The Hardness of Polynomial Equation Solving[*]

D. Castro[1], M. Giusti[2], J. Heintz[1,3,4], G. Matera[4,5], L.M. Pardo[1,2]

13th February 2003

Dedicated to Michel Demazure

> *".......Il est fréquent, devant un problème concret, de trouver un théorème qui "s'applique presque"....... . Le rôle des contre–exemples est justement de délimiter le possible, et ce n'est pas par perversité (ou en tout cas pas totalement) que les textes mathématiques exhibent des monstres"* M. Demazure, 1987

Abstract

Elimination theory is at the origin of algebraic geometry in the 19-th century and deals with algorithmic solving of multivariate polynomial equation systems over the complex numbers, or, more generally, over an arbitrary algebraically closed field. In this paper we investigate the *intrinsic* sequential time complexity of *universal* elimination procedures for *arbitrary continuous* data structures encoding input and output objects of elimination theory (i.e. polynomial equation systems) and admitting the representation of certain limit objects.

Our main result is the following: let be given such a data structure and together with this data structure a universal elimination algorithm, say $\mathcal{P}$, solving arbitrary parametric polynomial equation systems. Suppose that the algorithm $\mathcal{P}$ avoids "unnecessary" branchings and that $\mathcal{P}$ admits the efficient computation of certain natural limit objects (as

[*] Research was partially supported by the following Argentinian, French and Spanish grants : UBACyT X198, PIP CONICET 2461, UNGS 30/3003, CNRS FRE 2341 MEDICIS, DGCYT BFM2000–0349, HF-1999-055 and ALA 01–E3/02.

[1] *Depto. de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, E-39071 Santander, Spain.*

[2] *Laboratoire GAGE, Ecole Polytechnique, F-91128 Palaiseau Cedex, France.*

[3] *Depto. de Matemáticas, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I (1428) Buenos Aires, Argentina.*

[4] *Member of the National Council of Science and Technology (CONICET), Argentina.*

[5] *Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, Campus Universitario, José M. Gutiérrez 1150 (1613) Los Polvorines, Pcia. de Buenos Aires, Argentina.*

e.g. the Zariski closure of a given constructible algebraic set or the parametric greatest common divisor of two given algebraic families of univariate polynomials). Then $\mathcal{P}$ cannot be a polynomial time algorithm.

The paper contains different variants of this result and discusses their practical implications.

Keywords. Polynomial equation solving, elimination theory, complexity, continuous data structure, holomorphic and continuous encoding.

Contents

1 Introduction. Basic notions.

Complexity theory deals with the efficiency of answering mathematical questions about mathematical objects. In this context, mathematical objects happen usually to posses a *unique* encoding in a previously fixed data structure (e.g. integers are encoded by their bit representation, polynomials by their coefficients, etc.). Once a data structure is fixed, standard complexity theory searches for an efficient algorithm answering the mathematical questions under consideration and tries to certify the optimality of this algorithm.

However, things become somewhat more complicated in the particular case of geometric elimination theory (polynomial equation solving in algebraically or real closed fields). Complexity theory for geometric elimination requires *simultaneous* optimization of data structures *and* algorithms. In order to illustrate this statement, let us consider the following first order formula, say Φ, belonging to the language of the elementary theory of algebraically closed fields of characteristic zero:

$$(\exists X_1)\cdots(\exists X_n)\big(X_1-T-1=0\wedge X_1^2-X_2=0\wedge\cdots\wedge X_{n-1}^2-X_n=0\wedge Y=X_n^2\big).$$

The formula Φ contains two free variables, namely T and Y. Moreover Φ is logically equivalent to the following quantifier–free formula, which we denote by Ψ:

$$Y-\sum_{i=0}^{2^n}\binom{2^n}{i}T^i=0.$$

If we choose as our data structure the standard dense or sparse encoding of polynomials by their coefficients, then Φ has length $O(n)$, whereas the length of Ψ exceeds 2^n. However, if we encode polynomials by *arithmetic circuits* (or straight–line programs), then Φ and Ψ happen both to be of length $O(n)$, since the polynomial $\sum_{i=0}^{2^n}\binom{2^n}{i}T^i=(1+T)^{2^n}$ can be evaluated in $n+1$ steps, using iterated squaring.

For the dense (or sparse) representation of polynomials *superexponential* (sequential) time is necessary (and sufficient) in order to eliminate a *single* quantifier block (see e.g. [CGH89], [DFGS91], [GV88], [HRS89], [Can88]), whereas the elimination of an *arbitrary* number of quantifier blocks requires *doubly exponential* time in this data structure (see [Hei83], [Wei88], [DH88], [FGM90a], [FGM90b], [MP93] for lower and upper complexity bounds and [Ier89], [HRS90], [Ren92] for upper complexity bounds only).

The existing superexponential (mostly Gröbner basis) algorithms for the elimination of a single quantifier block are often asymptotically optimal for the dense and sparse encoding of polynomials. Nevertheless their complexity makes them infeasible for real world sized problems (however not so for impressive software demos). Moreover, a simple minded Gröbner basis approach to the elimination of a single block of quantifiers may lead to a doubly exponential complexity.

This situation suggests that these elimination algorithms require alternative data structures if one wishes to improve their complexity behaviour substantially. This observation led in the past to the idea of using arithmetic circuits for the representation of the polynomials occurring in the basic elimination procedures of algebraic and semialgebraic geometry (see [HS82], [HS81] and [Kal88] for an early application of this idea). This change of data structure allowed in a first attempt to reduce the complexity of the elimination of a single block of quantifiers from superexponential to single exponential time ([GH93], [GHS93], [FGS95], [KP94], [KP96], [Mat99]). However, the corresponding algorithms required the dense representation of the input polynomials and returned a circuit encoding of the output polynomials. Therefore these algorithms were unadapted to successive elimination of several quantifier blocks (see [PS98] for more details) and unable to profit from a possible special geometric feature of the input system.

In a second attempt ([GHMP95], [Par95], [GHM$^+$98], [GHH$^+$97], [GHMP97]), this problem could be settled by means of a new elimination procedure which transforms a given circuit representation of the input polynomials into a circuit representation of the output polynomials. The time complexity of this new procedure is roughly the circuit size of the input polynomials multiplied by a *polynomial* function of a certain geometric invariant of the input system, called its *degree.* Let us observe that the degree is always bounded by the Bézout–number of the input system and happens often to be considerably smaller.

For worst case input systems, the new algorithm becomes polynomial in the Bézout–number of the system, and this was the first time that this complexity goal could be reached without hiding an exponential extra factor (compare [MP97], [Roj00]).

Afterwards the new algorithm and its data structure was extended and refined in [HKP$^+$00], [GS99], [HMPS00], [HMW01], [GLS01], [Sch00], [Lec01], and in [BGHM97], [BGHM01] it was adapted to the problem of polynomial equation solving over the *reals.* A successful implementation of the full algorithm ([Lec00]) is based on [GLS01]. A partial implementation of the algorithm (including basic subroutines) is described in [BHMW02] (see also [CHLM00]). So far the account of successive improvements of data structures and algorithms for *symbolic* elimination. The complexity aspect of *numeric* elimination was treated in a series of papers ([SS93a], [SS93b], [SS93c], [SS96], [SS94], [CS99]; see also [BCSS98]). In [CHMP01] and [CMPS02] the bit complexity aspect of the above mentioned symbolic and numeric algorithms was analyzed and compared. Taking bit complexity and the bit representation of rational numbers into account, it turns out that a suitable numerical adaptation of the above mentioned new symbolic elimination algorithm has the best complexity performance between all known numerical elimination algorithms. Therefore we shall limit our attention in this paper to *symbolic* elimination procedures.

Let us now briefly sketch the known lower bound results for the complexity of arithmetic circuit based procedures for the elimination of a single quantifier block. Any such elimination algorithm which is *geometrically robust* in the sense of [HMPW98] requires necessarily exponential time on infinitely many inputs. Geometric robustness is a very mild condition that is satisfied by all known (symbolic) elimination procedures.

Moreover, suppose that there is given an algorithm for the elimination of a single quantifier block and suppose that this algorithm is in a suitable sense "universal", avoiding "unnecessary branchings" and able to compute Zariski closures of constructible sets and "parametric" greatest common divisors of algebraic families of univariate polynomials. Then necessarily this algorithm has to be robust and hence of non–polynomial time complexity [GH01]. In particular, any "reasonable" and "sufficiently general" procedure for the elimination of a single quantifier block produces geometrically robust arithmetic circuit representations of suitable elimination polynomials and therefore outputs of non–polynomial size in worst case.

In this paper we are going to argue that the non–polynomial complexity character of the known symbolic geometric elimination procedures is not a special feature of a particular data structure (like the dense, sparse or arithmetic circuit encoding of polynomials), but rather a consequence of the information encoded by the respective data structure (see Theorem 4 below).

1.1 Data structures for geometric objects.

Informally, we understand by a *data structure* a class, say $\mathcal{D}$, of "simple" mathematical objects which encode another class, say $\mathcal{O}$, of "complicated" ones. An element $D \in \mathcal{D}$ which encodes a mathematical object $O \in \mathcal{O}$ is called a *code* of $\mathcal{O}$. The data structure $\mathcal{D}$ is supposed to be embedded in a context, where we may process its elements, in order to answer a certain catalogue of well defined *questions* about the mathematical objects belonging to $\mathcal{O}$ (or about the object class $\mathcal{O}$ itself). Of course, the choice of the data structure $\mathcal{D}$ depends strongly on the kind of potential questions we are going to ask and on the time we are willing to wait for the answers.

The mathematical objects we are going to consider in this paper will always be polynomial functions or algebraic varieties and their codes will always belong to suitable affine ambient spaces. The *size* of a code is measured by the dimension of its ambient space.

The (optimal) encoding of *discrete* (e.g. finite) sets of mathematical objects is a well known subject in theoretical computer science and the main theme of Kolmogorov complexity theory ([LV93]; see also [Bor48]).

This paper addresses the problem of optimal encoding of *continuous* classes of mathematical objects. The continuous case differs in many aspects from the discrete one and merits particular attention. Any object class $\mathcal{O}$ we are considering in this paper will possess a *natural topology* and may be thought to be embedded in a (huge) affine or projective ambient space. The given topology of $\mathcal{O}$ becomes always induced by the Zariski (or strong) topology of its ambient space. In this paper, the *closure* $\overline{\mathcal{O}}$ of the object class $\mathcal{O}$ in its ambient space will generally have a natural interpretation as a class of objects of the same nature as $\mathcal{O}$. In this sense we shall interpret a given element of $\overline{\mathcal{O}} \setminus \mathcal{O}$ as a *limit* (or *degenerate*) object of $\mathcal{O}$. We shall always suppose that data structures, object classes and graphs of encodings form *constructible* subsets of their respective ambient spaces.

If $\mathcal{O}$ is for example a class of equidimensional closed subvarieties of fixed dimension and degree of a suitable projective space, then the topology and the ambient space of $\mathcal{O}$ may be given by the Chow coordinates of the objects of $\mathcal{O}$. Or if $\mathcal{O}$ is the class of polynomial functions of bounded arithmetic circuit complexity L, then $\mathcal{O}$ is contained in a finite dimensional linear subspace of the corresponding polynomial ring and has therefore a natural topology. The limit objects of $\mathcal{O}$ are then those polynomials which have approximative complexity at most L (see [Ald84], [BCS97] and Section 3.3.2 for details).

Let be given a data structure $\mathcal{D}$ encoding an object class $\mathcal{O}$. By assumption, $\mathcal{D}$ is embedded in a suitable affine or projective ambient space from which $\mathcal{D}$ inherits a natural topology. We shall always assume that $\mathcal{D}$ encodes $\mathcal{O}$ *continuously* or *holomorphically* (see Section 3.1 for precise, mathematical definitions). However, in order to capture the important case of the arithmetic circuit representation of polynomials, we shall not insist on the injectivity of the given encoding. More precisely, we say that $\mathcal{D}$ encodes $\mathcal{O}$ *injectively* or *unambiguously* if for any object $O \in \mathcal{O}$ the data structure $\mathcal{D}$ contains a single element encoding O (otherwise we call the encoding *ambiguous*).

A fundamental problem addressed in this paper is the following:

given an "efficient" (i.e. short) data structure $\mathcal{D}$ encoding the object class $\mathcal{O}$, how may we find another data structure $\overline{\mathcal{D}}$ encoding the object class $\overline{\mathcal{O}}$? How does the *size* of $\overline{\mathcal{D}}$ (i.e. the size of its codes) depend on the size of $\mathcal{D}$?

In Theorem 1, Corollary 3, Corollary 9 and in Section 4 below we shall see that the solution of this problem depends strongly on the type of questions about the object class $\overline{\mathcal{O}}$ which the data structure $\overline{\mathcal{D}}$ allows to answer.

This leads us to the subject of the questions we wish to be answered by a given data structure $\mathcal{D}$ encoding a given object class $\mathcal{O}$. We shall always require that any element $D \in \mathcal{D}$ encoding an object $O \in \mathcal{O}$ contains enough information in order to distinguish O from other elements of the object class $\mathcal{O}$. Thus a typical question we wish to be answered by the data structure $\mathcal{D}$ is the following:

let D and D' be two elements of $\mathcal{D}$ encoding two objects O and O' of $\mathcal{O}$. Are O and O' identical?

In other words, we require to be able to deduce whether $O = O'$ holds by means of processing the codes D and D'. We call this problem the *identity question* associated to the data structure $\mathcal{D}$. A common way to solve this identity question consists of the transformation of the (supposedly ambiguous) data structure $\mathcal{D}$ in a new one, which encodes the objects of $\mathcal{O}$ injectively.

Another typical question arises in the following context:
suppose additionally that the object class $\mathcal{O}$ consists of (total) functions which can be evaluated on a continuous (or discrete) domain R. Suppose furthermore that we have free access to any element of R. Let O be a given element of the object class $\mathcal{O}$ and let $D \in \mathcal{D}$ be an arbitrary code of O.

The question we wish to be answered by the data structure $\mathcal{D}$ about the object O is the following:

for any given argument value $r \in R$, what is the function value $O(r)$?

In other words, we require to be able to compute the function value $O(r)$ by means of processing the code D and the argument value r. We call this problem the *value question* associated to the data structure $\mathcal{D}$. Of course, for a class $\mathcal{O}$ of polynomial functions whose number of variables and degree was previously bounded, the value question for a continuous domain R can be reduced by means of interpolation techniques to the value question for a discrete domain, namely to the task of determining, for any monomial M and any polynomial function $O \in \mathcal{O}$, the coefficient of M in the polynomial O.

1.2 The rôle of data structures in elimination theory.

In algebraic geometry, polynomial equation systems are the "simple" mathematical objects which encode the real objects of interest: algebraic varieties or schemes. Except for the particular case of hypersurfaces, there is no *a priori* privileged *canonical* equation system that defines a given algebraic variety. It depends on the questions we are going to ask about the given variety, whether we shall feel the need to transform a given equation system into a new, better suited one for answering our questions.

As far as possible, we wish just to modify the syntactical form of our equations, without changing their meaning, represented by the underlying variety or scheme. Let us explain this in two different situations.

Very often the new equation system we are looking for is *uniquely determined* by the underlying variety or scheme and the syntactical requirements the new system has to satisfy. We meet this situation in the particular case of the (reduced) Gröbner basis of a given ideal (representing a scheme) for a previously fixed monomial order. The monomial order we shall choose depends on the kind of questions we are going to ask about the given scheme: we choose an (e.g. lexicographical) elimination order if we wish to "solve" the given equation system (i.e. uncouple its variables) or we choose a graded order if we wish to compute the Hilbert polynomial (the dimension and the degree) of the given (projective) scheme, etc. If we want to analyze a given scheme or variety by means of deformations, suitable (i.e. flat) equation systems, like Gröbner bases, are even mandatory ([BM93]). Although Gröbner bases are able to answer all typical questions about the variety or scheme under consideration, they are not well suited for the less ambitious task of polynomial equation solving (this constitutes the main elimination problem the paper is focusing on).

Since Gröbner bases are able to answer too many questions about the scheme or variety they define, they may become difficult to encode: a complete intersection ideal given by low degree binomial equations, may have a Gröbner basis of doubly exponential degree for a suitable elimination order, whereas it is possible to solve the corresponding elimination problem in singly exponential time using only polynomials of singly exponential degree (see [DFGS91], [KP96], [HMPS00]).

Let us consider another case of this general situation:
for the particular task of polynomial equation solving it suffices to replace the original algebraic variety (which is supposed to be equidimensional) by a birationally equivalent hypersurface in a suitable ambient space. This hypersurface and its minimal equation may be produced by means of generic linear projections (see e.g. [Kro82], [CG83], [GM89], [Can88], [CGH89], [DFGS91], [GH91], [GH93], [KP96], [GHM$^+$98], [GHH$^+$97]) or by means of dual varieties (see [GKZ94] and the references cited there). The minimal equation encodes the necessary information about the dimension and degree of the original algebraic variety and about a suitable set of independent variables. However, as a consequence of Bézout's Theorem, the degree of the canonical output equation may increase exponentially with respect to the degree of the given input equations if we apply this strategy of elimination. We call an elimination procedure *Kronecker–like* if in terms of suitable data structures, the procedure computes from the representation of equations of the given variety a representation of the minimal equation of the corresponding hypersurface (see Section 5.1 for more details).

In either case of this general situation, we need an *input object* (a polynomial equation system describing an algebraic variety or scheme) and an *output object* that describes the same variety or scheme (or a birationally equivalent one) and satisfies some additional syntactical requirements (allowing e.g. the uncoupling of the variables of the original system). The corresponding elimination problem maps input objects to output objects. Since an output object may have degree exponential in the degree of the corresponding input object we are led to ask about short encodings of high degree polynomials in few variables. In this context let us mention the main outcome of [GHM$^+$98], namely the observation that using the arithmetic circuit representation, elimination polynomials (i.e. the output objects of Kronecker–like procedures) have always size polynomial in their degree, whereas the size of their sparse (or dense) representation may become exponential in this quantity. But unfortunately, elimination polynomials may have exponential degrees. This inhibits the elimination procedure of [GHM$^+$98] and [GHH$^+$97] to become polynomial in the input length, at least in worst case.

We consider therefore in more generality the following task:

let be given an elimination problem and a data structure $\mathcal{D}$ encoding the input objects. Find a data structure $\mathcal{D}^*$ encoding the corresponding output objects and an elimination algorithm $\mathcal{P}$ which maps input codes belonging to $\mathcal{D}$ to output codes belonging to $\mathcal{D}^*$ and solves the given elimination problem.

In this terminology, the main problem this paper tries to solve can be formulated as follows:

is it possible to find in the given situation a data structure $\mathcal{D}^*$ and a continuous algorithm $\mathcal{P}$ (in the sense specified in Sections 2 and 5) such that the size of each output code belonging to $\mathcal{D}^*$ is only polynomial in the size of the corresponding input code belonging to $\mathcal{D}$? Under which circumstances do such a data structure $\mathcal{D}^*$ and such an algorithm $\mathcal{P}$ exist and under which circumstances do they not?

As mentioned before, the solution of this problem depends strongly on the questions about the output objects we wish to be answered by the output data structure $\mathcal{D}^*$.

In view of the methodological progress made in [GHM$^+$98], [GHH$^+$97], [GHMP97], [HKP$^+$00], [GLS01] and [HMW01] (leading to a substantial improvement of previously known complexity bounds) and motivated by our interest in lower complexity bounds, we limit our attention to basic and relatively simple elimination problems of the following type:

(i) Let be given a zero–dimensional algebraic variety V by an input equation system in n variables $X_1, \ldots, X_n$ and let be given a supplementary input polynomial F in these n variables and possibly some additional parameters $U_1, \ldots, U_r$. Let $X := (X_1, \ldots, X_n)$ and $U := (U_1, \ldots, U_r)$ and let us suppose that the input equation system and F have short encodings in a previously fixed input data structure $\mathcal{D}$. The problem is to find an output data structure $\mathcal{D}^*$ and a Kronecker–like elimination procedure $\mathcal{P}$ such that $\mathcal{P}$ associates to each input code of $\mathcal{D}$ representing a specialization u of the parameters U of F, an output code of $\mathcal{D}^*$ representing the canonical elimination polynomial of $F(u, X)$ with respect to the given variety V (see Sections 5.1 and 5.3 for definitions and an example).

(*ii*) Let be given a class $\mathcal{O}$ of mathematical objects and a data structure $\mathcal{D}$ encoding the object class $\mathcal{O}$. Suppose that $\mathcal{O}$ and $\mathcal{D}$ satisfy all general assumptions we made before on this kind of mathematical entities. Find a data structure $\mathcal{D}^*$ and a procedure $\mathcal{P}$ such that $\mathcal{D}^*$ encodes the topological closure $\overline{\mathcal{O}}$ of the object class $\mathcal{O}$ and such that $\mathcal{P}$ maps any element of $\mathcal{D}$ encoding a given object O of $\mathcal{O}$ to an element of $\mathcal{D}^*$ encoding the same object O.

In case of problems of type (*ii*), a typical example of such a procedure $\mathcal{P}$ for arithmetic circuit represented rational functions of bounded degree d is the "Vermeidung von Divisionen" algorithm of [Str73b] (see also [KP96]). In this case the limit objects are polynomials of degree at most $2d + 1$ (see [Ald84] for details). Another example of such a procedure is the transformation (by means of "tensoring") of approximative algorithms for matrix multiplication into exact ones [BCS97].

In elimination theory one meets very natural non–closed input object classes with limit objects not encoded by the given input data structure. However, such a limit object may possess a well–defined output object. In this case one may require that the given output data structure is able to encode this output object. This is the typical context where a problem of type (*ii*) arises in elimination theory.

Another context, related to approximation and interpolation theory is the following:

let $\omega : \mathcal{D} \to \mathcal{O}$ be a given encoding of an object class of t–variate polynomial functions over $\mathbb{C}$ having degree bounded by an a priori constant Δ. Consider $\mathcal{O}$ as a metric space equipped with the corresponding (strong) topology. Suppose that the encoding ω is holomorphic, allowing for each code $D \in \mathcal{D}$ and any argument $r \in \mathbb{C}^t$ the computation of the value $\omega(D)(r)$ using a fixed number of arithmetic operations in $\mathbb{C}$ (see Section 3.1 for details). Let $O \in \overline{\mathcal{O}} \backslash \mathcal{O}$ be a limit object of $\mathcal{O}$, let $(D_i)_{i \in \mathbb{N}}$ be a sequence of codes of $\mathcal{D}$ such that the sequence $(\omega(D_i))_{i \in \mathbb{N}}$ converges to the limit object O and let $r \in \mathbb{C}^t$ be a given argument. As one easily sees, O is again a t–variate polynomial over $\mathbb{C}$ of degree at most Δ and therefore the value $O(r)$ is well defined. Moreover, the sequence of complex numbers $(\omega(D_i)(r))_{i \in \mathbb{N}}$ converges to the value $O(r)$. However, the convergence rate of $(\omega(D_i)(r))_{i \in \mathbb{N}}$ will typically depend on the argument r. Our goal is to compute the value $O(r)$ using only a *fixed* number of arithmetic operations and limit processes in $\mathbb{C}$ for sequences which do not depend on the argument r. We reach this goal if we are able to solve in this context problem (*ii*) by a data structure which answers the value question.

All known algorithms solving problem (*i*) or, limited to the context of classical elimination theory, problem (*ii*), possess branching–free versions of the same order of complexity. We shall therefore consider only *branching–free* algorithms for the solution of these two elimination problems. In this case, we shall always assume that our output codes depend *holomorphically* (or at least continuously) on our input codes (see Section 2.2 for details).

An elimination algorithm is called *universal* if it solves for appropriate input and output data structures any standard elimination problem on arbitrary inputs consisting of boolean combinations of *parameter dependent* polynomial equations. A universal elimination algorithm is called *branching–parsimonious* if it avoids branchings for the solution of suitable instances of problems of type (*i*) and (*ii*).

This paper is organized as follows:

In Section 2 we introduce the language and tools from algebraic geometry and algebraic complexity theory we are going to use in this paper. In Section 3 we discuss different types of encodings of object classes: holomorphic, robust and continuous ones. We prove our first main result, namely Theorem 1, saying that any holomorphic (ambiguous) encoding may be replaced by a continuous and unambiguous one of similar size. We retake the subject of this section in an appendix of this paper, namely in Section A, generalizing Theorem 1 to Corollary 9 and estimating the VC–dimension of a given, holomorphically encoded object class in terms of the size of its encoding.

In Section 4 we introduce the main technique we are going to apply in this paper in order to prove lower bounds for robust encodings of specific object classes. We exemplify this technique by two fundamental examples.

In Section 5 we apply the tools developed in the preceding sections to elimination theory. We introduce the notion of a robust elimination procedure for flat families of zero–dimensional elimination problems and show that any robust elimination procedure requires necessarily exponential (sequential) time on infinitely many inputs (Theorem 3). This result is then used in order to prove the second main result of this paper, namely Theorem 4, which may be paraphrased as follows:

Suppose that there is given a universal, branching–parsimonious elimination procedure $\mathcal{P}$ which is also able to solve in the context of elimination theory suitable problems of the above type (*ii*). In particular, we suppose that the procedure $\mathcal{P}$ is able to eliminate quantifiers in parametric existential first order formulas of the language of the elementary theory of algebraically closed fields of characteristic zero and that $\mathcal{P}$ is able to compute equations for the Zariski closure of any given constructible set and the generically square–free parametric greatest common divisor of any given algebraic family of univariate polynomials (see Sections 2.2, 5.2 and 5.4 for precise, mathematical definitions). Then, the elimination procedure $\mathcal{P}$ cannot be of polynomial (sequential) time complexity.

In conclusion, a universal, branching–parsimonious procedure for the elimination of a single existential quantifier block which is able to solve suitable problems of type (ii) cannot be polynomial. Let us remark that all known universal elimination procedures satisfy this requirement since they are based on subroutines (in particular greatest common divisor computations) which behave well under specialization.

All these results are formulated in an *exact* computation model which allows to represent all known symbolic and seminumeric elimination procedures (based on the sparse or dense or the arithmetic circuit representation of polynomials).

2 Notions and notations.

2.1 Language and tools from algebraic geometry.

Let k be an infinite, perfect field which we think to be "effective" with respect to arithmetic operations as addition/subtraction, multiplication/division and extraction of p–th roots in case k has positive characteristic p. Let $\overline{k}$ be an algebraically closed field containing k (in the sequel we shall call such a field *an algebraic closure of* k.

Most of the statements and arguments of this paper will be independent of the characteristic of k. Therefore the reader may assume without loss of generality that k is of characteristic zero. For the sake of simplicity we shall assume in this case $k := \mathbb{Q}$ and $\overline{k} = \mathbb{C}$. We denote by $\mathbb{N}$ the set of natural numbers and by $\mathbb{Z}_{\geq 0}$ the set of nonnegative integers.

Fix $n \in \mathbb{Z}_{\geq 0}$ and let $X_0, \dots, X_n$ be indeterminates over k. We denote by $\mathbb{A}^n := \mathbb{A}^n(\overline{k})$ the n–dimensional affine space and by $\mathbb{P}^n := \mathbb{P}^n(\overline{k})$ the n–dimensional projective space over $\overline{k}$. The spaces $\mathbb{A}^n$ and $\mathbb{P}^n$ are thought to be endowed with their respective Zariski topologies over k and with their respective sheaves of k–rational functions with values in $\overline{k}$. Thus the points of $\mathbb{A}^n$ are elements $(x_1, \dots, x_n)$ of $\overline{k}$ and the points of $\mathbb{P}^n$ are (non uniquely) represented by nonzero elements $(x_0, \dots, x_n)$ of $\overline{k}^{n+1}$ and denoted by $(x_0 : \cdots : x_n)$. The indeterminates $X_1, \dots, X_n$ are considered as the coordinate functions of the affine space $\mathbb{A}^n$. The coordinate ring (of polynomial functions) of $\mathbb{A}^n$ is identified with the polynomial ring $k[X_1, \dots, X_n]$. Similarly we consider the (graded) polynomial ring $k[X_0, \dots, X_n]$ as the projective coordinate ring of $\mathbb{P}^n$. Consequently we represent rational functions of $\mathbb{P}^n$ as quotients of homogeneous polynomials of equal degree belonging to $k[X_0, \dots, X_n]$. Let $F_1, \dots, F_s$ be polynomials which belong to

$k[X_1, \dots, X_n]$ or are homogeneous and belong to $k[X_0, \dots, X_n]$. We denote by $\{F_1 = 0, \dots, F_s = 0\}$ or $V(F_1, \dots, F_s)$ the algebraic set of common zeroes of the polynomials $F_1, \dots, F_s$ in $\mathbb{A}^n$ and $\mathbb{P}^n$ respectively. We consider the set $V := \{F_1 = 0, \dots, F_s = 0\}$ as (Zariski–)closed (affine or projective) subvariety of its ambient space $\mathbb{A}^n$ or $\mathbb{P}^n$ and call V the affine or projective variety defined by the polynomials $F_1, \dots, F_s$. We think the variety V to be equipped with the induced Zariski topology and its sheaf of rational functions. The irreducible components of V are defined with respect to its Zariski topology over k . We call V irreducible if V contains a single irreducible component and equidimensional if all its irreducible components have the same dimension. The dimension $dim\, V$ of the variety V is defined as the maximal dimension of all its irreducible components. If V is equidimensional we define its (geometric) degree as the number of points arising when we intersect V with $dim\, V$ many generic (affine) linear hyperplanes of its ambient space $\mathbb{A}^n$ or $\mathbb{P}^n$. For an arbitrary closed variety V with irreducible components $\mathcal{C}_1, \dots, \mathcal{C}_t$ we define its degree as $\deg V := \deg \mathcal{C}_1 + \cdots + \deg \mathcal{C}_t$. With this definition of degree the intersection of two closed subvarieties V and W of the same ambient space satisfies the Bézout inequality

$$\deg V \cap W \leq \deg V \deg W$$

(see [Hei83], [Ful84], [Vog84]).

We denote by $k[V]$ the affine or (graded) projective coordinate ring of the variety V. If V is irreducible we denote by $k(V)$ its field of rational functions. In case that V is a closed subvariety of the affine space $\mathbb{A}^n$ we consider the elements of $k[V]$ as $\overline{k}$–valued functions mapping V into $\overline{k}$. The restrictions of the projections $X_1, \dots, X_n$ to V generate the coordinate ring $k[V]$ over k and are called the coordinate functions of V. The data of n coordinate functions of V fixes an embedding of V into the affine space $\mathbb{A}^n$. Morphisms between affine and projective varieties are induced by polynomial maps between their ambient spaces which are supposed to be homogeneous if the source and target variety is projective.

