In fact, Slepian's inequality (see [LT91]) implies that for centred Gaussian vectors $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$ we have

$$\mathrm{P}\left[\max_i X_i \leq u\right] \leq \mathrm{P}\left[\max_i Y_i \leq u\right]$$

provided $\mathrm{E}(X_i^2) = \mathrm{E}(Y_i^2)$ and $\mathrm{E}(X_i X_j) \leq \mathrm{E}(Y_i Y_j)$ for all i, j.

We may also assume that all the X_i have variance 1 since the distribution function

$$F_\sigma(u) := \frac{1}{\sigma\sqrt{2\pi}} \int_\infty^u \exp(-\frac{t^2}{2\sigma^2}) dt.$$

of a centred normal random variable with variance $\sigma^2 \leq 1$ satisfies $F_1(u) \leq F_\sigma(u)$ for all $u \geq 0$. Hence, if X is a Gaussian vector with uncorrelated components X_i of variance $\sigma_i^2 \leq 1$, we have

$$F_1(u)^n \leq \prod_{i=1}^n F_{\sigma_i}(u) = \mathrm{P}\left[\max_i X_i \leq u\right].$$

In the case where $X_1, \ldots, X_n$ are independent and standard normal distributed we have according to [Cra46] that

$$\mathrm{E}(\max_i X_i) = \sqrt{2\ln n} + o(1), \quad \mathrm{Var}(\max_i X_i) = \frac{\pi^2}{12}\frac{1}{\ln n}(1 + o(1)), \quad n \to \infty$$

and Claim (3.1) follows from Chebychev's inequality.

2. The second assertion follows from the first one applied to the Gaussian vector W with values in $\mathbb{R}^{2n}$ given by the real and imaginary parts of the Z_i (in some order). Note that $\max_{1\leq i\leq n} |Z_i| \leq \sqrt{2} \max_{1\leq j\leq 2n} |W_j|$. □

3.3 Cyclic Convolution and Help Gates

Our goal is to prove the following extension of Theorem 2.4.

Theorem 3.4 *The bounded coefficient complexity with at most $(1-\epsilon)n$ help gates of the n-dimensional cyclic convolution* conv_n *is at least $\Omega(n \log n)$ for fixed $0 < \epsilon \leq 1$.*

The proof follows the same line of argument as in Section 2.2. The next lemma is an extension of Lemma 2.6.

Lemma 3.5 *Let $U \subseteq \mathbb{C}^n$ be a subspace of dimension r and $h \in \mathbb{N}$ with $h < r$. For a standard Gaussian vector a in U, we have*

$$\mathrm{P}\left[\mathcal{C}_h(\mathrm{Circ}(a)) \geq \frac{1}{2}(r-h)\log n - n(c + \log\log n)\right] > \frac{1}{2},$$

for some constant $c > 0$.

Proof. As in the proof of Lemma 2.6 it is assumed that the random vector $\alpha = n^{-1/2}\mathrm{DFT}_n a$ is standard Gaussian with values in some r-dimensional subspace W. Recall that $\sqrt{n}\,|\alpha_i|$ are the singular values of $\mathrm{Circ}(a)$. We denote by $|\alpha^{(1)}| \geq \ldots \geq |\alpha^{(n)}|$ the components of α with decreasing absolute values. In particular, $|\alpha^{(1)}| = \max_i |\alpha^{(i)}|$. Proposition 3.1 implies that

$$\begin{aligned} \mathcal{C}_h(\mathrm{Circ}(a)) &\geq \sum_{i=h+1}^{r} \log(\sqrt{n}\,|\alpha^{(i)}|) - \frac{n}{2} + h \\ &= \frac{1}{2}(r-h)\log n + \log\left(\prod_{i=h+1}^{r} |\alpha^{(i)}|\right) - \frac{n}{2} + h. \end{aligned}$$

In the proof of Lemma 2.6 (2.12) we showed that $\mathrm{msv}_r^2(\mathrm{Circ}(a)) \geq n^r\delta^r 2^{-n}$ with probability at least 1/2. In the same way, one can show that with probability at least 3/4 we have $\mathrm{msv}_r^2(\mathrm{Circ}(a)) \geq n^r c_1^n$ for some fixed constant $c_1 > 0$. From the estimate

$$\sum_{|I|=r} \prod_{i \in I} |\alpha_i|^2 \;\leq\; 2^n \prod_{i=1}^{r} |\alpha^{(i)}|^2$$

we thus obtain that $\prod_{i=1}^r |\alpha^{(i)}|^2 \geq (c_1/2)^n$ with probability at least 3/4.

By applying Lemma 3.3 to the centred Gaussian random variable α we obtain that with probability at least 3/4

$$\max_i |\alpha^{(i)}|^2 = |\alpha^{(1)}|^2 \leq c_2 \log n$$

for some fixed constant $c_2 > 0$. (Recall that $\mathrm{E}(|\alpha^{(i)}|^2) \leq 1$.)

Altogether, we obtain that with probability at least 1/2 we have

$$\prod_{i=h+1}^{r} |\alpha^{(i)}|^2 \;\geq\; \frac{\prod_{i=1}^r |\alpha^{(i)}|^2}{|\alpha^{(1)}|^{2h}} \;\geq\; \left(\frac{c_1}{2c_2\log n}\right)^n.$$

This completes the proof of the lemma. □

Proof. (of Theorem 3.4) Let Γ be a b.c. bilinear circuit computing conv_n using at most $h \le (1-\epsilon)n$ help gates, $0 < \epsilon \le 1$. Referring to the partition of instructions in Definition 1.2, we assume that $\Gamma^{(1)}$ uses h_1 help gates, and that $\Gamma^{(2)}, \Gamma^{(3)}, \Gamma^{(4)}$ use a total of h_2 help gates. Thus $h_1 + h_2 = h$. Let $f_1, \ldots, f_k$ denote the linear forms computed by $\Gamma^{(1)}$.

Assume $h_2 < r < n - h_1$ and set $R = \mathrm{rig}_{n-r}(f_1, \ldots, f_k)$. By Lemma 2.5 and Lemma 3.5 there exists an $a \in \mathbb{C}^n$, such that the following conditions hold:

1. $\max_{1\le i\le k} \log |f_i(a)| \le \log(2\sqrt{\ln(4k)}\,R) \le \log R + O(\log\log n)$,
2. $\mathcal{C}_{h_2}(\mathrm{Circ}(a)) \ge \frac{1}{2}(r - h_2)\log n - O(n \log\log n)$.

On the other hand, by Proposition 3.1 and using $\sigma_{n-r}(f_1, \ldots, f_k) \ge R$, we get

$$\mathcal{S}(\Gamma) \ge \mathcal{C}_{h_1}(f_1, \ldots, f_k) \ge (n - r - h_1)\log R - \frac{k}{2}.$$

The proof of Lemma 1.4 shows that

$$\mathcal{S}(\Gamma) + n \max_{1\le i\le k} \log|f_i(a)| \;\ge\; \mathcal{C}_{h_2}(\mathrm{Circ}(a)).$$

By combining all this we obtain

$$\Big(1 + \frac{n}{n-r-h_1}\Big)\mathcal{S}(\Gamma) + \frac{nk}{2(n-r-h_1)} + O(n\log\log n) \ge \frac{1}{2}(r-h_2)\log n.$$

We set now $r := \lfloor (h_2 + n - h_1)/2 \rfloor$. Then $r + h_1 \le (1 - \frac{\epsilon}{2})n$ and $r - h_2 \ge \frac{\epsilon}{2}\,n - 1$. By plugging this into the above inequality we obtain

$$\frac{\epsilon+2}{\epsilon}\,\mathcal{S}(\Gamma) + \frac{k}{\epsilon} + O(n\log\log n) \ge \frac{\epsilon}{4}\,n\log n.$$

Let $\kappa := \frac{\epsilon^2}{8}$. If $k \le \kappa n \log n + n$, then $\mathcal{S}(\Gamma) \ge \frac{\epsilon^2}{8(\epsilon+2)}\,n\log n - O(n\log\log n)$. On the other hand, if $k > \kappa n\log n + n$, then trivially

$$\mathcal{S}(\Gamma) \ge \mathcal{C}_{h_1}(f_1, \ldots, f_k) \ge k - n \ge \kappa n \log n.$$

This completes the proof of the theorem. □

Part II

Computational Complexity of Euler Characteristics

Chapter 4

Preliminaries II

Some fundamental geometric and topological concepts, including the definitions of the Hilbert polynomial and the topological Euler characteristic, are recalled. Also, a short introduction to complexity theory in the setting of the Blum-Shub-Smale model of computation is given. The methods used in the proofs of Chapters 6, 7, and 8 assume familiarity with algebraic geometry at a level beyond of what can reasonably be presented here. The main purpose of the geometric and topological part of this chapter is therefore to fix notation and terminology. More specialised concepts are introduced in Chapters 6, 7, and 8, as needed.

4.1 Algebraic Geometry

Most of what is presented in this section can be found in standard textbooks on algebraic geometry, such as [Sha74, Har77, Har95].

4.1.1 Basic Terminology

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

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

of finitely many polynomials $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$. Likewise, the term *projective variety* is used to denote the common zero set of a finite set of homogeneous polynomials in complex projective space $\mathbb{P}^n$. Sometimes $\mathcal{Z}_{\mathbb{C}^n}$ or $\mathcal{Z}_{\mathbb{P}^n}$ is written to emphasise that the zero set is to be considered in affine or projective space. The *vanishing ideal* $\mathcal{I}(V)$ of an affine (projective) variety V consists of all the (homogeneous) polynomials vanishing on V.

The affine (projective) varieties in $\mathbb{C}^n$ ($\mathbb{P}^n$) are the closed sets of the *Zariski topology.* Non-empty open sets in this topology are dense in $\mathbb{C}^n$ ($\mathbb{P}^n$). Locally closed sets in the Zariski topology are called *basic quasi-algebraic (quasi-projective).* Finite unions of basic quasi-algebraic are called *quasi-algebraic (quasi-projective).* A property is said to hold *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.

If V is an affine variety and $f_1, \dots, f_r$ generate the ideal $\mathcal{I}(V)$, then the *Zariski tangent space* T_xV of V at a point $x \in V$ is defined by $T_xV = \mathcal{Z}_{\mathbb{C}^n}(d_xf_1, \dots, d_xf_r)$, where the *differential* $d_xf\colon \mathbb{C}^n \to \mathbb{C}$ of f at x is the linear function $d_xf = \sum_{j=1}^n \frac{\partial}{\partial X_j} f(x) X_j$. The point $x \in V$ is called a *smooth point* of V if the dimension of T_xV equals the local dimension of V at x. Otherwise, x is called a *singular point* of V.

4.1.2 Grassmannians and Products of Projective Space

For $0 \leq k \leq n$ the *Grassmannian* $\mathbb{G}(k,n)$ is the set of all $k+1$-dimensional vector subspaces of $\mathbb{C}^{n+1}$. The simplest example is $\mathbb{G}(0,n)$ which is isomorphic to $\mathbb{P}^n$. In general, the Grassmannian can be embedded as a closed subset $\mathbb{G}(k,n) \subseteq \mathbb{P}^{\binom{n+1}{k+1}-1}$ of projective space, and as such it is an irreducible projective variety of dimension $(k+1)(n-k)$, see [Har95, Lecture 6]. Elements in $\mathbb{G}(k,n)$ are in bijective correspondence with subspaces $\mathbb{P}^k \subseteq \mathbb{P}^n$. We often write L^{n-k} for an element in $\mathbb{G}(k,n)$, the superscript emphasising the codimension.

Another important class of varieties are products of projective spaces. The product $\mathbb{P}^n \times \mathbb{P}^m$ has the structure of a projective variety via the Segre embedding $\mathbb{P}^n \times \mathbb{P}^m \hookrightarrow \mathbb{P}^{(n+1)(m+1)-1}$, see [Har95, Example 2.11].

4.1.3 The Hilbert Polynomial

Let $S := \mathbb{C}[X_0, \dots, X_n]$ 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 can be found in [Har77, I.7].

Theorem 4.1 (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 $I = \mathcal{I}(V)$ 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. It thus follows that $\deg p_V = \dim V$.

Example 4.2

1. The Hilbert polynomial of $V = \mathbb{P}^n$ is $p_V(T) = \binom{T+n}{n}$.

2. Let $f \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous and squarefree of degree d and let $V = \mathcal{Z}_{\mathbb{P}^n}(f)$. 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 [Har95, Lect. 18]. Moreover, $\deg(V_1 \cup V_2) = \deg V_1 + \deg V_2$ if V_1, V_2 have the same 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 (see [Har77, Ex. III.5.3]).

4.2 Algebraic Topology

General references on algebraic topology are [Bre97] and [Hat02]. Further good summaries of singular homology theory and the associated intersection theory can be found in [Ful97, Appendix B] and [Man01, Appendix A].

4.2.1 Euler Characteristic

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

For possibly more general topological spaces, the Euler characteristic is defined via singular homology (see Section 8.1). In the following definition, $H_k(X)$ denotes the k-th singular homology group of a topological space X.

Definition 4.3 The *Euler characteristic* $\chi(X)$ of a topological space X is defined as the alternating sum $\chi(X) = \sum_{k\in\mathbb{N}}(-1)^k \operatorname{rank} H_k(X)$, provided this sum is finite.

If $V \subseteq \mathbb{P}^n$ is an m-dimensional variety over $\mathbb{C}$, then it can be seen as an $2m$-dimensional real variety, and we have $H_j(V) = 0$ for $j > 2m$.

In [BC04a], the complexity of computing the modified Euler characteristic $\chi^*(S)$ of a semi-algebraic set S was studied. The latter is a minor variation of the Euler characteristic, introduced by Andew Yao [Yao92], which is additive with respect to disjoint unions and coincides with the usual Euler characteristic for compact semi-algebraic sets.

The following proposition expresses that for complex quasi-algebraic sets, the modified Euler characteristic coincides with the Euler characteristic. A proof can be found in [Ful93, Exercise §4.5, p. 95 and Notes §4.13, p. 141].

Proposition 4.4 *If $V = \bigsqcup_{i=1}^{N} V_i$ is a disjoint union of complex quasi-algebraic sets, then $\chi(V) = \sum_{i=1}^{N} \chi(V)$.*

The Euler characteristic satisfies the following principle of inclusion and exclusion.

Lemma 4.5 *Let $V_1, \ldots, V_r$ be complex quasi-algebraic sets. Write $V_I := \cup_{i \in I} V_i$ for an index set $I \subseteq [r]$. Then*

$$\chi(V_1 \cap \cdots \cap V_r) = \sum_{\emptyset \neq I \subseteq [r]} (-1)^{|I|-1} \chi(V_I).$$

Proof. This follows easily from Proposition 4.4 and [BC04a, Corollary 6.4] by passing to the complement. □

4.3 Transversality

A central concept in differential topology is the concept of *transversality.* In many cases, the notion of transversality allows to formalise "general position" arguments. For the following definition, recall that a morphism $\varphi\colon V \to Y$ of smooth varieties induces a differential $d_x\varphi\colon T_xV \to T_{\varphi(x)}Y$ of tangent spaces at each $x \in V$.

Definition 4.6 Let $X \subseteq Y$ be a subvariety of a smooth variety Y and $\varphi\colon V \to Y$ a morphism of smooth varieties. Then φ meets X *transverse* at $x \in \varphi^{-1}(X)$, written $\varphi \pitchfork_x X$, if X is smooth at $\varphi(x)$ and $T_{\varphi(x)}X + d_x\varphi(T_xV) = T_xY$. The map φ is *transverse* to X, written $\varphi \pitchfork X$, if $\varphi \pitchfork_x X$ holds for all $x \in \varphi^{-1}(X)$.

A common special case is when φ is the inclusion. In this case, $V \pitchfork X$ is written. The relationship of transversality to regular points and regular values, which is central in differential topology, is described in Section 6.5. It is not immediately obvious how to generalise the definition to possibly singular varieties. One approach is to stratify the varieties in question into smooth subvarieties in a certain way, and require the morphism to meat each stratum transversely [GM88]. In the special case of a decomposition of a Schubert variety into Schubert cells, this approach is taken in Chapter 7.

An important fact is that transversality is a *generic condition.* A special case is the following well-known statement, see [Har95, Lecture 18].

Theorem 4.7 *Let $V \subseteq \mathbb{P}^n$ be a smooth projective variety. Then almost all linear subspaces $L \subseteq \mathbb{P}^n$ meet V transversely. Moreover, there is an integer d, such that for all L of dimension $n - \dim V$, $L \pitchfork V$ implies that the number of intersection points equals d.*

In fact, the constant d in the theorem equals the degree $\deg V$ of V. A similar result for subvarieties of $\mathbb{P}^n \times \mathbb{P}^n$ is given in Proposition 6.3 and used in Chapter 6. A generalisation of Theorem 4.7 for homogeneous spaces (for example, the Grassmannian) is Kleiman's transversality lemma [Kle74], a variant of which is given in Lemma 7.9 and used in Chapter 7. These two variations lead to the concepts of *projective degrees* (see [Har95, Lecture 18]) and *projective characters* (see [Ful98, Example 14.3.3]), which play a fundamental role in the complexity results in Chapters 6 and Chapter 7 for the Euler characteristic and the Hilbert polynomial, respectively.

4.4 Model of Computation and Complexity

This section gives a short introduction to complexity theory in the Blum-Shub-Smale model of computation. Throughout this section, $\mathbb{K}$ denotes one of the fields $\mathbb{F}_2$, $\mathbb{R}$, or $\mathbb{C}$, and $\mathbb{K}^\infty$ is the set of all finite strings of elements of $\mathbb{K}$. The notation $\mathbb{F}_2$ is used to denote the field with two elements.

The notions of *algorithm* and *complexity* acquire a precise meaning only after a model of computation has been specified. In classical complexity theory, the model of choice is the (multi-tape) *Turing machine.* For algorithmic problems arising in areas of mathematics such as numerical analysis or algebraic geometry, it seems worthwhile to extend the power of Turing machines, allowing them to do arithmetic in structures such as the real or complex numbers. Such enhanced Turing machines were introduced by Lenore Blum, Michael Shub, and Steve Smale in [BSS89] and are commonly referred to as *BSS machines.* Roughly speaking, a BSS machine over a field $\mathbb{K}$ takes inputs from $\mathbb{K}^\infty$, performs a number of arithmetic operations and comparisons following a finite list of instructions, and either halts returning an element of $\mathbb{K}^\infty$ or loops forever. For a comprehensive exposition the reader may consult the monograph [BCSS98].

The following brief treatment of complexity classes in the BSS model is based on the characterisation by John B. Goode [Goo94] and Bruno Poizat [Poi95]. This characterisation does not depend on a formal specification of a BSS machine, using uniform families of circuits instead.

4.4.1 Circuits

The presentation given here follows [BC04b] and also [BCSS98, 18.4], other references are [Poi95, Koi00a]. More comprehensive information on circuits in general may be found in [Gat86][1].

Definition 4.8 An (algebraic) circuit $\mathscr{C}$ over $\mathbb{K}$ is an acyclic directed graph, whose nodes are either *input gates* of in-degree 0, *constant gates* of in-degree 0 labelled with constants from $\mathbb{K}$, *arithmetic gates* of in-degree 2, labelled by one of $\{+, -, \times, /\}$, *sign gates* of in-degree 1, and *output gates* of in-degree 1 and out-degree 0.

The *size* of a circuit $\mathscr{C}$ is the number nodes in it, while the *depth* is the number of nodes on the longest path from an input to an output node. Given an assignment of elements of $\mathbb{K}$ to each input gate, each arithmetic gate performs an arithmetic operation on the values of $\mathbb{K}$ provided by its parent nodes (if defined), while each sign gate returns 1 if the value x provided by its parent node satisfies $x \neq 0$, and 0 else. If $\mathbb{K}$ is ordered, then a sign gate returns 1 if $x \geq 0$ and 0 else. Sign gates allow the computation to *branch* according to sign tests. A circuit with n input gates and m output gates thus defines a (partial) map $\mathbb{K}^n \to \mathbb{K}^m$ (assuming an order on the nodes of the circuit). The value of this map on $x \in \mathbb{K}^n$ is denoted by $\mathscr{C}(x)$.

Example 4.9 The following circuit over $\mathbb{R}$ returns $x^2 + y^2$ if (x, y) satisfies $x^2 + y^2 \geq 1$.

