On the Complexity of Counting Components of Algebraic Varieties ⋆⋆

Peter Bürgisser and Peter Scheiblechner ⋆

Department of Mathematics, University of Paderborn, D-33095 Paderborn, Germany

Abstract

We give a uniform method for the two problems of counting the connected and irreducible components of complex algebraic varieties. Our algorithms are purely algebraic, i.e., they use only the field structure of $\mathbb{C}$. They work in parallel polynomial time, i.e., they can be implemented by algebraic circuits of polynomial depth. The design of our algorithms relies on the concept of algebraic differential forms. A further important building block is an algorithm of Szántó computing a variant of characteristic sets. Furthermore, we use these methods to obtain a parallel polynomial time algorithm for computing the Hilbert polynomial of a projective variety which is arithmetically Cohen-Macaulay.

Key words: characteristic sets, complexity, connected components, differential forms, irreducible components

1. Introduction

1.1. Counting Connected Components

The algorithmic problem of getting connectivity information about semialgebraic sets is well-studied, see Basu et al. (2003) and the numerous citations given there. In particular, work of Canny (1988) yields algorithms that count the connected components of a semialgebraic set given by rational polynomials in polynomial space (and thus in single exponential time). By separating real and imaginary parts these methods can be applied to complex algebraic varieties as well. However, these algorithms use the ordering of the

⋆ Partially supported by DFG grants BU 1371 and 1371/2-1.

⋆⋆This paper contains results of the PhD thesis of the second author (Scheiblechner, 2007a). An extended abstract of this work appeared in (Bürgisser and Scheiblechner, 2007).

Email address: {pbuerg|pscheib}@math.uni-paderborn.de (Peter Bürgisser and Peter Scheiblechner).

URL: http://www-math.uni-paderborn.de/agpb (Peter Bürgisser and Peter Scheiblechner).

real field in an essential way, in particular sign tests are allowed. Thus it remained an open problem whether one can efficiently count the connected components of a complex algebraic variety by algebraic methods only.

A complex variety is connected in the Euclidean topology iff it is connected in the Zariski topology. Thus it makes sense to study the problem $\#\mathrm{CC}_k$ of counting the connected components of a variety $V \subseteq \mathbb{A}^n := \mathbb{A}^n(\overline{k})$ given over an arbitrary field k of characteristic zero, where $\overline{k}$ denotes an algebraic closure of k.

We present an algorithm for counting the connected components in parallel polynomial time over k, i.e., $\#\mathrm{CC}_k \in \mathrm{FPAR}_k$ (Theorem 3.1, cf. Bürgisser and Cucker (2004) and §2.3 for notation). The idea of our method is to characterise the number of connected components of a variety V as the dimension of the zeroth *algebraic de Rham cohomology* $H^0(V)$, which is the space of locally constant regular functions on V. The effective Nullstellensatz (Kollár, 1988) implies that $H^0(V)$ has a basis induced by polynomials of single exponential degree.

A fundamental computational tool in our algorithm is the concept of *characteristic sets*, which goes back to Ritt (1950) and was used by Wu (1986) for automated theorem proving. Their computational complexity was studied by Gallo and Mishra (1991). Subsequently, algorithms computing variants of this concept were studied by Kalkbrener (1993, 1994, 1998), Lazard (1991), and Wang (1992). See Aubry et al. (1999) for a comparison of the different notions of characteristic sets. Szántó (1997) has further refined the methods of Kalkbrener to obtain a provably efficient algorithm. It decomposes the radical of an ideal in parallel polynomial time into several unmixed radicals described by ascending sets, which we will call *squarefree regular chains* in compliance with Aubry et al. (1999) and Boulier et al. (2006). This result implies that one can describe the "truncated ideal" $I(V) \cap k[X]_{\leq D}$ of V, which consists of the polynomials of degree bounded by D vanishing on V, by a linear system of equations of single exponential size, if D is single exponential. In this way, it is possible to describe $H^0(V)$ by such systems and hence to compute its dimension efficiently.

1.2. Counting Irreducible Components

The problem of decomposing an algebraic variety into irreducible components has been attacked in the last decades with numerous methods. There are algorithms based on characteristic sets (Wu, 1986; Lazard, 1991; Kalkbrener, 1994), however, their complexity has not been analysed. Other methods use Gröbner bases (Gianni et al., 1988; Eisenbud et al., 1992), but according to Mayr (1997), computing those is exponential space-complete. The first single exponential time algorithms (in the bit model) for computing both the irreducible and absolutely irreducible components are due to (Chistov, 1984; Grigoriev, 1984). Giusti and Heintz (1991) succeeded in giving efficient parallel algorithms, but only for the equidimensional decomposition due to the lack of efficient parallel factorisation procedures.

Let $\#\mathrm{IC}_k$ denote the problem of counting the absolutely irreducible components of a variety $V \subseteq \mathbb{A}^n(\overline{k})$ given over an arbitrary field k of characteristic zero. We describe a new approach for $\#\mathrm{IC}_k$ analogous to our algorithm for $\#\mathrm{CC}_k$ showing that $\#\mathrm{IC}_k \in \mathrm{FPAR}_{\mathbb{C}}$ (Theorem 4.1). The key idea is to replace regular by rational functions on V. In particular, we use that the number of irreducible components of V is the dimension of the space of locally constant rational functions on V.

1.3. Hilbert Polynomial

As a by-product of our method for counting the connected and irreducible components we show how to obtain a parallel polynomial time algorithm for computing the Hilbert polynomial of a projective variety which is arithmetically Cohen-Macaulay (Theorem 6.6).

Algorithms for computing the Hilbert polynomial of a projective variety as given in Mora and Möller (1983), Bigatti et al. (1991), and Bayer and Stillman (1992) are based on Gröbner bases and hence show the same worst-case behaviour as the algorithms computing irreducible components mentioned above. For the restricted problem of computing the Hilbert polynomial of smooth equidimensional complex varieties, Bürgisser and Lotz (2007) have given a parallel polynomial time algorithm. In fact, they have shown the stronger statement that this problem is reducible in polynomial time to counting the complex solutions of systems of polynomial equations. The general problem of computing the Hilbert polynomial of a complex projective variety still lacks an efficient solution.

The idea of our algorithm is that with the above method we can efficiently evaluate the Hilbert function of a projective variety at not too large arguments. Hence we can compute the Hilbert polynomial by interpolation. The critical complexity parameter for this algorithm is the *index of regularity* (Stückrad and Vogel, 1986; Vasconcelos, 1998), which is closely related to the Castelnuovo-Mumford regularity (Bayer and Mumford, 1993). By a standard argument we prove a polynomial bound for the index of regularity of a projective arithmetically Cohen-Macaulay variety. Consequently one can compute the Hilbert polynomial in this case in parallel polynomial time.

1.4. Outline

This paper is organised as follows. In Section 2 we fix the notation and provide the necessary prerequisites. In Sections 3 and 4 we describe our algorithms for counting the connected and irreducible components of a variety, respectively. After transferring our results to the Turing model in Section 5, the algorithm computing the Hilbert polynomial is described in Section 6.

2. Preliminaries

2.1. Algebraic Geometry

As general references for the basic facts about algebraic geometry we refer to Mumford (1976), Shafarevich (1977), Kunz (1979), and Harris (1992).

2.1.1. Basic Terminology and Notation

Throughout this paper k denotes a field of characteristic zero, and $K := \overline{k}$ an algebraic closure of k. We denote by $k[X] := k[X_1, \ldots, X_n]$ the polynomial ring and by $\mathbb{A}^n := \mathbb{A}^n(K)$ the affine space over K. An *affine variety* V (defined over k) is defined as the zero set

$$V = \mathcal{Z}(f_1 \ldots, f_r) := \{x \in K^n \mid f_1(x) = \cdots = f_r(x) = 0\} \subseteq \mathbb{A}^n$$

of the polynomials $f_1 \ldots, f_r \in k[X]$. In the projective case we set $k[X] := k[X_0, \ldots, X_n]$ and denote by $\mathbb{P}^n := \mathbb{P}^n(K)$ the projective space over K. For homogeneous polynomials $f_1 \ldots, f_r \in k[X]$ we denote their common zero set in the projective space $\mathbb{P}^n$ also

with $\mathcal{Z}(f_1 \ldots, f_r)$ and call it a *projective variety*. The *(vanishing) ideal* $I(V)$ of an affine variety V is defined as $I(V) := \{f \in k[X] \,|\, \forall x \in V\, f(x) = 0\}$. The strong Hilbert Nullstellensatz states that the ideal $I(V)$ of $V = \mathcal{Z}(f_1, \ldots, f_r)$ is the radical of $(f_1, \ldots, f_r)$. For a projective variety V the ideal $I(V)$ is generated by the homogeneous polynomials vanishing on V. The *(homogeneous) coordinate ring* of V is defined as $k[V] := k[X]/I(V)$. The elements of $k[V]$ can be interpreted as functions $V \to K$ called *regular* on V.

The varieties (defined over K) form the closed sets of the *Zariski topology* on $\mathbb{A}^n$ or $\mathbb{P}^n$, respectively. A variety V is called *irreducible* iff it is not the union of two proper subvarieties. Each variety V admits an (up to order) unique irredundant decomposition $V = V_1 \cup \cdots \cup V_t$, i.e., $V_i \neq \emptyset$ and $V_i \nsubseteq V_j$ for all $1 \leq i \neq j \leq t$, into irreducible varieties V_i. The V_i are called the *irreducible components* of V. On $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ there exists a second natural topology induced by the Euclidean norm. It induces a quotient topology on the projective space $\mathbb{P}^n$ with respect to the natural projection $\pi\colon \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n$. We call each of these topologies the *Euclidean topology*. The continuity of the polynomials implies that the Euclidean topology is finer than the Zariski topology, i.e., a Zariski open subset of $\mathbb{A}^n$ or $\mathbb{P}^n$ is also Euclidean open. It follows that a Euclidean connected subset is also Zariski connected. The converse does not hold in general, but it is true for varieties. Moreover, the Euclidean and the Zariski connected components of a variety coincide. This is an easy consequence of the result that an irreducible variety is Euclidean connected, see (Shafarevich, 1977, VII, §2.2) or (Mumford, 1976, Corollary (4.16)).

2.1.2. Dimension, Smoothness, and Degree

If V is a nonempty algebraic variety, we define its *dimension* $\dim V$ to be its *Krull dimension*, i.e., $\dim V$ is the length ℓ of a maximal ascending chain

$$\emptyset \neq V_0 \subset V_1 \subset \cdots \subset V_\ell \subseteq V$$

of irreducible subvarieties V_i. The dimension of the empty set is set to -1.

Note that the dimension of V is the maximal dimension of its irreducible components. A variety all of whose irreducible components have the same dimension m is called *equidimensional* or more precisely *m-equidimensional*. For a point $x \in \mathbb{A}^n$ ($\mathbb{P}^n$) we define the *local dimension* $\dim_x V$ to be the dimension of the union of all irreducible components of V containing x.

For a polynomial $f \in k[X]$ its *differential* at $x \in \mathbb{A}^n$ is the linear function $d_x f\colon K^n \to K$ defined by $d_x f(v) := \sum_i \frac{\partial f}{\partial X_i}(x) v_i$. The *(Zariski) tangent space* of the affine variety V at $x \in V$ is defined as the vector subspace

$$T_x V := \{v \in K^n \,|\, \forall f \in I(V)\; d_x f(v) = 0\} \subseteq K^n.$$

Having generators $f_1, \ldots, f_r$ of the ideal $I(V)$ at hand, one can also write $T_x V = \mathcal{Z}(d_x f_1, \ldots, d_x f_r)$.

In general $\dim T_x V \geq \dim_x V$ holds. We say that $x \in V$ is a *smooth* or *regular* point of V or that V is *smooth* in x iff $\dim T_x V = \dim_x V$. Otherwise x is said to be a *singular* point of V. We denote the set of regular (singular) points of V by $\mathrm{Reg}\,(V)$ ($\mathrm{Sing}\,(V)$). The set $\mathrm{Sing}\,(V)$ is a subvariety of V of lower dimension, thus $\mathrm{Reg}\,(V)$ is dense in V.

The *degree* $\deg V$ of an irreducible affine variety V of dimension m is defined as the maximal cardinality of $V \cap A$ over all affine subspaces $A \subseteq \mathbb{A}^n$ of dimension $n - m$ (Mumford, 1976, §5A), (Harris, 1992, Lecture 18). This maximum is obtained for a generic affine subspace A of complementary dimension. We define the (cumulative) degree $\deg V$ of a reducible variety V to be the sum of the degrees of *all* irreducible components of V.

2.1.3. Important Bounds

The following is a well-known bound on the degree of a variety in terms of the degrees of its defining polynomials, which follows from Bézouts Theorem (Mumford, 1976). Let $V = \mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$ ($\mathbb{P}^n$) be an affine or projective variety defined by the (homogeneous) polynomials $f_1, \ldots, f_r$ of degree at most d. Then $\deg V \leq d^n$. An obvious but important observation is that the number of irreducible (connected) components of V is also bounded by d^n.

On the other hand, one can bound the degree of defining polynomials in terms of the degree of the variety. The following proposition is easily deduced from (Heintz, 1983, Proposition 3), where this statement is proved for irreducible varieties.

Proposition 2.1. *For each affine (projective) variety V there exist (homogeneous) polynomials $f_1, \ldots, f_r \in k[X]$ with $\deg f_i \leq \deg V$ and $V = \mathcal{Z}(f_1, \ldots, f_r)$.*

Another class of bounds which are extremely important for computational algebraic geometry are *effective* versions of Hilbert's Nullstellensatz. The following version is due to Kollár (1988) (see also Brownawell (1987); Fitchas and Galligo (1990)).

