Journal of Algorithms **41,** 52–68 (2001)
doi:10.1006/jagm.2001.1177, available online at http://www.idealibrary.com on IDEAL®

Computing Chow Forms and Some Applications[1]

Gabriela Jeronimo, Susana Puddu, and Juan Sabia[2]

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales,
Universidad de Buenos Aires, Ciudad Universitaria, Pab. I,
(1428) Buenos Aires, Argentina

Received February 3, 2000

We prove the existence of an algorithm that, from a finite set of polynomials defining an algebraic projective variety, computes the Chow form of its equidimensional component of the greatest dimension. Applying this algorithm, a finite set of polynomials defining the equidimensional component of the greatest dimension of an algebraic (projective or affine) variety can be computed. The complexities of the algorithms involved are lower than the complexities of the known algorithms solving the same tasks. This is due to a special way of coding output polynomials, called straight-line programs. © 2001 Academic Press

Key Words: polynomial equations; equidimensional decomposition; Chow form; complexity theory; algorithmic algebraic geometry.

1. INTRODUCTION

One of the basic problems in effective algebraic geometry is to give a geometric description of the set of solutions of a polynomial equation system. This set is an algebraic variety and a possible way to describe it is to decompose it into equidimensional subvarieties (i.e., varieties with all their irreducible components of the same dimension).

When all the equations involved are given by homogeneous polynomials, the set of solutions form a projective variety in the projective space. An equidimensional projective variety can be completely described by means of a polynomial called its *Chow form*. This is the reason several algorithms to compute the Chow form of a projective variety have been constructed (see, for example, [2, 5, 12]). The algorithm described in [12] only deals with

[1] Partially supported by the following Argentinian research grants: CONICET: PIP'97 4571; UBACyT: EX TW80 (1998); ANPCyT: PICT 03-0000001593 (1998).

[2] To whom correspondence should be addressed. E-mail: jsabia@dm.uba.ar.

0196-6774/01 $35.00

irreducible varieties and the one shown in [2] deals with equidimensional varieties (that is, one has to know *in advance* whether the variety considered is irreducible or equidimensional, respectively). In [5], the algorithm yields an equidimensional decomposition of a projective variety and computes the Chow form of every component. If the variety V is given by s homogeneous polynomials in $n+1$ variables of degrees bounded by d, the sequential complexities of the algorithms in [5], [2], and [12] are of order $(sd)^{n^{O(1)}}$ $s^5 d^{O((n-r)\cdot n^2)}$ and $s^{O(1)} d^{O(n\cdot r)}$ respectively, where r is the dimension of V.

In this paper we show the existence of a well-parallelizable algorithm which, given as input s homogeneous polynomials in $n+1$ variables of degrees bounded by $d \geq n$ which define a projective variety V, produces as output the Chow form of the equidimensional component of V of the greatest dimension. The sequential complexity of this algorithm is bounded by $s^{O(1)} d^{O(n)}$. Note that this algorithm solves the same task as the algorithms in [2] and [12] within lower complexity bounds and without further information on V. The significant reduction in complexity is partly due to the different way of coding polynomials with respect to [2] and [5]: the polynomials involved are not only encoded as vectors of coefficients but also as arithmetic circuits (straight-line programs) as well.

Using this algorithm, we obtain another one which, given a variety V (either affine or projective) produces polynomials defining its equidimensional component of the greatest dimension within the same complexity bounds. Moreover, an algorithm which decides whether a variety V is equidimensional or not can be obtained.

Besides the above-cited algorithm in [5], there are other algorithms which describe equidimensional components of algebraic varieties as the one shown in [3]. Both these algorithms have greater complexities than the ones we show in this paper. As we have mentioned before, this is partly due to the fact that they only use dense form encoding for polynomials.

2. PRELIMINARIES

2.1. *Notations*

Let k be a field of characteristic 0. We suppose k to be effective: this means that the arithmetic operations (addition, subtraction, multiplication) and basic equality checking (comparison) between elements of k are realizable by algorithms. Each operation or comparison is considered to have unitary cost, and the sequential complexity of an algorithm is the number of arithmetic operations and comparisons performed between elements of k.

If $X_0, \dots, X_n$ are indeterminates over k and $f \in k[X_0, \dots, X_n]$ is a polynomial, its total degree will be denoted by $\deg f$.

Let $\bar{k}$ be an algebraic closure of k. We denote by $\mathbb{P}^n(\bar{k})$ (or $\mathbb{P}^n$) and $\mathbb{A}^n(\bar{k})$ (or $\mathbb{A}^n$) the n-dimensional projective and affine spaces over $\bar{k}$, respectively, equipped with their Zariski topologies. If $S \subseteq \mathbb{P}^n$ (or $S \subseteq \mathbb{A}^n$), $\overline{S}$ will denote the closure of S with respect to these topologies.

The dimension of an algebraic variety V will be denoted by $\dim V$.

If $V \subseteq \mathbb{A}^n$ is an irreducible closed set of dimension r the *degree* of V is, as usual,

$$\begin{aligned}\deg V := \sup\{\# H_1 \cap \cdots \cap H_r \cap V;\ & H_1, \ldots, H_r \text{ affine} \\ & \text{hyperplanes in } \mathbb{A}^n \text{ such that } H_1 \cap \cdots \cap H_r \cap V \\ & \text{is a finite set}\}.\end{aligned}$$

For an arbitrary algebraic variety $V \subseteq \mathbb{A}^n$, $\deg V$ is defined as the sum of the degrees of all the irreducible components of V. This notion of degree can be extended to the projective case. Let $V \subseteq \mathbb{P}^n$ be an irreducible projective variety. The degree of V is the number of points in the intersection of V with a linear variety of complementary dimension. The degree of any projective variety is, again, the sum of the degrees of its irreducible components.

2.2. *Chow Form of an Equidimensional Projective Variety*

Let $X_0, \ldots, X_n$ be indeterminates over k. Let $V \subseteq \mathbb{P}^n$ be an equidimensional projective variety definable by polynomials in $k[X_0, \ldots, X_n]$, and let r be its projective dimension. For every i, $0 \le i \le r$, let

$$L^{(i)} = Y_0^{(i)} X_0 + \cdots + Y_n^{(i)} X_n,$$

where $Y_j^{(i)}$ $(0 \le i \le r,\ 0 \le j \le n)$ are new indeterminates over $k[X_0, \ldots, X_n]$.