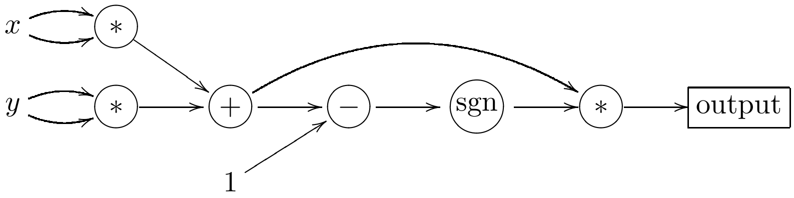


Figure 4.1: Algebraic circuit

A family $\{\mathscr{C}_n\}_{n\in\mathbb{N}}$ of circuits *computes* a function $f\colon \mathbb{K}^\infty \to \mathbb{K}^\infty$, if for each $n \in \mathbb{N}$ and $x \in \mathbb{K}^n$, $\mathscr{C}_n(x) = f(x)$ holds. The family *decides* a language $S \subseteq \mathbb{K}^\infty$, if it computes its characteristic function χ_S. A family $\{\mathscr{C}_n\}_{n\in\mathbb{N}}$ is called *uniform*, if there exists a fixed number of constants $\alpha_1, \dots, \alpha_m \in \mathbb{K}$, such that each circuit $\mathscr{C}_n$ contains exactly m constant nodes labelled with the α_i, and there exists a Turing machine, which on input (n, i) outputs a description of the i-th node of $\mathscr{C}_n$ (with respect to some natural order on the nodes of the circuit). Moreover, the family is called P-*uniform*, if the Turing machine operates in time polynomial in n. Uniform circuits with no constants other than 0 and 1 are called *constant free.*

[1] Our notion of circuit corresponds to the notion of arithmetic network in [Gat86].

4.4.2 Complexity Classes

It can be shown[2] that the functions computable by BSS machines over $\mathbb{K}$ are just the functions computable by uniform families of circuits. The next definitions thus characterise languages (functions) that are considered decidable (computable) by BSS machines over $\mathbb{K}$ with certain bounds on their resources.

Definition 4.10 (1) The class $\mathrm{P}_{\mathbb{K}}$ consists of all languages $S \subseteq \mathbb{K}^{\infty}$ decidable by a P-uniform family of circuits $\{\mathscr{C}_n\}_{n\in\mathbb{N}}$ of size polynomial in n. The corresponding function class is called $\mathrm{FP}_{\mathbb{K}}$.

(2) The class $\mathrm{PAR}_{\mathbb{K}}$ consists of all languages decidable by a P-uniform family of circuits $\{\mathscr{C}_n\}_{n\in\mathbb{N}}$ of depth polynomial in n. The corresponding function class is called $\mathrm{FPAR}_{\mathbb{K}}$.

(3) The class $\mathrm{EXP}_{\mathbb{K}}$ consists of all languages decidable by a P-uniform family of circuits $\{\mathscr{C}_n\}_{n\in\mathbb{N}}$ of size exponential in n. The corresponding function class is called $\mathrm{FEXP}_{\mathbb{K}}$.

The inclusions $\mathrm{P}_{\mathbb{K}} \subseteq \mathrm{PAR}_{\mathbb{K}} \subseteq \mathrm{EXP}_{\mathbb{K}}$ are clear. For $\mathbb{K} = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$ it is known that $\mathrm{PAR}_{\mathbb{K}} \neq \mathrm{EXP}_{\mathbb{K}}$ [Cuc92, BC04b], but in general only the inequality $\mathrm{P}_{\mathbb{K}} \neq \mathrm{EXP}_{\mathbb{K}}$ is known. The class $\mathrm{PAR}_{\mathbb{F}_2}$ equals the class PSPACE of languages decidable by Turing machines in polynomial space [Bor77]. However, the definition of PSPACE is not suited for generalisation to BSS machines over arbitrary fields $\mathbb{K}$: it was shown by Michaux [Mic89] that BSS machines over $\mathbb{R}$ can compute anything in constant space[3].

The next important class consists of those languages S, for which membership $x \in S$ is efficiently decidable with the help of a *witness* $y \in \mathbb{K}^{\infty}$[4]. A relation $R \subseteq (\mathbb{K}^{\infty})^{k+1}$ is called *balanced*, with associated polynomials $p_1, \ldots, p_k$, if for $x \in \mathbb{K}^n$, $(x, y_1, \ldots, y_k) \in R$ implies $y_i \in \mathbb{K}^{p_i(n)}$ for $1 \leq i \leq k$.

Definition 4.11 The class $\mathrm{NP}_{\mathbb{K}}$ consists of all languages $S \subseteq \mathbb{K}^{\infty}$, for which there exists a balanced relation $R_S \subseteq \mathbb{K}^{\infty} \times \mathbb{K}^{\infty}$ in $\mathrm{P}_{\mathbb{K}}$ with associated polynomial p, such that

$$x \in S \Leftrightarrow \exists y \in \mathbb{K}^{p(n)} (x, y) \in R_S$$

holds for an $x \in \mathbb{K}^n$.

At the time of this writing, it is not known whether $\mathrm{P}_{\mathbb{K}} \neq \mathrm{NP}_{\mathbb{K}}$ holds for $\mathbb{K} \in \{\mathbb{F}_2, \mathbb{R}, \mathbb{C}\}$. The definition of $\mathrm{NP}_{\mathbb{K}}$ can be generalised in order to define a whole hierarchy of complexity classes.

[2] This is implied by [Goo94, Poi95] and [BCSS98, Chapter 18].

[3] This is essentially because of the possibility of encoding a lot of information into a single real number.

[4] One way of viewing $\mathrm{NP}_{\mathbb{K}}$ is as consisting of languages S, such that for each $x \in S$ there is a short *proof* of membership, as explained, for example, in the first Lecture in [Rud04].

Definition 4.12 Let $w \in \mathbb{N}$. The class $\Sigma_{\mathbb{K}}^{w}$ consists of all languages $S \subseteq \mathbb{K}^{\infty}$, for which there exists a balanced relation $R_S \subseteq (\mathbb{K}^{\infty})^{w+1}$ in $\mathrm{P}_{\mathbb{K}}$, with associated polynomials $p_1, \dots, p_w$, such that for all $x \in \mathbb{K}^n$ and all $n \in \mathbb{N}$,

$$x \in S \Leftrightarrow Q_1 y_1 \in \mathbb{K}^{p_1(n)} \dots Q_w y_w \in \mathbb{K}^{p_w(n)} (x, y_1, \dots, y_w) \in R_S$$

where $Q_1 = \exists$ and the quantifiers $Q_i \in \{\exists, \forall\}$ alternate. If $Q_1 = \forall$, then the class is denoted by $\Pi_{\mathbb{K}}^{w}$. The cumulative *polynomial hierarchy* over $\mathbb{K}$ is defined as the union $\mathrm{PH}_{\mathbb{K}} = \cup_w \Sigma_{\mathbb{K}}^{w} = \cup_w \Pi_{\mathbb{K}}^{w}$.

The class $\Sigma_{\mathbb{K}}^{1}$ is just $\mathrm{NP}_{\mathbb{K}}$, and the class $\Pi_{\mathbb{K}}^{1}$ is the set of of languages whose complement is in $\mathrm{NP}_{\mathbb{K}}$. The latter is also called $\mathrm{coNP}_{\mathbb{K}}$.

All complexity classes considered so far have a constant free version. These are the classes arrived at by requiring all circuit families occurring in the definitions to be constant free. These classes will be denoted by $\mathrm{P}_{\mathbb{K}}^{0}$, $\mathrm{NP}_{\mathbb{K}}^{0}$, $\mathrm{PH}_{\mathbb{K}}^{0}$, etc. Following [BC04a], complexity classes over $\mathbb{F}_2$ are written $\mathsf{sans\text{-}serif}$ and without the subscript $\mathbb{F}_2$, e.g., P stands for $\mathrm{P}_{\mathbb{F}_2}$.

4.4.3 Decidability

There is an obvious but nonetheless useful way of characterising BSS decidable sets over a field $\mathbb{K}$. Given a set of constants $\alpha_1, \dots, \alpha_m \in \mathbb{K}$, let $\mathscr{F}_{\mathbb{K}}(\alpha_1, \dots, \alpha_m)$ denote the set of first-order formulas in the theory of fields (or, in case $\mathbb{K}$ is ordered, of ordered fields) with constants 0, 1, and $\alpha_1, \dots, \alpha_m$. The notion of P-uniformity for families $\{F_n\}_{n \in \mathbb{N}}$ of formulas is defined just as for circuits. A subset $S \subseteq \mathbb{K}^{\infty}$ is *definable* by a family of formulas $\{F_n\}_{n \in \mathbb{N}}$, if for each $n \in \mathbb{N}$,

$$S \cap \mathbb{K}^n = \{x \in \mathbb{K}^n \mid F_n(x)\}.$$

The next lemma follows from [BCSS98, Section 2.6].

Lemma 4.13 *Let $S \subseteq \mathbb{K}^{\infty}$. Then S is decidable by a P-uniform family of circuits $\{\mathscr{C}_n\}_{n \in \mathbb{N}}$ if and only if there exist constants $\alpha_1, \dots, \alpha_m$ such that L is definable by a a P-uniform family $\{F_n\}_{n \in \mathbb{N}}$ of existential formulas in $\mathscr{F}_{\mathbb{K}}(\alpha_1, \dots, \alpha_m)$.*

If the field $\mathbb{K}$ is one of $\mathbb{F}_2, \mathbb{R}$, and $\mathbb{C}$ (and in fact, any field allowing quantifier elimination), then the polynomial hierarchy is decidable. More specifically, over $\mathbb{R}$, the following theorem holds. In the form presented here, this is due to James Renegar [Ren92]. A general reference is [BPR03, Chapter 14].

Theorem 4.14 *Let $F \in \mathscr{F}_{\mathbb{R}}$ be a formula with k free variables, n bounded variables and w alternating quantifier blocks, of the form*

$$Q_1 y_1 \in \mathbb{K}^{n_1} \dots Q_w y_w \in \mathbb{K}^{n_w} G(x, y_1, \dots, y_w),$$

where $Q_i \in \{\exists, \forall\}$ and G is a quantifier-free formula with m atomic predicates of degree at most δ. Then F is equivalent to a quantifier-free formula F' in disjunctive normal form $\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{ij} \Delta_{ij} 0$, with M atomic predicates h_{ij} of degree at most D, where D and M satisfy the bounds

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

and $\Delta_{ij} \in \{\geq, >, =, <, \leq\}$. If moreover the coefficients in F are of bit size at most ℓ, then the h_{ij} can be assumed to be integer polynomials with coefficients of bit size at most L, with $\log L \leq 2^{O(w)} \log(m\delta) \prod_{i=1}^{w} n_i + O(\log(k + \ell))$.

The sets in $\mathbb{R}^n$ definable by quantifier-free formulae in $\mathscr{F}_{\mathbb{R}}$ are called *semi-algebraic*, the corresponding sets in $\mathbb{C}^n$ are called *quasi-algebraic* or *constructible*. Here, $\mathscr{F}_{\mathbb{R}}$ denotes the first-order language of the reals with arbitrary real constants (as opposed to $\mathscr{F}_{\mathbb{R}}^0$, which is used to denote the language without constants other than 0 and 1).

4.4.4 Coding Polynomial Systems

Algorithmic problems in algebraic geometry involve questions about systems of multivariate polynomials, the ideals they generate, and sets defined by them (i.e., semi- or quasi-algebraic sets, projective varieties, etc.). In order to study these problems within the complexity classes introduced, their coding as strings in $\mathbb{K}^\infty$ has to be addressed. Here and in the following, a polynomial $f = \sum_{e \in I} a_e X_1^{e_1} \cdots X_n^{e_n}$ is represented in the *sparse* encoding as a list of pairs (a_e, e) for $e \in I$, where $I = \{e \in \mathbb{N}^n \mid a_e \neq 0\}$. The exponent vector e is given by a bit vector of length at most $O(n \log \deg f)$. The a_e are usually assumed to be elements of $\mathbb{K}^\infty$, even though the case where $\mathbb{K} = \mathbb{F}_2$ and the $a_e \in \mathbb{Z}$ are represented as bit vectors is sometimes considered. The *sparse size* of f is defined as the sum of the sizes of the (a_e, e) for $e \in I$. This size can be exponential in n in the worst case. Other possible encodings are the *dense* encoding or the *straight-line program* encoding, see [Kri04] (and the references therein) for more on the latter. A set $Z \subseteq \mathbb{K}^n$ definable by a quantifier-free first-order formula over $\mathbb{K}$ (for example, algebraic, quasi-algebraic, or semi-algebraic) is coded by writing the defining formula in disjunctive normal form $F = \bigvee_i \bigwedge_j h_{ij} \Delta_{ij} 0$, where the h_{ij} are polynomial equations and inequalities given in sparse encoding. A set $\mathcal{C} \subseteq \mathbb{K}^\infty$ is called a *property* of first-order definable sets, if it consists of codings of polynomial systems, such that membership $F \in \mathcal{C}$ depends only on the underlying set $Z = \{x \mid F(x)\}$. By abuse of notation, $Z \in \mathcal{C}$ is sometimes used in order to express that any admissible coding of a first-order formula defining Z is in $\mathcal{C}$.

For many problems of interest, the choice between dense and sparse encoding turns out to be not so important from the point of view of complexity theory. For example, it is always possible to transform a system of polynomial equations into one of *quadratic equations* in polynomial time, by introducing new variables that allow to represent monomials of high degree by "repeated squaring". Over $\mathbb{C}$ and $\mathbb{R}$, these new quadratic systems have the same dimension, number of solutions (if finite), and homeomorphism type as the original system. More details, and a worked out example, can be found in [Koi97b].

4.4.5 Basic Decision Problems

The most elementary question to be asked about a system of polynomial equations is if there is a solution. This problem was named HN in [BSS89] in analogy to *Hilbert's Nullstellensatz.* The general specification follows.

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

The problem $\mathrm{HN}_{\mathbb{K}}$ is clearly in $\mathrm{NP}_{\mathbb{K}}$ for any field $\mathbb{K}$. For $\mathbb{K} = \mathbb{F}_2$, this problem is equivalent to SAT, the satisfiability problem for Boolean formulas[5]. The problem $\mathrm{HN}_{\mathbb{K}}$ is decidable over the fields $\mathbb{F}_2$, $\mathbb{R}$, and $\mathbb{C}$. Over $\mathbb{F}_2$ this is trivial. One way to establish decidability over $\mathbb{C}$ is by means of the *effective Nullstellensatz*[6]: A system of multivariate polynomials $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$ of degree at most d *does not* have a solution over $\mathbb{C}$ if and only if there is a representation $1 = \sum_{j=1}^{r} a_j f_j$, where the $a_j \in \mathbb{C}[X_1, \ldots, X_n]$ are polynomials such that $a_j f_j$ has degree degree at most $\max\{d, 3\}^n$. This reduces the problem $\mathrm{HN}_{\mathbb{C}}$ to the problem of deciding whether a system of linear equations has a solution.

Another fundamental problem involving systems of polynomial equations over the real and complex numbers is concerned with the *dimension* of an semi-algebraic and algebraic set.

$\mathrm{DIM}_{\mathbb{R}}$ (Semi-algebraic dimension). Given a set of multivariate real polynomials describing a semi-algebraic set Z and $d \in \mathbb{N}$, decide whether $\dim Z \geq d$.

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

[5] See [Pap94, Chapter 4] and [Rud04].

[6] The canonical reference is [Kol88]. There are variants of the effective Nullstellensatz for polynomials over $\mathbb{Z}$, including considerations about the size of coefficients as well. These are known as "arithmetic effective Nullstellensatz", see [KPS01] and the references therein.

For the algorithmic problem of computing the dimension of semi-algebraic sets, the reader may consult [BPR03, 14.4] and the references given there. The fact that $\textsc{Dim}_{\mathbb{C}}$ is solvable in parallel polynomial time follows from [CGH89, GH91, GH93]. The problem was shown to be in $\mathrm{NP}_{\mathbb{C}}$ by Pascal Koiran [Koi97b].

Another important problem is that of computing the local dimension of a semi-algebraic set at a point x. The local dimension at x is the largest dimension of an irreducible component containing x. It is known that the following problem is in $\mathrm{PH}_{\mathbb{R}}$: decide if the local dimension of a semi-algebraic set at a point x is at least d (see Lemma 4.16)[7].

4.4.6 Reduction and Completeness

The problem $\mathrm{HN}_{\mathbb{K}}$ is in a sense representative for $\mathrm{NP}_{\mathbb{K}}$. This is made precise by the notions of *reduction* and *completeness*.

Definition 4.15 Let $S, T \subseteq \mathbb{K}^\infty$. A function $\pi\colon \mathbb{K}^\infty \to \mathbb{K}^\infty$ is called a (many-one) *reduction* from S to T, if $\pi \in \mathrm{FP}_{\mathbb{K}}$ and for all $x \in \mathbb{K}^\infty$, $x \in S$ if and only if $\pi(x) \in T$. If $\mathcal{C}$ is a class of subsets of $\mathbb{K}^\infty$, then T is called *hard* for $\mathcal{C}$, if every $S \in \mathcal{C}$ reduces to T. If moreover $T \in \mathcal{C}$, then T is *complete* for $\mathcal{C}$.

It is a fundamental result, shown in [BSS89, BCSS98], that for any $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, the problem $\mathrm{HN}_{\mathbb{K}}$ is complete for $\mathrm{NP}_{\mathbb{K}}$. The NP-completeness of $\mathrm{HN}_{\mathbb{F}_2}$ (generally known as SAT) was shown by Stephen Cook [Coo71] and Leonid Levin [Lev73]. The problems $\textsc{Dim}_{\mathbb{R}}$ and $\textsc{Dim}_{\mathbb{C}}$ where shown to be complete for $\mathrm{NP}_{\mathbb{R}}$ and $\mathrm{NP}_{\mathbb{C}}$, respectively, by Pascal Koiran [Koi97b, Koi99b].

4.4.7 Relativisation

Let $\mathcal{C}$ be a class of functions $\varphi\colon \mathbb{K}^\infty \to \mathbb{K}^\infty$ (possibly characteristic functions of languages), computable by a uniform family of circuits. A circuit $\mathscr{C}$ can be enhanced by adding functions $\varphi \in \mathcal{C}$ to the set of operations $\{+, -, \times, /\}$ performed by arithmetic gates. These additional gates are then called *oracle gates* for $\mathcal{C}$. The relativised class $\mathrm{P}_{\mathbb{K}}^{\mathcal{C}}$ ($\mathrm{FP}_{\mathbb{K}}^{\mathcal{C}}$) consists of those languages (functions) decided (computed) by a P-uniform family of circuits with oracle for $\mathcal{C}$. The relativised classes $\mathrm{NP}_{\mathbb{K}}^{\mathcal{C}}$, $\mathrm{PH}_{\mathbb{K}}^{\mathcal{C}}$, etc., are defined in an obvious manner.

Relativisation allows to define a more liberal, yet natural, concept of reduction. Let $S, T \subseteq \mathbb{K}^\infty$. Then S *Turing reduces* to T, if $S \in \mathrm{P}_{\mathbb{K}}^{T}$. If $\mathcal{C}$ is a class of subsets of $\mathbb{K}^\infty$, then T is called *Turing hard* for $\mathcal{C}$, if every $S \in \mathcal{C}$ Turing reduces to T. If moreover $T \in \mathcal{C}$, then T is *Turing complete* for $\mathcal{C}$. The concept of Turing reduction also works if S, T are replaced by

[7] The corresponding problem over $\mathbb{C}$ is more involved. An analysis of this problem is given in [Koi00b].

functions. Clearly, many-one reduction implies Turing reduction, but the converse need not be the case.

4.4.8 Implicit Inputs

There are situations in which first-order definable sets Z_u, parametrised by some $u \in \mathbb{K}^\infty$, are not given explicitly by their defining polynomials, but for which the membership relation $x \in Z_u$ is nonetheless decidable in polynomial time. An example is provided by *determinantal varieties*: given a matrix M with with entries in $\mathbb{C}[X_1, \ldots, X_n]$ and $k \in \mathbb{N}$, define $Z_{M,k} := \{x \in \mathbb{C}^n \mid \mathrm{rank} M(x) \leq k\}$. Clearly, given M and k, membership to $Z_{M,k}$ can be decided in polynomial time, while writing down the rank condition in terms of non-vanishing of minors would lead to a representation of possibly exponential size.

Many properties $\mathcal{C} \in \mathrm{PH}_\mathbb{K}$ of semi-algebraic or constructible sets can be expressed by means of first-order formulas involving only the membership relation $x \in Z$ for a set $Z \in \mathcal{C}$. For example, the property “is bounded” can be expressed as

$$\exists B \forall x \left(B > 0 \wedge ((x \in Z) \Rightarrow \|x\|^2 \leq B^2)\right).$$

Assume $\mathcal{C}$ is such a property of first-order sets in $\mathrm{PH}_\mathbb{K}$, and let $R \subseteq \mathbb{K}^\infty \times \mathbb{K}^\infty$ be a balanced relation in $\mathrm{PH}_\mathbb{K}$ with associated polynomial p. For $u \in \mathbb{K}^n$ set

$$Z_u = \{x \in \mathbb{K}^{p(n)} \mid (u, x) \in R\}.$$

Then it is not hard to see that the set

$$S = \{u \in \mathbb{K}^\infty \mid Z_u \in \mathcal{C}\}$$

is also in $\mathrm{PH}_\mathbb{K}$.