Theorem 2.2. *Let $f_1, \ldots, f_r \in k[X]$ be polynomials in $n > 1$ indeterminates with $\deg f_i \leq d$, where $d \geq 3$. If $\mathcal{Z}(f_1, \ldots, f_r) = \emptyset$, then there exist $g_1, \ldots, g_r \in k[X]$ with $\deg(g_i f_i) \leq d^n$ and $1 = g_1 f_1 + \cdots + g_r f_r$.*

The *homogeneous* version of Hilbert's Nullstellensatz states that the projective zero set of a homogeneous ideal $I \subseteq k[X_0, \ldots, X_n]$ is empty iff $\mathfrak{m}^D \subseteq I$ for some sufficiently large D, where $\mathfrak{m} := (X_0, \ldots, X_n)$. We will also use the following effective homogeneous Nullstellensatz proved in (Lazard, 1981, Théorème 3.3).

Theorem 2.3. *Let $f_1, \ldots, f_r \in k[X_0, \ldots, X_n]$ be homogeneous polynomials with $d_1 \geq d_2 \geq \cdots \geq d_r$, where $d_i := \deg f_i$. If $\mathcal{Z}(f_1, \ldots, f_r) = \emptyset$, then $\mathfrak{m}^D \subseteq (f_1, \ldots, f_r)$ with $D := \sum_{i=1}^{n+1} d_i - n$.*

Note that in the case $r \leq n$ the projective zero set is never empty.

2.2. Differential Forms

We refer to Eisenbud (1995) for further details about derivations and differential forms. Let R be a ring, S an R-algebra, and M an S-module. An R-linear map $D\colon S \to M$ is called a *derivation* (or *R-derivation*) iff it satisfies Leibnitz' rule $D(fg) = gD(f) + fD(g)$ for all $f, g \in S$. In the important case $M = S$ we call D simply a derivation of S. We denote by $\Omega_{S/R}$ the *module of Kähler differentials* (or *differential forms*) of S over R. It is defined as the S-module generated by the symbols $\mathrm{d}f$ for all $f \in S$ subject to the relations given by Leibnitz' rule and R-linearity. We thus have the R-derivation $\mathrm{d}\colon S \to \Omega_{S/R},\ f \mapsto \mathrm{d}f$, which is called the *universal derivation* of S.

Clearly the partial derivations $\frac{\partial}{\partial X_i}\colon k[X] \to k[X]$ for $1 \leq i \leq n$ are k-linear derivations. In this case $\Omega_{k[X]/k}$ is the free $k[X]$-module generated by the $\mathrm{d}X_i$, and the universal derivation is given by $\mathrm{d}f = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i} \mathrm{d}X_i$ for all $f \in k[X]$. The partial derivations $\frac{\partial}{\partial X_i}$ can be uniquely extended to derivations of $k(X)$ by the usual quotient rule. Then analogous statements hold for $\Omega_{k(X)/k}$.

The *ring of rational functions* on an affine variety V is defined as the full quotient ring of the coordinate ring $K[V]$, i.e., $R(V)$ is the localisation of $K[V]$ with respect to the multiplicatively closed subset of non-zerodivisors. Each $f \in R(V)$ has a unique maximal open set of definition $D(f) \subseteq V$. The function $f \in R(V)$ is called *locally constant* iff for each point $x \in D(f)$ there exists an open neighbourhood $U \subseteq D(f)$ of x such that f is constant on U. A function f is locally constant if and only if $\mathrm{d}f = 0$ (for a detailed proof of this see (Scheiblechner, 2007a)).

2.3. Models of Computation and Complexity

Our model of computation is that of algebraic circuits, cf. von zur Gathen (1986); Bürgisser and Cucker (2004). We set $k^\infty := \bigsqcup_{n\in\mathbb{N}} k^n$ and call $|x| := n$ the *size* of the input $x \in k^n$. Recall that the *size* of an algebraic circuit $\mathcal{C}$ is the number of nodes of $\mathcal{C}$, and its *depth* is the maximal length of a path from an input to an output node. We say that a function $f\colon k^\infty \to k^\infty$ can be computed *in parallel time* $d(n)$ *and sequential time* $s(n)$ iff there exists a polynomial-time uniform family of algebraic circuits $(\mathcal{C}_n)_{n\in\mathbb{N}}$ over k of size $s(n)$ and depth $d(n)$ such that $\mathcal{C}_n$ computes $f|k^n$. The function f is called computable *in parallel polynomial (polylogarithmic) time* iff f can be computed in parallel time $n^{\mathcal{O}(1)}$ $((\log n)^{\mathcal{O}(1)})$ and sequential time $2^{n^{\mathcal{O}(1)}}$ $(n^{\mathcal{O}(1)})$. The set of functions $f\colon k^\infty \to k^\infty$ with $|f(x)| = |x|^{\mathcal{O}(1)}$ which are computable in parallel polynomial (polylogarithmic) time is denoted with FPAR_k (FNC_k). As usual, for the class FNC_k, we strengthen this definition by requiring logspace-uniformity. One denotes with FNC^i_k the set of functions computable in parallel time $\mathcal{O}(\log^i n)$ and polynomial sequential time.

In the case $k = \mathbb{F}_2$ algebraic circuits are equivalent to Boolean circuits and we retrieve the versions of the above complexity classes in the bit model, which we write in sans serif, e.g. FNC. The class $\mathrm{FPAR}_{\mathbb{F}_2}$ is denoted by $\mathsf{FPSPACE}$, since it coincides with the class of all functions computable by a polynomial-space Turing machine (Borodin, 1977).

2.4. Efficient Parallel Linear Algebra

We use differential forms to reduce a number of counting problems of algebraic geometry to computing the dimension of the solution space of linear systems of equations. Our complexity results follow from efficient parallel algorithms for the latter problem. The dimension of the solution space of a linear system can be obtained from the rank of its coefficient matrix. Mulmuley (1987) has reduced this problem to computing the characteristic polynomial of a matrix, which can be done in FNC^2_k using the algorithm of Berkowitz (1984). Via Cramers rule it is also possible to reduce the problem of solving a nonsingular linear system to the computation of the characteristic polynomial. It is shown in Gathen (1986) that one can also reduce most linear algebra problems to computing the characteristic polynomial. Hence this seems to be the most fundamental problem of linear algebra.

Later in §3.4 we will also need to invert a regular matrix $A \in k[X]^{m\times m}$ with entries of degree at most d. We do that using the following well-known method. Let $p(T) = p_m T^m + p_{m-1}T^{m-1} + \cdots + p_0 \in k[X,T]$ be the characteristic polynomial of A. Then $p_0 = \det A \neq 0$. By the Cayley-Hamilton Theorem we have $p(A) = 0$, hence

$$A^{-1} = -\frac{1}{\det A}(p_m A^{m-1} + p_{m-1}A^{m-2} + \cdots + p_1 E), \tag{2.1}$$

where E denotes the identity matrix. A straightforward analysis of Berkowitz' algorithm for matrices with polynomial entries shows that we can compute $(\det A)A^{-1}$ in parallel time $\mathcal{O}(n\log(md)\log m)$ and sequential time $(md)^{\mathcal{O}(n)}$, counting operations in k.

In our summary about this variant of characteristic sets we follow mainly the presentation of Szántó (1997, 1999). One difference is that we use the naming conventions introduced in Aubry et al. (1999) and Boulier et al. (2006), which seem more appropriate. A second difference is that we consider the saturated ideal $\mathrm{Sat}\,(G)$ as the fundamental object attached to a triangular set G, since it has nicer mathematical properties than the set $\mathrm{Red}\,(G)$ of polynomials which are pseudo divisible by G (cf. Example 2.5).

2.5.1. Definitions and Basic Properties

We introduce an ordering on the variables $X_1 < \cdots < X_n$ of the polynomial ring $k[X] = k[X_1, \ldots, X_n]$. For a non-constant polynomial $f \in k[X]$ we define its *class* by $\mathrm{class}\,(f) := \min\{X_i \,|\, f \in k[X_1, \ldots, X_i]\}$. The *leading coefficient* $\mathrm{lc}\,(f)$ of f is by convention its leading coefficient with respect to $\mathrm{class}\,(f)$. Thus, if $\mathrm{class}\,(f) = X_i$, then $f \in k[X_1, \ldots, X_i] \setminus k[X_1, \ldots, X_{i-1}]$ and $\mathrm{lc}\,(f) \in k[X_1, \ldots, X_{i-1}]$.

Definition 2.4. A finite set of polynomials $G = \{g_1, \ldots, g_t\} \subseteq k[X]$ is called a *triangular set* iff $\mathrm{class}\, g_i < \mathrm{class}\, g_{i+1}$ for all $1 \leq i < t$.

The well-known procedure of *pseudo division* is a generalisation of division with remainder from univariate to multivariate polynomials. For polynomials $f, g \in k[X]$ with $\mathrm{class}\,(g) = X_i$ there exist polynomials $q, r \in k[X]$ and an integer $\alpha \in \mathbb{N}$ with

$$\mathrm{lc}\,(g)^\alpha f = qg + r, \tag{2.2}$$

where $\deg_{X_i} r < \deg_{X_i} g$ and $0 \leq \alpha \leq \max\{\deg_{X_i} f - \deg_{X_i} g + 1, 0\}$. To make q and r unique one usually requires α to be minimal, but we note that any other sufficiently large choice of α is also possible. For instance, if we require $\alpha = \deg_{X_i} f - \deg_{X_i} g + 1$, then q and r are as well unique. For minimal α the *pseudo quotient* of f by g is denoted with $\mathrm{pquo}\,(f, g) := q$, and the *pseudo remainder* by $\mathrm{prem}\,(f, g) := r$.

Now we generalise the notion of pseudo remainder to triangular sets. Consider a triangular set $G = \{g_1, \ldots, g_t\} \subseteq k[X]$ and a polynomial $f \in k[X]$. The *pseudo remainder sequence* $f_t, \ldots, f_0$ of f is defined by $f_t = f$, $f_{i-1} = \mathrm{prem}\,(f_i, g_i)$ for $1 \leq i \leq t$. We denote by $\mathrm{prem}\,(f, G) := f_0$ the *pseudo remainder* of f by G. It follows from the defining equations that there exist polynomials $q_1, \ldots, q_t$ and $\alpha_1, \ldots, \alpha_t \in \mathbb{N}$ with

$$\mathrm{lc}\,(g_t)^{\alpha_t} \cdots \mathrm{lc}\,(g_1)^{\alpha_1} f = \sum_{i=1}^{t} q_i g_i + f_0. \tag{2.3}$$

We say that f is *reduced* modulo G iff $f = \mathrm{prem}\,(f, G)$. The polynomial f is reduced modulo G iff $\deg_{X_i} f < \deg_{X_i} g_j$ for all j where $X_i = \mathrm{class}\,(g_j)$. We say that f is *pseudo divisible* by G iff $\mathrm{prem}\,(f, G) = 0$. We denote the set of polynomials which are pseudo divisible by G by

$$\mathrm{Red}\,(G) := \{f \in k[X_1, \ldots, X_n] \,|\, \mathrm{prem}\,(f, G) = 0\}.$$

The set $\mathrm{Red}\,(G)$ is in general not an ideal as the following example shows.

Example 2.5. Let $G := \{g_1, g_2\} \subseteq k[X_1, X_2]$ with $g_1 := X_1(X_1 - 1)$ and $g_2 := X_1(X_2 - 1)$. Then G is a triangular set. Now consider $f_1 := X_2 - X_1$ and $f_2 := -X_2 + 1$. Then one easily checks that $\mathrm{prem}\,(f_1, g_2) = -g_1$, hence $\mathrm{prem}\,(f_1, G) = 0$. Furthermore, $X_1 f_2 =$

$-g_2$, thus $\operatorname{prem}(f_2, G) = 0$. But $f_1 + f_2 = -X_1 + 1$ is not pseudo divisible by G, since it is reduced modulo G.

Following Aubry et al. (1999) we assign to G the *saturated ideal*

$$\operatorname{Sat}(G) := (G) : \Gamma^\infty = \{f \in k[X] \mid \exists N \in \mathbb{N}\ f\Gamma^N \in (G)\}, \tag{2.4}$$

where $\Gamma := \prod_i \operatorname{lc}(g_i)$. It is clear that Γ is no zerodivisor on $k[X]/\operatorname{Sat}(G)$. Furthermore, equation (2.3) implies $\operatorname{Red}(G) \subseteq \operatorname{Sat}(G)$. Later we will impose conditions on G that imply equality.

Before defining the fundamental concept of squarefree regular chains, we need to introduce some more notation. For more information about associated primes and primary decomposition see (Eisenbud, 1995, §3). For an ideal $I \subseteq k[X]$ we denote by $\operatorname{Ass}(I)$ the set of associated primes of I, i.e., if $I = Q_1 \cap \cdots \cap Q_s$ is an irredundant primary decomposition of I and Q_i is P_i-primary, then $\operatorname{Ass}(I) = \{P_1, \ldots, P_s\}$. Now set $R := k[X_1, \ldots, X_{n-1}]$. For a prime ideal $P \subseteq R$ we denote by $K(P)$ the quotient field of the integral domain R/P. We have a natural map $R[X_n] \twoheadrightarrow (R/P)[X_n] \hookrightarrow K(P)[X_n]$, $f \mapsto f^P$.

Definition 2.6. Let $G = \{g_1, \ldots, g_t\}$ be a triangular set, and set $G_i := \{g_1, \ldots, g_i\}$ for $0 \le i \le t$.

(1) Then G is called a *regular chain* iff for all $0 \le i < t$ and each $P \in \operatorname{Ass}(\operatorname{Sat}(G_i))$ we have $\operatorname{lc}(g_{i+1}) \notin P$.
(2) The regular chain G is called *squarefree* iff for all $0 \le i < t$ and each $P \in \operatorname{Ass}(\operatorname{Sat}(G_i))$ the polynomial $g_{i+1}^{P_i}$ is squarefree in $K(P_i)[X_j]$, where $X_j = \operatorname{class}(g_{i+1})$ and $P_i := P \cap k[X_1, \ldots, X_{j-1}]$.