Replacing the ground field k by its algebraic closure $\overline{k}$, we may apply all this terminology again. In this sense we shall speak about the Zariski topologies and coordinate rings over $\overline{k}$ and sheaves of $\overline{k}$–rational functions. In this more general context varieties are defined by polynomials with coefficients in $\overline{k}$. If we want to stress that a particular variety V is defined by polynomials with coefficients in the ground field k, we shall say that V is *k–definable* or *k–constructible.* The same terminology is applied to any set determined by a (finite) boolean combination of k–definable closed subvarieties of $\mathbb{A}^n$ or $\mathbb{P}^n$. By a *constructible* set we mean simply a $\overline{k}$–constructible one. Constructible and k–constructible sets are always thought to be equipped with their corresponding Zariski topology. In case of $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$ we shall sometimes also consider the *euclidean* (i.e. "*strong*") topology of $\mathbb{A}^n$ and $\mathbb{P}^n$ and their constructible subsets.

The rest of our terminology and notation of algebraic geometry and commutative algebra is standard and can be found in [Lan58], [Sha84], [Mum88, Chapter I], and in [Lan93], [AM69], [Mat80].

2.2 Algorithmic models and complexity measures.

The algorithmic problems we are going to consider in this paper will depend on *continuous parameters* and therefore the corresponding input data structures have to contain entries for these parameters. We call them *problem* or *input parameters.*

Once such a parametric problem is given, the specialization of the parameters representing input objects are called (admissible) *problem* or *input instances.* Thus the problem parameters may in principle be algebraically dependent. An algorithm solving the given problem operates on the corresponding input data structure and produces for each admissible input instance an *output instance* which belongs to a previously chosen output data structure. We shall always require that output instances depend *rationally* on the input parameters. Since we limit in this paper our attention to branching–free algorithms, particular admissible input instances may not produce well defined output instances. In order to surmount this difficulty, we shall in the sequel admit certain limit processes which we modelize using the notion of places from valuation theory. These places will mimic the process of limit determination and calculation by means of de l'Hôpital's rule.

The chosen output data structure must enable us to answer certain previously fixed questions about the output objects of our algorithmic problem.

Let us consider the case that these output objects are polynomial functions and that we wish to answer the value question for these functions (we shall say that we want to "compute" or "evaluate" them). For the sake of definiteness let us suppose that there is given an algorithmic problem depending on r parameters and that this problem is expressible in the elementary language of algebraically closed fields over the ground field k. Let $U_1, \ldots, U_r$ be indeterminates representing the input parameters of the given problem. Let $S \subset \mathbb{A}^r$ be the Zariski closure of the set of admissible input instances and suppose that S is irreducible. Since our algorithmic problem is elementarily expressible over k, we conclude that S is k–definable. Let m be the size of the output data structure we are going to use for the solution of our problem. In the sense of this paper, a *(branching–free) continuous algorithm* computing for each admissible input instance the code of the corresponding output object, is given by certain rational functions $\theta_1, \ldots, \theta_m$ of $k(S)$ such that the rational map $\theta = (\theta_1, \ldots, \theta_m)$ is well–defined for any admissible input instance $u \in S$ and such that θ maps u to the corresponding output instance $\theta(u)$ (observe that the admissible input instances form a Zariski dense subset of S). Suppose now that our output objects are polynomial functions in the variables $Y_1, \dots, Y_t$. We call our algorithm *essentially division–free* if these polynomial functions belong to the polynomial ring $k[\theta_1, \dots, \theta_m][Y_1, \dots, Y_t]$. Thus essentially division–free algorithms do not contain divisions which involve any of the arguments $Y_1, \dots, Y_t$ of the output objects. Nevertheless such an algorithm is allowed to contain divisions involving exclusively elements of $k(U)$ which represent rational functions of $k(S)$. Once the value $\theta(u)$ is determined for an admissible input instance $u \in S$, the output objects may be evaluated in any point $y \in \mathbb{A}^t$ without using additional divisions. If moreover the parameter functions $\theta_1, \dots, \theta_m$ belong to the coordinate ring $k[S]$, we shall say that our algorithm if *totally division–free.* Unfortunately, the limitation to totally division–free algorithms would be too restrictive for an appropriate complexity analysis of geometric elimination problems. On the other hand, the notion of essentially division–free algorithm modelizes in a fairly realistic manner the intuitive meaning of algebraic (symbolic) tools in situations which admit branching–free procedures. In particular, it captures all today known parametric elimination procedures for these situations.

Suppose now that our algorithmic problem is well defined for any element of S. Thus the set of admissible input instances is the Zariski closed set S. Suppose furthermore that there are given rational functions $\theta_1, \dots, \theta_m \in k(U)$ and a constructible Zariski dense subset S_0 of S, such that the rational map $\theta = (\theta_1, \dots, \theta_m)$ is defined in any point of S_0 and such that θ represents an essentially division–free algorithm which solves our algorithmic problem for any input instance belonging to S_0 correctly. We shall say that the given algorithm can be (*uniquely*) *extended to the limit data structure S of S_0* (and to the corresponding limit input objects) if the following condition is satisfied:

for any input instance $u \in S$ and any place $\varphi : \overline{k}(S) \to \overline{k} \cup \{\infty\}$ whose valuation ring contains the local ring of the variety S at the point u, the values $\varphi(\theta_1), \dots, \varphi(\theta_m)$ are finite *and* uniquely determined *by the input instance u.*

We observe that this condition implies that $\theta_1, \dots, \theta_m$ belong to the integral closure of $k[S]$ in $k(S)$.

Intuitively speaking, we admit certain (algebraic) limit processes in the spirit of de l'Hôpital's rule in order to extend the given algorithms from S_0 to the limit data structure S. These limit processes are necessary because in elimination theory one often faces situations where parameters become algebraically dependent elements of domains which are not factorial. Greatest common divisor computations for polynomials with coefficients in these domains lead then to essential divisions of elements of these domains (i.e. to divisions whose results do not anymore belong to the given domain). These kind of situations can be found in [GH01] and Section 5.4.

In the context of this paper we shall not care about the representation of the rational map θ. However, in concrete situations, it is reasonable to think that the rational functions $\theta_1, \dots, \theta_m$ are represented by numerator and denominator polynomials belonging to $k[U_1, \dots, U_r]$, and that these polynomials are holomorphically encoded by a suitable data structure (see Section 3.1 for the notion of holomorphic encoding).

Let us finally exemplify the abstract notion of an essentially division–free algorithm in the context of arithmetic circuits (see [BCS97] for details).

An *essentially division–free arithmetic circuit* is an algorithmic device that can be represented by a labeled directed acyclic graph (*dag*) as follows: the circuit depends on certain input nodes, labeled by indeterminates over the ground field k. These indeterminates are thought to be subdivided in two disjoints sets, representing the *parameters* and the *variables* of the given circuit. For the sake of definiteness, let $U_1, \dots, U_r$ be the parameters and $Y_1, \dots, Y_t$ the variables of the circuit. Let $K := k(U_1, \dots, U_r)$. We call K the *parameter field* of the circuit. The circuit nodes of indegree zero which are not inputs are labeled by elements of k, which are called the *scalars* of the circuit (here "indegree" means the number of incoming edges of the corresponding node). Internal nodes are labeled by arithmetic operations (addition, subtraction, multiplication and division). We require that the internal nodes of the circuit represent polynomials in the variables $Y_1, \dots, Y_t$. We call these polynomials the intermediate results of the given circuit. The coefficients of these polynomials belong to the parameter field K. In order to achieve this requirement, we allow in an essentially division-free circuit only divisions which involve elements of K. Thus essentially division–free circuits do not contain divisions involving intermediate results which depend on the variables $Y_1, \dots, Y_t$. A circuit which contains only divisions by nonzero elements of k is called *totally division-free.*

Finally we suppose that the given circuit contains one or more nodes which are labeled as output nodes. The results of these nodes are called *outputs* of the circuit. Output nodes may occur labeled additionally by sign marks of the form "$= 0$" or "$\neq 0$" or may remain unlabeled. Thus the given circuit represents by means of the output nodes which are labeled by sign marks a system of parametric polynomial equations and inequations. This system determines in its turn for each admissible parameter instance a locally closed set (i.e. an embedded affine variety) with respect to the Zariski topology of the affine space $\mathbb{A}^t$ of variable instances. The output nodes of the given circuit which remain unlabeled by sign marks represent a parametric polynomial application (in fact a morphism of algebraic varieties) which maps for each admissible parameter instance the corresponding locally closed set into a suitable affine space. We shall interpret the system of polynomial equations and inequations represented by the circuit as a *parametric family of systems* in the variables of the circuit. The corresponding varieties constitute a *parametric family of varieties.* The same point of view is applied to the morphism determined by the unlabeled output nodes of the circuit. We shall consider this morphism as a *parametric family of morphisms.*

To a given essentially division–free arithmetic circuit we may associate different complexity measures and models. In this paper we shall be exclusively concerned with *sequential* computing *time*, measured by the *size* of the circuit. Our main complexity model is the non–scalar one, over the parameter field K. Exceptionally we will also consider the non–scalar complexity model over the ground field k. In the non–scalar complexity model over K we count only the *essential* multiplications (i.e. multiplications between intermediate results which actually involve variables and not exclusively parameters). This means that K–linear operations (i.e. additions and multiplications by arbitrary elements of K) are *cost free.* Similarly, k–linear operations are not counted in the non-scalar model over k.

Let $\theta_1, \dots, \theta_m$ be the elements of the parameter field K computed by the given circuit. Since this circuit is essentially division–free we conclude that its outputs belong to $k[\theta_1, \dots, \theta_m][Y_1, \dots, Y_t]$. Let L be the non–scalar size (over K) of the given circuit and suppose that the circuit contains q output nodes. Then the circuit may be rearranged (without affecting its non–scalar complexity nor its outputs) in such a way that the condition

$$m = L^2 + (2t-1)L + q(L+t+1) \tag{1}$$

is satisfied (see [BCS97, Chapter 9, Exercise 9.18]). In the sequel we shall always assume that we have already performed this rearrangement. Let $Y := (Y_1, \dots, Y_t)$, $\theta := (\theta_1, \dots, \theta_m)$ and let $f_1, \dots, f_q \in k[\theta][Y]$ be the outputs of the given circuit. Let $Z_1, \dots, Z_m$ be new indeterminates and write $Z := (Z_1, \dots, Z_m)$. Then there exist polynomials $F_1, \dots, F_q \in k[Z, Y]$ such that $f_1 = F_1(\theta, Y), \dots, f_q = F_q(\theta, Y)$ holds. Let us write $f := (f_1, \dots, f_q)$ and $F := (F_1, \dots, F_q)$. Consider the object class

$$\mathcal{O} := \{F(\zeta, Y) : \zeta \in \mathbb{A}^m\}$$

which we think represented by the data structure $\mathcal{D} := \mathbb{A}^m$ by means of the obvious encoding which maps each code $\zeta \in \mathcal{D}$ to the object $F(\zeta, Y) \in \overline{k}[Y]^q$.

For the moment, let us consider as input data structure the Zariski open subset $\mathcal{U}$ where the rational map $\theta = (\theta_1, \dots, \theta_m)$ is defined. Then the given essentially division–free arithmetic circuit represents an algorithm which computes for each input code $u \in \mathcal{U}$ an output code $\theta(u)$ representing the output object $f(u, Y) = F\big(\theta(u), Y\big)$. This algorithm is in the above sense essentially division–free. From identity (1) we deduce that the size m of the data structure $\mathcal{D}$ is closely related to the non–scalar size L of the given circuit. In particular we have the estimate

$$\sqrt{m} - (t+q) \leq L. \tag{2}$$

Later we shall meet specific situations where we are able to deduce from a previous (mathematical) knowledge of the mathematical object $f = (f_1, \ldots, f_q)$ a lower bound for the size of the output data structure of *any* essentially division–free algorithm which computes for an arbitrary input code $u \in \mathcal{U}$ the object $f(u, Y)$. Of course, in such situations we obtain by means of (2) a lower bound for the non–scalar size (over K) of *any* essentially division–free arithmetic circuit which solves the same task. In particular we obtain lower bounds for the total size and for the non–scalar size over k of all such arithmetic circuits.

3 Holomorphic, continuous and robust encodings.

3.1 Holomorphic and continuous encodings.

Let $\mathcal{O}$ be an object class of polynomial functions belonging to the polynomial ring $\overline{k}[Y_1, \ldots, Y_t]$. We shall say that $\mathcal{O}$ is *k–constructible* (or *k–definable*) if the following conditions are satisfied:

(*i*) The $\overline{k}$–vector space W generated by the elements of $\mathcal{O}$ in $\overline{k}[Y_1, \ldots, Y_t]$ is finite dimensional and there exists a $\overline{k}$–basis of W consisting of polynomials which belong to $k[Y_1, \ldots, Y_t]$ (we call such a basis of W *canonical*).

(*ii*) With respect to a given canonical basis of W, the object class $\mathcal{O}$ forms a k–constructible subset of W (observe that this condition does not depend on the particular canonical basis we have chosen).

Suppose now that the object class $\mathcal{O}$ is k–constructible and fix a canonical basis $P = (P_1, \ldots, P_{N'})$ of W. Without loss of generality we may assume $P_1, \ldots, P_{N'} \in \mathcal{O}$. The evaluation map $eval : W \times \mathbb{A}^t \to \mathbb{A}^1$ is defined by $eval(F, y) := F(y)$ for $F \in W$ and $y \in \mathbb{A}^t$. With respect to the canonical basis P, the evaluation map is k–definable and linear in its first argument. Since $P_1, \ldots, P_{N'}$ are polynomials of $k[Y_1, \ldots, Y_t]$ one sees easily that there exists a bound $\Delta \in \mathbb{N}$ with $\deg F \leq \Delta$ for any $F \in W$. Let $N \geq \binom{\Delta + t}{t}$. Then we have $N' \leq N$ and there exist suitable (generic interpolation) points $\eta_1, \ldots, \eta_N \in k^t$ such that the map $\varphi : W \to \mathbb{A}^N$ defined for $F \in W$ by $\varphi(F) := \big(eval(F, \eta_1), \ldots, eval(F, \eta_N)\big) = \big(F(\eta_1), \ldots, F(\eta_N)\big)$ induces a $\overline{k}$–linear embedding of W into the affine space $\mathbb{A}^N$. Observe that φ is k–definable with respect to the canonical basis P of W. In particular the image of φ is a k–definable linear subspace of $\mathbb{A}^N$ of dimension N'. Under the embedding φ, the object class $\mathcal{O}$ becomes a k–constructible subset of the *ambient space* $\mathbb{A}^N$ and the evaluation map becomes a k–definable morphism of algebraic varieties which is linear in its first argument and whose domain of definition can be extended (not uniquely) to the affine space $\mathbb{A}^N \times \mathbb{A}^t$.

This is the point of view we shall adopt in the sequel for k–constructible object classes of polynomial functions.

In particular we consider $\mathcal{O}$ and W as topological spaces equipped with the Zariski (or, in case $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$, with the strong topology) induced from the ambient space $\mathbb{A}^N$. Observe that the Zariski closure $\overline{\mathcal{O}}$ of the object class $\mathcal{O}$ is a k–definable closed subvariety of $\mathbb{A}^N$ whose degree does not depend on the particular $\overline{k}$–linear embedding φ we have chosen. We denote this degree by $\deg \overline{\mathcal{O}}$. Furthermore observe that any upper bound for the degree of the polynomials of $\overline{k}[Y_1, \ldots, Y_t]$ contained in $\mathcal{O}$ is also an upper bound for the degree of the polynomials in $\overline{\mathcal{O}}$.

We say that $\mathcal{O}$ is a *cone* if for any $\lambda \in \overline{k}$ the set $\lambda\mathcal{O} := \{\lambda f; f \in \mathcal{O}\}$ is contained in $\mathcal{O}$. Suppose that $\mathcal{O}$ is a cone. One immediately verifies that the $\overline{k}$–closure $\overline{\mathcal{O}}$ of $\mathcal{O}$ is a k–definable cone which is contained in W. Therefore the evaluation map $eval : W \times \mathbb{A}^t \to \mathbb{A}^1$ induces a k–definable morphism of algebraic varieties $\overline{\mathcal{O}} \times \mathbb{A}^t \to \mathbb{A}^1$ which we denote also by *eval*, which is homogeneous of degree one in its first argument (i.e. for $f \in \mathcal{O}$, $y \in \mathbb{A}^t$ and $\lambda \in \overline{k}$ we have $eval(\lambda f, y) = \lambda\, eval(f, y)$).

Let $\mathcal{O}$ be an arbitrary (not necessarily k–constructible) object class of polynomial functions belonging to the polynomial ring $\overline{k}[Y_1, \ldots, Y_t]$. Let $\gamma_1, \ldots, \gamma_m \in \mathbb{A}^t$ and let $\gamma := (\gamma_1, \ldots, \gamma_m)$. We say that m is the length of γ. We call γ a *correct test sequence* for the object class $\mathcal{O}$ if for any polynomial $F \in \mathcal{O}$ the following implication holds:

$$F(\gamma_1) = \cdots = F(\gamma_m) = 0 \Rightarrow F = 0.$$

We call γ an *identification sequence* for $\mathcal{O}$ if for any two polynomials $F_1, F_2 \in \mathcal{O}$ the following implication holds

$$F_1(\gamma_1) = F_2(\gamma_1), \ldots, F_1(\gamma_m) = F_2(\gamma_m) \Rightarrow F_1 = F_2.$$

Now we suppose that there exists a bound $\Delta \in \mathbb{N}$ with $\deg F \leq \Delta$ for any $F \in \mathcal{O}$. Let $N \geq \binom{\Delta + t}{t}$. We may interpret $\mathcal{O}$ as a subset of $\mathbb{A}^N$. Suppose now that there is given a k–definable data structure $\mathcal{D} \subset \mathbb{A}^L$ which encodes the object class $\mathcal{O}$ and contains a *Zariski–dense set of k–rational points.* Let $\omega : \mathcal{D} \to \mathcal{O}$ be this encoding and suppose that there exists a k–definable polynomial map $\rho : \mathbb{A}^L \times \mathbb{A}^t \to \mathbb{A}^1$ with $\rho(D, y) = \omega(D)(y)$ for any $D \in \mathcal{D}$ and any $y \in \mathbb{A}^t$. In these circumstances we say that ρ allows to answer the value question about the object class $\mathcal{O}$ *holomorphically.*

Remark 1 *Let assumptions and notations be as before. Then $\mathcal{O}$ is k–constructible and $\omega : \mathcal{D} \to \mathcal{O}$ is the restriction of a suitable k–definable polynomial map $\Omega : \mathbb{A}^L \to \mathbb{A}^N$.*

PROOF.– Let $N' \leq N$ be the dimension of the $\overline{k}$–vector space W generated in $\overline{k}[Y_1, \ldots, Y_t]$ by the elements of $\mathcal{O}$. Choose N generic interpolation points $\eta_1, \ldots, \eta_N \in k^t$ for the polynomials of $\overline{k}[Y_1, \ldots, Y_t]$ of degree at most Δ. Since the k–rational points are Zariski–dense in $\mathcal{D}$ we conclude that there exist $D_1, \ldots, D_{N'} \in \mathcal{D} \cap k^L$ such that for any choice of indices $1 \leq k_1 < \cdots < k_{N'} \leq N$ the $N' \times N'$–matrix

$$\big(\omega(D_i)(\eta_{k_j})\big)_{1 \leq i,j \leq N'} = \big(\rho(D_i, \eta_{k_j})\big)_{1 \leq i,j \leq N'}$$

is regular. Since for any such index choice this matrix is k–rational we deduce that $\omega(D_1), \ldots, \omega(D_{N'})$ are polynomials which belong to $\mathcal{O} \cap k[Y_1, \ldots, Y_t]$ and form a basis of the $\overline{k}$–vector space W. In the same manner as before, using the k–rational interpolation points $\eta_1, \ldots, \eta_N$, we may construct from ρ a k–definable polynomial map $\Omega : \mathbb{A}^L \to \mathbb{A}^N$ with $\Omega|_{\mathcal{D}} = \omega$ (here $\Omega|_{\mathcal{D}}$ denotes the restriction of the map Ω to the set $\mathcal{D}$). In particular we have $\Omega(\mathcal{D}) = \mathcal{O}$. Since the polynomial map Ω is k–definable we conclude that $\mathcal{O}$ is a k–constructible subset of $\mathbb{A}^N$. ■

The preceding considerations about object classes of polynomial functions and their encodings lead us to the following fundamental notions of this paper:

Definition 1 *Let be given a data structure $\mathcal{D} \subset \mathbb{A}^L$, an object class $\mathcal{O} \subset \mathbb{A}^N$ and an encoding $\omega : \mathcal{D} \to \mathcal{O}$.*

We call ω a k–definable encoding if the graph of ω is a k–constructible subset of the affine space $\mathbb{A}^L \times \mathbb{A}^N$.

Similarly the data structure $\mathcal{D}$ and the object class $\mathcal{O}$ are called k–constructible (or k–definable) if they form k–constructible subsets of the affine spaces $\mathbb{A}^L$ and $\mathbb{A}^N$ respectively.

Let $\omega : \mathcal{D} \to \mathcal{O}$ be k–definable. We call ω a continuous encoding if ω is a continuous map with respect to the Zariski topologies of $\mathcal{D}$ and $\mathcal{O}$ (or, in case $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$, with respect to their strong topologies).

We call ω a holomorphic encoding if there exists a k–definable polynomial map $\Omega : \mathbb{A}^L \to \mathbb{A}^N$ with $\omega = \Omega \mid_{\mathcal{D}}$.

In case that the k–definable encoding $\omega : \mathcal{D} \to \mathcal{O}$ is holomorphic, we observe that ω can be extended uniquely to a morphism of algebraic varieties mapping $\overline{\mathcal{D}}$ into $\overline{\mathcal{O}}$. We denote this morphism also by ω.

3.2 Robust encodings.

For data structures, object classes and encodings which are defined over $\mathbb{Q}$ and interpreted over $\mathbb{C}$, it may happen that an unbounded sequence of codes produces a convergent sequence of objects. This is for example a typical behaviour of circuit encodings of polynomials (see Sections 4 and 5.3).

A *continuous* encoding which does not admit this phenomenon is called *robust.* Unfortunately, this notion of robustness is only well defined in case $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$. In order to obtain a more operative notion of robustness which is also applicable to ground fields of arbitrary characteristic, we are going to analyze this notion of robustness under the restriction that the given encoding is not only continuous, but also *holomorphic.* This will lead us to a new definition of robustness which is equivalent to the previous one in case $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ and in case that the given encoding is holomorphic.

Let $\mathcal{D} \subset \mathbb{A}^L(\mathbb{C})$ and $\mathcal{O} \subset \mathbb{A}^N(\mathbb{C})$ be $\mathbb{Q}$–constructible sets and let $\omega : \overline{\mathcal{D}} \rightarrow \overline{\mathcal{O}}$ be a $\mathbb{Q}$–definable map with $\omega(\mathcal{D}) = \mathcal{O}$. Suppose that ω is continuous with respect to the strong topologies of $\overline{\mathcal{D}}$ and $\overline{\mathcal{O}}$. Let us consider $\mathcal{D}$ as a data structure, $\mathcal{O}$ as an object class and $\omega|_{\mathcal{D}} : \mathcal{D} \rightarrow \mathcal{O}$ as a $\mathbb{Q}$–definable *continuous* encoding of the object class $\mathcal{O}$ by the data structure $\mathcal{D}$. In order to simplify notations we denote the map $\omega|_{\mathcal{D}}$ just by $\omega : \mathcal{D} \rightarrow \mathcal{O}$.

Definition 2 *(Robustness for continuous encodings)*
Let notations and assumptions be as before. We call the continuous encoding $\omega : \mathcal{D} \rightarrow \mathcal{O}$ robust if ω satisfies the following condition:

let $(D_i)_{i\in\mathbb{N}}$ be an arbitrary sequence of elements of $\mathcal{D}$ encoding a sequence $(O_i)_{i\in\mathbb{N}}$ of objects of $\mathcal{O}$. Let $O \in \mathcal{O}$ be an accumulation point of $(O_i)_{i\in\mathbb{N}}$ (with respect to the strong topology of $\mathbb{A}^N(\mathbb{C})$). Then there exists in $\overline{\mathcal{D}}$ an accumulation point Q of the sequence $(D_i)_{i\in\mathbb{N}}$ with $\omega(Q) = O$.

Remark 2 *Let notations and assumptions be as before. Suppose furthermore that the data structure $\mathcal{D}$ is a closed subvariety of its affine ambient space. Then the robustness of the encoding $\omega : \mathcal{D} \rightarrow \mathcal{O}$ is equivalent to the condition that ω is a surjective and $\mathbb{Q}$–definable proper continuous map of topological spaces. If ω is robust, then ω has finite, non-empty fibers. Moreover, if $\mathcal{O}$ is a closed subvariety of its affine ambient space, then ω–preimages of compact subsets of $\mathcal{O}$ are compact.*

PROOF.– One sees easily that properness of the $\mathbb{Q}$–definable, continuous map ω implies its robustness.

Suppose now that ω is robust. Since $\mathcal{D}$ is closed, we conclude that ω is a closed, continuous map with (sequentially) compact fibers. Hence ω is proper.

From the arguments used at the beginning of the proof of Lemma 2 below, one deduces easily that ω has finite fibers.

Suppose furthermore that $\mathcal{O}$ is a closed subvariety of its affine ambient space. Then $\mathcal{D}$ and $\mathcal{O}$ are locally compact topological spaces. Therefore, since ω is a proper continuous map, we conclude that ω–preimages of compact subsets of $\mathcal{O}$ are compact. ■

We are now going to discuss the notion of robustness in terms of algebraic geometry in order to obtain a suitable and well motivated definition of robustness for k–definable *holomorphic* encodings over any ground field k. For the rest of this subsection we assume that ω is a holomorphic encoding.

We are going to use the following fact:

Lemma 1 *Let S be a locally closed subvariety of $\mathbb{A}^n(\mathbb{C})$. Suppose $dim\, S > 0$. Then S is unbounded in $\mathbb{A}^n(\mathbb{C})$.*

Proof.– Let $r := dim\, S$. From Noether's Normalization Lemma we deduce that there exists a linear map $\varphi : \mathbb{A}^n(\mathbb{C}) \to \mathbb{A}^r(\mathbb{C})$ with $\varphi(\overline{S}) = \mathbb{A}^r(\mathbb{C})$ (see [Mum88, I.7]). Observe that the $\mathbb{C}$–Zariski closure $\overline{S}$ of S coincides with the closure of S in the strong topology of $\mathbb{A}^n(\mathbb{C})$ (see [Mum88, I.10, Corollary 1]). Suppose that S is bounded. Then $\overline{S}$ is compact in the strong topology and therefore also its image $\varphi(\overline{S})$. However $\varphi(\overline{S}) = \mathbb{A}^r(\mathbb{C})$ is not compact since r is positive. ■

The following key result will lead us to the intended notion of robustness for holomorphic encodings defined over ground fields of arbitrary characteristic:

Lemma 2 *Let notations and assumptions be as before and suppose that $\omega : \mathcal{D} \to \mathcal{O}$ is a holomorphic encoding. Suppose that ω is robust in the sense of Definition 2. Let V be a closed irreducible ($\mathbb{C}$–definable) subvariety of $\mathbb{A}^L(\mathbb{C})$ and suppose that there exists a nonempty Zariski open subset $\mathcal{U}$ of V such that $\mathcal{U}$ is contained in $\mathcal{D}$. Let $W := \overline{\omega(\mathcal{U})}$ and let O be a point of $\omega(\mathcal{U})$. Let $\mathfrak{m}$ be the maximal ideal of $\mathbb{C}[W]$ which defines the point O. Then $\mathbb{C}[V]_{\mathfrak{m}}$ is a finite $\mathbb{C}[W]_{\mathfrak{m}}$–module (i.e. the $\mathbb{C}$–algebra extension $\mathbb{C}[W]_{\mathfrak{m}} \to \mathbb{C}[V]_{\mathfrak{m}}$ induced by ω is integral).*

Proof.– Since $\mathcal{U}$ Zariski dense in V and $\mathcal{U}$ is contained in $\mathcal{D}$, we conclude that V is contained in $\overline{\mathcal{D}}$.

By assumption $\omega : \mathcal{D} \to \mathcal{O}$ is a $\mathbb{Q}$–definable morphism of algebraic varieties. Therefore there exists a (unique) extension of $\omega|_{\mathcal{U}} : \mathcal{U} \to \mathcal{O}$ to a morphism of algebraic varieties which maps V into W. We denote this morphism by $\omega : V \to W$ and observe that it is a dominant morphism of irreducible affine varieties. Thus $\omega : V \to W$ induces an injective $\mathbb{C}$–algebra homomorphism $\mathbb{C}[W] \to \mathbb{C}[V]$ and consequently a field extension $\mathbb{C}(W) \to \mathbb{C}(V)$. Observe that $\omega^{-1}(O) \cap \mathcal{U}$ is a locally closed algebraic subvariety of $\mathbb{A}^L(\mathbb{C})$. From $O \in \omega(\mathcal{U})$ we deduce that $\omega^{-1}(O) \cap \mathcal{U}$ is not empty. Therefore $r := dim\, \omega^{-1}(O) \cap \mathcal{U}$ is nonnegative. Suppose $r > 0$. Then from Lemma 1 we deduce that $\omega^{-1}(O) \cap \mathcal{U}$ is unbounded. Thus there exists a sequence $(D_i)_{i\in\mathbb{N}}$ of points of $\omega^{-1}(\mathcal{O})\cap\mathcal{U}\subset\overline{\mathcal{D}}$ which has no accumulation point. On the other hand we have $O=\omega(D_i)$ for any $i\in\mathbb{N}$. Therefore $\big(\omega(D_i)\big)_{i\in\mathbb{N}}$ is a sequence of elements of the object class $\mathcal{O}$ which converges to the point O. Since ω is by assumption a robust encoding in the sense of Definition 2, we conclude that $(D_i)_{i\in\mathbb{N}}$ must contain an accumulation point in $\overline{\mathcal{D}}$. This contradicts the choice of the sequence $(D_i)_{i\in\mathbb{N}}$. Thus we conclude $r=0$.

From the Theorem of Fibers we deduce now that $dim\, W = dim\, V$ holds and that $\mathbb{C}(W)\hookrightarrow\mathbb{C}(V)$ is a finite field extension. Following [Lan58, Chapter V] (see also [Sha84, Chapter II, 5.2]) we may choose a finite morphism of irreducible affine varieties $\psi:\widetilde{W}\to W$ such that the coordinate ring $\mathbb{C}[\widetilde{W}]$ is isomorphic to the integral closure of $\mathbb{C}[W]$ in $\mathbb{C}[V]$. Observe that there exists a unique morphism of affine varieties $\widetilde{\omega}:V\to\widetilde{W}$ such that the diagram

$$\begin{tikzcd} & \widetilde{W} \arrow[dd, "\psi"] \\ V \arrow[ur, "\widetilde{\omega}"] \arrow[dr, "\omega"'] & \\ & W \end{tikzcd}$$

commutes. Since ω is dominant we conclude that $\widetilde{\omega}$ is dominant too. Thus $\widetilde{\omega}$ induces an injective $\mathbb{C}$–algebra homomorphism $\mathbb{C}[\widetilde{W}]\to\mathbb{C}[V]$ which maps $\mathbb{C}[\widetilde{W}]$ onto a subring of $\mathbb{C}[V]$ which is integrally closed in $\mathbb{C}[V]$. In this sense we shall say that $\mathbb{C}[\widetilde{W}]$ *is integrally closed in* $\mathbb{C}[V]$.