A special case of this observation is given by the next lemma. The lemma is stated using the constant free polynomial hierarchy, since this situation is needed later on.

Lemma 4.16 *Let $R \subseteq \mathbb{R}^\infty \times \mathbb{R}^\infty$ be a balanced relation in $\mathrm{PH}^0_\mathbb{R}$ with associated polynomial p and consider for $u \in \mathbb{R}^n$ the semi-algebraic 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 $\mathrm{PH}^0_\mathbb{R}$.*

Proof. It is known that $\dim S_u \geq d$ if and only if there exists a d-dimensional coordinate subspace such that the projection of S_u on this subspace has a non-empty interior. Writing this condition as a first order formula over $\mathbb{R}$ yields the claim for the dimension [8].

[8] For a more economic description, see [Koi99b].

Let $B_\epsilon(x)$ denote the open ball with radius ϵ centred at x. Then $\dim_x S_u \geq d$ if and only if $\dim(S_u \cap B_\epsilon(x)) \geq d$ for sufficiently small $\epsilon > 0$, cf. [BPR03]. Writing this as a first order formula over $\mathbb{R}$ implies the claim about the local dimension. $\square$

Chapter 5

Counting Complexity Theory

The counting theory presented here was developed by Peter Bürgisser and Felipe Cucker in [BC04a, BC04b, BCL05].

5.1 Counting Complexity Classes

Counting complexity classes consist of functions related to *counting* the number of witnesses to problem instances in $\mathrm{NP}_{\mathbb{K}}$. The most prominent such problem is the problem of counting the number of solutions to a system of polynomial equations.

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

The counting functions considered may not alway have finite values. It is therefore convenient to extend the set of integers by adding infinities. Let $\widehat{\mathbb{N}} := \mathbb{N} \cup \{\infty\}$ and $\widehat{\mathbb{Z}} := \mathbb{Z} \cup \{-\infty, \infty, \mathrm{nil}\}$, with additional symbols $-\infty, \infty$, and nil. The addition and multiplication of integers extends to maps $\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ by setting

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

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

Definition 5.1 The class $\#\mathrm{P}_{\mathbb{K}}$ consists of all functions $\varphi\colon \mathbb{K}^\infty \to \widehat{\mathbb{N}}$, for which there exists a balanced relation $R \subseteq \mathbb{K}^\infty \times \mathbb{K}^\infty$ in $\mathrm{P}_{\mathbb{K}}$ with associated polynomial p, such that

$$\varphi(x) = |\{y \in \mathbb{K}^{p(n)} \mid (x, y) \in R\}|$$

holds for all $x \in \mathbb{K}^n$ and all $n \in \mathbb{N}$. The class $\textsc{Gap}_{\mathbb{K}}$ consists of all functions $\gamma\colon \mathbb{K}^\infty \to \widehat{\mathbb{Z}}$ of the form $\gamma = \varphi - \psi$ for $\varphi, \psi \in \#\mathrm{P}_{\mathbb{K}}$.

Clearly, $\#\mathrm{HN}_{\mathbb{K}}$ belongs to $\#\mathrm{P}_{\mathbb{K}}$. The corresponding problem for $\textsc{Gap}_{\mathbb{K}}$ is the problem $\Delta\mathrm{HN}_{\mathbb{K}}$ of computing the difference of the cardinalities of zero sets of multivariate polynomials.

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

If $A \subseteq \mathbb{K}^\infty$ and φ is a function in $\textsc{Gap}_{\mathbb{K}}$ that vanishes outside A, then this function is sometimes specified as $\varphi\colon A \to \widehat{\mathbb{Z}}$. (An example are functions $\{0,1\}^\infty \to \mathbb{Z}$ in $\textsc{Gap}_{\mathbb{K}}$.)

5.1.1 Properties of Counting Functions

Counting functions satisfy useful closure properties with respect to algebraic operations and composition. The first such property, given in following lemma, is easy to verify.

Lemma 5.2 *Let $\varphi \in \textsc{Gap}_{\mathbb{K}}$ and $\psi \in \mathrm{FP}_{\mathbb{K}}$. Then $\varphi \circ \psi \in \textsc{Gap}_{\mathbb{K}}$.*

The next lemma from [BCL05] lists some algebraic properties of $\#\mathrm{P}_{\mathbb{K}}$ and $\textsc{Gap}_{\mathbb{K}}$ [1].

Lemma 5.3 *(i) The sum of two functions in $\#\mathrm{P}_{\mathbb{K}}$ is in $\#\mathrm{P}_{\mathbb{K}}$. The sum and difference of two functions in $\textsc{Gap}_{\mathbb{K}}$ is in $\textsc{Gap}_{\mathbb{K}}$.*

(ii) The product of two finite valued functions in $\#\mathrm{P}_{\mathbb{K}}$ ($\textsc{Gap}_{\mathbb{K}}$) is in $\#\mathrm{P}_{\mathbb{K}}$ ($\textsc{Gap}_{\mathbb{K}}$).

(iii) [BC04a, Lemma 8] Let $\varphi\colon \mathbb{K}^\infty \times \{0,1\}^\infty \to \mathbb{Z}$ be a function in $\textsc{Gap}_{\mathbb{K}}$ and q be a polynomial. Define $\widetilde{\varphi}\colon \mathbb{K}^\infty \to \mathbb{Z}$ by setting for $u \in \mathbb{K}^m$

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

Then $\widetilde{\varphi}$ belongs to $\textsc{Gap}_{\mathbb{K}}$.

Proof. (i) Let $\varphi, \psi \in \#\mathrm{P}_{\mathbb{K}}$ and let R_φ, R_ψ the corresponding relations with associated polynomials p, q (recall Definition 5.1). Then for all $u \in \mathbb{K}^m$,

$$\begin{aligned}(\varphi + \psi)(u) = \big|\{(b,y,z) \in & \mathbb{K}^{1+p(m)+q(m)} \mid (b = 0 \ \wedge \ y = 0 \ \wedge \ (u,z) \in R_\psi) \\ & \vee \ (b = 1 \ \wedge \ z = 0 \ \wedge \ (u,y) \in R_\varphi)\}\big|,\end{aligned}$$

[1] The case of $\#\mathsf{P}$ and GapP is treated in [For97].

This shows that $\#\mathrm{P}_{\mathbb{K}}$ is closed under taking sums. Moreover, using the associativity of $+$ and the fact that $(-1)\cdot(b+c) = (-1)\cdot b + (-1)\cdot c$ for $b, c \in \widehat{\mathbb{Z}}$, it is straightforward to verify that $\mathrm{GAP}_{\mathbb{K}}$ is closed under sums and differences.

(ii) With the notation of (i), the following holds:

$$(\varphi\psi)(u) = \bigl|\{(y,z) \in \mathbb{K}^{p(m)+q(m)} \mid (u,z) \in R_\psi \ \wedge \ (u,y) \in R_\varphi\}\bigr|.$$

From this it follows that $\#\mathrm{P}_{\mathbb{K}}$ is closed under products. The statement for $\mathrm{GAP}_{\mathbb{K}}$ follows from the distributivity law, which holds for finite valued functions.

(iii) Assume first that $\varphi \in \#\mathrm{P}_{\mathbb{K}}$ and let R be the relation associated to φ, with polynomial p. Then

$$\widetilde{\varphi}(u) = \bigl|\{(y,z) \in \{0,1\}^{q(m)} \times \mathbb{K}^{p(m+q(m))} \mid (u,y,z) \in R\}\bigr|.$$

The case $\varphi \in \mathrm{GAP}_{\mathbb{K}}$ follows by applying (i). □

The rest of this work is concerned mainly with the case $\mathbb{K} = \mathbb{C}$. The other cases that have been studied are $\mathbb{K} = \mathbb{F}_2$ and $\mathbb{K} = \mathbb{R}$. The counting class $\#\mathsf{P} = \#\mathrm{P}_{\mathbb{F}_2}$ was introduced and studied by Leslie Valiant, in his influential work [Val79a, Val79b], starting the area of counting complexity theory. The class $\#\mathrm{P}_{\mathbb{R}}$ was introduced by Klaus Meer [Mee00], who also studied its descriptive complexity theory, and was further explored in [BC04a].

Remark 5.4 Let $\mathbb{K}$ be any field. A function $g\colon \mathbb{F}_2^\infty \to \mathbb{Z}$ in GapP can be considered as a function $\mathbb{K}^\infty \to \mathbb{Z}$ by identifying $\mathbb{F}_2$ with $\{0,1\} \subseteq \mathbb{K}$ and letting g vanish outside $\{0,1\}^\infty$. Given functions $g \in \mathsf{GapP}$ and $\varphi \in \mathrm{GAP}_{\mathbb{K}}$, it is thus possible to interpret the function $\mathbb{K}^\infty \times \mathbb{F}_2^\infty \to \mathbb{Z}$, $(x,y) \mapsto g(y)\varphi(x)$ as a function $\mathbb{K}^\infty \times \{0,1\}^\infty \to \mathbb{Z}$ in $\mathrm{GAP}_{\mathbb{K}}$.

5.1.2 Completeness and Reductions

The concepts of reduction and completeness known for decision problems naturally extend into the framework of counting problems.

Definition 5.5 Let $\varphi, \psi\colon \mathbb{K}^\infty \to \widehat{\mathbb{Z}}$. A function $\pi\colon \mathbb{K}^\infty \to \mathbb{K}^\infty$ is a *parsimonious reduction* from φ to ψ if π can be computed in polynomial time and, for all $x \in \mathbb{K}^\infty$, $\varphi(x) = \psi(\pi(x))$.

Let $\mathcal{C}$ be a class of functions $\varphi\colon \mathbb{K}^\infty \to \widehat{\mathbb{Z}}$. A function ψ is *hard* for $\mathcal{C}$ if for every $\varphi \in \mathcal{C}$ there is a parsimonious reduction from φ to ψ. A function ψ is *$\mathcal{C}$-complete*, if in addition $\psi \in \mathcal{C}$ holds.

The notation $\varphi \preceq \psi$ is used to express that there exists a parsimonious reduction from φ to ψ. The notions of Turing reduction and completeness are defined as expected. Thus $\mathrm{GAP}_{\mathbb{K}}$ Turing reduces to $\#\mathrm{P}_{\mathbb{K}}$, meaning $\mathrm{GAP}_{\mathbb{K}} \in \mathrm{FP}_{\mathbb{K}}^{\#\mathrm{P}_{\mathbb{K}}}$. The following is clear.

Lemma 5.6 *The classes $\#\mathrm{P}_{\mathbb{K}}$ and $\mathrm{GAP}_{\mathbb{K}}$ are closed under parsimonious reductions. This means that if $\psi \#\mathrm{P}_{\mathbb{K}}(\mathrm{GAP}_{\mathbb{K}})$ and $\varphi \preceq \psi$, then $\varphi \in \#\mathrm{P}_{\mathbb{K}}(\mathrm{GAP}_{\mathbb{K}})$.*

As expected, the fundamental $\#\mathrm{P}_{\mathbb{C}}$-complete problem with respect to parsimonious reductions is the problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of solutions of a system of polynomial equations. Completeness also holds if inequalities are allowed, as in the problem $\#\mathrm{QAS}_{\mathbb{C}}$ defined next.

$\#\mathrm{QAS}_{\mathbb{C}}$ (*Quasi-algebraic point counting*). Given a quasi-algebraic set $S \subseteq \mathbb{C}^n$ count the number of points in S, returning ∞ if this number is not finite.

Theorem 5.7 ([BC04a]) *The problems $\#\mathrm{HN}_{\mathbb{C}}$ and $\#\mathrm{QAS}_{\mathbb{C}}$ are $\#\mathrm{P}_{\mathbb{C}}$-complete with respect to parsimonious reductions. The problem $\Delta\mathrm{HN}_{\mathbb{C}}$ is $\mathrm{GAP}_{\mathbb{C}}$-complete with respect to parsimonious reductions.*

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 [DFGS91, Lak91, LL91]. The number of solutions can then be determined using linear algebra techniques[2].

5.2 Generic Parsimonious Reductions

The concept of generic parsimonious reduction, as introduced in [BCL05] and implicit in [BC04a], 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. Of interest are 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". This can be achieved by only requiring the genericity condition to be describable in terms of the constant free polynomial hierarchy over $\mathbb{R}$.

5.2.1 Generic Quantifiers and Reductions

A useful piece of notation are Koiran's *generic quantifiers*[3], which are introduced in the following definition.

Definition 5.8 Let $F \in \mathscr{F}_{\mathbb{R}}$, with free variables $x_1, \dots, x_k$. Then F is *Zariski-generically true*, written $\forall^* a F(a)$, if the set of values $a \in \mathbb{R}^k$ not satisfying F has dimension strictly less than k.

[2] See for example [CCS99, Chapter 2].

[3] These were introduced in [Koi97b, Koi99a, Koi99b]. See also [BC04a, Def. 4.2].

The same definition applies over $\mathbb{C}$. It is known that the condition $\forall^* a F(a)$ is equivalent to the statement that the set of $a \in \mathbb{R}^n$ satisfying F is dense in the Euclidean topology. This can be expressed as

$$\forall \epsilon \in \mathbb{R}\ \forall a \in \mathbb{R}^n\ \exists a' \in \mathbb{R}^n (\epsilon > 0 \Rightarrow F(a') \wedge \|a - a'\| < \epsilon), \qquad (5.1)$$

which shows that the formula $\forall^* a F(a)$ is expressible in $\mathscr{F}_{\mathbb{R}}$.

In the following, relations $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ are considered. It makes sense to say that such a relation is in $\mathrm{PH}^0_{\mathbb{R}}$ by representing points in $\mathbb{C}^n$ as points in $\mathbb{R}^{2n}$ in the obvious way. Relations can be treated as predicates rather than as subsets, and thus the notation $R(a)$ will often be used instead of $a \in R$. Given a balanced relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$, the restriction $R \cap \mathbb{C}^m \times \mathbb{C}^\infty$ is denoted by R_m.

Definition 5.9 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) $\forall u \in \mathbb{C}^m\ \forall^* a \in \mathbb{C}^{p(m)}\ R(u,a)$.

The notation $\varphi \preceq_* \psi$ is used to express that there exists a generic parsimonious reduction from φ to ψ.

5.2.2 Properties of Generic Reductions

Generic parsimonious reductions share many fundamental properties with parsimonious reductions. The first such property is transitivity.

Lemma 5.10 *The generic parsimonious reduction $\preceq_*$ is transitive.*

Proof. Assume that $\varphi \preceq_* \psi$ via the reduction given by (π, R) and $\psi \preceq_* \chi$ via the reduction given by (ρ, S). Define the function σ by $\sigma(u,a,b) := \rho(\pi(u,a), b)$ and the relation T by setting $T(u,a,b) \equiv R(u,a) \wedge S(\pi(u,a),b)$. It remains to be seen that (σ, T) is a generic parsimonious reduction $\varphi \preceq_* \chi$.

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

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

which gives Condition (i) in Definition 5.9. Finally,

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

which implies

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

hence Condition (ii) in Definition 5.9 is also satisfied. □

The following important fact is shown in [BCL05, Theorem 4.4].

Theorem 5.11 *Let $\varphi, \psi \colon \mathbb{C}^\infty \to \widehat{\mathbb{Z}}$. If $\varphi \preceq_* \psi$ then φ Turing reduces to ψ .*

The proof relies on the elimination of generic quantifiers in parameterised formulas due to Koiran [Koi97b, Koi99a], as well as its extension developed in [BC04a]. The proof uses the notion of partial witness sequences from [BC04a].

Definition 5.12 Let $R_m \subseteq \mathbb{R}^{2m} \times \mathbb{R}^k$ be a semi-algebraic subset. A *partial witness sequence* for R_m is a sequence $(\boldsymbol{\alpha}^{(1)}, \ldots, \boldsymbol{\alpha}^{(4m+1)})$ of points in $\mathbb{R}^k$ such that

$$\forall u \in \mathbb{R}^{2m} \ \Big(\big(\forall^* a \in \mathbb{R}^k \ R_m(u,a)\big) \Longrightarrow |\{i \in [4m+1] \mid R_m(u, \boldsymbol{\alpha}^{(i)})\}| > 2m \Big). \quad (5.2)$$

The next result, Theorem 5.13 below, is a consequence of [BC04a, Theorem 4.9 and Remark 4.10]. Only a rough outline of the proof is given, details can be found in the above reference.

Theorem 5.13 *Let $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ be a balanced relation in $\mathrm{PH}^0_{\mathbb{R}}$. Then there is a constant-free machine over $\mathbb{C}$, which computes upon input $m \in \mathbb{N}$ a partial witness sequence $\boldsymbol{\alpha}_m$ for $R_m(u,a)$ in time polynomial in m.*

The following lemma from [Koi97a] plays an important role in the proof. See also [HS82] and [BCSS96] for similar constructions. This lemma is also needed later on in Section 5.3.

Lemma 5.14 *For positive integers k, ℓ, d compute*

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

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

Proof of Theorem 5.13. (Rough idea.) According to Theorem 4.14, the formula (5.2) is equivalent to a quantifier free formula F satisfying certain bounds. Moreover, using a transcendence degree argument, it is shown that Equation (5.2) (and thus F) is satisfied for generic sequences $\boldsymbol{\alpha} \in \mathbb{R}^{p(m)(4m+1)}$, where p is the polynomial associated to the balanced relation R. From this it can be deduced that an $\boldsymbol{\alpha}$ satisfying $h(\boldsymbol{\alpha}) \neq 0$ for all polynomials h appearing in F, also satisfies F. Now Lemma 5.14 can be invoked in order to obtain such a sequence $\boldsymbol{\alpha} \in \mathbb{R}^{p(m)(4m+1)}$. This $\boldsymbol{\alpha}$ satisfies F, and thus Equation (5.2). □

Remark 5.15 The partial witness sequence $\boldsymbol{\alpha}_m$ constructed in the proof of Theorem 5.13 is a sequence of integers obtained by repeated squaring. Since the components of $\boldsymbol{\alpha}_m$ have bit-size exponential in m, the computation of $\boldsymbol{\alpha}_m$ is not possible in time polynomial in m in the classical setting of Turing machines. It follows, however, that a system of equations $F_m(y, \alpha)$ with integer coefficients can be obtained by a Turing machine in time polynomial in m such that there exists a unique solution $(\overline{y}, \overline{\alpha})$ of $F_m(y, \alpha)$ with $\overline{\alpha} = \boldsymbol{\alpha}_m$.

Proof of Theorem 5.11. Let (π, R) be a generic parsimonious reduction from φ to ψ. By Theorem 5.13, a partial witness sequence $\boldsymbol{\alpha}_m$ for R_m can be computed by a machine over $\mathbb{C}$ in time polynomial in m. Hence the following algorithm can be implemented by a P-uniform family of circuits over $\mathbb{C}$ with oracle for ψ:

```
input $u \in \mathbb{C}^m$
compute a partial witness sequence $(\boldsymbol{\alpha}_m^{(1)}, \ldots, \boldsymbol{\alpha}_m^{(4m+1)})$ for $R_m$
for $i = 1$ to $4m+1$ do
  compute $\pi(u, \boldsymbol{\alpha}_m^{(i)})$
  get $N_i := \psi(\pi(u, \boldsymbol{\alpha}_m^{(i)}))$ by an oracle call to $\psi$
compute the number $N$ occurring most among the numbers $N_1, \ldots, N_{4m+1}$
return $N$.
```

Condition (ii) of Definition 5.9 states that $\forall^* a \in \mathbb{C}^{p(m)}\ R_m(u, a)$. Hence, since $\boldsymbol{\alpha}_m$ is a partial witness sequence, $R_m(u, \boldsymbol{\alpha}_m^{(i)})$ holds for the majority of the indices $i \in [4m{+}1]$. On the other hand, by Condition (i) of Definition 5.9,

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

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

5.2.3 Generic Complexity Classes

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

Definition 5.16 (i) The class $\#\mathrm{P}_{\mathbb{C}}^*$ is the class of all functions $\varphi\colon \mathbb{C}^\infty \to \widehat{\mathbb{N}}$ such that there exists $\psi \in \#\mathrm{P}_{\mathbb{C}}$ with $\varphi \preceq_* \psi$.

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

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

Remark 5.17 Let ψ be in $\#\mathrm{P}_{\mathbb{C}}$. According to Lemma 5.2, the function $\psi \circ \pi$ is itself in $\#\mathrm{P}_{\mathbb{C}}$. Therefore, without lack of generality the reduction π can be assumed to be the identity. This simplification is used in the proofs throughout this section, and a generic parsimonious reduction is only specified by the balanced relation R.

