Differential Forms in Computational Algebraic Geometry

[Extended Abstract] *

Peter Bürgisser[†]
pbuerg@math.upb.de

Peter Scheiblechner[†]
pscheib@math.upb.de

Dept. of Mathematics
University of Paderborn
Warburger Str. 100
33098 Paderborn, Germany

ABSTRACT

We give a uniform method for the two problems $\#\mathrm{CC}_{\mathbb{C}}$ and $\#\mathrm{IC}_{\mathbb{C}}$ of counting connected and irreducible components of complex algebraic varieties, respectively. Our algorithms are purely algebraic, i.e., they use only the field structure of $\mathbb{C}$. They work efficiently in parallel and can be implemented by algebraic circuits of polynomial depth, i.e., in parallel polynomial time. The design of our algorithms relies on the concept of algebraic differential forms. A further important building block is an algorithm of Szántó [40] computing a variant of characteristic sets.

The crucial complexity parameter for $\#\mathrm{IC}_{\mathbb{C}}$ turns out to be the number of equations. We describe a randomised algorithm solving $\#\mathrm{IC}_{\mathbb{C}}$ for a fixed number of rational equations given by straight-line programs (slps), which runs in parallel polylogarithmic time in the length and the degree of the slps.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*Algebraic algorithms*; F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems—*Geometrical problems and computations*

General Terms

Algorithms, Theory

Keywords

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. [3] and the numerous citations given there. In particular, work of Canny [12] 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 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 only algebraic methods.

A complex variety is connected in the Euclidean topology iff it is connected in the Zariski topology (this follows easily from the fact that irreducible varieties are connected in the Euclidean topology [39, VII, 2.2]). 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 ($\overline{k}$ an algebraic closure of k).

We present an algorithm counting connected components in parallel polynomial time over k, i.e., $\#\mathrm{CC}_k \in \mathrm{FPAR}_k$ (cf. [8] and §2.1 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 [27] 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 [36] and was used by Wu [44] for automated theorem proving. Their computational complexity was studied by Gallo and Mishra [16]. Subsequently, algorithms computing variants of this concept were studied by Kalkbrener [23, 24, 25], Lazard [30], and Wang [43]. See [1] for a comparison of the different notions of characteristic sets. Szántó [40] 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

[*] This paper is a summary of main results of the PhD Thesis of the second author.

[†] Partially supported by DFG grant BU1371.

ISSAC'07 July 29-August 1, 2007, Waterloo, Ontario, Canada
Copyright 2007 ACM 978-1-59593-743-8/07/0007 ...$5.00.

described by ascending sets, which we will call *squarefree regular chains* in compliance with [1, 7]. 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 V into irreducible components has been attacked in the last decades with numerous methods. There are algorithms based on characteristic sets [44, 30, 24], however, their complexity has not been analysed. Other methods use Gröbner bases [18, 15], but according to Mayr [32], computing those is exponential space-complete. The first single exponential time algorithms for computing both the irreducible and absolutely irreducible components are due to Chistov and Grigoriev [13, 20] (in the bit model). Giusti and Heintz [19] 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 $\#\mathrm{CC}_k$. 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 Fixing Parameters

A standard argument [8, Remark 6.3] shows that the complexity of $\#\mathrm{CC}_k$ and $\#\mathrm{IC}_k$ does not depend on whether the input polynomials are given in dense encoding or by straight-line programs (slps). However, when input parameters like the number of variables, the number of equations, or their maximal degree are fixed, then the choice of the input data structure matters. We thus study the complexity of $\#\mathrm{IC}_k$ for fixed input parameters. We focus here on the number r of equations, which turns out to be crucial. We first discuss the case $r = 1$.

1.3.1 *Counting Irreducible Factors*

The algorithmic factorisation of polynomials is a widely studied problem. Here we restrict ourselves to factorisation into absolutely irreducible polynomials. The first work on absolute irreducibility we are aware of is Heintz et al. [22] providing a randomised single exponential time algorithm for testing absolute irreducibility. Kaltofen [26] gave the first parallel polylogarithmic time algorithm testing absolute irreducibility of a rational bivariate polynomial. A parallel polylogarithmic time algorithm to compute the number and degrees of the absolutely irreducible factors of a rational polynomial was described by Bajaj et al. [2].

A new approach to factorisation was found by Gao [17], based on work of Ruppert [37], who characterised absolute irreducibility of a bivariate polynomial f by the nonexistence of a closed differential form with denominator f and a numerator satisfying certain degree bounds. We interpret the space of these differential forms as the first algebraic de Rham cohomology $H^1(\mathbb{A}^n_f)$ of the hypersurface complement defined by f and prove that the "logarithmic differentials" of the absolutely irreducible factors of f induce a basis of $H^1(\mathbb{A}^n_f)$. In this way $H^1(\mathbb{A}^n_f)$ can be described by systems of linear equations of polynomial size. Hence the number of factors of f can be obtained by a uniform family of algebraic circuits of polylogarithmic depth, i.e., $\#\mathrm{IF}_k \in \mathrm{FNC}^2_k$. This result seems to be new (the algorithm of [2] only works in the bit model).

