COUNTING IRREDUCIBLE COMPONENTS OF COMPLEX ALGEBRAIC VARIETIES

Peter Bürgisser and Peter Scheiblechner

Abstract. We present an algorithm for counting the irreducible components of a complex algebraic variety defined by a fixed number of polynomials encoded as straight-line programs (slps). It runs in polynomial time in the Blum-Shub-Smale (BSS) model and in randomized parallel polylogarithmic time in the Turing model, both measured in the lengths and degrees of the slps. Our algorithm is obtained from an explicit version of Bertini's theorem. For its analysis we further develop a general complexity theoretic framework appropriate for algorithms in algebraic geometry.

Keywords. algebraic varieties, complexity, irreducible components, Bertini's theorem

Subject classification. 14Q15, 68Q15, 68Q25, 68W30, 68W40

1. Introduction

Finding the unique decomposition of a polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ as a product of irreducible factors is the problem of *factorization*. A natural extension is the problem of finding the irreducible components of the complex zero set of given polynomials $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$. As a prototype of the latter we focus on the problem of counting the irreducible components. The goal of this paper is to describe a very efficient algorithm for counting these, that even allows the input polynomials f_i to be given in the powerful datastructure of straight-line programs (slps). For a fixed number r of polynomials with integer coefficients, our algorithm works in the Turing model in randomized parallel polylogarithmic time in the lengths and the formal degrees of the given slps.

In the following let us place this result into the context of the rather large body of work on factorization. First of all, one has to distinguish between the problems of *rational* and *absolute factorization*. The first asks for the rational irreducible factors of a given $f \in \mathbb{Q}[X_1, \ldots, X_n]$, while the latter seeks the factorization into irreducible polynomials over the algebraic closure of $\mathbb{Q}$. For the latter, one has to agree on how to represent these factors. In this paper,

we are only concerned with the absolute factorization and its generalization to several polynomials.

1.1. Rational Factorization of Polynomials. This is a widely studied problem and we refer to the surveys by Kaltofen (1990, 1992) for information and references. A major result due to Kaltofen (1989) is an algorithm computing the rational factorization of a multivariate rational polynomial encoded as an slp that works in randomized polynomial time in the formal degree and the length of the slp. If the formal degree of the slp is not included in the input size, then the problem becomes at least NP-hard (Plaisted 1977). We note that it is still unknown whether the rational factorization of a univariate rational polynomial (even in dense representation) can be computed in parallel polylogarithmic time, see von zur Gathen (1984). A disturbing fact is that we do not even know whether the gcd of integers can be computed in parallel polylogarithmic time.

1.2. Absolute Factorization of Polynomials. Kaltofen (1985b) was the first to present an efficient parallel algorithm for testing absolute irreducibility. Bajaj *et al.* (1993) described a geometric-topological algorithm for computing the number and degrees of the absolute factors of a rational polynomial in parallel polylogarithmic time. An algebraic algorithm for counting absolute factors (working over $\mathbb{C}$) was given by Bürgisser & Scheiblechner (2007), based on Gao (2003). For more information on absolute factorization we refer to Chèze & Galligo (2005).

1.3. Irreducible Components. The first single exponential time algorithms (in the bit model) for computing both the irreducible and absolutely irreducible components of an algebraic variety are due to (Chistov 1984; Grigoriev 1984). Giusti & Heintz (1991) succeeded in giving efficient parallel algorithms, but only for the equidimensional decomposition due to the lack of efficient parallel factorization procedures. Bürgisser & Scheiblechner (2007, 2008) used quite different techniques (algebraic differential forms, triangular sets) to design an algorithm for counting the irreducible components in parallel polynomial time. This is used as a basic building block for the algorithms in the present paper. Scheiblechner (2007b) showed that the related problem of counting the connected components of a complex algebraic variety is PSPACE-hard. It is unclear whether this extends to irreducible components.

1.4. Main Result. For fixed $r \in \mathbb{N}$ consider the following problem $\#\mathrm{IC}(r)_{\mathbb{C}}$: Given $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$ encoded as slps and an upper bound on their

formal degrees in unary, compute the number of irreducible components of their zero set $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{C}^n$. We shall denote with $\#\mathrm{IC}(r)_{\mathbb{Z}}$ the restriction of this problem to polynomials f_i with integer coefficients. The complexity class of functions computable in polynomial time in the Blum-Shub-Smale (BSS) model over $\mathbb{C}$ is denoted $\mathrm{FP}_{\mathbb{C}}$. The main result of this paper is

THEOREM 1.1. *We have* $\#\mathrm{IC}(r)_{\mathbb{C}} \in \mathrm{FP}_{\mathbb{C}}$ *and* $\#\mathrm{IC}(r)_{\mathbb{Z}} \in \mathsf{FRNC}$.

Here, FRNC is a new complexity class, which can be seen as a randomized functional version of the class NC, see Section 3.3 for the definition. In a way this result can be interpreted as a generalization of Kaltofen's 1989 result from one polynomial to a constant number of them. However, we consider absolute factorization and in turn achieve good parallelization.

1.5. Effective Bertini Theorem. The key idea of all efficient algorithms for factoring multivariate polynomials is a reduction to a fixed number of variables. The mathematical result allowing this is an effective version of *Hilbert's irreducibility theorem* stating that an irreducible polynomial remains irreducible when making a generic linear substitution to a bivariate polynomial. Von zur Gathen (1985); Kaltofen (1985a) provide effective versions of this theorem that allow to analyze randomized algorithms based on that.

The analogue of Hilbert's irreducibility theorem in our situation is *Bertini's theorem* stating that the intersection of an irreducible variety V of codimension r with a generic linear subspace L of dimension $r+1$ remains irreducible. In Theorem 5.5 we provide an effective version of Bertini's theorem that gives an explicit condition for a "good subspace" L. This can be applied for reducing to a fixed number $r+1$ of variables. We note that the algorithm of Bürgisser & Scheiblechner (2008) works a fixed number of variables in parallel polylogarithmic time.

In order to analyze the resulting algorithm we use the complexity theoretic framework developed in Bürgisser *et al.* (2005) for problems from algebraic geometry, in particular the concept of *generic parsimonious reductions*, cf. Section 3.1. In fact, our explicit Bertini theorem yields a generic parsimonious reduction to the case of a fixed dimension of the ambient space. A fundamental result from Bürgisser *et al.* (2005) says that generic parsimonious reductions always yield polynomial time Turing reductions in the BSS model, which leads to the first assertion of Theorem 1.1.

As an analogue for the bit model we define in Section 3.2 the new notion of *randomized parsimonious reductions*. The second assertion of Theorem 1.1 then follows with the help of a new transfer principle (Theorem 3.8) stating that

a generic parsimonious reduction between two counting problems (computable in parallel polylogarithmic time) yields a randomized parsimonious reduction between their discrete versions.

1.6. Outline. First we fix notations and collect the necessary prerequisites in Section 2. In Section 3 we define randomized parsimonious reductions that work efficiently in parallel and we prove general transfer results from the BSS to the Boolean model. Section 4 outlines the proof Theorem 1.1. The explicit genericity condition for Bertini's Theorem is formulated in Section 5. Finally, Section 6 contains the proofs of the required results from algebraic geometry.

2. Preliminaries

2.1. Algebraic Geometry. As general references for basic algebraic geometry we refer to Harris (1992); Mumford (1976).

2.1.1. Basic Terminology and Notation. Let $\mathbb{C}[X] := \mathbb{C}[X_1, \dots, X_n]$ denote the polynomial ring and $\mathbb{A}^n := \mathbb{A}^n(\mathbb{C})$ the affine space over $\mathbb{C}$. An *affine variety* V is defined as the zero set

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

of finitely many polynomials $f_1 \dots, f_r \in \mathbb{C}[X]$. In the projective case we set $\mathbb{C}[X] := \mathbb{C}[X_0, \dots, X_n]$ and denote by $\mathbb{P}^n := \mathbb{P}^n(\mathbb{C})$ the projective space over $\mathbb{C}$. The projective zero set of homogeneous polynomials $f_1 \dots, f_r \in \mathbb{C}[X]$ is called a *projective variety* and it is also denoted by $\mathcal{Z}(f_1 \dots, f_r) \subseteq \mathbb{P}^n$. The *(vanishing) ideal* $I(V)$ of an affine variety V is $I(V) := \{f \in \mathbb{C}[X] \mid \forall x \in V\, f(x) = 0\}$.

The varieties form the closed sets of a topology on $\mathbb{A}^n$ ($\mathbb{P}^n$), the *Zariski topology*. A subset of $\mathbb{A}^n$ ($\mathbb{P}^n$) is called *irreducible* iff it is not the union of two proper closed subsets. Each variety V admits an (up to order) unique irredundant decomposition into irreducible varieties V_i, i.e., $V = V_1 \cup \cdots \cup V_t$ with $V_i \nsubseteq V_j$ for all $1 \le i \ne j \le t$. This will be called the *irreducible decomposition*, and the V_i the *irreducible components* of V. We will write $\#\mathrm{ic}(V)$ for the number of irreducible components of V. On $\mathbb{A}^n$ there exists a second natural topology induced by the Euclidean norm. It induces a quotient topology on $\mathbb{P}^n$ with respect to the natural projection $\pi\colon \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n$. We call both of these topologies the *Euclidean topology*. By (Mumford 1976, (4.16)) a non-empty Zariski-open subset of an irreducible variety is connected with respect to the Euclidean topology. An easy consequence of this is that for constructible sets (i.e., Boolean combinations of varieties) Zariski-connectedness is equivalent to Euclidean-connectedness. By (Mumford 1976, (2.33)) a Zariski-open subset

of an irreducible variety is dense in the Euclidean topology. This implies that the closures of a constructible set with respect to the two topologies coincide.

2.1.2. Dimension, Tangent Space, and Smoothness. The dimension $\dim V$ of an algebraic variety V is the maximal (Krull) dimension of its irreducible components. A variety all of whose irreducible components have the same dimension m is called *(m-)equidimensional*. By grouping the irreducible components of equal dimension one obtains the *equidimensional decomposition* $V = V_{(0)} \cup \cdots \cup V_{(n)}$, where $V_{(m)}$ is either m-equidimensional or empty. For $x \in \mathbb{A}^n$ ($\mathbb{P}^n$) we define the *local dimension* $\dim_x V$ as the dimension of the union of all irreducible components of V containing x. We will frequently use the argument that an irreducible subset $Z \subseteq V$ with $x \in Z$ and $\dim Z = \dim_x V$ must be an irreducible component of V. The Dimension Theorem (Mumford 1976, (3.28)) states that for two subvarieties V, W of $\mathbb{A}^n$ or $\mathbb{P}^n$, each irreducible component Z of $V \cap W$ satisfies $\dim Z \geq \dim V + \dim W - n$. Furthermore, if $V, W \subseteq \mathbb{P}^n$ and $\dim V + \dim W \geq n$, then $V \cap W \neq \emptyset$ (Mumford 1976, (3.30)).

The *differential* of a polynomial $f \in \mathbb{C}[X]$ at $x \in \mathbb{A}^n$ is the linear function $d_x f \colon \mathbb{C}^n \to \mathbb{C}$ 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

$$T_x V := \{v \in \mathbb{C}^n \mid \forall f \in I(V)\ d_x f(v) = 0\} \subseteq \mathbb{C}^n.$$

With generators $f_1, \ldots, f_r$ of the ideal $I(V)$ we have $T_x V = \mathcal{Z}(d_x f_1, \ldots, d_x f_r)$.

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

Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine varieties. A map $f \colon V \to W$ is called *regular* iff there exist polynomials $f_1, \ldots, f_m$ such that $f(x) = (f_1(x), \ldots, f_m(x))$ for all $x \in V$. The differential $d_x f \colon T_x V \to T_x W$ of f is induced by the differentials of the polynomials f_i. Following Mumford (1976) we call f *smooth* at a point $x \in V$ iff x and $f(x)$ are smooth points of V and W respectively, and its differential $d_x f \colon T_x V \to T_{f(x)} W$ at x is surjective. We call f smooth *over* $y \in W$ iff f is smooth at all $x \in f^{-1}(y)$.