Just like $\mathrm{GAP}_{\mathbb{C}}$ (Lemma 5.3), the class $\mathrm{GAP}^*_{\mathbb{C}}$ satisfies some important algebraic closure properties.

Lemma 5.18 *(i) The sum of two functions in* $\#\mathrm{P}^*_{\mathbb{C}}$ *is in* $\#\mathrm{P}^*_{\mathbb{C}}$. *The sum and difference of two functions in* $\mathrm{GAP}^*_{\mathbb{C}}$ *is in* $\mathrm{GAP}^*_{\mathbb{C}}$.

(ii) The product of two finite valued functions in $\#\mathrm{P}^*_{\mathbb{C}}$ *(*$\mathrm{GAP}^*_{\mathbb{C}}$*) is in* $\#\mathrm{P}^*_{\mathbb{C}}$ *(*$\mathrm{GAP}^*_{\mathbb{C}}$*).*

Proof. The proof is just given for the case of addition of functions in $\#\mathrm{P}^*_{\mathbb{C}}$. The other cases are similar. Let $\varphi, \psi \in \#\mathrm{P}^*_{\mathbb{C}}$ and $\chi_1, \chi_2 \in \#\mathrm{P}^*_{\mathbb{C}}$ such that $\varphi \preceq_* \chi_1$ and $\psi \preceq_* \chi_2$ with respect to the generic parsimonious reductions given by relations R and S, respectively. Let p, q be the polynomials associated to R and S. Then, for all $u \in \mathbb{C}^m$,

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

Moreover, $\forall^* a \in \mathbb{C}^{p(m)}\ R_m(u,a)$ and $\forall^* b \in \mathbb{C}^{q(m)}\ S_m(u,b)$. From Lemma 5.3(i), it can be deduced that the function χ defined by $\chi(u,a,b) := \chi_1(u,a) + \chi_2(u,b)$ is in $\mathrm{GAP}_{\mathbb{C}}$. It follows that for all $u \in \mathbb{C}^m$

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

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

Lemma 5.19 *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* $g\colon \mathbb{F}_2^\infty \to \mathbb{Z}$ *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. It follows from Lemma 5.18(ii) and Remark 5.4 that the function $\mathbb{C}^\infty \times \{0,1\}^\infty \to \mathbb{Z}, (u,y) \mapsto g(y)\varphi(u,y)$ is in $\mathrm{GAP}^*_{\mathbb{C}}$, and we may reduce to the case of a sum $\widetilde{\varphi}(u) = \sum_{y \in \{0,1\}^{q(m)}} \varphi(u,y)$ with $\varphi \in \mathrm{GAP}^*_{\mathbb{C}}$. Let $\psi \in \mathrm{GAP}_{\mathbb{C}}$ such that $\varphi \preceq_* \psi$ via the reduction given by a balanced relation R with associated polynomial p. Then, for all $m \in \mathbb{N}$,

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

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

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

where the function $\widetilde{\psi}$ is defined by $\widetilde{\psi}(u,a) = \sum_{y\in\{0,1\}^{q(m)}} \psi(u,y,a)$. It is now easy to see that $\widetilde{\varphi} \preceq_* \widetilde{\psi}$. Moreover, from Lemma 5.3 it follows that the map

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

is in $\text{GAP}_\mathbb{C}$.. Since the assertion of the lemma is true for the class $\text{GAP}_\mathbb{C}$, it follows that $\widetilde{\psi}$ belongs to $\text{GAP}_\mathbb{C}$ and hence $\widetilde{\varphi} \in \text{GAP}^*_\mathbb{C}$. □

5.2.4 Complexity of Computing the Degree

In [BC04a] the problem of computing the geometric degree of the zero set $Z \subseteq \mathbb{C}^n$ of given complex polynomials was Turing reduced to $\text{HN}_\mathbb{C}$. An analysis of the proof reveals that this reduction is generic parsimonious except for the computation of the dimension of Z. The following slight modification of the degree problem, however, is in $\#\text{P}^*_\mathbb{C}$.

Degree (*Geometric degree*). Given an algebraic set $Z \subseteq \mathbb{C}^n$ and $d \in \mathbb{N}$ such that $\dim Z \leq d$, compute the geometric degree of the d-dimensional part of Z.

Theorem 5.20 ([BC04a]) *The problem* Degree *is* $\#\text{P}^*_\mathbb{C}$*-complete with respect to parsimonious reductions.*

The lower bound is easy. The proof that Degree is in $\#\text{P}^*_\mathbb{C}$ consists of a generic parsimonious reduction to $\#\text{HN}_\mathbb{C}$, by intersecting Z *transversely* with a subspace of codimension d. The key point in the proof is finding a way to express transversality in $\text{PH}^0_\mathbb{R}$.

Theorem 5.20 generalises to the case 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 in polynomial time. (The degree of a constructible set is defined as the sum of the degrees of its components of maximal dimension.)

Lemma 5.21 *Let R be a polynomial time decidable relation over $\mathbb{C}$, let p be a polynomial, and consider for $u \in \mathbb{C}^n$ the constructible set*

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

Then there is a function φ in $\#\text{P}^*_\mathbb{C}$ 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 follows from Theorem 5.20, using arguments as in Section 4.4.8. The fact that Theorem 5.20 generalises to constructible sets follows from the proof given in [BC04a], see also [BC04b, Theorem 7.2]. □

Example 5.22 Let F be a matrix with entries in $\mathbb{C}[X_1, \dots, X_n]$, $k, d \in \mathbb{N}$ such that $Z := \{x \in \mathbb{C}^n \mid \operatorname{rank} F(x) \leq k\}$ has dimension at most d. Then, by Lemma 5.21, the degree of the d-dimensional part 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.)

5.3 Boolean Parts of Complexity Classes

It is natural and important to consider the *discrete* versions of problems regarding polynomial systems. These are the problems arrived at by restricting the input to integer polynomials coded in binary. If $L \subseteq \mathbb{K}^{\infty}$ is a language consisting of first-order formulas, then the discrete version is regarded as a language in $\mathbb{F}_2^{\infty}$ and is denoted by $L^{\mathbb{Z}}$. Examples are the problems $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ and $\mathrm{DIM}_{\mathbb{C}}^{\mathbb{Z}}$. The corresponding restrictions of complexity classes over $\mathbb{K}$ to languages over binary inputs are called *Boolean parts.*

5.3.1 Boolean Parts of Counting Classes

Determining Boolean parts amounts to characterise, in terms of classical complexity classes, the power of resource bounded machines over $\mathbb{R}$ or $\mathbb{C}$ when their inputs are restricted to be binary [4].

Definition 5.23 (i) The Boolean part of a class $\mathcal{C}$ of decision problems over $\mathbb{K}$ is the class $\mathrm{BP}(\mathcal{C}) = \{S \cap \{0,1\}^{\infty} \mid S \in \mathcal{C}\}$.

(ii) The Boolean part $\mathrm{BP}(\mathcal{C})$ of a class $\mathcal{C}$ of functions $\mathbb{K}^{\infty} \to \mathbb{K}^{\infty}$ is the class of functions $\{0,1\}^{\infty} \to \{0,1\}^{\infty}$ which can be obtained from functions in the class $\mathcal{C}$ by restricting inputs to $\{0,1\}^{\infty}$.

(iii) The Boolean part $\mathrm{BP}(\mathcal{C})$ of class $\mathcal{C}$ of counting functions $\mathbb{K}^{\infty} \to \widehat{\mathbb{Z}}$ is the class of functions $\{0,1\}^{\infty} \to \widehat{\mathbb{Z}}$ which can be obtained by restricting inputs to $\{0,1\}^{\infty}$.

The *constant-free Boolean part* of $\mathcal{C}$ is defined as $\mathrm{BP}^0(\mathcal{C}) := \mathrm{BP}(\mathcal{C}^0)$.

Boolean parts can are regarded as classes of languages in $\mathbb{F}_2^{\infty}$ (or functions defined on $\mathbb{F}_2^{\infty}$) by identifying $\mathbb{F}_2$ with $\{0,1\}$, see also Remark 5.4.

In [BC04a], the class of *geometric counting complex problems* GCC was defined as the constant-free Boolean part of $\#\mathrm{P}_{\mathbb{C}}$. This is a class of Boolean

[4] These have been studied, for example, in [Bür00, CG97, CKK$^+$95, CK95, Koi94, Koi97c].

counting problems, closed under parsimonious reductions, which can be located in a small region in the general landscape of Boolean complexity classes, namely,

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

It is not hard to see (although not completely immediate) that $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ is in GCC. In [BC] it is moreover shown that this problem is complete for GCC. The class GCC may be alternatively defined as the Boolean part of $\#\mathrm{P}_{\mathbb{C}}$. That is, the restriction to constant-free machines is not necessary.

Lemma 5.24 $\mathrm{BP}(\#\mathrm{P}_{\mathbb{C}}) = \mathsf{GCC}$.

Proof. Let $\varphi\colon \{0,1\}^\infty \to \widehat{\mathbb{N}}$ be in $\mathrm{BP}(\#\mathrm{P}_{\mathbb{C}})$. Then there is a balanced relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ with associated polynomial p, decidable by a P-uniform family of circuits $\{\mathscr{C}_n\}$ of polynomial size, such that for all $x \in \{0,1\}^n, \varphi(x) = |\{y \in \mathbb{C}^{p(n)} \mid R(x,y)\}|$. Without loss of generality [BCSS98, §7], the machine constants $a_1, \dots, a_k \in \mathbb{C}$ in the circuits can be assumed to be algebraically independent over $\mathbb{Q}$ and it can be assumed that the circuits do not perform divisions.

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

The following constant-free circuit $\mathscr{C}_n^0$ defines φ on input $x \in \{0,1\}^n$: Compute a test vector $\alpha := (\alpha_1, \dots, \alpha_k) \in \mathbb{Z}^n$ satisfying $g_n(\alpha) \neq 0$ as described in Lemma 5.14, and then simulate the computation of $\mathscr{C}_n$ by replacing the constants a_i by α_i. The resulting circuit has the same branching behaviour as $\mathscr{C}_n$. The verification that the resulting family of circuits $\{\mathscr{C}_n^0\}$ is P-uniform and that the $\mathscr{C}_n^0$ have size polynomially bounded in n follows from Lemma 5.14. □

The next proposition shows the effect of taking Boolean parts on relativisation.

Proposition 5.25 *(i)* $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}^*}) = \mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}) = \mathsf{P}^{\mathsf{GCC}}$.

(ii) $\mathrm{BP}(\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}^*}) = \mathrm{BP}(\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}) = \mathsf{FP}^{\mathsf{GCC}}$.

By Theorem 5.11 it follows that $\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}^*} = \mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$ (and the same for function classes), so it remains to prove the second equalities in the statement of the proposition.

The proof needs some preparation. In the following, the polynomial ring $R := \mathbb{Z}[a_1, \dots, a_k]$ in the indeterminates $a_1, \dots, a_k$ will serve as a coefficient ring. For a polynomial $f \in R[X_1, \dots, X_n]$ and $\alpha \in \mathbb{C}^k$, the notation $f^\alpha \in$

$\mathbb{Z}[X_1, \dots, X_n]$ is used for the polynomial obtained from f by specialising the vector of indeterminates $(a_1, \dots, a_k)$ to α.

Lemma 5.26 *Let $f_1, \dots, f_r$ be polynomials in $\mathbb{Z}[a_1, \dots, a_k, X_1, \dots, X_n]$ of total degree at most d and having coefficients of bit size at most ℓ, such that their zero set over the algebraic closure K of the quotient field $\mathrm{Quot}(R)$ is finite. Then there is a polynomial $h \in R$ with degree and bit size bounded by $(r\ell d^n)^{O(1)}$ satisfying the following property: For all $\alpha \in \mathbb{C}^k$ such that $h(\alpha) \neq 0$, the system $f_1^\alpha = 0, \dots, f_r^\alpha = 0$ has the same number of solutions as the system $f_1 = 0, \dots, f_r = 0$.*

The following auxiliary result, which follows from [GH93, §3.4.7], is needed.

Lemma 5.27 *Assuming the situation of Lemma 5.26, there exist integers $\gamma_1, \dots, \gamma_n$ and an irreducible univariate polynomial $g \in R[Y]$ such that*

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

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

Proof of Lemma 5.26. Let $h_1 \in R$ denote the product of θ, the discriminant of g, and of the leading coefficient of g. We are going to show that there exists a polynomial $h_2 \in R$ of the required size such that if $h_1(\alpha)h_2(\alpha) \neq 0$, then the map

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

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

The polynomials $P_0 := g(\gamma_1 X_1 + \cdots + \gamma_n X_n)$ and $P_k := r_k(\gamma_1 X_1 + \cdots + \gamma_n X_n) - \theta X_k$ $(1 \leq k \leq n)$ vanish on $Z := \mathcal{Z}_{K^n}(f_1, \dots, f_r)$. In fact, note that $(P_1(x), \dots, P_n(x)) = \theta(\psi(\varphi(x)) - x)$ for $x \in Z$. By the effective arithmetic Nullstellensatz (cf. [KP94, KPS01]), there are representations

$$\rho_k P_k^{e_k} = u_{k,1} f_1 + \cdots + u_{k,r} f_r, \quad 0 \leq k \leq n, \tag{5.3}$$

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

Assume that $h(\alpha) \neq 0$ and $x \in \mathcal{Z}_{\mathbb{C}^n}(f_1, \dots, f_r)$. Specialising a_j to α_j in Equation (5.3), we get $P_k^\alpha(x) = 0$ for all k, since $\rho_k(\alpha) \neq 0$. In particular, $P_0^\alpha(x) = 0$, which implies that the map φ^α is well defined.

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

Proof of Proposition 5.25. (i) It is sufficient to show $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}) \subseteq \mathsf{P}^{\mathsf{GCC}}$, the reverse inclusion is straightforward.

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

Let $S \subseteq \{0,1\}^\infty$ be a set in $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}})$. Then there exists a P-uniform family of circuits deciding S in polynomial time with oracle gates for $\#\mathrm{HN}_{\mathbb{C}}$. The elimination of the machine constants can be done as in the proof of Lemma 5.24. Moreover, Lemma 5.26 ensures that the test sequence α, which replaces the machine sequence, can be computed so that the oracle calls to $\#\mathrm{HN}_{\mathbb{C}}$ in the modified family of circuits give the same result as in the original family.

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

Let $\{\mathscr{C}_n\}$ be a constant-free P-uniform family of circuits deciding $S \subseteq \{0,1\}^\infty$ in polynomial time with oracle gates for $\#\mathrm{HN}_{\mathbb{C}}$.

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

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

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

This construction is used in the following Turing machine deciding S. Given $x \in \{0,1\}^n$ as input, simulate the computation of $\mathscr{C}_n$ by keeping straight-line program representations of intermediate results. When reaching a sign node, if the tested value is z, then query $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ with input $\{\varphi_\zeta(x,y), y_m = 0\}$. When reaching a query node, then if the input to the query is a system of equations $f_1 = 0, \ldots, f_r = 0$ whose coefficients are $z_1, \ldots, z_s$, query $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$ with input $\{f_1^y = 0, \ldots, f_r^y = 0, \varphi_{\zeta_1}(x, y^{(1)}), \ldots, \varphi_{\zeta_s}(x, y^{(s)})\}$ (where f_ρ^y is obtained from f_ρ by replacing z_j by $y_{m_j}^{(j)}, j = 1, \ldots, s$). This machine runs in polynomial time and queries $\#\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}} \in \mathsf{GCC}$. This shows $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}) \subseteq \mathsf{P}^{\mathsf{GCC}}$.

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

From Theorem 5.11 it follows that $\mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}^{*}}) = \mathrm{BP}(\mathrm{P}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}})$. Therefore, as far as Boolean parts are concerned, the generic class $\#\mathrm{P}_{\mathbb{C}}^{*}$ does not introduce more power than $\#\mathrm{P}_{\mathbb{C}}$ when considering Turing reductions.

Remark 5.28 Let $\varphi, \psi \colon \{0,1\}^{\infty} \to \widehat{\mathbb{Z}}$. It is natural to define a notion of *randomised parsimonious reduction* from φ to ψ as a pair (π, R) where $\pi \colon \{0,1\}^{\infty} \times \{0,1\}^{\infty} \to \{0,1\}^{\infty}$ is computable in polynomial time by a Turing machine, and $R \subseteq \{0,1\}^{\infty} \times \{0,1\}^{\infty}$ is a balanced relation such that, for all $m \in \mathbb{N}$, the following holds (where p, q are polynomials and p is associated to R):

(i) $\forall u \in \{0,1\}^{m}\ \forall a \in \{0,1\}^{p(m)}\ \big(R(u,a) \Rightarrow \varphi(u) = \psi(\pi(u,a))\big)$,

(ii) $\forall u \in \{0,1\}^{m}\ \mathrm{Prob}\{a \in \{0,1\}^{p(m)} \mid \neg R(u,a)\} \leq 2^{-q(m)}$.

As in the proof of Proposition 5.25 one may show that for any φ in $\mathrm{BP}(\#\mathrm{P}_{\mathbb{C}}^{*})$ there exists a randomised parsimonious reduction from φ to $\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$. Recall from the proof that the intermediate results of the computation are integers represented by straight-line programs. The point is now that testing those for zero can be done in coRP [IM83, Sch80, Kal87]. Similarly, for any φ in $\mathrm{BP}(\mathrm{G{\scriptsize AP}}_{\mathbb{C}}^{*})$ there exists a randomised parsimonious reduction from φ to $\Delta\mathrm{HN}_{\mathbb{C}}^{\mathbb{Z}}$.

Chapter 6

Topological Euler Characteristic

The problems considered in this chapter are specified as follows.

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

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

The goal is to show is that these problems are on essentially the same level of difficulty as the problem of counting the number of solutions to a polynomial system of equations. Within the framework developed in Chapter 5, the precise statement reads as follows.

Theorem 6.1 *The problems* $\mathrm{EULER}_{\mathbb{C}}$ *and* $\mathrm{PROJEULER}_{\mathbb{C}}$ *are* $\mathrm{GAP}_{\mathbb{C}}^{*}$*-complete for Turing reductions.*

In conjunction with Theorem 5.11, this implies that the problems $\mathrm{EULER}_{\mathbb{C}}$ and $\mathrm{PROJEULER}_{\mathbb{C}}$ Turing reduce to the problem $\#\mathrm{HN}_{\mathbb{C}}$ of counting the number of solutions to a system of polynomial equations. A similar result applies in the classical Turing machine model of computation, when restricting to inputs with integer coefficients.

Theorem 6.2 *The problems* $\mathrm{EULER}_{\mathbb{C}}^{\mathbb{Z}}$ *and* $\mathrm{PROJEULER}_{\mathbb{C}}^{\mathbb{Z}}$ *are* $\mathsf{FP}^{\mathsf{GCC}}$*-complete with respect to Turing reductions.*

The upper bound in Theorem 6.1 is based on a formula due to Paolo Aluffi [Alu03], expressing the Euler characteristic of a projective hypersurface in terms of certain quantities called *projective degrees*. Furthermore, Aluffi describes (and implements) an algorithm for computing the Euler characteristic (and other quantities) using his formula. The main difference between Aluffis algorithm and the algorithm underlying Theorem 6.1 is in the computation of the projective degrees. While Aluffis algorithm depends on the computation of Gröbner bases, the algorithm presented here uses transversality arguments in order to obtain a generic parsimonious reduction to $\#\mathrm{HN}_{\mathbb{C}}$.

6.1 Projective Degrees and Euler Characteristics

An extension of the notion of degree of a projective variety is the sequence of projective degrees of a rational morphism [Har95, Lecture 19].

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

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

on the domain of definition $U := \mathbb{P}^n \setminus \Sigma$, which is open and dense in the Zariski topology. Thus φ defines a rational morphism $\varphi\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^n$. Let $\Gamma_U \subseteq \mathbb{P}^n \times \mathbb{P}^n$ denote the graph of φ and let Γ denote the closure of Γ_U in the Zariski topology. Then $\Gamma = \Gamma_U \cup \Gamma_\Sigma$, where Γ_Σ is the inverse image of Σ under the projection $\pi_1\colon \Gamma \to \mathbb{P}^n$ onto the first factor. Clearly, $\dim \Gamma_\Sigma < n = \dim \Gamma$.

Next, consider $L^i \in \mathbb{G}(n-i, n)$ and $L^{n-i} \in \mathbb{G}(i, n)$ in the Grassmannians. Since $\dim \Gamma = n$, the intersection $\Gamma \cap (L^i \times L^{n-i})$ is finite for generic (L^i, L^{n-i}). The natural question arises under which conditions the number of points in this intersection does not depend on (L^i, L^{n-i}). The next proposition gives an answer and leads to the concept of projective degrees. A proof is given at the end of this chapter.