The first part of following proposition was proved in Boulier et al. (2006), the second part in (Aubry et al., 1999, Theorem 6.1). The third part was essentially proved already in Kalkbrener (1998), see also Szántó (1999); Aubry et al. (1999); Boulier et al. (2006).

Proposition 2.7. *Let $G = \{g_1, \ldots, g_t\}$ be a triangular set.*
(1) The ideal $\operatorname{Sat}(G)$ is unmixed, i.e., each associated prime P of $\operatorname{Sat}(G)$ has the same codimension t.
(2) If G is a regular chain, then $\operatorname{Sat}(G) = \operatorname{Red}(G)$.
(3) If G is a squarefree regular chain, then $\operatorname{Sat}(G)$ is a proper radical ideal in $k[X]$.

2.5.2. Decomposition of Radicals

It is a major open problem in computational algebraic geometry to compute generators of the radical of an ideal in single exponential sequential time. It is not even known whether generators of single exponential degree exist. In this light the following result of Szántó (1997) is remarkable.

Theorem 2.8. *Let k be a field of characteristic zero, and the ideal $I \subseteq k[X]$ be given by generators $f_1, \ldots, f_r$ of degree at most d. Then there exist squarefree regular chains $G_1, \ldots, G_s$ with saturated ideals $I_i = \operatorname{Sat}(G_i)$ such that*

$$\sqrt{I} = I_1 \cap \cdots \cap I_s. \tag{2.5}$$

Furthermore, the degree of the polynomials in G_i and s are bounded by $d^{\mathcal{O}(n^2)}$. Finally, the G_i can be computed in parallel (sequential) time $(n \log d)^{\mathcal{O}(1)}$ $(d^{n^{\mathcal{O}(1)}})$.

Remark 2.9. (1) We note that unlike the claim in Szántó (1997) the above decomposition is in general *not* irredundant, i.e., setting $V_i := \mathcal{Z}(I_i)$ there may be some irreducible component C of V_i with $C \subseteq V_j$ where $j \neq i$. We point out that in this case C is either also an irreducible component of V_j or it is *embedded* in V_j, i.e., C is contained in some higher dimensional component of V_j.

(2) It is so far not known whether there exist generators of single exponential degree for the above ideals I_i. In fact, it is easy to see that if one could prove the existence of such generators, they could also be computed in parallel polynomial time.

3. Connected Components

The main result of this section is concerned with the following problem:

$\#\mathrm{CC}_k$ (*Counting connected components*) Given polynomials $f_1, \ldots, f_r \in k[X]$, compute the number of connected components of $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$.

A standard argument (cf. Bürgisser and Cucker (2004, Remark 6.3) and Koiran (1997, §1.2)) shows that the problem $\#\mathrm{CC}_k$ for the different data structures dense, sparse, and straight-line program (slp) encoding are polynomial time equivalent. To fix ideas we therefore think of the dense encoding. The following is our first main result.

Theorem 3.1. *We have $\#\mathrm{CC}_k \in \mathrm{FPAR}_k$ for every field k of characteristic zero.*

Before we prove Theorem 3.1, we complement it by lower bounds for the problem. For the bit model it is shown in Scheiblechner (2007b) that $\#\mathrm{CC}_{\mathbb{Q}}$ is FPSPACE-hard. For the algebraic model there is a gap between the upper and the best known lower bound we prove now. For the definition of $\#\mathrm{P}_{\mathbb{C}}$ and related notations see Bürgisser and Cucker (2006).

Proposition 3.2. *The problem $\#\mathrm{CC}_{\mathbb{C}}$ is $\#\mathrm{P}_{\mathbb{C}}$-hard with respect to Turing reductions.*

Proof. Since the points of a zerodimensional variety V coincide with its connected components, one can solve the $\#\mathrm{P}_{\mathbb{C}}$-complete problem $\#\mathrm{HN}_{\mathbb{C}}$ in this case by one oracle call to $\#\mathrm{CC}_{\mathbb{C}}$. According to Koiran (1997) to decide whether V has dimension zero is Turing reducible to $\mathrm{HN}_{\mathbb{C}}$, hence to $\#\mathrm{CC}_{\mathbb{C}}$. □

3.1. The Zeroth de Rham Cohomology

It is known from topology that the connected components of a topological space can be characterised by locally constant continuous functions. We follow this idea and show that in the algebraic setting these functions can be realised by polynomials of moderate degree.

3.1.1. Definition and Main Theorem

Let $V \subseteq \mathbb{A}^n$ be a variety. We define the zeroth *algebraic de Rham cohomology* of V as

$$H^0(V) := \{f \in K[V] \mid \mathrm{d}f = 0\},$$

where $K[V] = K[X]/I(V)$ denotes the coordinate ring of V over K. This is the K-vector space of locally constant regular functions on V. Our algorithm relies on the following property of $H^0(V)$.

Theorem 3.3. *Each affine variety $V \subseteq \mathbb{A}^n$ has $\dim H^0(V)$ connected components. If $n \geq 2$ and V is the zero set of polynomials of degree at most $d \geq 2$, then $H^0(V)$ has a basis given by polynomials of degree bounded by d^{n^2+n}.*

The following section is devoted to the proof of this theorem.

3.1.2. Connected Components by Idempotents

Let us recall some notations and facts about idempotents. Let S be a commutative ring. An element $e \in S$ is called an *idempotent* iff $e^2 = e$. It is a *nontrivial* idempotent iff in addition $e \notin \{0, 1\}$. Two idempotents $e, f \in S$ are said to be *orthogonal* iff $ef = 0$. A set of nontrivial idempotents $e_1, \ldots, e_s \in S$ is called *complete* iff $e_1 + \cdots + e_s = 1$. The ring S has a complete set of pairwise orthogonal idempotents $e_1, \ldots, e_s$ if and only if S is isomorphic to the direct product of the rings $S_i = Se_i$, $1 \leq i \leq s$ (Eisenbud, 1995, §0.1). In this case e_i serves as a unit for S_i. A complete set of orthogonal idempotents $e_1, \ldots, e_s$ is called *maximal* iff none of the e_i can be written as a sum of two nontrivial orthogonal idempotents. A maximal complete set of orthogonal idempotents is unique.

The following lemma relates idempotents with the zeroth de Rham cohomology.

Lemma 3.4. *Each maximal complete set of orthogonal idempotents $e_1, \ldots, e_s$ of $K[V]$ is a basis of $H^0(V)$.*

Proof. In greatest generality, idempotents have vanishing differential: For an idempotent e in a commutative ring S we have

$$e^2 = e \quad \overset{\mathrm{d}}{\Rightarrow} \quad 2e\mathrm{d}e \overset{(*)}{=} \mathrm{d}e \quad \overset{\cdot e}{\Rightarrow} \quad 2e\mathrm{d}e = e\mathrm{d}e \quad \overset{-e\mathrm{d}e}{\Rightarrow} \quad e\mathrm{d}e = 0 \quad \overset{(*)}{\Rightarrow} \quad \mathrm{d}e = 0.$$

Hence $e_i \in H^0(V)$. Furthermore, the e_i are linearly independent: Let $\sum_i \lambda_i e_i = 0$ with some $\lambda_i \in K$. Then $0 = e_j \sum_i \lambda_i e_i = \lambda_j e_j$, which shows $\lambda_j = 0$ for all j. Finally, the e_i generate $H^0(V)$, since every locally constant function f can be written as $f = \sum_i \lambda_i e_i$ with $\lambda_i = f(x)$ for all $x \in V_i$, where $V_i := \mathcal{Z}(e_i - 1)$. Indeed, one easily checks that the V_i are the connected components of V. Thus $e_1, \ldots, e_s$ is a basis of $H^0(V)$. □

Proof of Theorem 3.3. Let $V = V_1 \cup \cdots \cup V_s$ be the decomposition of V into connected components. We will construct a maximal complete set of orthogonal idempotents $e_1, \ldots, e_s$, where $e_i = 1$ on V_i and 0 elsewhere. This shows the direct product decomposition

$$K[V] \simeq \prod_{i=1}^{s} K[V_i].$$

Let $I_i := I(V_i)$ be the vanishing ideal of V_i in $S := K[V]$. Then $I_i \neq S$ for all i (since $V_i \neq \emptyset$), and $I_1 \cap \cdots \cap I_s = (0)$ (since $V = \bigcup_i V_i$). Furthermore, since $V_i \cap V_j = \emptyset$, from Hilbert's Nullstellensatz we obtain $\varphi_{ij} \in I_i$ and $\psi_{ij} \in I_j$ for all $1 \leq i < j \leq s$ with

$$\varphi_{ij} + \psi_{ij} = 1. \tag{3.1}$$

Now define

$$e_i := \prod_{j<i} \varphi_{ji} \cdot \prod_{j>i} \psi_{ij} \in I_1 \cap \cdots \cap \widehat{I_i} \cap \cdots \cap I_s. \tag{3.2}$$

Then for all $i \neq j$ we have $e_i e_j \in I_1 \cap \cdots \cap I_s = (0)$. Furthermore, from (3.1) it follows $\varphi_{ji} \equiv 1 \pmod{I_i}$ for $j < i$, and $\psi_{ij} \equiv 1 \pmod{I_i}$ for $j > i$. Thus

$$e_i \equiv \begin{cases} 1 \pmod{I_i} \\ 0 \pmod{I_j} \end{cases}$$

for all $i \neq j$. We conclude $e_i^2 \equiv e_i \pmod{I_j}$ for all i, j, hence $e_i^2 = e_i$. Finally, $\sum_i e_i \equiv e_j \equiv 1 \pmod{I_j}$, thus $\sum_i e_i = 1$, and the $e_1, \ldots, e_s$ constitute a complete set of nontrivial orthogonal idempotents.

Now we show that this set is maximal. So assume $e_1 = f_1 + f_2$, say, where f_1, f_2 are nontrivial orthogonal idempotents. We show that then V_1 must be disconnected. Since $e_1 = e_1^2 = f_1 e_1 + f_2 e_1$, by replacing f_i by $f_i e_1$ we can assume $f_1, f_2 \in I_j$ for all $j > 1$. We set $W_i := \mathcal{Z}_V(J_i)$ with $J_i := (1 - f_i)$ for $i = 1, 2$. Then we have $W_i \subseteq V_1$, since by assumption $1 - f_i(x) = 1$ for all $x \in V_j$ with $j > 1$. We show $V_1 = W_1 \cup W_2$. For $x \in V_1$ we have $1 = e_1(x) = f_1(x) + f_2(x)$, hence $f_i(x) \neq 0$ for some i. Since $f_i(x)^2 = f_i(x)$, it follows $f_i(x) = 1$, hence $x \in W_i$. Furthermore $W_i \neq \emptyset$, since otherwise by Hilbert's Nullstellensatz there exists $f \in S$ with $(1 - f_i)f = 1$, thus $f_i = f_i(1 - f_i)f = 0$, a contradiction. Finally we have

$$f_2(1 - f_1) + \left(f_1 + \sum_{j>1} e_j \right)(1 - f_2) = f_2 + f_1 + \sum_{j>1} e_j = 1,$$

hence $J_1 + J_2 = S$, which shows $W_1 \cap W_2 = \emptyset$. Thus V_1 is disconnected, a contradiction.

Finally we prove the claimed degree bounds. According to Proposition 2.1 each V_i can be defined by equations $f_{i\nu}$ of degree $\leq \deg V_i \leq \deg V \leq d^n$. Since $V_i \cap V_j = \emptyset$ for $i < j$, we obtain from the effective Nullstellensatz (Theorem 2.2) polynomials $g_{i\nu}$ and $g_{j\nu}$ of degree $\leq d^{n^2}$ with

$$1 = \sum_\nu g_{i\nu} f_{i\nu} + \sum_\nu g_{j\nu} f_{j\nu},$$

thus the functions represented by $\varphi_{ij} := \sum_\nu g_{i\nu} f_{i\nu}$ and $\psi_{ij} := \sum_\nu g_{j\nu} f_{j\nu}$ satisfy (3.1). Since the number of connected components of V is bounded by d^n, it follows from (3.2) that e_i is represented by a polynomial of degree bounded by $sd^{n^2} \leq d^{n^2+n}$. $\square$

Example 3.5. Let $V = V_1 \cup V_2 \subseteq \mathbb{A}^3$, where $V_1 = \mathcal{Z}(Y - X^2, Z - X^3)$ is the twisted cubic and $V_2 = \mathcal{Z}(X - Y - 1, Y - Z)$ is a disjoint line. Then $e_1 := 1 + 2Y - Z - 2X^2 + XZ + X^3 - X^2Y$ and $e_2 := 1 - e_1$ are the corresponding idempotents, as one checks best in a parametrisation.

3.1.3. Algorithmic Idea

Theorem 3.3 reduces our problem of counting the connected components of a variety V to computing the dimension of $H^0(V)$. Furthermore, it yields a basis of this space of moderate degree. We denote $k[X]_{\le d} := \{f \in k[X] \mid \deg f \le d\}$, and for an ideal I we set $I_{\le d} := I \cap k[X]_{\le d}$. Now let V be the zero set of polynomials of degree $\le d$ and let $D = d^{\mathcal{O}(n^2)}$ be sufficiently large. Consider the map $\pi\colon K[X]_{\le D} \hookrightarrow K[X] \twoheadrightarrow K[V]$, and let $Z := \pi^{-1}(H^0(V))$. Then $\pi|Z\colon Z \to H^0(V)$ is surjective by Theorem 3.3, and its kernel is $I(V)_{\le D}$. Note that $I(V)_{\le D} \subseteq Z$, since a function vanishing on V has trivially vanishing differential. Hence

$$H^0(V) \simeq Z/I(V)_{\le D}. \tag{3.3}$$

Our goal is now to express the conditions $f \in Z$ and $f \in I(V)_{\le D}$ by linear equations in the coefficients of f. This way, we will be able to compute $\dim Z$ and $\dim I(V)_{\le D}$ and hence $\dim H^0(V)$ in parallel polynomial time. We begin with the second condition.