Let $\Gamma(V) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ be the set

$$\begin{aligned}\Gamma(V) = \{(y^{(0)}, \ldots, y^{(r)}, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n : x \in V \wedge L^{(0)}(y^{(0)}, x) = 0 \\ \wedge \cdots \wedge L^{(r)}(y^{(r)}, x) = 0\}.\end{aligned}$$

Let $\pi : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to (\mathbb{P}^n)^{r+1}$ be the cannonical projection map. Then $\pi(\Gamma(V))$ is a closed set of codimension 1 in $(\mathbb{P}^n)^{r+1}$ (see [13]).

Therefore there exists a square-free polynomial $P \in k[Y_j^{(i)}]_{\substack{0 \le i \le r \\ 0 \le j \le n}}$ (uniquely determined by V up to a constant factor) such that

$$\pi(\Gamma(V)) = \{y \in (\mathbb{P}^n)^{r+1} / P(y) = 0\}.$$

The polynomial P is called the *Chow form of the projective variety* V.

Note that, given $H_0, \ldots, H_r \subseteq \mathbb{P}^n$ hyperplanes whose equations are determined by $y^{(0)}, \ldots, y^{(r)} \in \mathbb{P}^n$, then

$$P(y^{(0)}, \ldots, y^{(r)}) = 0 \Leftrightarrow V \cap H_0 \cap \cdots \cap H_r \neq \emptyset.$$

2.3. *Codification of Polynomials*

The multivariate polynomials we deal with in our algorithms will be encoded in one of the following ways:

- *Dense form*, that is, as arrays (vectors) of elements of k.
- *Straight-line programs*, which are arithmetic circuits (networks without branches). They contain neither selectors nor (propositional) Boolean operations. (For an exact definition and elementary properties of the notion of a straight-line program we refer to [7] and [8].)
- Combining both dense form and straight-line programs.

2.4. *Algorithmic Tools*

The algorithms we construct in this paper are based on the effective well-parallelizable algorithm for quantifier elimination over algebraically closed fields developed in [12]. Whenever we need to compute the dimension of an affine or projective variety from a finite set of polynomials defining it, we will apply the well-parallelizable algorithm in [6]. Both these algorithms use well-parallelizable algorithms for linear algebra like the ones described in [1] and [11].

To determine whether a polynomial encoded by a straight-line program is the zero polynomial, we will evaluate it in a suitable sequence of points (called a *correct test sequence*) with coordinates in k (see [8, Theorem 4.4]). Although the choice of such sequences could be done algorithmically, the cost of doing so would exceed the main complexity class considered in this paper. However, for fixed input parameters (number of indeterminates, quantity and degrees of the polynomials involved), this choice is independent of the problem. For this reason, we will suppose that the correct test sequences are given by means of a preprocessing whose cost will not be considered in the complexity bounds obtained and, therefore, our algorithms will be non-uniform as they depend on the choice of these sequences. Our non-uniform algorithms can be turned into uniform probabilistic ones if the elements of the correct test sequences are chosen randomly.

In order to compute the greatest common divisor of a finite set of polynomials encoded by a straight-line program, we adapt the techniques given in [9] using correct test sequences to obtain a deterministic non-uniform algorithm. We will compute quotients of polynomials given by straight-line programs using Strassen's procedure of Vermeidung von Divisionen ([14], see also [10]). Finally, we will need to compute the radical of a polynomial given by a straight-line program. A standard (non-uniform) computation involving greatest common divisor and Vermeidung von Divisionen shows that if $f \in k[X_1, \dots, X_n]$ is a polynomial of total degree $D \geq n$ given by a straight-line program of length L, there exists a straight-line program of length $(L.D)^{O(1)}$ which computes $\mathrm{rad}(f)$.

3. RESULTS

Let $F_1, \ldots, F_s$ be homogeneous polynomials in $k[X_0, \ldots, X_n]$ and let $V \subseteq \mathbb{P}^n(\bar{k})$ be the projective variety consisting of the common zeroes of these polynomials; that is,

$$V = \{x \in \mathbb{P}^n(\bar{k}) / F_1(x) = 0 \wedge \cdots \wedge F_s(x) = 0\}.$$

Let r be the dimension of V and let V_r be the equidimensional component of V of dimension r.

In a first step, we are going to obtain a straight-line program that computes the Chow form of V_r. Then, we will use this Chow form to obtain a finite set of polynomials defining this component. We will adapt conveniently our algorithm to find the equidimensional component of the greatest dimension for the case of an affine variety. Finally, we will describe an algorithm to decide whether an algebraic variety is equidimensional or not.

3.1. *Computing the Chow Form of the Equidimensional Component of V of Dimension* dim V

In this step, we will describe an algorithm that, from polynomials defining a projective variety V of dimension r, computes the Chow form of its equidimensional component of dimension r.

THEOREM 1. *Let $F_1, \ldots, F_s$ be homogeneous polynomials in $k[X_0, \ldots, X_n]$ and let $d \geq n$ be an integer such that* $\deg F_i \leq d$ $(1 \leq i \leq s)$. *Let*

$$V := \{x \in \mathbb{P}^n(\bar{k}) / F_1(x) = 0 \wedge \cdots \wedge F_s(x) = 0\}.$$

Let r be the projective dimension of V and let V_r be the equidimensional component of V of dimension r.

Then, there exists a well-parallelizable algorithm with sequential complexity bounded by $s^{O(1)} d^{O(n)}$ whose input is the set of polynomials $\{F_1, \ldots, F_s\}$ encoded in dense form and whose output is the Chow form P_r of V_r, given by a straight-line program of length $s^{O(1)} d^{O(n)}$.

Proof. First we apply the well-parallelizable algorithm of Giusti and Heintz (see [6]) to compute $r = \dim V$. The sequential complexity of this step is $s^{O(1)} d^{O(n)}$.

We introduce $(n+1)(r+1)$ new indeterminates $\{Y_j^{(i)}\}_{\substack{0 \leq i \leq r \\ 0 \leq j \leq n}}$ over $k[X_0, \ldots, X_n]$.