Let now $P\in\widetilde{W}$ be an arbitrary point with $\psi(P)=O$ (observe that such a point exists since ψ is surjective). Since $\widetilde{\omega}$ is dominant, we conclude that $\widetilde{\omega}(\mathcal{U})$ contains a nonempty Zariski open subset of $\widetilde{W}$. Hence $\widetilde{\omega}(\mathcal{U})$ is dense in the strong topology of $\widetilde{W}$. Therefore we may choose a sequence $(D_i)_{i\in\mathbb{N}}$ of elements of $\mathcal{U}\subset\mathcal{D}$ such that $\big(\widetilde{\omega}(D_i)\big)_{i\in\mathbb{N}}$ converges in the strong topology of $\widetilde{W}$ to the point P. Thus the sequence $\big(\omega(D_i)\big)_{i\in\mathbb{N}}$ is a sequence of elements of the object class $\mathcal{O}$ which converges to the object $O\in\mathcal{O}$. Since by assumption the encoding $\omega:\mathcal{D}\to\mathcal{O}$ is robust in the sense of Definition 2, we conclude that there exists an accumulation point $D\in\overline{\mathcal{D}}$ of the sequence $(D_i)_{i\in\mathbb{N}}$. Without loss of generality we may assume that $(D_i)_{i\in\mathbb{N}}$ converges to D. This implies $D\in V$ and $\widetilde{\omega}(D)=P$.

Thus the fiber $\widetilde{\omega}^{-1}(P)$ has nonnegative dimension. Suppose now that the dimension of $\widetilde{\omega}^{-1}(P)$ is positive. Then Lemma 1 implies that $\widetilde{\omega}^{-1}(P)$ is unbounded. Therefore we may choose a sequence $(Q_n)_{n\in\mathbb{N}}$ of points of $\widetilde{\omega}^{-1}(P)$ which has no accumulation point. Since $\mathcal{U}$ is dense in the strong topology of V there exists a family $(D_i^{(n)})_{n,i\in\mathbb{N}}$ of elements of $\mathcal{U}$ such that for any $n\in\mathbb{N}$ the sequence $(D_i^{(n)})_{i\in\mathbb{N}}$ converges to the point Q_n. Without loss of generality we may suppose that this convergence is uniform in the parameter

n. Observe that we have $\omega(Q_n) = \psi(P) = O$ for any index $n \in \mathbb{N}$. Therefore we may assume without loss of generality that the sequence $(\omega(D_n^{(n)}))_{n\in\mathbb{N}}$ converges to the object O. From the robustness of ω we infer now that the sequence $(D_n^{(n)})_{n\in\mathbb{N}}$ has an accumulation point Q in $\overline{\mathcal{D}}$. Since for any index $n \in \mathbb{N}$ the convergence of the sequence $(D_i^{(n)})_{i\in\mathbb{N}}$ to Q_n is uniform in n, we conclude that Q is an accumulation point of the sequence $(Q_n)_{n\in\mathbb{N}}$. This contradicts the choice of the sequence $(Q_n)_{n\in\mathbb{N}}$.

Therefore we have $dim\, \widetilde{\omega}^{-1}(P) = 0$. Let $\mathfrak{m}_P$ be the maximal ideal of $\mathbb{C}[\widetilde{W}]$ which defines the point P and consider $\mathbb{C}[V]$ as a $\mathbb{C}[\widetilde{W}]$–module. Since $\mathbb{C}[\widetilde{W}]$ is integrally closed in $\mathbb{C}[V]$, we deduce now from Zariski's Main Theorem (see e.g. [Ive73, IV.2]) that

$$\mathbb{C}[V]_{\mathfrak{m}_P} = \mathbb{C}[\widetilde{W}]_{\mathfrak{m}_P} \tag{3}$$

holds. Consider $\mathbb{C}[V]_{\mathfrak{m}}$ as a $\mathbb{C}[\widetilde{W}]_{\mathfrak{m}}$–module and observe that the maximal ideals of $\mathbb{C}[\widetilde{W}]_{\mathfrak{m}}$ correspond bijectively to the maximal ideals of $\mathbb{C}[\widetilde{W}]$ of the form $\mathfrak{m}_P$ with $P \in \widetilde{W}$ and $\psi(P) = O$. From (3) one deduces now $\mathbb{C}[V]_{\mathfrak{m}} = \mathbb{C}[\widetilde{W}]_{\mathfrak{m}}$. Since by definition of $\widetilde{W}$ the coordinate ring $\mathbb{C}[\widetilde{W}]$ is a finite $\mathbb{C}[W]$–module, this implies that $\mathbb{C}[V]_{\mathfrak{m}}$ is a finite $\mathbb{C}[W]_{\mathfrak{m}}$–module. ■

Let notations and assumptions be as before. From Lemma 2 and its proof we infer that the encoding ω satisfies the following conditions:

(i) for any object $O \in \mathcal{O}$ there are only finitely many encodings $D \in \mathcal{D}$ with $\omega(D) = O$ (in this sense we shall call the *ambiguity* of ω *finite*).

(ii) for any object $O \in \mathcal{O}$ with maximal defining ideal $\mathfrak{m}$ in $\mathbb{C}[\overline{\mathcal{O}}]$, the local ring $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{m}}$ is a *finite* $\mathbb{C}[\overline{\mathcal{O}}]_{\mathfrak{m}}$–module.

If the algebraic variety $\overline{\mathcal{D}}$ is irreducible then $\overline{\mathcal{O}}$ is irreducible too and we may replace condition (ii) by the following equivalent one:

(iii) Let O be an arbitrary object of $\mathcal{O}$. Then any place $\varphi : \mathbb{C}(\overline{\mathcal{D}}) \to \mathbb{C} \cup \{\infty\}$ whose valuation ring which contains the local ring of the variety $\overline{\mathcal{O}}$ at the point O, takes only finite values on $\mathbb{C}[\overline{\mathcal{D}}]$.

Although somewhat weaker and limited to the case $\overline{\mathcal{D}}$ irreducible, condition (iii) is the genuine algebraic–geometric counterpart of the notion of robustness given by Definition 2. This indicates that the following definition of robustness for *holomorphic* encodings (not simply continuous ones) captures the intuitive meaning of the previous Definition 2 in case of a ground field k of arbitrary characteristic with arbitrary algebraic closure $\overline{k}$.

Definition 3 *(Robustness of holomorphic encodings)*

Let $\omega : \mathcal{D} \to \mathcal{O}$ be a k–definable holomorphic encoding of a k–constructible object class $\mathcal{O}$ by a k–constructible data structure $\mathcal{D}$. Then we call ω robust if for any object $O \in \mathcal{O}$ with maximal defining ideal $\mathfrak{m}$ in $\overline{k}[\overline{\mathcal{O}}]$ the localization ring $\overline{k}[\overline{\mathcal{D}}]_{\mathfrak{m}}$ is a finite $\overline{k}[\overline{\mathcal{O}}]_{\mathfrak{m}}$–module.

In case that a k–definable holomorphic encoding $\omega : \mathcal{D} \to \mathcal{O}$ induces a finite morphism of affine varieties which maps $\overline{\mathcal{D}}$ onto $\overline{\mathcal{O}}$, we conclude that the encoding ω is robust in the sense of Definition 3.

We are now going to show that in case $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ and ω holomorphic, Definition 2 and Definition 3 represent the same notion of robustness.

Lemma 3 *Let $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$, and let $\mathcal{D}$ and $\mathcal{O}$ be a $\mathbb{Q}$–constructible data structure and object class respectively. Let $\omega : \mathcal{D} \to \mathcal{O}$ a $\mathbb{Q}$–definable, holomorphic encoding. Then ω is robust in the sense of Definition 2 (as a continuous encoding with respect to the strong topologies of $\mathcal{D}$ and $\mathcal{O}$) if and only if ω is robust in the sense of Definition 3 (as a holomorphic encoding).*

Proof.– Suppose that ω is robust in the sense of Definition 2. Then, from the statement (ii) above, we deduce that ω is a robust encoding in the sense of Definition 3.

Suppose now that ω is robust in the sense of Definition 3. Let be given a sequence $(D_i)_{i \in \mathbb{N}}$ of elements of the data structure $\mathcal{D}$ which encodes a sequence $(O_i)_{i \in \mathbb{N}}$ of objects of $\mathcal{O}$. Let be given an accumulation point $O \in \mathcal{O}$ of the sequence $(O_i)_{i \in \mathbb{N}}$ with respect to the strong topology $\mathcal{O}$. For the sake of simplicity we shall assume that $(O_i)_{i \in \mathbb{N}}$ converges to O. Let $\mathfrak{m}$ be the maximal defining ideal of O in $\mathbb{C}[\overline{\mathcal{O}}]$.

Let us consider an arbitrary element f of $\mathbb{C}[\overline{\mathcal{O}}]$. In case that $f(O_i) = 0$ holds for infinitely many indices $i \in \mathbb{N}$, we conclude $f(O) = 0$. Therefore, if f does not belong to the maximal ideal $\mathfrak{m}$, then f vanishes on all but finitely many entries of the sequence $(O_i)_{i \in \mathbb{N}}$. Since ω is robust in the sense of Definition 3, we may now conclude that there exists an element g of $\mathbb{C}[\overline{\mathcal{O}}]$ with the following properties:

(a) $g(O) \neq 0$ and $g(O_i) \neq 0$ for all but finitely many indices $i \in \mathbb{N}$.

(b) $\mathbb{C}[\overline{\mathcal{D}}]_g$ is a finite $\mathbb{C}[\overline{\mathcal{O}}]_g$–module.

For the sake of simplicity we shall suppose $g(O_i) \neq 0$ for any $i \in \mathbb{N}$.

Consider now an arbitrary element h of $\mathbb{C}[\overline{\mathcal{D}}]$. Let Y be an indeterminate.

From properties (a) and (b) above we deduce that there exists a monic polynomial $P \in \mathbb{C}[\overline{\mathcal{O}}]_g[Y]$ with $P(h) = 0$ and such that P can be specialized for the object O and any index $i \in \mathbb{N}$ into well–defined elements $P(O)$ and $P(O_i)$ of the polynomial ring $\mathbb{C}[Y]$. Without loss of generality we may suppose that P is the minimal polynomial of h over $\mathbb{C}(\overline{\mathcal{O}})$. Thus for any

$i \in \mathbb{N}$ we have $P(O_i)(h(D_i)) = 0$. Therefore the sequence $(h(D_i))_{i\in\mathbb{N}}$ has an accumulation point which is a zero of the polynomial $P(O)(Y) \in \mathbb{C}[Y]$. Since P is the minimal polynomial of h over $\mathbb{C}(\overline{\mathcal{O}})$ we deduce from property (b) above that there exists an element $Q \in \overline{\mathcal{D}}$ with $g(Q) \neq 0$ and $\omega(Q) = O$ such that $h(Q)$ is an accumulation point of the sequence $(h(D_i))_{i\in\mathbb{N}}$.

Generalizing this argument to a finite set of generators of the $\mathbb{C}[\overline{\mathcal{O}}]_g$–module $\mathbb{C}[\overline{\mathcal{D}}]_g$ we conclude that the sequence $(D_i)_{i\in\mathbb{N}}$ has an accumulation point in $\overline{\mathcal{D}}$. Therefore the encoding ω is robust in the sense of Definition 2. ■

Remark 3 *Let $k := \mathbb{Q}$ and $\overline{k} = \mathbb{C}$. Then, in terms of algebraic geometry, Lemma 2 and Remark 2 imply the following folkloric statement:*

let V and W be closed, equidimensional subvarieties of suitable complex affine spaces and let $\varphi : V \to W$ be a morphism of affine varieties mapping V onto W. Suppose that φ is a proper continuous map with respect to the strong topologies of V and W. Then φ is a finite morphism of affine varieties.

3.3 Correct test and identification sequences.

3.3.1 Correct test and identification sequences for holomorphic encodings.

We are now going to develop the fundamental technical tools we shall need in Section 3.4 for the formulation and proof of the first main result of this paper, namely Theorem 1.

The following statement generalizes [HS82, Theorem 4.4].

Lemma 4 *Let $\mathcal{O}$ be a k–constructible object class of polynomial functions belonging to $\overline{k}[Y_1, \ldots, Y_t]$. Let $\Delta \in \mathbb{N}$ be an upper bound for the degree of the polynomials contained in $\mathcal{O}$. Suppose that there is given a k–constructible data structure $\mathcal{D} \subset \mathbb{A}^L$ and a k–definable holomorphic encoding $\omega : \mathcal{D} \to \mathcal{O}$. Suppose that there exists a quantifier–free first–order formula which defines the data structure $\mathcal{D}$ and whose equations involve only K distinct polynomials of degree at most Δ_1 in L indeterminates over k. Moreover, assume that the encoding ω is definable by polynomials of degree at most $\Delta_2 \geq 1$ in L indeterminates over k. Then the degrees of the algebraic varieties $\overline{\mathcal{D}}$ and $\overline{\mathcal{O}}$ satisfy the estimates*

$$\deg \overline{\mathcal{D}} \leq (1 + K\Delta_1)^L$$

and

$$\deg \overline{\mathcal{O}} \leq (L+1)\Delta_2^L \deg \overline{\mathcal{D}} \leq (L+1)\big((1 + K\Delta_1)\Delta_2\big)^L.$$

For $\overline{\mathcal{O}}$ equidimensional this estimate may be improved to

$$\deg \overline{\mathcal{O}} \leq \Delta_2^L \deg \overline{\mathcal{D}} \leq \big((1 + K\Delta_1)\Delta_2\big)^L.$$

Let M be a finite subset of k having at least two elements. Suppose $\# M \geq \Delta^2 (\deg \overline{\mathcal{O}})^{\frac{1}{L}}$ (observe that this is the case if

$$\# M \geq \Delta^2 (1+L)^{\frac{1}{L}} (1+K\Delta_1)\Delta_2$$

holds). Let $m \geq 2L+2$. Then there exist points $\gamma_1, \ldots, \gamma_m$ of M^t such that $\gamma := (\gamma_1, \ldots, \gamma_m)$ is a correct test sequence for the object class $\overline{\mathcal{O}}$ (and hence for $\mathcal{O}$).

Suppose that the points of the finite set M^t are equidistributed. Then the probability of finding in M^{mt} by a random choice such a correct test sequence is at least $1 - \frac{1}{\# M} \geq \frac{1}{2}$.

Proof.– The proof is subdivided in three parts. Let us start with the first one. With the terminology introduced before, suppose that the object class $\mathcal{O}$ is given as a k–constructible subset of some affine space $\mathbb{A}^N$. Let $Z_1, \ldots, Z_L$ be the coordinate functions of the affine space $\mathbb{A}^L$. By hypothesis there exists a quantifier–free definition of $\mathcal{D}$ whose equations involve only K distinct polynomials $G_1, \ldots, G_K \in k[Z_1, \ldots, Z_L]$ of degree at most Δ_1. Observe that for any irreducible component $\mathcal{C}$ of $\overline{\mathcal{D}}$ there exists a subset $\mathcal{G}$ of $\{G_1, \ldots, G_K\}$ such that $\mathcal{C}$ is an irreducible component of the closed subvariety $\{G = 0; G \in \mathcal{G}\}$ of $\mathbb{A}^L$. From [JS00, Theorem 2] (see also [Hei83, Corollary 1]) one deduces now easily the estimate

$$\deg \overline{\mathcal{D}} \leq \sum_{h=0}^{L} \binom{K}{h} \Delta_1^h \leq (1+K\Delta_1)^L.$$

By assumption there exist polynomials $\Omega_1, \ldots, \Omega_N \in k[Z_1, \ldots, Z_L]$ of degree at most Δ_2 such that $\Omega := (\Omega_1, \ldots, \Omega_N)$ defines a polynomial map $\Omega : \mathbb{A}^L \to \mathbb{A}^N$ with $\Omega|_{\mathcal{D}} = \omega$. Observe that Ω induces a morphism of (possibly reducible) affine varieties $\overline{\mathcal{D}} \to \overline{\mathcal{O}}$ which we denote also by ω. From $\omega(\mathcal{D}) = \mathcal{O}$ we deduce that ω is dominant. This implies $dim\, \overline{\mathcal{O}} \leq dim\, \overline{\mathcal{D}} \leq L$.

Let $0 \leq h \leq L$ and let E_h be the union of the irreducible components of $\overline{\mathcal{O}}$ of dimension h. Suppose that E_h is nonempty. Let $T_1, \ldots, T_N$ be the coordinate functions of $\mathbb{A}^N$. Since the morphism ω is dominant, we may choose a nonempty, Zariski open subset $\mathcal{U}$ of E_h which is contained in the image $\omega(\overline{\mathcal{D}})$ (see e.g. [Mum88, I.8, Theorem 3]). On the other hand, we may choose $N-h$ generic affine–linear equations $H_1, \ldots, H_{n-h} \in k[T_1, \ldots, T_N]$ such that $E_h \cap \{H_1 = 0, \ldots, H_{N-h} = 0\}$ consists of $\deg E_h$ points, all contained in $\mathcal{U}$ and therefore in $\omega(\overline{\mathcal{D}})$ (see [Hei83], Remark 2). Each of these points is the image of a $\overline{k}$–irreducible component of the closed subvariety

$$\omega^{-1}(E_h) = \overline{\mathcal{D}} \cap \{H_1(\Omega) = 0, \ldots, H_{N-h}(\Omega) = 0\}$$

of $\mathbb{A}^L$. From the Bézout Inequality (in the variant of [HS82, Proposition 2.3]) we conclude now

$$\deg E_h \leq \deg \omega^{-1}(E_h) \leq \deg \overline{\mathcal{D}} \cdot \Delta_2^{dim\, \overline{\mathcal{D}}} \leq \deg \overline{\mathcal{D}} \cdot \Delta_2^L.$$

Thus, if $\overline{\mathcal{O}}$ is equidimensional of dimension h, we have $\overline{\mathcal{O}} = E_h$ and therefore

$$\deg \overline{\mathcal{O}} \leq \deg \overline{\mathcal{D}} \cdot \Delta_2^L \leq \big((1 + K\Delta_1)\Delta_2\big)^L.$$

In the general case we obtain the following estimate:

$$\deg \overline{\mathcal{O}} = \sum_{h=0}^{L} \deg E_h \leq (L+1)\Delta_2^L \deg \overline{\mathcal{D}} \leq (L+1)\big((1 + K\Delta_1)\Delta_2\big)^L.$$

This proves the first statement of the Lemma.

In the second part of the proof we consider the closed subvariety

$$V = \{(F, y^{(1)}, \ldots, y^{(m)}); F \in \overline{\mathcal{O}}, y^{(1)}, \ldots, y^{(m)} \in \mathbb{A}^t, \\ F(y^{(1)}) = \cdots = F(y^{(m)}) = 0\}$$

of the affine space $\mathbb{A}^N \times \mathbb{A}^{mt}$ and the morphisms of algebraic varieties $\pi_1 : V \to \mathbb{A}^N$ and $\pi_2 : V \to \mathbb{A}^{mt}$ induced by the canonical projections of $\mathbb{A}^N \times \mathbb{A}^{mt}$ onto $\mathbb{A}^N$ and A^{mt}.

Since any polynomial of $\overline{\mathcal{O}}$ has degree at most Δ, we deduce from the Bézout Inequality the estimate

$$\deg V \leq \deg \overline{\mathcal{O}} \cdot \Delta^m. \tag{4}$$

Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the irreducible components of V whose π_1–image contains at least one nonzero polynomial of $\overline{\mathcal{O}}$. Let $V^* := \bigcup_{1 \leq j \leq s} \mathcal{C}_j$. Thus $\pi_2(V^*) = \bigcup_{1 \leq j \leq s} \pi_2(\mathcal{C}_j)$ is the set of all "incorrect" test sequences of length m for the object class $\overline{\mathcal{O}}$. From (4) we deduce the estimate

$$\deg V^* \leq \deg \overline{\mathcal{O}} \cdot \Delta^m. \tag{5}$$

Let $1 \leq j \leq s$. There exists a polynomial $F \in \overline{\mathcal{O}}$ with $F \neq 0$ and $F \in \pi_1(\mathcal{C}_j)$. Observe that the fiber $\pi_1^{-1}(F)$ is isomorphic to the equidimensional algebraic variety

$$\{(y^{(1)}, \ldots, y^{(m)}) \in \mathbb{A}^{mt}; y^{(1)}, \ldots, y^{(m)} \in \mathbb{A}^t, F(y^{(1)}) = \cdots = F(y^{(m)}) = 0\}.$$

Thus $F \neq 0$ implies $dim\, \pi_1^{-1}(F) = m(t-1)$. Applying the Theorem of Fibers (see e.g. [Mum88, I.8, Corollary]) to the morphism of irreducible affine varieties

$$\pi_1|_{\mathcal{C}_j} : \mathcal{C}_j \to \overline{\pi_1(\mathcal{C}_j)}$$

we deduce

$$dim\, \mathcal{C}_j - dim\, \overline{\pi_1(\mathcal{C}_j)} \leq m(t-1).$$

Since $\overline{\pi_1(\mathcal{C}_j)}$ is contained in the affine variety $\overline{\mathcal{O}}$ we conclude $dim\, \overline{\pi_1(\mathcal{C}_j)} \leq dim\, \overline{\mathcal{O}}$ and therefore $dim\, \mathcal{C}_j - dim\, \overline{\mathcal{O}} \leq m(t-1)$. This implies

$$dim\, \mathcal{C}_j \leq m(t-1) + dim\, \overline{\mathcal{O}}. \tag{6}$$

By assumption the data structure $\mathcal{D}$ encodes the object class $\mathcal{O}$ holomorphically by means of the encoding ω. This means that the encoding determines a morphism of affine varieties $\overline{\mathcal{D}} \to \overline{\mathcal{O}}$ which contains $\mathcal{O}$ in its image. Therefore this morphism is dominant and this implies $dim\, \overline{\mathcal{O}} \leq dim\, \overline{\mathcal{D}}$. From (6) we conclude now

$$dim\, \mathcal{C}_j \leq m(t-1) + dim\, \overline{\mathcal{D}}.$$

Since $1 \leq j \leq s$ was arbitrary, we obtain the estimate

$$dim\, V^* \leq m(t-1) + dim\, \overline{\mathcal{D}}. \tag{7}$$

This implies $dim\, \overline{\pi_2(V^*)} \leq m(t-1) + dim\, \overline{\mathcal{D}} \leq m(t-1) + L$.

Before continuing with the proof, observe that by assumption $m \geq 2L + 2 > L$ and therefore $mt > m(t-1) + L$ holds. Hence $\overline{\pi_2(V^*)}$ is a proper closed subset of $\mathbb{A}^{mt}$. Thus any element $\gamma := (\gamma_1, \ldots, \gamma_m)$ of the Zariski open, dense subset $\mathcal{U} := \mathbb{A}^{mt} \setminus \overline{\pi_2(V^*)}$ of $\mathbb{A}^{mt}$ with $\gamma_1, \ldots, \gamma_m \in \mathbb{A}^t$ is a correct test sequence for the object class $\overline{\mathcal{O}}$.

Let us finally pass to the third and final part of the proof. For $1 \leq k \leq m$ and $1 \leq \ell \leq t$ let Y_{ke} be a new indeterminate and let $H_{ke} := \prod_{\mu \in M}(Y_{k\ell} - \mu)$. Thus $H_{k\ell}$ is a univariate polynomial of degree $\#M$ belonging to the polynomial ring $k[Y_{k\ell}]$. We consider the indeterminates $Y_{k\ell}$ with $1 \leq k \leq m$, $1 \leq \ell \leq t$ as coordinate functions of the affine space $\mathbb{A}^{mt}$. Observe that $M^{mt} = \{H_{k\ell} = 0; 1 \leq k \leq m, 1 \leq \ell \leq t\}$ holds and that the set of "incorrect" test sequences contained in M^{mt}, namely $\pi_2(V^*) \cap M^{mt} = \pi_2\left(V^* \cap \{H_{k\ell} = 0; 1 \leq k \leq m, 1 \leq \ell \leq t\}\right)$, is a finite k–definable (and hence Zariski closed) subset of $\mathbb{A}^{mt}$.

From [HS82, Proposition 2.3] (i.e. from the Bézout Inequality) and from (5), (7) we conclude now

$$\begin{aligned}
\#\left(\pi_2(V^*) \cap M^{mt}\right) &= \#\pi_2\left(V^* \cap \{H_{k\ell} = 0; 1 \leq k \leq m, 1 \leq \ell \leq t\}\right) \\
&\leq \deg(V^* \cap \{H_{k\ell} = 0; 1 \leq k \leq m, 1 \leq \ell \leq t\}) \\
&\leq \deg(V^*)\, (\#M)^{dim\, V^*} \\
&\leq \deg(\overline{\mathcal{O}})\, \Delta^m\, (\#M)^{m(t-1) + dim\, \overline{\mathcal{D}}} \\
&\leq \deg(\overline{\mathcal{O}})\, \Delta^m\, (\#M)^{m(t-1)+L}.
\end{aligned}$$

Suppose now that the points of the finite set M^t are equidistributed. By assumption we have $m \geq 2L + 2$, $\#M \geq \Delta^2 (\deg \overline{\mathcal{O}})^{\frac{1}{L}}$ and $\Delta \geq 1$. From the estimate $\#\left(\pi_2(V^*) \cap M^{mt}\right) \leq \deg(\overline{\mathcal{O}})\, \Delta^m\, (\#M)^{m(t-1)+L}$ we deduce that the probability of finding in M^{mt} by a random choice an "incorrect" test sequence for the object class $\overline{\mathcal{O}}$ is at most

$$\begin{aligned}\frac{\deg(\overline{\mathcal{O}})\,\Delta^m}{(\#M)^{m-L}} &\leq \frac{\deg(\overline{\mathcal{O}})\,\Delta^m}{\#M\,\left(\Delta^2(\deg\mathcal{O})^{\frac{1}{L}}\right)^{m-L-1}}\\ &= \frac{\deg(\overline{\mathcal{O}})\,\Delta^{2(L+1)}}{\#M\,\Delta^m\,(\deg\mathcal{O})^{\frac{1}{L}(m-L-1)}}\\ &\leq \frac{\deg(\overline{\mathcal{O}})}{\#M\,\left(\deg(\overline{\mathcal{O}})\right)^{1+\frac{1}{L}}} \leq \frac{1}{\#M} \leq \frac{1}{2}\end{aligned}$$

(recall that by assumption M has at least two elements). Hence the probability of finding in M^{mt} by a random choice a correct test sequence for the object class $\overline{\mathcal{O}}$ is at least

$$1 - \frac{1}{\#M} \geq \frac{1}{2}.$$

Since this probability is positive, we conclude that M^{mt} really contains a correct test sequence $\gamma = (\gamma_1, \ldots, \gamma_m)$ with $\gamma_1, \ldots, \gamma_m \in \mathbb{A}^t$ for the object class $\overline{\mathcal{O}}$. ■

Corollary 1 *Let notations and assumptions be as in Lemma 4. Let M be a finite subset of k of cardinality at least $max\{\Delta^2(\deg\overline{\mathcal{O}})^{\frac{1}{L}}, 2\}$ and let $m \geq 4L+2$. Then there exist points $\gamma_1, \ldots, \gamma_m$ of M^t such that $\gamma := (\gamma_1, \ldots, \gamma_m)$ is an identification sequence for the object class $\overline{\mathcal{O}}$ (and hence for $\mathcal{O}$). Suppose that the points of the finite set M^t are equidistributed. Then the probability of finding in M^{mt} by a random choice such an identification sequence is at least $1 - \frac{1}{\#M} \geq \frac{1}{2}$.*

Proof.– We use the same notations and assumptions as in the proof of Lemma 4. Let $\omega : \mathcal{D} \to \mathcal{O}$ be the given k–definable holomorphic encoding of the object class $\mathcal{O}$. Let $\mathcal{D}_* := \mathcal{D} \times \mathcal{D}$, $\mathcal{O}_* := \{F_1 - F_2; F_1, F_2 \in \mathcal{O}\}$ and let $\omega_* : \mathcal{D}_* \to \mathcal{O}_*$ be the encoding of the object class $\mathcal{O}_*$ defined by $\omega_*(D_1, D_2) = \omega(D_1) - \omega(D_2)$ for $(D_1, D_2) \in \mathcal{D}_*$.

One verifies immediately that the data structure $\mathcal{D}_*$ and the object class $\mathcal{O}_*$ are k–constructible subsets of $\mathbb{A}^{2L}$ and $\mathbb{A}^N$ respectively and that ω_* is a k–definable holomorphic encoding of the object class $\mathcal{O}_*$. In particular $\mathcal{O}_*$ turns out to be a k–constructible object class in the sense introduced before. Furthermore Δ is an upper bound for the degree of the t–variate polynomials over $\overline{k}$ contained in the object class $\mathcal{O}_*$. From [Hei83], Proposition 2 and Lemma 2 we deduce the estimate $\deg\overline{\mathcal{O}}_* \leq (\deg\overline{\mathcal{O}})^2$. Hence $\#M \geq \Delta^2(\deg\overline{\mathcal{O}})^{\frac{1}{L}}$ implies $\#M \geq \Delta^2(\deg\overline{\mathcal{O}}_*)^{\frac{1}{2L}}$.

Suppose now that the points of the finite set M^t are equidistributed. From Lemma 4 we deduce that the probability of finding in M^{mt} by a random choice a correct test sequence for the object class $\overline{\mathcal{O}}_*$ is at least $1 - \frac{1}{\#M} \geq \frac{1}{2}$.

Let $\gamma = (\gamma_1, \ldots, \gamma_m) \in M^{mt}$ with $\gamma_1, \ldots, \gamma_m \in M^t$ such a correct test sequence and let F_1, F_2 be given elements of $\overline{\mathcal{O}}$ (thus F_1 and F_2 are t–variate polynomials over $\overline{k}$). Suppose that $F_1(\gamma_1) = F_2(\gamma_1), \ldots, F_1(\gamma_m) = F_2(\gamma_m)$ holds. Hence, for $F := F_1 - F_2$, we have $F(\gamma_1) = \cdots = F(\gamma_m) = 0$. Since F belongs to the object class $\overline{\mathcal{O}}_*$ and γ is a correct test sequence for $\overline{\mathcal{O}}_*$ we infer $F = 0$. This implies $F_1 = F_2$.