Since all these definitions are local, they also apply to projective varieties $V \subseteq \mathbb{P}^n$ working in the *affine charts* $U_i = V \cap \{X_i \neq 0\}$, $0 \leq i \leq n$. In this case we also use another version of the tangent space. For its definition we denote by V^c the *affine cone* of V, i.e., $V^c = \pi^{-1}(V) \cup \{0\}$, where $\pi \colon \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ is the natural projection. The *projective tangent space* $\mathbb{T}_x V$ at $x \in V$ is the projective linear subspace of $\mathbb{P}^n$ corresponding to the Zariski tangent space $T_v V^c$, where $v \in \pi^{-1}(x)$ (Harris 1992, pp. 181ff.).

Now let $f\colon V \to W$ be a surjective regular map between equidimensional varieties of the same dimension. Assume that f has finite fibers, i.e., for all $y \in W$ the set $f^{-1}(y)$ is finite. Let $B := \{y \in W \mid f \text{ not smooth over } y\}$ the set of *branching values* of f. Then by the Inverse Function Theorem, f is on $f^{-1}(W \setminus B)$ a local diffeomorphism, hence f restricts to a topological covering map $f^{-1}(W \setminus B) \to W \setminus B$ (cf. Section 2.2). If furthermore $P \subseteq W$ is an equidimensional subvariety, then f is transversal to $\operatorname{Reg}(P) \setminus B$ (i.e., $\operatorname{im} d_x f + T_{f(x)}P = T_{f(x)}W$ for all $x \in f^{-1}(\operatorname{Reg}(P) \setminus B)$), hence $f^{-1}(\operatorname{Reg}(P) \setminus B)$ is a submanifold of $f^{-1}(W \setminus B)$ by (Bredon 1997, Theorem 15.2). The same argument as above shows that f restricts further to a covering $f^{-1}(\operatorname{Reg}(P) \setminus B) \to \operatorname{Reg}(P) \setminus B$.

2.1.3. Blow-Ups. We will need some elementary facts about blow-ups, see Harris (1992, pp. 80 ff.) and Mumford (1976, p. 32 and 73 ff.). Let $V \subseteq \mathbb{P}^n$ be a variety and $y = (y_0 : \cdots : y_n) \in V$. Assume w.l.o.g. $y_0 \neq 0$. Then the map $p_y\colon \mathbb{P}^n \setminus \{y\} \to \mathbb{P}^{n-1}$, $(x_0 : \cdots : x_n) \mapsto (y_0x_1 - y_1x_0 : \cdots : y_0x_n - y_nx_0)$ is called a *projection centered at* y. Let $\widetilde{V}$ be the closure of the graph Γ of $p_y|V \setminus \{y\}$ in $V \times \mathbb{P}^{n-1}$. The restriction $\pi\colon \widetilde{V} \to V$ of the projection onto the first component is called the *blow-up* of V at y. The inverse image $E := \pi^{-1}(y)$ is called the *exceptional fiber* of the blow-up. It is easy to see that $\widetilde{V}$ is the disjoint union of Γ and E. It follows that π restricts to a homeomorphism $\widetilde{V} \setminus E \to V \setminus \{y\}$, whose inverse is given by $x \mapsto (x, p_y(x))$ for $x \in V \setminus \{y\}$. Furthermore, the complement $\widetilde{V} \setminus E = \Gamma$ is dense in $\widetilde{V}$. If V is irreducible, so is $V \setminus \{y\}$. Hence $\widetilde{V} \setminus E$ is irreducible and thus its closure $\widetilde{V}$ as well. In general, we have $\#\mathrm{ic}(V) = \#\mathrm{ic}(\widetilde{V})$.

To visualize the blow-up at a smooth point, we first consider the case $V = \mathbb{P}^n$. Then, denoting for $z \in \mathbb{P}^{n-1}$ by ℓ_z the line $p_y^{-1}(z) \cup \{y\}$ in $\mathbb{P}^n$, the blow-up becomes $\widetilde{\mathbb{P}}^n = \{(x, z) \in \mathbb{P}^n \times \mathbb{P}^{n-1} \mid x \in \ell_z\}$ with exceptional fiber $E = \{y\} \times \mathbb{P}^{n-1}$. This means that $\widetilde{\mathbb{P}}^n$ is obtained from $\mathbb{P}^n$ by replacing y with a copy E of $\mathbb{P}^{n-1}$ in such a way that approaching E from different directions one ends up in different points. Thus $\widetilde{\mathbb{P}}^n$ looks like a spiral staircase winding around E. Harris (1992, p. 83) also gives an analytic construction of the blow-up of a complex manifold and shows that it is again a manifold. Furthermore, the blow-up is locally functorial in the sense that a biholomorphic map $f\colon U \to U$ of a neighborhood U of y with $f(y) = y$ lifts to a biholomorphic map $\widetilde{f}\colon \widetilde{U} \to \widetilde{U}$. Now a variety V of dimension m is near a smooth point y a manifold, hence $\widetilde{V}$ is smooth in all point of E, where it looks locally like $\widetilde{\mathbb{P}}^m$.

2.1.4. Grassmannians and Degree. The linear subspaces of $\mathbb{P}^n$ of dimension s form an irreducible projective variety $\mathbb{G}_s(\mathbb{P}^n)$ of dimension $(s+1)(n-s)$ embedded in $\mathbb{P}^{\binom{n+1}{s+1}-1}$ (Harris 1992, Lecture 6). This variety is called the *Grassmannian*. For a linear subspace $L \subseteq \mathbb{P}^n$ we also use the notation $\mathbb{G}_s(L)$ with the obvious meaning. We say that a property holds for *almost all* or *generic* $x \in V$ iff there exists an open dense subset $U \subseteq V$ such that the property holds for all $x \in U$. The degree $\deg V$ of an irreducible projective variety V of dimension m is defined as the cardinality of $V \cap L$ for a generic $L \in \mathbb{G}_{n-m}(\mathbb{P}^n)$, see (Mumford 1976, §5A) or (Harris 1992, Lecture 18). We define the degree $\deg V$ of a reducible variety V to be the sum of the degrees of *all* irreducible components of V.

Bézout's Theorem implies a well-known bound on the degree of a variety in terms of the degrees of its defining polynomials (cf. Scheiblechner (2007a)). Let $V \subseteq \mathbb{A}^n$ ($\mathbb{P}^n$) be a variety defined by (homogeneous) polynomials of degree at most d. Then $\deg V \leq d^n$. An obvious but important observation is that the number of irreducible components of V is also bounded by d^n.

2.2. Topology. We will use some topological arguments concerning coverings, fibrations, and fiber bundles. Algebraic varieties with the Euclidean topology are locally conic (Dimca 1992, Theorem (1.5.1)). It follows that they are locally contractible, paracompact, and Hausdorff. In this section all maps are assumed to be continuous and space means topological space.

A *covering* is a map $p\colon T \to B$ with the property that each $b \in B$ has an open neighborhood U such that $p^{-1}(U)$ is the disjoint union of open subsets of T each of which p maps homeomorphically onto U. Coverings have the important *path lifting property*: Given a path $c\colon [0,1] \to B$ and $e \in T$ with $p(e) = c(0)$, there exists a path $\widetilde{c}\colon [0,1] \to T$ with $\widetilde{c}(0) = e$ and $c = p \circ \widetilde{c}$. This follows from the fact that coverings are fibrations (see below). If B is connected, then $p\colon T \to B$ is a covering iff there exists a discrete space D such that each $b \in B$ has an open neighborhood U and a homeomorphism $\varphi\colon p^{-1}(U) \to U \times D$ with $\mathrm{pr}_1 \circ \varphi = p$. As a generalization one obtains the definition of a *fiber bundle* by replacing the discrete space D by an arbitrary space F. Since all fibers $p^{-1}(b)$ of a fiber bundle $p\colon T \to B$ are homeomorphic to F, it is called the *fiber* of p. The simplest example of a fiber bundle is the *trivial* or *product bundle* $\mathrm{pr}_1\colon B \times F \to B$. In this sense one says that fiber bundles are *locally trivial* and can be seen as twisted products. A more flexible homotopy-theoretic generalization of fiber bundles are fibrations. A *fibration* is a map $p\colon T \to B$ which has the *homotopy lifting property* with respect to all spaces X. This means that for all maps $\widetilde{f}\colon X \to T$ and *homotopies* $H\colon X \times [0,1] \to B$,

$(x,t) \mapsto H_t(x)$, with $H_0 = p \circ \widetilde{f}$ there exists a homotopy $\widetilde{H}\colon X \times [0,1] \to T$ with $\widetilde{H}_0 = \widetilde{f}$ and $H = p \circ \widetilde{H}$. By (Spanier 1966, Theorem 2.2.3) coverings are fibrations. More generally, fiber bundles over paracompact and Hausdorff base spaces are fibrations (Spanier 1966, Corollary 2.7.14). Fibrations are in a homotopy-theoretic sense locally trivial. Let $p_i\colon T_i \to B$, $i \in \{1,2\}$, be two fibrations. A map $f\colon T_1 \to T_2$ is called *fiber-preserving* iff $p_1 = p_2 \circ f$. A fiber-preserving map $f\colon T_1 \to T_2$ is called *fiber homotopy equivalence* iff there exists a fiber-preserving map $g\colon T_2 \to T_1$ such that $f \circ g$ and $g \circ f$ are both homotopic to the identity via homotopies H such that H_t is fiber-preserving for all t. It follows from (Spanier 1966, Corollary 2.8.15) that fibrations over locally contractible base spaces are locally fiber homotopy equivalent to a trivial fibration. In particular, any two fibers of a fibration over a path-connected base space are homotopy equivalent (Spanier 1966, Corollary 2.8.13). One advantage of working with fibrations is that the composition of fibrations is a fibration (Spanier 1966, Theorem 2.2.6). This statement is false for fiber bundles or coverings (Spanier 1966, Example 2.2.8). Later we will use the easy to see argument that if $f\colon X \to Y$ is a homotopy equivalence and $Z \subseteq Y$ is a path component (i.e., a maximal path connected subspace), then $f^{-1}(Z)$ is a path component of X.

2.3. Complexity Theory.

2.3.1. Models of Computation. Our model of computation is that of algebraic circuits, cf. Blum *et al.* (1998); von zur Gathen (1986). Let k be a field. 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. An algebraic circuit containing only the constants 0 and 1 is called *constant-free*. A circuit without division nodes is called *division-free*.

We call a division-free algebraic circuit without sign nodes an *arithmetic circuit* or *straight-line program* (*slp* for short). We note that the usual definition of straight-line programs as a *sequence* of arithmetic instructions is essentially equivalent to ours. Detailed information on slps can be found in Bürgisser *et al.* (1997). We define the *formal degree* $\deg \mathcal{C}$ of an slp $\mathcal{C}$ by assigning the degree 1 to constant and input nodes. The degree of an arithmetic node from $\{+,-\}$ ($\{\times,/\}$) is the maximum (sum) of the degrees of its parents. The degree of an output node is the degree of its parent. The degree of the circuit $\mathcal{C}$ is then defined as the maximal degree of its nodes. It is clear that the degree of a polynomial computed by an slp is bounded by its formal degree. Furthermore, the formal degree also controls the bit-size of the computation of an slp on

integer inputs. In particular, the bit-size of the output of an slp $\mathcal{C}$ of depth t on inputs of bit-size at most ℓ is at most $\mathcal{O}(\ell t \deg \mathcal{C})$.

2.3.2. Complexity Classes. 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 $f|k^n$. In the case $d(n) = (\log n)^{\mathcal{O}(1)}$ we require logspace-uniformity. 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). A function is called computable in *polynomial time* iff it can be computed in sequential time $n^{\mathcal{O}(1)}$. The class FP_k consists of all functions computable in polynomial time.

The decisional version $\mathscr{C}$ of one of the above functional classes $\mathrm{F}\mathscr{C}$ is defined as the set of all languages $A \subseteq k^\infty$ whose characteristic function lies in $\mathrm{F}\mathscr{C}$.

Next we define the polynomial hierarchy. For $m \in \mathbb{N}$ define Σ_k^m to be the class of all languages $A \subseteq k^\infty$ such that there exist polynomials $p_1, \ldots, p_m$ and a language $B \in \mathrm{P}_k$ with

$$x \in A \iff Q_1 y_1 \in k^{p_1(n)} \cdots Q_m y_m \in k^{p_m(n)} (x, y_1, \ldots, y_m) \in B,$$

for all $x \in k^\infty$ with $n = |x|$, where $Q_1, \ldots, Q_m$ is an alternating sequence of quantifiers $\exists$ and $\forall$, and $Q_1 = \exists$. One important special case is $\mathrm{NP}_k := \Sigma_k^1$. The *polynomial hierarchy* is defined by $\mathrm{PH}_k := \bigcup_{m\in\mathbb{N}} \Sigma_k^m$.