For every i, $0 \le i \le r$, let

$$L^{(i)} = Y_0^{(i)} X_0 + \cdots + Y_n^{(i)} X_n$$

and let $\Gamma(V) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ be the set

$$\Gamma(V) = \{(y, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n / F_1(x) = 0 \wedge \cdots \wedge F_s(x) = 0 \\ \wedge L^{(0)}(y, x) = 0 \wedge \cdots \wedge L^{(r)}(y, x) = 0\}.$$

We are going to adapt the arguments used for defining the Chow form in [13] in order to obtain a relation between the Chow form of V_r, the equidimensional component of V of dimension r, and the set $\Gamma(V)$.

Let C be an irreducible component of V. We define $\Gamma(C) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ as

$$\Gamma(C) = \{(y, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n / x \in C \wedge L^{(0)}(y, x) = 0 \\ \wedge \cdots \wedge L^{(r)}(y, x) = 0\}.$$

Then, $\Gamma(V) = \bigcup_C \Gamma(C)$, where the union ranges over all the irreducible components of V.

Let π_1: $(\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to (\mathbb{P}^n)^{r+1}$ and π_2: $(\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to \mathbb{P}^n$ be the cannonical projection maps.

If $\dim C = r$, then $\pi_1(\Gamma(C))$ is a closed set of codimension 1 in $(\mathbb{P}^n)^{r+1}$ (see [13]). Consider now the case when $\dim C < r$. As $\pi_2(\Gamma(C)) = C$ and for every $x \in C$, $\pi_2^{-1}(x) \cong (\mathbb{P}^{n-1})^{r+1} \times \{x\}$ is an irreducible set of dimension $(n-1)(r+1)$, then $\Gamma(C)$ is irreducible and $\dim \Gamma(C) = \dim \pi_2^{-1}(x) + \dim C < n(r+1) - 1$. Therefore, $\dim \pi_1(\Gamma(C)) < n(r+1) - 1$.

Consider

$$\Gamma(V_r) := \{(y, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n / x \in V_r \wedge L^{(0)}(y, x) = 0 \\ \wedge \cdots \wedge L^{(r)}(y, x) = 0\}.$$

As V_r is the union of all the irreducible components of V of dimension r, $\pi_1(\Gamma(V_r))$ is the equidimensional component of $\pi_1(\Gamma(V))$ of codimension 1.

Recalling that the Chow form P_r of V_r is, by definition, the square-free polynomial whose set of zeroes is $\pi_1(\Gamma(V_r))$, to compute P_r we are going to find a square-free polynomial which defines the equidimensional component of codimension 1 of $\pi_1(\Gamma(V))$.

In order to apply the quantifier elimination algorithm in [12], we are going to consider the homogeneous coordinates of the points in $\pi_1(\Gamma(V))$ as points in the affine space $\mathbb{A}^{(n+1)(r+1)}$.

Let φ be the formula

$$\begin{aligned}&\exists x_0 \cdots \exists x_n : (x_0 \neq 0 \vee \cdots \vee x_n \neq 0) \wedge F_1(x_0, \ldots, x_n) = 0\\&\quad \wedge \cdots \wedge F_s(x_0, \ldots, x_n) = 0 \wedge L^{(0)}(y_0^{(0)}, \ldots, y_n^{(0)}, x_0, \ldots, x_n) = 0\\&\quad \wedge \cdots \wedge L^{(r)}(y_0^{(r)}, \ldots, y_n^{(r)}, x_0, \ldots, x_n) = 0\end{aligned}$$

and let $W \subseteq \mathbb{A}^{(n+1)(r+1)}$ be the set

$$W = \{(y_0^{(0)}, \ldots, y_n^{(r)}) \in \bar{k}^{(n+1)(r+1)} / \varphi(y_0^{(0)}, \ldots, y_n^{(r)})\}.$$

Note that the polynomials in $k[Y_j^{(i)}]_{\substack{0\le i\le r\\ 0\le j\le n}}$ which define $\pi_1(\Gamma(V))$ in $(\mathbb{P}^n)^{r+1}$, define W in $\mathbb{A}^{(n+1)(r+1)}$ and, therefore, W is a closed set. Moreover, the Chow form P_r we want to compute is the square-free polynomial defining the equidimensional component of codimension 1 of W in $\mathbb{A}^{(n+1)(r+1)}$.

As the polynomials $F_1, \ldots, F_s, L^{(0)}, \ldots, L^{(r)}$ are homogeneous, we obtain the following formula equivalent to φ

$$\bigvee_{k=0}^{n} \varphi_k,$$

where φ_k is the formula

$$\begin{aligned}&\exists x_0 \cdots \exists x_{k-1} \exists x_{k+1} \cdots \exists x_n : F_1(x_0, \ldots, x_{k-1}, 1, x_{k+1}, \ldots, x_n) = 0\\&\quad \wedge \cdots \wedge F_s(x_0, \ldots, x_{k-1}, 1, x_{k+1}, \ldots, x_n) = 0\\&\quad \wedge L^{(0)}(y_0^{(0)}, \ldots, y_n^{(0)}, x_0, \ldots, x_{k-1}, 1, x_{k+1}, \ldots, x_n) = 0\\&\quad \wedge \cdots \wedge L^{(r)}(y_0^{(r)}, \ldots, y_n^{(r)}, x_0, \ldots, x_{k-1}, 1, x_{k+1}, \ldots, x_n) = 0.\end{aligned}$$

Let $W_k \subseteq \mathbb{A}^{(n+1)(r+1)}$ be the set defined by φ_k.

As W is a closed set, we have

$$W = \bigcup_{k=0}^{n} W_k = \bigcup_{k=0}^{n} \overline{W}_k.$$

Therefore the irreducible components of W having codimension 1 are precisely the irreducible components of codimension 1 of the sets $\overline{W_k}$.

Then, to find the square-free polynomial which defines the equidimensional component of W of codimension 1, we are going to deal with the closed sets $\overline{W_k}$.