1.3.2 *Fixed Number of Equations*

We show that for a fixed number r of rational equations, given by straight-line programs, one can solve the problem $\#\mathrm{IC}_{\mathbb{C}}$ in randomised parallel polylogarithmic time in the length and the degree of the slps. Our proof of this result essentially uses the concept of *generic parsimonious reductions* defined by Bürgisser et al. in [11]. The idea is Bertini's Theorem stating that the intersection of an irreducible variety with a generic hyperplane remains irreducible. By intersecting with a linear subspace of fixed dimension we can establish a generic parsimonious reduction to a constant number of variables. The result for the discrete setting then follows by a new transfer principle.

2. PRELIMINARIES

2.1 Models of Computation and Complexity

Our model of computation is that of algebraic circuits, cf. [42, 8]. 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 [6].

2.2 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 [33] 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 [4].

For $k = \mathbb{Q}$ the bitsize of this algorithm has been analysed in [31] showing that the corresponding problem lies in FNC^2.

2.3 Squarefree Regular Chains

Here we give basic definitions which we adopt from [1] and outline results of Szántó [40].

2.3.1 Definitions and Basic Properties

We fix an ordering on the variables $X_1 < \ldots < X_n$ 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 $\mathrm{class}\,(f) := \min\{X_i \mid f \in k[X_1, \ldots, X_i]\}$. Its *leading coefficient* $\mathrm{lc}\,(f)$ is its leading coefficient with respect to $\mathrm{class}\,(f)$. A finite set of non-constant polynomials $G = \{g_1, \ldots, g_t\}$ in $k[X]$ is called a *triangular set* iff $\mathrm{class}\,(g_i) < \mathrm{class}\,(g_{i+1})$ for all $1 \le i < t$.

The procedure of *pseudo division* is a generalisation of univariate division with remainder to multivariate polynomials. For polynomials $f, g \in k[X]$ with $\mathrm{class}\,(g) = X_i$ we divide f by g over the univariate polynomial ring $k(X_1, \ldots, \widehat{X_i}, \ldots, X_n)[X_i]$ and multiply the resulting equation by a suitable power of $\mathrm{lc}\,(g)$ to obtain polynomial expressions. Thus, there exist polynomials $q, r \in k[X]$ and an integer $\alpha \in \mathbb{N}$ with

$$\mathrm{lc}\,(g)^\alpha f = qg + r, \tag{1}$$

where $\deg_{X_i} r < \deg_{X_i} g$ and $0 \le \alpha \le \deg_{X_i} f - \deg_{X_i} g + 1$. To make q and r unique one usually requires α to be minimal, but also any other sufficiently large choice of α is possible. For minimal α the *pseudo quotient* and *remainder* of f by g are denoted with $\mathrm{pquo}\,(f, g) := q$ resp. $\mathrm{prem}\,(f, g) := r$. For some other large enough α such that there exist q, r with (1), we denote the *modified pseudo quotient* and *remainder* by $\mathrm{pquo}_\alpha(f, g) := q$ resp. $\mathrm{prem}_\alpha(f, g) := r$.

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

$$f_t := f, \quad f_{i-1} := \mathrm{prem}\,(f_i, g_i) \quad \text{for} \quad 1 \le i \le t.$$

We denote by $\mathrm{prem}\,(f, G) := f_0$ the *pseudo remainder* of f by G. It follows easily from the defining equations that there exist polynomials $q_1, \ldots, q_t$ and integers $\alpha_1, \ldots, \alpha_t \in \mathbb{N}$ with

$$\mathrm{lc}\,(g_1)^{\alpha_1} \cdots \mathrm{lc}\,(g_t)^{\alpha_t} f = \sum_{i=1}^{t} q_i g_i + f_0. \tag{2}$$

Note that $\deg_{X_i} f_0 < \deg_{X_i} g_j$ for $X_i = \mathrm{class}\,(g_j)$. We define

$$\mathrm{Red}\,(G) := \{f \in k[X] \mid \mathrm{prem}\,(f, G) = 0\}.$$

The set $\mathrm{Red}\,(G)$ is in general not an ideal. We assign to G the *saturated ideal* $\mathrm{Sat}\,(G) := (G) : \Gamma^\infty$, where $\Gamma := \prod_i \mathrm{lc}\,(g_i)$. Equation (2) implies $\mathrm{Red}\,(G) \subseteq \mathrm{Sat}\,(G)$.

Before defining the fundamental concept of squarefree regular chains, we need to introduce some more notation. For an ideal $I \subseteq k[X]$ we denote by $\mathrm{Ass}\,(I)$ 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 $\mathrm{Ass}\,(I) = \{P_1, \ldots, P_s\}$. 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 1. Let $G = \{g_1, \ldots, g_t\}$ be a triangular set, and set $G_i := \{g_1, \ldots, g_i\}$ for $0 \le i \le t$. Then G is called a *squarefree regular chain* iff for all $0 \le i < t$ and each $P \in \mathrm{Ass}\,(\mathrm{Sat}\,(G_i))$ we have

(a) $\mathrm{lc}\,(g_{i+1}) \notin P$ and

(b) $g_{i+1}^{P_i}$ is squarefree in $K(P_i)[X_j]$, where $X_j = \mathrm{class}\,(g_{i+1})$ and $P_i := P \cap k[X_1, \ldots, X_{j-1}]$.

The following result was essentially proved in [25], see also [41, 1, 7].

Proposition 2.1. *Let G be a squarefree regular chain. Then $\mathrm{Sat}\,(G)$ coincides with $\mathrm{Red}\,(G)$ and is a proper unmixed radical ideal in $k[X]$.*

2.3.2 Decomposition of Radicals

The crucial complexity result on squarefree regular chains is the following theorem from Szántó [40].