Proposition 6.3 *Let $\varphi\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ be a rational morphism defined on U and let Γ be the closure of the graph of φ.*

(i) For $0 \le i < n$ there exists a non-negative integer d_i such that, if

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

then

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

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

Definition 6.4 The integers $d_0, \ldots, d_{n-1}$ are called the *projective degrees* of the rational morphism φ (compare [Har95, Chapter 19]).

Example 6.5 Let $f_0 = X_1X_2$, $f_1 = X_0X_2$, $f_2 = X_0X_1$ in the case $n = 2$. Then $\Sigma = \mathcal{Z}(f_0, f_1, f_2) = \{(1:0:0), (0:1:0), (0:0:1)\}$. It is easy to see that $d_1 = 2$, and the claim is that $d_0 = 1$. Indeed, a point L^2 is given by $L^2 = \mathcal{Z}_{\mathbb{P}^2}(a_0Y_0 + a_1Y_1 + a_2Y_2, b_0Y_0 + b_1Y_1 + b_2Y_2)$ and

$$\varphi^{-1}(L^2) = \mathcal{Z}(a_0/X_0 + a_1/X_1 + a_2/X_2, b_0/X_0 + b_1/X_1 + b_2/X_2,\ X_0X_1X_2 \neq 0)$$

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

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

The following proposition is stated in order to illustrate the notion of projective degrees, and is not used elsewhere.

Proposition 6.6 *Let $f_0, \dots, f_n \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous nonzero polynomials of the same degree d and let r be the codimension of $\Sigma := \mathcal{Z}(f_0, \dots, f_n)$ in $\mathbb{P}^n$. Then the projective degrees d_i of the corresponding rational map φ satisfy $d_{n-i} = d^i$ for $1 \leq i < r$ and $d_{n-r} = d^r - \deg(\Sigma)$.*

Proof. For generic L^r, $\varphi^{-1}(L^r) = \mathcal{Z}(g_1, \dots, g_r) \setminus \Sigma$, where $g_1, \dots, g_r$ form a generic linear combination of $f_0, \dots, f_n$. It is known [Mat86] that $(g_1, \dots, g_r)$ is a regular sequence. Let $C_1, \dots, C_s$ be the irreducible components of $V := \mathcal{Z}_{\mathbb{P}^n}(g_1, \dots, g_r)$. Then all C_j have codimension r and we have $\deg V = \sum_{j=1}^{s} \deg C_j = d^r$. Suppose that $C_1, \dots, C_k$ are the irreducible components of V that are contained in Σ. Then these are the irreducible components of Σ of maximal dimension and hence $\deg \Sigma = \sum_{j=1}^{k} \deg C_j$. Therefore, for generic L^{n-r},

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

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

Let $V = \mathcal{Z}(f) \subseteq \mathbb{P}^n$ be a smooth, irreducible hypersurface. Then the formula

$$\chi(V) = \frac{1}{d}((1-d)^{n+1} - 1) + n + 1. \tag{6.1}$$

expresses the Euler characteristic in terms of the degree d of V [Dim92, §5].

Example 6.7 (i) $\mathbb{P}^n = \mathcal{Z}(X_0) \subset \mathbb{P}^{n+1}$ implies $\chi(\mathbb{P}^n) = n + 1$.

(ii) For a smooth planar curve $V \subset \mathbb{P}^2$ of degree d, Equation (6.1) implies the well-known formula $\chi(V) = \frac{1}{d}((1-d)^3 - 1) + 3 = d(3-d) = 2(1 - g_a(V))$, where $g_a(V)$ is the arithmetic genus of V.

A generalisation of Equation (6.1) to the case of possibly singular hypersurfaces follows from a formula of Aluffi [Alu03] for Chern-Schwartz-MacPherson classes for arbitrary hypersurfaces. The statement below follows from Theorem 2.1 and the remark at the end of §2.6 in [Alu03].

Theorem 6.8 (Aluffi [Alu03]) *Let $f \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous and non-constant. The Euler characteristic of the projective hypersurface $V = \mathcal{Z}(f)$ is given by*

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

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

$$\mathbb{P}^n \setminus \Sigma \to \mathbb{P}^n, \quad x = (x_0 \colon \cdots \colon x_n) \mapsto \left(\frac{\partial}{\partial X_0} f(x) \colon \cdots \colon \frac{\partial}{\partial X_n} f(x) \right)$$

and $\Sigma := \mathcal{Z}(\frac{\partial}{\partial X_0} f, \dots, \frac{\partial}{\partial X_n} f)$.

Example 6.9 (i) Let $f = \prod_{i=1}^{s} (\alpha_i X_0 + \beta_i X_1)^{e_i}$. Then $\mathcal{Z}(f) \subseteq \mathbb{P}^1$ consists of exactly s points. Theorem 6.8 says $\chi(\mathcal{Z}(f)) = 1 + d_0$. On the other hand, a straight-forward calculation shows that indeed $d_0 = s-1$. (This example illustrates that Theorem 6.8 works for reducible f.)

(ii) Proposition 6.6 implies that $d_{n-i} = (d-1)^i$ for $1 \leq i < \operatorname{codim}_{\mathbb{P}^n} \Sigma$. In the special case of a smooth irreducible hypersurface we have $\Sigma = \emptyset$ and therefore $d_{n-i} = (d-1)^i$ for $1 \leq i \leq n$. Plugging this into the formula in Theorem 6.8, Equation (6.1) follows.

(iii) Consider $f = X_0 X_1 X_2$ with zero set $V \subseteq \mathbb{P}^2$. Note that V is a singular hypersurface. Example 6.5 shows that $d_0 = 1, d_1 = 2$. Theorem 6.8 therefore gives $\chi(V) = 2 + d_1 - d_0 = 3$. This can be easily verified using the principle of inclusion and exclusion: Set $V_i := \mathcal{Z}(X_i) \simeq \mathbb{P}^1$. Then, for $i < j$, each $V_i \cap V_j$ consists of one point only and

$$\begin{aligned} \chi(V) = & \chi(V_0) + \chi(V_1) + \chi(V_2) \\ & - \chi(V_0 \cap V_1) - \chi(V_0 \cap V_2) - \chi(V_1 \cap V_2) = 3. \end{aligned}$$

(iv) The last example can be generalised by considering the zero set $V \subset \mathbb{P}^n$ of $f = X_0 X_1 \cdots X_n$. Note that the hypersurface V is highly singular. Its singular locus $\Sigma = \cup_{i<j} \mathcal{Z}_{\mathbb{P}^n}(X_i, X_j)$ is a subspace arrangement with an interesting combinatorial structure. The projective degrees of V thus contain information about Σ which does not follow from $\deg V$. It is an instructive exercise to prove that $d_i = \binom{n}{i}$ for $0 \leq i < n$ and to check the formula in Theorem 6.8. To compute $\chi(V)$, note that $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ is homotopy equivalent to the circle S^1 and $(\mathbb{C}^*)^n \to \mathbb{P}^n \setminus V$, $(x_1, \dots, x_n) \mapsto (1 \colon x_1 \colon \cdots \colon x_n)$ is an isomorphism, hence $\chi(V) = \chi(\mathbb{P}^n) - \chi(\mathbb{C}^*)^n = n + 1$ since $\chi(S^1) = 0$.

6.2 Computing Projective Degrees

In this section, the complexity of the problems $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$ is determined. To do so, the following auxiliary problems are considered:

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

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

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

The main results of this section are that $\text{PROJDEGREE}_{\mathbb{C}}$ is in $\#\text{P}_{\mathbb{C}}^*$ and that $\text{EULER}_{\mathbb{C}}$ and $\text{PROJEULER}_{\mathbb{C}}$ are $\text{GAP}_{\mathbb{C}}^*$-complete with respect to Turing reductions. To prove them, the following auxiliary result is needed.

Lemma 6.10 *The problems* $\#\text{QPROJ}_{\mathbb{C}}$ *and* $\#\text{BIQPROJ}_{\mathbb{C}}$ *are in* $\#\text{P}_{\mathbb{C}}$.

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

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

Let $\varphi(x_0, \dots, x_n)$ be the system of homogeneous polynomials describing the set $S \subseteq \mathbb{P}^n$. The above partition of $\mathbb{P}^n$ then induces a partition of S as a disjoint union of the quasi-algebraic subsets of $\mathbb{C}^{n+1}$ defined by the systems $\varphi_i := \varphi(0, \dots, 0, 1, x_{i+1}, \dots, x_n)$ of (non-homogeneous) polynomials. It follows that the number of points of S is equal to the number of points of the quasi-algebraic subset of $\mathbb{C}^{n+1}$ described by $\bigvee_{i=0}^n \varphi_i$. This reduces $\#\text{QPROJ}_{\mathbb{C}}$ to $\#\text{QAS}_{\mathbb{C}}$ (see Chapter 5) and thus shows that $\#\text{QPROJ}_{\mathbb{C}} \in \#\text{P}_{\mathbb{C}}$. The proof for $\#\text{BIQPROJ}_{\mathbb{C}}$ is similar. □

Proposition 6.11 *The problem* $\text{PROJDEGREE}_{\mathbb{C}}$ *is in* $\#\text{P}_{\mathbb{C}}^*$.

The proof consists of finding a generic parsimonious reduction (π, R) from $\text{PROJDEGREE}_{\mathbb{C}}$ to $\#\text{BIQPROJ}_{\mathbb{C}}$. The proof is based on the technical Lemma 6.12 stated below, whose proof is deferred to §6.4. In order to state this lemma, some notation is needed.

Let $u \in \mathbb{C}^m$ be a vector parameterising the homogeneous polynomials $f_0, \dots, f_n$ and let $\Gamma^u = \Gamma_U^u \cup \Gamma_\Sigma^u \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be the closure of the graph associated to $f_0, \dots, f_n$ as described in §6.1. Also, to a point $a \in \mathbb{C}^{i(n+1)}$

(seen as a matrix with i rows and $n+1$ columns), we associate the linear space L_a^i defined by $ax = 0$. Note that, for generic a, $\dim L_a^i = n+1-i$, i.e., $L_a \in \mathbb{G}(n-i,n)$. So, L_a^i is written for an element in $\mathbb{G}(n-i,n)$ parameterised by a, even though for a thin subset of $\mathbb{C}^{i(n+1)}$, one has $L_a^i \notin \mathbb{G}(n-i,n)$. Similarly for $b \in \mathbb{C}^{(n-i)(n+1)}$ and L_b^{n-i}.

Define the following transversality relation for $m \in \mathbb{N}$ and $0 \le i < n$:

$$\begin{aligned}&\mathtt{trans}_{m,n,i} := \\ &\Big\{(u,a,b) \in \mathbb{C}^{m+n(n+1)} \mid \Gamma_\Sigma^u \cap (L_a^i \times L_b^{n-i}) = \emptyset \;\wedge\; \Gamma_U^u \pitchfork (L_a^i \times L_b^{n-i})\Big\}\end{aligned}$$

and write $\mathtt{trans} := \bigcup_{m,n,i} \mathtt{trans}_{m,n,i}$.

Lemma 6.12 *The relation* `trans` *is in* $\mathrm{PH}_{\mathbb{R}}^0$.

The proof of this lemma is postponed to Section 6.4. With the help of this Lemma, the proof of Proposition 6.11 can be given.

Proof of Proposition 6.11. We construct a generic parsimonious reduction (π, R) from $\mathrm{P{\small ROJ}D{\small EGREE}}_{\mathbb{C}}$ to $\#\mathrm{B{\small I}QP{\small ROJ}}_{\mathbb{C}}$. Let $0 \le i < n$, let $f_0, \dots, f_n \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous given by a parameter $u \in \mathbb{C}^m$, and let (L_a^i, L_b^{n-i}) be given by a parameter $(a,b) \in \mathbb{C}^{n(n+1)}$. The following formula expresses that $(p,q) \in L_a^i \times L_b^{n-i}$:

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

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

$$\mathtt{memb}_U(p,q,u) := \bigwedge_{0 \le r < s \le n} (F_{r,s}(p,q) = 0) \wedge \bigvee_{r=0}^{n} (f_r(p) \neq 0). \tag{6.2}$$

It follows that a description of the set $\Gamma_U^u \cap (L_a^i \times L_b^{n-i})$ can be computed in polynomial time from i, a, b and $f_0, \dots, f_n$ by a constant-free machine. Define π as the function mapping (u,a,b) to the above description of the set $\Gamma_U^u \cap (L_a^i \times L_b^{n-i})$ and let $R := \mathtt{trans}$ be the above defined relation, which, according to Lemma 6.12, is in $\mathrm{PH}_{\mathbb{R}}^0$.

Part (i) of Proposition 6.3 shows that the number of points in $\pi(u,(a,b))$ is the ith projective degree of $(f_0, \dots, f_n)$, provided $R(u,a,b)$ holds. Part (ii) of Proposition 6.3 says that $\forall u \in \mathbb{C}^m\ \forall^*(a,b) \in \mathbb{C}^{n(n+1)}\ R(u,a,b)$. Therefore, (π, R) is a generic parsimonious reduction from $\mathrm{P{\small ROJ}D{\small EGREE}}_{\mathbb{C}}$ to $\#\mathrm{B{\small I}QP{\small ROJ}}_{\mathbb{C}}$ and the statement follows from Lemma 6.10. □

6.3 The Complexity of Computing the Euler Characteristic

In this section, Theorem 6.1, which states that $\mathrm{EULER}_{\mathbb{C}}$ and $\mathrm{PROJEULER}_{\mathbb{C}}$ are $\mathrm{GAP}_{\mathbb{C}}^{*}$-complete for Turing reductions, is proven. The next lemma gives the upper bounds in Theorem 6.1. To state it, the following auxiliary problem is defined:

$\mathrm{PHSEULER}_{\mathbb{C}}$ (*Euler characteristic of projective hypersurfaces*). Given a non-constant complex homogeneous polynomial, compute the Euler characteristic of its projective zero set.

Proposition 6.13 *(i)* $\mathrm{PHSEULER}_{\mathbb{C}} \in \mathrm{GAP}_{\mathbb{C}}^{*}$,

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

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

Proof. (i) Let $f \in \mathbb{C}[X_0, \ldots, X_n]$ be an instance of $\mathrm{PHSEULER}_{\mathbb{C}}$, that is, a non-constant homogeneous polynomial. Put $d := \deg f$ and let $V \subset \mathbb{P}^n$ denote the projective zero set of f. Let $d_0, \ldots, d_{n-1}$ be the projective degrees of the rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^n$ defined by the gradient $(\partial f/\partial X_0, \ldots, \partial f/\partial X_n)$ of f. Theorem 6.8 states that

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

Now consider the function

$$\varphi\colon \mathbb{C}^\infty \times \{0,1\}^\infty \to V, \qquad (V, i) \mapsto \begin{cases} (-1)^{i-1} d_{n-i} + 1 & \text{if } 0 \le i < n \\ 0 & \text{otherwise.} \end{cases}$$

where $i \in \mathbb{N}$ is identified with its binary encoding. By Proposition 6.11, the problem $\mathrm{PROJDEGREE}_{\mathbb{C}}$ belongs to $\#\mathrm{P}_{\mathbb{C}}^{*}$. Using Lemma 5.18, it follows that $\varphi \in \mathrm{GAP}_{\mathbb{C}}^{*}$. Using Lemma 5.19, it follows that $\mathrm{PHSEULER}_{\mathbb{C}}$ belongs to $\mathrm{GAP}_{\mathbb{C}}^{*}$.

(ii) Let $f_1, \ldots, f_r \in \mathbb{C}[X_0, \ldots, X_n]$ be an instance of $\mathrm{PROJEULER}_{\mathbb{C}}$. For an index set $I \subseteq [r]$ write V_I for the projective zero set of the product $f_I := \prod_{i \in I} f_i$. Lemma 4.5 implies that $\chi(\mathcal{Z}_{\mathbb{P}^n}(f_1, \ldots, f_r)) = \chi_+(f_1, \ldots, f_r) - \chi_-(f_1, \ldots, f_r)$, where

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

By part (i), $\mathrm{PHSEULER}_{\mathbb{C}}$ belongs to $\mathrm{GAP}_{\mathbb{C}}^{*}$. Therefore, Lemma 5.19 implies that both functions χ_+ and χ_- belong to $\mathrm{GAP}_{\mathbb{C}}^{*}$ as well. This proves that $\mathrm{PROJEULER}_{\mathbb{C}}$ belongs to $\mathrm{GAP}_{\mathbb{C}}^{*}$.

(iii) Let $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$ be an instance of $\text{EULER}_{\mathbb{C}}$ and d be an upper bound on the degrees of these polynomials. Define the homogeneous polynomials F_i of degree $d+1$ by $F_i := X_0^{d+1} f_i(X_1/X_0, \dots, X_n/X_0)$ and put $V := \mathcal{Z}_{\mathbb{P}^n}(F_1, \dots, F_r)$ and $U := V \cap \{X_0 \neq 0\}$. The set U is homeomorphic to the affine zero set $\mathcal{Z}_{\mathbb{C}^n}(f_1, \dots, f_r)$. Moreover, by construction, we have $V - U = \mathcal{Z}_{\mathbb{P}^n}(X_0)) \simeq \mathbb{P}^{n-1}$. Proposition 4.4 implies that $\chi(U) = \chi(V) - \chi(\mathbb{P}^{n-1}) = \chi(V) - n$. The assertion (iii) therefore follows from (ii). □

The next lemma gives the lower bounds in Theorem 6.1.

Lemma 6.14 *Both problems* $\text{EULER}_{\mathbb{C}}$ *and* $\text{PROJEULER}_{\mathbb{C}}$ *are* $\#\mathrm{P}_{\mathbb{C}}$*-hard for Turing reductions.*

Proof. In the proof of part (iii) of Proposition 6.13, a Turing reduction from $\text{EULER}_{\mathbb{C}}$ to $\text{PROJEULER}_{\mathbb{C}}$ was given. To prove the hardness, a Turing reduction from DEGREE to $\text{EULER}_{\mathbb{C}}$ is established.

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

$$R_{m,n} := \Big\{ (u,a) \in \mathbb{C}^{m+n(n+1)} \mid \\ (Z_u = \emptyset) \vee \bigvee_{k=0}^{n} \bigwedge_{i<k} \big(A_i \cap Z_u = \emptyset \wedge A_k \cap Z_u \neq \emptyset \wedge A_k \pitchfork Z_u \big) \Big\}. \tag{6.3}$$

According to [BC04a, Lemma 5.9], the set $R := \bigcup_{m,n} R_{m,n}$ is expressible in $\mathrm{PH}^0_{\mathbb{R}}$. Moreover, for fixed $u \in \mathbb{C}^m$, we have $\forall^* a \in \mathbb{C}^{n(n+1)}\ R_{m,n}(u,a)$.

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

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

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

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

As in the proof of Theorem 5.11, it can be shown that the following algorithm computes the degree of Z_u.

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

The algorithm can be implemented as a polynomial time BSS machine over $\mathbb{C}$ making oracle calls to $\text{EULER}_{\mathbb{C}}$. □

6.4 Expressing Transversality

This section is dedicated to the proof of Lemma 6.12. For an irreducible variety $V \subseteq \mathbb{P}^n \times \mathbb{P}^n$ given as the zero set of bihomogeneous polynomials $f_1, \dots, f_r$, write $\widehat{V}$ for the zero set of these polynomials in $\mathbb{C}^{n+1} \times \mathbb{C}^{n+1}$. Let $(p,q) \in V$ and $\widehat{p}, \widehat{q} \in \mathbb{C}^{n+1}$ be affine representatives of p, q, respectively. From the homogeneity of the defining equations it follows that the tangent space of $\widehat{V}$ at $(\widehat{p}, \widehat{q})$ does not depend on the particular $\widehat{p}, \widehat{q}$ chosen, and may therefore be written $T_{(p,q)}\widehat{V}$.

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

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

Lemma 6.15 *Let Γ_U be the graph of a rational morphism $\varphi\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ defined by polynomials $f_0, \dots, f_n$ of the same degree. Let $0 \leq i < n$, $(L^i, L^{n-i}) \in \mathbb{G}(n-i, n) \times \mathbb{G}(i, n)$, and $(p,q) \in \Gamma_U \cap (L^i \times L^{n-i})$. Then $\Gamma_U \pitchfork_{(p,q)} (L^i \times L^{n-i})$ if and only if*

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

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

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

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

Proof of Lemma 6.12. Denote by $\mathbb{C}^{n+1}_*$ the set $\mathbb{C}^{n+1} \setminus \{0\}$ and write $\Gamma_U := \Gamma^u_U$. By Lemma 6.15, $\Gamma_U \pitchfork (L^i_a \times L^{n-i}_b)$ if and only if

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

The condition $(p,q) \in \widehat{\Gamma}_U \cap (\widehat{L}^i_a \times \widehat{L}^{n-i}_b)$ is expressed by the formula $\mathtt{memb}_U(p,q,u) \ \wedge \ \mathtt{memb}_L(p,q,a,b)$ (see the proof of Proposition 6.11) and can thus be checked in polynomial time. Also, the last two statements concerning dimension can be checked in polynomial time.