In conclusion, we see that γ is an identification sequence for the object class $\overline{\mathcal{O}}$. Since the probability of finding such identification sequences in M^{mt} is positive, we infer that M^{mt} contains at least one of them. ■

Let $\mathcal{O}$ be k–definable object class of polynomial functions and $\omega : \mathcal{D} \to \mathcal{O}$ be a k–definable holomorphic encoding of $\mathcal{O}$ by a k–constructible data structure of size L. By means of the data structure $\mathcal{D}$ we are able to answer the value question about the object class $\mathcal{O}$ holomorphically. In this sense, an identification sequence γ of length m allows to answer the *identity question* about the object class $\mathcal{O}$ *holomorphically.* From Corollary 1 we conclude that there exist always *short* identification sequences (of length m linear in L) and that they are easy to find by means of a suitable random choice. This means that the identity question about the object class $\mathcal{O}$ can always be answered "efficiently".

3.3.2 Correct test and identification sequences for circuit encodings.

In order to exemplify the ideas behind Lemma 4 and Corollary 1 of Section 3.3.1 we are now going to apply the concept of identification sequence to circuit encoded object classes of polynomial functions.

Let ε be a new indeterminate and let us consider ε as a parameter and $Y_1, \ldots, Y_t$ as variables. Let $F \in \overline{k}[Y_1, \ldots, Y_t]$. We denote by $L(F)$ the minimal nonscalar size over $\overline{k}$ of all totally division–free arithmetic circuits with inputs $Y_1, \ldots, Y_t$ and scalars in $\overline{k}$ which evaluate the polynomial F. Moreover we denote by $\overline{L}(F)$ the minimal nonscalar size over $\overline{k}(\varepsilon)$ of all essentially division–free arithmetic circuits which evaluate a rational function of the form $F + \varepsilon Q$ with Q belonging to $\overline{k}[\varepsilon, Y_1, \ldots, Y_t]_\varepsilon$. Obviously we have $\overline{L}(F) \leq L(F)$. We call $L(F)$ the *nonscalar (sequential time) complexity of F over $\overline{k}$* and $\overline{L}(F)$ the corresponding *approximative* complexity. Let $L \in \mathbb{N}$ and let $W_{L,t} := \{F \in \overline{k}[Y_1, \ldots, Y_t]; L(F) \leq L\}$. From [BCS97, Chapter 9, Exercise 9.18] (see also [HS82, Theorem 3.2]) we deduce that all polynomials contained in $W_{L,t}$ have degree bounded by 2^L and that $W_{L,t}$ forms a k–constructible object class which has a k–definable holomorphic encoding by the data structure $\mathbb{A}^{(L+t+1)^2}$. Moreover any polynomial $F \in \overline{k}[Y_1, \dots, Y_t]$ with $\overline{L}(F) \leq L$ has degree at most 2^L.

Let $N \in \mathbb{N}$ with $N \geq 2^L$. Then $W_{L,t}$ can be considered as a k–constructible subset of $\mathbb{A}^N$. From [Ald84], Lemma 2 and Satz 4 one deduces easily the following statement:

$$\overline{W}_{L,t} := \{F \in \overline{k}[Y_1, \dots, Y_t]; \overline{L}(F) \leq L\}.$$

In this sense the Zariski closure of the object class $W_{L,t}$ has a natural interpretation as the set of polynomials of $\overline{k}[Y_1, \dots, Y_t]$ which have approximative nonscalar (sequential time) complexity over $\overline{k}$ at most L.

Finally observe that $W_{L,t}$ and $\overline{W}_{L,t}$ are cones and contain the zero polynomial. In particular any identification sequence of $W_{L,t}$ or $\overline{W}_{L,t}$ is a correct test sequence.

Corollary 2 (compare [HS82, Theorem 4.4] and [GH01, Lemma 3]) *Let notations be as before and let L, m, t be natural numbers with $m \geq 4(L+t+1)^2 + 2$. Let M be a finite subset of k of cardinality at least $2^{4(L+1)}$. Then there exist points $\gamma_1, \dots, \gamma_m$ of M^t such that $\gamma := (\gamma_1, \dots, \gamma_m)$ is an identification sequence for the object class $\overline{W}_{L,t}$ of all polynomials $F \in \overline{k}[Y_1, \dots, Y_t]$ which have approximative nonscalar (sequential time) complexity over $\overline{k}$ at most L.*

Suppose that the points of the finite set M^t are equidistributed. Then the probability of finding in M^{mt} by a random choice such an identification sequence is at least $1 - \frac{1}{\#M} \geq \frac{1}{2}$.

Proof.– Let $N \geq 2^L$, $r := (L+t+1)^2$ and let $Z_1, \dots, Z_r$ be new indeterminates. From [BCS97, Chapter 9, Exercise 9.18] (compare also [Sch78, Theorem 2.1]) we deduce that there exist N polynomials of $k[Z_1, \dots, Z_r]$ having degree at most $L\,2^{L+1} + 2$ which induce a k–definable holomorphic encoding $\omega : \mathbb{A}^r \to W_{L,t}$ of the object class $W_{L,t}$ which we consider as a k–constructible subset of $\mathbb{A}^N$.

Taking into account that $\overline{W}_{L,t} = \overline{\omega(\mathbb{A}^r)}$ is irreducible, we deduce from Lemma 4 the estimate $\deg \overline{W}_{L,t} \leq (L\,2^{L+1} + 2)^r$. This implies

$$(\deg \overline{W}_{L,t})^{\frac{1}{r}} \leq L\,2^{L+1} + 2. \tag{8}$$

Observe that by hypothesis $m \geq 4(L+t+1)^2 + 2 = 4r + 2$ holds and that any polynomial contained in $W_{L,t}$ has degree at most $\Delta := 2^L$. From the assumption $\#M \geq 2^{4(L+1)}$ and (8) we deduce $\#M \geq \Delta^2 (\deg \overline{W}_{L,t})^{\frac{1}{r}}$. The statement to prove follows now immediately from Corollary 1. ■

3.4 Encodings of polynomial functions by values.

In this subsection we are going to prove the first main result of this paper.

Let $\mathcal{O}$ be a k–constructible object class of polynomial functions, $\mathcal{D}$ a k–constructible data structure and $\omega : \mathcal{D} \to \mathcal{O}$ a k–definable holomorphic encoding. Our first main result (Theorem 1 below) may be stated succinctly as follows:

assume that $\mathcal{O}$ is a class of polynomial functions and that its encoding by $\mathcal{D}$ is holomorphic. Suppose furthermore that the ambient space of $\mathcal{O}$ is affine and contains $\mathcal{O}$ as a cone (i.e. we assume that $\mathcal{O}$ is closed under multiplication by scalars). Then there exists a k–definable data structure $\overline{\mathcal{D}}$ which encodes the closure class $\overline{\mathcal{O}}$ of $\mathcal{O}$ *continuously* (with respect to the Zariski topologies of $\overline{\mathcal{D}}$ and $\overline{\mathcal{O}}$) and *unambiguously.* In particular, $\overline{\mathcal{O}}$ and $\overline{\mathcal{D}}$ are homeomorphic topological spaces. Moreover the size of $\overline{\mathcal{D}}$ (i.e. the dimension of its ambient space) is *linear* in the size of $\mathcal{D}$.

In other words, we may always replace *efficiently* the given data structure $\mathcal{D}$ by an unambiguous one, say $\overline{\mathcal{D}}$, if we are only interested in a *topological* characterization of the object class $\overline{\mathcal{O}}$ (or $\mathcal{O}$). By means of $\overline{\mathcal{D}}$ we are able to answer efficiently the *identity* question about $\overline{\mathcal{O}}$, but *not necessarily* the *value* question. The assumption that the object class forms a cone in case that $\mathcal{O}$ has affine ambient space is not restrictive in the context of this paper, since $\mathcal{O}$ will be typically a class of functions closed under multiplication by scalars. On the other hand, this assumption guarantees that the encoding of the object class $\overline{\mathcal{O}}$ by the data structure $\overline{\mathcal{D}}$ is not only continuous, but also a closed map with respect to the Zariski topologies of $\overline{\mathcal{D}}$ and $\overline{\mathcal{O}}$.

In the Appendix of this paper (Section A.1) we shall formulate a slight generalization of Theorem 1 below.

First we synthesize the essence of the technical Lemma 4 and its Corollary 1 of Section 3.3.1 in terms of continuous encodings.

Let $\mathcal{O} \subset \overline{k}[Y_1, \ldots , Y_t]$ be a k–constructible object class of polynomial functions and let $\gamma = (\gamma_1, \ldots , \gamma_m) \in k^{mt}$ with $\gamma_1, \ldots , \gamma_m \in k^t$ and $m \geq 1$ be an identification sequence for $\overline{\mathcal{O}}$ (from Corollary 1 one deduces easily that for $m \in \mathbb{N}$ sufficiently large such an identification sequence always exists).

Suppose now that $\mathcal{O}$ is a *cone* in $\overline{k}[Y_1, \ldots , Y_t]$. Then $\overline{\mathcal{O}}$ is a cone too. Let $\sigma : \overline{\mathcal{O}} \to \mathbb{A}^m$ be the map defined by $\sigma(F) := \big(F(\gamma_1), \ldots , F(\gamma_m)\big)$ for $F \in \overline{\mathcal{O}}$. Observe that σ is the restriction of a k–definable linear map $\mathbb{A}^N \to \mathbb{A}^m$, where $\mathbb{A}^N$ with $N \geq 1$ is a suitable affine ambient space which contains $\mathcal{O}$ and $\overline{\mathcal{O}}$ as cones. Thus σ is homogeneous of degree one and represents an *injective*, k–definable morphism of affine varieties. Therefore $\sigma(\overline{\mathcal{O}})$ is a k–definable subset of $\mathbb{A}^m$. Since σ is homogeneous of degree one and $\overline{\mathcal{O}}$ is a cone, the image $\sigma(\overline{\mathcal{O}})$ is a cone too. Hence the Zariski closure $\mathcal{D}^*$ of $\sigma(\overline{\mathcal{O}})$ in $\mathbb{A}^m$ is a k–definable cone of $\mathbb{A}^m$ and σ induces a dominant morphism of affine varieties which maps $\overline{\mathcal{O}}$ into $\mathcal{D}^*$ and is again homogeneous of degree one. We denote this morphism by $\sigma : \overline{\mathcal{O}} \to \mathcal{D}^*$.

Lemma 5 *Let notations and assumptions be as before. Then* $\sigma : \overline{\mathcal{O}} \to \mathcal{D}^*$ *is a finite, bijective, k–definable morphism of affine varieties. Let $\mathcal{C}$ be an arbitrary k–definable irreducible component of $\overline{\mathcal{O}}$. Then $\sigma|_{\mathcal{C}}$ is a birational, k–definable (finite and bijective) morphism of $\mathcal{C}$ onto the Zariski closed set $\sigma(\mathcal{C})$.*

Proof.– Let $Z_1, \ldots , Z_N$ be the coordinate functions of $\mathbb{A}^N$. There exist linear polynomials $S_1, \ldots , S_m \in k[Z_1, \ldots , Z_N]$ such that σ is the restriction of the linear map $(S_1, \ldots , S_m)$ to the closed subvariety $\overline{\mathcal{O}}$ of $\mathbb{A}^N$. Since $\overline{\mathcal{O}}$ and $\mathcal{D}^*$ are k–definable Zariski closed cones of the affine spaces $\mathbb{A}^N$ and $\mathbb{A}^m$ respectively, they are definable by homogeneous polynomials over k. Moreover $\overline{\mathcal{O}}$ and $\mathcal{D}^*$ contain the origins of the affine spaces $\mathbb{A}^N$ and $\mathbb{A}^m$ respectively. From the injectivity of $\sigma : \overline{\mathcal{O}} \to \mathcal{D}^*$ we deduce therefore that $\overline{\mathcal{O}} \cap \{S_1 = 0, \ldots , S_m = 0\}$ contains only the origin of $\mathbb{A}^N$. This implies that the homogeneous map σ induces a finite morphism between the closed projective subvarieties of $\mathbb{P}^{N-1}$ and $\mathbb{P}^{m-1}$ associated to the cones $\overline{\mathcal{O}}$ and $\mathcal{D}^*$ respectively. In fact, the standard proof of this classical result implies something more, namely that also the morphism $\sigma : \overline{\mathcal{O}} \to \mathcal{D}^*$ is finite (see [Sha84], I.5.3, Theorem 8 and proof of Theorem 7). In particular, σ is a surjective closed map. Since σ is also injective we conclude that σ is bijective.

Let $\mathcal{C}$ be an arbitrary k–definable irreducible component of $\overline{\mathcal{O}}$. Since σ is a closed map we conclude that $\sigma(\mathcal{C})$ is a closed irreducible subvariety of $\mathcal{D}^*$. Since σ is injective we infer that $\sigma|_{\mathcal{C}} : \mathcal{C} \to \sigma(\mathcal{C})$ is a bijective, k–definable morphism of affine varieties. Since for any point $y \in \sigma(\mathcal{C})$ we have $\#\big(\sigma^{-1}(y) \cap \mathcal{C}\big) = 1$ we deduce from [Mum88, Proposition 3.17] that $k\big(\sigma(\mathcal{C})\big) = k(\mathcal{C})$ holds. Hence $\sigma|_{\mathcal{C}}$ is a birational morphism. ∎

From Lemma 5 we deduce that with respect to the Zariski topologies of $\overline{\mathcal{O}}$ and $\mathcal{D}^*$, the morphism $\sigma : \overline{\mathcal{O}} \to \mathcal{D}^*$ is a homeomorphism and that $\mathcal{D}^* = \sigma(\overline{\mathcal{O}})$ holds. Consider now $\mathcal{D}^* \subset \mathbb{A}^m$ as a data structure. Then $\omega^* := \sigma^{-1} : \mathcal{D}^* \to \overline{\mathcal{O}}$ is an *unambiguous* encoding of the object class $\overline{\mathcal{O}}$ which is *continuous* with respect to the Zariski topologies of $\mathcal{D}^*$ and $\overline{\mathcal{O}}$. Suppose that ω^* allows to answer the value question about the object class $\overline{\mathcal{O}}$ holomorphically. Then from Remark 1 we deduce that $\omega^* : \mathcal{D}^* \to \overline{\mathcal{O}}$ is a k–definable morphism of algebraic varieties and therefore ω^* is an unambiguous, k–definable and *(bi–)holomorphic* encoding of the object class $\overline{\mathcal{O}}$ by the data structure $\mathcal{D}^*$. We shall see later that in general this will not be the case (see Corollary 5 and Theorem 2). Suppose for the moment $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$. Since σ, the inverse map of the unambiguous encoding ω^*, is a morphism of algebraic varieties, we conclude that σ is continuous with respect to the strong topologies of $\overline{\mathcal{O}}$ and $\mathcal{D}^*$. If ω^* is continuous with respect to the strong topology, this implies that ω^* is a *robust* encoding in the sense of Definition 2.

However, ω^* may be not continuous with respect to the strong topologies of $\overline{\mathcal{O}}$ and $\mathcal{D}^*$. On the other hand, ω^* induces a map Ω between the projective subvarieties of $\mathbb{P}^{m-1}(\mathbb{C})$ and $\mathbb{P}^{N-1}(\mathbb{C})$ associated to the cones $\mathcal{D}^*$ and $\overline{\mathcal{O}}$. The map Ω encodes the projective variety associated to the cone $\overline{\mathcal{O}}$ by the projective variety associated to the cone $\mathcal{D}^*$ and is continuous with respect to the corresponding strong topologies.

We may summarize the main results of this section by the following statement:

Theorem 1 *Let $\mathcal{O}$ be a k–constructible object class of polynomial functions belonging to $\overline{k}[Y_1, \ldots, Y_t]$. Let Δ be an upper bound for the degree of the polynomials contained in $\mathcal{O}$. Suppose that $\mathcal{O}$ is a cone in $\overline{k}[Y_1, \ldots, Y_t]$. Assume that there is given a k–constructible data structure $\mathcal{D} \subset \mathbb{A}^L$ and a k–definable holomorphic encoding $\mathcal{D} \to \mathcal{O}$. Let $m \geq 4L + 2$ and let M be a finite subset of k of cardinality at least $max\{\Delta^2(\deg \overline{\mathcal{O}})^{\frac{1}{L}}, 2\}$. Then there exist a k–definable, Zariski closed cone $\mathcal{D}^*$ of $\mathbb{A}^m$ and a continuous encoding $\omega^* : \mathcal{D}^* \to \overline{\mathcal{O}}$ of the object class $\overline{\mathcal{O}}$ by the data structure $\mathcal{D}^*$ which satisfies the following conditions:*

(i) ω^* is a homeomorphism between the data structure $\mathcal{D}^*$ and the object class $\overline{\mathcal{O}}$,

(ii) there exist a point $\gamma := (\gamma_1, \ldots, \gamma_m) \in M^{mt}$ with $\gamma_1, \ldots, \gamma_m \in M^t$ such that for any $F \in \overline{\mathcal{O}}$ the identity $(\omega^*)^{-1}(F) = \big(F(\gamma_1), \ldots, F(\gamma_m)\big)$ holds,

(iii) $(\omega^*)^{-1} : \overline{\mathcal{O}} \to \mathcal{D}^*$ is a k–definable, bijective and finite morphism of affine varieties. The morphism $(\omega^*)^{-1}$ is homogeneous of degree one,

(iv) for any k–definable irreducible component $\mathcal{C}$ of $\overline{\mathcal{O}}$ the restriction map $(\omega^*)^{-1}|_{\mathcal{C}} : \mathcal{C} \to (\omega^*)^{-1}(\mathcal{C})$ is a birational k–definable (finite and surjective) morphism of $\mathcal{C}$ onto the irreducible Zariski closed set $(\omega^*)^{-1}(\mathcal{C})$.

In particular ω^* is an unambiguous continuous encoding of the object class $\overline{\mathcal{O}}$ by the data structure $\mathcal{D}^*$. The encoding ω^* is holomorphic if and only if ω^* allows to answer holomorphically the value question about the object class $\overline{\mathcal{O}}$.

In case $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ and ω^* continuous with respect to the strong topology, the encoding ω^* is robust (in the sense of Definition 2).

Suppose that the elements of the finite set M^t are equidistributed. Then the probability of finding by a random choice a point $\gamma := (\gamma_1, \ldots, \gamma_m) \in M^{mt}$ with $\gamma_1, \ldots, \gamma_m \in M^t$ such that the map $\sigma_\gamma : \overline{\mathcal{O}} \to \mathbb{A}^m$ defined by $\sigma_\gamma(F) := \big(F(\gamma_1), \ldots, F(\gamma_m)\big)$ for $F \in \mathcal{O}$ induces a k–definable, bijective morphism of $\overline{\mathcal{O}}$ onto a Zariski closed cone $\mathcal{D}^*_\gamma$ of $\mathbb{A}^m$ is at least $1 - \frac{1}{\#M} \geq$

$\frac{1}{2}$. *Any such morphism* $\sigma_\gamma : \overline{\mathcal{O}} \to \mathcal{D}^*_\gamma$ *defines by* $\omega^*_\gamma := \sigma_\gamma^{-1}$ *a continuous unambiguous encoding of the object class* $\overline{\mathcal{O}}$ *by the data structure* $\mathcal{D}^*_\gamma$*. This encoding satisfies conditions* (*i*)*–*(*iv*)*.*

The proof of Theorem 1 is an immediate consequence of Corollary 1, Lemma 5 and the subsequent considerations.

The following statement represents a version of Theorem 1 for object classes of arithmetic–circuit–represented polynomials.

Corollary 3 [GH01, Lemma 4] *Let notions and notations be as in Corollary 2. Let* L, m, t *be natural numbers with* $m \geq 4(L+t+1)^2+2$*. Let* M *be a finite subset of cardinality at least* $2^{4(L+1)}$*. Let* $\overline{W}_{L,t}$ *be the object class of all polynomials* $F \in \overline{k}[Y_1, \dots, Y_t]$ *which have approximative non-scalar (sequential) complexity over* $\overline{k}$ *at most* L*. Then* $\overline{W}_{L,t}$ *is a cone and there exists a* k*–definable, Zariski closed cone* $\mathcal{D}^*_{L,t}$ *of* $\mathbb{A}^m$ *and a continuous encoding* $\omega^* : \mathcal{D}^*_{L,t} \to \overline{W}_{L,t}$ *of the object class* $\overline{W}_{L,t}$ *by the data structure* $\mathcal{D}^*_{L,t}$ *which satisfies the conditions (i)–(iv) of Theorem 1. The encoding* ω^* *is holomorphic if and only if* ω^* *allows to answer holomorphically the value question about the object class* $\overline{W}_{L,t}$*.*

In case $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ *and* ω^* *continuous with respect to the strong topology, the encoding* ω^* *is robust (in the sense of Definition 2).*

Suppose that the elements of the finite set M^t *are equidistributed. Then we may find by a random choice with probability of success at least* $1 - \frac{1}{\#M}$ *a point* $\gamma = (\gamma_1, \dots, \gamma_m) \in M^{mt}$ *with* $\gamma_1, \dots, \gamma_m \in M^t$ *such that the map* $\sigma_\gamma : \overline{W}_{L,t} \to \mathbb{A}^m$ *defined by* $\sigma_\gamma(F) := \big(F(\gamma_1), \dots, F(\gamma_m)\big)$ *for* $F \in \overline{W}_{L,t}$ *produces as in Theorem 1 a* k*–definable, Zariski closed cone* $\mathcal{D}^*_{L,t,\gamma}$ *of* $\mathbb{A}^m$ *and a continuous encoding* $\omega^*_\gamma : \mathcal{D}^*_{L,t,\gamma} \to \overline{W}_{L,t}$*.*

Proof.– Since in the nonscalar complexity model $\overline{k}$–linear operations are free, we conclude that $W_{L,t} = \{F \in \overline{k}[Y_1, \dots, Y_t]; L(F) \leq L\}$ is a cone of $\overline{k}[Y_1, \dots, Y_t]$. Therefore its closure $\overline{W}_{L,t}$ is a cone too. The statement of Corollary 3 follows now immediately from Corollary 2 and Lemma 5. ■

We call a continuous encoding of an object class of polynomial functions as in Theorem 1 and Corollary 3 of this section and Corollary 9 of Section A.1 an *encoding by an identification sequence* or simply an *encoding by values*. An encoding by an identification sequence allows us to answer the identity question about the object class $\mathcal{O}$. However, the corresponding value question requires a holomorphic encoding. In the next section we shall exhibit an example of a $\mathbb{Q}$–constructible object class $\mathcal{O}$ of univariate polynomials which has a $\mathbb{Q}$–definable, holomorphic, *robust* but *ambiguous* encoding by a data structure of small size. However we shall show that any *holomorphic* encoding of $\mathcal{O}$ by an identification sequence requires a data structure of (exponentially) big size.

A given object class of polynomial functions has many, mostly artificial encodings. However, encodings by values seem particularly natural. This becomes evident in the situation of Corollary 3. Encodings of object classes of polynomial functions by arithmetic circuits are typically ambiguous. In Corollary 3 a given encoding of an object class of polynomial functions by arithmetic circuits is replaced by an *unambiguous* continuous and robust encoding by means of an identification sequence (observe that evaluation is particularly well–adapted to circuit encoding).

3.5 Unirational encodings.

Let $\mathcal{O}$ be a k–constructible object class and let $\mathcal{D}$ be a k–constructible data structure of size L, contained in the ambient space $\mathbb{A}^L$ or $\mathbb{P}^L$. Let $\omega : \mathcal{D} \to \mathcal{O}$ be a k–definable holomorphic encoding of the object class $\mathcal{O}$ by the data structure $\mathcal{D}$. We call ω *unirational* if $\mathcal{D}$ contains a nonempty, Zariski open set of its ambient space. Suppose that ω is unirational. Then $\overline{\mathcal{D}}$ equals its ambient space $\mathbb{A}^L$ or $\mathbb{P}^L$ and $\overline{\mathcal{O}}$ is an irreducible k–Zariski closed set in some suitable affine or projective space. We call the encoding ω *rational* if it defines a birational map between the ambient space and $\overline{\mathcal{O}}$.

Let L and t be natural numbers. Then the generic computation scheme of length L in the nonscalar sequential complexity model (see [BCS97], Chapter 9, Theorem 9.9 and Exercise 9.18, or [Hei89]) defines a unirational encoding of the object classes $W_{L,t}$ and $\overline{W}_{L,t}$ of polynomial functions of $\overline{k}[Y_1, \dots, Y_t]$ having exact or approximative (sequential) nonscalar complexity over $\overline{k}$ at most L. Analogously, the standard representation of polynomials of $\overline{k}[Y_1, \dots, Y_t]$ of degree at most d by their coefficients is a rational encoding of size $\binom{d+t}{t}$. Similarly the L–sparse polynomials of $\overline{k}[Y_1, \dots, Y_t]$ containing only a previously fixed set of L monomials are rationally encoded by the data structure $\mathbb{A}^L$.

One may ask why we do not limit our attention exclusively to unirational encodings of object classes. A technical reason for this is that such encodings represent only a limited range of object classes. In order to exemplify this, let us observe that a limitation to unirational data structures would automatically exclude from our considerations important object classes as e.g. the set of all k–definable equidimensional projective varieties of dimension r and degree d contained in a projective space $\mathbb{P}^n$ with $n \geq r$. The traditional data structures for these object classes are the Chow varieties which encode (unambiguously) a given object by its Chow coordinates.

Similarly the Hilbert varieties are data structures which encode unambiguously the (reduced) projective subvarieties of a given projective space with previously fixed Hilbert polynomial. The natural topology of Chow and Hilbert varieties induces a topology on the object classes they represent and hence a notion of limit object. Typical Chow varieties, encoding complete intersection varieties, are unirational and it is not clear whether they could be also rational. In general, Hilbert varieties cannot be expected to be unirational.

4 Two paradigmatic object classes.

In this section we are going to exhibit two paradigmatic object classes of polynomial functions and to discuss different holomorphic encodings of them. We shall always assume $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$.

4.1 First paradigm.

Let d be a natural number, let U and Y be indeterminates over $\mathbb{Q}$ and let $F_d := \sum_{j=0}^{d}(U^d - 1)U^jY^j \in \mathbb{Q}[U, Y]$. We are going to interpret U as parameter and Y as variable. Let us consider the object class of univariate polynomials $\mathcal{O}_d := \{F_d(u, Y); u \in \mathbb{A}^1\}$ and the encoding $\omega_d : \mathbb{A}^1 \to \mathcal{O}_d$ defined for $u \in \mathbb{C}$ by $\omega_d(u) := F_d(u, Y)$. Representing the polynomials belonging to $\mathcal{O}_d$ by their coefficients, we identify the object class $\mathcal{O}_d$ with the corresponding subset of $\mathbb{A}^{d+1}$. With this interpretation ω_d becomes a polynomial map which is defined for $u \in \mathbb{A}^1$ by

$$\omega_d(u) := \big(u^d - 1, (u^d - 1)u, \ldots, (u^d - 1)u^d\big).$$

Therefore ω_d is a finite morphism of algebraic varieties which maps the affine space $\mathbb{A}^1$ onto its image, namely $\mathcal{O}_d$. Hence $\mathcal{O}_d$ is a closed, rational (and hence irreducible), $\mathbb{Q}$–definable curve contained in the affine ambient space $\mathbb{A}^{d+1}$. The coordinate ring of the curve $\mathcal{O}_d$ is canonically isomorphic to the $\mathbb{Q}$–algebra $\mathbb{Q}[U^d - 1, (U^d - 1)U, \ldots, (U^d - 1)U^d]$. Therefore, the encoding $\omega_d : \mathbb{A}^1 \to \mathcal{O}_d$ of the object class $\mathcal{O}_d$ is $\mathbb{Q}$–definable, holomorphic and *robust*.

Let $M := \{e^{\frac{2\pi i}{d}k}; 0 \leq k < d\}$ and denote by $0 := (0, \ldots, 0)$ the origin of the affine space $\mathbb{A}^{d+1}$. Observe that the point $0 \in \mathbb{A}^{d+1}$ belongs to the curve $\mathcal{O}_d$, because ω_d maps any point of M onto the origin of $\mathbb{A}^{d+1}$. Thus ω_d represents an *ambiguous* robust encoding of the object class $\mathcal{O}_d$. One verifies easily that the point 0 is the only (ordinary) singularity of the rational curve $\mathcal{O}_d$ and that this singularity can be resolved by a single blowing up. Moreover ω_d induces an isomorphism between the affine curves $\mathbb{A}^1 \setminus M$ and $\mathcal{O}_d \setminus \{0\}$.

Suppose now that there is given a $\mathbb{Q}$–definable data structure $\mathcal{D}_d$ and a $\mathbb{Q}$–definable holomorphic encoding $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$. Let us denote the size of $\mathcal{D}_d$ by m_d. Suppose furthermore that there is given a $\mathbb{Q}$–definable polynomial map $\theta_d : \mathbb{A}^1 \to \mathbb{A}^{m_d}$ with $\theta_d(\mathbb{A}^1) \subset \mathcal{D}_d$ and $\sigma_d \circ \theta_d = \omega_d$. We interpret the polynomial map θ_d as a branching–free algorithm which transforms the encoding ω_d into the unambiguous encoding σ_d (see Section 4.3 for a motivation of this notion of algorithm).

Although the object class $\mathcal{O}_d$ admits an (ambiguous) robust encoding by a data structure of size one, namely ω_d, any *unambiguous* holomorphic encoding σ_d of $\mathcal{O}_d$, obtained by an algorithmic transformation of ω_d, requires a data structure of large size (of approximately the dimension of the ambient space of the object class $\mathcal{O}_d$). This is the content of the following result:

Proposition 1 *Let notations and assumptions be as before. Suppose that $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ is an unambiguous holomorphic encoding of the object class $\mathcal{O}_d$. Then the size m_d of the data structure $\mathcal{D}_d$ satisfies the estimate*

$$m_d \geq d.$$

Proof.– Let $0 \leq k_1 < k_2 < d$. Since $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ is injective we deduce from $\omega_d(e^{\frac{2\pi i}{d}k_1}) = \omega_d(e^{\frac{2\pi i}{d}k_2}) = 0$ and from $\sigma_d \circ \theta_d = \omega_d$ that $\theta_d(e^{\frac{2\pi i}{d}k_1}) = \theta_d(e^{\frac{2\pi i}{d}k_2})$ holds. Therefore there exists a code $\alpha \in \mathcal{D}_d$ satisfying the condition $\alpha = \theta_d(e^{\frac{2\pi i}{d}k})$ for any $0 \leq k < d$. The encoding $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ is induced by a polynomial map $\mathbb{A}^{m_d} \to \mathbb{A}^{d+1}$ which we also denote by σ_d.