Theorem 2.2. *Let the ideal $I \subseteq k[X]$ be given by generators $f_1, \ldots, f_r$ of degree $\le d$. Then there exist squarefree regular chains $G_1, \ldots, G_s$ with*

$$\sqrt{I} = \mathrm{Sat}\,(G_1) \cap \cdots \cap \mathrm{Sat}\,(G_s). \tag{3}$$

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 $(n \log d)^{\mathcal{O}(1)}$ ($d^{n^{\mathcal{O}(1)}}$).

2.4 Differential Forms

For the definition and basic properties of differentials and the de Rham complex we refer to [14]. For a commutative ring extension S/R we denote with $\Omega_{S/R}$ the *S-module of Kähler differentials* (or *differential forms*) of S over R. We have the *universal derivation* $\mathrm{d}\colon S \to \Omega_{S/R},\ f \mapsto \mathrm{d}f$. The module of differential forms extends to a complex of R-modules

$$\Omega^\bullet_{S/R} \colon 0 \longrightarrow S \xrightarrow{\mathrm{d}^0} \Omega^1_{S/R} \xrightarrow{\mathrm{d}^1} \Omega^2_{S/R} \xrightarrow{\mathrm{d}^2} \cdots,$$

where $\Omega^r_{S/R} := \wedge^r \Omega_{S/R}$ is the rth exterior power as S-modules, and the R-linear differential d^r is given by

$$\mathrm{d}^r \colon \Omega^r_{S/R} \to \Omega^{r+1}_{S/R}, \quad \mathrm{d}^r(f \mathrm{d}f_1 \wedge \cdots \wedge f_r) := \mathrm{d}f \wedge \mathrm{d}f_1 \wedge \cdots \wedge \mathrm{d}f_r.$$

This is the *de Rham complex* of S relative to R. An r-form ω is called *closed* if $\mathrm{d}\omega = 0$, and it is called *exact* if there exists an $(r-1)$-form η with $\mathrm{d}\eta = \omega$.

Since $\Omega_{k[X]/k}$ is free of rank n, the de Rham complex $\Omega^\bullet_{k[X]/k}$ terminates at the nth level, and $\Omega^r_{k[X]/k}$ is the free $k[X]$-module generated by the elements $\mathrm{d}X_{i_1} \wedge \cdots \wedge \mathrm{d}X_{i_r}$, $1 \le i_1 < \cdots < i_r \le n$. Similar statements hold for $\Omega^\bullet_{k(X)/k}$. One can show that for $r > 0$ the rth cohomology of the de Rham complex $\Omega^\bullet_{k[X]/k}$ vanishes. Obviously, its zeroth cohomology is isomorphic to k. By contrast, the cohomology of $\Omega^\bullet_{k(X)/k}$ is nontrivial. E.g., we will characterise closed 1-forms with rational coefficients over algebraically closed fields in §5.1.1.

3. CONNECTED COMPONENTS

For polynomials $f_1, \ldots, f_r \in k[X]$ denote by $\mathcal{Z}(f_1, \ldots, f_r)$ their common zero set in $\mathbb{A}^n := \mathbb{A}^n(\overline{k})$.

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

$\#\mathrm{CC}_k$ (*Counting connected components*) Given polynomials $f_1, \dots, f_r \in k[X_1, \dots, X_n]$, compute the number of connected components of $\mathcal{Z}(f_1, \dots, f_r)$.

THEOREM 3.1. *$\#\mathrm{CC}_k \in \mathrm{FPAR}_k$, $\#\mathrm{CC}_{\mathbb{Q}} \in \mathsf{FPSPACE}$.*

We remark that in [38] the $\mathsf{FPSPACE}$-hardness of $\#\mathrm{CC}_{\mathbb{Q}}$ was shown.

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 an algebraic variety, and set $K := \overline{k}$. We define the zeroth *algebraic de Rham cohomology* of V as the zeroth cohomology of the de Rham complex $\Omega^\bullet_{K[V]/K}$, where $K[V] = K[X]/I(V)$ denotes the coordinate ring of V:

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

This is the space of locally constant regular functions on V. Our algorithm relies on the following property of $H^0(V)$.

THEOREM 3.2. *Let $V \subseteq \mathbb{A}^n$ be the zero set of polynomials of degree at most d. Then V has $\dim H^0(V)$ connected components, and $H^0(V)$ has a basis given by polynomials of degree bounded by $d^{\mathcal{O}(n^2)}$.*

3.1.2 Proof of Theorem 3.2

The statement about the dimension of the zeroth de Rham cohomology can be rephrased as follows.

PROPOSITION 3.3. *Let $V = \bigcup_{i=1}^s V_i$ be the decomposition of V into connected components. Then $K[V] \simeq \prod_{i=1}^s K[V_i]$.*

This statement follows easily from the Chinese Remainder Theorem [29, Theorem 2.1] using Hilbert's Nullstellensatz. To connect this statement with the de Rham cohomology, we use the following well-known characterisation of direct products by idempotents [14, §0.1]. A commutative ring S is isomorphic to the direct product $\prod_{i=1}^s S_i$ of commutative rings S_i iff there exists a *complete set of pairwise orthogonal idempotents* $e_1, \dots, e_s$ with $S_i \simeq Se_i$. This means that $e_i^2 = e_i$, $e_i \neq 0$, $e_ie_j = 0$ for all $i \neq j$, and $e_1 + \dots + e_s = 1$. If moreover none of the e_i can be written as a sum of two nontrivial orthogonal idempotents, then $e_1, \dots, e_s$ will be called *maximal*. Such a system is unique up to permutation.