A Boolean combination of polynomial equations over k is called a *quantifier-free formula* over k. A *first-order formula* over k is a formula of type

$$Q_1 y_1 \in k \cdots Q_m y_m \in k \; F(x, y_1, \ldots, y_m),$$

where the Q_i are quantifiers and $F(x, y_1, \ldots, y_m)$ is a quantifier-free formula over k. It is a well-known fact that for a language $A \in \mathrm{P}_k$ there exists a polynomial p and a sequence $F_n(x, y)$ of quantifier-free formulas of polynomial size, such that for all $n \in \mathbb{N}$ and all $x \in k^n$ we have

$$x \in A \iff \exists y \in k^{p(n)} F_n(x, y).$$

To be more precise, let $\alpha_1, \ldots, \alpha_t$ be the constants of the circuit family deciding A. Then the formulas $F_n(x, y)$ can be chosen to be conjunctions of polynomially many equations of constant degree, whose coefficients are integer polynomials of constant bit-size in $\alpha_1, \ldots, \alpha_t$ (Blum *et al.* 1998). It follows

that a language $A \in \mathrm{PH}_k$ can be described by a family of first-order formulas of polynomial size over k.

For any of the classes defined so far there is also a *constant-free* version, where the corresponding circuits are required to be constant-free. For a class $\mathscr{C}$ its constant-free version is denoted by $\mathscr{C}^0$.

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 $\mathrm{PAR}_{\mathbb{F}_2}$ is denoted by PSPACE, since it coincides with the class of all languages decidable by a polynomial-space Turing machine (Borodin 1977).

A classical randomized complexity class is RNC (Johnson 1990), which is defined as the set of languages $A \subseteq \{0,1\}^\infty$ such that there exists a polynomial p and a language $B \in \mathsf{NC}$ with

$$\begin{aligned} x \in A \quad &\Rightarrow \quad \Pr\left(\{y \in \{0,1\}^{p(n)} \mid (x,y) \in B\}\right) \geq \frac{1}{2}, \\ x \notin A \quad &\Rightarrow \quad \Pr\left(\{y \in \{0,1\}^{p(n)} \mid (x,y) \notin B\}\right) = 1, \end{aligned}$$

for all $n \in \mathbb{N}$ and $x \in \{0,1\}^n$.

The concept of reductions is fundamental in complexity theory. We recall the notion of Turing reductions. An *oracle* for a function g is a black box which on input x outputs $g(x)$ in one time-step. Now let $f, g\colon k^\infty \to k^\infty$ be two functions. A *Turing reduction* from f to g is a polynomial time algorithm computing f with an oracle for g.

3. Transfer, Generic, and Randomized Reductions

3.1. Generic Parsimonious Reductions. Constructions in algebraic geometry often rely on generic choices in the sense of Section 2.1.4. Informally, a generic parsimonious reduction as defined by Bürgisser *et al.* (2005) is a parsimonious reduction, in whose computation generic choices are allowed, provided that the genericity condition can be expressed by formulas of moderate size.

We call a relation $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ *balanced* with *associated* polynomial p iff for all $u, a \in \mathbb{C}^\infty$ satisfying $R(u,a)$ we have $|a| = p(|u|)$. By identifying $\mathbb{C}^m$ with $\mathbb{R}^{2m}$ and thus $\mathbb{C}^\infty$ with $\mathbb{R}^\infty$ it makes sense to say that a relation R is in the constant-free polynomial hierarchy over $\mathbb{R}$. Recall the notion $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$.

Definition 3.1. *Let $\varphi, \psi\colon \mathbb{C}^\infty \longrightarrow \overline{\mathbb{N}}$. A* generic parsimonious reduction *from φ to ψ is a pair (π, R), where $\pi\colon \mathbb{C}^\infty \times \mathbb{C}^\infty \longrightarrow \mathbb{C}^\infty$ is in $\mathrm{FP}_{\mathbb{C}}$ and R is a balanced relation in $\mathrm{PH}^0_{\mathbb{R}}$ with associated polynomial p, such that for all $n \in \mathbb{N}$:*

(a) $\forall u \in \mathbb{C}^n \, \forall a \in \mathbb{C}^{p(n)} \, \big(R(u,a) \Rightarrow \varphi(u) = \psi(\pi(u,a))\big)$,

(b) $\forall u \in \mathbb{C}^n \, \{a \in \mathbb{C}^{p(n)} \mid R(u,a)\}$ *is Euclidean dense in* $\mathbb{C}^{p(n)}$.

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

The following theorem from (Bürgisser *et al.* 2005, Theorem 4.4) essentially states that for $u \in \mathbb{C}^\infty$, witnesses a satisfying $R(u,a)$ can be computed in polynomial time over $\mathbb{C}$.

THEOREM 3.2. *Let* $\varphi, \psi \colon \mathbb{C}^\infty \longrightarrow \overline{\mathbb{N}}$. *If* $\varphi \preceq_* \psi$, *then* φ *Turing reduces to* ψ.

3.2. Randomized Parsimonious Reductions. One may interpret the second condition in Definition 3.1 by saying that for each $u \in \mathbb{C}^n$, a randomly chosen $a \in \mathbb{C}^{p(n)}$ satisfies $R(u,a)$ almost surely. Following (Bürgisser *et al.* 2005, Remark 6.7) we give now a definition of a randomized reduction in the discrete setting. We require that this reduction works efficiently in parallel.

DEFINITION 3.3. *Let* $\varphi, \psi \colon \{0,1\}^\infty \to \{0,1\}^\infty$. *A* randomized parsimonious reduction *from* φ *to* ψ *is a function* $\pi \colon \{0,1\}^\infty \times \{0,1\}^\infty \longrightarrow \{0,1\}^\infty$ *in* FNC *such that there exists a polynomial* p *and a constant* $0 < q < 1$ *such that for all* $n \in \mathbb{N}$ *and all* $x \in \{0,1\}^n$

$$\Pr\big(\{y \in \{0,1\}^{p(n)} \mid \varphi(x) \neq \psi(\pi(x,y))\}\big) \leq q^n. \tag{3.4}$$

We write $\varphi \preceq_R \psi$ *iff there exists a randomized parsimonious reduction from* φ *to* ψ.

In (Bürgisser *et al.* 2005, Lemma 4.3) it is shown that the generic parsimonious reduction is transitive. The same holds for the randomized reduction.

LEMMA 3.5. *The relation* $\preceq_R$ *is transitive.*

PROOF. Let $\varphi, \psi, \chi \colon \{0,1\}^\infty \to \{0,1\}^\infty$ with $\varphi \preceq_R \psi$ via π_1 and $\psi \preceq_R \chi$ via π_2. Let p_1, p_2 be the corresponding polynomials and $0 < q_1, q_2 < 1$ the corresponding constants such that (3.4) holds. Set $p := p_1 + p_2$ and define $\pi(x,y) := \pi_2(\pi_1(x,y_1),y_2)$ for $x \in \{0,1\}^n$, $y = (y_1,y_2) \in \{0,1\}^{p(n)}$. Then clearly $\pi \in \mathsf{FNC}$. To prove the probability estimate, we write $\Pr_y$ for the probability with randomly chosen y, where its range is clear from the context. For each $x \in \{0,1\}^n$ we have

$$\begin{aligned}\Pr_y(\varphi(x) \neq \chi(\pi(x,y))) &= \Pr_{(y_1,y_2)}(\varphi(x) \neq \chi(\pi_2(\pi_1(x,y_1),y_2))) \\ &\leq \Pr_{y_1}(\varphi(x) \neq \psi(\pi_1(x,y_1))) + \Pr_{(y_1,y_2)}(\psi(\pi_1(x,y_1)) \neq \chi(\pi_2(\pi_1(x,y_1),y_2))).\end{aligned}$$

The first of these probabilities is at most q_1^n. To bound the second one, consider for fixed y_1 the conditional probability $\Pr_{y_2}(\psi(\pi_1(x,y_1)) \neq \chi(\pi_2(\pi_1(x,y_1),y_2)))$, which is bounded by $q_2^{|\pi_1(x,y_1)|} \leq q_2^n$, since w.l.o.g. $|\pi_1(x,y_1)| \geq n$. This holds for all y_1, therefore the second probability is bounded by q_2^n. Hence $\Pr_y(\varphi(x) \neq \chi(\pi(x,y))) \leq q_1^n + q_2^n$. Any q with $\max\{q_1,q_2\} < q < 1$ satisfies $q_1^n + q_2^n \leq q^n$ for sufficiently large n, hence (3.4) holds for such q. One can easily modify π on a finite number of instances such that this holds for all $n \in \mathbb{N}$. □

3.3. The Complexity Class FRNC. Recall the well-known parallel randomized complexity class RNC of decision problems (cf. Section 2.3.2). We aim at defining a parallel randomized class of functional problems by allowing errors for any result.

Definition 3.6. *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 function* $\psi\colon \{0,1\}^\infty \times \{0,1\}^\infty \to \{0,1\}^\infty$ *in* FNC*, such that for all* $x \in \{0,1\}^\infty$ *with* $n = |x|$

$$\Pr\left(\{y \in \{0,1\}^{p(n)} \mid \varphi(x) \neq \psi(x,y)\}\right) \leq q^n.$$

To motivate this definition we note that in the context of decision problems, it is common to require a failure probability bounded by a constant. This probability can then be made exponentially small by repeating the algorithm polynomially often. Since it is not clear how to do this for functional problems, we have chosen the above definition.

We also note that (Johnson 1990, p. 133) has a definition of a similar, but a bit more restricted class. For our purposes we need the above definition.

Lemma 3.7. *(i) The class* FRNC *consists of all* $\varphi\colon \{0,1\}^\infty \to \{0,1\}^\infty$ *such that there exists* $\psi\colon \{0,1\}^\infty \to \{0,1\}^\infty$ *in* FNC *with* $\varphi \preceq_R \psi$*. Hence* FRNC *is the closure of* FNC *with respect to randomized reductions.*

(ii) The class FRNC *is closed under* $\preceq_R$*.*

(iii) $\mathsf{NC}^{\mathsf{RNC}} \subseteq$ FRNC*.*

Proof. (i) Let $\varphi \in$ FRNC and $\psi \in$ FNC according to Definition 3.6. Then ψ defines a randomized reduction from φ to the identity. On the other hand, if $\varphi \preceq_R \psi$ via π and $\psi \in$ FNC, then $\psi \circ \pi \in$ FNC, hence the function $\widetilde{\psi} := \psi \circ \pi$ satisfies Definition 3.6.

(ii) Let $\varphi \preceq_R \psi$ and $\psi \in$ FRNC. By (i) there exists $\chi \in$ FNC with $\psi \preceq_R \chi$. Transitivity implies $\varphi \preceq_R \chi$, thus $\varphi \in$ FRNC by (i) again.

(iii) This is clear by definition. □

3.4. A Transfer Theorem for Counting Problems. Let $\varphi\colon \mathbb{C}^\infty \to \mathbb{C}^\infty$ be a function. If φ maps $\mathbb{Z}^\infty$ to $\mathbb{Z}^\infty$, we define $\varphi^{\mathbb{Z}}\colon \{0,1\}^\infty \to \{0,1\}^\infty$ to be the restriction of φ to $\mathbb{Z}^\infty$, using a common binary encoding of tuples of integers. For counting functions $\varphi\colon \mathbb{C}^\infty \to \overline{\mathbb{N}} := \mathbb{N} \cup \{\infty\}$, we similarly define $\varphi^{\mathbb{Z}}\colon \{0,1\}^\infty \to \{0,1\}^\infty$.

The following transfer principle is the main result of this section.