3.2. Modified Pseudo Remainders

In this section we characterise the radical of an ideal by a linear system of equations. The idea is to use squarefree regular chains, based on the observation that equation (2.2) defining pseudo division is linear if one knows the exponent α in advance. As remarked in §2.5.1, instead of the choice of a minimal α one can also take a fixed value for α to make the results unique. We will find values small enough for efficient computations and large enough to work for all polynomials of a given degree. Using these values we define a modified version of pseudo division.

3.2.1. Definition and Basis Properties

First we state degree bounds for usual pseudo quotients and remainders. The following lemma is a slightly modified and improved version of Lemma 3.3.3 in Szántó (1999).

Lemma 3.6. *Let $X_\ell := \operatorname{class}(g)$, $d := \deg_{X_\ell} f$, and $e := \deg_{X_\ell} g$ with $d \ge e$. Denote $q := \operatorname{pquo}(f,g)$ and $r := \operatorname{prem}(f,g)$. For $j \ne \ell$ we have*

$$\deg_{X_j} q \le (d-e)\deg_{X_j} g + \deg_{X_j} f$$

and

$$\deg_{X_j} r \le (d-e+1)\deg_{X_j} g + \deg_{X_j} f.$$

Now we want to derive bounds on the exponents and degrees of pseudo remainder sequences. So let $G = \{g_1, \dots, g_t\} \subseteq k[X]$ be a triangular set, and denote $\delta := \max\{\deg g_i \mid 1 \le i \le t\}$. In the following we will abbreviate $\deg_i := \deg_{\operatorname{class}(g_i)}$.

Lemma 3.7. *Let f be a polynomial of degree $d \ge 1$, and consider its pseudo remainder sequence $f_t, \dots, f_0$, so that there exist polynomials $q_1, \dots, q_t$ and integers $\alpha_1, \dots, \alpha_t \in \mathbb{N}$ with $\operatorname{lc}(g_i)^{\alpha_i} f_i = q_i g_i + f_{i-1}$ for all $1 \le i \le t$. Then the following bounds hold for all $1 \le i \le t$.*

$$\alpha_i \le \deg_i f_i, \tag{3.4}$$

$$\deg_{X_j} f_i \le d(\delta+1)^{t-i} \quad \text{for} \quad 1 \le j \le n. \tag{3.5}$$

$$\deg_{X_j} q_i \le d(\delta+1)^{t-i+1} \quad \text{for} \quad 1 \le j \le n. \tag{3.6}$$

Proof. By definition of pseudo division the α_i satisfy $\alpha_i \leq \deg_i f_i - \deg_i g_i + 1 \leq \deg_i f_i$, hence (3.4). The bound (3.6) follows easily from (3.4) and (3.5). We prove (3.5) by descending induction on i. The claim is obvious for $i = t$. Now let (3.5) be valid for some $i \leq t$. Then for $X_j \neq \operatorname{class}(g_i)$, Lemma 3.6 implies

$$\begin{aligned}\deg_{X_j} f_{i-1} &\leq (\deg_i f_i - \deg_i g_i + 1)\deg_{X_j} g_i + \deg_{X_j} f_i \\ &\overset{(3.4)}{\leq} \delta \deg_i f_i + \deg_{X_j} f_i \\ &\overset{(*)}{\leq} \delta d(\delta+1)^{t-i} + d(\delta+1)^{t-i} \\ &= d(\delta+1)^{t-i+1}.\end{aligned}$$

In step $(*)$ we have used the induction hypothesis. In the case $X_j = \operatorname{class}(g_i)$ we clearly have $\deg_{X_j} f_{i-1} < \delta \leq d(\delta+1)^{t-i+1}$. □

In view of Lemma 3.7 we introduce a modified version of pseudo division.

Definition 3.8.

(1) Let $f, g \in k[X]$ and $\alpha \in \mathbb{N}$ be large enough such that there exist polynomials q, r with $\operatorname{lc}(g)^\alpha f = qg + r$. We denote the *modified pseudo quotient* and *remainder* by $\operatorname{pquo}_\alpha(f,g) := q$ respectively $\operatorname{prem}_\alpha(f,g) := r$.

(2) Let $G = \{g_1, \ldots, g_t\}$ be a triangular set. Let $d \geq 1$ be some integer and $\delta := \max\{\deg g_i \mid 1 \leq i \leq t\}$. Set $\alpha_i := d(\delta+1)^{t-i}$ for $1 \leq i \leq t$. For any polynomial $f \in k[X]$ of degree d its *modified pseudo remainder sequence* $f_t, \ldots, f_0$ is defined by $f_t := f$, $f_{i-1} := \operatorname{prem}_{\alpha_i}(f_i, g_i)$ for $1 \leq i \leq t$. We define the *modified pseudo remainder* of f by G to be

$$\operatorname{prem}_d(f, G) := f_0.$$

Lemma 3.9. *Let $\overline{d} := nd(\delta+1)^t$. The map*

$$k[X]_{\leq d} \longrightarrow k[X]_{\leq \overline{d}}, \quad f \mapsto \operatorname{prem}_d(f, G)$$

is well-defined and k-linear.

Proof. By the bounds (3.5) the map is well-defined. We conclude by adding/scalar-multiplying the defining equations that $f \mapsto \operatorname{prem}_{\alpha_i}(f, g_i)$ is k-linear. Since $\operatorname{prem}_d(f, G)$ is the composition of modified pseudo remainders $\operatorname{prem}_{\alpha_i}(f, g_i)$, the claim follows. □

This linear map is efficiently computable.

Lemma 3.10. *One can compute the matrix of the linear map of Lemma 3.9 with respect to the monomial bases in parallel time $(n \log(d\delta))^{\mathcal{O}(1)}$ and sequential time $(d\delta)^{n^{\mathcal{O}(1)}}$.*

Proof. We show that given $f \in k[X]_{\leq d}$ one can compute $\operatorname{prem}_d(f, G)$ within the claimed resources. Having already computed $f = f_t, \ldots, f_i$, one has to compute $f_{i-1} = \operatorname{prem}_{\alpha_i}(f_i, g_i)$, i.e., we have to solve the linear system of equations

$$\operatorname{lc}(g_i)^{\alpha_i} f_i = q_i g_i + f_{i-1}$$

in the coefficients of q_i and f_{i-1}. By the bounds (3.5) and (3.4) this system has size $(d\delta)^{n^{\mathcal{O}(1)}}$. Hence the lemma follows with the algorithms from §2.4. □

3.2.2. Describing Radicals by Linear Algebra

Now we prove that we can use the modified pseudo division to calculate the saturated ideals of squarefree regular chains.

Proposition 3.11. *Let $G = \{g_1, \ldots, g_t\}$ be a squarefree regular chain with saturated ideal I. Then for any $d \in \mathbb{N}$ we have*

$$I_{\leq d} = \{f \in k[X]_{\leq d} \mid \operatorname{prem}_d(f, G) = 0\}.$$

Proof. "$\subseteq$". Since G is a regular chain, we have $I = \operatorname{Red}(G)$ by Proposition 2.7, hence each $f \in I_{\leq d}$ satisfies $\operatorname{prem}(f, G) = 0$. It is easy to see that this implies $\operatorname{prem}_d(f, G) = 0$.

"$\supseteq$". On the other hand, let $f \in k[X]_{\leq d}$ with $\operatorname{prem}_d(f, G) = 0$. We have to show $f \in I = \operatorname{Red}(G)$. For this purpose, let $\widetilde{f}_t = f, \ldots, \widetilde{f}_0 = 0$ be the modified pseudo remainder sequence of f with α_i as in Definition 3.8, so that there exist $\widetilde{q}_i$ such that $\operatorname{lc}(g_i)^{\alpha_i} \widetilde{f}_i = \widetilde{q}_i g_i + \widetilde{f}_{i-1}$ for $1 \leq i \leq t$. Now let $\beta_i \in \mathbb{N}$ be the maximal exponent such that $\operatorname{lc}(g_i)^{\beta_i}$ divides both $\widetilde{q}_i$ and $\widetilde{f}_{i-1}$. Then $\alpha_i' := \alpha_i - \beta_i$ is minimal with

$$\operatorname{lc}(g_i)^{\alpha_i'} \widetilde{f}_i = q_i g_i + f_{i-1} \quad \text{for} \quad 1 \leq i \leq t, \tag{3.7}$$

where $f_{i-1} := \widetilde{f}_{i-1} / \operatorname{lc}(g_i)^{\beta_i}$, $f_t := \widetilde{f}_t$, and $q_i := \widetilde{q}_i / \operatorname{lc}(g_i)^{\beta_i}$. Hence $f_{i-1} = \operatorname{prem}(\widetilde{f}_i, g_i)$.

Writing $G_i := \{g_1, \ldots, g_i\}$ we show by induction on i that

$$\operatorname{prem}(f_i, G_i) = 0 \quad \text{for} \quad 1 \leq i \leq t, \tag{3.8}$$

which is obvious for $i = 1$. Assuming (3.8) for $i - 1$, we conclude from (3.7) that $\widetilde{f}_i \in \operatorname{Red}(G_i)$. If $i = t$, then $\widetilde{f}_t = f$, and we are done. Otherwise, let P be any associated prime of the radical $\operatorname{Red}(G_i)$. Then $\widetilde{f}_i = f_i \operatorname{lc}(g_{i+1})^{\beta_{i+1}} \in P$. By the Definition 2.6 of regular chains it follows $f_i \in P$. Since this holds for all $P \in \operatorname{Ass}(\operatorname{Red}(G_i))$, we have $f_i \in \operatorname{Red}(G_i)$. $\square$

3.3. Computing Differentials

In order to compute the dimension of the zeroth de Rham cohomology via the isomorphism (3.3), it remains to describe the space Z by a linear system.

The idea is to use squarefree regular chains (cf. §2.5) in the following way. Assume for simplicity that $I = I(V)$ is the saturated ideal of a single squarefree regular chain $G = \{g_1, \ldots, g_t\}$. In general G does not generate the whole ideal I, but it generates it *almost everywhere* in the following sense. Let $\Gamma := \prod_{i=1}^{t} \operatorname{lc}(g_i)$ be the product of the leading coefficients of the g_i. Then Equation (2.3) shows that G generates I in the localisation $k[X]_\Gamma$. Furthermore we clearly have

$$\mathcal{Z}(G) \setminus \mathcal{Z}(\Gamma) \subseteq V \subseteq \mathcal{Z}(G).$$

Here the set on the left hand side is dense in V, since Γ is no zerodivisor on $k[V]$ by (2.4). If f is locally constant on a dense subset of V, it is clearly locally constant on V by continuity. Hence we have to check whether the differential of f vanishes on $\mathcal{Z}(G) \setminus \mathcal{Z}(\Gamma)$. We will shrink this subset a little further by considering some multiple h of Γ such that $\mathcal{Z}(G) \setminus \mathcal{Z}(h)$ is still dense in V.

In other (more algebraic) words, we work in $k[V]_h$. For a polynomial $f \in k[X]$ we denote by $\overline{f} := f + I(V)$ its residue class in $k[V]$. Then we have to check $\mathrm{d}\overline{f} = 0$

in $\Omega_{k[V]_h/k}$. We will give an explicit formula for $\mathrm{d}\overline{f}$ in $\Omega_{k[V]_h/k}$ in terms of the partial derivatives of f and of $g_1, \ldots, g_t$.

To simplify notation we reorder and rename the variables in a way such that $X_1, \ldots, X_m$ are the *free* variables, i.e., those which are *not* the class of some g_i, and the $Y_1, \ldots, Y_t$ are the *dependent* variables with $Y_i = \mathrm{class}\,(g_i)$ for $1 \leq i \leq t$. Thus we are working in $k[X, Y] := k[X_1, \ldots, X_m, Y_1, \ldots, Y_t]$ with $m + t = n$. Furthermore we set $g := (g_1, \ldots, g_t)^T$ and consider the Jacobian matrix

$$Dg := \left(\frac{\partial g}{\partial X}, \frac{\partial g}{\partial Y}\right) := \begin{pmatrix} \frac{\partial g_1}{\partial X_1} & \cdots & \frac{\partial g_1}{\partial X_m} & \frac{\partial g_1}{\partial Y_1} & \cdots & \frac{\partial g_1}{\partial Y_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_t}{\partial X_1} & \cdots & \frac{\partial g_t}{\partial X_m} & \frac{\partial g_t}{\partial Y_1} & \cdots & \frac{\partial g_t}{\partial Y_t} \end{pmatrix}.$$

Note that since G is a triangular set, the matrix $\frac{\partial g}{\partial Y}$ is lower triangular. In the promised formula we have to invert this matrix, so that its determinant $\Delta := \det(\frac{\partial g}{\partial Y}) = \prod_{i=1}^{t} \frac{\partial g_i}{\partial Y_i}$ yields the multiple $h := \Gamma\Delta$. We first prove that h does not cut away any component of V. Recall that this statement means that h is a non-zerodivisor on $k[V] = k[X]/\mathrm{Sat}\,(G)$. Since Γ is no zerodivisor, it remains to show that neither is Δ. The second statement of the following lemma will be relevant later.

Lemma 3.12. *The determinant Δ is not a zerodivisor on $k[V]$, hence $V \setminus \mathcal{Z}(\Delta)$ is dense in V. Furthermore, V is smooth at each point in $V \setminus \mathcal{Z}(\Delta)$.*

Proof. We make induction on n. For $n = 1$ we have either $G = \emptyset$, where there is nothing to prove, or $G = \{g\}$ with some squarefree g. Then V is the set of zeros of g. But g and g' have no common zeros.