Let $0 \leq k < d$. Denote by $(D\sigma_d)_\alpha$ the derivative of this polynomial map in the point $\alpha \in \mathbb{A}^{m_d}$ and by $\theta'_d(e^{\frac{2\pi i}{d}k}) \in \mathbb{A}^{m_d}$ and $\omega'_d(e^{\frac{2\pi i}{d}k}) \in \mathbb{A}^{d+1}$ the derivatives of the polynomial maps θ_d and ω_d in the point $e^{\frac{2\pi i}{d}k} \in \mathbb{A}^1$. Observe that the encoding ω_d is represented by the $(d+1)$–tuple of univariate polynomials $\big(U^d - 1, (U^d-1)U, \ldots, (U^d-1)U^d\big)$. Deriving this representation with respect to the parameter U and evaluating the result in the point $e^{\frac{2\pi i}{d}k} \in \mathbb{A}^1$, we conclude that

$$(de^{\frac{2\pi i}{d}kj}; -1 \leq j < d) = \omega'_d(e^{\frac{2\pi i}{d}k}) = (D\sigma_d)_\alpha\big(\theta'_d(e^{\frac{2\pi i}{d}k})\big)$$

holds.

One sees easily that the matrix $A := \big(d(e^{\frac{2\pi i}{d}kj})\big)_{0\leq k<d, -1\leq j<d}$ has maximal rank d. Indeed, the $d \times d$ submatrix of the matrix A consisting of the last d columns of the matrix A is nonsingular, because it is the product of a $d \times d$ nonsingular diagonal matrix by a $d \times d$ nonsingular Vandermonde matrix. Therefore the d tangent vectors $\omega'_d(e^{\frac{2\pi i}{d}k})$, $0 \leq k < d$, of the curve $\mathcal{O}_d$ at the point 0 are $\mathbb{C}$–linearly independent. Since $(D\sigma_d)_\alpha : \mathbb{A}^{m_d} \to \mathbb{A}^{d+1}$ is a $\mathbb{C}$–linear map, we conclude that the d points $\theta'_d(e^{\frac{2\pi i}{d}k})$, $0 \leq k < d$ of the $\mathbb{C}$–linear space $\mathbb{A}^{m_d}$ are linearly independent too. This implies $m_d \geq d$. ∎

We observe that the proof of Proposition 1 implies that the local embedding dimension of the curve $\mathcal{O}_d$ at the point 0 (and hence the global embedding dimension of $\mathcal{O}_d$) is at least d. We are now going to apply the conclusion of Proposition 1 to the arithmetic circuit complexity model.

Let $\mathcal{A} := \mathbb{Q}[U]$ and $\mathcal{B}_d := \mathbb{Q}[U^d - 1, (U^d-1)U, \ldots, (U^d-1)U^d]$. Assume $d \geq 3$. Observe that $F_d = \sum_{0\leq j\leq d}(U^d-1)U^jY^j$ belongs to the polynomial rings $\mathcal{A}[Y]$ and $\mathcal{B}_d[Y]$ and that $\mathcal{B}_d$ is isomorphic to the coordinate ring of the curve $\mathcal{O}_d$.

For $R \in \{\mathcal{A}, \mathcal{B}_d\}$ denote by $L_R(F_d)$ the minimal non–scalar size of the totally division–free arithmetic circuits with single input Y which evaluate the polynomial F_d using only scalars from R. In case $d = 2^{r+1} - 1$ for some $r \in \mathbb{N}$, one infers from the representation

$$F_d = (U^d - 1) \prod_{0 \le k \le r} \left(1 + (UY)^{2^k}\right)$$

the estimate

$$L_{\mathcal{A}}(F_d) = r + 1 = \log(d+1)$$

(here by log we denote the logarithm to the base 2).

In a similar way one sees easily that $L_{\mathcal{A}}(F_d) = O(\log d)$ holds for arbitrary $d \in \mathbb{N}$. From the trivial lower bound $L_{\mathcal{A}}(F_d) \ge \log d$ (see [BCS97, Chapter 8, 8.1]) one deduces finally that the functions $L_{\mathcal{A}}(F_d)$ and $\log d$ have the same asymptotic growth (in symbols: $L_{\mathcal{A}}(F_d) = \Theta(\log d)$).

Let us now analyze $L_{\mathcal{B}_d}(F_d)$. Since F_d is a polynomial of degree d in the variable Y we deduce from [BCS97, Chapter 9, Proposition 9.1] the estimate $L_{\mathcal{B}_d}(F_d) \le 2\sqrt{d}$. Let $L_d := L_{\mathcal{B}_d}(F_d)$. Then there exists a totally division–free circuit β_d of non–scalar size L_d with single input Y which evaluates the polynomial F_d using only scalars from $\mathcal{B}_d$. From [BCS97, Chapter 9, Theorem 9.9] we deduce that without loss of generality the circuit β_d may be supposed to use only $m_d := L_d^2 + 2L_d + 2$ scalars $\theta_1^{(d)}, \dots, \theta_{m_d}^{(d)}$ from $\mathcal{B}_d := \mathbb{Q}[U^d - 1, (U^d - 1)U, \dots, (U^d - 1)U^d]$. Let $\theta_d : \mathbb{A}^1 \to \mathbb{A}^{m_d}$ be the polynomial map defined by $\theta_d := (\theta_1^{(d)}, \dots, \theta_{m_d}^{(d)})$ and let $\mathcal{D}_d$ be the image of θ_d. Observe that $\mathcal{D}_d$ is a $\mathbb{Q}$–constructible subset of $\mathbb{A}^{m_d}$. Again from [BCS97, Chapter 9, Theorem 9.9] we infer that there exists a polynomial map $\sigma_d : \mathbb{A}^{m_d} \to \mathbb{A}^{d+1}$ which satisfies the condition

$$\sigma_d(\theta_1^{(d)}, \dots, \theta_{m_d}^{(d)}) = \left(U^d - 1, (U^d - 1)U, \dots, (U^d - 1)U^d\right).$$

Thus we have $\sigma_d \circ \theta_d = \omega_d$ and $\sigma_d(\mathcal{D}_d) = \mathcal{O}_d$. Let us denote the restriction of the polynomial map $\sigma_d : \mathbb{A}^{m_d} \to \mathbb{A}^{d+1}$ to $\mathcal{D}_d$ by $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$. Since $\theta_1^{(d)}, \dots, \theta_{m_d}^{(d)}$ are polynomials in the coefficients $U^d - 1, (U^d - 1)U, \dots, (U^d - 1)U^d$ of $F_d \in \mathcal{B}_d[Y]$ we conclude that $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ is an unambiguous holomorphic encoding of the object class $\mathcal{O}_d$. From Proposition 1 we deduce now $L_d^2 + 2L_d + 2 = m_d \ge d$. This implies the lower bound $L_{\mathcal{B}_d}(F_d) = L_d \ge \sqrt{d - 2}$. In summary, we obtain the following complexity result:

Corollary 4 *Let notations be as before. Then we have $L_{\mathcal{A}}(F_d) = \Theta(\log d)$ and $L_{\mathcal{B}_d}(F_d) = \Theta(\sqrt{d})$.*

In terms of [Hei89] this result means that the sequence of polynomials $\mathcal{F} := (F_d)_{d \in \mathbb{N}}$ is easy to evaluate in $\mathcal{A}[Y]$, whereas $\mathcal{F}$ becomes difficult to evaluate if we require that for any $d \in \mathbb{N}$ the univariate polynomial $F_d \in \mathcal{B}_d[Y]$ has to be computed by a totally division–free arithmetic circuit whose scalars belong to $\mathcal{B}_d$. In conclusion, the evaluation complexity of a polynomial depends strongly on the ring of scalars admitted.

We are now going to describe another application of Proposition 1. Let m_d be a natural number and let $\gamma_d := (\gamma_1^{(d)}, \ldots, \gamma_{m_d}^{(d)}) \in \mathbb{Q}^{m_d}$ be an identification sequence of length m_d for the Zariski closure C_d of the cone generated by the object class $\mathcal{O}_d$ in the $(d+1)$–dimensional $\mathbb{C}$–linear subspace of polynomials of $\mathbb{C}[X]$ having degree at most d. Observe that C_d is a $\mathbb{Q}$–definable, closed, irreducible subvariety of $\mathbb{A}^{d+1}$. Let $\mathcal{D}_d := \{\big(G(\gamma_1^{(d)}), \ldots, G(\gamma_{m_d}^{(d)})\big); G \in \mathcal{O}_d\}$ and let $\tau_d : \mathcal{O}_d \to \mathcal{D}_d$ be the bijective map defined for $G \in \mathcal{O}_d$ by $\tau_d(G) := \big(G(\gamma_1^{(d)}), \ldots, G(\gamma_{m_d}^{(d)})\big)$. One sees easily that $\tau_d : \mathcal{O}_d \to \mathcal{D}_d$ is induced by a $\mathbb{Q}$–definable linear map from $\mathbb{A}^{d+1}$ to $\mathbb{A}^{m_d}$. On the other hand, this linear map induces an injective, homogeneous morphism from the cone C_d into the affine space $\mathbb{A}^{d+1}$. From Lemma 5 we deduce now that this morphism is closed with respect to the Zariski topologies of C_d and $\mathbb{A}^{d+1}$. Therefore $\mathcal{D}_d = \tau_d(\mathcal{O}_d)$ is a closed, $\mathbb{Q}$–definable, irreducible curve contained in $\mathbb{A}^{m_d}$ and $\tau_d : \mathcal{O}_d \to \mathcal{D}_d$ is a bijective, birational morphism of $\mathbb{Q}$–definable, irreducible curves. Let $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ be the inverse map of τ_d. We consider $\mathcal{D}_d$ as a $\mathbb{Q}$–constructible data structure of size m_d and σ_d as an encoding by values of the object class $\mathcal{O}_d$ in the sense of Section 3.4. In particular σ_d is a $\mathbb{Q}$–definable, continuous encoding. With these notations we are able to state the following result:

Corollary 5 *Suppose that the encoding by values $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ is holomorphic. Then the size m_d of the data structure $\mathcal{D}_d$ satisfies the estimate*

$$m_d \geq d.$$

Proof.– Since σ_d and τ_d are inverse morphisms of $\mathbb{Q}$–definable, irreducible curves, there exists a polynomial map $\theta_d : \mathbb{A}^1 \to \mathbb{A}^{m_d}$ with $\theta_d(u) = \tau_d\big(\omega_d(u)\big)$ for any $u \in \mathbb{A}^1$. This implies $\theta_d(\mathbb{A}^1) \subset \mathcal{D}_d$. Moreover we have $\sigma_d \circ \theta_d = \sigma_d \circ (\tau_d \circ \omega_d) = \omega_d$. Since $\sigma_d : \mathcal{D}_d \to \mathcal{O}_d$ is an unambiguous $\mathbb{Q}$–definable holomorphic encoding of the object class $\mathcal{O}_d$, we deduce from Proposition 1 that $m_d \geq d$ holds. ■

Corollary 5 says that there exists a family of object classes, namely $(\mathcal{O}_d)_{d \in \mathbb{N}}$, encoded by a single data structure of size one, namely $\mathbb{A}^1$, such that any *holomorphic* encoding of these object classes by values becomes necessarily large, namely of size at least d for any object class $\mathcal{O}_d$. Nevertheless in view of Theorem 1, the object class $\mathcal{O}_d$ admits a *continuous* robust encoding of *constant* length (in fact of length 2).

From Corollary 5 we infer the following general result:

Theorem 2 *Let L, m be natural numbers and let $\gamma = (\gamma_1, \ldots, \gamma_m) \in \mathbb{Q}^m$ be an identification sequence for the object class $\overline{W}_{L,1}$ of all univariate polynomials over $\mathbb{C}$ which have approximative non–scalar sequential time complexity at most L. Let $\mathcal{D}^* := \{(F(\gamma_1), \ldots, F(\gamma_m)); F \in \overline{W}_{L,1}\}$ and let $\tau : \overline{W}_{L,1} \to \mathcal{D}^*$ be the bijective map defined by $\tau(F) := (F(\gamma_1), \ldots, F(\gamma_m))$. Then $\mathcal{D}^*$ is a $\mathbb{Q}$–definable closed cone of $\mathbb{A}^m$ and $\tau : \overline{W}_{L,1} \to \mathcal{D}^*$ is a $\mathbb{Q}$–definable, bijective, finite morphism of algebraic varieties. Let $\sigma : \mathcal{D}^* \to \overline{W}_{L,1}$ be the inverse map of τ. Consider $\mathcal{D}^*$ as a $\mathbb{Q}$–definable data structure of size m and suppose that $\sigma : \mathcal{D}^* \to \overline{W}_{L,1}$ is a $\mathbb{Q}$–definable, holomorphic encoding by values of the object class $\overline{W}_{L,1}$. Then the size m of the data structure $\mathcal{D}^*$ satisfies the estimate $m \geq 2^{cL}$ for a suitable universal constant $c > 0$.*

Proof.– There exists a constant $c' > 0$ such that $L(G) \leq c' \log d$ holds for any $d \in \mathbb{N}$ and any univariate polynomial G belonging to the object class $\mathcal{O}_d$ (recall that $L(G)$ denotes the non–scalar time complexity of the polynomial G).

Let $d := \lfloor 2^{\frac{L}{c'}} \rfloor := max\{z \in \mathbb{Z}; z \leq 2^{\frac{L}{c'}}\}$. Then we have $G \in \overline{W}_{L,1}$ for any $G \in \mathcal{O}_d$. Therefore γ is an identification sequence for the object class $\mathcal{O}_d$. From Corollary 5 we deduce now $m \geq d \geq 2^{\frac{L}{c'}} - 1$. Choose now any constant $c > 0$ with $2^{\frac{1}{c'}} - 1 \geq 2^c$. Then we have $m \geq 2^{cL}$. ■

One proves easily a similar complexity result for multivariate polynomials. This question will be reconsidered in a forthcoming paper.

4.2 Second paradigm.

Let n be a fixed natural number and let T, $U_1, \ldots, U_n$ and Y be indeterminates over $\mathbb{Q}$. Let $U := (U_1, \ldots, U_n)$. We are going to consider T, $U_1, \ldots, U_n$ as parameters and Y as variable. In the sequel we shall use the following notation: for arbitrary natural numbers i and j we shall denote by $[j]_i$ the ith digit of the binary representation of j. Let P_n be the following polynomial of $\mathbb{Q}[T, U, Y]$:

$$P_n(T, U, Y) := \prod_{j=0}^{2^n-1} \big(Y - (j + T \prod_{i=1}^{n} U_i^{[j]_i})\big). \tag{9}$$

We observe that the dense representation of P_n with respect to the variable Y takes the form

$$P_n(T, U, Y) = Y^{2^n} + B_1^{(n)} Y^{2^n-1} + \cdots + B_{2^n}^{(n)},$$

where $B_1^{(n)}, \ldots, B_{2^n}^{(n)}$ are suitable polynomials of $\mathbb{Q}[T, U]$.

Let $1 \leq k \leq 2^n$. In order to determine the polynomial $B_k^{(n)}$, we observe, by expanding the right hand side of (9), that $B_k^{(n)}$ collects the contribution of all terms of the form

$$\prod_{h=1}^{k} \big(- (j_h + T \prod_{i=1}^{n} U_i^{[j_h]_i})\big)$$

with $0 \leq j_1 < \cdots < j_k \leq 2^n - 1$. Therefore the polynomial $B_k^{(n)}$ can be expressed as follows:

$$\begin{aligned} B_k^{(n)} &= \sum_{0\leq j_1<\cdots<j_k<2^n} \prod_{h=1}^{k} \big(- (j_h + T \prod_{i=1}^{n} U_i^{[j_h]_i})\big) \\ &= \sum_{0\leq j_1<\cdots<j_k<2^n} (-1)^k \prod_{h=1}^{k} \big(j_h + T \prod_{i=1}^{n} U_i^{[j_h]_i}\big). \end{aligned}$$

Observe that for $0 \leq j_1 < \cdots < j_k < 2^n$ the expression

$$\prod_{h=1}^{k} \big(j_h + T \prod_{i=1}^{n} U_i^{[j_h]_i}\big)$$

can be rewritten as:

$$j_1 \cdots j_k + T\big(\sum_{h=1}^{k} j_1 \cdots \widehat{j_h} \cdots j_k \prod_{i=1}^{n} U_i^{[j_h]_i}\big) + \text{terms of higher degree in } T.$$

Therefore, we conclude that $B_k^{(n)}$ has the form:

$$\begin{aligned} B_k^{(n)} = & \sum_{0\leq j_1<\cdots<j_k<2^n} j_1 \cdots j_k \\ & + T\left(\sum_{0\leq j_1<\cdots<j_k<2^n} \sum_{h=1}^{k} j_1 \cdots \widehat{j_h} \cdots j_k \prod_{i=1}^{n} U_i^{[j_h]_i} \right) \qquad (10) \\ & + \text{terms of higher degree in } T. \end{aligned}$$

Let us denote by $L_k^{(n)}$ the coefficient of T in the representation (10), namely:

$$L_k^{(n)} := \sum_{0\leq j_1<\cdots<j_k<2^n} \sum_{h=1}^{k} j_1 \cdots \widehat{j_h} \cdots j_k \prod_{i=1}^{n} U_i^{[j_h]_i}.$$

We shall need the following technical result of [GH01]. In order to maintain this paper self–contained we are going to reproduce its proof here.

Lemma 6 *The polynomials $L_1^{(n)}, \ldots, L_{2^n}^{(n)}$ are $\mathbb{Q}$-linearly independent in $\mathbb{Q}[U]$.*

Proof.– Let us abbreviate $N := 2^n - 1$ and $L_1 := L_1^{(n)}, \ldots, L_{N+1} := L_{2^n}^{(n)}$. We observe that for $1 \le k \le N+1$ and $0 \le j \le N$ the coefficient $\ell_{k,j}$ of the monomial $\prod_{i=1}^n U_i^{[j]_i}$ occuring in the polynomial L_k can be represented as

$$\ell_{k,j} = \sum_{\substack{0 \le j_1 < \cdots < j_{k-1} \le N \\ j_r \ne j \text{ for } r=1,\ldots,k-1}} j_1 \cdots j_{k-1}.$$

Claim: *For fixed N and k, the coefficient $\ell_{k,j}$ can be written as a polynomial expression of degree exactly $k-1$ in the index j. Moreover, this polynomial expression for $\ell_{k,j}$ has integer coefficients.*

Proof of the Claim. We proceed by induction on the index parameter k.

For $k = 1$ we have $\ell_{1,j} = 1$ for any $0 \le j \le N$ and therefore $\ell_{1,j}$ is a polynomial of degree $k - 1 = 0$ in the index j.

Let $1 \le k \le N+1$. Assume inductively that $\ell_{k,j}$ is a polynomial of degree exactly $k-1$ in the index j and that the coefficients of this polynomial are integers. We are now going to show that $\ell_{k+1,j}$ is a polynomial of degree exactly k in j and that the coefficients of this polynomial are integers too. Observe that

$$\begin{aligned} \ell_{k+1,j} &= \sum_{\substack{0 \le j_1 < \cdots < j_k \le N \\ j_r \ne j \text{ for } r=1,\ldots,k}} j_1 \cdots j_k \\ &= \sum_{0 \le j_1 < \cdots < j_k \le N} j_1 \cdots j_k - j \left(\sum_{\substack{0 \le j_1 < \cdots < j_{k-1} \le N \\ j_r \ne j \text{ for } r=1,\ldots,k-1}} j_1 \cdots j_{k-1} \right). \end{aligned}$$

holds. Since the term

$$\sum_{0 \le j_1 < \cdots < j_k \le N} j_1 \cdots j_k$$

does not depend on j and since by induction hypothesis

$$\ell_{k,j} = \sum_{\substack{0 \le j_1 < \cdots < j_{k-1} \le N \\ j_r \ne j \text{ for } r=1,\ldots,k-1}} j_1 \cdots j_{k-1}$$

is a polynomial of degree exactly $k-1$ in j, we conclude that $\ell_{k+1,j}$ is a polynomial of degree exactly k in j. Moreover, the coefficients of this polynomial are integers. This proves our claim.

It is now easy to finish the proof of Lemma 6. By our claim there exist for arbitrary $1 \le k \le N+1$ integers $c_0^{(k)}, \cdots, c_{k-1}^{(k)}$ with $c_{k-1}^{(k)} \ne 0$ such that for any $0 \leq j \leq N$ the identity $\ell_{k,j} = c_0^{(k)} + \cdots + c_{k-1}^{(k)} j^{k-1}$ holds. Hence for arbitrary $0 \leq k \leq N$ there exist rational numbers $\lambda_1^{(k)}, \ldots, \lambda_{k+1}^{(k)}$ (not depending on j) such for any $0 \leq j \leq N$ the condition

$$j^k = \lambda_1^{(k)} \ell_{1,j} + \cdots + \lambda_{k+1}^{(k)} \ell_{k+1,j}$$

is satisfied (here we use the convention $0^0 := 1$). This implies for any index $0 \leq k \leq N$ the polynomial identity

$$\lambda_1^{(k)} L_1 + \cdots + \lambda_{k+1}^{(k)} L_{k+1} = \sum_{0 \leq j \leq N} j^k \prod_{i=1}^{n} U_i^{[j]_i}.$$

Hence for any $0 \leq k \leq N$ the polynomial $Q_k := \sum\limits_{0 \leq j \leq N} j^k \prod\limits_{i=1}^{n} U_i^{[j]_i}$ belongs to the $\mathbb{Q}$–vector space generated by $L_1, \ldots, L_{N+1}$. On the other hand, we deduce from the nonsingularity of the Vandermonde matrix $\left(j^k\right)_{0 \leq k,j \leq N}$ that the polynomials $Q_0, \ldots, Q_N$ are $\mathbb{Q}$-linearly independent. Therefore the $\mathbb{Q}$–vector space generated by $L_1, \ldots, L_{N+1}$ in $\mathbb{Q}[U]$ has dimension $N + 1 = 2^n$. This implies that $L_1, \ldots, L_{N+1}$ are $\mathbb{Q}$-linearly independent. ■

Let us now consider the object class of univariate polynomials $\mathcal{O}^{(n)} := \{P_n(t, u, Y); t \in \mathbb{A}^1, u \in \mathbb{A}^n\}$ and the encoding $\omega^{(n)} : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}^{(n)}$ defined for $t \in \mathbb{A}^1$, $u \in \mathbb{A}^n$ by $\omega^{(n)}(t, u) := P_n(t, u, Y)$. We are going to analyze the object class $\mathcal{O}^{(n)}$ and its encoding $\omega^{(n)}$ in the same way as in Section 4.1.

Representing the univariate polynomials belonging to $\mathcal{O}^{(n)}$ by their coefficients, we identify the object class $\mathcal{O}^{(n)}$ with the corresponding subset of the ambient space $\mathbb{A}^{2^n}$. With this interpretation $\omega^{(n)}$ becomes a polynomial map over $\mathbb{Q}$ which is defined for $t \in \mathbb{A}^1$, $u \in \mathbb{A}^n$ by $\omega^{(n)}(t, u) := \left(B_1^{(n)}(t, u), \ldots, B_{2^n}^{(n)}(t, u)\right)$. Thus $\omega^{(n)} : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}^{(n)}$ is a $\mathbb{Q}$–definable holomorphic encoding of the object class $\mathcal{O}^{(n)}$. Let $\beta^{(n)} := (\beta_1^{(n)}, \ldots, \beta_{2^n}^{(n)})$ with $\beta_k^{(n)} := \sum_{0 \leq j_1 < \cdots < j_k < 2^n} j_1 \cdots j_k$ for $1 \leq k \leq 2^n$. From (10) one deduces immediately that $\beta^{(n)}$ belongs to $\mathcal{O}^{(n)}$ and that $P_n(0, u, Y) = Y^{2^n} + \beta_1^{(n)} Y^{2^n - 1} + \cdots + \beta_{2^n}^{(n)}$ holds for any $u \in \mathbb{A}^n$. Hence the fiber $(\omega^{(n)})^{-1}(\beta^{(n)})$ contains the hyperplane $\{0\} \times \mathbb{A}^n$ of the affine space $\mathbb{A}^1 \times \mathbb{A}^n$. This implies that the encoding $\omega^{(n)}$ is ambiguous and *not robust*.

Suppose now that there is given a $\mathbb{Q}$–definable, holomorphic encoding $\sigma^{(n)} : \mathcal{D}^{(n)} \to \mathcal{O}^{(n)}$. Let us denote the size of $\mathcal{D}^{(n)}$ by $m^{(n)}$. Suppose furthermore that there is given a $\mathbb{Q}$–definable polynomial map $\theta^{(n)} : \mathbb{A}^1 \times \mathbb{A}^n \to \mathbb{A}^{m^{(n)}}$ with $\theta^{(n)}(\mathbb{A}^n) \subset \mathcal{D}^{(n)}$ and $\sigma^{(n)} \circ \theta^{(n)} = \omega^{(n)}$. As before, we interpret the polynomial map $\theta^{(n)}$ as a branching–free algorithm which transforms the encoding $\omega^{(n)}$ into the encoding $\sigma^{(n)}$. Although the object class $\mathcal{O}^{(n)}$ admits a (non–robust) encoding of small size (i.e. small in comparison with the embedding dimension of the object class $\mathcal{O}^{(n)}$), the requirement of *robustness* for the encoding $\sigma^{(n)}$ entails that the size of the data structure $\mathcal{D}^{(n)}$ must be necessarily large. This is the content of the following result.

Proposition 2 *Let notations and assumptions be as before. Suppose that $\sigma^{(n)} : \mathcal{D}^{(n)} \to \mathcal{O}^{(n)}$ is a robust, holomorphic encoding of the object class $\mathcal{O}^{(n)}$. Then the size of the data structure $\mathcal{D}^{(n)}$ satisfies the estimate*

$$m^{(n)} \geq 2^n.$$

PROOF.– Since $\sigma^{(n)}$ is a robust encoding we conclude that $(\sigma^{(n)})^{-1}(\beta^{(n)})$ is a nonempty finite subset of $\mathcal{D}^{(n)}$. From $\{0\} \times \mathbb{A}^n \subset (\omega^{(n)})^{-1}(\beta^{(n)})$ and $\omega^{(n)} = \sigma^{(n)} \circ \theta^{(n)}$ we infer $\theta^{(n)}(\{0\} \times \mathbb{A}^n) \subset (\sigma^{(n)})^{-1}(\beta^{(n)})$. Since $(\sigma^{(n)})^{-1}(\beta^{(n)})$ is finite and $\{0\} \times \mathbb{A}^n$ irreducible there exists a point $\alpha \in (\sigma^{(n)})^{-1}(\beta^{(n)})$ with $\theta^{(n)}(\{0\} \times \mathbb{A}^n) = \{\alpha\}$. Let u be arbitrary point of $\mathbb{A}^n$ and let $\gamma_u : \mathbb{A}^1 \to \mathbb{A}^{m^{(n)}}$ and $\delta_u : \mathbb{A}^1 \to \mathbb{A}^{2^n}$ be the polynomial maps defined for $t \in \mathbb{A}^1$ by $\gamma_u(t) := \theta^{(n)}(t, u)$ and $\delta_u(t) := \omega^{(n)}(t, u)$. Then we have $\gamma_u(0) = \alpha$, $\delta_u(0) = \beta^{(n)}$ and $\sigma^{(n)} \circ \gamma_u = \delta_u$. From (10) we deduce now

$$\big(L_1^{(n)}(u), \ldots , L_{2^n}^{(n)}(u)\big) = \frac{\partial}{\partial t}\omega^{(n)}(0, u) = \delta_u'(0) = (D\sigma^{(n)})_\alpha\big(\gamma_u'(0)\big).$$

Lemma 6 implies that there exist points $u_1, \ldots , u_{2^n} \in \mathbb{A}^n$ such that the $(2^n \times 2^n)$–matrix $\big(L_i^{(n)}(u_j)\big)_{1 \leq i,j \leq 2^n}$ is nonsingular. Therefore $\delta_{u_1}'(0), \ldots , \delta_{u_{2^n}}'(0)$ are linearly independent elements of the $\mathbb{C}$–vector space $\mathbb{A}^{2^n}$. Since $(D\, \sigma^{(n)})_\alpha : \mathbb{A}^{m^{(n)}} \to \mathbb{A}^{2^n}$ is a $\mathbb{C}$–linear map, we conclude that $\gamma_{u_1}'(0), \ldots , \gamma_{u_{2^n}}'(0)$ are linearly independent elements of the $\mathbb{C}$–linear space $\mathbb{A}^{m^{(n)}}$. This implies $m^{(n)} \geq 2^n$. ■

We observe that the proof of Proposition 2 implies that the local embedding dimension of the closed algebraic variety $\overline{\mathcal{O}}$ at the point $\beta^{(n)}$ (and hence the global embedding dimension of $\mathcal{O}^{(n)}$) is exactly 2^n.

Let $\mathcal{B}^{(n)} := \mathbb{Q}[B_1^{(n)}, \ldots , B_{2^n}^{(n)}]$ and let us denote by $L_{\mathcal{B}^{(n)}}(P_n)$ the minimal non–scalar size of the totally division–free arithmetic circuit with single input Y which evaluates the polynomial P_n using only scalars belonging to the $\mathbb{Q}$–algebra $\mathcal{B}^{(n)}$. In the same way as in Section 4.1 we may deduce from Proposition 2 the following result:

Corollary 6 *With the notations introduced before we have*

$$L_{\mathcal{B}^{(n)}}(P_n) = \Theta(2^{\frac{n}{2}}).$$

Corollary 6 says that the sequence of polynomials $(P_n)_{n \in \mathbb{N}}$ becomes hard to evaluate, if we require that for any $n \in \mathbb{N}$ the univariate polynomial $P_n \in \mathcal{B}^{(n)}[Y]$ has to be evaluated by a totally division–free arithmetic circuit whose scalars belong only to the $\mathbb{Q}$–algebra $\mathcal{B}^{(n)}$.

4.3 Rationality considerations.

In this section we motivate the algorithmic model used in Sections 4.1 and 4.2 for the algorithmic transformation of encodings of a given object class. For this purpose we are going to discuss the effect of certain rationality conditions on the encoding of an object class. Our first rationality condition requires to fix not only the ground field, namely $\mathbb{Q}$, but also its algebraic closure, namely $\mathbb{C}$.

Let be given a data structure $\mathcal{D}$ and an object class $\mathcal{O}$ and suppose that $\mathcal{D}$ and $\mathcal{O}$ are $\mathbb{Q}$–constructible subsets of the ambient spaces $\mathbb{A}^L$ and $\mathbb{A}^N$ respectively. Let be given an encoding $\omega : \mathcal{D} \to \mathcal{O}$ and suppose that ω is $\mathbb{Q}$–definable and holomorphic. Let us denote by m the maximal local embedding dimension of the $\mathbb{Q}$–Zariski closure $\overline{\mathcal{O}}$ of the object class $\mathcal{O}$ at any point of $\overline{\mathcal{O}}$ (i.e. m is the maximal $\mathbb{C}$–vector space dimension of the Zariski tangent space of the algebraic variety $\overline{\mathcal{O}}$ at any point).