THEOREM 3.8. *Let $\varphi, \psi\colon \mathbb{C}^\infty \to \overline{\mathbb{N}}$ with $\varphi \preceq_* \psi$ via (π, R), where $\pi^{\mathbb{Z}}$ is defined and lies in* FNC. *Then $\varphi^{\mathbb{Z}} \preceq_R \psi^{\mathbb{Z}}$.*

PROOF. Let p be the polynomial associated to R. Since $R \in \mathrm{PH}^0_{\mathbb{R}}$, we have for all $n \in \mathbb{N}$ and all $(u,a) \in \mathbb{C}^n \times \mathbb{C}^{p(n)} \simeq \mathbb{R}^{2n} \times \mathbb{R}^{2p(n)}$

$$R(u,a) \iff Q_1 z_1 \in \mathbb{R}^{p_1(n)} \cdots Q_m z_m \in \mathbb{R}^{p_m(n)} F_n(u,a,z_1,\ldots,z_m), \tag{3.9}$$

where $Q_1,\ldots,Q_m$ is an alternating sequence of quantifiers $\exists$ or $\forall$, $p_1,\ldots,p_m$ are polynomials, and $F_n(u,a,z_1,\ldots,z_m)$ is a conjunction of polynomially many equations of constant degree with integer coefficients of constant size (cf. Section 2.3.2). By quantifier elimination there exists a quantifier free formula $\Phi_n(u,a)$ in disjunctive normal form $\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{ij}\Delta_{ij}0$, where $\Delta_{ij} \in \{\leq, <, =, \neq\}$, which is equivalent to (3.9). Note that the h_{ij} are nonzero integer polynomials in the real and imaginary parts of u and a. The bounds on efficient quantifier elimination of Renegar (1992) imply that there exists such a formula $\Phi_n(u,a)$ having $M = \sum_i J_i$ atomic predicates with integer polynomials of degree D and bitsize L, where M, D, and L are all bounded by $2^{n^{\mathcal{O}(1)}}$.

Now for $u \in \mathbb{C}^n$ let $W_u := \{a \in \mathbb{C}^{p(n)} \mid R(u,a)\} = \{a \in \mathbb{C}^{p(n)} \mid \Phi_n(u,a)\}$ be the set of its witnesses. By definition, W_u is Euclidean dense in $\mathbb{C}^{p(n)}$. We claim that

$$U_u := \{a \in \mathbb{C}^{p(n)} \mid \bigwedge_{i,j} h_{ij}(u,a) \neq 0\} \subseteq W_u.$$

Otherwise there would exist $a \in U_u \setminus W_u$. Since the sign of h_{ij} does not change in a small neighbourhood of a, the complement of W_u would contain a ball around a, a contradiction to W_u being dense.

Setting $f_u := \prod_{ij} h_{ij}(u,\cdot)$ we can write $U_u = \{f_u \neq 0\}$. By the above bounds we have $\deg f_u \leq MD \leq 2^{n^{\mathcal{O}(1)}}$. Now let $E_n := \{1,\ldots,c_n\}$ with some integer $c_n \in \mathbb{N}$ and sample a witness $a \in E_n^{2p(n)}$ uniformly at random. Then

$U_u \cap E_n^{2p(n)}$ is a set of "good" witnesses. The Schwartz-Zippel Lemma (Schwartz 1980, Lemma 1) implies

$$\Pr\left(\{a \in E_n^{2p(n)} \mid f_u(a) = 0\}\right) \leq \frac{\deg f_u}{c_n}. \tag{3.10}$$

Hence for $c_n \geq 2^n \deg f_u$, which is of order $2^{n^{\mathcal{O}(1)}}$, the failure probability (3.10) is bounded by 2^{-n}. By encoding the samples in set $E_n^{2p(n)}$ as bitstrings of fixed length $\mathcal{O}(p(n) \log c_n) = n^{\mathcal{O}(1)}$ it follows that $\pi^{\mathbb{Z}}$ defines a randomized parsimonious reduction from $\varphi^{\mathbb{Z}}$ to $\psi^{\mathbb{Z}}$. □

We finish this section with another transfer result. The Boolean part of a decisional complexity class $\mathscr{C}$ in the BSS-model is defined as $\mathrm{BP}(\mathscr{C}) := \{A \cap \{0,1\}^\infty \mid A \in \mathscr{C}\}$, see Blum *et al.* (1998). It is not clear whether $\mathrm{BP}(\mathrm{NC}_\mathbb{C})$ is contained in FNC. However, we can prove the following.

THEOREM 3.11. *We have* $\mathrm{BP}(\mathrm{NC}_\mathbb{C}) \subseteq \mathsf{NC}^{\mathsf{RNC}} \subseteq \mathsf{FRNC}$.

The proof is a variation of some well known techniques. Consider the problem ACIT of deciding whether the polynomial computed by a given constant-free arithmetic circuit $\mathcal{C}$ on the input variables $c_1, \ldots, c_p$ equals zero. It is well known that ACIT lies in coRP (Ibarra & Moran 1983). Consider now the subproblem ACIT_k consisting of those arithmetic circuits $\mathcal{C}$ having depth at most $(\log \mathrm{size}(\mathcal{C}))^k$, where k denotes fixed constant. An analysis of the proof of Ibarra & Moran (1983) shows that ACIT_k lies in coRNC.

PROOF (Theorem 3.11). (Sketch) Let $(\mathcal{C}_n)_n$ be a uniform family of algebraic circuits of depth $(\log n)^{\mathcal{O}(1)}$ and size $n^{\mathcal{O}(1)}$ using complex constants $c_1, \ldots, c_p$. By a well-known construction (Blum *et al.* 1998, §7.2) we may assume that the constants $c_1, \ldots, c_p$ are algebraically independent over $\mathbb{Q}$.

We simulate the algebraic circuit $\mathcal{C}_n$ on input $x \in \{0,1\}^n$ by a Boolean circuit of depth $(\log n)^{\mathcal{O}(1)}$ and size $n^{\mathcal{O}(1)}$. The point is to represent the intermediate results, which are polynomials in $\mathbb{Z}[c_1, \ldots, c_p]$, by the slps computing them. To test such a polynomial for zero, we use the fact that ACIT_k lies in coRNC. □

Note that even when there are no constants, it is not clear how to avoid randomization, since the integers computed by the slps might have quasipolynomial bitsize in n.

Likewise as above we can show the following result, which is very similar to the result $\mathrm{BP}(\mathrm{PAR}_\mathbb{R}^{=}) = \mathsf{PSPACE}$ proved by Cucker *et al.* (1995).

COROLLARY 3.12. *We have* $\mathrm{BP}(\mathrm{PAR}_{\mathbb{C}}) = \mathsf{PSPACE}$.

Cucker & Grigoriev (1997) showed the related result $\mathrm{BP}(\mathrm{PAR}^0_{\mathbb{R}}) = \mathsf{PSPACE}$ over $\mathbb{R}$.

4. Outline of Proof of Main Result

Recall the problem $\#\mathrm{IC}(r)_{\mathbb{C}}$ of computing the number of irreducible components of $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$ for polynomials $f_1, \ldots, f_r \in \mathbb{C}[X]$ given as slps together with an upper bound on their formal degrees in unary. We denote by $\#\textsc{ProjIC}(r)_{\mathbb{C}}$ the corresponding projective version of the problem, where the input polynomials are assumed to be homogeneous and their zero set is considered in $\mathbb{P}^n$. The restriction of this problem to input polynomials with integer coefficients is denoted by $\#\textsc{ProjIC}(r)_{\mathbb{Z}}$.

It is easy to reduce $\#\mathrm{IC}(r)_{\mathbb{C}}$ to $\#\textsc{ProjIC}(r)_{\mathbb{C}}$ by homogenizing the given polynomials of degree at most d with respect to degree $d+1$. Then the hyperplane at infinity becomes an irreducible component of the resulting variety, and so the number of irreducible components increases exactly by one.

For proving the main Theorem 1.1 it will be therefore sufficient to prove an upper bound for $\#\textsc{ProjIC}(r)_{\mathbb{C}}$. Let $\#\textsc{ProjIC}(r,n)_{\mathbb{C}}$ denote the restriction of $\#\textsc{ProjIC}(r)_{\mathbb{C}}$ to varieties in $\mathbb{P}^n$, i.e., the dimension n of the ambient affine space is fixed. As above, $\#\textsc{ProjIC}(r,n)_{\mathbb{Z}}$ denotes its restriction to polynomials with integer coefficients. For this problem efficient parallel algorithms are essentially known.

PROPOSITION 4.1. *(i) We have* $\#\textsc{ProjIC}(r,n)_{\mathbb{C}} \in \mathrm{FNC}_{\mathbb{C}}$.

(ii) We have $\#\textsc{ProjIC}(r,n)_{\mathbb{Z}} \in \mathsf{FRNC}$.

PROOF. Suppose the input polynomials have degree at most d.

(i) Given slps encoding a polynomial system with zero set V, we first compute their dense representation by interpolation. For the evaluation we use the efficient parallel algorithm of Miller *et al.* (1988). Then we use the algorithm of Bürgisser & Scheiblechner (2008) to compute the number of irreducible components of V by uniform algebraic circuits of size $d^{n^{\mathcal{O}(1)}}$ and depth $(n \log d)^{\mathcal{O}(1)}$. Since n is fixed, this is an $\mathrm{FNC}_{\mathbb{C}}$-algorithm.

(ii) We believe one could avoid randomization by analysing the growth of bitsize in the algorithm of part (i). However, this is not essential so that we argue more conveniently using our general transfer principles. The zero set of the given polynomials has at most d^n irreducible components (cf. Section 2.1.4). Hence the output size of $\#\textsc{ProjIC}(r,n)_{\mathbb{Z}}$ is logarithmic in the input size.

We now observe that for any function $\varphi\colon \mathbb{C}^\infty \to \mathbb{N}$ such that $\varphi^{\mathbb{Z}}$ has logarithmic output size, $\varphi \in \mathrm{FNC}_{\mathbb{C}}$ implies $\varphi^{\mathbb{Z}} \in \mathsf{FRNC}$. Indeed, suppose that for inputs x of bitsize m, $\varphi^{\mathbb{Z}}(x)$ has bitsize $\ell = \mathcal{O}(\log m)$. On input x we check in parallel for all nonnegative integers y of bitsize ℓ whether $y = \varphi(x)$. Clearly, this describes an algorithm implementable in $\mathrm{FNC}_{\mathbb{C}}$. The assertion follows now from Theorem 3.11. □

The crucial step in the proof of Theorem 1.1 is the generic parsimonious reduction stated below.

Proposition 4.2. *We have* $\#\mathrm{ProjIC}(r)_{\mathbb{C}} \preceq_* \#\mathrm{ProjIC}(r, r+1)_{\mathbb{C}}$ *via a reduction map* π *such that* $\pi^{\mathbb{Z}}$ *is defined and lies in* FNC.

We postpone the proof and discussion of this proposition and continue with the proof of Theorem 1.1

Proof (Theorem 1.1). Proposition 4.2 combined with Theorem 3.2 yields a Turing reduction from $\#\mathrm{ProjIC}(r)_{\mathbb{C}}$ to $\#\mathrm{ProjIC}(r, r+1)_{\mathbb{C}}$. Together with Proposition 4.1(i) this proves $\#\mathrm{ProjIC}(r)_{\mathbb{C}} \in \mathrm{FP}_{\mathbb{C}}$.

Proposition 4.2 combined with Theorem 3.8 yields a randomized reduction from $\#\mathrm{ProjIC}(r)_{\mathbb{Z}}$ to $\#\mathrm{ProjIC}(r, r+1)_{\mathbb{Z}}$. Since FRNC is closed under randomized parsimonious reductions (Lemma 3.7), this implies together with Proposition 4.1(ii) that $\#\mathrm{ProjIC}(r)_{\mathbb{Z}} \in \mathsf{FRNC}$. □

5. Explicit Genericity Condition for Bertini

The geometric idea behind Proposition 4.2 is Bertini's Theorem (Mumford 1976, (4.18)). In this version it says that an irreducible projective variety V of dimension m and a generic linear subspace L of codimension $m-1$ meet in an irreducible curve. It follows that if V is m-equidimensional, then the number of irreducible components is preserved under intersections with generic linear subspaces of codimension $m-1$. For the general case assume that V is defined by r polynomials. Then the dimension of each of its irreducible components is at least $n-r$, hence the intersection of V with a generic linear subspace L of dimension $r+1$ preserves the number of irreducible components. To turn this idea into a generic parsimonious reduction, we have to identify an explicit condition on L under which $V \cap L$ has the same number of components as V. This condition will consist of a combinatorial and a geometric part.