So assume the lemma holds for some $n - 1 \geq 1$. In the case $t = 0$ there is nothing to prove, so let $t > 0$. Set $R := k[X_1, \ldots, X_m, Y_1, \ldots, Y_{t-1}]$, and let J be the saturated ideal of G_{t-1} in R, where $G_{t-1} = \{g_1, \ldots, g_{t-1}\} \subseteq R$. We adopt the notation introduced preceding Definition 2.6. Let $\mathrm{Ass}\,(J) = \{P_1, \ldots, P_s\}$. Since by part (3) of Proposition 2.7 J is radical, we have $J = P_1 \cap \cdots \cap P_s$. Let $\pi_i \colon R[Y_t] \to K(P_i)[Y_t]$ be the mapping $f \mapsto f^{P_i}$. Recall that $K(P)$ denotes the quotient field of R/P, and f^P the residue class $f \pmod P$ mapped into $K(P)$. Furthermore, let $g_t^{P_i} = \prod_{j=1}^{\ell_i} q_{ij}$ be an irreducible factorisation of $g_t^{P_i}$ (recall that $g_t^{P_i}$ is squarefree by assumption). Then $Q_{ij} := \pi_i^{-1}((q_{ij}))$ is as a preimage of a prime ideal clearly a prime ideal. It is shown in Kalkbrener (1998) (cf. Szántó (1999)) that

$$I = \bigcap_{ij} Q_{ij}. \tag{3.9}$$

We give the proof of (3.9) for completeness.

"$\subseteq$" Let $f \in I$ and perform pseudo division to obtain $\alpha \in \mathbb{N}$ and $q, r \in k[X]$ with $\mathrm{lc}\,(g_t)^\alpha f = qg_t + r$. By assumption (use part (2) of Proposition 2.7) $r \in J$. Since for all i we have $J \subseteq P_i$, it follows $\pi_i(\mathrm{lc}\,(g_t))^\alpha \pi_i(f) = \pi_i(q)\pi_i(g_t) \in (q_{ij})$ for all i, j. By definition of regular chains $\mathrm{lc}\,(g_t) \notin P_i$, hence $\pi_i(f) \in (q_{ij})$ for all i, j.

"$\supseteq$" Let $f \in \bigcap_{i,j} Q_{ij}$, i.e., $f^{P_i} \in \bigcap_j (q_{ij}) = (g_t^{P_i})$ for all i. Write again $\mathrm{lc}\,(g_t)^\alpha f = qg_t + r$ with $\alpha \in \mathbb{N}$ and $q, r \in k[X]$. Applying π_i yields $r^{P_i} \in (g_t^{P_i})$ for all i. Since by the definition of pseudo division $\deg_{Y_t} r < \deg_{Y_t} g_t$, it follows $r^{P_i} = 0$, hence $r \in P_i$. As this holds for all i, we conclude $r \in J$, thus $f \in \mathrm{Red}\,(G) = \mathrm{Sat}\,(G) = I$.

By the induction hypothesis we know that $\Delta_{t-1} := \prod_{i=1}^{t-1} \frac{\partial g_i}{\partial Y_i}$ is no zerodivisor on R/J, hence it lies in no associated prime P_i of J. Thus, $\Delta_{t-1}^{P_i}$ is a non-zero element of $K(P_i)$. Since $g_t^{P_i} = \prod_j q_{ij}$ is an irreducible decomposition, no q_{ij} is constant. It follows $\Delta_{t-1}^{P_i} \notin (q_{ij})$, hence $\Delta_{t-1} \notin Q_{ij} = \pi_i^{-1}((q_{ij}))$.

Furthermore, since by definition of squarefree regular chains $g_t^{P_i}$ is squarefree, none of its factors q_{ij} divides $\frac{d}{dY_t} g_t^{P_i}$, hence $\frac{d}{dY_t} g_t^{P_i} = (\frac{\partial g_t}{\partial Y_t})^{P_i} \notin (q_{ij})$, thus $\frac{\partial g_t}{\partial Y_t} \notin Q_{ij}$. Since by (3.9) all associated primes of I are among the Q_{ij}, it follows that $\Delta = \Delta_{t-1} \frac{\partial g_t}{\partial Y_t}$ is in no associated prime of I, hence it is no zerodivisor in $k[V] = R[Y_t]/I$.

Finally, the Jacobi criterion implies that each point in $V \setminus \mathcal{Z}(\Delta)$ is smooth. □

Proposition 3.13. *Let* $\Delta := \det(\frac{\partial g}{\partial Y})$ *and* $h := \Gamma\Delta$. *Then*

$$\Omega_{k[V]_h/k} = \bigoplus_{i=1}^{m} k[V]_h \mathrm{d}\overline{X}_i \tag{3.10}$$

is a free $k[V]_h$*-module, and for each* $f \in k[X]$ *we have*

$$\mathrm{d}\overline{f} = \sum_{i=1}^{m} \left(\frac{\partial f}{\partial X_i} - \frac{\partial f}{\partial Y} \left(\frac{\partial g}{\partial Y} \right)^{-1} \frac{\partial g}{\partial X_i} \right) \mathrm{d}\overline{X}_i. \tag{3.11}$$

Proof. We first show (3.10). We denote by I_h the ideal generated by $I := I(V)$ in the local ring $k[X,Y]_h$. Then $g_1, \ldots, g_t$ generate I_h, which is the kernel of the projection $k[X,Y]_h \twoheadrightarrow k[V]_h =: R$. Since localisation commutes with formation of differentials (Eisenbud, 1995, Proposition 16.9), $\Omega_{k[X,Y]_h/k}$ is the free $k[X,Y]_h$-module generated by $\mathrm{d}X_1, \ldots, \mathrm{d}X_m, \mathrm{d}Y_1, \ldots, \mathrm{d}Y_t$. Hence the exact conormal sequence (Eisenbud, 1995, Proposition 16.3) reads as

$$I_h/I_h^2 \xrightarrow{\mathrm{d}} \bigoplus_{i=1}^{m} R\mathrm{d}\overline{X}_i \oplus \bigoplus_{i=1}^{t} R\mathrm{d}\overline{Y}_i \longrightarrow \Omega_{R/k} \longrightarrow 0.$$

Consider the free R-module with basis $\varepsilon_1, \ldots, \varepsilon_t$ and the surjective map $\bigoplus_{j=1}^{t} R\varepsilon_j \to I_h/I_h^2$ sending ε_j to the class of g_j. The composition with d yields the map

$$\alpha\colon \bigoplus_{j=1}^{t} R\varepsilon_j \longrightarrow \bigoplus_{i=1}^{m} R\mathrm{d}\overline{X}_i \oplus \bigoplus_{i=1}^{t} R\mathrm{d}\overline{Y}_i, \quad \varepsilon_j \mapsto \sum_{i=1}^{m} \frac{\partial g_j}{\partial X_i} \mathrm{d}\overline{X}_i + \sum_{i=1}^{t} \frac{\partial g_j}{\partial Y_i} \mathrm{d}\overline{Y}_i,$$

which is described by the matrix $(Dg)^T \in R^{n \times t}$, where $g = (g_1, \ldots, g_t)^T$. By construction the determinant of $A := (\frac{\partial g}{\partial Y})^T$ is a unit in R, hence A is invertible in $R^{t \times t}$.

Now set $B := A^{-1} = (b_{ij}) \in R^{t \times t}$ and define the map

$$\beta\colon \bigoplus_{i=1}^{m} R\mathrm{d}\overline{X}_i \oplus \bigoplus_{i=1}^{t} R\mathrm{d}\overline{Y}_i \to \bigoplus_{j=1}^{t} R\varepsilon_j, \quad \mathrm{d}\overline{X}_i \mapsto 0, \mathrm{d}\overline{Y}_i \mapsto \sum_{j=1}^{t} b_{j,i}\varepsilon_j.$$

Then one easily checks that $\beta \circ \alpha = \mathrm{id}$, thus α is injective. The exact sequence

$$0 \longrightarrow \bigoplus_{j=1}^{t} R\varepsilon_j \xrightarrow{\alpha} \bigoplus_{i=1}^{m} R\mathrm{d}\overline{X}_i \oplus \bigoplus_{i=1}^{t} R\mathrm{d}\overline{Y}_i \longrightarrow \Omega_{R/k} \longrightarrow 0$$

splits by β, hence $\bigoplus_{i=1}^m R\mathrm{d}\overline{X}_i = \ker\beta \simeq \operatorname{coker}\alpha \simeq \Omega_{R/k}$, which shows (3.10).

To compute the differential, note that in $\Omega_{k[V]_h/k}$ the relation

$$0 = \sum_{j=1}^{m} \frac{\partial g_i}{\partial X_j}\mathrm{d}\overline{X}_j + \sum_{j=1}^{t} \frac{\partial g_i}{\partial Y_j}\mathrm{d}\overline{Y}_j$$

holds for all $1 \le i \le t$, hence symbolically

$$\begin{pmatrix} \frac{\partial g_1}{\partial Y_1} & \cdots & \frac{\partial g_1}{\partial Y_t} \\ \vdots & & \vdots \\ \frac{\partial g_t}{\partial Y_1} & \cdots & \frac{\partial g_t}{\partial Y_t} \end{pmatrix} \begin{pmatrix} \mathrm{d}\overline{Y}_1 \\ \vdots \\ \mathrm{d}\overline{Y}_t \end{pmatrix} = - \begin{pmatrix} \frac{\partial g_1}{\partial X_1} & \cdots & \frac{\partial g_1}{\partial X_m} \\ \vdots & & \vdots \\ \frac{\partial g_t}{\partial X_1} & \cdots & \frac{\partial g_t}{\partial X_m} \end{pmatrix} \begin{pmatrix} \mathrm{d}\overline{X}_1 \\ \vdots \\ \mathrm{d}\overline{X}_m \end{pmatrix},$$

thus

$$\begin{pmatrix} \mathrm{d}\overline{Y}_1 \\ \vdots \\ \mathrm{d}\overline{Y}_t \end{pmatrix} = - \left(\frac{\partial g}{\partial Y}\right)^{-1} \left(\frac{\partial g}{\partial X}\right) \begin{pmatrix} \mathrm{d}\overline{X}_1 \\ \vdots \\ \mathrm{d}\overline{X}_m \end{pmatrix}.$$

From this a straightforward calculation shows (3.11). □

3.4. Proof of Theorem 3.1

Let $V = \mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$ with polynomials $f_i \in k[X]$ of degree bounded by $d \ge 2$, let $n > 1$, and set $I := I(V) \subseteq K[X]$. By Theorem 2.8 we can compute squarefree regular chains $G_1, \ldots, G_s$ in $k[X]$ with saturated ideals $I_1, \ldots, I_s$ such that $I = I_1 \cap \cdots \cap I_s$. Now let δ be an upper bound on the degree of the polynomials in all G_i.

By Proposition 3.11 we have for each $D \in \mathbb{N}$

$$I_{\le D} = \{f \in K[X]_{\le D} \mid \bigwedge_{i=1}^{s} \operatorname{prem}_D(f, G_i) = 0\}, \tag{3.12}$$

and by Lemma 3.9 this is the solution space of some linear system of equations of size $s(D\delta)^{n^{\mathcal{O}(1)}}$, which can be constructed in parallel time $(n\log(D\delta))^{\mathcal{O}(1)}$ and sequential time $s(D\delta)^{n^{\mathcal{O}(1)}}$ by Lemma 3.10.

Now let $D = d^{\mathcal{O}(n^2)}$ be the degree bound from Theorem 3.3. According to (3.3), the number of connected components of V is given by

$$\dim H^0(V) = \dim Z - \dim I_{\le D}, \tag{3.13}$$

where $Z = \pi^{-1}(H^0(V))$ with $\pi\colon K[X]_{\le D} \to K[V],\ f \mapsto \overline{f}$.

To describe Z by linear equations, we consider the case $s = 1$ first. We use Proposition 3.13, whose notation we adopt. Note that the coefficients of the $\mathrm{d}\overline{X}_i$ in (3.11) are rational functions, since the matrix $\left(\frac{\partial g}{\partial Y}\right)^{-1}$ contains rational functions. But the only denominator in that matrix is the determinant Δ, which is a non-zerodivisor on $K[V]$ according to Lemma 3.12. Hence we can multiply equation (3.11) with Δ to obtain polynomial functions. Then we have for all $f \in K[X]_{\le D}$

$$\mathrm{d}\overline{f} = 0 \iff \bigwedge_{i=1}^{m} \Delta\frac{\partial f}{\partial X_i} - \frac{\partial f}{\partial Y}\Delta\left(\frac{\partial g}{\partial Y}\right)^{-1}\frac{\partial g}{\partial X_i} \in I.$$

The degree of the polynomials in this expression is of order $(D\delta)^{n^{\mathcal{O}(1)}}$, hence it can be expressed as a linear system of equations with the same asymptotic size bound. Moreover, the matrix $\Delta\left(\frac{\partial g}{\partial Y}\right)^{-1}$ can be computed using Formula (2.1) and Berkowitz' algorithm (cf. §2.4) in parallel time $(n \log \delta)^{\mathcal{O}(1)}$ and sequential time $\delta^{n^{\mathcal{O}(1)}}$.

Now, for general s, we have $V = V_1 \cup \cdots \cup V_s$ with $V_i := \mathcal{Z}(I_i)$. As we have seen, we can express the condition that f is locally constant on V_i by a linear system of equations. And f is locally constant on V iff if it is locally constant on each V_i, so that we can combine the equations for all V_i to obtain equations for Z.