Fix $k, 0 \le k \le n$. The formula φ_k is a conjunction involving only atomic formulas of the type $f = 0$ with only one block of existential quantifiers. Note that φ_k involves $s + r + 1$ polynomials in $(n+1)(r+1) + n$ variables; their degrees with respect to $X_0, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n$ are bounded by

$d \geq n$ and their degrees with respect to the remaining variables are bounded by 1.

Applying the algorithm described in [12, Theorem 3.2.1.] we obtain a quantifier-free formula ψ_k equivalent to φ_k. The sequential complexity of this step is bounded by $s^{O(1)}d^{O(n)}$. Then

$$W_k = \{(y_0^{(0)}, \ldots, y_n^{(r)}) \in \bar{k}^{(n+1)(r+1)} / \psi_k(y_0^{(0)}, \ldots, y_n^{(r)})\}. \tag{1}$$

Let $H_1, \ldots, H_t \in k[Y_j^{(i)}]_{\substack{0\leq i\leq r\\ 0\leq j\leq n}}$ be the polynomials appearing in ψ_k. Then $t \leq s^{O(1)}d^{O(n)}$, $\deg H_i \leq d^{O(n)} (1 \leq i \leq t)$, and $H_1, \ldots, H_t$ are given by a straight-line program of length $s^{O(1)}d^{O(n)}$.

In order to give a characterization of the irreducible components of codimension 1 of $\overline{W_k}$ we will use the normal disjunctive form of the formula ψ_k which defines W_k.

Let $I = \{1, 2, \ldots, t\}$. For every $M \subseteq I$ let

$$\mathcal{Z}_M := \{w \in \bar{k}^{(n+1)(r+1)} / H_i(w) = 0 \, \forall \, i \in M \wedge H_j(w) \neq 0 \, \forall \, j \in I - M\}.$$

There exists a subset S of $\{M \subseteq I / \mathcal{Z}_M \neq \emptyset\}$ such that

$$W_k = \bigcup_{M \in S} \mathcal{Z}_M.$$

Therefore

$$\overline{W_k} = \bigcup_{M \in S} \overline{\mathcal{Z}_M}$$

and we conclude that the irreducible components of $\overline{W_k}$ of codimension 1 are the irreducible components of the sets $\overline{\mathcal{Z}_M}$ which have codimension 1.

Now we will determine which sets $\overline{\mathcal{Z}_M}$, $M \subseteq I$, are of codimension 1 and, for each of them, we will find a polynomial $G_M \in k[Y_j^{(i)}]$ $(0 \leq i \leq r,\ 0 \leq j \leq n)$ such that $\{G_M = 0\}$ is the equidimensional component having codimension 1 of $\overline{\mathcal{Z}_M}$.

First, let us obtain an upper bound for the number of sets $M \subseteq \{1, 2, \ldots, t\}$ such that $\overline{\mathcal{Z}_M}$ has codimension 1.

Let M be such a set and let C be an irreducible component of codimension 1 of $\overline{\mathcal{Z}_M}$. Then, there exists i $(1 \leq i \leq t)$ such that C is an irreducible component of $\{H_i = 0\}$. Taking into account that the number of irreducible components of a closed set is bounded by its degree, we deduce that there are at most $\sum_{i=1}^t \deg H_i$ irreducible components of codimension 1. As the set of irreducible components of $\overline{\mathcal{Z}_{M_1}}$ and $\overline{\mathcal{Z}_{M_2}}$ are disjoint whenever $M_1 \neq M_2$, the number of sets $M \subseteq I$ such that $\overline{\mathcal{Z}_M}$ has codimension 1 is also bounded by $\sum_{i=1}^t \deg H_i$.

To determine the sets M we are looking for, we are going to adapt a method that appears in [4].

In order to simplify notation, given $M, N \subseteq I$, the set

$$\{w \in \bar{k}^{(n+1)(r+1)} / H_i(w) = 0 \,\forall\, i \in M \wedge H_j(w) \neq 0 \,\forall\, j \in N\}$$

will be denoted by

$$\left\{ \bigwedge_{i \in M} H_i = 0 \wedge \bigwedge_{j \in N} H_j \neq 0 \right\}.$$

We may assume that the number t of polynomials appearing in ψ_k is 2^h for a positive integer h (considering $H_i \equiv 0$ for $t+1 \leq i \leq 2^{1+[\log(t-1)]}$ if necessary).

In a first step we consider the sets

$$A_i^{(0)} := \{\{H_i = 0\}, \{H_i \neq 0\}\} \ (1 \leq i \leq t).$$

We will determine which sets $\{H_i = 0\}$ and $\{H_i \neq 0\}(1 \leq i \leq t)$ are non-empty to obtain

$$B_i^{(0)} := \{\Delta \in A_i^{(0)} / \Delta \neq \emptyset\} \ (1 \leq i \leq t).$$

In the next step, we consider the sets

$$A_i^{(1)} := \{\Delta_1 \cap \Delta_2 / \Delta_1 \in B_{2i-1}^{(0)} \wedge \Delta_2 \in B_{2i}^{(0)}\} \left(1 \leq i \leq \frac{t}{2}\right).$$

We will determine which elements of $A_i^{(1)}$ have closures of codimension at most 1 to obtain

$$B_i^{(1)} := \{\Delta \in A_i^{(1)} / \operatorname{codim} \overline{\Delta} \leq 1\} \left(1 \leq i \leq \frac{t}{2}\right).$$

Supposing we have obtained $B_i^{(j)}(1 \leq j \leq (\log t) - 1, 1 \leq i \leq \frac{t}{2^j})$, we consider the sets

$$A_i^{(j+1)} := \{\Delta_1 \cap \Delta_2 / \Delta_1 \in B_{2i-1}^{(j)} \wedge \Delta_2 \in B_{2i}^{(j)}\} \left(1 \leq i \leq \frac{t}{2^{j+1}}\right)$$

and determine which elements of $A_i^{(j+1)}$ have closures of codimension at most 1 to obtain

$$B_i^{(j+1)} := \{\Delta \in A_i^{(j+1)} / \operatorname{codim} \overline{\Delta} \leq 1\} \left(1 \leq i \leq \frac{t}{2^{j+1}}\right).$$

Note that in this way, in $1 + \log t$ steps, we obtain a single set $B_1^{(\log t)}$ whose elements are the sets $\mathcal{Z}_M$ such that $\overline{\mathcal{Z}_M}$ has codimension at most 1.