Recall that $\mathbb{G}_{r+1}(\mathbb{P}^n)$ denotes the Grassmannian consisting of all linear subspaces of dimension $r+1$. Let V_i denote the irreducible components of the va-

riety $V \subseteq \mathbb{P}^n$. The *combinatorial genericity condition* $\mathcal{C}_V(L)$ on $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ expresses that for $i \neq j$, no irreducible component of $V_i \cap L$ is contained in V_j.

To explain the meaning of this, let $V_i \cap L = \bigcup_j Z_{ij}$ denote the decomposition of $V_i \cap L$ into irreducible components. Then, if $\mathcal{C}_V(L)$ holds, the union $V \cap L = \bigcup_{ij} Z_{ij}$ is irredundant and hence is the decomposition of $V \cap L$ into irreducible components. In particular, we have

$$\#\mathrm{ic}(V \cap L) = \sum_i \#\mathrm{ic}(V_i \cap L).$$

For the formulation of the geometric genericity condition we need an appropriate notion of transversality, which we define here for a lack of reference. Our definition modifies the one of (Mumford 1976, pp. 80-81) to the case where one variety is reducible and the other one is linear. Recall that we say that a statement holds for almost all x in a variety V iff it holds for all x in an open dense subset of V.

Definition 5.1. *Let $V \subseteq \mathbb{P}^n$ be a projective variety and $L \subseteq \mathbb{P}^n$ be a linear subspace. We say that V and L are* transversal *in $x \in V \cap L$, written $V \pitchfork_x L$, iff x is smooth in V, and $\dim(T_xV \cap T_xL) = \dim T_xV + \dim T_xL - n$. Moreover, V and L are said to be* transversal*, $V \pitchfork L$, iff we have $V \pitchfork_x L$ for almost all $x \in V \cap L$.*

We note that disjoint varieties are transversal by definition.

The following example shows that for Bertini's Theorem it is not sufficient to require transversality.

Example 5.2. Let $V = \mathcal{Z}(X_0X_3 - X_1^2) \subseteq \mathbb{P}^3$ be the cylinder over a parabola, and consider the plane $L = \mathcal{Z}(X_0 - X_3)$. Then V is irreducible and $V \pitchfork L$, but $V \cap L = \mathcal{Z}(X_1 + X_3, X_0 - X_3) \cup \mathcal{Z}(X_1 - X_3, X_0 - X_3)$ is reducible (cf. Figure 5.1). ◊

We need some further notations. Let $M \in \mathbb{G}_{n-m-1}(\mathbb{P}^n)$ be defined by the linearly independent linear forms $\alpha_0, \ldots, \alpha_m$ on $\mathbb{P}^n$. Then a *projection centered at M* is defined by

$$p_M \colon \mathbb{P}^n \setminus M \longrightarrow \mathbb{P}^m, \quad x \mapsto (\alpha_0(x) : \cdots : \alpha_m(x)).$$

Notice that we have abused notation here, since p_M depends on the choice of the linear forms $\alpha_0, \ldots, \alpha_m$. The map p_M is surjective and the closure of its fibers are projective linear spaces of dimension $n-m$. We note that if $r \geq n-m$

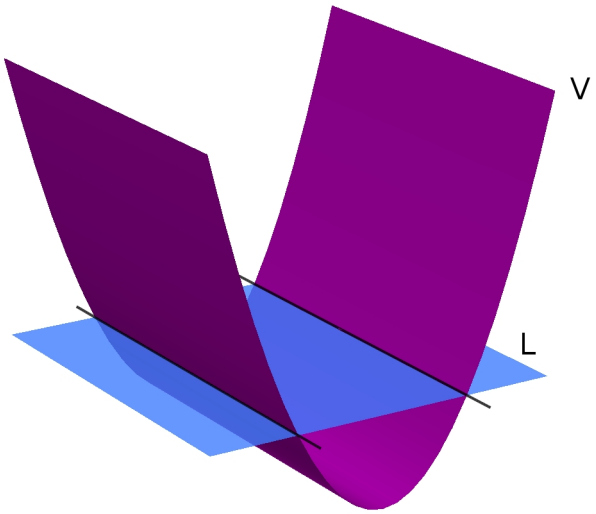

Figure 5.1: The plane L cuts V into two components.

and $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ is a linear space containing M, then $p_M(L) := p_M(L \setminus M)$ is a linear subspace of $\mathbb{P}^m$ of dimension $r+1-(n-m) \geq 1$.

Let V be an m-equidimensional variety and $M \in \mathbb{G}_{n-m-1}(\mathbb{P}^n)$ be disjoint to V. Denote the restriction of p_M to V by $p\colon V \to \mathbb{P}^m$. Then by the Noether Normalization Lemma (Mumford 1976, (2.29)), p is a closed surjective map with finite fibers. We define the set of *branching values* (cf. Section 2.1.2)

$$B_M(V) := \{y \in \mathbb{P}^m \mid p \text{ is not smooth over } y\}.$$

Note that $B_M(V)$ depends on the choice of the linear forms defining M, whereas the set $p^{-1}(B_M(V))$ does not. It follows from (Mumford 1976, (3.6)) that $B_M(V)$ is a variety, and from the algebraic version of Sard's Lemma (Mumford 1976, (3.7)) that $B_M(V) \neq \mathbb{P}^m$.

We note the following: if $\ell \subseteq \mathbb{P}^m$ is a line, then $\ell \pitchfork B_M(V)$ means that ℓ avoids the singular part of $B_M(V)$ and meets the smooth part of $B_M(V)$ transversally in finitely many points of $B_M(V)$.

Now let $n-m \leq r < n$. We define the *geometric genericity condition* $\mathcal{G}_V(L)$ on the linear space $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ as follows:

$$\exists M \in \mathbb{G}_{n-m-1}(L)\ \exists \ell \in \mathbb{G}_1(p_M(L))\colon M \cap V = \emptyset \ \wedge\ \ell \pitchfork B_M(V). \tag{5.3}$$

Note that condition (5.3) is well-defined: the existence of $\ell \in \mathbb{G}_1(p_M(L))$ with

$\ell \pitchfork B_M(V_m)$ is independent of the choice of the linear forms α_i defining M. Furthermore, $\mathcal{G}_\emptyset(L)$ is defined to be always true.

EXAMPLE 5.4. (continued) The condition $\mathcal{G}_V(L)$ states that there exists a point M in the plane L outside of V such that the line $\ell = p_M(L)$ is transversal to $B := B_M(V)$. However, one can show that for each $M \in L \setminus V$ the set of branching values B is the union of two lines meeting in some point of ℓ. Since ℓ meets B in a singular point, they are not transversal, hence $\mathcal{G}_V(L)$ is violated (cf. Figure 5.2). On the other hand, the plane $L' := \mathcal{Z}(X_0 + X_2 - X_3)$ satisfies $\mathcal{G}_V(L')$ (cf. Figure 5.3). ◊

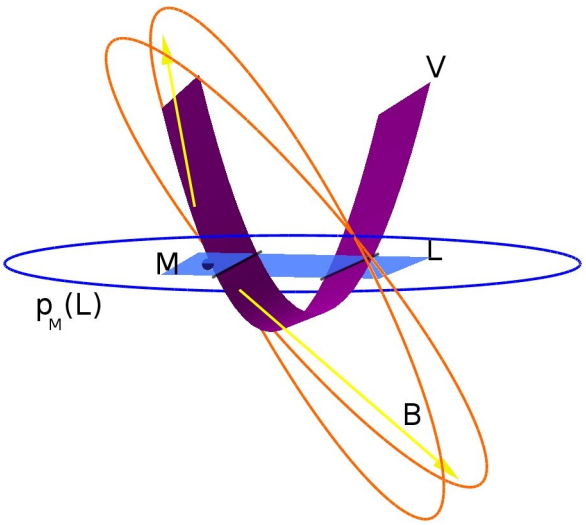

Figure 5.2: The line $p_M(L)$ meets B in a singular point.

Now let $V \subseteq \mathbb{P}^n$ be defined by r homogeneous polynomials, and $V = V_{(n-r)} \cup \cdots \cup V_{(n)}$ be its decomposition into equidimensional components. We define the *genericity condition* $\mathcal{B}_V(L)$ on $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ as

$$\mathcal{C}_V(L) \wedge \bigwedge_{m=n-r}^{n} \mathcal{G}_{V_{(m)}}(L).$$

THEOREM 5.5. *Let the variety $V \subseteq \mathbb{P}^n$ be defined by $r < n$ homogeneous polynomials. Then, for each $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ satisfying the condition $\mathcal{B}_V(L)$, the intersection $V \cap L$ has the same number of irreducible components as V.*

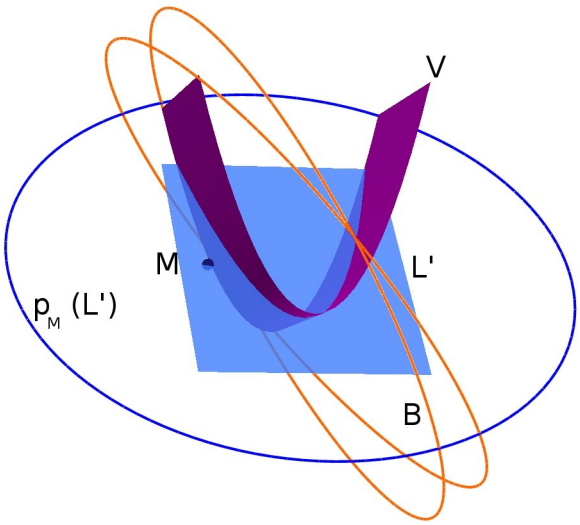

Figure 5.3: For the plane L' we have $p_M(L') \pitchfork B$.

6. Proofs

6.1. Genericity of $\mathcal{B}_V(L)$. We first prove some basic facts about transversality.

LEMMA 6.1. *Let $V \subseteq \mathbb{P}^n$ be a variety and $L \subseteq \mathbb{P}^n$ be a linear subspace.*

(i) If $V \pitchfork_x L$ holds in $x \in V \cap L$, then x is smooth in $V \cap L$ and we have $T_x(V \cap L) = T_xV \cap T_xL$.

(ii) The set $\{x \in V \cap L \mid V \pitchfork_x L\}$ is open in $V \cap L$.

(iii) If $V \pitchfork L$, then we have $\dim_x(V \cap L) = \dim_x V + \dim L - n$ for all $x \in V \cap L$. This conclusion also holds under the assumption that all irreducible components V_i of V are transversal to L.

PROOF. (i) By the Dimension Theorem we have for all $x \in V \cap L$

$$\dim_x(V \cap L) \geq \dim_x V + \dim L - n. \tag{6.2}$$

Now let $V \pitchfork_x L$. We have $\dim T_xV = \dim_x V$ since x is smooth in V. Hence

$$\begin{aligned} \dim_x(V \cap L) &\leq \dim T_x(V \cap L) \leq \dim(T_xV \cap T_xL) \\ &= \dim T_xV + \dim T_xL - n = \dim_x V + \dim L - n. \end{aligned}$$

Equality follows with (6.2), which proves (i).

(ii) This follows easily from the upper-semicontinuity of the dimension.

(iii) Assume $V \pitchfork L$. Let $x \in V \cap L$ and Z be an irreducible component of $V \cap L$ of maximal dimension with $x \in Z$. By (ii), $V \pitchfork L$ implies that $U := \{y \in V \cap L \,|\, V \pitchfork_y L\}$ is open and dense in $V \cap L$. Hence $U \cap Z$ is nonempty. By the upper-semicontinuity of the local dimension, the set $U' := \{y \in V \mid \dim_y V \leq \dim_x V\}$ is open in V. Hence $U' \cap Z$ is open in Z and nonempty, as it contains x. Therefore, $U \cap U' \cap Z$ contains a points y. By the proof of (i), (6.2) is satisfied with equality in the point y. Hence

$$\begin{aligned} \dim_x(V \cap L) &= \dim Z \leq \dim_y(V \cap L) = \dim_y V + \dim L - n \\ &\leq \dim_x V + \dim L - n. \end{aligned}$$

Together with (6.2), this proves the first assertion. The simpler proof of the second assertion is left to the reader. □

Now we present some facts about the combinatorial condition $\mathcal{C}_V(L)$.