The first rationality condition we are going to consider is the following: *for any object $\beta = (\beta_1, \dots, \beta_N) \in \mathcal{O}$ there exists a code $\alpha = (\alpha_1, \dots, \alpha_L) \in \omega^{-1}(\beta)$ with $\alpha_1, \dots, \alpha_L \in \mathbb{Q}[\beta]$.*

Suppose now that ω satisfies this rationality condition, that $\mathcal{D}$ and $\mathcal{O}$ are $\mathbb{Q}$–definable closed subvarieties of $\mathbb{A}^L$ and $\mathbb{A}^N$ and that $\mathcal{O}$ is $\mathbb{Q}$–irreducible. Since the transcendence degree of $\mathbb{C}$ over $\mathbb{Q}$ is infinite, there exists a generic element $b = (b_1, \dots, b_N)$ of $\mathcal{O}$ such that the canonical specialization of the coordinate ring $\mathbb{Q}[\mathcal{O}]$ of the irreducible algebraic variety $\mathcal{O}$ onto $\mathbb{Q}[b]$ is injective. Therefore we have $\mathbb{Q}[\mathcal{O}] \cong \mathbb{Q}[b]$. By hypothesis there exists a code $a = (a_1, \dots, a_L) \in \omega^{-1}(b)$ with $a_1, \dots, a_L \in \mathbb{Q}[b]$. Denote by $Y_1, \dots, Y_N$ the coordinate functions of the affine space $\mathbb{A}^N$. Then there exist polynomials $\psi_1, \dots, \psi_L \in \mathbb{Q}[Y_1, \dots, Y_N]$ with $a_k = \psi_k(b_1, \dots, b_N)$ for $1 \leq k \leq L$.

Since $\mathcal{O}$ and $\mathcal{D}$ are closed subvarieties of $\mathbb{A}^N$ and $\mathbb{A}^L$ respectively, this implies that $\psi := (\psi_1, \dots, \psi_L)$ induces a $\mathbb{Q}$–definable morphism of algebraic varieties which maps $\mathcal{O}$ into $\mathcal{D}$ and which we denote by $\psi : \mathcal{O} \to \mathcal{D}$. Moreover we have $\omega \circ \psi = id_{\mathcal{O}}$. Therefore for any $\beta \in \mathcal{O}$ the $\mathbb{C}$–linear map $T_{\psi(\beta)}(\omega) : T_{\psi(\beta)}(\mathcal{D}) \to T_\beta(\mathcal{O})$ is surjective (here $T_{\psi(\beta)}(\mathcal{D})$ and $T_\beta(\mathcal{O})$ denote the Zariski tangent spaces of the algebraic varieties $\mathcal{D}$ and $\mathcal{O}$ at the points $\psi(\beta)$ and β respectively and $T_{\psi(\beta)}(\omega)$ denotes the tangent map induced by ω at the point $\psi(\beta)$).

Since the object class $\mathcal{O}$ is irreducible and Zariski closed in $\mathbb{A}^N$, we may choose a point $\beta_0 \in \mathcal{O}$ with $dim_{\mathbb{C}} T_{\beta_0}(\mathcal{O}) = m$ (here $dim_{\mathbb{C}} T_{\beta_0}(\mathcal{O})$ denotes the $\mathbb{C}$–vector space dimension of the Zariski tangent space $T_{\beta_0}(\mathcal{O})$). Since $T_{\psi(\beta_0)}(\omega) : T_{\psi(\beta_0)}(\mathcal{D}) \to T_{\beta_0}(\mathcal{O})$ is a surjective $\mathbb{C}$–linear map, we conclude $L \geq dim_{\mathbb{C}} T_{\psi(\beta_0)}(\mathcal{D}) \geq m$. Therefore any encoding of the data structure $\mathcal{O}_d$ of Section 4.1 or of the data structure $\mathcal{O}^{(n)}$ of Section 4.2 which satisfies the rationality condition above has at least size d or size 2^n respectively.

Now we are going to discuss a second rationality condition which comes much closer to the usual requirements in the design of practical algorithms. For the sake of succinctness of exposition we shall omit proofs (they are based on Hilbert's Irreducibility Theorem and Lüroth's Theorem and will be published in forthcoming paper).

Informally, we may state our second rationality requirement as follows: *suppose that the object class $\mathcal{O}$ contains "many" integer objects (i.e. points which belong to $\mathbb{Z}^N$). Then there exist "sufficiently many" integer objects of $\mathcal{O}$ such that for each such object $O \in \mathcal{O} \cap \mathbb{Z}^N$ there exists an integer code $D \in \mathcal{D} \cap \mathbb{Z}^L$ with $\omega(D) = O$. In order to guarantee the existence of sufficiently many integer objects in $\mathcal{O}$ we require that there is given an encoding $\omega^* : \mathbb{A}^{L^*} \to \mathcal{O}$ of the object class $\mathcal{O}$ such that ω^* is definable by polynomials with integer coefficients. Thus ω^* maps integer codes of $\mathbb{A}^{L^*}$ onto integer objects of $\mathcal{O}$.*

For technical reasons we shall need the following additional assumptions: we suppose that $\mathcal{D}$ is a $\mathbb{Q}$–definable, $\mathbb{Q}$–irreducible subvariety of $\mathbb{A}^L$ and that the given encoding $\omega : \mathcal{D} \to \mathcal{O}$ is definable by polynomials with integer coefficients. This implies that the closed subvariety $\overline{\mathcal{O}}$ of $\mathbb{A}^N$ is $\mathbb{Q}$–definable and $\mathbb{Q}$–irreducible too. Moreover we suppose $dim\, \mathcal{D} = dim\, \overline{\mathcal{O}}$. Therefore there exists a Zariski open subset of $\overline{\mathcal{O}}$ which is contained in $\mathcal{O} = \omega(\mathcal{D})$, such that each point of this subset has a nonempty, finite ω–fiber. With these notations and assumptions we are able to state the following result:

Proposition 3 *Suppose that there exists a nonempty $\mathbb{Q}$–definable, Zariski open subset $\mathcal{U}$ of $\mathbb{A}^{L^*}$ with the following property: for any code $D^* \in \mathcal{U} \cap \mathbb{Z}^{L^*}$ there exists a code $D \in \mathcal{D} \cap \mathbb{Z}^L$ with $\omega^*(D^*) = \omega(D)$.*

Then there exists a $\mathbb{Q}$–definable morphism $\theta : \mathbb{A}^{L^*} \to \mathcal{D}$ and a subset $\mathcal{U}_0$ of $\mathcal{U} \cap \mathbb{Z}^{L^*}$ such that the following conditions are satisfied:

(i) $\mathcal{U}_0$ is Zariski–dense in $\mathbb{A}^{L^*}$.

(ii) $\omega \circ \theta = \omega^*$.

(iii) $\theta(D^*) \in \mathcal{D} \cap \mathbb{Z}^L$ for any $D^* \in \mathcal{U}_0$.

Suppose additionally $L^* := 1$ and that the leading coefficients of all nonconstant polynomials occurring in the definition of ω^* have greatest common divisor one. Suppose furthermore that for any integer object $O \in \mathcal{O} \cap \mathbb{Z}^N$ there exists an integer code $D \in \mathcal{D} \cap \mathbb{Z}^L$ with $O = \omega(D)$. Then ω is a robust encoding.

We may paraphrase the first part of Proposition 3 as follows: if the encoding $\omega : \mathcal{D} \to \mathcal{O}$ admits for any object of $\mathcal{O}$, which allows an *integer* encoding by ω^*, an *integer* encoding by ω, then the encoding ω^*

may be transformed into the encoding ω by means of an algorithm in the sense of Sections 4.1 and 4.2. This motivates the notion of (branching–free) algorithm which we introduced before and which we shall continue to use in the remaining part of this paper.

The second part of Proposition 3 says roughly the following: if a given $\mathbb{Q}$–definable holomorphic encoding of an infinite object class by a data structure of size one satisfies our second rationality condition, then this encoding is necessarily robust. Therefore the paradigm of Section 4.1 is representative for this type of encodings.

5 The complexity of elimination algorithms.

5.1 Flat families of zero–dimensional elimination problems.

Let, as before, k be an infinite and perfect field with algebraic closure $\bar{k}$ and let $U_1, \ldots, U_r, X_1, \ldots, X_n, Y$ be indeterminates over k. In the sequel we shall consider $X_1, \ldots, X_n$ and Y as variables and $U_1, \ldots, U_r$ as parameters. Let $U := (U_1, \ldots, U_r)$ and $X := (X_1, \ldots, X_n)$ and let $G_1, \ldots, G_n$ and F be polynomials belonging to the k-algebra $k[U,X] := k[U_1, \ldots, U_r, X_1, \ldots, X_n]$. Suppose that the polynomials $G_1, \ldots, G_n$ form a regular sequence in $k[U,X]$ defining thus an equidimensional subvariety $V := \{G_1 = 0, \ldots, G_n = 0\}$ of the $(r+n)$–dimensional affine space $\mathbb{A}^r \times \mathbb{A}^n$. The algebraic variety V has dimension r. Let δ be the (geometric) degree of V (observe that this degree does not take into account multiplicities or components at infinity). Suppose furthermore that the morphism of affine varieties $\pi : V \to \mathbb{A}^r$, induced by the canonical projection of $\mathbb{A}^r \times \mathbb{A}^n$ onto $\mathbb{A}^r$, is finite and generically unramified (this implies that π is flat and that the ideal generated by $G_1, \ldots, G_n$ in $k[U,X]$ is radical). Let $\tilde{\pi} : V \to \mathbb{A}^{r+1}$ be the morphism defined by $\tilde{\pi}(z) := (\pi(z), F(z))$ for any point z of the variety V. The image of $\tilde{\pi}$ is a hypersurface of $\mathbb{A}^{r+1}$ whose minimal equation is a polynomial of $k[U,Y] := k[U_1, \ldots, U_r, Y]$ which we denote by P. Let us write $\deg P$ for the total degree of the polynomial P and $\deg_Y P$ for its partial degree in the variable Y. Observe that P is monic in Y and that $\deg P \leq \delta \deg F$ holds. Furthermore, for a Zariski dense set of points u of $\mathbb{A}^r$, we have that $\deg_Y P$ is the cardinality of the image of the restriction of F to the finite set $\pi^{-1}(u)$. The polynomial $P(U,F)$ vanishes on the variety V.

Let us consider an arbitrary point $u := (u_1, \ldots, u_r)$ of $\mathbb{A}^r$. For arbitrary polynomials $A \in k[U,X]$ and $B \in k[U,Y]$ we denote by $A^{(u)}$ and $B^{(u)}$ the polynomials $A(u_1, \ldots, u_r, X_1, \ldots, X_n)$ and $B(u_1, \ldots, u_r, Y)$ which belong to $k(u)[X] := k(u_1, \ldots, u_r)[X_1, \ldots, X_n]$ and $k(u)[Y] := k(u_1, \ldots, u_r)[Y]$ respectively. Similarly we denote for an arbitrary polynomial $C \in k[U]$ by $C^{(u)}$ the value $C(u_1, \ldots, u_r)$ which belongs to the field $k(u) := k(u_1, \ldots, u_r)$. The polynomials $G_1^{(u)}, \ldots, G_n^{(u)}$ define a zero dimensional subvariety $V^{(u)} :=$

$\{G_1^{(u)} = 0, \ldots, G_n^{(u)} = 0\} = \pi^{-1}(u)$ of the affine space $\mathbb{A}^n$. The degree (i.e. the cardinality) of $V^{(u)}$ is bounded by δ. Denote by $\tilde{\pi}^{(u)} : V^{(u)} \to \mathbb{A}^1$ the morphism induced by the polynomial $F^{(u)}$ on the variety $V^{(u)}$. Observe that the polynomial $P^{(u)}$ vanishes on the (finite) image of the morphism $\tilde{\pi}^{(u)}$. Observe also that the polynomial $P^{(u)}$ is not necessarily the minimal equation of the image of $\tilde{\pi}^{(u)}$.

We call the equation system $G_1 = 0, \ldots, G_n = 0$ and the polynomial F *a flat family of zero–dimensional elimination problems depending on the parameters* $U_1, \ldots, U_r$ and we call P the associated *elimination polynomial.* An element $u \in \mathbb{A}^r$ is considered as a *parameter point* which determines a *particular problem instance.* The equation system $G_1 = 0, \ldots, G_n = 0$ together with the polynomial F is called the *general instance* of the given flat family of elimination problems and the elimination polynomial P is called the *general solution* of this flat family. A branching–free algorithm which in terms of suitable data structures computes from a given representation of the general problem instance $G_1 = 0, \ldots, G_n = 0, F$ a representation of its general solution P is called a *Kronecker–like elimination procedure* (see Section 1.2).

The *particular problem instance* determined by the parameter point $u \in \mathbb{A}^r$ is given by the equations $G_1^{(u)} = 0, \ldots, G_n^{(u)} = 0$ and the polynomial $F^{(u)}$. The polynomial $P^{(u)}$ is called *a solution* of this particular problem instance. We call two parameter points $u, u' \in \mathbb{A}^r$ *equivalent* (in symbols: $u \sim u'$) if $G_1^{(u)} = G_1^{(u')}, \ldots, G_n^{(u)} = G_n^{(u')}$ and $F^{(u)} = F^{(u')}$ holds. Observe that $u \sim u'$ implies $P^{(u)} = P^{(u')}$. We call polynomials $A \in k[U, X]$, $B \in k[U, Y]$ and $C \in k[U]$ *invariant* (with respect to $\sim$) if for any two parameter points u, u' of $\mathbb{A}^r$ with $u \sim u'$ the respective identities $A^{(u)} = A^{(u')}$, $B^{(u)} = B^{(u')}$ and $C^{(u)} = C^{(u')}$ hold.

Let us consider the set of parameter points of $\mathbb{A}^r$ as data structure which encodes the object class $\mathcal{O} := \{(G_1^{(u)}, \ldots, G_n^{(u)}, F^{(u)}); u \in \mathbb{A}^r\}$. The corresponding encoding $\omega : \mathbb{A}^r \to \mathcal{O}$ is defined for $u \in \mathbb{A}^r$ by $\omega(u) := (G_1^{(u)}, \ldots, G_n^{(u)}, F^{(u)})$. Observe that ω is $\mathbb{Q}$–definable and holomorphic. Let $\mathcal{D}^*$ be a k–constructible data structure of size L^* which encodes the object class $\mathcal{O}^* := \{P^{(u)}; u \in \mathbb{A}^r\}$ by means of a given k–definable, holomorphic encoding $\omega^* : \mathcal{D}^* \to \mathcal{O}^*$. Let us consider $\mathcal{O}$ as input and $\mathcal{O}^*$ as output object class of a given branching–free Kronecker–like elimination procedure. Suppose that this elimination procedure is determined by polynomials $\theta_1, \ldots, \theta_{L^*} \in k[U]$ such that $\theta := (\theta_1, \ldots, \theta_{L^*})$ induces a k–definable map from $\mathbb{A}^r$ into $\mathcal{D}^*$ which we denote by $\theta : \mathbb{A}^r \to \mathcal{D}^*$. This means that for any parameter point $u \in \mathbb{A}^r$, the given elimination procedure, which we denote also by θ, satisfies the condition $\omega^*\big(\theta(u)\big) = P^{(u)}$. Suppose furthermore that the elimination procedure θ is totally *division–free* (this means that the general solution P of the given elimination problem belongs to $k[\theta][Y]$; see

Section 2.2). We call θ *invariant* (with respect to the equivalence relation $\sim$) if $\theta_1, \ldots, \theta_{L^*}$ are invariant polynomials. The invariance of the elimination procedure θ means that for any input code $u \in \mathbb{A}^r$ the code $\theta(u) \in \mathcal{D}^*$ of the corresponding output object $P^{(u)}$ depends only on the input *object*, namely $(G_1^{(u)}, \ldots, G_n^{(u)}, F^{(u)}) \in \big(k(u)[X]\big)^{n+1}$ and not on its particular representation u. Said otherwise, an invariant elimination procedure produces the solution of a particular problem instance in a way which is independent of the possibly different representations of the given problem instance.

Since all known Kronecker–like elimination procedures produce for flat families of zero–dimensional elimination problems a branching and totally division–free representation of the output polynomial, and since they are based on the manipulation of the input objects (and not on their particular representations) by means of linear algebra or comprehensive Gröbner basis techniques, we conclude that these algorithms are in fact invariant elimination procedures.

Typical examples of such procedures are furnished by black–box algorithms. With the notations introduced before, we call the elimination procedure θ a *black–box algorithm* if for any input code $u \in \mathbb{A}^r$, the procedure θ calls only for evaluations of the input object $(G_1^{(u)}, \ldots, G_n^{(u)}, F^{(u)})$ on specializations of the variables $X_1, \ldots, X_n$ to assignment values which belong to suitable commutative $k[u]$–algebras.

A (branching–parsimonious) computer program for elimination tasks which calls its input polynomials only by their specification as evaluation procedures, represents necessarily a black–box algorithm.

We are now going to introduce a slight generalization of the notion of invariance of the elimination procedure θ.

Let $\mathcal{D}_\theta := \big\{\big(\omega(u), \theta(u)\big); u \in \mathbb{A}^r\big\}$ and let $\omega_\theta : \mathcal{D}_\theta \to \mathcal{O}$ be the canonical first projection of $\mathcal{D}_\theta$ onto the object class $\mathcal{O}$. One verifies immediately that $\mathcal{D}_\theta$ is a $\mathbb{Q}$–definable data structure and that ω_θ is a $\mathbb{Q}$–definable holomorphic encoding of the object class $\mathcal{O}$. Observe that $\overline{\mathcal{D}_\theta}$ and $\overline{\mathcal{O}}$ are irreducible closed subvarieties of their corresponding affine ambient spaces.

Definition 4 *Let notations and assumptions be as before. We call the elimination procedure θ robust if the following condition is satisfied:*

let $u \in \mathbb{A}^r$ be a given parameter point determining the input object $(G_1^{(u)}, \ldots, G_n^{(u)}, F^{(u)}) \in \mathcal{O}$ and let $\mathfrak{m}_u$ be the maximal defining ideal of this input object in $\mathbb{C}[\overline{\mathcal{O}}]$. Then the local ring $\mathbb{C}[\overline{\mathcal{D}_\theta}]_{\mathfrak{m}_u}$ is a finite $\mathbb{C}[\overline{\mathcal{O}}]_{\mathfrak{m}_u}$–module.

In other words, the elimination procedure θ is robust if and only if ω_θ is a robust holomorphic encoding.

Observe that an invariant elimination procedure is robust.

If θ is a robust elimination procedure, then one sees easily that the following condition is satisfied:

(*i*) *for any parameter point* $u \in \mathbb{A}^r$*, the set*

$$\{\theta(v); v \in \mathbb{A}^r, G_1^{(v)} = G_1^{(u)}, \ldots, G_n^{(v)} = G_n^{(u)}, F^{(v)} = F^{(u)}\}$$

is finite.

In case $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$, one deduces easily from Lemma 3 that Definition 4 is equivalent to the following condition:

(*ii*) *let* $(u_i)_{i\in\mathbb{N}}$ *be a sequence of parameter points of* $\mathbb{A}^r$ *encoding a sequence of input objects* $\big((G_1^{(u_i)}, \ldots, G_n^{(u_i)}, F^{(u_i)})\big)_{i\in\mathbb{N}}$. *Suppose that there exists a parameter point* $u \in \mathbb{A}^r$ *such that* $(G_1^{(u)}, \ldots, G_n^{(u)}, F^{(u)}) \in \mathcal{O}$ *is an limit point of the sequence of input objects* $\big((G_1^{(u_i)}, \ldots, G_n^{(u_i)}, F^{(u_i)})\big)_{i\in\mathbb{N}}$ *(with respect to the strong topology). Then the sequence* $(\theta(u_i))_{i\in\mathbb{N}}$ *has an accumulation point.*

Observe that condition (*ii*) gives an intuitive meaning to the technical Definition 4.

5.2 Parametric greatest common divisors and their computation.

Let us now introduce the notion of parametric greatest common divisor of a given algebraic family of polynomials and let us consider the corresponding algorithmic problem. We are going to use the same notations as in Sections 2.2 and 5.1.

Suppose that there is given a positive number s of nonzero polynomials, say $B_1, \ldots, B_s \in k[U_1, \ldots, U_r, Y]$. Let $V := \{B_1 = 0, \ldots, B_s = 0\}$. Suppose that V is nonempty. We consider now the morphism of affine varieties $\pi : V \longrightarrow \mathbb{A}^r$, induced by the canonical projection of $\mathbb{A}^r \times \mathbb{A}^1$ onto $\mathbb{A}^r$. Let S be the Zariski closure of $\pi(V)$ and suppose that S is an *irreducible* closed subvariety of $\mathbb{A}^r$. Let us denote by $k[S]$ the coordinate ring of S. Since S is irreducible we conclude that $k[S]$ is a domain with a well defined function field which we denote by $k(S)$.

Let $b_1, \ldots, b_s \in k[S][Y]$ be the polynomials in the variable Y with coefficients in $k[S]$, induced by $B_1, \ldots, B_s$. Suppose that there exists an index $1 \le k \le s$ with $b_k \ne 0$. Without loss of generality we may suppose that for some index $1 \le q \le s$ the polynomials $b_1, \ldots, b_q$ are exactly the non–zero elements of $b_1, \ldots, b_s$. Observe that each polynomial $b_1, \ldots, b_q$ has positive degree (in the variable Y).

We consider $b_1, \ldots, b_q$ as an *algebraic family of polynomials* (in the variable Y) and $B_1, \ldots, B_q$ as their representatives. The polynomials $b_1, \ldots, b_q$ have in $k(S)[Y]$ a well defined *normalized* (i.e. monic) greatest common divisor, which we denote by h. Let D be the degree of h (with respect to the variable Y).

We are now going to describe certain geometric requirements which will allow us to consider h as a parametric greatest common divisor of the algebraic family of polynomials $b_1, \ldots, b_q$.

Our first requirement is $D \geq 1$. Moreover we require that for any point $u \in S$ and any place $\varphi : \overline{k}(S) \to \overline{k} \cup \{\infty\}$, whose valuation ring contains the local ring of the variety S at the point u, the values of the coefficients of the polynomial $h \in k(S)[Y]$ under φ are *finite* and *uniquely determined* by the point u. In this way the place φ maps the polynomial h to a monic polynomial of degree D in Y with coefficients in $\overline{k}$. This polynomial depends only on the point $u \in S$ and we denote it therefore by $h(u)(Y)$. In analogy with this notation we write $b_k(u)(Y) := B_k(u)(Y)$ for $1 \leq k \leq q$. Since h is monic one concludes easily that $h(u)(Y)$ divides the polynomials $b_1(u)(Y), \ldots, b_q(u)(Y)$ (and hence their greatest common divisor if not all of them are zero).

We say that a polynomial H of $k(U_1, \ldots, U_r)[Y]$ with *$deg_Y H = D$ represents* the greatest common divisor $h \in k(S)[Y]$ if the coefficients of H with respect to the variable Y induce well–defined rational functions of the variety S and if these rational functions are exactly the coefficients of h (with respect to the variable Y).

Suppose now that the polynomials $B_1, \ldots, B_s \in k[U_1, \ldots, U_r, Y]$ satisfy all our requirements for any point $u \in S$. Then we say that for the algebraic family of polynomials $b_1, \ldots, b_q \in k(S)[Y]$ a parametric common divisor exists and we call $h \in k(S)[Y]$ the *parametric greatest common divisor* of $b_1, \ldots, b_q$. Any polynomial $H \in k(U_1, \ldots, U_r)[Y]$ which represents h is said to *represent the parametric greatest common divisor associated to the polynomials $B_1, \ldots, B_s$*.

A monic *squarefree* polynomial $\widehat{h} \in k(S)[Y]$ with the same zeroes as h in an algebraic closure of $k(S)$, is called the *generically squarefree* parametric greatest common divisor of the algebraic family $b_1, \ldots, b_q \in k[S][Y]$ if $\widehat{h}$ satisfies the requirements imposed above on h. In this case we say that for the algebraic family of polynomials $b_1, \ldots, b_q \in k[S][Y]$ a generically squarefree parametric greatest common divisor exists. The notion of a representative of $\widehat{h}$ is defined in the same way as for h.

Let us consider $\mathbb{A}^r$ as input data structure of size r with S the set of admissible input instances and let us consider the problem of computing the parametric greatest common divisor h by means of an essentially division–free algorithm for any admissible input instance $u \in S$.

Such an algorithm, with output data structure of size m, is represented by m rational functions $\theta_1, \ldots, \theta_m \in k(S)$ such that the parametric greatest common divisor h belongs to the k–algebra $k[\theta_1, \ldots, \theta_m][Y]$. Recall that our assumptions on h imply that for any input instance $u \in S$ the polynomial $h(u)(Y) \in \overline{k}[Y]$ is well defined. Consequently we shall require that for any input instance $u \in S$ and any place $\varphi : k(S) \to \overline{k} \cup \{\infty\}$, whose valuation ring contains the local ring of the variety S at the point u, the values $\varphi(\theta_1), \ldots, \varphi(\theta_m)$ are finite and uniquely determined by the input instance u. If this requirement is satisfied we shall say that our algorithm *computes* the parametric greatest common divisor h of the algebraic family of polynomials $b_1, \ldots, b_q$ *for any admissible input instance* $u \in S$. Observe that in this case the rational functions $\theta_1, \ldots, \theta_m$ belong to the integral closure of $k[S]$ in $k(S)$.

In concrete situations it is reasonable, however not required by the mathematical arguments we will apply in this paper, to include the following items in the notion of an algorithm which computes the parametric greatest common divisor h of the algebraic family of polynomials $b_1, \ldots, b_q$:

- an explicit representation of the rational functions $\theta_1, \ldots, \theta_m$ by numerator and denominator polynomials belonging to $k[U_1, \ldots, U_r]$,

- an explicit definition of the closed subvariety S of $\mathbb{A}^r$ by polynomials belonging to $k[U_1, \ldots, U_r]$.

The numerator and denominator polynomials representing the rational functions $\theta_1, \ldots, \theta_m$ and the polynomials of $k[U_1, \ldots, U_r]$ defining the closed variety S should then be holomorphically encoded by a suitable data structure.

If there exists for the algebraic family of polynomials $b_1, \ldots, b_q$ a generically squarefree parametric greatest common divisor $\widehat{h}$, we shall apply the same terminology to any essentially division–free algorithm which computes $\widehat{h}$.

5.3 A particular flat elimination problem.

Changing slightly the notations of Section 5.1 put now $r := n+1$, $T := U_{n+1}$, $U := (U_1, \ldots, U_n)$. Let us consider the following polynomials of $\mathbb{Q}[T, U, X]$:

$$G_1 := X_1^2 - X_1, \ldots, G_n := X_n^2 - X_n,$$

$$F_n := \sum_{i=1}^{n} 2^{i-1} X_i + T \prod_{i=1}^{n} \big(1 + (U_i - 1) X_i\big). \tag{11}$$

It is clear from their definition that the polynomials $G_1, \ldots, G_n$ and F can be evaluated by a totally division–free arithmetic circuit β of size $O(n)$ in $\mathbb{Q}[T, U, X]$. Observe that the polynomials $G_1, \ldots, G_n$ do not depend on the parameters $T, U_1, \ldots, U_n$ and that their degree is two. The polynomial F_n is of degree $2n + 1$. More precisely, we have $\deg_X F_n = n$, $\deg_U F_n = n$, and $\deg_T F_n = 1$. Although the polynomial F_n may be evaluated by a totally division–free circuit of size $O(n)$, the sparse representation of F_n, as a polynomial over $\mathbb{Q}$ in the variables $T, U_1, \ldots, U_n, X_1, \ldots, X_n$, contains 3^n nonzero monomial terms and, as a polynomial over $\mathbb{Q}[T, U_1, \ldots, U_n]$ in the variables $X_1, \ldots, X_n$, it contains 2^n nonzero terms.

Let us now verify that the polynomials $G_1, \ldots, G_n$ and F_n form a flat family of elimination problems depending on the parameters $T, U_1, \ldots, U_n$.

The variety $V := \{G_1 = 0, \ldots, G_n = 0\}$ is nothing but the union of 2^n affine linear subspaces of $\mathbb{A}^{n+1} \times \mathbb{A}^n$, each of them of the form $\mathbb{A}^{n+1} \times \{\xi\}$, where ξ is a point of the hypercube $\{0,1\}^n$. The canonical projection $\mathbb{A}^{n+1} \times \mathbb{A}^n \to \mathbb{A}^{n+1}$ induces a morphism $\pi : \ V \to \mathbb{A}^{n+1}$ which glues together the canonical projections $\mathbb{A}^{n+1} \times \{\xi\} \to \mathbb{A}^{n+1}$ for any ξ in $\{0,1\}^n$. Obviously the morphism π is finite and unramified. In particular π has constant fibres which are all canonically isomorphic to the hypercube $\{0,1\}^n$.

Let $(j_1, \ldots, j_n)$ be an arbitrary point of $\{0,1\}^n$ and let $j := \sum_{1 \leq i \leq n} j_i 2^{i-1}$ be the integer $0 \leq j < 2^n$ whose bit representation is $j_n j_{n-1} \cdots j_1$. One verifies immediately the identity

$$F_n(T, U_1, \ldots, U_n, j_1, \ldots, j_n) = j + T \prod_{i=1}^{n} U_i^{j_i}.$$

Therefore for any point $(t, u_1, \ldots, u_n, j_1, \ldots, j_n) \in V$ with $j := \sum_{i=1}^{n} j_i 2^{i-1}$ we have

$$F_n(t, u_1, \ldots, u_n, j_1, \ldots, j_n) = j + t \prod_{i=1}^{n} u_i^{j_i}.$$

From this observation we deduce easily that the elimination polynomial associated with the flat family of zero–dimensional elimination problems determined by the polynomials $G_1, \ldots, G_n$ and F is in fact the polynomial

$$P_n = \prod_{j=0}^{2^n-1} (Y - (j + T \prod_{i=1}^{n} U_i{}^{[j]_i}))$$

of Section 4.2. With the notations of Section 4.2, this polynomial has the form

$$\begin{aligned} P_n &= Y^{2^n} + \textstyle\sum_{1 \leq k \leq 2^n} B_k^{(n)} Y^{2^n-k} \\ &\equiv Y^{2^n} + \textstyle\sum_{1 \leq k \leq 2^n} (\beta_k^{(n)} + T L_k^{(n)}) Y^{2^n-k} \text{ modulo } T^2, \end{aligned} \tag{12}$$

with $\beta_k^{(n)} := \sum_{1 \leq j_1 < \cdots < j_k < 2^n} j_1 \cdots j_k$ for $1 \leq k \leq 2^n$.