We are going to show how to determine if the closure of a set Δ of the form

$$\Delta = \left\{ \bigwedge_{i \in M} H_i = 0 \wedge \bigwedge_{j \in N} H_j \neq 0 \right\},$$

where M, N are disjoint subsets of I, has codimension at most 1.

First, let us observe that $\overline{\Delta} = \mathbb{A}^n$ if and only if Δ is a non-empty open set, which is equivalent to

- $M = \emptyset$ or $H_i \equiv 0 \, \forall \, i \in M$ and
- $H_j \not\equiv 0 \, \forall \, j \in N$,

which is easily checked because in the first step we can determine which of the polynomials are the zero polynomial. (This can be done by means of a correct test sequence.)

Let us suppose now that $M \neq \emptyset$ and there exists $\ell \in M$ such that $H_\ell \not\equiv 0$. Without loss of generality, we assume $H_i \not\equiv 0 \, \forall \, i \in M$ and $H_j \not\equiv 0 \, \forall \, j \in N$, and we will show how to determine whether $\operatorname{codim}(\overline{\Delta}) = 1$ or not.

Let $H = \prod_{j \in N} H_j$ and, given $i \in M$, let $H_i = \prod_{l=1}^{n_i} H_{il}^{\alpha_l}$ be the irreducible factorization of H_i in $\bar{k}[Y_j^{(i)}]_{\substack{0 \le i \le r \\ 0 \le j \le n}}$. Let $M = \{i_1, \ldots, i_m\}$ and let $\mathcal{P} = \{1, \ldots, n_{i_1}\} \times \cdots \times \{1, \ldots, n_{i_m}\}$. Then

$$\overline{\Delta} = \bigcap_{(l_1, \ldots, l_m) \in \mathcal{P}} \overline{\left\{ \bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0 \right\}}$$

and therefore the equidimensional component of codimension 1 of $\overline{\Delta}$ is the union of the equidimensional components of codimension 1 of the sets

$$\overline{\left\{ \bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0 \right\}}.$$

Note that as the polynomials $H_{i_j l_j}$ are irreducible and

$$\overline{\left\{ \bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0 \right\}} \subseteq \left\{ \bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \right\} \tag{2}$$

then there exists a component of codimension 1 in $\overline{\{\bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0\}}$ only if all the polynomials $H_{i_j l_j}$ appearing in (2) are (up to a constant factor) the same.

On the other hand, if there exists a polynomial G such that $H_{i_j l_j} = \lambda_j G$ for every $1 \le j \le m$ then, as G is irreducible,

$$\overline{\{G = 0 \wedge H \neq 0\}} = \begin{cases} \emptyset & \text{if } G \mid H \\ \{G = 0\} & \text{otherwise.} \end{cases}$$

Therefore an irreducible component of $\overline{\Delta}$ of codimension 1 is defined by a common factor of the polynomials H_i, $i \in M$, which does not divide H. Then, the equidimensional component of $\overline{\Delta}$ of codimension 1 is the set of zeroes of the polynomial

$$H_\Delta := \frac{\operatorname{rad}(\gcd(H_i, i \in M))}{\gcd(\operatorname{rad}(\gcd(H_i, i \in M)), H)}.$$

To determine if $\overline{\Delta}$ has codimension 1 we only need to decide whether H_Δ is a nonzero constant or not. Following the methods in [9], but using correct test sequences (see [8]) to determine if a polynomial is the zero polynomial, we obtain a straight-line program which computes $\gcd(H_i, i \in M)$. We compute $\operatorname{rad}(\gcd(H_i, i \in M))$ and then we obtain a straight-line program which computes $\gcd(\operatorname{rad}(\gcd(H_i, i \in M)), H)$. Finally, applying Strassen's procedure of *Vermeidung von Divisionen* (see [14]) we obtain a straight-line program which computes a scalar multiple of H_Δ. We decide if H_Δ is a nonzero constant by means of an appropriate correct test sequence.

Therefore, we can determine if $\overline{\Delta}$ has codimension at most 1 in sequential time $s^{O(1)}d^{O(n)}$. We proceed in this way to determine, in each step $0 \le j \le \log t$ and for each $1 \le i \le \frac{t}{2^j}$, which elements of the sets $A_i^{(j)}$ have closures of codimension at most 1.

As, for each $0 \le j \le \log t$ and each $1 \le i \le \frac{t}{2^j}$, the number of elements of $B_i^{(j)}$ is bounded by the number of sets $M \subseteq I$ such that $\overline{\mathcal{Z}_M}$ has codimension at most 1, then it is bounded by $\sum_{i=1}^t \deg H_i + 1 \le s^{O(1)}d^{O(n)}$.

So, for each of the sets $A_i^{(j)}$ we apply the algorithm to decide if the closure of one of its elements Δ has codimension 1 at most $s^{O(1)}d^{O(n)}$ times. Note that the number of sets $A_i^{(j)}$ is bounded by $2t \le s^{O(1)}d^{O(n)}$.

Therefore we obtain $B_1^{(\log t)} = \{\mathcal{Z}_M / M \subseteq I, \operatorname{codim} \overline{\mathcal{Z}_M} \le 1\}$ in sequential time $s^{O(1)}d^{O(n)}$ and for each of its elements we decide if it is a subset of the set W_k using the quantifier-free formula ψ_k which define W_k with the same complexity bounds.