LEMMA 6.3. *Let $V \subseteq \mathbb{P}^n$ be an algebraic variety with irreducible components V_i and let L denote a linear subspace in $\mathbb{G}_{r+1}(\mathbb{P}^n)$.*

(i) If $\mathcal{C}_V(L)$ holds, then $V \pitchfork L$ iff $V_i \pitchfork L$ for all i.

(ii) We have $V \pitchfork L$ for almost all L.

(iii) The condition $\mathcal{C}_V(L)$ is satisfied for almost all L.

PROOF. (i) Put $V_i^o := V_i \setminus \bigcup_{k \neq i} V_k$. Then $\operatorname{Reg}(V) \cap V_i = \operatorname{Reg}(V_i) \cap V_i^o$. For $x \in V_i^o$ we have $T_x V = T_x V_i$, and hence $V \pitchfork_x L$ iff $V_i \pitchfork_x L$.

Consider the open subsets $T := \{x \in V \cap L \mid V \pitchfork_x L\}$ and $T_i := \{x \in V_i \cap L \mid V_i \pitchfork_x L\}$, cf. Lemma 6.1(ii). Then $T \cap V_i \subseteq T_i$. Let Z_{ij} denote the irreducible components of $V_i \cap L$. We suppose that $\mathcal{C}_V(L)$ holds. Then $V \pitchfork L$ iff $T \cap Z_{ij} \neq \emptyset$ for all i, j. Similarly, $V_i \pitchfork L$ iff $T_i \cap Z_{ij} \neq \emptyset$ for all j. Since $T \cap Z_{ij} \subseteq T_i \cap Z_{ij}$, it follows that $V \pitchfork L$ implies $V_i \pitchfork L$ for all i. For the other direction assume by way of contradiction that $T_i \cap Z_{ij} \neq \emptyset$ but $T \cap Z_{ij} = \emptyset$. As $T \cap V_i^o = T_i \cap V_i^o$ by the reasoning at the beginning of the proof, we have $T_i \cap Z_{ij} \subseteq \bigcup_{k \neq i} V_k$. Hence $Z_{ij} \subseteq V_k$ for some $k \neq i$, which contradicts $\mathcal{C}_V(L)$.

(ii) If V is irreducible, this is a slight generalization of (Mumford 1976, p. 70), that is proved in essentially the same way. The general case follows by combining this with (i) and (iii).

(iii) Part (ii) for irreducible varieties implies that almost all $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ are transversal to V_i and to all the irreducible components of $V_i \cap V_j$, for all

$i \neq j$. It is therefore sufficient to show that such a linear space L satisfies the condition $\mathcal{C}_V(L)$. Suppose by way of contradiction that there exists an irreducible component Z of $V_i \cap L$ that is contained in V_j, for some $i \neq j$. Choose $x \in Z$ such that $\dim_x(V_i \cap L) = \dim Z$. Then we have $\dim_x(V_i \cap V_j \cap L) \geq \dim Z = \dim_x(V_i \cap L)$. On the other hand, using the transversality of L and applying Lemma 6.1(iii) twice, we get

$$\dim_x(V_i \cap V_j \cap L) = \dim_x(V_i \cap V_j) + r + 1 - n < \dim V_i + r + 1 - n = \dim_x(V_i \cap L),$$

which is a contradiction. □

LEMMA 6.4. *Suppose V is m-equidimensional and let $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$, where $n - m \leq r < n$. Then $\mathcal{G}_V(L)$ implies $V \pitchfork L$.*

PROOF. Let M be as in (5.3), and set $p := p_M|V$, $L' := p_M(L)$, $B := B_M(V)$, and $U := p^{-1}(L' \setminus B)$. By the definition of transversality it suffices to show

1. $V \pitchfork_x L$ for all $x \in U$, and
2. U is dense in $p^{-1}(L') = V \cap L$.

1. By definition of B, each $x \in U$ is a smooth point of V, and the differential $d_x p \colon T_x V \to T_{p(x)}\mathbb{P}^m$ is an isomorphism. So $d_x p$ maps $T_x V \cap T_x L$ injectively into $T_{p(x)}L'$, hence $\dim(T_x V \cap T_x L) \leq \dim L' = m + r + 1 - n$. Since the opposite inequality is trivial, equality follows. Hence $V \pitchfork_x L$.

2. We have $\dim(B \cap L') < \dim L'$ (otherwise $\ell \subseteq L' \subseteq B$, which is impossible). Since $p \colon V \to \mathbb{P}^m$ has finite fibers it follows that

$$\dim p^{-1}(B \cap L') = \dim(B \cap L') < \dim L' = m + r + 1 - n \leq \dim Z$$

for each irreducible component Z of $V \cap L$. Hence $U \cap Z = Z \setminus p^{-1}(B \cap L')$ is not empty. Thus U is dense in $V \cap L$. □

LEMMA 6.5. *Let $V \subseteq \mathbb{P}^n$ be defined by $r < n$ polynomials. Then almost all $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$ satisfy the condition $\mathcal{B}_V(L)$.*

PROOF. According to Lemma 6.3(iii) it is sufficient to prove that the geometric condition $\mathcal{G}_V(L)$ holds for almost all L, where V is m-equidimensional.

Put $\mathbb{G}_k := \mathbb{G}_k(\mathbb{P}^n)$ and $\mathbb{G}'_k := \mathbb{G}_k(\mathbb{P}^m)$. For dimension reasons, almost all $M \in \mathbb{G}_{n-m-1}$ satisfy $M \cap V = \emptyset$. By Lemma 6.3(ii) for each such M, almost all lines $\ell \subseteq \mathbb{P}^m$ meet $B_M(V)$ transversally. Hence the set D of all

$(M,\ell) \in \mathbb{G}_{n-m-1} \times \mathbb{G}'_1$ satisfying $M \cap V = \emptyset$ and $\ell \pitchfork B_M(V)$ is dense in $\mathbb{G}_{n-m-1} \times \mathbb{G}'_1$. The morphism

$$\varphi\colon \mathbb{G}_{n-m-1} \times \mathbb{G}'_1 \to \mathbb{G}_{n-m+1}, (M,\ell) \mapsto \overline{p_M^{-1}(\ell)}$$

is easily seen to be surjective. It follows that $\varphi(D)$ is dense in $\mathbb{G}_{n-m+1}$. From this it is not hard to deduce that the set of all $L \in \mathbb{G}_{r+1}$ satisfying $\mathcal{G}_V(L)$ is dense. □

6.2. Proof of Theorem 5.5. This result is shown via connectivity properties. For this purpose we need two lemmas. The first one relates the connected components of a dense subset of a variety with its irreducible components.

LEMMA 6.6. *Let V be an algebraic variety and U an open dense subset of V with $U \subseteq \operatorname{Reg}(V)$. Then the number of irreducible components of V equals the number of connected components of U.*

PROOF. Let $V = V_1 \cup \cdots \cup V_t$ be the irreducible decomposition of V. Since U is dense in V, U meets each V_i. Since $U \subseteq \operatorname{Reg}(V)$, each point of U lies in exactly one V_i. Hence, $U = \bigcup_{i=1}^{t}(U \cap V_i)$ is a disjoint decomposition into nonempty closed subsets. Since $U \cap V_i$ is open in V_i, it is connected (cf. Section 2.1.1). It follows that U has t connected components. □

The second lemma is a purely topological statement about the relation of the number of connected components of the total space of a fibration with that of its fibers. Recall from Section 2.2 that a fibration $\pi\colon E \to B$ over a locally contractible base space is locally fiber-homotopically trivial. A section of π is a continuous map $s\colon B \to E$ with $\pi \circ s = \mathrm{id}_B$.

LEMMA 6.7. *Let $\pi\colon T \to B$ be a fibration with T locally path-connected and B locally contractible and connected. Let $T = T_1 \cup \cdots \cup T_t$ be the decomposition into connected components. Assume that for each $1 \le \nu \le t$ there exists a section $s_\nu\colon B \to T_\nu$. Then each fiber of π has t connected components.*

PROOF. Fix ν. For $y \in B$ let $\pi^{-1}(y)_1$ denote the connected component of $\pi^{-1}(y) \cap T_\nu$ containing $s_\nu(y)$, and set $\pi^{-1}(y)_2 := (\pi^{-1}(y) \cap T_\nu) \setminus \pi^{-1}(y)_1$. Then

$$T_\nu = \Big(\bigcup_{y\in B} \pi^{-1}(y)_1\Big) \cup \Big(\bigcup_{y\in B} \pi^{-1}(y)_2\Big)$$

is a disjoint union, whose first set we denote by A_ν and the second by B_ν. We now prove that A_ν is open.

For that purpose, let $(U_i)_{i\in I}$ be an open covering of B over which π is fiber-homotopically trivial, i.e., for each i there exists F and a fiber homotopy equivalence $\varphi\colon \pi^{-1}(U_i) \to U_i \times F$ such that the diagram

$$\begin{array}{ccc} \pi^{-1}(U_i) & \xrightarrow{\varphi} & U_i \times F \\ & \searrow^{\pi} \quad \swarrow_{\mathrm{pr}_1} & \\ & U_i & \end{array}$$

commutes. We can assume U_i to be non-empty and connected. Then $\mathrm{pr}_2 \circ \varphi \circ s_\nu(U_i)$ is also connected, hence lies in a connected component F_1 of F. By a remark at the end of Section 2.2 it follows that $\pi^{-1}(y)_1 = \varphi^{-1}(\{y\} \times F_1)$ for all $y \in U_i$. Thus $A_\nu \cap \pi^{-1}(U_i) = \bigcup_{y\in U_i} \pi^{-1}(y)_1 = \varphi^{-1}(U_i \times F_1)$ is open. Since this holds for all i, we conclude that A_ν is open. Analogously one sees that B_ν is open.

The connectedness of T_ν implies $B_\nu = \emptyset$. Hence $\pi^{-1}(y) = \bigcup_\nu (\pi^{-1}(y) \cap T_\nu)$ is the decomposition into connected components, for $y \in B$. Therefore $\pi^{-1}(y)$ has exactly t connected components. □

Now we are able to prove Theorem 5.5. We follow the lines of Fulton & Lazarsfeld (1981).

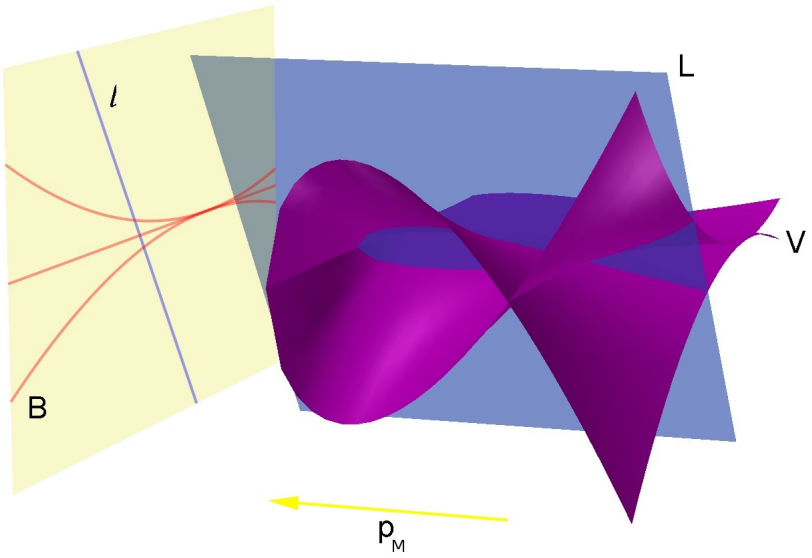

Figure 6.1: Proof of Theorem 5.5.

PROOF (Theorem 5.5). As before let $V = \bigcup_{m=n-r}^{n} V_{(m)}$ denote the equidimensional decomposition of $V \subseteq \mathbb{P}^n$. We first show that the $V_{(m)} \cap L$ are the equidimensional components of $V \cap L$. By Lemma 6.4, $\mathcal{G}_{V_{(m)}}(L)$ implies $V_{(m)} \pitchfork L$. Using Lemma 6.1(iii) we see that $V_{(m)} \cap L$ is equidimensional of dimension $m+r+1-n$. Furthermore, $\mathcal{C}_V(L)$ implies that $V \cap L = \bigcup_m (V_{(m)} \cap L)$ is irredundant (cf. Section 5), hence it is indeed the equidimensional decomposition. Now we have to show that

$$\#\mathrm{ic}(V_{(m)} \cap L) = \#\mathrm{ic}(V_{(m)}) \quad \text{for all} \quad m, \tag{6.8}$$

since then we can conclude

$$\#\mathrm{ic}(V \cap L) = \sum_m \#\mathrm{ic}(V_{(m)} \cap L) = \sum_m \#\mathrm{ic}(V_{(m)}) = \#\mathrm{ic}(V),$$

which is the claim of the theorem.