Let $(p,q) \in \widehat{\Gamma}_U$ and $\xi, \eta \in \mathbb{C}^{n+1}$. Since locally at (p,q) the vanishing ideal of $\widehat{\Gamma}_U$ is given by the polynomials $F_{r,s}(X,Y)$ (cf. (6.2)), we have $(\xi,\eta) \in T_{(p,q)}\widehat{\Gamma}_U$ if and only if

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

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

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

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

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

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

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

$$\forall p, q \in \mathbb{C}^{n+1}_* \ \big((p,q) \in \overline{\Gamma_U} \cap (L^i_a \times L^{n-i}_b) \Rightarrow (p,q) \in \Gamma_U\big), \tag{6.4}$$

since Γ is the Zariski closure of Γ_U. To express this condition we use the fact [Mum76] that Γ is also the closure of Γ_U with respect to the Euclidean topology. This topology can be defined by a metric in projective space as follows. Define, for $p, q \in \mathbb{C}^{n+1}_*$,

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

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

We note that "$d_{\mathbb{P}^n}(p,q) < \varepsilon$ for sufficiently small $\varepsilon > 0$" is equivalent to "$|\langle p,q\rangle|/(\|p\| \cdot \|q\|) \ge 1 - \delta$ for sufficiently small δ" and thus can be expressed by a first order formula over $\mathbb{R}$. (It is not clear how to express condition (6.4) by a formula over $\mathbb{C}$.)

Condition (6.4) can now be expressed in $\mathrm{PH}^0_{\mathbb{R}}$ as follows:

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

The completes the proof. □

6.5 Proof of Proposition 6.3

The goal is to give a proof of Proposition 6.3. This section begins with a definition of the concepts of regular points and regular values, tailored to the situation of not necessarily smooth varieties.

Definition 6.16 Let $\varphi\colon X \to Y$ be a surjective morphism of irreducible complex projective varieties of the same dimension. A point $p \in X$ is called a *regular point* of φ if p is a smooth point of X and $d_p\varphi\colon T_pX \to T_{\varphi(p)}Y$ is an isomorphism (and hence $\varphi(p)$ is smooth in Y). A point $q \in Y$ is called a *regular value* of φ if all $p \in \varphi^{-1}(q)$ are regular points of φ.

Lemma 6.17 *Let $\varphi\colon X \to Y$ be a surjective morphism of irreducible complex projective varieties of the same dimension. Then all fibres of regular values of φ have the same finite cardinality.*

Proof. In [Mum76, Cor. 4.16] it is proved that any nonempty Zariski open subset of an irreducible complex projective variety is connected in the Euclidean topology. Sard's lemma [Mum76, 3.7] implies that the set R of regular values of φ is a nonempty Zariski open subset of Y. Therefore, R is connected. It is thus sufficient to prove that the function $\psi : R \to \mathbb{N}, y \mapsto |\varphi^{-1}(y)|$ is well defined and locally constant.

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

Recall that the Grassmannian $\mathbb{G}(k, n)$ is an irreducible smooth projective variety of dimension $\dim \mathbb{G}(k, n) = (k + 1)(n - k)$, see Chapter 4.

Lemma 6.18 *Let $\Gamma \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be an irreducible projective variety of dimension n and $0 \le i \le n$. Define the closed subvariety*

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

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

(i) The incidence relation Φ *is an irreducible projective variety of dimension* $\dim \Phi = \dim(\mathbb{G}(n-i,n) \times \mathbb{G}(i,n)) = 2i(n-i) + n$.

(ii) Let (p,q) *be a smooth point of* Γ *and* $(L^i, L^{n-i}) \in \mathbb{G}(n-i,n) \times \mathbb{G}(i,n)$. *Then* $\Gamma \pitchfork_{(p,q)} (L^i \times L^{n-i})$ *holds if and only if* (p,q,L^i,L^{n-i}) *is a regular point of the projection* π_2.

Proof. (i) Consider the projection $\pi_1 \colon \Phi \to \Gamma$ onto the first factor. For any $(p,q) \in \Gamma$, there is the following isomorphism of varieties

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

This is an irreducible variety of dimension $\dim \pi_1^{-1}(p,q) = 2i(n-i)$ (we use the convention $\mathbb{G}(-1,m) := \emptyset$). Using [Har95, Theorem 11.14], it follows that Φ is irreducible and

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

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

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

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

(Note that this notation L_a^i slightly differs from the one used in §6.2.) It is well known that [Har95, Lecture 6]

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

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

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

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

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

This induces the following local isomorphism φ around the origin:

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

Assume now that (p,q) is a smooth point of Γ. Let $f_1,\dots,f_n$ be polynomials in $X_1,\dots,X_n,Y_1,\dots,Y_n$ having the zero set $\widetilde{\Gamma} \subseteq \mathbb{C}^n \times \mathbb{C}^n$ locally around $(0,0)$ such that the differentials $df_1,\dots,df_n$ at $(0,0)$ are linearly independent (this is possible, see [Mum76]). Let $\widetilde{\Phi}$ denote the zero set of $f_1,\dots,f_n,g_1,\dots,g_n$ in $\mathbb{C}^n \times \mathbb{C}^n \times \mathbb{C}^{i\times(n+1-i)} \times \mathbb{C}^{(n-i)\times(i+1)}$. Then the map φ gives a local isomorphism of $\widetilde{\Phi}$ to Φ around the origin.

The differentials of the g_i at the origin satisfy

$$\begin{aligned} d_0 g_1 = d_0 a_{1,0} - d_0 X_{n-i+1}, \dots, d_0 g_i = d_0 a_{i,0} - d_0 X_n,\\ d_0 g_{i+1} = d_0 b_{1,0} - d_0 Y_{i+1}, \dots, d_0 g_n = d_0 b_{n-i,0} - d_0 Y_n.\end{aligned}$$

Clearly, these differentials are linearly independent of $d_0 f_1,\dots,d_0 f_n$. Therefore, the tangent space of $\widetilde{\Phi}$ at 0 is the zero set of $d_0 f_1,\dots,d_0 f_n, d_0 g_1,\dots,d_0 g_n$. In particular, $\dim T_0\widetilde{\Phi} = \dim \widetilde{\Phi}$ and hence 0 is a smooth point of $\widetilde{\Phi}$.

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

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

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

Proof of Proposition 6.3. Let $\Gamma \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be the closure of the graph of a rational map $\varphi\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^n$. Fix $0 \le i < n$ and consider the incidence relation

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

introduced in Lemma 6.18. Then the projection $\pi_2\colon \Phi \to \mathbb{G}(n-i,n)\times\mathbb{G}(i,n)$ satisfies all the assumptions of Lemma 6.17. Hence there is an integer d_i such that all fibres of π_2 at regular values (L^i, L^{n-i}) have cardinality d_i.

(i) If $\Gamma_U \pitchfork (L^i \times L^{n-i})$ and $\Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$, then all $(p,q) \in \pi_2^{-1}(L^i, L^{n-i})$ are in Γ_U and thus smooth points of Γ. Hence (p,q,L^i,L^{n-i}) is a regular value of π_2 by Lemma 6.18. Therefore,

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

which shows claim (i).

For part (ii), note first that the property $\Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$ holds for generic (L^i, L^{n-i}) since $\dim \Gamma_\Sigma < n$. Moreover, if $\Gamma_\Sigma \cap (L^i \times L^{n-i}) = \emptyset$ holds, then Lemma 6.18 implies that $\Gamma_U \pitchfork (L^i \times L^{n-i})$ if and only if (L^i, L^{n-i}) is a regular value of π_2. Hence the claim (ii) follows from Sard's lemma [Mum76, 3.7]. $\square$

Chapter 7

Hilbert Polynomial

In its most general form, the problem of computing the Hilbert polynomial can be specified as follows.

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 $f_1, \ldots, f_r$.

It can be shown that the problem of computing the Hilbert polynomial is FPSPACE-hard, see Section 7.4.2. A consequence of this is 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 7.22), which improves the #P-lower bound in Bach [Bac99].

The main theme of this chapter, however, is the study of the restricted problem of computing the Hilbert polynomial of a smooth equidimensional complex projective variety $V \subseteq \mathbb{P}^n$ within the framework of counting complexity theory, as developed in Chapter 5. More precisely, it is shown that this problem, called $\text{Hilbert}_{\text{sm}}$ for the moment (the exact specification is given below), is in $\text{Gap}_{\mathbb{C}}^{*}$ by means of a generic parsimonious reduction to the problem $\#\text{HN}_{\mathbb{C}}$. In particular, in the Turing model an FPSPACE-upper bound for the discrete version $\text{Hilbert}_{\text{sm}}^{\mathbb{Z}}$ is obtained.

7.1 Problem Specification and Statement of Results

When trying to formally define the problem under consideration, the question arises whether the smoothness condition can be tested at all within reasonable resources. The obvious idea of checking the Jacobian criterion at all points in the variety V (which is possible in $\text{coNP}_{\mathbb{C}}$) 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 $\mathcal{I}(V)$ of V. Indeed, it is not known whether a set of generators of $\mathcal{I}(V)$ can be computed from $f_1, \ldots, f_r$ in parallel polynomial time or even weaker, in single exponential time.

To overcome these difficulties, an input specification is given 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.

Given homogeneous polynomials $f_1, \dots, f_r$ in $\mathbb{C}[X_0, \dots, X_n]$ and $m \in \mathbb{N}$, the following condition will be referred to as the *input condition*:

$$\begin{aligned} &\forall x \in \mathcal{Z}(f_1, \dots, f_r) - \{0\} \\ &\dim\{z \in \mathbb{C}^{n+1} \mid d_x f_1(z) = 0, \dots, d_x f_r(z) = 0\} \leq m + 1. \end{aligned} \tag{7.1}$$

This input condition (7.1) can be tested in $\mathrm{coNP}_{\mathbb{C}}$.

Lemma 7.1 *Assume $V' = \mathcal{Z}(f_1, \dots, f_r)$ satisfies the input condition (7.1) for some $m \in \mathbb{N}$. 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 $\dim W < m$.*

Proof. For all $x \in V'$, $\mathbb{T}_x V' \subseteq \mathbb{P}(\cap_{i=1}^r \ker d_x f_i)$ holds, where $\mathbb{T}_x V'$ is the projective tangent space of V' at x. The input condition implies that for all $x \in V'$, $\dim_x V' \leq \dim \mathbb{T}_x V' \leq m$ is satisfied. Therefore, all points $x \in V'$ of local dimension m are smooth. The claim follows since there is exactly one irreducible component passing through a smooth point. □

In particular, from the input condition it follows that the irreducible components of the m-dimensional part V of V' are pairwise disjoint and 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 $n - m$.

The formal specification of $\mathrm{HILBERT}_{\mathrm{sm}}$ can now be given. In order to make sure that the output is an integer, a certain multiple of the k-th coefficient of the Hilbert polynomial is computed.

$\mathrm{HILBERT}_{\mathrm{sm}}$ (*Hilbert polynomial of smooth equidimensional varieties*). Given integers $0 \leq k \leq m \leq n$ and a family $f_1, \dots, f_r$ of homogeneous polynomials in $\mathbb{C}[X_0, \dots, X_n]$ 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 chapter.

Theorem 7.2 *The problem $\mathrm{HILBERT}_{\mathrm{sm}}$ is in $\mathrm{GAP}^*_{\mathbb{C}}$. In particular, the problem $\mathrm{HILBERT}_{\mathrm{sm}}$ Turing reduces (over $\mathbb{C}$) to $\mathrm{HN}_{\mathbb{C}}$.*

This theorem immediately implies the following corollary, cf. Section 5.3.

Corollary 7.3 *The problem $\mathrm{HILBERT}^{\mathbb{Z}}_{\mathrm{sm}}$ is in $\mathrm{BP}(\mathrm{GAP}^*_{\mathbb{C}})$. In particular, the problem $\mathrm{HILBERT}^{\mathbb{Z}}_{\mathrm{sm}}$ Turing reduces to $\mathrm{HN}^{\mathbb{Z}}_{\mathbb{C}}$.*

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

1. 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 [Hir95] 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 pull-back of a Schubert variety under the Gauss map (cf. Fulton [Ful98, Ex. 14.3.3]). The geometric degree of such a degeneracy locus is called a projective character.

This allows to express (certain integer multiples of) the coefficients of the Hilbert polynomial as integer linear combinations of projective characters. Next, 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 5.19), is used.

7.2 Projective Characters

General references for the material presented in this section are [Ful97, Man01]. In the following we assume $0 \le m \le n$ and consider the Grassmannian

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

as defined in Chapter 4.

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 $0 \le i \le n$. It is an irreducible smooth projective variety [Ful97, 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 $(\dim(A \cap F_j))_{0 \le j \le n}$ and denote by $0 \le \sigma_0 < \sigma_1 < \cdots < \sigma_m \le n$ the positions where the "jumps" occur, that is, $\dim(A \cap F_j) = i$ for $\sigma_i \le j < \sigma_{i+1}$ (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 $n - m \ge \lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_{m+1} \ge 0$ 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 $\mathbb{G}(m,n)$ [Ful97, III.9.4]. (Note that since λ is admissible, we have $|\lambda| \leq \dim \mathbb{G}(m,n)$.) In general, Schubert varieties are singular [Man01, §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 $F_{-1} = \emptyset$)

$$e_\lambda(\underline{F}) := \{A \in \Omega_\lambda(\underline{F}) \mid \dim(A \cap F_{\sigma_i - 1}) = i - 1 \text{ for } 0 \leq i \leq m\}. \tag{7.2}$$

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

$$\Omega_\lambda(\underline{F}) = \bigcup_{\lambda \subseteq \mu} e_\mu(\underline{F}), \tag{7.3}$$

where the union is over all admissible partitions μ containing λ, cf. [Ful97, III.9.4, Ex. 13] or [Man01, §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. [Man01, §3.4].

Example 7.4 (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 $\mathbb{T}_xV \subseteq \mathbb{P}^n$ at x. For an admissible partition λ and a flag $\underline{F} \in \mathcal{F}$ we define the *generalised polar variety*

$$P_\lambda(\underline{F}) := \varphi^{-1}(\Omega_\lambda(\underline{F})) = \{x \in V \mid \dim(\mathbb{T}_xV \cap F_{\sigma_i}) \geq i \text{ for } 0 \leq i \leq m\} \quad (7.4)$$

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

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

correspond to the special case $\lambda = (1^k) = (1,\ldots,1,0,\ldots,0)$, see [Pie78, Bra00]. We remark that a different concept of generalised polar varieties has been previously used for algorithmic purposes, see [BGHM01, BGHP04].

Note that the case where V is a linear space is degenerate: then we have $\dim\varphi(V) = 0$ and thus $P_\lambda(\underline{F})$ is empty for almost all $\underline{F} \in \mathcal{F}$, provided $|\lambda| > 0$. A result by Zak, cf. [FL81, §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 from Section 4.3 the important notion of transversality. For $x \in V$ we denote by T_xV the Zariski tangent space and by $d_x\varphi\colon T_xV \to T_{\varphi(x)}\mathbb{G}(m,n)$ 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

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

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 7.5 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 (7.3) by Schubert cells.

Definition 7.6 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 of central importance, since it allows to define the projective characters.

Lemma 7.7 *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* $\mathrm{codim}_V P_\lambda(\underline{F}) = |\lambda|$,

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

We call $\deg P_\lambda := d_\lambda$ the *projective character* of V corresponding to λ. These quantities were studied by Severi [Sev02], see also [Ful98, Ex. 14.3.3]. Note that the degree of V equals the projective character for $\lambda = 0$.

Example 7.8 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.

For the proof of Lemma 7.7 we need the following result of Kleiman [Kle74], see also [Har77, III.10].

Lemma 7.9 *Let* $\varphi\colon V \to Y$ *be a morphism of smooth irreducible varieties and let* $X \subseteq Y$ *be a quasi-projective 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* $\delta := \dim \varphi(V) + \dim X - \dim Y \geq 0$, *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 $\lambda_1 \leq n - m$ and the length is at most $m + 1$.

Corollary 7.10 *Let* $Z \subseteq \mathbb{G}(m, n)$ *be a quasi-projective 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* $|\lambda| \leq \dim Z$, *and it is empty otherwise.*

Proof. Recall from (7.3) 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. [Man01, §3.6]) and we have $g e_\lambda(\underline{F}) = e_\lambda(g\underline{F})$. Decompose Z as finite disjoint union of smooth irreducible quasi-projective varieties Z_j. We can then apply Lemma 7.9 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 7.7. 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 [FL81, §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. [Har95, Thm.17.24].

(i) Let $\mu \supseteq \lambda$ be an admissible partition. Lemma 7.9 implies that for almost all flags $\underline{F} \in \mathcal{F}$, φ meets $e_\mu(\underline{F})$ transversely. Looking at the cell decomposition (7.3) of $\Omega_\lambda(\underline{F})$, the claim follows (recall Definition 7.6).

(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 (7.3) 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 7.5, $\varphi^{-1}(e_\mu(\underline{F}))$ 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 fibres 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* neighbourhood of g'.

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

$$A \cap \varphi^{-1}(g'\partial e) = \emptyset \ \text{ and } A \pitchfork \varphi^{-1}(g'e). \tag{7.5}$$

Then the intersection $A \cap \varphi^{-1}(g'\Omega)$ consists of exactly N elements, say $x_1, \ldots, x_N$, cf. [Mum76, §5A]. It is therefore sufficient to show that for all g in some neighbourhood of g' condition (7.5) 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 neighbourhood U of g' and a Euclidean neighbourhood 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. □

The following is used later.

Lemma 7.11 *Let W be a quasi-projective 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.*

Proof. 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 [Sha74, §I.6.3 Thm. 7] (see also [Har95, 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 7.10, 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 [Har95, Thm. 17.24]. □

7.3 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:

$$\begin{aligned}\Delta_\lambda(c) &:= \det\left((c_{\lambda_i - i + j})_{1\leq i,j\leq r}\right)\\ &= \det\begin{pmatrix} c_{\lambda_1} & c_{\lambda_1+1} & \cdots & c_{\lambda_1+r-1}\\ c_{\lambda_2-1} & c_{\lambda_2} & \cdots & c_{\lambda_2+r-2}\\ \cdots & \cdots & \cdots & \cdots\\ c_{\lambda_r-r+1} & c_{\lambda_r-r+2} & \cdots & c_{\lambda_r}\end{pmatrix},\end{aligned} \tag{7.6}$$

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

$$\sum_{i\geq 0} b_i t^i := \frac{t}{1-e^{-t}} = 1 + \frac{t}{2} + \sum_{j\geq 1}(-1)^{j-1}\frac{B_j}{(2j)!}t^{2j}, \tag{7.7}$$

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 7.12 It is known that $B_n = (-1)^{n-1}\sum_{k=1}^{2n}\frac{1}{k+1}\sum_{r=1}^{k}(-1)^r\binom{k}{r}r^n$ [GKP94, 6.5]. 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

$$\delta^{m,k}_\mu := (-1)^{|\mu|}\sum_{\substack{\mu\subseteq\lambda\\ |\lambda|=m-k}}\Delta_\lambda(b)d^m_{\lambda\mu}, \tag{7.8}$$

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

The following crucial statement is proved in Chapter 8.

Theorem 7.13 *Let $V \subseteq \mathbb{P}^n$ be a smooth complex projective variety of pure dimension m and $0 \le k \le m$. Then the k-th coefficient $p_k(V)$ of the Hilbert polynomial of V is given by*

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

where $\deg P_\mu$ is the projective character introduced in §7.2. In particular, $[(m-k+1)! \cdots 2!1!]^2\, k!\, p_k(V)$ is an integer.

Example 7.14 1. The above formula yields $p_m(V) = \frac{1}{m!}\,\delta_0^{m,m} \deg P_0 = \frac{1}{m!} \deg V$, as expected (check that $\Delta_0(b) = 1, d_{0,0}^m = 1$).

2. In the case where $V \subseteq \mathbb{P}^n$ is a smooth curve ($n \ge 2$), the above formula implies that $p_0 = \delta_0^{1,0} \deg P_0 + \delta_1^{1,0} \deg P_1 = \deg V - \frac{1}{2} \deg P_1$, 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 7.8), 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 $\deg P_1 = 2(n-1)$.

7.4 Complexity of Computing the Hilbert Polynomial

The goal of this section is to prove Theorem 7.2, that is, that the problem of computing the Hilbert polynomial of a smooth equidimensional projective variety lies in the class $\mathrm{GAP}_{\mathbb{C}}^*$.