Let

$$\mathcal{J} := \{M \subseteq I / \mathcal{Z}_M \subseteq W_k \wedge \operatorname{codim} \overline{\mathcal{Z}_M} = 1\}.$$

For each $M \in \mathcal{J}$ let

$$G_M := \frac{\operatorname{rad}(\gcd(H_i, i \in M))}{\gcd(\operatorname{rad}(\gcd(H_i, i \in M)), \prod_{j \in I - M} H_j)}$$

and let

$$G_k := \prod_{M \in \mathcal{J}} G_M.$$

Then $\{G_k = 0\}$ is the equidimensional component of codimension 1 of $\overline{W_k}$ because this component is the union of the components of codimension 1 of all the sets $\overline{\mathcal{Z}_M}$, $M \in \mathcal{J}$. Recalling that the Chow form P_r we want to compute is the square-free polynomial defining the equidimensional component of codimension 1 of $W = \cup_{k=0}^{n} \overline{W_k}$ then

$$P_r = \mathrm{rad}\left(\prod_{k=o}^{n} G_k \right).$$

The polynomial P_r is given by a straight-line program of length $s^{O(1)} d^{O(n)}$ and the sequential complexity of this algorithm is bounded by $s^{O(1)} d^{O(n)}$. ∎

3.2. *Computing the Greatest Equidimensional Component of V*

In this section we show how to obtain from the Chow form of an equidimensional projective variety, a finite set of polynomials which defines it. This procedure, together with the algorithm exhibited in the previous section, allows us to find polynomials defining the equidimensional component of the greatest dimension of an arbitrary projective variety.

LEMMA 2. *Let $V \subseteq \mathbb{P}^n$ be an equidimensional projective variety of dimension r and let $P \in k[Y_j^{(i)}]_{\substack{0 \le i \le r \\ 0 \le j \le n}}$ be its Chow form. Suppose P is given by a straight-line program of length L.*

Then, there exists $N \le 6(L + 2(r+2)n(n+1))^2$ polynomials $Q_1, \dots, Q_N$ whose degrees are bounded by $(r+1) \deg V$ such that each of them can be evaluated by a straight-line program of length of order $L + 2(r+1)n(n+1)$ and

$$V = \{x \in \mathbb{P}^n \colon Q_1(x) = 0 \wedge \cdots \wedge Q_N(x) = 0\}.$$

Proof. By the definition of the Chow form of an equidimensional projective variety (see Section 2.2), the following equivalence holds in $\mathbb{P}^n$:

$$x \notin V \iff \exists\, y^{(0)}, \dots, y^{(r)} \in \mathbb{P}^n \colon L^{(0)}(y^{(0)}, x) = 0 \wedge \cdots \wedge$$
$$\wedge L^{(r)}(y^{(r)}, x) = 0 \wedge P(y^{(0)}, \dots, y^{(r)}) \neq 0.$$

Using this equivalence, we are going to obtain a quantifier-free formula describing the set $\mathbb{P}^n - V$.

Let us fix $x \in \mathbb{P}^n$ and let $(x_0 : \cdots : x_n)$ be a fixed system of homogeneous coordinates of x. We consider the linear space of $\bar{k}^{n+1}$ determined by the equation $x_0 Y_0 + \cdots + x_n Y_n = 0$. We denote by $e_j \in \bar{k}^{n+1}$ the $(n+1)$-tuple whose coordinates are 0 except for the jth which is 1. For each pair (j, l), $0 \le j < l \le n$, let

$$x_{jl} := x_l e_j - x_j e_l.$$

Note that $\{x_{jl}, 0 \leq j < l \leq n\}$ is a generator system of the linear space considered. Then, for each $0 \leq i \leq r$, the condition $L^{(i)}(y^{(i)}, x) = 0$ is equivalent to

$$\exists\, \alpha_{jl}^{(i)}, 0 \leq j < l \leq n / y^{(i)} = \sum_{j,l} \alpha_{jl}^{(i)} x_{jl}$$

and therefore

$$x \notin V \iff \exists\, \alpha_{jl}^{(i)}, 0 \leq i \leq r, 0 \leq j < l \leq n$$
$$P\left(\sum_{j,l} \alpha_{jl}^{(0)} x_{jl}, \ldots, \sum_{j,l} \alpha_{jl}^{(r)} x_{jl}\right) \neq 0.$$

Let $Q \in k[\alpha_{jl}^{(i)}, 0 \leq i \leq r, 0 \leq j < l \leq n, X_0, \ldots, X_n]$ be the polynomial

$$Q := P\left(\sum_{j,l} \alpha_{jl}^{(0)}(X_l e_j - X_j e_l), \ldots, \sum_{j,l} \alpha_{jl}^{(r)}(X_l e_j - X_j e_l)\right)$$

which is given by a straight-line program of length bounded by $L + 2(r+1)n(n+1)$. Let $\Omega := \{\omega_1, \ldots, \omega_N\}$ be a correct test sequence for polynomials in the variables $\alpha_{jl}^{(i)}, 0 \leq i \leq r, 0 \leq j < l \leq n$, of degree bounded by $(r+1)\deg V$, which can be evaluated by a straight-line program of length bounded by $L + 2(r+1)n(n+1)$. Then $N \leq 6(L + 2(r+2)n(n+1))^2$ and

$$x \notin V \iff \bigvee_{i=1}^{N} Q(\omega_i, x) \neq 0.$$

For each $1 \leq i \leq N$, let $Q_i := Q(\omega_i, x)$. It is immediate that the polynomials $Q_1, \ldots, Q_N$ verify the conditions stated. ∎

Now we are able to state our second result which follows immediately from Theorem 1 and Lemma 2.

PROPOSITION 3. *Let $F_1, \ldots, F_s$ be homogeneous polynomials in $k[X_0, \ldots, X_n]$ and let $d \geq n$ be an integer such that* $\deg F_i \leq d$ $(1 \leq i \leq s)$. *Let*

$$V := \left\{x \in \mathbb{P}^n \colon F_1(x) = 0 \wedge \cdots \wedge F_s(x) = 0\right\}.$$

Let $r = \dim V$ and let V_r be the equidimensional component of V of dimension r.

Then, there exists a well-parallelizable algorithm with sequential complexity bounded by $s^{O(1)} d^{O(n)}$ whose input is the set of polynomials $\{F_1, \ldots, F_s\}$ encoded in dense form and whose output is a set of $N \leq s^{O(1)} d^{O(n)}$ polynomials $Q_1, \ldots, Q_N$ whose degrees are bounded by $(r+1) \cdot \deg V_r$, given by a straight-line program of length $s^{O(n)} d^{O(n)}$, such that

$$V_r = \{x \in \mathbb{P}^n : Q_1(x) = 0 \wedge \cdots \wedge Q_N(x) = 0\}. \qquad ∎$$

Remark 4. Let k be a field and let $\bar{k}$ be an algebraic closure of k. We can consider $\mathbb{P}^n(\bar{k})$ with the Zariski topology induced by polynomials with coefficients in k (i.e., the closed sets are the sets of zeroes of homogeneous polynomials in $k[X_0, \ldots, X_n]$). There is a well-known notion of irreducible variety associated to this topology and, therefore, a notion of unique irreducible decomposition of varieties over k.