Let us consider

$$\begin{aligned} \mathcal{O}_n := \Big\{ F_n^{(t,u)}; t \in \mathbb{A}^1, u := (u_1, \ldots, u_n) \in \mathbb{A}^n, \\ F_n^{(t,u)} := \textstyle\sum_{i=1}^{n} 2^{i-1} X_i + t \prod_{i=1}^{n} \big(1 + (u_i - 1) X_i\big) \Big\} \end{aligned}$$

as input object class of our flat family of zero–dimensional elimination problems, the affine space $\mathbb{A}^1 \times \mathbb{A}^n$ as input data structure and the map $\omega_n : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}_n$ defined for $(t,u) \in \mathbb{A}^1 \times \mathbb{A}^n$ by $\omega_n(t,u) := F_n^{(t,u)}$ as a $\mathbb{Q}$–definable holomorphic encoding of the input object class $\mathcal{O}_n$.

Let us consider the set of univariate polynomials

$$\mathcal{O}_n^* := \Big\{ P_n^{(t,u)}; t \in \mathbb{A}^1, u := (u_1, \dots, u_n) \in \mathbb{A}^n, \\ P_n^{(t,u)} := \textstyle\prod_{j=0}^{2^n-1} \big(Y - (j + t \prod_{i=1}^n u_i{}^{[j]_i})\big) \Big\}$$

as output object class and let be given a $\mathbb{Q}$–constructible output data structure $\mathcal{D}_n^*$ of size m_n^* and a $\mathbb{Q}$–definable, holomorphic encoding $\omega_n^* : \mathcal{D}_n^* \to \mathcal{O}_n^*$. Finally let be given a totally division–free elimination procedure $\theta_n : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{D}_n^*$ (in the sense of Section 5.1) which solves the zero–dimensional elimination problem determined by the polynomials $G_1, \dots, G_n$ and F_n. Observe that the size of our input data structure is $n+1$. With this notations we have the following result:

Theorem 3 *Assume that the elimination procedure θ_n is robust in the sense of Definition 4. Then the size m_n^* of the output data structure $\mathcal{D}_n^*$ satisfies the estimate*

$$m_n^* \geq 2^n.$$

PROOF.– Since the arguments of this proof are similar to those used in Section 4.2, we shall be concise in our presentation.

Representing the univariate polynomials belonging to $\mathcal{O}_n^*$ by their coefficients we may identify the output object class $\mathcal{O}^*$ with the corresponding subset of the ambient space $\mathbb{A}^{2^n}$. With this interpretation the encoding $\omega_n^* : \mathcal{D}^* \to \mathcal{O}^*$ becomes induced by a polynomial map from the affine space $\mathbb{A}^{m_n^*}$ to the affine space $\mathbb{A}^{2^n}$. Therefore $\omega_n^* \circ \theta_n : \mathbb{A}^{n+1} \to \mathbb{A}^{2^n}$ is a polynomial map too.

Let $f_n := \sum_{i=1}^n 2^{i-1} X_i$, let

$$\beta_n := (\beta_1^{(n)}, \dots, \beta_{2^n}^{(n)}) = \left(\sum_{1 \leq j_1 \leq \cdots \leq j_k < 2^n} j_1 \cdots j_k \right)_{1 \leq k \leq 2^n}$$

and let u be an arbitrary point of $\mathbb{A}^n$. From (11) and (12) we deduce $F_n^{(0,u)} = f_n$ and $P_n^{(0,u)} = Y^{2^n} + \beta_1^{(n)} Y^{2^n-1} + \cdots + \beta_{2^n}^{(n)}$. In particular we have $\beta_n = \omega_n^*\big(\theta_n(0,u)\big)$. This implies that the fiber $(\omega_n^* \circ \theta_n)^{-1}(\beta_n)$ contains the hypersurface $\{0\} \times \mathbb{A}^n$ of the affine space $\mathbb{A}^1 \times \mathbb{A}^n$. Moreover, since the elimination algorithm θ_n is robust, we deduce from condition (i) of Section 5.1 and from $F_n^{(0,u)} = f_n$ that there are only finitely many possible values for $\theta_n(0,u)$. More precisely, the set $\{\theta_n(0,v); v \in \mathbb{A}^n\}$ is finite. Since $\{0\} \times \mathbb{A}^n$

is irreducible we conclude now that there exists an output code $\alpha \in \mathcal{D}^*$ with $\theta_n(\{0\} \times \mathbb{A}^n) = \{\alpha\}$. From $\{0\} \times \mathbb{A}^n \subset (\omega_n^* \circ \theta_n)^{-1}(\beta_n)$ we deduce $\omega_n^*(\alpha) = \beta_n$.

Let $\gamma_u : \mathbb{A}^1 \to \mathbb{A}^{m_n^*}$ and $\delta_u : \mathbb{A}^1 \to \mathbb{A}^{2^n}$ be the polynomial maps defined for $t \in \mathbb{A}^1$ by $\gamma_u(t) := \theta_n(t,u)$ and $\delta_u(t) := \omega_n^*\big(\theta_n(t,u)\big)$. We have $\gamma_u(0) := \alpha$, $\delta_u(0) = \beta_n$ and $\omega_n^* \circ \gamma_u = \delta_u$.

The following argumentation is exactly the same as in the proof of Proposition 2 of Section 4.2. First we deduce from (12) that

$$\big(L_1^{(n)}(u), \ldots, L_{2^n}^{(n)}(u)\big) = \delta_u'(0) = (D\omega_n^*)_\alpha\big(\gamma_u'(0)\big)$$

holds. Then we infer from Lemma 6 that there exist points $u_1, \ldots, u_{2^n} \in \mathbb{A}^n$ such that the $(2^n \times 2^n)$–matrix $\big(L_i^{(n)}(u_j)\big)_{1 \leq i,j \leq 2^n}$ is nonsingular. This implies that $\delta_{u_1}'(0), \ldots, \delta_{u_{2^n}}'(0)$ are linearly independent elements of the $\mathbb{C}$–vector space $\mathbb{A}^{2^n}$. Since $(D\,\omega_n^*)_\alpha : \mathbb{A}^{m_n^*} \to \mathbb{A}^{2^n}$ is a $\mathbb{C}$–linear map, we conclude that $\gamma_{u_1}'(0), \ldots, \gamma_{u_{2^n}}'(0)$ are linearly independent elements of the $\mathbb{C}$–linear space $\mathbb{A}^{m_n^*}$ and finally that $m_n^* \geq 2^n$ holds. ■

Suppose that there is given a procedure $\mathcal{P}$ which finds for suitable encodings of input and output objects the solution for each instance of any flat family of zero–dimensional elimination problems. Suppose furthermore that the procedure $\mathcal{P}$, applied to any flat family of zero–dimensional elimination problems produces a robust (e.g. black box) algorithm in the sense of Section 5.1 and that $\mathcal{P}$ can be applied to the encoding $\omega : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}_n$ of the input object class of the flat family of zero–dimensional elimination problems (11). Then Theorem 3 implies that $\mathcal{P}$ requires *exponential* sequential time on infinitely many inputs. On the other hand one sees easily that there do exist single exponential time procedures of this kind (see [GH01, Section 3.4] and the references cited there). Therefore the sequential time complexity of zero–dimensional (parametric) elimination performed by this kind of procedures is *intrinsically exponential*. Observe in particular that this conclusion is valid for suitable circuit encodings of input and output objects (see [HMPW98, Theorem 1] and [GH01, Theorem 2]).

The sparse encoding of the object class $\mathcal{O}_n$, defined by the polynomial $F_n = \sum_{i=1}^n 2^{i-1}X_i + T\prod_{i=1}^n \big(1 + (U_i - 1)X_i\big)$, is of size 3^n. Therefore, from the point of view of "classical" parametric (i.e. branching–free) elimination procedures (based on the sparse or dense encoding of polynomials by their coefficients), it is not surprising that the sequential time becomes exponential in n for the computation of the solution of the general problem instance (11), even if we change the data structure representing the output objects (see e.g. [GH93] and [KP94], [KP96] for this type of change of data structures).

Let us therefore look at the following flat family of zero–dimensional elimination problems $\widetilde{G}_1, \ldots, \widetilde{G}_{3n-1}, \widetilde{F} \in \mathbb{Q}[T, U_1, \ldots, U_n, X_1, \ldots, X_{3n-1}]$

in the parameters $T, U_1, \dots, U_n$ and the variables $X_1, \dots, X_{3n-1}$. This family contains only sparse polynomials of at most four monomial terms:

$$\begin{array}{rcl}
\widetilde{G}_1 & := & X_1^2 - X_1, \dots, \widetilde{G}_n := X_n^2 - X_n, \\[2ex]
\widetilde{G}_{n+1} & := & X_{n+1} - 2^1 X_2 - X_1, \\[2ex]
\widetilde{G}_{n+2} & := & X_{n+2} - X_{n+1} - 2^2 X_3, \\
& \vdots & \\
\widetilde{G}_{2n-1} & := & X_{2n-1} - X_{2n-2} - 2^{n-1} X_n \\[2ex]
\widetilde{G}_{2n} & := & X_{2n} - U_1 X_1 + X_1 - 1 = X_{2n} - \big(1 + (U_1 - 1)X_1\big), \\[2ex]
\widetilde{G}_{2n+1} & := & X_{2n+1} - U_2 X_{2n} X_2 + X_{2n} X_2 - X_{2n} \\
& = & X_{2n+1} - X_{2n}\big(1 + (U_2 - 1)X_2\big), \\
& \vdots & \\
\widetilde{G}_{3n-1} & := & X_{3n-1} - U_n X_{3n-2} X_n + X_{3n-2} X_n - X_{3n-2} \\
& = & X_{3n-1} - X_{3n-2}\big(1 + (U_n - 1)X_n\big) \\[2ex]
\widetilde{F}_n & := & X_{2n-1} + T X_{3n-1}.
\end{array}$$

One sees easily that the solution of the general problem instance $\widetilde{G}_1 = 0, \dots, \widetilde{G}_{3n-1} = 0, \widetilde{F}_n$ is again the polynomial $P_n \in \mathbb{Q}[T, U, Y]$ of Section 4.2. The polynomials $\widetilde{G}_1, \dots, \widetilde{G}_{3n-1}, \widetilde{F}_n$ determine, with the notations of Section 5.1, the input object class

$$\widetilde{\mathcal{O}}_n := \Big\{ \big(\widetilde{G}_1^{(t,u)}, \dots, \widetilde{G}_{3n-1}^{(t,u)}, \widetilde{F}_n^{(t,u)}\big); (t,u) \in \mathbb{A}^1 \times \mathbb{A}^n \Big\}$$

and the encoding $\widetilde{\omega}_n : \mathbb{A}^1 \times \mathbb{A}^n \to \widetilde{\mathcal{O}}_n$ which for $t \in \mathbb{A}^1$, $u \in \mathbb{A}^n$ is defined by $\widetilde{\omega}_n(t,u) := \big(\widetilde{G}_1^{(t,u)}, \dots, \widetilde{G}_{3n-1}^{(t,u)}, \widetilde{F}_n^{(t,u)}\big)$. Since these polynomials contain altogether exactly $9n-3$ monomials in the variables $X_1, \dots, X_{3n-1}$, we may consider the input object class $\widetilde{\mathcal{O}}_n$ as a $\mathbb{Q}$–constructible subset of the affine space $\mathbb{A}^{9n-3}$. With this interpretation, the encoding $\widetilde{\omega}_n : \mathbb{A}^1 \times \mathbb{A}^n \to \widetilde{\mathcal{O}}_n$ becomes $\mathbb{Q}$–definable and holomorphic. Applying to this situation the same argumentation as in the proof of Theorem 3 we conclude again that any branching– and totally division–free, robust elimination procedure, which finds from any input code $(t,u) \in \mathbb{A}^1 \times \mathbb{A}^n$ the code of the output object $P_n^{(t,u)}$ in a given data structure, requires an output data structure of size at least 2^n.

Let us turn back to the polynomial $F_n = \sum_{i=1}^n 2^{i-1} X_i + T \prod_{i=1}^n \big(1 + (U_i - 1)X_i\big)$ of (11), to the object class $\mathcal{O}_n := \big\{F_n^{(t,u)}; t \in \mathbb{A}^1, u := (u_1, \dots, u_n) \in \mathbb{A}^n\big\}$ defined by F_n and to its encoding $\omega_n := \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}_n$. Since the polynomial F_n contains in the variables $X_1, \dots, X_n$ exactly 2^n nonzero monomial terms we may consider $\mathcal{O}_n$ as a $\mathbb{Q}$–constructible subset of the affine space $\mathbb{A}^{2^n}$ and $\omega_n := \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}_n$ as $\mathbb{Q}$–definable, holomorphic encoding of the object class $\mathcal{O}_n$. One sees easily that $\mathcal{O}_n$ is a closed, irreducible and $\mathbb{Q}$–definable subvariety of $\mathbb{A}^{2^n}$ and that ω_n induces a robust encoding of the object class $\mathcal{O}_n \setminus \{\sum_{i=1}^n 2^{i-1}X_i\}$ by the data structure $\mathbb{A}^1 \times \mathbb{A}^n \setminus \big(\{0\} \times \mathbb{A}^n\big)$. On the other hand $\{0\} \times \mathbb{A}^n$ is an exceptional fiber of the morphism of algebraic varieties $\omega_n : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}_n$. Therefore the encoding ω_n of the object class $\mathcal{O}_n$ is not robust. On the other hand, by similar arguments as in Section 4.2, we may show that any *robust* encoding of $\mathcal{O}_n$ has size at least 2^n. Therefore Theorem 3 says only that any branching– and totally division–free *robust* elimination procedure necessarily transfers a certain obstruction hidden in the given encoding of the input object F_n to the encoding of the output object P_n.

However, Theorem 3 does *not* say that the process of elimination creates a *genuine* complexity problem for the encoding of the output object. In particular we are not able to deduce from Theorem 3 that the sequence of polynomials $(P_n)_{n\in\mathbb{N}}$ is hard to evaluate. In fact, for $n \in \mathbb{N}$ the polynomial P_n admits a short, $\mathbb{Q}$–definable, holomorphic encoding by the data structure $\mathbb{A}^1 \times \mathbb{A}^n$ and the sequence of polynomials $(P_n)_{n\in\mathbb{N}}$ may in principle be easy to evaluate. However, in the latter case, no branching– and totally division–free, robust elimination procedure will be able to discover this fact.

5.4 The hardness of universal elimination.

In this section we are going to show the second main result of this paper, namely Theorem 4 below, which says that there exists no universal polynomial sequential time elimination algorithm $\mathcal{P}$ satisfying the following condition:

$\mathcal{P}$ is able to compute equations for the Zariski closure of any given constructible set and the generically square–free parametric greatest common divisor of any given algebraic family of univariate polynomials (see Sections 2.2 and 5.1 for the computational model).

The following considerations are devoted to the precise statement and the proof of Theorem 4 below.

Let us suppose again $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$. Let n be a fixed natural number, let $m(n) := 4n + 10$ and let $T, U_1, \ldots, U_n, X_1, \ldots, X_n$ and $S_1, \ldots, S_{m(n)}, Y$ be indeterminates over $\mathbb{Q}$. Let $U := (U_1, \ldots, U_n)$, $X := (X_1, \ldots, X_n)$, $S := (S_1, \ldots, S_{m(n)})$ and let

$$R_n := Z\left(\sum_{i=1}^{n} 2^{i-1}X_i + T\prod_{i=1}^{n}\big(1 + (U_i - 1)X_i\big)\right) \in \mathbb{Q}[Z, T, U, X].$$

One sees easily that the polynomial R_n may be evaluated by a totally division–free arithmetic circuit of size $O(n)$.

Let $\widehat{\mathcal{O}}_n$ be the Zariski closure of the set

$$\Bigg\{ R_n^{(z,t,u)}; (z,t) \in \mathbb{A}^2, u = (u_1, \dots, u_n) \in \mathbb{A}^n,$$

$$R_n^{(z,t,u)} := z \left(\sum_{i=1}^{n} 2^{i-1} X_i + t \prod_{i=1}^{n} \big(1 + (u_i - 1) X_i\big) \right) \Bigg\}$$

in a suitable finite dimensional $\mathbb{C}$–linear subspace of $\mathbb{C}[X]$ and let $\gamma_n := (\gamma_1^{(n)}, \dots, \gamma_{m(n)}^{(n)}) \in \mathbb{Z}^{m(n)\times n}$ be an identification sequence for $\widehat{\mathcal{O}}_n$. From Corollary 1 we deduce that such an identification sequence exists and that we may assume without loss of generality that the absolute values of the entries of the $\big(m(n) \times n\big)$–matrix γ_n are bounded by $3n^3$. Observe that $\widehat{\mathcal{O}}_n$ is a $\mathbb{Q}$–definable, irreducible, closed cone of dimension at most $n+2$. We shall consider $\widehat{\mathcal{O}}_n$ as object class of n–variate polynomial functions.

Let us now consider the following prenex existential formula $\Phi_n(S, Y)$ in the free variables $S_1, \dots, S_{m(n)}, Y$ and the bounded variables $X_1, \dots, X_n, Z, T, U_1, \dots, U_n$:

$$\begin{aligned}
&(\exists X_1) \cdots (\exists X_n)(\exists Z)(\exists T)(\exists U_1) \cdots (\exists U_n) \\
&\qquad \Big(\bigwedge_{i=1}^{n} X_i^2 - X_i = 0 \ \wedge \bigwedge_{k=1}^{m(n)} S_k = R_n(Z, T, U_1, \dots, U_n, \gamma_k^{(n)}) \ \wedge \\
&\qquad\qquad\qquad\qquad \wedge\ Y = R_n(Z, T, U_1, \dots, U_n, X_1, \dots, X_n) \Big).
\end{aligned}$$

Using the previously mentioned arithmetic circuit encoding of the polynomial R_n and the bit encoding for integers, we see that the length $|\Phi_n|$ of the formula $\Phi_n(S, Y)$ is $O(n^2)$.

Observe that the quantifier free formula

$$Y = R_n(Z, T, U_1, \dots, U_n, X_1, \dots, X_n)$$

is equivalent to the following formula

$$\Pi_n(Z, T, U_1, \dots, U_n, X_1, \dots, X_n, Y)$$

in the free variables $Z, T, U_1, \dots, U_n, X_1, \dots, X_n, Y$ and the bounded variables $X_{n+1}, \dots, X_{3n-1}$, i.e. both formulas define the same subset of $\mathbb{A}^{2n+2}$ (compare Section 5.3):

$$
\begin{aligned}
&(\exists X_{n+1})\cdots(\exists X_{3n-1})\Big(X_{n+1}-2X_2-X_1=0\ \wedge\\
&\wedge \bigwedge_{j=n+2}^{2n-1} X_j-X_{j-1}-2^{j-n}X_{j-n+1}=0\ \wedge X_{2n}-U_1X_1+X_1-1=0\ \wedge\\
&\ \wedge \bigwedge_{k=2n+1}^{3n-1} X_k-U_{k-2n+1}X_{k-1}X_{k-2n+1}+X_{k-1}X_{k-2n+1}-X_{k-1}=0\ \wedge\\
&\qquad\qquad\qquad\qquad\qquad\qquad\wedge\ Y=ZX_{2n-1}+ZTX_{3n-1}\Big).
\end{aligned}
$$

Replacing now in the formula $\Phi_n(S,Y)$ for $1\le k\le m(n)$ the occurrencies of the subformulas $S_k=R_n(Z,T,U_1,\dots,U_n,\gamma_k^{(n)})$ by $\Pi_n(Z,T,U,\gamma_k^{(n)}, S_k)$ and the occurrency of $Y = R_n(Z,T,U_1,\dots,U_n,X_1,\dots,X_n)$ by $\Pi_n(Z,T,U,X,Y)$, we obtain another prenex existential formula $\widetilde{\Phi}_n(S,Y)$ in the free variables $S_1,\dots,S_{m(n)},Y$ and $8n^2+20n-9$ bounded variables. The formula $\widetilde{\Phi}_n(S,Y)$ has length $|\widetilde{\Phi}_n|=O(n^2)$ for the sparse encoding of polynomials and the bit representation of integers. Observe that the formulas $\Phi_n(S,Y)$ and $\widetilde{\Phi}_n(S,Y)$ are equivalent and asymptotically of the same length $O(n^2)$. Thus the formulas Φ_n and $\widetilde{\Phi}_n$ are logical expressions of asymptotically the same length which describe the same constructible subset of the affine space $\mathbb{A}^{m(n)}\times\mathbb{A}^1$. The polynomials occurring in $\Phi_n(X,Y)$ are given in arithmetic circuit encoding, whereas the polynomials occurring in $\widetilde{\Phi}_n(X,Y)$ are given in sparse encoding. The formulas $\Phi_n(X,Y)$ and $\widetilde{\Phi}_n(X,Y)$ will be the inputs for an elimination problem which we are now going to describe in detail.

In the sequel we shall restrict our attention to the formula $\Phi_n(S,Y)$. Our considerations will be identically valid for the formula $\widetilde{\Phi}_n(S,Y)$.

Let $\widehat{\sigma}_n:\widehat{\mathcal{O}}_n\to\mathbb{A}^{m(n)}$ be the map defined for $R\in\widehat{\mathcal{O}}_n$ by $\widehat{\sigma}_n(R):=\big(R(\gamma_1^{(n)}),\dots,R(\gamma_{m(n)}^{(n)})\big)$ and let $\widehat{\mathcal{D}}_n$ be the image of $\widehat{\sigma}_n$. From Lemma 5 we deduce that $\widehat{\mathcal{D}}_n$ is a $\mathbb{Q}$–definable, irreducible, closed cone of $\mathbb{A}^{m(n)}$ and that $\widehat{\sigma}_n$ induces a finite, bijective morphism of algebraic varieties $\widehat{\sigma}_n:\widehat{\mathcal{O}}_n\to\widehat{\mathcal{D}}_n$ which is therefore a homeomorphism with respect to the Zariski topologies of $\widehat{\mathcal{O}}_n$ and $\widehat{\mathcal{D}}_n$. In particular $\widehat{\sigma}_n:\widehat{\mathcal{O}}_n\to\widehat{\mathcal{D}}_n$ is a homogeneous, birational map. We consider $\widehat{\mathcal{D}}_n$ as a $\mathbb{Q}$–definable data structure and $(\widehat{\sigma}_n)^{-1}:\widehat{\mathcal{D}}_n\to\widehat{\mathcal{O}}_n$ as a $\mathbb{Q}$–definable, continuous encoding of the object class $\widehat{\mathcal{O}}_n$. From a similar argument as in the proof of Proposition 2 we deduce that $\widehat{\sigma}_n:\widehat{\mathcal{O}}_n\to\widehat{\mathcal{D}}_n$ is not an isomorphism of affine varieties. Thus $\widehat{\sigma}_n^{-1}:\widehat{\mathcal{D}}_n\to\widehat{\mathcal{O}}_n$ is not a *holomorphic* encoding of the object class $\widehat{\mathcal{O}}_n$ by the data structure $\widehat{\mathcal{D}}_n$, but only a *continuous* one (compare Theorem 1). This circumstance contributes to a certain technical intricateness of the argumentation which now follows.

Observe first that the prenex existential formula $(\exists Y)\Phi_n(S,Y)$ describes a $\mathbb{Q}$–constructible subset of $\mathbb{A}^{m(n)}$ whose Zariski closure is $\widehat{\mathcal{D}}_n$. Observe then that $dim\,\widehat{\mathcal{D}}_n \leq dim\,\widehat{\mathcal{O}}_n \leq n+2 < 4n+10 = m(n)$ holds. Therefore $\widehat{\mathcal{D}}_n$ is strictly contained in the affine space $\mathbb{A}^{m(n)}$. Thus the formula $\Phi_n(S,Y)$ introduces an implicit semantical dependence between the indeterminates $S_1,\dots,S_{m(n)}$. In the sequel we shall consider the indeterminates $S_1,\dots,S_{m(n)}$ as parameters and Y as variable.

Let us now consider an arbitrary point $s=(s_1,\dots,s_{m(n)}) \in \mathbb{A}^{m(n)}$ which satisfies the formula $(\exists Y)\Phi_n(S,Y)$. Then there exist points $(z,t)\in\mathbb{A}^2$ and $u=(u_1,\dots,u_n)\in\mathbb{A}^n$ such that the n–variate polynomial

$$R_n^{(z,t,u)} = z\left(\sum_{i=1}^{n} 2^{i-1}X_i + t\prod_{i=1}^{n}(1+(u_i-1)X_i)\right)$$

satisfies the condition

$$s_1 = R_n^{(z,t,u)}(\gamma_1^{(n)}),\dots,s_{m(n)} = R_n^{(z,t,u)}(\gamma_{m(n)}^{(n)}).$$

Since $\gamma_n = (\gamma_1^{(n)},\dots,\gamma_{m(n)}^{(n)}) \in \mathbb{Z}^{m(n)\times n}$ is an identification sequence for the object class $\mathcal{O}_n$, we conclude that the polynomial $R_n^{(z,t,u)} \in \mathbb{C}[X_1,\dots,X_n]$ depends only on the point $s\in\mathbb{A}^{m(n)}$ and not on its particular encoding (z,t,u) belonging to the data structure $\mathbb{A}^2\times\mathbb{A}^n$. We write therefore $R_n^{(s)} := R_n^{(z,t,u)}$. Let

$$\widehat{P}_n^{(s)} := \prod_{(\varepsilon_1,\dots,\varepsilon_n)\in\{0,1\}^n}\Big(Y - R_n^{(s)}(\varepsilon_1,\dots,\varepsilon_n)\Big)$$

and let us write $\Phi_n(s,Y)$ for the formula of the elementary language of algebraically closed fields of characteristic zero with constants in $\mathbb{C}$ which is obtained by specializing in the formula $\Phi_n(S,Y)$ the variables $S_1,\dots,S_{m(n)}$ into the values $s_1,\dots,s_{m(n)}\in\mathbb{C}$. Observe that the polynomial $\widehat{P}_n^{(s)}$ is monic of degree 2^n and $\Phi_n(s,Y)$ contains a single free variable, namely Y. One sees easily that the formula $\Phi_n(s,Y)$ is equivalent to the quantifier–free formula $\widehat{P}_n^{(s)}(Y)=0$.

Observe that for a suitable point $s=(s_1,\dots,s_{m(n)})$ of $\mathbb{A}^{m(n)}$ satisfying the formula $(\exists Y)\Phi_n(S,Y)$ (e.g. choosing s such that for $f_n := \sum_{i=1}^n 2^{i-1}X_i$ the condition $s_1 = f_n(\gamma_1^{(n)}),\dots,s_{m(n)} = f_n(\gamma_{m(n)}^{(n)})$ is satisfied) we obtain a univariate *separable* polynomial $\widehat{P}_n^{(s)}$ of degree 2^n. This implies that there exists a nonempty Zariski open subset $\mathcal{U}$ of the closed, $\mathbb{Q}$–definable, irreducible subvariety $\widehat{\mathcal{D}}_n$ of the affine space $\mathbb{A}^{m(n)}$ such that $\mathcal{U}$ is contained in the $\mathbb{Q}$–constructible subset of $\mathbb{A}^{m(n)}$ defined by the formula $(\exists Y)\Phi_n(S,Y)$ and such that for any point $s\in\mathcal{U}$ the polynomial $\widehat{P}_n^{(s)}\in\mathbb{C}[Y]$ is monic and separable of degree 2^n. Since the $\mathbb{Q}$–definable morphism $\widehat{\sigma}_n : \widehat{\mathcal{O}}_n \to \widehat{\mathcal{D}}_n$ is finite, bijective and birational, there exists a polynomial $\widehat{R}_n \in \mathbb{Q}(\widehat{\mathcal{D}}_n)[X]$ satisfying the following two conditions:

- for any point $s \in \widehat{\mathcal{D}}_n$, any coefficient ρ of $\widehat{R}_n$ and any place $\varphi : \mathbb{C}(\widehat{\mathcal{D}}_n) \to \mathbb{C} \cup \{\infty\}$ whose valuation ring contains the local ring of $\widehat{\mathcal{D}}_n$ at the point s, the value $\varphi(\rho)$ is finite and uniquely determined by s.
- if additionally the point s satisfies the formula $(\exists Y)\Phi_n(S,Y)$, then the polynomial $\varphi(\widehat{R}_n) \in \mathbb{C}[X]$, obtained by specializing the coefficients of $\widehat{R}_n$ by means of the place φ, satisfies the equation $\varphi(\widehat{R}_n) = R_n^{(s)}$.

With these notations, we shall write $R_n^{(s)} := \varphi(\widehat{R}_n)$ also if s does not satisfy the formula $(\exists Y)\Phi_n(S,Y)$. Let

$$\widehat{P}_n := \prod_{(\varepsilon_1,\dots,\varepsilon_n)\in\{0,1\}^n} \Big(Y - \widehat{R}_n(\varepsilon_1,\dots,\varepsilon_n)\Big) \in \mathbb{Q}(\widehat{\mathcal{D}}_n)[Y].$$

One sees easily that $\widehat{P}_n$ satisfies mutatis mutandis the above two conditions (note that in the second condition $\varphi(\widehat{R}_n) = R_n^{(s)}$ has to be replaced by $\varphi(\widehat{P}_n) = P_n^{(s)}$).

In particular the coefficients of $\widehat{P}_n$ belong to the integral closure of the domain $\mathbb{Q}[\widehat{\mathcal{D}}_n]$ in its function field $\mathbb{Q}(\widehat{\mathcal{D}}_n)$.

Since for any $s \in \mathcal{U}$ the polynomial $\widehat{P}_n^{(s)}$ is separable of degree 2^n, we conclude that $\widehat{P}_n$ is a monic, separable polynomial of degree 2^n in the variable Y.

Let us denote by V_n the Zariski closure of the $\mathbb{Q}$–constructible subset of $\mathbb{A}^{m(n)} \times \mathbb{A}^1$ defined by the formula $\Phi_n(S,Y)$ and by $\pi_n : \mathbb{A}^{m(n)} \times \mathbb{A}^1 \to \mathbb{A}^{m(n)}$ the canonical projection which maps each point of $\mathbb{A}^{m(n)} \times \mathbb{A}^1$ on its first $m(n)$ coordinates. Observe that V_n is nonempty and that the $\mathbb{Q}$–definable, irreducible variety $\widehat{\mathcal{D}}_n$ is the Zariski closure of $\pi_n(V_n)$ in $\mathbb{A}^{m(n)}$. Let C be any irreducible component of V_n satisfying the condition $\overline{\pi_n(C)} = \widehat{\mathcal{D}}_n$ (observe that such an irreducible component exists). Let us now fix a point $s \in \widehat{\mathcal{D}}_n$ which we think chosen generically between the points of $\widehat{\mathcal{D}}_n$. From this choice we infer immediately that the set $\pi_n^{-1}(s) \cap C$ is not empty and that its elements satisfy the formula $\Phi_n(S,Y)$. One now sees easily that $\pi_n^{-1}(s) \cap C$ is a nonempty and finite set. This implies $dim\, C = dim\, \widehat{\mathcal{D}}_n$.