We construct the idempotents $e_1, \dots, e_s \in K[V]$ according to Proposition 3.3 explicitly in the following way. Since $V_i \cap V_j = \emptyset$ for $i \neq j$, Hilbert's Nullstellensatz implies that there are polynomials $\varphi_{ij} \in I(V_i)$ and $\psi_{ij} \in I(V_j)$ with $\varphi_{ij} + \psi_{ij} = 1$. Then one checks that $e_i := \prod_{j<i} \varphi_{ji} \cdot \prod_{j>i} \psi_{ij}$, $1 \leq i \leq s$, defines the desired idempotents.

Since $e_i \in K[V]$ takes the value 1 on V_i and vanishes on all other connected components, it is locally constant. And every locally constant function f can be written as $f = \sum_i \lambda_i e_i$ with $\lambda_i = f(x)$ for all $x \in V_i$. Thus $e_1, \dots, e_s$ is a basis of $H^0(V)$.

To obtain the degree bounds of Theorem 3.2, we first use [21, Proposition 3] to prove that V_i can be defined by polynomials of degree bounded by $\deg V_i \leq d^n$. By the effective Nullstellensatz [27] there exist φ_{ij}, ψ_{ij} of degree $\leq d^{n^2}$. From this the claimed bounds easily follow.

3.1.3 Algorithmic Idea

Theorem 3.2 reduces our problem to computing the dimension of $H^0(V)$. Furthermore, it yields a basis of this space of moderate degree. In particular, let $D = d^{\mathcal{O}(n^2)}$ and denote with $K[X]_{\leq D}$ the space of polynomials of degree bounded by D. Consider the map $\pi \colon K[X]_{\leq D} \hookrightarrow K[X] \twoheadrightarrow K[V]$, and let $Z := \pi^{-1}(H^0(V))$. Then $\pi|Z \colon Z \to H^0(V)$ is surjective by Theorem 3.2, and its kernel is $I(V) \cap Z$, hence

$$H^0(V) \simeq Z/(I(V) \cap Z). \tag{4}$$

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

3.2 Modified Pseudo Remainder

3.2.1 Definition and Basic Properties

The idea for the characterisation of $I(V)$ by a linear system is to use squarefree regular chains, based on the observation that equation (1) defining pseudo division is linear if one knows the exponent α in advance. As remarked in §2.3.1, instead of the choice of a minimal α, one can also take a fixed value for α to make the results unique. Recall that we write $\mathrm{prem}_\alpha(f, g)$ for the modified pseudo remainder with respect to α. By showing bounds for the exponents and degrees of the pseudo quotients and remainders one checks that the following choices for the exponents α_i will do.

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

$$f_t := f, \quad f_{i-1} := \mathrm{prem}_{\alpha_i}(f_i, g_i) \quad \text{for } 1 \leq i \leq t.$$

We define the *modified pseudo remainder* of f by G to be

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

LEMMA 3.4. *Let $D := nd(2\delta + 1)^t(2\delta)^t$. The map*

$$k[X]_{\leq d} \to k[X]_{\leq D}, \quad f \mapsto \mathrm{prem}_d(f, G)$$

is well-defined and k-linear.

Since the computation of the modified pseudo remainder of two polynomials reduces to solving a linear system of equations, the algorithms from §2.2 imply the following lemma.

LEMMA 3.5. *One can compute the matrix of the linear map of Lemma 3.4 with respect to the monomial bases in parallel time $(n \log d\delta)^{\mathcal{O}(1)}$ and sequential time $(d\delta)^{n^{\mathcal{O}(1)}}$.*

3.2.2 Describing Radicals by Linear Algebra

Modified pseudo division can be used to test membership to the saturated ideals of squarefree regular chains.

PROPOSITION 3.6. *Let $G = \{g_1, \dots, g_t\}$ be a squarefree regular chain with saturated ideal I. Then for any $d \in \mathbb{N}$*

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

The significance of Proposition 3.6 for us is that given the squarefree regular chain G, the property $\mathrm{prem}_d(f, G) = 0$ can be described by a linear system of equations in the coefficients of f. This system has size $(d\delta)^{n^{\mathcal{O}(1)}}$, and can be constructed in parallel polynomial time by Lemma 3.5.

3.3 Computing Differentials

In order to compute the dimension of the zeroth de Rham cohomology via the isomorphism (4), it remains to describe the space Z by a linear system.

The idea is to use squarefree regular chains in the following way. Assume for simplicity that $I = I(V)$ is the saturated ideal of a squarefree regular chain $G = \{g_1, \dots, g_t\}$. 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) shows that G generates I in the localisation $k[X]_\Gamma$. Furthermore we clearly have

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

where the set on the left hand side is Zariski-dense in V by [41, Corollary 2.4.7]. If f is locally constant on a Zariski-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 also 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 $g_1, \dots, g_t$.