Provided we are given an efficient algorithm to factorize multivariate polynomials over k given by straight-line programs, our algorithm can be adapted to obtain from homogeneous polynomials $F_1, \ldots, F_s \in k[X_0, \ldots, X_n]$ defining a variety V, the k-irreducible decomposition of its equidimensional component of the greatest dimension: once we obtain its Chow form, we factorize it and apply Lemma 2 to each factor.

3.3. *The Affine Case*

Now we are going to adapt the algorithm given in Theorem 1 in order to obtain polynomials defining the equidimensional component of the greatest dimension of an affine variety.

We consider the embedding $\iota : \mathbb{A}^n \to \mathbb{P}^n$ such that $\iota(x_1, \ldots, x_n) = (1 : x_1 : \ldots : x_n)$. If $W \subseteq \mathbb{A}^n$ is an affine variety, the closure of $\iota(W)$ in $\mathbb{P}^n$ will be called the projective closure of W and will be denoted by $\overline{W}$. Note that $\deg W = \deg \overline{W}$ holds.

Let $f_1, \ldots, f_s$ be polynomials $k[X_1, \ldots, X_n]$ whose degrees are bounded by an integer $d \geq n$ and let

$$V = \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0\}.$$

Let $r = \dim V$ and let V_r be the equidimensional component of V of dimension r. We will recover the equidimensional component V_r of V from the equidimensional component of the greatest dimension of the projective closure of V.

LEMMA 4. *Let $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$ and let $d \geq n$ be an integer such that* $\deg f_i \leq d\,(1 \leq i \leq s)$. *Let $V = \{x \in \mathbb{A}^n\colon f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0\}$ and let $r = \dim(V)$.*

Then, there exists a well-parallelizable algorithm with sequential complexity bounded by $s^{O(1)}d^{O(n)}$ whose input is the set of polynomials $\{f_1, \ldots, f_s\}$ encoded in dense form, and whose output is the Chow form P of the equidimensional component $\overline{V_r}$ of $\overline{V}$ of dimension r, given by a straight-line program of length $s^{O(1)}d^{O(n)}$.

Proof. For a given set $A \subseteq \mathbb{P}^n$ we denote by $\Gamma(A)$ the set

$$\Gamma(A) = \big\{(y, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n / x \in A \wedge L^{(0)}(y, x) = 0 \wedge \cdots \wedge L^{(r)}(y, x) = 0\big\}.$$

Let U be the set

$$U = \{x \in \mathbb{P}^n(\bar{k}) / f_1^{(h)}(x) = 0 \wedge \cdots \wedge f_s^{(h)}(x) = 0 \wedge x_0 \neq 0\},$$

where $f_i^{(h)}$ are the homogenizations of the polynomials f_i with respect to the variable X_0. Note that the set $\overline{U}$ is the projective closure of V and, therefore, $\dim \overline{U} = \dim V = r$. Let π: $(\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \longrightarrow (\mathbb{P}^n)^{r+1}$ be the projection map.

Under these notations, the arguments given in the proof of Theorem 1 imply that the Chow form of the equidimensional component $\overline{V}_r$ of $\overline{V}$ of the greatest dimension is a square-free polynomial whose set of zeroes is the equidimensional component of codimension 1 of $\pi(\Gamma(\overline{U}))$.

We assert that $\Gamma(\overline{U}) = \overline{\Gamma(U)}$. Let $V^{(h)} := \{x \in \mathbb{P}^n(\bar{k}) / f_1^{(h)}(x) = 0 \wedge \cdots \wedge f_s^{(h)}(x) = 0\}$, and let $V^{(h)} = \bigcup_{C \in \mathscr{C}} C$ be the decomposition of $V^{(h)}$ into irreducible components. Let $\mathscr{C}' := \{C \in \mathscr{C} : C \subseteq \{X_0 = 0\}\}$. Then $U = \bigcup_{C \notin \mathscr{C}'} (C \cap \{X_0 \neq 0\})$ and $\overline{U} = \bigcup_{C \notin \mathscr{C}'} C$. Taking into account that, for each irreducible closed set C, the set $\Gamma(C)$ is irreducible, it follows that

$$\overline{\Gamma(U)} = \bigcup_{C \notin \mathscr{C}'} \overline{\Gamma(C \cap \{X_0 \neq 0\})} = \bigcup_{C \notin \mathscr{C}'} \Gamma(C) = \Gamma(\overline{U}).$$

As the projection is a closed map, it suffices to compute a polynomial whose set of zeroes is the equidimensional component of codimension 1 of $\overline{\pi(\Gamma(U))}$. In order to do so, we will follow the ideas in Theorem 1.

Note that $\pi(\Gamma(U))$ is the set defined in $(\mathbb{P}^n)^{r+1}$ by the formula

$$\begin{aligned} \exists x_0 \cdots \exists x_n \colon f_1^{(h)}(x_0, \ldots, x_n) = 0 \wedge \cdots \wedge f_s^{(h)}(x_0, \ldots, x_n) = 0 \wedge x_0 \neq 0 \\ \wedge L^{(0)}(y_0^{(0)}, \ldots, y_n^{(0)}, x_0, \ldots, x_n) = 0 \wedge \cdots \\ \wedge L^{(r)}(y_0^{(r)}, \ldots, y_n^{(r)}, x_0, \ldots, x_n) = 0, \end{aligned}$$

which is equivalent to

$$\begin{aligned} \exists x_1 \cdots \exists x_n : f_1(x_1, \ldots, x_n) = 0 \wedge \cdots \wedge f_s(x_1, \ldots, x_n) = 0 \\ \wedge L^{(0)}(y_0^{(0)}, \ldots, y_n^{(0)}, 1, x_1, \ldots, x_n) = 0 \wedge \cdots \\ \wedge L^{(r)}(y_0^{(r)}, \ldots, y_n^{(r)}, 1, x_1, \ldots, x_n) = 0. \end{aligned}$$