7.4.1 Upper Bounds

The upper bound on $\mathrm{HILBERT}_{\mathrm{sm}}$ is based on Theorem 7.13. We therefore first study the problem to compute projective characters (recall Lemma 7.7 for their definition).

PROJCHAR (*Projective characters*). Given $0 \le m \le n$, 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 7.15 *The problem* ProjChar *is in* $\#\mathrm{P}^*_{\mathbb{C}}$.

We prove Proposition 7.15 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 $\sigma_i = n - m + i - \lambda_{i+1}$)

$$Q_\lambda(\underline{F}) := \{x \in V' \mid \dim(\psi(x) \cap F_{\sigma_i}) \geq i \text{ for } 0 \leq i \leq m\}. \tag{7.9}$$

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 7.16 *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 5.22). The claim follows now from Lemma 5.21. □

Proof of Proposition 7.15. 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 (7.9). By the input condition (7.1), $\psi(x)$ 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 7.1, 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 generalised polar variety introduced in (7.4) 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 7.7, 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

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

where Φ is the function from Lemma 7.16, 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 5.9).

Lemma 7.7 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 7.11 to the quasi-projective 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 $\mathrm{PH}_{\mathbb{R}}^{0}$. According to Definition 7.6, $\varphi \pitchfork \Omega_\lambda(\underline{F})$ can be expressed as follows:

$$\forall \mu \; (\mu \supseteq \lambda \wedge \mu \text{ admissible } \Longrightarrow \varphi \pitchfork e_\mu(\underline{F})), \tag{7.10}$$

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

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

Lemma 7.24 in Section 7.5 says that the local transversality condition in the parenthesis is decidable in $\mathrm{P}_{\mathbb{C}}^{0}$. This implies that condition (7.10) is expressible in $\mathrm{coNP}_{\mathbb{C}}^{0}$ and thus in $\mathrm{PH}_{\mathbb{R}}^{0}$.

In order to express $\dim R_\lambda(\underline{F}) < m - |\lambda|$, we recall that the points $x \in W$ can be characterised among the points of V' as those having local dimension smaller than m, cf. Lemma 7.1. The local dimension of (semi-)algebraic sets is expressible in the constant-free polynomial hierarchy over the reals (compare Lemma 4.16). We can thus express membership to $R_\lambda(\underline{F})$ in $\mathrm{PH}_{\mathbb{R}}^{0}$. Finally, using Lemma 4.16 again, we conclude that the condition $\dim R_\lambda(\underline{F}) < m - |\lambda|$ is expressible in $\mathrm{PH}_{\mathbb{R}}^{0}$. □

Using Proposition 7.15, we can proceed to prove the main Theorem 7.2.

Proof of Theorem 7.2. 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 $|\mu| \le m-k$, $\mu_1 \le n-m$ and $\delta_\mu^{m,k}$ is defined in Equation (7.8), i.e., $\delta_\mu^{m,k} := (-1)^{|\mu|}\sum_{\mu\subseteq\lambda,|\lambda|=m-k}\Delta_\lambda(b)d^m_{\lambda\mu}$. By Remark 7.12, 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. [For97]) 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 7.15, $\varphi \in \#\mathrm{P}_{\mathbb{C}}^*$, so we can apply the Summation Lemma 5.19 to the main formula in Theorem 7.13 to conclude that $\text{Hilbert}_{\text{sm}} \in \text{Gap}_{\mathbb{C}}^*$. □

7.4.2 Lower Bounds

We first complement the upper bound in Corollary 7.3 by a lower bound.

Proposition 7.17 *The problem* $\text{Hilbert}^{\mathbb{Z}}_{\text{sm}}$ *is* $\#\mathsf{P}$*-hard.*

Proof. We proceed as in [Bac99]. 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 $\#\mathsf{P}$-complete [Val79b, Val79a].

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 homogenisation 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 (7.1) 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 $\text{Hilbert}^{\mathbb{Z}}_{\text{sm}}$. □

Remark 7.18 Due to the input condition (7.1) it is not clear whether $\text{Hilbert}_{\text{sm}}$ and $\text{Hilbert}^{\mathbb{Z}}_{\text{sm}}$ are $\#\mathrm{P}_{\mathbb{C}}$-hard and GCC-hard, respectively.

Corollary 7.3 states that the problem $\text{HILBERT}_{\text{sm}}^{\mathbb{Z}}$ to compute the Hilbert polynomial of smooth varieties is in $\text{BP}(\text{GAP}_{\mathbb{C}}^{*})$. 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 $\text{HIM}^{\mathbb{Z}}$ to $\text{HILBERT}^{\mathbb{Z}}$, and then invoke a result in Mayr [May97, Thm. 17], which states that $\text{HIM}^{\mathbb{Z}}$ is PSPACE-complete.

Lemma 7.19 *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 7.20 *The problem* $\text{HILBERT}^{\mathbb{Z}}$ *is* FPSPACE-*hard.*

Based on this theorem, we can now improve the #P-lower bound in [Bac99] 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 [Har77, Iit82]. We encode the input to our problems as in [Bac99]. Thus we specify a coherent sheaf on $\mathbb{P}^n$ by giving a *graded matrix*. This is a matrix $(p_{ij})_{1 \leq i \leq s, 1 \leq j \leq r}$ 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. [Har77, 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 $i > n$ [Har77, III.2.7].) The Euler characteristic of the sheaf $\widetilde{M}$ is defined as

$$\chi(\widetilde{M}) := \sum_{i=0}^{n} (-1)^i \dim H^i(\mathbb{P}^n, \widetilde{M}). \tag{7.11}$$

The link to the Hilbert polynomial is given by the following proposition, a proof of which can be found in [Iit82, Section 7.6], see also [Har77, Ex. III.5.2].

Proposition 7.21 *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 [Bac99].

Corollary 7.22 *The problems* RankSheaf$^{\mathbb{Z}}$ *and* EulerSheaf$^{\mathbb{Z}}$ *are both* FPSPACE*-hard.*

Proof. Clearly, EulerSheaf$^{\mathbb{Z}}$ can be Turing reduced to RankSheaf$^{\mathbb{Z}}$. Theorem 7.20 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 7.21 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 7.23 The algorithm in [BS92] combined with the upper bounds in [May97] implies that Hilbert$^{\mathbb{Z}}$ is in $\mathsf{FEXPSPACE}$. We do not know of any better upper bound on this problem. The known algorithms for sheaf cohomology (cf. [Vas98, Chapter 8], [DE02]) suggest that RankSheaf$^{\mathbb{Z}}$ is in $\mathsf{FEXPSPACE}$.

7.5 Expressing Transversality

In this section we conclude the proof of Proposition 7.15. 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 (7.1) 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 7.1 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 $\mathtt{trans} \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty \times \mathbb{C}^\infty$ by

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

where φ is the Gauss map of V.

Lemma 7.24 *The relation* $\mathtt{trans}$ *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 [Ful97, III.9] and [Man01].

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 (7.2). (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:

$$\begin{pmatrix} * & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & 0 & * & * & 1 & 0 & 0 & 0 \\ * & 0 & * & * & 0 & * & 1 & 0 \\ * & 0 & * & * & 0 & * & 0 & 1 \end{pmatrix}. \tag{7.12}$$

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 $\ell_{\sigma_0}, \dots, \ell_{\sigma_m}$ and $\{\ell_j \mid j \notin \{\sigma_0, \dots, \sigma_m\}\}$, 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

$$\alpha_\mu \colon U_\mu \xrightarrow{\sim} \mathrm{Hom}(L_\mu, \overline{L}_\mu) \xrightarrow{\sim} \mathbb{C}^{(n-m)\times(m+1)}, \tag{7.13}$$

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 (7.12) 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 $e_\mu \subseteq U_\mu$ and that the image of e_μ under α_μ can be described as follows:

$$\alpha_\mu(e_\mu) = \left\{ (a_{ij}) \in \mathbb{C}^{(n-m)\times(m+1)} \mid a_{ij} = 0 \text{ for } j \ge \sigma_i - i, \begin{array}{c} 0 \le i \le m, \\ 0 \le j < n - m \end{array} \right\}. \tag{7.14}$$

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

Proof of Lemma 7.24. Assume that $x \in V$ and $\varphi(x) \in e_\mu(\ell)$. The claim is that the transversality condition

$$T_{\varphi(x)}\mathbb{G}(m, n) = d_x\varphi(T_xV) + T_{\varphi(x)}e_\mu(\ell). \tag{7.15}$$

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 (7.13). 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 (7.15) translates into

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

Equation (7.14) 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 $X_0, \dots, X_n$ 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 $f_1, \dots, f_r$. 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 $(\frac{\partial f_s}{\partial X_t}(x))_{1\le s\le r, m<t\le n}$ has rank $n-m$. After a permutation, we assume that $(\frac{\partial f_s}{\partial X_t}(x))_{1\le s\le n-m, m<t\le n}$ is invertible. It will be convenient to use the abbreviations $X' := (X_0, \dots, X_m)$ and $X'' := (X_{m+1}, \dots, X_n)$.

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

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

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

$$\frac{\partial f_s}{\partial X_i}(X', h(X')) + \sum_{t=m+1}^{n} \frac{\partial f_s}{\partial X_t}(X', h(X'))\frac{\partial h_t}{\partial X_i}(X') = 0 \tag{7.16}$$

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 (7.16) with respect to X_j for $0 \leq j \leq m$ 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. □

Chapter 8

Hilbert Polynomial and Degeneracy Loci

This chapter is devoted to the proof of Theorem 7.13. Some preliminary material is presented first. As in Chapter 4, the aim is mainly to fix terminology. We base the rudimentary intersection theory used in this chapter on singular homology theory. For a more general setting, a good reference is Fultons treatment [Ful98].

8.1 Singular Homology Theory

Associated to a topological space X are the singular homology groups $H_i(X)$ and cohomology groups $H^i(X)$, with coefficients in $\mathbb{Z}$. These groups are homotopy invariants.

There is a cup product

$$H^i(X) \otimes H^j(X) \to H^{i+j}(X), \ \alpha \otimes \beta \mapsto \alpha \smile \beta,$$

and a cap product

$$H^i(X) \otimes H_j(X) \to H_{j-i}(X), \ \alpha \otimes b \mapsto \alpha \frown b.$$

The cup product turns $H^*(X) = \oplus H^i(X)$ into a skew-commutative ring with $1 \in H^0(X)$ as unit. The cap product gives the total homology group $H_*(X) = \oplus H_i(X)$ the structure of a $H^*(X)$-module. In particular, the identity

$$(\alpha \smile \beta) \frown a = \alpha \frown (\beta \frown a)$$

holds for $\alpha \in H^i(X)$, $\beta \in H^j(X)$ and $a \in H_k(X)$. A special case is the evaluation map $H^i(X) \otimes H_i(X) \to \mathbb{Z}, \alpha \otimes a \mapsto \langle \alpha, a \rangle = \epsilon_*(\alpha \frown a)$, where ϵ_* is the augmentation map [Bre97, IV.2]. If $H_{k-1}(X)$ is torsion-free, then $H^k(X) = \mathrm{Hom}(H_k(X), \mathbb{Z})$ by the universal coefficient theorem [Bre97, V.7], and $\langle \cdot, \cdot \rangle$ is just the usual evaluation.

A continuous map $f \colon X \to Y$ induces a push-forward $f_* \colon H_*(X) \to H_*(Y)$ and pull-back $f^* \colon H^*(Y) \to H^*(X)$. These maps satisfy the identity

$$f_*(f^*(\alpha) \frown a) = \alpha \frown f_*(a)$$

for $\alpha \in H^*(Y)$ and $a \in H_*(X)$. The $\smile$ for the cup product is often omitted, and $\alpha \cdot \beta$ or simply $\alpha\beta$ is written instead for $\alpha \smile \beta$.

For a connected, compact, oriented manifold M of dimension m, the top homology $H_m(M)$ is isomorphic to $\mathbb{Z}$, and its distinguished generator is called the fundamental class μ_M [Bre97, VI.7]. It consists of the sum of all top-dimensional simplices in a triangulation. A nonsingular, irreducible subvariety of $\mathbb{P}^n$ is a compact, connected, $2m$-dimensional manifold with the orientation induced from the complex structure, and thus possesses a fundamental class [MS74, Chapter 13].

A fundamental class can be associated to any irreducible variety. According to [Hir75], any variety can be triangulated, such that the singular locus is a subcomplex of strictly smaller dimension. The fundamental class is then the sum of the top dimensional simplices, the orientation being provided by the complex structure. For another approach to showing the existence of a fundamental class, based on Borel-Moore homology, cf. [Ful97, Appendix B].

Let V be an m-dimensional, irreducible variety. There is the Poincaré duality map

$$H^i(V) \to H_{2m-i}(V), \alpha \mapsto \alpha \frown \mu_V$$

which is an isomorphism for nonsingular V, see [Bre97, VI.8].

In the nonsingular case, the Poincaré dual of the cup product is called the intersection product $\cdot\colon H_i(V) \times H_j(V) \to H_{i+j}(V)$ defined by

$$(\alpha \frown \mu_V) \cdot (\beta \frown \mu_V) = (\alpha \smile \beta) \frown \mu_V.$$

Let $i\colon V \to M$ be the inclusion of an irreducible m-dimensional variety into a smooth, irreducible, n-dimensional variety M. The push-forward $[V]_M := i_*\mu_V$ of the fundamental class is called the class of V in $H_{2m}(M)$. If the ambient variety M is understood or not important, we omit the index and write $[V]$ instead of $[V]_M$. The most common case we will encounter is where $M = \mathbb{P}^n$. If V is not irreducible, define

$$[V] = [W_1] + \cdots + [W_\ell],$$

where the sum goes over the irreducible components of maximal dimension. The intersection product has the property that if V, W meet transversely in M, then

$$[V] \cdot [W] = [V \cap W],$$

see [Bre97, VI.11] for a detailed discussion. Note that the intersection product operating on $[V]$ and $[W]$ is defined in $H_*(M)$, and we do not require V and W to be nonsingular.

Of special importance is the cohomology of complex projective space $\mathbb{P}^n$. As a ring, $H^*(\mathbb{P}^n) = \mathbb{Z}[a]/(a^{n+1})$, with distinguished generator $a \in H^2(\mathbb{P}^n)$. The even cohomology groups are torsion-free and given by $H^{2i}(\mathbb{P}^n) = \mathbb{Z}a^i$, the odd ones are zero. A linear subspace L^k of codimension k satisfies the relation $\langle a^{n-k}, [L^k]\rangle = 1$, and since $H^k(\mathbb{P}^n) = \operatorname{Hom}(H_k(\mathbb{P}^n), \mathbb{Z})$, the class $[L^k]$ generates $H_{2n-2k}(\mathbb{P}^n)$.

In particular, linear subspaces of the same dimension are homologous to one another. Let $[L]$ be the class of a hyperplane. From the previous discussion it follows that $[L]^k = [L^k]$, where $[L]^k$ means the k-fold intersection product and L^k is a subspace of codimension k. Moreover, if $a \in H^2(\mathbb{P}^n)$ is the distinguished generator mentioned above and $V \subseteq \mathbb{P}^n$ is a smooth, projective subvariety, then

$$a^k \frown [V] = [L^k] \cdot [V] = [L^k \cap V], \tag{8.1}$$

where L^k is a generic linear subspace of codimension k in $\mathbb{P}^n$.

Let $i\colon V \hookrightarrow \mathbb{P}^n$ be the inclusion of an m-dimensional irreducible variety. From the homology of $\mathbb{P}^n$ it follows that $i_*\mu_V = [V] = d[L^{n-m}]$ for some integer d. This coefficient is in fact equal to the geometric degree of the embedding of V into $\mathbb{P}^n$. If $f\colon V \to \mathbb{P}^n$ is any morphism such that $f(V)$ has the same dimension as V, then

$$f_*\mu_V = d[f(V)],$$

where d is the degree of the generic fibre of f [Ful97, Appendix B]. This is simply called the degree of f.

8.2 Chern Classes and Riemann-Roch

References for the material presented here are [Che46, Hir95, MS74]. See also [Ful98] for the algebraic geometry perspective. Let $V \subseteq \mathbb{P}^n$ be a projective variety. 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 characterised 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 $f^*(E)$ is the pull-back bundle with respect to f.

3. (Whitney formula.) An exact sequence $0 \to E' \to E \to E'' \to 0$ of bundles implies $c_k(E) = \sum_i c_i(E') \smile c_{k-i}(E'')$.

From Equation (8.1) it follows that for a smooth, closed subvariety $V \subseteq \mathbb{P}^n$, the cap product $c_1(\mathscr{L})^k \frown [V]$ corresponds to intersecting V with k generic hyperplanes.

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 [MS74, 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 in order 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 (7.7) 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

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

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

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

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

$$\operatorname{ch}(\mathcal{O}_V(d)) = e^{c_1(\mathcal{O}_V(d))} = \sum_{i\geq 0} \frac{d^i}{i!} c_1(\mathscr{L}_V)^i. \tag{8.2}$$

To a vector bundle E on a variety V there corresponds a locally free sheaf $\mathscr{E}$, see [Sha74, VI.1.3] or [Har77, 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 (7.11).

Lemma 8.1 *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 $H^j(V, \mathscr{F}) = H^j(\mathbb{P}^n, i_*\mathscr{F})$ for all j, cf. [Har77, 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 7.21 we have $\chi(\mathcal{O}_V(d)) = p_V(d)$. □

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

Theorem 8.2 (Hirzebruch-Riemann-Roch, [Hir95]) *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 8.2 combined with Lemma 8.1 and Equation (8.2) immediately yields the following.

Corollary 8.3 *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.

8.3 Generalities on Symmetric Functions

We gather some results from the theory of symmetric functions that will be used later. Reference for this material are [Mac95, Man01], [FH91, Appendix A] and [Ful98, Appendix A.9].

For a partition λ, we denote by λ' its conjugate partition. Recall the definition of $\Delta_\lambda(c)$ in Equation (7.6). Claims 1 and 2 of the following lemma are easy to verify, a proof of the third one is given in [Ful98, Lemma A.9.2].

Lemma 8.4 *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 8.5 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

$$s_\lambda(\gamma) := s_\lambda(\gamma_1, \ldots, \gamma_m) = \frac{\det(\gamma_i^{\lambda_j+m-j})_{1\leq i,j\leq m}}{\det(\gamma_i^{m-j})_{1\leq i,j\leq m}}. \qquad (8.3)$$

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 [Man01, 1.2.4], [Mac95, I.3], and [FH91, Appendix A][1].

Lemma 8.6 *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 $\Delta_\lambda(c) = s_{\lambda'}(\gamma)$.

[1] The formula presented is sometimes referred to as Jacobi-Trudi formula [Man01] or Giambelli's formula [FH91, Appendix A].

Example 8.7 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 [Ful98, Example A.9.1] (see also [Mac95, Example I.3.10]).

Lemma 8.8 *Let λ be a partition with $|\lambda| \le m$. Then*

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

where

$$d^m_{\lambda\mu} = \det\begin{pmatrix}\lambda_i+m+1-i\\ \mu_j+m+1-j\end{pmatrix}_{1\le i,j\le m}$$

Example 8.9 Let $\lambda = (1^k)$. Then any subpartition $\mu \subseteq \lambda$ is of the form (1^j) for some $j \le k$ and $d^m_{\lambda\mu} = \binom{m-j+1}{m-k+1}$. This follows from looking at the coefficients of the expansion of $s_{(1^k)}(\gamma_1+\beta,\dots,\gamma_{m+1}+\beta)$, using the fact that $s_{(1^k)}$ is an elementary symmetric function (see Example 8.7).

8.4 Proof of Theorem 7.13

In this section we derive Theorem 7.13 from Corollary 8.3 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 $T_m(c_1,\dots,c_m)$.

Lemma 8.10 *Let $b = \{b_i\}_{i\in\mathbb{N}}$ be the sequence of rational numbers from Equation (7.7), $c_0 = 1$ and let $c_1,\dots,c_m$ be variables. Then the m-th Todd polynomial is given by*

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

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

Proof. Consider the (formal) factorisations

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

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 [Mac95, I.4(4.2'-3')] we have

$$\sum_{|\lambda|\leq m}\sigma_\lambda(\beta)m_\lambda(\gamma)=\prod_{1\leq i,j\leq m}(1+\beta_j\gamma_i)=\sum_{|\lambda|\leq m}s_{\lambda'}(\beta)s_\lambda(\gamma), \tag{8.4}$$

where s_λ is the Schur polynomial of the partition λ. Lemma 8.6 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 (8.4) 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 generalised 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 $x\in V$, $\mathbb{T}_xV=\mathbb{P}(\widetilde{T}_xV)$.

The proof of the following proposition uses a result of Kempf and Laksov [KL74, Theorem 10], see also [Ful98, Theorem 14.3] or [Man01, 3.8].