To simplify notation we reorder and rename the variables in a way such that $X_1, \dots, X_m$ are the *free* variables, i.e., those which are *not* the class of some g_i, and the $Y_1, \dots, Y_t$ are the *dependent* variables with $Y_i = \operatorname{class}(g_i)$ for $1 \le i \le t$. Thus we are working in $k[X, Y] := k[X_1, \dots, X_m, Y_1, \dots, Y_t]$ with $m + t = n$. Furthermore we set $g := (g_1, \dots, g_t)^T$ 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 irreducible component of V. Note that this statement means that h is a non-zerodivisor on $k[V]$. Since Γ is no zerodivisor by [41], it remains to show that neither is Δ. The second statement of the following lemma, which follows immediately from the Jacobi criterion [28, VI, Satz 1.5], will be relevant later.

LEMMA 3.7. *The determinant Δ is a not a zero divisor on $k[V]$, hence $V \setminus \mathcal{Z}(\Delta)$ is Zariski-dense in V. Furthermore, V is smooth at each point in $V \setminus \mathcal{Z}(\Delta)$.*

Now we state the desired formula.

PROPOSITION 3.8. *Let $\Delta := \det(\frac{\partial g}{\partial Y})$ and $h := \Gamma\Delta$. Then*

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

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

$$\mathrm{d}\overline{f} = \sum_{i=1}^{m} \left(\frac{\partial f}{\partial X_i} - \frac{\partial f}{\partial Y} \left(\frac{\partial g}{\partial Y} \right)^{-1} \frac{\partial g}{\partial X_i} \right) \mathrm{d}\overline{X}_i. \qquad (5)$$

Note that we have abused notation in that the coefficients of the $\mathrm{d}\overline{X}_i$ in formula (5) are to be mapped into $k[V]_h$.

3.4 Proof of Theorem 3.1

Let $V = \mathcal{Z}(f_1, \dots, f_r) \subseteq \mathbb{A}^n$ with polynomials $f_i \in k[X]$ of degree bounded by d, and set $I := I(V)$. By Theorem 2.2 we can compute squarefree regular chains $G_1, \dots, G_s$ in $k[X]$ with saturated ideals $I_1, \dots, I_s$ such that $I = I_1 \cap \dots \cap I_s$. Let δ be an upper bound on the degree of the polynomials in all G_i.

By Proposition 3.6 we have for each $D \in \mathbb{N}$

$$I \cap K[X]_{\le D} = \{f \in K[X]_{\le D} \mid \bigwedge_{i=1}^{s} \operatorname{prem}_D(f, G_i) = 0\}, \quad (6)$$

and by Lemma 3.4 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 $(D\delta)^{n^{\mathcal{O}(1)}}$ by Lemma 3.5.

Now let $D = d^{\mathcal{O}(n^2)}$ be the degree bound from Theorem 3.2. According to (4), the number of connected components of V is given by

$$\dim H^0(V) = \dim Z - \dim(I \cap Z), \qquad (7)$$

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

To compute the dimension of Z we consider the case $s = 1$ first. We use Proposition 3.8, whose notation we adopt. Note that the coefficients of the $\mathrm{d}\overline{X}_i$ in (5) 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 its determinant Δ, which is a non-zerodivisor on $K[V]$ according to Lemma 3.7. Hence we can multiply equation (5) with Δ to obtain polynomial functions. Then we have for all $f \in K[X]_{\le D}$

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

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, since the matrix $\Delta \left(\frac{\partial g}{\partial Y}\right)^{-1}$ can be computed by plugging the matrix $\frac{\partial g}{\partial Y}$ into its characteristic polynomial, it can be computed with Berkowitz' algorithm [4]. A straightforward analysis shows that this algorithm runs in parallel time $(n \log \delta)^{\mathcal{O}(1)}$ and sequential time $\delta^{n^{\mathcal{O}(1)}}$.

Now, for general s, we have $V = V_1 \cup \dots \cup V_s$ 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 Z as the solution space of a linear system over k of size $s(D\delta)^{n^{\mathcal{O}(1)}}$. Using the bounds for δ and s of Theorem 2.2 one sees that it has size $d^{n^{\mathcal{O}(1)}}$. The combination of the systems for Z and (6) is a linear system of size $d^{n^{\mathcal{O}(1)}}$ for $I \cap Z$.

By the results of §2.2 one can compute the dimensions in (7) in parallel time $(n \log d)^{\mathcal{O}(1)}$ and sequential time $d^{n^{\mathcal{O}(1)}}$ over k.

4. IRREDUCIBLE COMPONENTS

The methods of §3 yield also a new algorithm for counting the irreducible components of a variety.

$\#\mathrm{IC}_k$ (*Counting irreducible components*) Given polynomials $f_1, \dots, f_r \in k[X_1, \dots, X_n]$, compute the number of absolutely irreducible components of $\mathcal{Z}(f_1, \dots, f_r)$.

The main result of this section is

THEOREM 4.1. *$\#\mathrm{IC}_k \in \mathrm{FPAR}_k$, $\#\mathrm{IC}_{\mathbb{Q}} \in \mathsf{FPSPACE}$.*

It is not difficult to see that $\#\mathrm{IC}_{\mathbb{C}}$ is $\#\mathrm{P}_{\mathbb{C}}$-hard. This is also valid in the bit model: $\#\mathrm{IC}_{\mathbb{Q}}$ is $\#\mathsf{P}$-hard or even GCC-hard. (For definitions of these counting complexity classes see [9].)

Open question. 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. [10] 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 $\#\mathsf{P}$.

4.1 Locally Constant Rational Functions

For a variety $V \subseteq \mathbb{A}^n$ let $R(V)$ denote the ring of *rational functions* on V. This 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.