Finally we have expressed both $I_{\leq D}$ and Z as solution spaces of linear systems over k of size $s(D\delta)^{n^{\mathcal{O}(1)}}$. Using the bounds for δ and s of Theorem 2.8 and $D = d^{\mathcal{O}(n^2)}$ one sees that this size is $d^{n^{\mathcal{O}(1)}}$. By the results of §2.4 one can compute the dimensions of (3.13) in parallel time $(n \log d)^{\mathcal{O}(1)}$ and sequential time $d^{n^{\mathcal{O}(1)}}$ over k. This shows $\#\mathrm{CC}_k \in \mathrm{FPAR}_k$. □

4. Irreducible Components

We will give an algorithm counting the irreducible components of a variety using methods very similar to those used in the last section. As usual k denotes a field of characteristic zero. We consider the following problem.

$\#\mathrm{IC}_k$ (*Counting irreducible components*) Given the polynomials $f_1, \ldots, f_r \in k[X]$, compute the number of irreducible components of their affine zero set $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$.

The same argument as in §3 shows that the versions of the problem $\#\mathrm{IC}_k$ for the different data structures dense, sparse, and slp encoding are polynomial time equivalent. The main result of this chapter is the following theorem.

Theorem 4.1. *We have $\#\mathrm{IC}_k \in \mathrm{FPAR}_k$ for every field k of characteristic zero.*

Before proving Theorem 4.1 we make some comments on lower bounds for the problem. The same proof as for Proposition 3.2 shows

Proposition 4.2. *The problem $\#\mathrm{IC}_{\mathbb{C}}$ is $\#\mathrm{P}_{\mathbb{C}}$-hard with respect to Turing reductions.*

However, up to now we are not able to show that $\#\mathrm{IC}_{\mathbb{Q}}$ is FPSPACE-hard. The best lower bound for the problem in the Turing model is GCC-hardness. The class GCC is defined in Bürgisser and Cucker (2006) as the Boolean part of $\#\mathrm{P}_{\mathbb{C}}$, and it is located between #P and FPSPACE in the landscape of binary complexity classes. Hence the GCC-hardness follows trivially from Proposition 4.2.

Problem 4.3. What is the inherent complexity of $\#\mathrm{IC}_{\mathbb{C}}$? Can it be reduced in polynomial time to counting complex solutions of polynomial equations, i.e., to $\#\mathrm{P}_{\mathbb{C}}$?

Bürgisser et al. (2006) recently showed that in the restricted setting of semilinear sets given by additive circuits over the reals, the problem of counting irreducible components is indeed captured by the class #P.

We prove Theorem 4.1 analogously to the case of connected components, but we work with rational instead of regular functions. The basic idea is the fact that the ring of rational functions on a variety is the direct product of the rings of rational functions of its irreducible components.

Recall that for an affine variety $V \subseteq \mathbb{A}^n$ we have denoted by $R(V)$ the ring of rational functions on V. By (Kunz, 1979, III, Satz 2.8) we have

Proposition 4.4. *Let $V = V_1 \cup \cdots \cup V_s$ be the decomposition of V into irreducible components. Then $R(V) \simeq \prod_{i=1}^{s} R(V_i)$.*

Hence according to the beginning of §3.1.2 the number of irreducible components is the cardinality of a maximal complete set of orthogonal idempotents in $R(V)$. Since these idempotents correspond to rational functions vanishing on all but one component, where they take the value 1, on each intersection of two components at least two of them are not defined. Thus the product h of the denominators of all idempotents lies in $\bigcap_{i \neq j} I(V_i \cap V_j)$. Since all denominators in $R(V)$ are non-zerodivisors in $K[V]$, so is h. On the other hand, given such a non-zerodivisor h, one can find the idempotents in $K[V]_h$ (see Theorem 4.6 below).

Example 4.5. (1) Let $V = V_1 \cup V_2 \subseteq \mathbb{A}^2$ with $V_1 = \mathcal{Z}(X)$ and $V_2 = \mathcal{Z}(Y)$. Then the two idempotents are $e_1 = \frac{Y}{X+Y}$ and $e_2 = \frac{X}{X+Y}$.

(2) Let $V = \mathcal{Z}(f) \subseteq \mathbb{A}^n$ be a hypersurface. We assume that $\gcd(f, \frac{\partial f}{\partial X_1}) = 1$, which implies that f is squarefree and each of its factors depends on X_1. Let $f = \prod_{i=1}^{s} f_i$ be its irreducible factorisation, hence $V = \bigcup_i V_i$ with $V_i = \mathcal{Z}(f_i)$. Then the corresponding idempotents are given by

$$e_i := \frac{f}{f_i} \frac{\frac{\partial f_i}{\partial X_1}}{\frac{\partial f}{\partial X_1}}, \quad 1 \leq i \leq s.$$

Note that the common denominator $\frac{\partial f}{\partial X_1}$ of the e_i lies in $\bigcap_{i \neq j} I(V_i \cap V_j)$ and it is a non-zerodivisor on $K[V]$. Note also that the first example is not a special case of the second one, since the assumption is not satisfied. However, one can perform a variable transformation to obtain e.g. $f = (X + Y)(X - Y)$ satisfying the assumption.

Similar as in §3.1 we consider the space of locally constant rational functions on V, which we denote (by analogy) with

$$H_r^0(V) := \{f \in R(V) \mid \mathrm{d}f = 0\}.$$

Then we have

Theorem 4.6. *Each affine variety $V \subseteq \mathbb{A}^n$ has $\dim H_r^0(V)$ irreducible components. Furthermore, let V be the zero set of polynomials of degree at most d and $h \in K[X]$ be a non-zerodivisor on $K[V]$ with $\deg h < d$ vanishing on all pairwise intersections of irreducible components of V. Sufficient for this condition is that h vanishes on the singular locus $\mathrm{Sing}\,(V)$. Then $H_r^0(V)$ has a basis of rational functions of the form f/h^N with $\max\{\deg f, N\} = d^{\mathcal{O}(n^2)}$.*

Proof. Introducing a new variable Y, the dense open subset $U := V \setminus \mathcal{Z}(h)$ of V is isomorphic to

$$W := (V \times \mathbb{A}^1) \cap \mathcal{Z}(hY - 1) \subseteq \mathbb{A}^{n+1}.$$

On the other hand, if $V = \bigcup_{i=1}^{s} V_i$ is the irreducible decomposition, then $U = \bigcup_{i=1}^{s}(V_i \setminus \mathcal{Z}(h))$ is the decomposition into connected components. By Theorem 3.3 there exists a maximal complete set of orthogonal idempotents in $K[W]$ induced by polynomials of degree bounded by $d^{\mathcal{O}(n^2)}$. The isomorphism $K[W] \simeq K[V]_h$ identifies Y with $1/h$, which shows that in $K[V]_h$ we obtain idempotents of the form f/h^N with the claimed bounds.

We show that this maximal complete set of orthogonal idempotents $E \subseteq K[V]_h$ is also maximal in $R(V)$. Fix i, and let $e \in E$ be the idempotent corresponding to V_i. Assume $e = f_1 + f_2$ with nontrivial orthogonal idempotents $f_j \in R(V)$. By replacing f_j with ef_j we can assume that the f_j vanish outside V_i. Since $f_1 f_2 = 0$, their numerators g_1, g_2 satisfy $g_1 g_2 = 0$ as well. Hence $V_i = \mathcal{Z}_{V_i}(g_1) \cup \mathcal{Z}_{V_i}(g_2)$. Since V_i is irreducible, we conclude w.l.o.g. $V_i = \mathcal{Z}_{V_i}(g_1)$, hence $g_1 = 0$ on V_i. Since g_1 vanishes outside V_i as well, $f_1 = 0$, a contradiction.

Literally as Lemma 3.4 one proves that the maximal complete set of orthogonal idempotents E is a basis of $H_r^0(V)$. □

4.2. Proof of Theorem 4.1

Before proving the theorem we have to cope with the redundancy of Szántó's decomposition (2.5) (cf. Remark 2.9). We prove that by computing ideal quotients we obtain an irredundant decomposition. Recall that the quotient of two ideals I, J is defined as

$$I : J = \{f \in k[X] \mid \forall g \in J \; fg \in I\}. \tag{4.1}$$

The ideal of the difference $V \setminus W$ of two affine varieties V and W is given by the quotient of their ideals (Cox et al., 1998, §4.4, Corollary 8)

$$I(V \setminus W) = I(V) : I(W),$$

hence $\mathcal{Z}(I(V) : I(W)) = \overline{V \setminus W}$. Set $N_{n,d} := \binom{n+d}{n}$. For a matrix $A \in k^{N \times N_{n,d}}$ and a polynomial $f \in k[X]_{\leq d}$ we write Af for the product of A with the column vector consisting of the coefficients of f.

Lemma 4.7. *Let $I_1, \ldots, I_s \subseteq k[X]$ be the saturated ideals of the squarefree regular chains $G_1, \ldots, G_s$. Let δ be an upper bound on the degrees of all polynomials occurring in the G_i. Then for each $1 < i \leq s$ and $d \in \mathbb{N}$ there exists a matrix $A_i \in k^{N_i \times N_{n,d}}$ with $N_i = (sd\delta)^{n^{\mathcal{O}(1)}}$ such that*

$$(I_i : (I_1 \cap \cdots \cap I_{i-1}))_{\leq d} = \{f \in k[X]_{\leq d} \mid A_i f = 0\}.$$

Furthermore, given $G_1, \ldots, G_s$ one can compute A_i in parallel time $(n \log(sd\delta))^{\mathcal{O}(1)}$ and sequential time $(sd\delta)^{n^{\mathcal{O}(1)}}$.

Proof. We fix i and set $J := I_1 \cap \cdots \cap I_{i-1}$. By Lemma 3.9, $J_{\leq D}$ is the solution space of some linear system of equations of size $s(D\delta)^{n^{\mathcal{O}(1)}}$, which can be constructed in parallel time $(n \log(D\delta))^{\mathcal{O}(1)}$ and sequential time $s(D\delta)^{n^{\mathcal{O}(1)}}$ by Lemma 3.10.

To represent $(I_i : J)_{\le d}$ by a linear system, we first have to show that for the "test polynomial" g in (4.1) it suffices to use a polynomial of single exponential degree. Indeed, we prove that with $D := s\delta^n$ we have

$$(\forall g \in J_{\le D} \quad fg \in I_i) \quad \Rightarrow \quad f \in I_i : J \tag{4.2}$$

for all $f \in k[X]$. For this purpose let f be given with $f \notin I_i : J$. We denote $V_j := \mathcal{Z}(I_j)$ for all j and $W := V_1 \cup \cdots \cup V_{i-1}$. Since $I_i : J = I(V_i \setminus W)$, there exists $x \in V_i \setminus W$ such that $f(x) \neq 0$. By Proposition 2.1, W can be defined by polynomials $g_1, \ldots, g_r$ with $\deg g_j \le \deg W$. From $x \notin W$ we conclude that some g_j does not vanish on x. Then $f(x)g_j(x) \neq 0$ and $fg_j \notin I_i$. It remains to bound $\deg W$. First recall that we have the inclusions

$$\mathcal{Z}(G_j) \setminus \mathcal{Z}(\Gamma) \subseteq V_j \subseteq \mathcal{Z}(G_j),$$

where Γ is the product of the leading coefficients of the polynomials in G_i. Since the first inclusion is dense, each irreducible component of V_j coincides with some irreducible component of $\overline{\mathcal{Z}(G_j) \setminus \mathcal{Z}(\Gamma)}$ and hence of $\mathcal{Z}(G_i)$. It follows $\deg V_j \le \deg \mathcal{Z}(G_j) \le \delta^n$. Thus $\deg W \le \sum_{j=1}^{i-1} \deg V_j \le s\delta^n$ which proves the claim (4.2).

By the methods of §2.4 one can compute a vector space basis $b_1, \ldots, b_u$ of $J_{\le D}$ in parallel time $(n \log(sD\delta))^{\mathcal{O}(1)}$ and sequential time $s^{\mathcal{O}(1)}(D\delta)^{n^{\mathcal{O}(1)}}$ (Compare the beginning of §3.4). It is further easy to compute the matrix L_j describing the linear map $k[X]_{\le d} \to k[X]_{\le d+D}$, $f \mapsto fb_j$. Hence by (4.2) we can write

$$\begin{aligned}
(I_i : J)_{\le d} &= \{f \in k[X]_{\le d} \mid \forall g \in J_{\le D}\ fg \in I_i\} \\
&= \{f \in k[X]_{\le d} \mid \bigwedge_{j=1}^{u} fb_j \in (I_i)_{\le d+D}\} \\
&= \{f \in k[X]_{\le d} \mid \bigwedge_{j=1}^{u} BL_j f = 0\},
\end{aligned}$$

where B is the coefficient matrix of the linear system describing $(I_i)_{\le d+D}$. □

Proof of Theorem 4.1. Let $V = \mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$ with polynomials $f_i \in k[X]$ of degree bounded by $d \ge 2$, let $n \ge 2$, and set $I := I(V)$. By Theorem 2.8 we can compute squarefree regular chains G_i with saturated ideals I_i, $1 \le i \le s$, such that $I = \bigcap_i I_i$. Denote $V_i := \mathcal{Z}(I_i)$. We order the ideals such that $\dim V_i \ge \dim V_{i+1}$ for $1 \le i < s$. Now set $Q_i := I_i : (I_1 \cap \cdots \cap I_{i-1})$. Then

$$W_i := \mathcal{Z}(Q_i) = \overline{V_i \setminus (V_1 \cup \cdots \cup V_{i-1})},$$

and we have

$$V = W_1 \cup \cdots \cup W_s. \tag{4.3}$$

We claim

(1) Each irreducible component C of W_i is an irreducible component of V_i, in particular $W_i \subseteq V_i$.
(2) Each W_i is equidimensional with $\dim W_i = \dim V_i$.
(3) The decomposition (4.3) is irredundant, i.e., no irreducible component of W_i is contained in any W_j with $j \neq i$.