We apply to this formula the algorithm in [12] to obtain a quantifier-free formula equivalent to it, and we proceed as in Theorem 1 to compute a polynomial P whose set of zeroes is the equidimensional component of codimension 1 of $\overline{\pi(\Gamma(U))}$. This polynomial P is the Chow form of $\overline{V}_r$ and it is given by a straight-line program of length $s^{O(1)} d^{O(n)}$. The sequential complexity of this algorithm is bounded by $s^{O(1)} d^{O(n)}$. ∎

Note that, using the same notations, from Lemmas 5 and 2 we obtain polynomials $Q_1, \dots, Q_N$ such that

$$\overline{V}_r = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n : Q_1(x_0, \dots, x_n) = 0 \wedge \cdots \wedge Q_N(x_0, \dots, x_n) = 0\}$$

and, therefore

$$V_r = \overline{V}_r \cap \mathbb{A}^n = \{x \in \mathbb{A}^n : Q_1(1, x_1, \dots, x_n) = 0 \wedge \cdots \wedge Q_N(1, x_1, \dots, x_n) = 0\}.$$

Then, we have proved the following

PROPOSITION 5. *Let $f_1, \dots, f_s$ be polynomials in $k[X_1, \dots, X_n]$ and let $d \geq n$ be an integer such that* $\deg f_i \leq d (1 \leq i \leq s)$. *Let*

$$V := \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0\}.$$

Let $r = \dim V$ and let V_r be the equidimension component of V of dimension r.

Then, there exists a well-parallelizable algorithm with sequential complexity bounded by $s^{O(1)} d^{O(n)}$ whose input is the set of polynomials $\{f_1, \dots, f_s\}$ encoded in dense form and whose output is a finite set of $N \leq s^{O(1)} d^{O(n)}$ polynomials $q_1, \dots, q_N$ with degrees bounded by $(r+1) \cdot \deg(V_r)$ given by a straight-line program of length $s^{O(1)} d^{O(n)}$, such that

$$V_r = \{x \in \mathbb{A}^n : q_1(x) = 0 \wedge \cdots \wedge q_N(x) = 0\}. \quad \blacksquare$$

Again, provided we are given an efficient algorithm to factorize multivariate polynomials over k given by straight-line programs, our algorithm can be adapted in the sense of Remark 4 to obtain the k-irreducible decomposition of the equidimensional component of the greatest dimension of an affine variety.

Remark 7. From the previous results and the quantifier elimination algorithm in [12] we can deduce that there exists a well-parallelizable algorithm that, given polynomials $f_1, \dots, f_s \in k[X_1, \dots, X_n]$ whose degrees are bounded by $d \geq n$ defining an algebraic variety V, decides whether V is equidimensional or not. The sequential complexity of the algorithm is of order $s^{O(1)} d^{O(n)}$:

Applying the algorithm described in Proposition 6, we get $N \leq s^{O(1)} d^{O(n)}$ polynomials $q_1, \dots, q_N$ defining V_r, the equidimensional component of the greatest dimension of V. Note that V is equidimensional if and only if $V - V_r = \emptyset$. As

$$V - V_r = \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0 \wedge (q_1(x) \neq 0 \vee \cdots \vee q_N(x) \neq 0)\}$$

applying the algorithm in [12] to

$$\exists x_1 \cdots \exists x_n \left(\bigvee_{i=1}^{N} f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0 \wedge q_i(x) \neq 0 \right)$$

we can decide whether $V - V_r$ is empty or not.

As $\deg q_i \leq (r+1) \cdot d^n$, the sequential complexity of this algorithm is bounded by $s^{O(1)} d^{O(n)}$. This procedure can be applied in the projective case within the same complexity bounds.

REFERENCES

1. S. J. Berkowitz, On computing the determinant in small parallel time using a small number of processors, *Inform. Process. Lett.* **18** (1984), 147–150.
2. L. Caniglia, How to compute the Chow Form of an unmixed polynomial ideal in single exponential time, *in* "AAECC," pp. 25–41, Springer-Verlag, Berlin, 1990.
3. A. L. Chistov and D. Y. Grigor'ev, "Subexponential Time Solving Systems of Algebraic Equations," LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.
4. Noaï Fitchas, A. Galligo, and J. Morgenstern, Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields, *J. Pure Appl. Algebra* **67** (1990), 1–14.
5. M. Giusti and J. Heintz, Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles, *in* "Effective Methods in Algebraic Geometry" (T. Mora and C. Traverso, Eds.), Progress in Mathematics, Vol. 94, pp. 169–193, Birkhauser, Basel, 1991.
6. M. Giusti and J. Heintz, La détermination des points isolés et de la dimension d'une veriété algébrique peut se faire en temps polynomial, *in* "Computational Algebraic Geometry and Commutative Algebra, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra," *Symposia Matematica*, Vol. XXXIV, pp. 216–256, 1993.
7. J. Heintz, On the computational complexity of polynomials and bilinear mappings, a survey, *in* "Proc. 5th Internat. Conf. AAECC 5, Menorca, 1987" (L. Huguet and A. Poli, Eds.), Lecture Notes in Computer Science, Vol. 356, pp. 269–300, Springer-Verlag, Berlin/New York, 1989.
8. J. Heintz and C. P. Schnorr, Testing polynomials which are easy to compute, *Monogr. de l'Enseignement Math.* **30** (1982), 237–254.
9. E. Kaltofen, Greatest common divisors of polynomials given by straight line programs, *J. Assoc. Comput. Mach.* **35**, No. 1 (1988), 231–264.
10. T. Krick and L. M. Pardo, A computational method for diophantine approximation, *Progress Math.* **143** (1996), 193–253.
11. K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, *Proc. 18th ACM Symp. Theory of Computing* (1986), 338–339.
12. S. Puddu and J. Sabia, An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs, *J. Pure Appl. Algebra* **129** (1998), 173–200.
13. I. R. Shafarevich, "Basic Algebraic Geometry," Springer-Verlag, Berlin/New York, 1974.
14. V. Strassen, Vermeidung von Divisionen, *Crelle J. Reine Angew. Math.* **264** (1973), 184–202.