Similarly to §3.1.2 we have $R(V) \simeq \prod_{i=1}^{s} R(V_i)$ where $V = V_1 \cup \dots \cup V_s$ is the decomposition of V into irreducible components, cf. [28, III, Satz 2.8]. Hence the number of irreducible components is the cardinality of a maximal complete set of orthogonal idempotents in $R(V)$.

We consider the space of locally constant rational functions on V, which we denote (by analogy) with

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

THEOREM 4.2. *Let $V \subseteq \mathbb{A}^n$ be the zero set of polynomials of degree at most d. Then V has $\dim H_r^0(V)$ irreducible components. Let furthermore h be a non-zerodivisor on $K[V]$ vanishing on the singular locus $\operatorname{Sing} V$ with $\deg h < d$. Then $H_r^0(V)$ has a basis of rational functions of the form f/h^N with $\max\{\deg f, N\} = d^{\mathcal{O}(n^2)}$.*

4.2 Proof of Theorem 4.1

Let $V = \mathcal{Z}(f_1, \dots, f_r)$ with polynomials f_i of degree $\le d$, and set $I := I(V)$. First we compute squarefree regular chains G_i with saturated ideals I_i such that $I = \bigcap_i I_i$. This decomposition can be redundant, i.e., an irreducible component of $\mathcal{Z}(I_i)$ may be contained in $\mathcal{Z}(I_j)$ with $j \neq i$. We compute an irredundant decomposition $I = \bigcap J_i$ as follows. We order the I_i by descending dimension. Then the ideal quotient $J_i := I_i : (I_1 \cap \dots \cap I_{i-1})$ is the ideal of the union V_i of all irreducible components of $\mathcal{Z}(I_i)$ not contained in some other $\mathcal{Z}(I_j)$ for $j < i$. By irredundancy the number of irreducible components of V is the sum of the numbers of components of all V_i.

To compute the number of components of V_i, let h_i be defined as in Proposition 3.8 for G_i. For $D, N \in \mathbb{N}$ consider the map $\varphi\colon K[X]_{\le D} \to K[V_i]_{h_i}$, $f \mapsto \overline{f}/\overline{h_i}^N$, and let $Z := \varphi^{-1}(H_r^0(V_i))$. For sufficiently large $D, N \le d^{n^{\mathcal{O}(1)}}$, the restriction $\varphi|Z\colon Z \to H_r^0(V_i)$ is surjective by Theorem 4.2, hence

$$H_r^0(V_i) \simeq Z/(J_i \cap Z).$$

Therefore, the number of irreducible components of V_i is given by $\dim H_r^0(V_i) = \dim Z - \dim(J_i \cap Z)$.

We can express Z as in §3.4 as the solution space of a linear system of equations of size $d^{n^{\mathcal{O}(1)}}$ and conclude by efficient parallel linear algebra.

5. FIXING PARAMETERS

5.1 Counting Irreducible Factors

The complexity of the following problem depends on the encoding of the input polynomial, so that we add superscripts to specify its encoding.

$\#\mathrm{IF}_k$ (*Counting irreducible factors*) Given a polynomial $f \in k[X_1, \dots, X_n]$, compute the number of its absolutely irreducible factors.

THEOREM 5.1. *$\#\mathrm{IF}_k^{(\mathrm{dense})} \in \mathrm{FNC}_k^2$, $\#\mathrm{IF}_{\mathbb{Q}}^{(\mathrm{dense})} \in \mathsf{FNC}^2$.*

This statement over $\mathbb{Q}$ was already shown in [2]. A new proof, working over any field k of characteristic zero and using differential forms, is provided in §5.1.1.

Note that Theorem 4.1 implies $\#\mathrm{IF}_{\mathbb{Q}}^{(\mathrm{slp})} \in \mathsf{FPSPACE}$. With regard to the optimality of this statement, we only know the following lower bound implied by [35].

PROPOSITION 5.2. *$\#\mathrm{IF}_{\mathbb{Q}}^{(\mathrm{slp})}$ is NP-hard with respect to polynomial time Turing reductions.*

Open question. Is $\#\mathrm{IF}_{\mathbb{Q}}^{(\mathrm{slp})}$ $\#\mathsf{P}$-hard?

5.1.1 Cohomology of a Hypersurface Complement

For $f \in k[X]$ we denote by $\mathbb{A}_f^n := \mathbb{A}^n \setminus \mathcal{Z}(f)$ the complement of the zero set of f. The ring of regular functions on $\mathbb{A}_f^n$ is given by the localisation $K[X]_f$ of the polynomial ring $K[X]$ at the multiplicatively closed subset consisting of powers of f. We consider the *first algebraic de Rham cohomology* $H^1(\mathbb{A}_f^n)$ of $\mathbb{A}_f^n$, which is defined as the first cohomology vector space of the de Rham complex of $K[X]_f$.

Note that logarithmic differentials $\frac{\mathrm{d}g}{g}$ are closed forms and behave additively on products, i.e., $\frac{\mathrm{d}(fg)}{fg} = \frac{\mathrm{d}f}{f} + \frac{\mathrm{d}g}{g}$.

The following is a refinement of a structure theorem for closed 1-forms in $\Omega_{K(X_1,X_2)/K}$ due to Ruppert [37]. Its usefulness for algorithmic purposes was first discovered by Gao [17].