Proof of Claim 1: Fix i, and let $V_i = \bigcup_\nu C_\nu$ be the irreducible decomposition of V_i. Then for all ν we have either $C_\nu \subseteq \bigcap_{j<i} V_j$ or not. In the first case $C_\nu \setminus \bigcap_{j<i} V_j = \emptyset$, and in the second $\overline{C_\nu \setminus \bigcap_{j<i} V_j} = C_\nu$. Hence W_i is the union over those C_ν with $C_\nu \not\subseteq \bigcap_{j<i} V_j$.

Claim 2 follows immediately from Claim 1 and the equidimensionality of V_i.

Proof of Claim 3: Assume that C is an irreducible component of W_i contained in W_j with $j \neq i$. Then C is a component of V_i by the Claim 1, and $\dim C \leq \dim W_j = \dim V_j$ by Claim 2. If $\dim C = \dim V_j$, then C is a common component of V_i and V_j, which have the same dimension. Thus, if $i > j$, then $W_i = \overline{V_i \setminus \bigcup_{\ell<i} V_\ell} \subseteq \overline{V_i \setminus C}$ does not contain C, a contradiction. The case $i < j$ is treated analogously. In the case $\dim C < \dim V_j$ it follows $j < i$ by the ordering with respect to dimension. But this implies also the contradiction $C \subseteq W_i \subseteq \overline{V_i \setminus C}$, which completes the proof of Claim 3.

By Claim 3 we have $\#\mathrm{ic}(V) = \sum_{i=1}^{s} \#\mathrm{ic}(W_i)$, where $\#\mathrm{ic}(V)$ denotes the number of irreducible components of V. Hence we can compute $\#\mathrm{ic}(W_i)$ for all i in parallel and sum up.

According to Lemma 3.12 the polynomial h_i defined as in Proposition 3.13 for G_i is a non-zerodivisor on $K[W_i]$ and vanishes on $\mathrm{Sing}\,(W_i)$. Hence h_i satisfies the conditions for the denominator h in Theorem 4.6 with respect to the variety W_i. Furthermore, $h_i = \prod_{g\in G_i} \mathrm{lc}\,(g) \cdot \prod_{g\in G_i} \frac{\partial g}{\partial \mathrm{class}\,(g)}$. Using $\max_{g\in G_i} \deg g = d^{n^{\mathcal{O}(1)}}$ we see that $\deg h_i = d^{n^{\mathcal{O}(1)}}$ and h_i can be computed from G_i in parallel polynomial time.

Now we describe how to compute the number of components of W_i. To simplify notation we drop the index i which is fixed from now on. For $D, N \in \mathbb{N}$ consider the linear map $\varphi\colon K[X]_{\leq D} \to K[W]_h$, $f \mapsto \overline{f}/\overline{h}^N$, and let $Z := \varphi^{-1}(H^0_r(W))$. Then for sufficiently large $D, N \leq d^{n^{\mathcal{O}(1)}}$ the restriction $\varphi|Z\colon Z \to H^0_r(W)$ is surjective by Theorem 4.6, hence

$$H^0_r(W) \simeq Z/Q_{\leq D}.$$

Note that $Q_{\leq D} \subseteq Z$. Therefore the number of irreducible components of W is given by

$$\dim H^0_r(W) = \dim Z - \dim Q_{\leq D}.$$

By Lemma 4.7 we can efficiently compute a linear system of equations for $Q_{\leq D}$. It remains to describe also Z by a linear system. We have for all $\overline{f} \in K[W]$

$$\mathrm{d}\left(\frac{\overline{f}}{\overline{h}^N}\right) = \frac{\overline{h}\,\mathrm{d}\overline{f} - N\overline{f}\mathrm{d}\overline{h}}{\overline{h}^{N+1}} = 0 \quad \iff \quad \overline{h}\,\mathrm{d}\overline{f} - N\overline{f}\mathrm{d}\overline{h} = 0.$$

Using Proposition 3.13 we can write

$$\overline{h}\,\mathrm{d}\overline{f} - N\overline{f}\mathrm{d}\overline{h} = \sum_{i=1}^{m} \left(h\frac{\partial f}{\partial X_i} - Nf\frac{\partial h}{\partial X_i} - \left(h\frac{\partial f}{\partial Y} - Nf\frac{\partial h}{\partial Y}\right)\left(\frac{\partial g}{\partial Y}\right)^{-1}\frac{\partial g}{\partial X_i}\right) \mathrm{d}\overline{X}_i.$$

By the direct sum decomposition of Proposition 3.13, $\overline{h}\mathrm{d}\overline{f} - N\overline{f}\mathrm{d}\overline{h} = 0$ iff all the coefficients of the $\mathrm{d}\overline{X}_i$ are zero. We further multiply with the determinant Δ and arrive at

$$f \in Z \quad \Longleftrightarrow \quad \bigwedge_{i=1}^{m} \left(\Delta \left(h \frac{\partial f}{\partial X_i} - N f \frac{\partial h}{\partial X_i} \right) - \right.$$
$$\left. - \left(h \frac{\partial f}{\partial Y} - N f \frac{\partial h}{\partial Y} \right) \Delta \left(\frac{\partial g}{\partial Y} \right)^{-1} \frac{\partial g}{\partial X_i} \in Q \right)$$

for all $f \in K[X]_{\leq D}$. The degree of the polynomials in this expression is bounded by $d^{n^{\mathcal{O}(1)}}$, hence this condition can be formulated by a linear system of the same asymptotic size. It follows $\#\mathrm{IC}_k \in \mathrm{FPAR}_k$, which completes the proof of Theorem 4.1. □

5. Transfer to the Turing Model

In the case $k = \mathbb{Q}$ we study the problems $\#\mathrm{CC}_{\mathbb{Q}}$ and $\#\mathrm{IC}_{\mathbb{Q}}$ in the classical Turing model. Our aim is to show that these problems lie in FPSPACE, the classical analogue of FPAR_k. Usually, if one has an algorithm which is analysed with respect to the algebraic operations, one studies the bitsize of all intermediate results of the algorithm in order to count the bit operations. One could do this also for the algorithms described above. We note that it would suffice to analyse the bitsize in Szántó's algorithm. The reason for this is that the rest of our algorithms consists of linear algebra computations, which behave well with respect to bitsize.

Instead we use the following general Transfer Theorem, which we prove in a subsequent paper (Bürgisser and Scheiblechner, 2008), see also (Scheiblechner, 2007a).

Theorem 5.1. *If a function $f \in \mathrm{FPAR}_{\mathbb{C}}$ maps rational inputs to rational outputs of polynomial bitsize, then the restriction of f to rational inputs is in* FPSPACE.

The condition of this theorem is satisfied for $\#\mathrm{CC}_{\mathbb{Q}}$ and $\#\mathrm{IC}_{\mathbb{Q}}$ (cf. §2.1.3). Thus, Theorems 3.1 and 4.1 imply with Theorem 5.1

Corollary 5.2. *We have $\#\mathrm{CC}_{\mathbb{Q}}, \#\mathrm{IC}_{\mathbb{Q}} \in$* FPSPACE.

As we have noted in the introduction, this upper bound for $\#\mathrm{CC}_{\mathbb{Q}}$ has already been obtained by real methods (Canny, 1988).

6. Hilbert Polynomial of Arithmetically Cohen-Macaulay Varieties

As mentioned in the introduction, we will apply the technique of §3.2 to the problem of computing the Hilbert polynomial of a projective variety. To compute the Hilbert polynomial by interpolation in parallel polynomial time, we need a single exponential bound for the minimal index, from which on the Hilbert function coincides with the Hilbert polynomial. This number is called the *index of regularity* or *a-invariant* (Stückrad and Vogel, 1986; Vasconcelos, 1998). Unfortunately a single exponential bound for the index of regularity of a radical is not known. We show a polynomial bound for projective varieties which are arithmetically Cohen-Macaulay.

We first fix some notations. As before let k be a field of characteristic zero and K be an algebraic closure of k. Consider the graded polynomial ring $S := K[X] = K[X_0, \ldots, X_n] = \bigoplus_{t\geq 0} S_t$, where $S_t = K[X]_t$ denotes the vector space of homogeneous polynomials of degree t. Consider a finitely generated graded S-module $M = \bigoplus_{t\in\mathbb{Z}} M_t$. The function $h_M \colon \mathbb{Z} \to \mathbb{N},\ t \mapsto \dim_k M_t$ is called the *Hilbert function* of M. It is well-known that there exists a unique polynomial $p_M \in \mathbb{Q}[T]$, the *Hilbert polynomial of* M, such that $h_M(t) = p_M(t)$ for $t \gg 0$ (Hartshorne, 1977; Eisenbud, 1995). Furthermore, the degree of p_M equals the dimension of the projective zero set of the annihilator $\{f \in S \mid fM = 0\}$. For a projective variety $V \subseteq \mathbb{P}^n$ we consider its homogeneous coordinate ring $M = S/I(V)$, and call $h_V := h_{S/I(V)}$ and $p_V := p_{S/I(V)}$ the *Hilbert function* respectively the *Hilbert polynomial of* V.

For a finitely generated S-module M we call

$$a(M) := \inf\{t_0 \in \mathbb{Z} \mid \forall t \geq t_0\ h_M(t) = p_M(t)\}$$

the *index of regularity of* M. For a projective variety $V \subseteq \mathbb{P}^n$ we denote with $a(V) := a(S/I(V))$ the *index of regularity of* V.

We start by observing what happens with hyperplane sections.

Lemma 6.1. *Let $I \subseteq S$ be a homogeneous ideal with $\sqrt{I} \neq \mathfrak{m} := (X_0, \ldots, X_n)$, and let $\ell \in S_1$ be a linear form with $\ell \notin \bigcup_{P\in \mathrm{Ass}\,(I)} P$. Then*

$$a(S/I) \leq a(S/(I + (\ell))).$$

Proof. The proof follows the lines of the proof for the existence of the Hilbert polynomial (Eisenbud, 1995, Theorem 1.11) observing that the first difference $h'_{S/I}(t) := h_{S/I}(t) - h_{S/I}(t-1)$, of $h_{S/I}$ satisfies $h'_{S/I}(t) = h_{S/(I+(\ell))}(t)$ for all $t \in \mathbb{Z}$. The claim now follows from Lemma 1.12 of (Eisenbud, 1995) stating that if the first difference $h'(t)$ of a function $h(t)$ agrees a polynomial for all $t \geq t_0$, then $h(t)$ agrees also with a polynomial for all $t \geq t_0$. □

The idea is now to cut down the variety $V(I)$ iteratively with linear forms until we get the empty set, in which case $\sqrt{I} = \mathfrak{m}$. The latter case can then be handled with the effective Nullstellensatz. Unfortunately, a linear form ℓ as in Lemma 6.1 does not exist if $\mathfrak{m} \in \mathrm{Ass}\,(I)$. One might think that this cannot harm us, since we only consider radical ideals I. But, by adding linear forms, we might destroy the radical property. In particular when I is a radical and ℓ a linear form as in Lemma 6.1, the ideal $I + (\ell)$ could have $\mathfrak{m}$ as associated prime and we could not proceed further. The following (astonishingly simple) example shows exactly this behaviour.

Example 6.2. Consider $I = (X_0, X_1) \cap (X_2, X_3) = (X_0X_2, X_0X_3, X_1X_2, X_1X_3) \subseteq K[X_0, X_1, X_2, X_3]$. Of course I is radical, $P_1 := (X_0, X_1)$ and $P_2 := (X_2, X_3)$ are the associated primes and $I = P_1 \cap P_2$ is the primary decomposition of I. Geometrically, $V = V(I) \subseteq \mathbb{P}^3$ is the union of two disjoint lines. The linear form $\ell = X_0 - X_2$ satisfies $\ell \notin P_1 \cup P_2$, but leads to the primary decomposition

$$I + (\ell) = (X_0, X_1, X_2) \cap (X_0, X_2, X_3) \cap (X_0^2, X_0X_1, X_0X_3, X_1^2, X_1X_3, X_3^2, X_0 - X_2).$$

The latter of these ideals is $\mathfrak{m}$-primary but not a radical, thus $I + (\ell)$ is not radical and $\mathfrak{m} \in \operatorname{Ass}(I + (\ell))$. Although we have considered a special linear form ℓ, one easily sees that the same phenomenon appears with generic ℓ.

This example shows that we cannot prove the desired bound for the general case with the help of Lemma 6.1. Hartshorne's Connectedness Theorem (Eisenbud, 1995, Theorem 18.12) says that a variety which is Cohen-Macaulay in a point, is locally connected in codimension 1, i.e., removing a subvariety of codimension 2 or more cannot disconnect it. Applying this theorem to the affine cone of the variety of Example 6.2 shows that this cone is not Cohen-Macaulay at the origin. However, it turns out that our method works well under this Cohen-Macaulayness condition.

For convenience we recall some definitions from commutative algebra. Let R be a commutative ring. A sequence $x_1, \ldots, x_n \in R$ is called a *regular sequence* iff $(x_1, \ldots, x_n) \neq R$ and x_i is a non-zerodivisor on $R/(x_1, \ldots, x_{i-1})$ for each $1 \leq i \leq n$. Now let $I \subset R$ be a proper ideal. Then $\operatorname{depth} I$ is defined as the length of a maximal regular sequence in I. On the other hand, there exists also the notion of codimension (or height) of I. If I is a prime ideal, then the *codimension* $\operatorname{codim} I$ is defined as the maximal length of an ascending chain of prime ideals in I. For general I, $\operatorname{codim} I$ is defined to be the minimal codimension of all primes containing I. A commutative ring R such that for all maximal ideals $M \subseteq R$ we have $\operatorname{depth} M = \operatorname{codim} M$ is called *Cohen-Macaulay*. In this case, we have $\operatorname{depth} I = \operatorname{codim} I$ for all proper ideals I in R.