To prove (6.8), we can fix m and assume V to be m-equidimensional. Furthermore, the first interesting case is $m \geq 2$.

By condition $\mathcal{G}_V(L)$ there exists a linear space $M \in \mathbb{G}_{n-m-1}(L)$ disjoint to V and a line $\ell \subseteq p_M(L)$ transversal to $B := B_M(V)$ (cf. Figure 6.1). With $p := p_M|V$ denote $V^o := p^{-1}(\mathbb{P}^m \setminus B) = V \setminus p^{-1}(B)$. Then V^o is a dense open subset of V contained in $\mathrm{Reg}\,(V)$. Let V have t irreducible components. Then V^o has also t irreducible components. We consider the commutative diagram

$$\begin{array}{ccc} p^{-1}(\ell \setminus B) & \subseteq & V^o \\ \downarrow & & \downarrow \\ \ell \setminus B & \subseteq & \mathbb{P}^m \setminus B. \end{array} \tag{6.9}$$

By the remarks at the end of Section 2.1.2 the downwards maps are coverings. We show that

$$p^{-1}(\ell \setminus B) \text{ has } t \text{ connected components.} \tag{6.10}$$

Choose a point $y_0 \in \ell \setminus B$ and let $q\colon \mathbb{P}^m \setminus \{y_0\} \to \mathbb{P}^{m-1}$ be a projection centered at y_0. Now denote by $B_0 \subseteq \mathbb{P}^{m-1}$ the set of branching values of $q|B$. Then $q|B$ restricts over $\mathbb{P}^{m-1} \setminus B_0$ to a covering map. Furthermore, each line through y_0 has the form $\ell_z := \overline{q^{-1}(z)}$ for some unique $z \in \mathbb{P}^{m-1}$. It is easy to see that $\ell_z \pitchfork B$ if and only if $z \in \mathbb{P}^{m-1} \setminus B_0$. Hence for all $z \in \mathbb{P}^{m-1} \setminus B_0$ we have $|\ell_z \cap B| = e$, where e is the degree of the $(m-1)$-dimensional component of B (which could be empty). Thus the fibers of $q|(\mathbb{P}^m \setminus B)$ over $\mathbb{P}^{m-1} \setminus B_0$ are 2-spheres with a continuously varying set of e points removed.

Now we consider the blow-up of $\mathbb{P}^m \setminus B$ at y_0 (cf. Section 2.1.3)

$$P := \{(y, z) \in (\mathbb{P}^m \setminus B) \times \mathbb{P}^{m-1} \mid y \in \ell_z\}.$$

The projection $\mathrm{pr}_2 \colon P \to \mathbb{P}^{m-1}$ restricts over $\mathbb{P}^{m-1} \setminus B_0$ to a fiber bundle whose fiber is a 2-sphere with e points removed.

The blow-up of V^o at the points of $p^{-1}(y_0)$ can be identified with the set

$$V^* := \{(x, z) \in V^o \times \mathbb{P}^{m-1} \mid p(x) \in \ell_z\}.$$

The map $p \times \mathrm{id} \colon V^* \to P$ is a covering. This is clear over the complement of the exceptional fiber $\{y_0\} \times \mathbb{P}^{m-1}$ of P. On the other hand, if φ is a local inverse of p near $x \in p^{-1}(y_0)$, then $\varphi \times \mathrm{id}$ is a local inverse of $p \times \mathrm{id}$ near all points in the exceptional fiber $\{x\} \times \mathbb{P}^{m-1}$ of V^*.

Since fiber bundles are fibrations, it follows that the restriction of the composition $\mathrm{pr}_2 \circ (p \times \mathrm{id}) \colon V^* \to \mathbb{P}^{m-1}$ to $T := \{(x, z) \in V^* \mid z \notin B_0\}$ is a fibration

$$\pi \colon T \to \mathbb{P}^{m-1} \setminus B_0.$$

As a blow-up, V^* has the same number t of irreducible components as V^o, and as an open and dense subset of V^*, T has also t irreducible components. Since T is smooth, T has also t connected components. Now choose points $x_1, \ldots, x_t \in p^{-1}(y_0)$, one in each connected component of V^o. This is possible, since p maps each irreducible component V_i of V surjectively onto $\mathbb{P}^m$, and y_0 does not lie in the set of branching values of V_i. Then the maps $s_\nu \colon \mathbb{P}^{m-1} \setminus B_0 \to T$, $s_\nu(z) := (x_\nu, z)$, $1 \le \nu \le t$, are sections of π into each connected component of T. Lemma 6.7 implies that each fiber $\pi^{-1}(z)$ has t connected components, in particular $p^{-1}(\ell \setminus B)$, which proves (6.10).

Now let $L' := p_M(L)$. We prove that

(6.11) $\quad U := p^{-1}(L' \setminus B) = (V \cap L) \setminus p^{-1}(B)$ has t connected components.

Let $V = V_1 \cup \cdots \cup V_t$ be the irreducible decomposition of V. Since by (6.10) the set $p^{-1}(\ell \setminus B) \cap V_i$ is connected, for (6.11) it suffices to show that each point in $U \cap V_i$ can be connected by a path with a point in that set. So let $x \in U \cap V_i$ and $y := p(x)$. As a non-empty open subset of L' the set $L' \setminus B$ is connected (cf. Section 2.1.1). Hence there exists a path c in $L' \setminus B$ connecting y with a point in $\ell \setminus B$. From the path lifting property applied to the covering $p|U \colon U \to L' \setminus B$ we obtain a path $\widetilde{c}$ in $U \cap V_i$ with $\widetilde{c}(0) = x$ (cf. Section 2.2). This path obviously connects x with a point in $p^{-1}(\ell \setminus B) \cap V_i$.

Finally, in the proof of Lemma 6.4 it was shown that U is a dense open subset of $V \cap L$ in which the intersection is transversal. Lemma 6.1(i) implies that U is contained in $\mathrm{Reg}\,(V \cap L)$. From (6.11) it follows with Lemma 6.6 that $V \cap L$ has t irreducible components. $\square$

6.3. Proof of Proposition 4.2. We represent an slp of length s with $n+1$ input variables in some standard way as a complex vector. Let $\mathcal{S}_{n,s}$ denote the set of encodings obtained this way. Accordingly, we will encode polynomial systems by vectors $\gamma = (\gamma_1, \ldots, \gamma_r) \in \mathcal{S}_{n,s}^r$ and write $V_\gamma \subseteq \mathbb{P}^n$ for the projective variety defined by the polynomials encoded by the slps γ_i, provided that these polynomials are homogeneous. (We note that the homogeneous parts of a polynomial encoded by an slp can be computed in parallel polylogarithmic time, cf. Scheiblechner (2007a).)

Let $M_{r,n}$ denote the set of matrices in $\mathbb{C}^{(n-r)\times(n+1)}$ having full rank. The kernel of a matrix $\alpha \in M_{r,n}$ is a linear subspace in $\mathbb{C}^{n+1}$ of dimension $r+1$, and will be interpreted as a projective linear subspace $L_\alpha \subseteq \mathbb{P}^n$ of dimension r.

LEMMA 6.12. *Given $\gamma \in \mathcal{S}_{n,s}^r$ and $\alpha \in M_{r+1,n}$, one can express the condition $\mathcal{B}_{V_\gamma}(L_\alpha)$ by a first order formula in* $\mathrm{PH}_{\mathbb{R}}^0$.

We postpone the proof of this lemma to the remainder of this section and continue with the proof of Proposition 4.2.

PROOF (Proposition 4.2). We have to set up a generic parsimonious reduction (π, R) from $\#\mathrm{PROJIC}(r)_{\mathbb{C}}$ to $\#\mathrm{PROJIC}(r, r+1)_{\mathbb{C}}$. The condition $\mathcal{B}_{V_\gamma}(L_\alpha)$ defines the required relation R, which is in $\mathrm{PH}_{\mathbb{R}}^0$ according to Lemma 6.12. The reduction map π maps (γ, α) to a suitable encoding of the intersection $V_\gamma \cap L_\alpha$. More precisely, given γ encoding a homogeneous polynomial system and a matrix α defining $L_\alpha \in \mathbb{G}_{r+1}(\mathbb{P}^n)$, we express the slps in homogeneous coordinates of $L_\alpha \simeq \mathbb{P}^{r+1}$ to define $V_\gamma \cap L_\alpha$. These new slps constitute $\pi(\gamma, \alpha)$. Theorem 5.5 and Lemma 6.5 imply that (π, R) is a generic parsimonious reduction.

We still have to check that $\pi^{\mathbb{Z}}$ is computable in FNC. This follows since linear algebra over $\mathbb{Q}$ can be done in FNC (Berkowitz 1984; von zur Gathen 1986). Furthermore, the output of $\pi^{\mathbb{Z}}$ can be made integral by multiplying with a common denominator. Note that multiplying a matrix with a scalar does not affect its kernel or image. □

In the following we express conditions on varieties V_γ by first order formulas. An important feature of these formulas is that the only way V_γ appears therein is as a predicate expressing membership to V_γ. We call a formula using such a predicate an *enhanced formula*. Note that if a property of V_γ is expressed by enhanced formulas in $\mathrm{PH}_{\mathbb{R}}^0$, and if the predicate $x \in V_\gamma$ is also expressed by formulas in $\mathrm{PH}_{\mathbb{R}}^0$, then by replacing all the predicates with the appropriate formula one obtains usual first order formulas in $\mathrm{PH}_{\mathbb{R}}^0$. In the following we will freely use this fact.

LEMMA 6.13. *Given $\gamma \in \mathcal{S}^r_{n,s}$, $\alpha \in M_{n-m,n}$, and $x, v \in \mathbb{P}^n$, one can express the following properties by enhanced formulas in* $\mathrm{PH}^0_{\mathbb{R}}$.

(i) $\dim_x V_\gamma = m$,

(ii) $\dim_x V_\gamma = m \ \wedge \ V_\gamma \pitchfork_x L_\alpha$,

(iii) x *is a smooth point in* V_γ,

(iv) $x \in (V_\gamma)_{(m)}$,

(v) $x \in V_\gamma$ *is smooth and* $v \in \mathbb{T}_x V_\gamma$.

PROOF. (i) follows from (Bürgisser & Cucker 2007, Proposition 3.1).

(ii) is a consequence of (Bürgisser & Cucker 2006, Lemma 5.8), which characterizes transversality of L_α to V_γ in x by the property that each sufficiently small perturbation of L_α meets V_γ locally in exactly one point.

(iii) Smoothness at x means $\bigvee_m \big(\exists \alpha \in M_{m-n,n} \ \dim_x V_\gamma = m \wedge L_\alpha \pitchfork_x V_\gamma\big)$.

(iv) Let $W := \{x \in V_\gamma \mid \dim_x V_\gamma = m\}$. The Zariski closure $\overline{W}$ of W equals the m-equidimensional component $(V_\gamma)_{(m)}$ of V_γ. Since W is constructible, its Zariski closure coincides with its Euclidean closure (cf. Section 2.1.1). If $W^c \subseteq \mathbb{C}^{n+1}$ denotes the affine cone of W, we have

$$\overline{W}^c = \overline{W^c} = \{x \in \mathbb{C}^{n+1} \mid \forall \varepsilon > 0 \, \exists y \in \mathbb{C}^{n+1} \ y \in W^c \ \wedge \ \|x - y\| < \varepsilon\},$$

where $\| \ \|$ denotes the Euclidean norm on $\mathbb{C}^{n+1}$. The assertion follows by combining this insight with Part (i).