THEOREM 5.3. *Let $f = \prod_{i=1}^{s} f_i^{e_i}$ be the factorisation of $f \in k[X]$ into pairwise coprime absolutely irreducible polynomials. Then $\frac{\mathrm{d}f_1}{f_1}, \dots, \frac{\mathrm{d}f_s}{f_s}$ induce a basis of $H^1(\mathbb{A}_f^n)$. In particular, the dimension of $H^1(\mathbb{A}_f^n)$ equals the number of absolutely irreducible factors of f.*

PROOF OF THEOREM 5.1. Let Z denote the space of the closed forms $\frac{1}{f}\sum_i g_i \mathrm{d}X_i$ with $\deg g_i < d$, and let B be the space of the exact forms $\mathrm{d}(g/f)$ where $\deg g < d+1$. The induced map $Z/B \to H^1(\mathbb{A}_f^n)$ is surjective by Theorem 5.3. One can show that each exact form of Z lies in B, hence the map is also injective. Thus $H^1(\mathbb{A}_f^n) \simeq Z/B$. Furthermore, Z is the solution space of a linear system over k of polynomial size. Similarly, B is the projection of the solution space of a linear system of polynomial size. Hence $\dim Z$ and $\dim B$ can both be computed in FNC_k^2 resp. FNC^2, cf. §2.2. □

5.2 Fixed Number of Equations

Here we consider the powerful slp encoding of polynomials together with a bound on the formal degree of the slp in unary. We denote the restriction of $\#\mathrm{IC}_k$ in this encoding to a fixed number r of equations by $\#\mathrm{IC}(r)_k^{(\text{d-slp})}$.

The main result of this section can be conveniently phrased in terms of the following randomised parallel complexity class.

Definition 3. We denote by FRNC the class of all functions $\varphi\colon \{0,1\}^\infty \to \{0,1\}^\infty$ such that there exists a polynomial p, a constant $0 < q < 1$, and a logspace-uniform family $(\mathcal{C}_n)_{n\in\mathbb{N}}$ of Boolean circuits of polynomial size and polylogarithmic depth, where $\mathcal{C}_n$ computes the function $\psi_n\colon \{0,1\}^n \times \{0,1\}^{p(n)} \to \{0,1\}^\infty$, such that for all $x \in \{0,1\}^n$

$$P\left(\{y \in \{0,1\}^{p(n)} | \varphi(x) \neq \psi_n(x,y)\}\right) \leq q^n.$$

Theorem 5.4. *We have* $\#\mathrm{IC}(r)_{\mathbb{Q}}^{(\text{d-slp})} \in \mathsf{FRNC}$.

The key idea of the proof is the reduction to a constant number of variables by a Bertini type argument formally expressed in Proposition 5.5 below (its proof is sketched in §5.2.1). This can be naturally captured by the notion of generic parsimonious reductions between counting problems $\varphi, \psi\colon \mathbb{C}^\infty \to \overline{\mathbb{N}}$ defined in [11].

Proposition 5.5. *There is a generic parsimonious reduction from the projective version of* $\#\mathrm{IC}(r)_{\mathbb{C}}^{(\text{d-slp})}$ *to its restriction to the fixed ambient space* $\mathbb{P}^{r+1}$.

Theorem 5.4 follows with the help of a new transfer theorem saying that if there exists a generic parsimonious reduction (π, R) from φ to ψ, and if $\pi^{\mathbb{Q}}$ and $\psi^{\mathbb{Q}}$ are in FNC, then $\varphi^{\mathbb{Q}}$ is in FRNC. Here $\varphi^{\mathbb{Q}}$ denotes the restriction of φ to rational inputs.

We remark that in the Blum-Shub-Smale model [5] it is possible to avoid randomisation at the price of losing good parallelisation: we can show that $\#\mathrm{IC}(r)_{\mathbb{C}}^{(\text{d-slp})}$ is computable in (deterministic) polynomial time over $\mathbb{C}$.

5.2.1 *An explicit genericity condition for Bertini*

Bertini's Theorem [34, Corollary 4.18] states that the intersection of an irreducible variety of dimension m with a generic linear subspace of codimension $m-1$ is an irreducible curve. We generalise this statement to reducible varieties and formulate an explicit genericity condition on the linear space under which the conclusion holds.

Let us fix some notation. Denote with $\mathbb{G}_s(\mathbb{P}^n)$ the *Grassmannian* variety of all s-dimensional linear subspaces of $\mathbb{P}^n$. If $M \in \mathbb{G}_s(\mathbb{P}^n)$ is defined by the linear forms $\alpha_1, \ldots, \alpha_{n-s}$, the *projection* $p_M\colon \mathbb{P}^n \setminus M \to \mathbb{P}^{n-s-1}$ *centered at* M is defined by $x \mapsto (\alpha_1(x) : \cdots : \alpha_{n-s}(x))$. We say that the variety $V \subseteq \mathbb{P}^n$ is *transversal* to $L \in \mathbb{G}_s(\mathbb{P}^n)$ and write $V \pitchfork L$ iff $\dim_x(V \cap L) = \dim_x V + s - n$ for all $x \in V \cap L$, and $\dim(T_xV \cap T_xL) = \dim T_xV + s - n$ for almost all smooth points $x \in V \cap L$. ($\dim_x$ denotes the local dimension and T_xV the tangent space of V at x.)