If $R = S = K[X]$ is the polynomial ring as above, then $\operatorname{codim} I$ is exactly the codimension of the projective variety $V := \mathcal{Z}(I) \subseteq \mathbb{P}^n$, hence $\operatorname{codim} I$ depends only on the radical of I.

Definition 6.3. A projective variety $V \subseteq \mathbb{P}^n$ is called *arithmetically Cohen-Macaulay* iff $(S/I(V))_{\mathfrak{m}}$ is Cohen-Macaulay, where $\mathfrak{m} = (X_0, \ldots, X_n)$.

The following lemma shows that the Cohen-Macaulayness of the local ring we consider is preserved under generic hyperplane sections. It easily follows from the definitions and (Eisenbud, 1995, Proposition 18.13).

Lemma 6.4. *Let $I \subseteq S$ be a homogeneous ideal with $\sqrt{I} \neq \mathfrak{m}$, such that $(S/I)_{\mathfrak{m}}$ is Cohen-Macaulay. Then there exists a non-zerodivisor $\ell \in S_1$ on S/I. Furthermore, the ring $(S/(I, \ell))_{\mathfrak{m}}$ is again Cohen-Macaulay.*

The main result in this section is the following proposition.

Proposition 6.5. *Let $V \subseteq \mathbb{P}^n$ be a projective variety defined by homogeneous polynomials of degree bounded by d. If V is arithmetically Cohen-Macaulay, then its index of regularity satisfies*

$$a(V) \leq (n+1)d - n. \tag{6.1}$$

Proof. Let $m := \dim V$ and $I := I(V)$. We can assume $I \neq \mathfrak{m}$. We first prove the

Claim. There exist linear forms $\ell_0, \ldots, \ell_m \in S_1$ such that
(a) $\sqrt{I_i} \neq \mathfrak{m}$ for all $0 \leq i < m$, where $I_i := I + (\ell_0, \ldots, \ell_i)$,
(b) $\ell_i \notin \bigcup_{P \in \operatorname{Ass}(I_{i-1})} P$ for all $0 \leq i \leq m$ (set $I_{-1} := I$),
(c) $(S/I_i)_{\mathfrak{m}}$ is Cohen-Macaulay for all $0 \leq i \leq m$.

Suppose that $\ell_0, \ldots, \ell_{i-1}$ according to the claim are already constructed for some $0 \leq i \leq m$. Then $\sqrt{I_{i-1}} \neq \mathfrak{m}$, and $(S/I_{i-1})_{\mathfrak{m}}$ is Cohen-Macaulay. Thus, by Lemma 6.4, there exists $\ell_i \in S_1$ such that (b) and (c) hold. In the case $i = m$ we are done. If $i < m$, then by the Principal Ideal Theorem (Eisenbud, 1995, Theorem 10.2) we have $\operatorname{codim} I_i \leq \operatorname{codim} I + i + 1 \leq \operatorname{codim} I + m = n$, since the codimension depends only on the radical. Hence (a) also holds, which proves the claim.

Setting $I_m := I + (\ell_0, \ldots, \ell_m)$ we have $\sqrt{I_m} = \mathfrak{m}$. Now let V be defined by the homogeneous polynomials $f_1, \ldots, f_r$ with $\deg f_i \leq d$, and set $J := (f_1, \ldots, f_r, \ell_0, \ldots, \ell_m)$. Then $\sqrt{J} = \sqrt{I_m} = \mathfrak{m}$. By Theorem 2.3 we have $\mathfrak{m}^D \subseteq J \subseteq I_m$, where $D := (n+1)d - n$. This means that all monomials of degree $\geq D$ are in I_m, i.e., $h_{S/I_m}(t) = 0$ for all $t \geq D$. Of course, the Hilbert polynomial of S/I_m is the zero polynomial, hence $a(S/I_m) \leq D$. Further, by repeated application of Lemma 6.1 we obtain $a(S/I) \leq a(S/I_m) \leq D$. □

6.2. Computing the Hilbert Polynomial

Now we use what we have learned to compute the Hilbert polynomial in the arithmetical Cohen-Macaulay case.

Theorem 6.6. *Let k be a field of characteristic zero. Let $V = \mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{P}^n$ be a projective variety given by homogeneous polynomials $f_i \in k[X]$ with $\deg f_i \leq d$. If V is arithmetically Cohen-Macaulay, then one can compute the Hilbert polynomial p_V in parallel time $(n \log d)^{\mathcal{O}(1)}$ and sequential time $d^{n^{\mathcal{O}(1)}}$.*

Proof. Set $I := I(V)$. By Theorem 2.8 we can compute within the desired bounds squarefree regular chains G_i with saturated ideals I_i, $1 \leq i \leq s$, such that $I = \bigcap_{i=1}^{s} I_i$. Now fix some $t \in \mathbb{N}$. We have

$$\dim(S/I)_t = \binom{n+t}{n} - \dim(I \cap S_t),$$

hence it remains to compute the latter dimension. Let δ be an upper bound on the degrees of the polynomials in all G_i. By Theorem 2.8 we have $\delta = d^{\mathcal{O}(n^2)}$. Then by Proposition 3.11

$$I \cap S_t = \bigcap_{i=1}^{s} I_i \cap S_t = \{f \in S_t \mid \bigwedge_i \operatorname{prem}_t(f, G_i) = 0\}.$$

Recall from Definition 3.8 that prem_t denotes the modified pseudo remainder for polynomials of degree t. Now let $(n+1)d - n \leq t \leq (n+1)d$. Then $I \cap S_t$ is the solution space of a linear system of size $d^{\mathcal{O}(n)}\delta^{\mathcal{O}(n^2)}$, which we can construct by Lemma 3.10 in parallel time $(n \log d\delta)^{\mathcal{O}(1)}$ and sequential time $(d\delta)^{n^{\mathcal{O}(1)}}$. Hence, we can compute the value of the Hilbert function $h_V(t)$ within the desired resources.

Now we compute $h_V(t)$ for each $(n+1)d - n \leq t \leq (n+1)d$. Since by Proposition 6.5 these values coincide with the values of p_V, which is a polynomial of degree $\leq n$, we can compute p_V by interpolation. □

Acknowledgements

The authors would like to thank Thilo Pruschke for pointing out the necessity of a Cohen-Macaulayness condition in the result about the Hilbert polynomial. We further thank the anonymous referees of ISSAC '07 for their valuable comments and for pointing us to further literature on triangular sets. Finally we thank Agnes Szántó for informing us about the redundancy of her decomposition.

References

Aubry, P., Lazard, D., Maza, M. M., 1999. On the theories of triangular sets. J. Symb. Comp. 28 (1-2), 105–124.

Basu, S., Pollack, R., Roy, M.-F., 2003. Algorithms in Real Algebraic Geometry. Vol. 10 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin Heidelberg New York.

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

Bayer, D., Stillman, M., 1992. Computation of Hilbert functions. J. Symbolic Comput. 14 (1), 31–50.

Berkowitz, S., 1984. On computing the determinant in small parallel time using a small number of processors. Inf. Process. Lett. 18 (3), 147–150.

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

Borodin, A., 1977. On relating time and space to size and depth. SIAM J. Comp. 6, 733–744.

Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the D5 principle. In: Proc. of *Transgressive Computing 2006*. Granada, Spain, pp. 79–91.

Brownawell, W., 1987. Bounds for the degrees in the Nullstellensatz. Ann. of Math. (2) 126 (3), 577–591.

Bürgisser, P., Cucker, F., 2004. Variations by complexity theorists on three themes of Euler, Bézout, Betti, and Poincaré. In: Krajíček, J. (Ed.), Complexity of computations and proofs. Vol. 13 of Quaderni di Matematica [Mathematics Series]. Department of Mathematics, Seconda Università di Napoli, Caserta, pp. 73–152.

Bürgisser, P., Cucker, F., 2006. Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets. J. Compl. 22, 147–191.

Bürgisser, P., Cucker, F., de Naurois, P., 2006. The complexity of semilinear problems in succinct representation. Comp. Compl. 15 (3), 197–235.

Bürgisser, P., Lotz, M., 2007. The complexity of computing the Hilbert polynomial of smooth equidimensional complex projective varieties. Foundations of Computational Mathematics 7 (1), 59–86.

Bürgisser, P., Scheiblechner, P., 2007. Differential forms in computational algebraic geometry. In: ISSAC '07: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation. ACM Press, New York, NY, USA, pp. 61–68.

Bürgisser, P., Scheiblechner, P., 2008. Counting irreducible components of complex algebraic varieties, Preprint University of Paderborn.
URL `http://www2.math.upb.de/people/peter-scheiblechner/research.html`

Canny, J., 1988. Some algebraic and geometric computations in PSPACE. In: Proc. 20th Ann. ACM STOC. pp. 460–467.

Chistov, A., 1984. Algorithm of polynomial complexity for factoring polynomials, and finding the components of varieties in subexponential time. Theory of the complexity of computations, II., Zap. Nauchn. Sem. Leningrad Otdel. Mat. Inst. Steklov (LOMI) 137, 124–188, english translation: J. Sov. Math. 34(1986).

Cox, D., Little, J., O'Shea, D., 1998. Using algebraic geometry. Vol. 185 of Graduate Texts in Mathematics. Springer-Verlag, New York.

Eisenbud, D., 1995. Commutative Algebra with a View Toward Algebraic Geometry. Vol. 150 of Graduate Texts in Mathematics. Springer-Verlag, New York.

Eisenbud, D., Huneke, C., Vasconcelos, W., 1992. Direct methods for primary decomposition. Invent. Math. 110, 207–235.

Fitchas, N., Galligo, A., 1990. Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel. Math. Nachr. 149, 231–253.

Gallo, G., Mishra, B., 1991. Wu-Ritt characteristic sets and their complexity. In: Discrete and Computational Geometry: Papers from the DIMACS Special Year. pp. 111–136.

Gathen, J. v. z., 1986. Parallel arithmetic computations: a survey. In: MFOCS86. No. 233 in LNCS. SV, pp. 93–112.

Gianni, P., Trager, B., Zacharias, G., 1988. Gröbner bases and primary decomposition of polynomial ideals. J. Symb. Comp. 6 (2-3), 149–167.

Giusti, M., Heintz, J., 1991. Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In: Traverso, T. M. C. (Ed.), Effective Methods in Algebraic Geometry (Proceedings of MEGA'90). Vol. 94 of Progress in Math. Birkhäuser, New York, NY, USA, pp. 169–193.

Grigoriev, D., 1984. Factoring polynomials over a finite field and solution of systems of algebraic equations. Theory of the complexity of computations, II., Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137, 20–79, english translation: J. Sov. Math. 34(1986).

Harris, J., 1992. Algebraic geometry. Vol. 133 of Graduate Texts in Mathematics. Springer-Verlag, New York Berlin Heidelberg.

Hartshorne, R., 1977. Algebraic geometry. Springer-Verlag, New York.

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

Kalkbrener, M., 1993. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. J. Symb. Comp. 15, 143–167.

Kalkbrener, M., 1994. Prime decomposition of radicals in polynomial rings. J. Symb. Comp. 18, 365–372.

Kalkbrener, M., 1998. Algorithmic properties of polynomial rings. J. Symb. Comp. 26 (5), 525–581.

Koiran, P., 1997. Randomized and deterministic algorithms for the dimension of algebraic varieties. In: Proc. 38th IEEE Symposium on Foundations of Computer Science. pp. 36–45.

Kollár, J., 1988. Sharp effective Nullstellensatz. J. Amer. Math. Soc. 1 (4), 963–975.

Kunz, E., 1979. Einführung in die kommutative Algebra und algebraische Geometrie. Vol. 46 of Vieweg-Studium: Aufbaukurs Mathematik. Vieweg, Wiesbaden.

Lazard, D., 1981. Résolution des systèmes d'équations algébriques. Theoret. Comp. Sci. 15, 77–110.

Lazard, D., 1991. A new method for solving algebraic equations of positive dimension. Discr. Appl. Math. 33, 147–160.

Mayr, E., 1997. Some complexity results for polynomial ideals. J. Compl. 13 (3), 303–325.

Mora, F., Möller, H., 1983. The computation of the Hilbert function. In: EUROCAL '83: Proceedings of the European Computer Algebra Conference on Computer Algebra. Springer-Verlag, London, UK, pp. 157–167.

Mulmuley, K., 1987. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. Combinatorica 7 (1), 101–104.

Mumford, D., 1976. Algebraic Geometry I: Complex Projective Varieties. Vol. 221 of Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin Heidelberg New York.

Ritt, J., 1950. Differential Algebra. Americal Mathematical Society.

Scheiblechner, P., 2007a. On the complexity of counting irreducible components and computing Betti numbers of complex algebraic varieties, PhD Thesis.
URL `http://www2.math.upb.de/people/peter-scheiblechner/research.html`

Scheiblechner, P., 2007b. On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety. J. Compl. 23, 359–379.

Shafarevich, I., 1977. Basic Algebraic Geometry. Vol. 213 of Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin Heidelberg New York.

Stückrad, J., Vogel, W., 1986. Buchsbaum Rings and Applications. Springer-Verlag, Berlin Heidelberg New York.

Szántó, Á., 1997. Complexity of the Wu-Ritt decomposition. In: PASCO '97: Proceedings of the second international symposium on Parallel symbolic computation. ACM Press, New York, NY, USA, pp. 139–149.

Szántó, Á., 1999. Computation with polynomial systems, PhD Thesis.
URL `http://www4.ncsu.edu/~aszanto/papers.html`

Vasconcelos, W., 1998. Computational methods in commutative algebra and algebraic geometry. Vol. 2 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin.

Wang, D., 1992. Irreducible decomposition of algebraic varieties via characteristics sets and Gröbner bases. Computer Aided Geometric Design 9, 471–484.

Wu, W.-T., 1986. Basic principles of mechanical theorem proving in elementary geometries. J. of Automated Reasoning 2, 221–252.