Proposition 8.11 *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 sub-bundles of E with A_i corresponding to $F_{\sigma_{i-1}}$ for $1\leq i\leq m$. Thus $\mathrm{rank}(A_i)=\sigma_{i-1}+1=n-m+i-\lambda_i$. 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 [Ful98, Chapter 14] coincides with the generalised polar variety $P_\lambda(\underline{F})$. Here, by $\dim(\ker \pi(x) \cap A_i(x))$ we mean the affine dimension. The statement of [Ful98, 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 [Ful98], $\Omega_\lambda(\underline{A};\pi)$ 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 7.7. Moreover, there is a cycle map $A_*(\Omega_\lambda(\underline{A};\pi)) \to H_*(\Omega_\lambda(\underline{A};\sigma))$ [Ful98, 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 $c_i(\widetilde{T}V^\vee) = (-1)^i c_i(\widetilde{T}V)$ [Ful98]. Using Lemma 8.4, 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 8.12 *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 8.8.

Proof. It is well known (compare [Har95, Chapter 16]) that the tangent bundle TV of a smooth variety is given by $TV \cong \mathrm{Hom}\left(\mathscr{L}_V^\vee, \widetilde{T}V/\mathscr{L}_V^\vee\right)$. Taking the direct sum with the trivial bundle $E = \mathrm{Hom}(\mathscr{L}_V^\vee, \mathscr{L}_V^\vee)$ we get

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

By the Whitney product formula (see §8.2) 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 factorisation and set $\beta := c_1(\mathscr{L}_V)$. By Lemma 8.6 we have for a partition μ with $|\mu| \leq m$

$$\Delta_{\mu'}(c(\widetilde{T}V)) = s_\mu(\gamma_1, \ldots, \gamma_{m+1}). \tag{8.5}$$

On the other hand, it is known that (see [Ful98, Remark 3.2.3b])

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

Using Lemma 8.6 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 8.8 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 8.11 and (8.5) 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 8.13 Let $\lambda = (1^k)$. Then $\Delta_{\lambda'}(c) = c_k(TV)$, the k-th Chern class of the tangent bundle. By Example 8.9 we have $d^m_{\lambda\mu} = \binom{m-j+1}{m-k+1}$, where $\mu = (1^j)$. Plugging this into the formula of Lemma 8.12, 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 [Pie78, Bra00].

Proof of Theorem 7.13. 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 8.10 and Lemma 8.12:

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

(Recall the definition of $\delta_\mu^{m,k}$ in Equation (7.8).) By Corollary 8.3 we obtain for the k-th coefficient $p_k(V)$ of the Hilbert polynomial of V

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

Since capping with $c_1(\mathscr{L}_V)^{m-|\mu|}$ corresponds to intersecting with a generic linear subspace of codimension $m - |\mu|$ in V, it follows that the degree $\deg \big(c_1(\mathscr{L}_V)^{m-|\mu|} \frown [P_\mu] \big) = \deg P_\mu$. 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. □

Bibliography

[Alu03] P. Aluffi. Computing characteristic classes of projective schemes. *J. Symbolic Comput.*, 35(1):3–19, 2003.

[AS00] N. Alon and J. H. Spencer. *The probabilistic method.* Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience [John Wiley & Sons], New York, 2000.

[Bac99] E. Bach. Sheaf cohomology is #P-hard. *J. Symbolic Comput.*, 27(4):429–433, 1999.

[Bas99] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. *Discrete Comput. Geom.*, 22(1):1–18, 1999.

[Bau02] H. Bauer. *Wahrscheinlichkeitstheorie.* de Gruyter Lehrbuch. Walter de Gruyter & Co., Berlin, 2002.

[BC] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets. `http://www.arxiv.org/abs/cs/cs.CC/0312007`. Extended abstract in *Proc. 36th Ann. ACM STOC*, pages 475–485, 2004.

[BC04a] 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`.

[BC04b] 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*, volume 13 of *Quaderni di Matematica*, pages 73–151. Aracne, 2004.

[BCL04] 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.

[BCL05] P. Bürgisser, F. Cucker, and M. Lotz. Counting complexity classes for numeric computations III: Complex projective sets. *Foundations of Computational Mathematics*, 2005. To appear.

[BCR91] 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.

[BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften.* Springer Verlag, 1997.

[BCSS96] L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic Settings for the Problem "$P \neq NP$?". In *The mathematics of numerical analysis*, number 32 in Lectures in Applied Mathematics, pages 125–144. Amer. Math. Soc., 1996.

[BCSS98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer, 1998.

[Bel97] R. Bellman. *Introduction to matrix analysis.* SIAM, Philadelphia, PA, 1997.

[BGHM01] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.

[BGHP04] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties: Geometry and algorithms. 2004. Preprint.

[Big97] A. M. Bigatti. Computation of Hilbert-Poincaré series. *J. Pure Appl. Algebra*, 119(3):237–253, 1997.

[BK81] E. Brieskorn and H. Knörrer. *Ebene algebraische Kurven.* Birkhäuser Verlag, Basel, 1981.

[BL02] P. Bürgisser and M. Lotz. Lower bounds on the bounded coefficient complexity of bilinear maps. In *Proc. 43rd FOCS, Vancouver*, pages 658–668, 2002.

[BL04] P. Bürgisser and M. Lotz. Lower bounds on the bounded coefficient complexity of bilinear maps. *J. ACM*, 51(3):464–482, 2004.

[BL05] P. Bürgisser and M. Lotz. The complexity of computing the Hilbert polynomial of smooth equidimensional complex projective varieties. `www.arxiv.org/abs/cs/cs.CC/0502044`, 2005.

[BM93] 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.

[Bor77] A.B. Borodin. On relating time and space to size and depth. *SIAM J. Comp.*, 6:733–744, 1977.

[Bou70] N. Bourbaki. *Elément de Mathématique. Algèbre*, volume I. Hermann, 1970.

[BPR03] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics.* Springer-Verlag, 2003.

[Bra00] 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.

[Bre97] G. E. Bredon. *Topology and Geometry*, volume 139 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1997.

[BS83] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comp. Sci.*, 22:317–330, 1983.

[BS88] D. Bayer and M. Stillman. On the complexity of computing syzygies. *J. Symb. Comp.*, 6:135–147, 1988.

[BS92] D. Bayer and M. Stillman. Computation of Hilbert functions. *J. Symb. Comp.*, 14:31–50, 1992.

[BSS89] 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.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universität Innsbruck, 1965.

[Buc85] B. Buchberger. Gröbner bases: an algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Recent trends in multidimensional system theory*, pages 184–232. K. Reidel publishing company, Dordrecht, Holland, 1985.

[Bür00] P. Bürgisser. Cook's versus Valiant's hypothesis. *Theoret. Comp. Sci.*, 235:71–88, 2000.

[CCS99] 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.

[CG97] F. Cucker and D.Yu. Grigoriev. On the power of real Turing machines over binary inputs. *SIAM J. Comp.*, 26:243–254, 1997.

[CGH89] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In *Proc. 6th AAECC*, number 357 in LNCS, pages 131–151. Springer Verlag, 1989.

[CH31] R. Courant and D. Hilbert. *Methoden der mathematischen Physik. I.* Springer-Verlag, Berlin, 1931. Zweite Auflage.

[Cha98] B. Chazelle. A spectral approach to lower bounds with applications to geometric searching. *SIAM Journal on Computing*, 27(2):545–556, 1998.

[Cha00] B. Chazelle. *The discrepancy method.* Cambridge University Press, Cambridge, 2000.

[Che46] S-S. Chern. Characteristic classes of Hermitian manifolds. *Annals of Mathematics (2)*, 47:85–121, 1946.

[CK95] F. Cucker and P. Koiran. Computing over the reals with addition and order: Higher complexity classes. *J. Compl.*, 11:358–376, 1995.

[CKK$^+$95] F. Cucker, M. Karpinski, P. Koiran, T. Lickteig, and K. Werther. On real Turing machines that toss coins. In *Proc. 27th ACM STOC, Las Vegas*, pages 335–342, 1995.

[CLO98] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1998.

[CoC] CoCoATeam. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[Coo71] S.A. Cook. The complexity of theorem proving procedures. In *Proc. 3rd ACM STOC*, pages 151–158, 1971.

[Cra46] H. Cramér. *Mathematical Methods of Statistics*, volume 9 of *Princeton Mathematical Series.* Princeton University Press, 1946.

[Cuc92] F. Cucker. $\mathrm{P_R} \neq \mathrm{NC_R}$. *J. Compl.*, 8:230–238, 1992.

[DE02] 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.

[DFGS91] 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.

[Dim92] A. Dimca. *Singularities and Topology of Hypersurfaces.* Universitext. Springer Verlag, 1992.

[DZ98] A. Dembo and O. Zeitouni. *Large deviations techniques and applications*, volume 38 of *Applications of Mathematics (New York).* Springer-Verlag, New York, 1998.

[Eis95] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

[Fel71] W. Feller. *An introduction to probability theory and its applications*, volume 2. John Wiley & Sons, 1971.

[FH91] W. Fulton and J. Harris. *Representation Theory.* Number 129 in GTM. Springer Verlag, 1991.

[FL81] 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.

[For97] L. Fortnow. Counting complexity. In *Complexity theory retrospective, II*, pages 81–107. Springer, New York, 1997.

[Ful89] W. Fulton. *Algebraic Curves.* Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989.

[Ful93] W. Fulton. *Introduction to Toric Varieties.* Annals of Math. Studies. Princeton University Press, 1993.

[Ful97] W. Fulton. *Young tableaux*, volume 35 of *London Mathematical Society Student Texts.* Cambridge University Press, Cambridge, 1997.

[Ful98] W. Fulton. *Intersection Theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete.* Springer-Verlag, Berlin, 1998.

[Gat86] J. von zur Gathen. Parallel arithmetic computations: a survey. In *Proc. 12th Symp. Math. Found. Comput. Sci., Bratislava*, number 233 in LNCS, pages 93–112, 1986.

[GG03] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2003.

[GH91] M. Giusti and J. Heintz. Algorithmes—disons rapides—pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 169–194. Birkhäuser Boston, Boston, MA, 1991.

[GH93] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une varieté algébrique peut se faire en temps polynomial. In D. Eisenbud and L. Robbiano, editors, *Proc. Cortona Conference on Computational Algebraic Geometry and Commutative Algebra*. Cambridge University Press, 1993.

[Giu84] 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.

[GKP94] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, 1994.

[GM88] M. Goresky and R. MacPherson. *Stratified Morse theory*, volume 14 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1988.

[Goo94] J. B. Goode. Accessible telephone directories. *J. Symbolic Logic*, 59(1):92–105, 1994.

[GP02] G.-M. Greuel and G. Pfister. *A* SINGULAR *introduction to commutative algebra*. Springer-Verlag, Berlin, 2002.

[GPS01] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 2.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2001. `http://www.singular.uni-kl.de`.

[GS] D.R. Grayson and M.E. Stillman. Macaulay 2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[GVL96] G. H. Golub and C. Van Loan. *Matrix Computations*. The John Hopkins University Press, Baltimore, 1996.

[Har77] R. Hartshorne. *Algebraic Geometry.* GTM. Springer Verlag, 1977.

[Har95] J. Harris. *Algebraic Geometry*, volume 133 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

[Hat02] A. Hatcher. *Algebraic Topology.* Cambridge University Press, Cambridge, 2002.

[Hir75] H. Hironaka. Triangulation of algebraic sets. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974)*, volume 29 of *Proceedings of Symposia in Pure Mathematics*, pages 165–185. Amer. Math. Soc., 1975.

[Hir95] F. Hirzebruch. *Topological methods in algebraic geometry.* Classics in Mathematics. Springer-Verlag, Berlin, 1995.

[HS82] J. Heintz and C.P. Schnorr. Testing polynomials which are hard to compute. In *Logic and Algorithmic: An international Symposium held in honor of Ernst Specker*, pages 237–254. Monogr. No. 30 de l'Enseign. Math., 1982.

[Huy86] D.T. Huyn. A superexponential lower bound for Gröbner bases and Church-rosser commutative Thue systems. *Information and Control*, 68:196–206, 1986.

[Iit82] S. Iitaka. *Algebraic geometry*, volume 76 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1982.

[IM83] O.H. Ibarra and S. Moran. Equivalence of straight-line programs. *J. ACM*, 30:217–228, 1983.

[JR04] M.J. Jansen and K.W. Regan. Towards arithmetical lower bounds with unbounded coefficients. 2004. Preprint.

[JSV01] M.R. Jerrum, A. Sinclair, and E. Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with non-negative entries. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pages 712–721 (electronic), New York, 2001. ACM.

[Kal87] E. Kaltofen. Factorization of polynomials given by straight-line programs. In *Adv. Comput. Res.* In Press, 1987.

[KL72] S. L. Kleiman and D. Laksov. Schubert calculus. *Amer. Math. Monthly*, 79:1061–1082, 1972.

[KL74] G. Kempf and D. Laksov. The determinantal formula of Schubert calculus. *Acta Math.*, 132:153–162, 1974.

[Kle74] S. L. Kleiman. The transversality of a general translate. *Compositio Math.*, 28:287–297, 1974.

[Knu98] D.E. Knuth. *The Art of Computer Programming*, volume 2: semi-numerical algorithms. Addison-Wesley, 1998.

[Koi94] P. Koiran. Computing over the reals with addition and order. *Theoret. Comp. Sci.*, 133:35–47, 1994.

[Koi97a] P. Koiran. Elimination of constants from machines over algebraically closed fields. *J. Compl.*, 13:65–82, 1997.

[Koi97b] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th FOCS*, pages 36–45, 1997.

[Koi97c] P. Koiran. A weak version of the Blum, Shub & Smale model. *J. Comp. Syst. Sci.*, 54:177–189, 1997.

[Koi99a] P. Koiran. Elimination of parameters in the polynomial hierarchy. *Theoret. Comp. Sci.*, 215:289–304, 1999.

[Koi99b] P. Koiran. The real dimension problem is $\mathrm{NP}_{\mathbf{R}}$-complete. *J. Compl.*, 15(2):227–238, 1999.

[Koi00a] P. Koiran. Circuits versus trees in algebraic complexity. In *Proc. STACS 2000*, number 1770 in LNCS, pages 35–52. Springer Verlag, 2000.

[Koi00b] P. Koiran. The complexity of local dimensions for constructible sets. *J. Compl.*, 16(1):311–323, 2000.

[Kol88] J. Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.

[KP94] T. Krick and L.M. Pardo. Une approche informatique pour l'approximation diophantienne. *C.R. Acad. Sc. Paris*, 318:407–412, 1994.

[KPS01] T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109(3):521–598, 2001.

[Kri04] T. Krick. Straight-line Programs in Polynomial Equation Solving. In R. Olver F. Cucker, R. DeVore and E. Süli, editors, *Foundations of Computational Mathematics, Minneapolis 2002*, volume 312 of *LMS Lecture Notes*, pages 96–136. Cambridge, 2004.

[Kun74] H.T. Kung. On computing reciprocals of power series. *Num. Math.*, 22:341–348, 1974.

[Lak76] I. Lakatos. *Proofs and refutations: the logic of mathematical discovery.* Cambridge University Press, 1976.

[Lak91] 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.

[Lev73] L.A. Levin. Universal search problems. *Problems of Information Transmission*, 9:265–266, 1973.

[LL91] 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.

[Lok95] S.V. Lokam. Spectral methods for matrix rigidity with applications to size-depth tradeoffs and communication complexity. In *Proc. 36th FOCS*, pages 6–15, 1995.

[LT91] M. Ledoux and M. Talagrand. *Probability in Banach Spaces*, volume 23 of *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge.* Springer Verlag, 1991.

[Mac27] F.S. Macaulay. Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc.*, 26:531–555, 1927.

[Mac95] I. G. Macdonald. *Symmetric functions and Hall polynomials.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1995.

[Man01] L. Manivel. *Symmetric functions, Schubert polynomials and degeneracy loci*, volume 6 of *SMF/AMS Texts and Monographs.* American Mathematical Society, Providence, RI, 2001.

[Mat86] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1986.

[May97] E.W. Mayr. Some Complexity Results for Polynomial Ideals. *J. Compl.*, 13:303–325, 1997.

[Mee00] K. Meer. Counting problems over the reals. *Theoret. Comp. Sci.*, 242:41–58, 2000.

[Mic89] C. Michaux. Une remarque à propos des machines sur $\mathbb{R}$ introduites par Blum, Shub et Smale. *C. R. Acad. Sci. Paris*, 309, Série I:435–437, 1989.

[MM82] 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.

[MM83] F. Mora and H.M. Möller. The computation of the Hilbert function. In *EUROCAL*, number 162 in LNCS, pages 157–167. Springer Verlag, 1983.

[Mor73] J. Morgenstern. Note on a lower bound of the linear complexity of the fast Fourier transform. *J. ACM*, 20:305–306, 1973.

[MS74] J. Milnor and J.D. Stasheff. *Characteristic classes.* Princeton University Press, Princeton, N. J., 1974.

[Mum76] D. Mumford. *Algebraic Geometry I: Complex Projective Varieties.* Springer Verlag, 1976.

[NW95] N. Nisan and A. Wigderson. On the complexity of bilinear forms. In *Proc. of the 27th ACM Symposium on the Theory of Computing*, pages 723–732, 1995.

[Pap94] C.H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[Pie78] R. Piene. Polar classes of singular varieties. *Ann. Sci. École Norm. Sup. (4)*, 11(2):247–276, 1978.

[Poi95] B. Poizat. *Les Petits Cailloux.* Number 3 in Nur Al-Mantiq War-Ma'rifah. Aléas, Lyon, 1995.

[Pud98] P. Pudlák. A note on the use of determinant for proving lower bounds on the size of linear circuits. *ECCC Report*, 42, 1998.

[Raz02] R. Raz. On the complexity of matrix product. In *Proc. 34th STOC*, pages 144–151, 2002. Also available as ECCC Report 12, 2002.

[Raz03] R. Raz. On the complexity of matrix product. *SIAM J. Comput.*, 32(5):1356–1369 (electronic), 2003.

[Ren92] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. part I, II, III. *J. Symb. Comp.*, 13(3):255–352, 1992.

[Rud04] S. Rudich. Complexity theory: from Gödel to Feynman. In *Computational complexity theory*, volume 10 of *IAS/Park City Math. Ser.*, pages 5–87. Amer. Math. Soc., Providence, RI, 2004.

[Sch79] H. Schubert. *Kalkül der abzählenden Geometrie.* B. G. Teubner, Leipzig, 1879.

[Sch80] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27:701–717, 1980.

[Sev02] F. Severi. Sulle intersezioni delle varieta algebriche e sopra i loro caratteri e singolarita proiettive. *Mem. Accad. Sci. Torino*, 52(2):61–118, 1902.

[Sha74] I.R. Shafarevich. *Basic Algebraic Geometry.* Springer Verlag, 1974.

[Sie72] M. Sieveking. An algorithm for division of power series. *Computing*, 10:153–156, 1972.

[Str73a] V. Strassen. Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten. *Num. Math.*, 20:238–251, 1973.

[Str73b] V. Strassen. Vermeidung von Divisionen. *Crelles J. Reine Angew. Math.*, 264:184–202, 1973.

[Stu02] B. Sturmfels. *Solving systems of polynomial equations*, volume 97 of *CBMS Regional Conference Series in Mathematics.* Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2002.

[Tra96] C. Traverso. Hilbert functions and the Buchberger algorithm. *J. Symbolic Comput.*, 22(4):355–376, 1996.

[Val76] L.G. Valiant. Graph theoretic properties in computational complexity. *J. Comp. Syst. Sci.*, 13:278–285, 1976.

[Val77] L.G. Valiant. Graph theoretic arguments in low-level complexity. Number 53 in LNCS, pages 162–176. Springer Verlag, 1977.

[Val79a] L.G. Valiant. The complexity of computing the permanent. *Theoret. Comp. Sci.*, 8:189–201, 1979.

[Val79b] L.G. Valiant. The complexity of enumeration and reliability problems. *SIAM J. Comp.*, 8:410–421, 1979.

[Vas98] W.V. Vasconcelos. *Computational methods in commutative algebra and algebraic geometry*, volume 2 of *Algorithms and Computation in Mathematics.* Springer-Verlag, Berlin, 1998.

[vL99] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1999.

[Wal00] U. Walther. Algorithmic computation of de Rham cohomology of complements of complex affine varieties. *J. Symbolic Comput.*, 29(4-5):795–839, 2000.

[Wal02] U. Walther. D-modules and cohomology of varieties. In *Computations in algebraic geometry with Macaulay 2*, volume 8 of *Algorithms Comput. Math.*, pages 281–323. Springer, Berlin, 2002.

[Yao92] A.C. Yao. Algebraic decision trees and Euler characteristic. In *Proc. 33rd FOCS*, 1992.