(v) If x is an isolated point of V_γ, then $\mathbb{T}_x V_\gamma = \{x\}$. Since this case can easily be tested by enhanced formulas in $\mathrm{PH}^0_{\mathbb{R}}$, we can assume $\dim_x V_\gamma > 0$. If furthermore $x \in V_\gamma$ is smooth, we have $v \notin \mathbb{T}_x V_\gamma$ iff

$$\bigvee_m \big(\exists \alpha \in M_{n-m,n} \quad x, v \in L_\alpha \ \wedge \ \dim_x V_\gamma = m \ \wedge \ V_\gamma \pitchfork_x L_\alpha\big). \qquad \square$$

LEMMA 6.14. *Let $V \subseteq \mathbb{P}^n$ be defined by $r < n$ equations. Let $V_{(m)}$ for $n - r \le m \le n$ denote its m-equidimensional component, and let $L \in \mathbb{G}_{r+1}(\mathbb{P}^n)$. Assume that $\mathcal{G}_{V_{(m)}}(L)$ holds for all m. Then the condition $\mathcal{C}_V(L)$ is equivalent to $\dim_x(V_{(m)} \cap V_{(m')} \cap L) < \dim_x(V_{(m)} \cap L)$ for all $m < m'$ and all $x \in V_{(m)} \cap V_{(m')} \cap L$.*

PROOF. We first note that $\mathcal{G}_{V_{(m)}}(L)$ implies $V_{(m)} \pitchfork L$ by Lemma 6.4. Using Lemma 6.1(iii) we see that $V_{(m)} \cap L$ is equidimensional of dimension $m+r+1-n$. Denote by V_i the irreducible components of V.

Assume that $\mathcal{C}_V(L)$ is violated. Then there exists an irreducible component Z of $V_i \cap L$ that is contained in V_j for some $i \neq j$. Let $m := \dim V_i$ and $m' := \dim V_j$. Since $V_{(m)} \cap L$ is equidimensional of the right dimension, Z must be an irreducible component of $V_{(m)} \cap L$. We have $\dim_x(V_{(m)} \cap L) = \dim Z \leq \dim_x(V_{(m)} \cap V_{(m')} \cap L)$ for any $x \in Z$ and now need to show that $m < m'$. By the observation at the beginning of the proof, $V_{(m')} \cap L$ is equidimensional of dimension $m' + r + 1 - n$ and contains Z. Hence $m \leq m'$. Note that $U := \{x \in V_{(m)} \cap L \mid V_{(m)} \pitchfork_x L\} \subseteq \operatorname{Reg}(V_{(m)})$ meets Z since $V_{(m)} \pitchfork L$. Hence $Z \cap \operatorname{Reg}(V_{(m)}) \neq \emptyset$. This implies $m \neq m'$, since otherwise $Z \subseteq V_i \cap V_j \subseteq \operatorname{Sing}(V_{(m)})$, which is a contradiction.

For the converse we assume that there exist $m < m'$ and $x \in V_{(m)} \cap V_{(m')} \cap L$ such that $\dim_x(V_{(m)} \cap V_{(m')} \cap L) = \dim_x(V_{(m)} \cap L)$. Let Z be an irreducible component of $V_{(m)} \cap V_{(m')} \cap L$ through x of maximal dimension. Then $\dim Z = \dim_x(V_{(m)} \cap V_{(m')} \cap L) = \dim_x(V_{(m)} \cap L)$ and hence Z is an irreducible component of $V_{(m)} \cap L$. Thus Z is an irreducible component of $V_i \cap L$ for some i. But Z is also contained in some irreducible component V_j of $V_{(m')}$. Since $\dim V_i = m < m' = \dim V_j$, it follows $i \neq j$, hence $\mathcal{C}_V(L)$ is violated. □

PROOF (Lemma 6.12). Lemma 6.13 and Lemma 6.14 imply that the combinatorial part $\mathcal{C}_V(L)$ can be expressed in $\mathrm{PH}^0_{\mathbb{R}}$, if this is true for the geometric part $\mathcal{G}_{V_{(m)}}(L)$.

For $\gamma \in \mathcal{S}^r_{n,s}$ and fixed m we write $V := (V_\gamma)_{(m)}$. Denote $L = L_\alpha$ for $\alpha \in M_{r+1,n}$. It remains to express the geometric condition $\mathcal{G}_V(L)$:

$$\exists \beta \in M_{n-m-1,n}\ \exists \ell \in \mathbb{G}_1(p_{L_\beta}(L)):\ L_\beta \subseteq L \ \wedge\ L_\beta \cap V = \emptyset \ \wedge\ \ell \pitchfork B_{L_\beta}(V)$$

The only non-trivial part is to express $\ell \pitchfork B_{L_\beta}(V)$. Denote $p = p_{L_\beta}|V$. We have $y \in B_{L_\beta}(V)$ iff

$$\exists x \in \mathbb{P}^n \ \big(x \in V \wedge p(x) = y \wedge (x \text{ singular in } V \vee d_x p \text{ not surjective})\big).$$

We use Lemma 6.13 to express the condition that x is singular in V in $\mathrm{PH}^0_{\mathbb{R}}$. It remains to express the condition that $d_x p$ is not surjective. This condition has to be checked only for smooth points $x \in V$, and in this case $d_x p$ is not surjective iff it is not injective, i.e.,

$$\exists\, v \in \mathbb{T}_x V\ (v \neq x \ \wedge\ p_M(v) = p_M(x)).$$

Here we used that the derivative of a linear map is the linear map itself. Lemma 6.13(v) implies that one can express $y \in B_{L_\beta}(V)$ by enhanced formulas in $\mathrm{PH}^0_{\mathbb{R}}$. To express the transversality $\ell \pitchfork B_{L_\beta}(V)$, we use Lemma 6.13(ii). $\square$

Acknowledgements

This paper contains results of the PhD thesis of the second author (Scheiblechner 2007a) that were announced in (Bürgisser & Scheiblechner 2007). This work has been supported by the DFG grant BU 1371. The second author also wants to thank David Blottière for a helpful discussion about the proof of Bertini's Theorem.

References

C.L. Bajaj, J.F. Canny, T. Garrity & J.D. Warren (1993). Factoring Rational Polynomials Over the Complex Numbers. *SIAM J. Comp.* **22**(2), 318–331.

S.J. Berkowitz (1984). On Computing the Determinant in Small Parallel Time Using a Small Number of Processors. *Inf. Process. Lett.* **18**(3), 147–150.

L. Blum, F. Cucker, M. Shub & S. Smale (1998). *Complexity and Real Computation*. Springer.

A.B. Borodin (1977). On relating Time and Space to Size and Depth. *SIAM J. Comp.* **6**, 733–744.

G.E. Bredon (1997). *Topology and Geometry*, volume 139 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, xiv+557.

P. Bürgisser, M. Clausen & M.A. Shokrollahi (1997). *Algebraic Complexity Theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, xxiv+618.

P. Bürgisser & F. Cucker (2006). Counting Complexity Classes for Numeric Computations II: Algebraic and Semialgebraic Sets. *J. Compl.* **22**, 147–191.

P. Bürgisser & F. Cucker (2007). Exotic Quantifiers, Complexity Classes, and Complete Problems. Accepted for Foundations of Computational Mathematics.

P. Bürgisser, F. Cucker & M. Lotz (2005). Counting Complexity Classes for Numeric Computations III: Complex Projective Sets. *Foundations of Computational Mathematics* **5**(4), 351–387.

P. Bürgisser & P. Scheiblechner (2007). Differential Forms in Computational Algebraic Geometry. In *ISSAC '07: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, 61–68. ACM Press, New York, NY, USA.

P. Bürgisser & P. Scheiblechner (2008). On the Complexity of Counting Components of Algebraic Varieties. Accepted for J. Symb. Comp.

G. Chèze & A. Galligo (2005). Four Lectures on Polynomial Absolute Factorization. In *Solving Polynomial Equations*, volume 14 of *Algorithms Comput. Math.*, 339–392. Springer, Berlin.

A.L. Chistov (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).

F. Cucker & D. Grigoriev (1997). On the Power of Real Turing Machines over Binary Inputs. *SIAM J. Comput.* **26**(1), 243–254.

F. Cucker, M. Karpinski, P. Koiran, T. Lickteig & K. Werther (1995). On real Turing Machines that Toss Coins. In *STOC '95: Proceedings of the twenty-seventh annual ACM Symposium on Theory of Computing*, 335–342. ACM Press, New York, NY, USA. ISBN 0-89791-718-9.

A. Dimca (1992). *Singularities and Topology of Hypersurfaces.* Universitext. Springer Verlag.

W. Fulton & R. Lazarsfeld (1981). Connectivity and its Applications in Algebraic Geometry. In *Algebraic geometry (Chicago, Ill., 1980)*, volume 862 of *Lecture Notes in Math.*, 26–92. Springer, Berlin.

S. Gao (2003). Factoring Multivariate Polynomials via Partial Differential Equations. *Math. Comput.* **72**(242), 801–822.

J. von zur Gathen (1984). Parallel Algorithms for Algebraic Problems. *SIAM J. Comput.* **13**(4), 802–824.

J. von zur Gathen (1986). Parallel Arithmetic Computations: a Survey. In *MFOCS86*, number 233 in LNCS, 93–112. SV.

J. von zur Gathen (1985). Irreducibility of Multivariate Polynomials. *J. Comp. Syst. Sci.* **31**(2), 225–264.

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

D.Yu Grigoriev (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).

J. Harris (1992). *Algebraic Geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York Berlin Heidelberg, xix+328.

O.H. Ibarra & S. Moran (1983). Equivalence of Straight-Line Programs. *J. ACM* **30**, 217–228.

D.S. Johnson (1990). A Catalog of Complexity Classes. In *Handbook of Theoretical Computer Science (vol. A): Algorithms and Complexity*, J.van Leeuwen, editor, 67–161. Elsevier, Amsterdam.

E. Kaltofen (1985a). Effective Hilbert Irreducibility. *Information and Control* **66**, 123–137.

E. Kaltofen (1985b). Fast Parallel Absolute Irreducibility Testing. *J. Symb. Comp.* **1**(1), 57–67. Misprint corrections: *J. Symbolic Comput.* vol. 9, p. 320 (1989).

E. Kaltofen (1989). Factorization of Polynomials given by Straight-Line Programs. In *Randomness and Computation, volume 5 of Advances in Computing Research*, S. Micali, editor, 375–412. JAI Press Inc., Greenwhich, Connecticut.

E. Kaltofen (1990). Polynomial Factorization 1982–1986. In *Computers in Mathematics (Stanford, CA, 1986)*, volume 125 of *Lecture Notes in Pure and Appl. Math.*, 285–309. Dekker, New York.

E. Kaltofen (1992). Polynomial Factorization 1987–1991. In *LATIN '92 (São Paulo, 1992)*, volume 583 of *Lecture Notes in Comput. Sci.*, 294–313. Springer, Berlin.

G.L. Miller, V. Ramachandran & E. Kaltofen (1988). Efficient Parallel Evaluation of Straight-Line Code and Arithmetic Circuits. *SIAM J. Comp.* **17**(4), 687–695.

D. Mumford (1976). *Algebraic Geometry I: Complex Projective Varieties*, volume 221 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin Heidelberg New York, x+186.

D.A. Plaisted (1977). Sparse Complex Polynomials and Polynomial Reducibility. *JCSS* **14**, 210–221.

J. Renegar (1992). On the Computational Complexity and Ceometry of the First-Order Theory of the Reals. Part I, II, III. *J. Symb. Comp.* **13**(3), 255–352.

P. Scheiblechner (2007a). On the Complexity of Counting Irreducible Components and Computing Betti Numbers of Complex Algebraic Varieties. URL `http://www2.math.uni-paderborn.de/people/peter-scheiblechner/research.html`. PhD Thesis.

P. Scheiblechner (2007b). On the Complexity of Deciding Connectedness and Computing Betti Numbers of a Complex Algebraic Variety. *J. Compl.* **23**, 359–379.

J.T. Schwartz (1980). Fast Probabilistic Algorithms for Verification of Polynomial Identities. *J. ACM* **27**(4), 701–717.

E.H. Spanier (1966). *Algebraic Topology*. McGraw-Hill Series in Higher Mathematics. McGraw-Hill Book Company, New York, xiv+528.

Peter Bürgisser
Institute of Mathematics
University of Paderborn
D-33095 Paderborn
Germany
`pbuerg@upb.de`

Peter Scheiblechner
Institute of Mathematics
University of Paderborn
D-33095 Paderborn
Germany
`pscheib@math.upb.de`