Now let V be m-equidimensional, and $M \in \mathbb{G}_{n-m-1}(\mathbb{P}^n)$ with $V \cap M = \emptyset$. Denote with $p\colon V \to \mathbb{P}^m$ the restriction of p_M to V. We define the set of branching values

$$B_M(V) := p\big(\mathrm{Sing}\,(V) \cup \{x \in V \mid d_xp \text{ not surjective}\}\big),$$

where d_xp denotes the differential of p. The set $B_M(V)$ is a proper subvariety of $\mathbb{P}^m$.

If $V = \mathcal{Z}(f_1, \ldots, f_r)$ is not equidimensional, let $V = V_{n-r} \cup \cdots \cup V_n$ its decomposition into equidimensional components, where $\dim V_m = m$. Our genericity condition for $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ is

$$\bigwedge_{m=n-r}^{n} \big(\exists M \in \mathbb{G}_{n-m-1}(L)\ \exists \ell \in \mathbb{G}_1(p_M(L))\colon \\ M \cap V_m = \emptyset \ \wedge\ \ell \pitchfork B_M(V_m)\big). \qquad (8)$$

We can show that almost all $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ satisfy condition (8), and in this case L is transversal to V.

Using ideas from [34] we can prove the following subtle technical statement.

Proposition 5.6. *Let* $V \subseteq \mathbb{P}^n$ *be a variety defined by homogeneous polynomials* $f_1, \ldots, f_r$. *Then for each* $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ *satisfying condition* (8) *the variety* $V \cap L$ *has the same number of irreducible components as* V.

In order to prove that $(V, L) \mapsto V \cap L$ is a generic parsimonious reduction it remains to show that, given V and L, one can check the genericity condition (8) in the constant free polynomial hierarchy over $\mathbb{R}$ (cf. [11]). This can be verified similarly as the transversality statements in [9].

6. ACKNOWLEDGMENTS

We thank the anonymous referees for their valuable comments and pointing us to further literature on triangular sets.

7. REFERENCES

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

[2] C. Bajaj, J. Canny, R. Garrity, and J. Warren. Factoring rational polynomials over the complexes. In *ISSAC '89: Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation*, pages 81–90, New York, NY, USA, 1989. ACM Press.

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

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

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

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

[7] F. Boulier, F. Lemaire, and M. Moreno Maza. Well known theorems on triangular systems and the D5 principle. In *Proc. of* Transgressive Computing 2006, Granada, Spain, 2006.

[8] P. Bürgisser and F. Cucker. Variations by complexity theorists on three themes of Euler, Bézout, Betti, and Poincaré. In J. Krajíček, editor, *Complexity of computations and proofs*, volume 13 of *Quaderni di*

Matematica [Mathematics Series], pages 73–152. Department of Mathematics, Seconda Università di Napoli, Caserta, 2004.

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

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

[11] P. Bürgisser, F. Cucker, and M. Lotz. Counting complexity classes for numeric computations III: Complex projective sets. *Foundations of Computational Mathematics*, 5(4):351–387, 2005.

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

[13] A. Chistov. 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, 1984. English translation: J. Sov. Math. 34(1986).

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

[15] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110:207–235, 1992.

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

[17] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comput.*, 72(242):801–822, 2003.

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

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

[20] D. Grigoriev. 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, 1984. English translation: J. Sov. Math. 34(1986).

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

[22] J. Heintz and M. Sieveking. Absolute primality of polynomials is decidable in random polynomial time in the number of variables. In *Proceedings of the 8th Colloquium on Automata, Languages and Programming*, pages 16–28, London, UK, 1981. Springer-Verlag.

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

[24] M. Kalkbrener. Prime decomposition of radicals in polynomial rings. *J. Symb. Comp.*, 18:365–372, 1994.

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

[26] E. Kaltofen. Fast parallel absolute irreducibility testing. *JSC*, 1(1):57–67, 1985. Misprint corrections: *J. Symbolic Comput.* vol. 9, p. 320 (1989).

[27] J. Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.

[28] E. Kunz. *Einführung in die kommutative Algebra und algebraische Geometrie*, volume 46 of *Vieweg-Studium: Aufbaukurs Mathematik*. Vieweg, Wiesbaden, 1979.

[29] S. Lang. *Algebra*. Addison-Wesley, second edition, 1984.

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

[31] G. Matera and J. M. T. Torres. The space complexity of elimination theory: Upper bounds. In *FoCM '97: Selected papers of a Conference on Foundations of computational mathematics*, pages 267–276, New York, NY, USA, 1997. Springer-Verlag New York, Inc.

[32] E. W. Mayr. Some complexity results for polynomial ideals. *J. Compl.*, 13(3):303–325, 1997.

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

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

[35] D. A. Plaisted. Sparse complex polynomials and polynomial reducibility. *JCSS*, 14:210–221, 1977.

[36] J. Ritt. *Differential Algebra*. Americal Mathematical Society, 1950.

[37] W. Ruppert. Reduzibilität ebener Kurven. *J. Reine Angew. Math.*, 369:167–191, 1986.

[38] P. Scheiblechner. On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety. To appear in J. Compl., 2007.

[39] I. R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, Berlin Heidelberg New York, 1972.

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

[41] Á. Szántó. Computation with polynomial systems. PhD Thesis, 1999.

[42] J. von zur Gathen. Parallel arithmetic computations: a survey. In *MFOCS86*, number 233 in LNCS, pages 93–112. SV, 1986.

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

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