Observe that for any point $s \in \mathbb{A}^{m(n)}$ satisfying $(\exists Y)\Phi_n(S,Y)$, the formula $\Phi_n(s,Y)$ is equivalent to the quantifier free formula $\widehat{P}_n^{(s)}(Y) = 0$.

Therefore we shall consider from now on $\widehat{P}_n$ as the canonical output object associated to the elimination problem given by the formula $\Phi_n(S,Y)$ in the parameters $S_1,\dots,S_{m(n)}$ and the single variable Y. More precisely, our elimination task will consists in the computation of the polynomial $\widehat{P}_n^{(s)} \in \mathbb{C}[Y]$ for any input instance $s \in \widehat{\mathcal{D}}_n$. In this sense, we are looking for output data structures which solve problem (ii) of Section 1.2 for the object class defined by the polynomial $\widehat{P}_n$ in the parameter instances defined by the formula $(\exists Y)\Phi_n(S, Y)$.

Suppose now that there is given an elimination procedure $\mathcal{P}$ which is universal and branching–parsimonious in the sense of Section 1.2. Suppose furthermore that $\mathcal{P}$ accepts as inputs prenex existential input formulas of the elementary theory of algebraically closed fields of characteristic zero, whose terms are polynomials in arithmetic circuit representation (or alternatively polynomials in sparse representation). Assume that $\mathcal{P}$ is associated with a suitable output data structure which allows the holomorphic encoding of polynomials and with a monotone sequential time measure $\mathcal{T}$, and suppose that $\mathcal{P}$ and $\mathcal{T}$ satisfy the following conditions:

(1) Let Φ be a given prenex existential formula of the elementary language $\mathcal{L}$ of algebraically closed fields of characteristic zero with constants 0, 1. Suppose that the polynomial terms occurring in the formula Φ are encoded by the *input data structure* associated with the elimination procedure $\mathcal{P}$. Then the elimination procedure $\mathcal{P}$ produces a quantifier–free formula Ψ whose polynomial terms are (holomorphically) encoded by the output data structure associated with $\mathcal{P}$, such that Φ and Ψ are equivalent formulas. The length $|\Psi|$ of the output formula Ψ satisfies the estimate $|\Psi| \leq \mathcal{T}(|\Phi|)$.

(2) Let $\Xi \in \mathcal{L}$ be a quantifier–free formula whose polynomial terms are encoded by the *output data structure* associated with $\mathcal{P}$. Then the procedure $\mathcal{P}$ produces from the input Ξ a system of polynomial equations $\mathcal{F}$, encoded by the output data structure associated with $\mathcal{P}$, such that $\mathcal{F}$ defines the Zariski closure of the $\mathbb{Q}$–constructible set defined by Ξ. The size $|\mathcal{F}|$ of the system of polynomial equations $\mathcal{F}$ satisfies the estimate $|\mathcal{F}| \leq \mathcal{T}(|\Xi|)$.

(3) Let $\mathcal{B}$ be a system of polynomials encoded by the *output data structure* associated with the elimination procedure $\mathcal{P}$. Suppose that $\mathcal{B}$ represents an algebraic family of univariate polynomials, for which a generically square–free parametric greatest common divisor $\widehat{h}$ in the sense of Section 2 exists. Then the procedure $\mathcal{P}$ produces from the input $\mathcal{B}$ an algorithm in the sense of Section 5.2 which computes for any admissible input instance of $\mathcal{B}$ the generically square–free greatest common divisor $\widehat{h}$ of the algebraic family of univariate polynomials represented by $\mathcal{B}$. Here we assume implicitly that $\widehat{h}$ is represented by a polynomial H which is encoded by the output data structure associated with the procedure $\mathcal{P}$. With respect to this data structure the size $|H|$ of the polynomial H satisfies the estimate $|H| \leq \mathcal{T}(|\mathcal{B}|)$.

Let us remark that condition (1) above characterizes $\mathcal{P}$ as a universal elimination procedure in the usual sense, whereas conditions (2) and (3) state that $\mathcal{P}$ solves suitable elimination problems of type (*ii*) of Section 1.2. In principle, input and output formulas mentioned in condition (1) may be represented by algorithms which admit branchings. If for example $\mathcal{P}$ uses as input and output data structures for the encoding of polynomials arithmetic circuits, quantifier–free (sub–)formulas in condition (1) may be represented by arithmetic networks (arithmetic–boolean circuits, see [vzG86], [vzG93]). Nevertheless we require that the outputs mentioned in conditions (2) and (3) represent branching–free evaluation procedures. All known universal elimination procedures satisfy with respect to a suitably defined sequential time complexity measure conditions (1), (2), (3) above.

Let us now apply the given elimination procedure $\mathcal{P}$ to the input formula $\Phi_n(S,Y)$. Since $\mathcal{P}$ satisfies condition (1), the output is a quantifier–free formula $\Psi_n(S,Y)$ of the elementary language $\mathcal{L}$, such that $\Psi_n(S,Y)$ is equivalent to $\Phi_n(S,Y)$. Moreover, the polynomial terms occurring in the formula $\Psi(S,Y)$ are represented by the output data structure associated with $\mathcal{P}$.

We apply now the procedure $\mathcal{P}$ to the quantifier–free formula $\Psi_n(S,Y)$. Since $\mathcal{P}$ satisfies condition (2), the output is a finite set $\mathcal{B}_n$ of polynomials of $\mathbb{Q}[S,Y]$ which define the algebraic variety V_n. Again, the polynomials contained in $\mathcal{B}_n$ are represented by the output data structure associated with $\mathcal{P}$.

Recall that V_n is the Zariski closure of the $\mathbb{Q}$–constructible subset of $\mathbb{A}^{m(n)} \times \mathbb{A}^1$ defined by the formula $\Phi_n(S,Y)$ (and hence by the formula $\Psi_n(S,Y)$), that V_n is nonempty, that $\widehat{\mathcal{D}}_n$ is the Zariski closure of the image of V_n under the canonical projection $\pi_n : \mathbb{A}^{m(n)} \times \mathbb{A}^1 \to \mathbb{A}^{m(n)}$ and that any irreducible component C of V_n with $\overline{\pi_n(C)} = \widehat{\mathcal{D}}_n$ satisfies the condition $dim\, C = dim\, \widehat{\mathcal{D}}_n$. Let $B_1^{(n)}, \ldots, B_{q_n}^{(n)}$ be the elements of $\mathcal{B}_n$ which do not vanish identically on the algebraic variety $\widehat{\mathcal{D}}_n \times \mathbb{A}^1$. Let $b_1^{(n)}, \ldots, b_{q_n}^{(n)}$ be the univariate polynomials of $\mathbb{Q}[\widehat{\mathcal{D}}_n][Y]$ induced by $B_1^{(n)}, \ldots, B_{q_n}^{(n)}$ on $\widehat{\mathcal{D}}_n \times \mathbb{A}^1$. Observe that $b_1^{(n)} \neq 0, \ldots, b_{q_n}^{(n)} \neq 0$ holds. Since any irreducible component C of V_n with $\overline{\pi_n(C)} = \widehat{\mathcal{D}}_n$ satisfies the condition $dim\, C = dim\, \widehat{\mathcal{D}}_n$ and since such an irreducible component exists, we conclude $q_n \geq 1$. Therefore $b_1^{(n)}, \ldots, b_{q_n}^{(n)}$ is an algebraic family of univariate polynomials in the sense of Section 5.2.

Let $h \in \mathbb{Q}(\widehat{\mathcal{D}}_n)[Y]$ be the greatest common divisor of the polynomials $b_1^{(n)}, \ldots, b_{q_n}^{(n)}$ in $\mathbb{Q}(\widehat{\mathcal{D}}_n)[Y]$. Since for any point $s \in \mathcal{U}$ the formula $\Phi_n(s,Y)$ (and hence the formula $\Psi_n(s,Y)$) is equivalent to the formula $\widehat{P}_n^{(s)}(Y) = 0$ and since $\mathcal{U}$ is a nonempty Zariski open subset of $\widehat{\mathcal{D}}_n$, we conclude that the monic polynomials h and $\widehat{P}_n$ of $\mathbb{Q}(\widehat{\mathcal{D}}_n)[Y]$ have the same roots in any algebraic closure of the field $\mathbb{Q}(\widehat{\mathcal{D}}_n)$.

Therefore we have $\deg h \geq \deg \widehat{P}_n = 2^n$. Thus the degree of h in the variable Y is positive.

Since the univariate polynomial $\widehat{P}_n$ is separable, we conclude, from our previous considerations concerning the definition of $P_n^{(s)}$ for arbitrary $s \in \widehat{\mathcal{D}}_n$, that there exists a generically square–free greatest common divisor for the algebraic family of univariate polynomials $b_1^{(n)}, \ldots, b_{q_n}^{(n)}$ and that this greatest common divisor is $\widehat{P}_n$.

Finally we apply the procedure $\mathcal{P}$ to the finite set of polynomials $\mathcal{B}_n$. Since $\mathcal{P}$ satisfies condition (3), the output are rational functions $\widehat{\theta}_1^{(n)}, \ldots, \widehat{\theta}_{\widehat{m}_n}^{(n)}$ of $\mathbb{Q}(\widehat{\mathcal{D}}_n)$, such that $\widehat{\theta}_n := (\widehat{\theta}_1^{(n)}, \ldots, \widehat{\theta}_{\widehat{m}_n}^{(n)})$ represents an algorithm in the sense of Section 2.2 which computes the generically square–free parametric greatest common divisor $\widehat{P}_n$ of the algebraic family of univariate polynomials $b_1^{(n)}, \ldots, b_{q_n}^{(n)}$ for any admissible input instance (which necessarily belongs to $\widehat{\mathcal{D}}_n$). Let us make this statement more precise:

let $\mathcal{D}_n^*$ be the $\mathbb{Q}$–constructible output data structure associated with the procedure $\mathcal{P}$, when $\mathcal{P}$ is applied to the input $\mathcal{B}_n$. Then the size of $\mathcal{D}_n^*$ is $\widehat{m}_n$ and we may suppose without loss of generality that $\mathcal{D}_n^*$ is a closed subvariety of the affine space $\mathbb{A}^{\widehat{m}_n}$. Then the closure of the image of $\widehat{\theta}_n$ is contained in $\mathcal{D}_n^*$ and therefore we may interpret $\widehat{\theta}_n$ as a dominant rational map from $\widehat{\mathcal{D}}_n$ to $\mathcal{D}_n^*$.

The output data structure $\mathcal{D}_n^*$ encodes a suitable output object class $\mathcal{O}_n^*$ of univariate polynomials by means of a $\mathbb{Q}$–definable, holomorphic encoding $\omega_n^* : \mathcal{D}_n^* \to \mathcal{O}_n^*$. The object class $\mathcal{O}_n^*$ contains the set $\{\widehat{P}_n^{(s)}; s \in \widehat{\mathcal{D}}_n\}$. Since $\widehat{\theta}_n$ is a dominant rational map, the composition $\omega_n^* \circ \widehat{\theta}_n$ is well defined and $\omega_n^* \circ \widehat{\theta}_n$ is a rational map from $\widehat{\mathcal{D}}_n$ to the Zariski closure of the object class $\mathcal{O}_n^*$ in a suitable affine ambient space. By assumption the algorithm $\widehat{\theta}_n$ computes the generically square–free parametric greatest common divisor $\widehat{P}_n \in \mathbb{Q}(\mathcal{D}_n)[Y]$ of the algebraic family of univariate polynomials $b_1^{(n)}, \ldots, b_{q_n}^{(n)}$ for any admissible input instance. Thus for any input instance $s \in \widehat{\mathcal{D}}_n$ and any place $\varphi : \mathbb{C}(\widehat{\mathcal{D}}_n) \to \mathbb{C} \cup \{\infty\}$ whose valuation ring contains the local ring of $\widehat{\mathcal{D}}_n$ at s, the values $\varphi(\widehat{\theta}_1^{(n)}), \ldots, \varphi(\widehat{\theta}_{\widehat{m}_n}^{(n)})$ are finite and uniquely determined by the input instance s. With these notations we may therefore consistently write $\widehat{\theta}_1^{(n)}(s) := \varphi(\widehat{\theta}_1^{(n)}), \ldots, \widehat{\theta}_{\widehat{m}_n}^{(n)}(s) := \varphi(\widehat{\theta}_{\widehat{m}_n}^{(n)})$ and $\widehat{\theta}_n(s) := (\widehat{\theta}_1^{(n)}(s), \ldots, \widehat{\theta}_{\widehat{m}_n}^{(n)}(s))$. Since $\mathcal{D}_n^*$ is a closed subvariety of $\mathbb{A}^{\widehat{m}_n}$ we have $\widehat{\theta}_n(s) \in \mathcal{D}_n^*$ for any $s \in \widehat{\mathcal{D}}_n$. We may therefore interpret $\widehat{\theta}_n$ as a *total* map from $\widehat{\mathcal{D}}_n$ to $\mathcal{D}_n^*$ whose value is defined for *any* argument from $\widehat{\mathcal{D}}_n$. With this interpretation $\omega_n^* \circ \widehat{\theta}_n$ is a total map from $\widehat{\mathcal{D}}_n$ to $\mathcal{O}_n^*$ satisfying the condition $\omega_n^* \circ \widehat{\theta}_n(s) = \omega_n^*\big(\widehat{\theta}_n(s)\big) = \widehat{P}_n^{(s)}$ for any $s \in \widehat{\mathcal{D}}_n$.

The above considerations imply that the rational functions $\widehat{\theta}_1^{(n)}, \ldots, \widehat{\theta}_{\widehat{m}_n}^{(n)}$ belong to the integral closure of the domain $\mathbb{Q}[\widehat{\mathcal{D}}_n]$ in its fraction field $\mathbb{Q}(\widehat{\mathcal{D}}_n)$.

Moreover they imply that the rational function $\widehat{\theta}_n$, which we may suppose well–defined for the Zariski open subset $\mathcal{U}$ of $\widehat{\mathcal{D}}_n$, represents an essentially division–free algorithm in the sense Section 5.2 which computes for each input instance $s \in \mathcal{U}$ a code $\widehat{\theta}_n(s)$ for the output object $\widehat{P}_n^{(s)}$ and which can be uniquely extended to the limit data structure $\widehat{\mathcal{D}}_n$ of $\mathcal{U}$.

Observe now, that specializing in the polynomial

$$R_n = Z\left(\sum_{i=1}^{n} 2^{i-1}X_i + T\prod_{i=1}^{n}\big(1+(U_i-1)X_i\big)\right) \in \mathbb{Q}[Z,T,U,X]$$

the variable Z into the value one, we obtain the polynomial

$$F_n = \sum_{i=1}^{n} 2^{i-1}X_i + T\prod_{i=1}^{n}\big(1+(U_i-1)X_i\big) \in \mathbb{Q}[T,U,X]$$

introduced in Section 5.3. Therefore the object class $\mathcal{O}_n := \{F_n^{(t,u)}; t \in \mathbb{A}^1, u \in \mathbb{A}^n\}$ is contained in the object class $\widehat{\mathcal{O}}_n$. Since $\widehat{\mathcal{O}}_n$ is Zariski closed in its ambient space we have $\overline{\mathcal{O}}_n \subset \widehat{\mathcal{O}}_n$. Let $\mathcal{D}_n := \widehat{\sigma}_n(\overline{\mathcal{O}}_n)$. Since $\overline{\mathcal{O}}_n$ is a $\mathbb{Q}$–definable, closed, irreducible subvariety of $\widehat{\mathcal{O}}_n$ and $\widehat{\sigma}_n : \widehat{\mathcal{O}}_n \to \widehat{\mathcal{D}}_n$ is a $\mathbb{Q}$–definable, finite, bijective morphism of algebraic varieties, we conclude that $\mathcal{D}_n$ is a (nonempty) $\mathbb{Q}$–definable, closed, irreducible subvariety of $\widehat{\mathcal{D}}_n$. For any point $s \in \mathcal{D}_n$ and any place $\varphi : \mathbb{C}(\widehat{\mathcal{D}}_n) \to \mathbb{C} \cup \{\infty\}$ whose valuation ring contains the local ring of $\widehat{\mathcal{D}}_n$ at s, and any coefficient β of $\widehat{P}_n \in \mathbb{Q}(\widehat{\mathcal{D}}_n)[Y]$, the values of $\varphi(\beta)$ and of $\varphi(\widehat{\theta}_1^{(n)}), \dots, \varphi(\widehat{\theta}_{\widehat{m}_n}^{(n)})$ are finite and *uniquely* determined by s. Therefore there exists a monic polynomial $\check{P}_n \in \mathbb{Q}(\mathcal{D}_n)[Y]$ of degree 2^n, rational functions $\check{\theta}_1^{(n)}, \dots, \check{\theta}_{\widehat{m}_n}^{(n)}$ and a nonempty Zariski open subset $\mathcal{U}_0$ of $\mathcal{D}_n$ such that $\check{P}_n$ and $\check{\theta}_n := (\check{\theta}_1^{(n)}, \dots, \check{\theta}_{\widehat{m}_n}^{(n)})$ are well defined in any point s of $\mathcal{U}_0$ and such that the conditions $\check{P}_n^{(s)} = \widehat{P}_n^{(s)}$ and $\check{\theta}_n^{(s)} = \widehat{\theta}_n^{(s)}$ are satisfied.

Since $\mathbb{Q}[\mathcal{D}_n]$ is a holomorphic image of $\mathbb{Q}[\widehat{\mathcal{D}}_n]$ and since the coefficients of $\widehat{P}_n$ and $\widehat{\theta}_1^{(n)}, \dots, \widehat{\theta}_{\widehat{m}_n}^{(n)}$ belong to the integral closure of $\mathbb{Q}[\widehat{\mathcal{D}}_n]$ in $\mathbb{Q}(\widehat{\mathcal{D}}_n)$, we conclude that $\check{\theta}_1^{(n)}, \dots, \check{\theta}_{\widehat{m}_n}^{(n)}$ and the coefficients of $\check{P}_n$ belong to the integral closure of the domain $\mathbb{Q}[\mathcal{D}_n]$ in its fraction field $\mathbb{Q}(\mathcal{D}_n)$. In the same way one sees that $\check{\theta}_n$ represents an essentially division–free algorithm which computes the polynomial $\check{P}_n$ and which can be uniquely extended to the limit data structure $\mathcal{D}_n$ of $\mathcal{U}_0$. For any $s \in \mathcal{D}_n$ we infer therefore that $\check{\theta}_n(s) := (\check{\theta}_1^{(n)}, \dots, \check{\theta}_{\widehat{m}_n}^{(n)})$ is a well defined point of $\mathcal{D}_n^*$ and that $\check{P}_n^{(s)}$ is a well defined, monic, univariate polynomial of degree 2^n satisfying the conditions $\check{\theta}_n(s) = \widehat{\theta}_n(s)$ and $\check{P}_n^{(s)} = \widehat{P}_n^{(s)}$.

Consider now the $\mathbb{Q}$–definable, holomorphic encoding $\omega_n : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{O}_n$ of the object class $\mathcal{O}_n$ by the data structure $\mathbb{A}^1 \times \mathbb{A}^n$, defined for $(t,u) \in \mathbb{A}^1 \times \mathbb{A}^n$ by $\omega_n(t,u) := F_n^{(t,u)}$ (see Section 5.3).

Observe that $\widehat{\sigma}_n \circ \omega_n : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{D}_n$ is a dominant morphism of $\mathbb{Q}$–definable, irreducible varieties. Therefore $\theta_1^{(n)} := \check{\theta}_1^{(n)} \circ \widehat{\sigma}_n \circ \omega_n, \dots , \theta_{\widehat{m}_n}^{(n)} := \check{\theta}_{\widehat{m}_n}^{(n)} \circ \widehat{\sigma}_n \circ \omega_n$ are well–defined rational functions belonging to $\mathbb{Q}(T, U)$. Observe that $\widehat{\sigma}_n \circ \omega_n$ induces a $\mathbb{Q}$–algebra isomorphism which maps the coordinate ring $\mathbb{Q}[\mathcal{D}_n]$ onto the subdomain

$$\mathcal{A}_n := \mathbb{Q}[F_n(T, U, \gamma_1^{(n)}), \dots , F_n(T, U, \gamma_{m(n)}^{(n)})]$$

of the polynomial ring $\mathbb{Q}[T, U]$.

Since the rational functions $\check{\theta}_1^{(n)}, \dots , \check{\theta}_{\widehat{m}_n}^{(n)}$ belong to the integral closure of $\mathbb{Q}[\mathcal{D}_n]$ in $\mathbb{Q}(\mathcal{D}_n)$, we conclude that $\theta_1^{(n)}, \dots , \theta_{\widehat{m}_n}^{(n)}$ belong to the integral closure of $\mathcal{A}_n$ in $\mathbb{Q}(T, U)$. But $\mathbb{Q}[T, U]$ is integrally closed in its fraction field. This implies that $\theta_1^{(n)}, \dots , \theta_{\widehat{m}_n}^{(n)}$ are *polynomials* belonging to $\mathbb{Q}[T, U]$. Thus $\theta_n := (\theta_1^{(n)}, \dots , \theta_{\widehat{m}_n}^{(n)})$ defines a morphism of algebraic varieties $\theta_n : \mathbb{A}^1 \times \mathbb{A}^n \to \mathcal{D}_n^*$ which satisfies for any point $(t, u) \in \mathbb{A}^1 \times \mathbb{A}^n$ the identities

$$\begin{aligned}
\omega_n^*\big(\theta_n(t, u)\big) &= \omega_n^*\Big(\check{\theta}_n\Big(\widehat{\sigma}_n\big(\omega_n(t, u)\big)\Big)\Big) \\
&= \omega_n^*\Big(\widehat{\theta}_n\Big(\widehat{\sigma_n}\big(\omega_n(t, u)\big)\Big)\Big) \\
&= \widehat{P}_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)} \\
&= \prod_{(\varepsilon_1, \dots , \varepsilon_n) \in \{0,1\}^n} \Big(Y - R_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)}(\varepsilon_1, \dots , \varepsilon_n)\Big) .
\end{aligned}$$

Let $t \in \mathbb{A}^1$ and $u = (u_1, \dots , u_n) \in \mathbb{A}^n$ be fixed for the moment. Observe that $R_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)}$ is the *unique* polynomial of the object class $\widehat{\mathcal{O}}_n$ which satisfies the condition

$$\Big(R_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)}(\gamma_1^{(n)}), \dots , R_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)}(\gamma_{m(n)}^{(n)})\Big) = \widehat{\sigma}_n \circ \omega_n(t, u).$$

On the other hand we have

$$\widehat{\sigma}_n \circ \omega_n(t, u) = \Big(F_n^{(t,u)}(\gamma_1^{(n)}), \dots , F_n^{(t,u)}(\gamma_{m(n)}^n)\Big)$$

and $F_n^{(t,u)} \in \widehat{\mathcal{O}}_n$. This implies $R_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)} = F_n^{(t,u)}$ and therefore we have

$$\begin{aligned}
\omega_n^* \left(\theta_n(t,u)\right) &= \prod_{(\varepsilon_1,\dots,\varepsilon_n)\in\{0,1\}^n} \Big(Y - R_n^{(\widehat{\sigma}_n \circ \omega_n)(t,u)}(\varepsilon_1,\dots,\varepsilon_n)\Big) \\
&= \prod_{(\varepsilon_1,\dots,\varepsilon_n)\in\{0,1\}^n} \Big(Y - F_n^{(t,u)}(\varepsilon_1,\dots,\varepsilon_n)\Big) \\
&= \prod_{j=1}^{2^n-1} \left(Y - (j + t\prod_{i=1}^{n} u_i^{[j]_i})\right).
\end{aligned}$$

Let $P_n := \prod_{j=1}^{2^n-1}\Big(Y - (j + T\prod_{i=1}^{n} U_i^{[j]_i})\Big) \in \mathbb{Q}[T,U,Y]$ be the elimination polynomial introduced in Sections 4.2 and 5.3. Then we have $\omega_n^*\big(\theta_n(t,u)\big) = P_n^{(t,u)}$ for any point $(t,u) \in \mathbb{A}^1 \times \mathbb{A}^n$. Taking now $\mathbb{A}^1 \times \mathbb{A}^n$ as input data structure, $\theta_n(\mathbb{A}^1 \times \mathbb{A}^n)$ as output data structure, $\{P_n^{(t,u)}; t \in \mathbb{A}^1, u \in \mathbb{A}^n\}$ as output object class encoded by the restriction of ω_n^* to the $\mathbb{Q}$–definable subset $\theta_n(\mathbb{A}^1 \times \mathbb{A}^n)$ of $\mathcal{D}_n^*$, we see now that these data structures are $\mathbb{Q}$–constructible, that the encoding is $\mathbb{Q}$–definable and holomorphic and that θ_n represents a *totally division–free* algorithm which computes for each input code (t,u) of $\mathbb{A}^1 \times \mathbb{A}^n$ an output code $\theta_n(t,u)$ which encodes the output object $P_n^{(t,u)}$. Thus θ_n is a totally division–free elimination procedure which computes the general solution P_n of the flat family of zero–dimensional elimination problems given by the equations $X_1^2 - X_1 = 0, \dots, X_n^2 - X_n = 0$ and the polynomial F_n (see Section 5.3).

Recall that the polynomials $\theta_1^{(n)}, \dots, \theta_{\widehat{m}_n}^{(n)}$ belong to the integral closure of $\mathcal{A}_n = \mathbb{Q}[F_n(T,U,\gamma_1^{(n)}), \dots, F_n(T,U,\gamma_{m(n)}^{(n)})]$ in $\mathbb{Q}[T,U]$ and that the $\mathbb{Q}$–algebra $\mathcal{A}_n$ is canonically isomorphic to the coordinate ring $\mathbb{Q}[\overline{\mathcal{O}}_n]$ of the Zariski closure of the object class $\mathcal{O}_n$. Therefore θ_n is a *robust* elimination procedure in the sense of Definition 4. From Theorem 3 we deduce now the estimate $\widehat{m}_n \geq 2^n$.

Since by assumption the sequential time complexity measure $\mathcal{T}$ is monotone, we conclude now that

$$2^n \leq \widehat{m}_n = |\widehat{P}_n| \leq \mathcal{T}(|\mathcal{B}_n|) \leq \mathcal{T}^2(|\Psi_n|) \leq \mathcal{T}^3(|\Phi_n|) \leq \mathcal{T}^3(cn^2)$$

holds for a suitable universal constant $c > 0$.

Therefore $\mathcal{T}$ cannot be a polynomial function. Finally we remark that the same conclusion is valid if we replace in our argumentation the formula Φ_n by the formula $\widetilde{\Phi}_n$. We may now summarize these considerations by the following general result:

Theorem 4 *Let $\mathcal{P}$ be a universal elimination procedure for the theory of algebraically closed fields of characteristic zero with constants* 0, 1 *and let $\mathcal{T}$ a sequential time complexity measure for $\mathcal{P}$. Suppose that $\mathcal{P}$ accepts as inputs prenex existential formulas whose polynomial terms are given in arithmetic circuit or sparse representation. Suppose that $\mathcal{P}$ and $\mathcal{T}$ satisfy conditions (1), (2), (3) above. Then $\mathcal{T}$ is not a polynomial function.*

6 Conclusions.

There exists a general opinion between computer scientists that proving lower complexity bounds for specific problems defined by existential prenex formulas (see [Bor93]) is an extremely difficult task which requires tricky methods or deep mathematical insight. Simple minded algorithmic models and the absence of operative notions of uniformity make in our opinion excessively intricate or impossible to prove striking complexity results for many fundamental algorithmic problems of practical interest. A way out of this dilemma consists in the restriction of the computational model under consideration. Thus one may for example think to consider only unbounded fan–in and fan–out arithmetic circuits of *bounded depth* for the computation of polynomials of interest, as e.g. the resultant of two generic univariate polynomials or more generally, the general solution of a flat family of zero–dimensional elimination problems.

Asymptotically optimal lower sequential time complexity bounds become then easy to prove. However the restriction to bounded depth circuits represents a highly artificial limitation of the computational model (this restriction excludes for example the evaluation of monomials of high degree by means of iterated squaring) and the complexity result obtained in this way becomes irrelevant as a guide for future software developers.

The ultimate aim of this paper was not a theoretical but a practical one. We tried to give a partial answer to the following fundamental question:

what has to be changed in elimination theory in order to obtain practically efficient algorithms?

We established a list of implicit or explicit requirements satisfied by all known (symbolic or seminumeric) elimination algorithms. These requirements are: universality, no branchings and robustness for certain simple elimination problems, capacity of computing certain closures (as e.g. equations for the Zariski closure of a given constructible set or the greatest common divisor of two polynomials). Moreover, by means of a suitable preparation of the input equation, all known universal elimination procedures may be transformed easily into Kronecker–like procedures which are able to evaluate the corresponding canonical elimination polynomial in any given argument or to compute its coefficients. In this sense the known elimination procedures are all able to "compute canonical elimination polynomials".

The fulfillment of these requirements and the capacity of computing canonical elimination polynomials implies the experimentally certified non–polynomial complexity character of these elimination procedures and explains their practical inefficiency. The results of this paper demonstrate that the complexity problem we focus on is not a question of optimization of algorithms and data structures. There is no way out of the dilemma by changing for example from dense to sparse elimination or to fewnomial theory. Hybridization of symbolic and numeric algorithms leads us again back to the same complexity problems we started from.

In this sense the paper is devoted to the elaboration and discussion of a series of "uniformity" notions which restrict the (mostly implicit) computational models relevant for the present (and probably also the future) design of implementable elimination procedures in algebraic geometry. Emphasis was put on the motivation of these algorithmic restrictions and not on the mathematical depth of the techniques used in this paper in order to prove lower complexity bounds. In fact, it turns out that elementary methods of classical algebraic geometry are sufficient to answer the complexity questions addressed in this paper. It is not the first time that a refined analysis of the complexity model produces not only elementary and simpler proofs of lower bound results in algebraic complexity theory, but also stronger complexity statements. Examples are the "elementarizations" of Strassen's degree method [Str73a], due to Schönhage [Sch76] and Baur [BCS97, Theorem 8.5], and the combinatorial method of Aldaz and Montaña for the certification of the hardness of univariate polynomials (compare [BCS97, Chapter 9] with [AHM$^+$98] and [AM$^+$01]).

Nevertheless there are two points addressed in this paper, which call for the development of deep new tools in mathematics and computer science: the problem of algorithmic modeling addressed in Section 4.3 calls for the search of mathematical statements which generalize Hilbert's Irreducibility Theorem to (not necessarily unirational) algebraic varieties containing "many" integer or rational points and to the characterization of unirational varieties (in the sense of [Kol99]) by means of arithmetic properties.

On the other hand our discussion of the notion of robustness of elimination procedures in Section 5.1 leads to the question in which sense the concept of programmable function can be distinguished from the notion of elementarily recursive function (here the concepts of specification and data type make the main difference). A programmable function appears always together with a certificate ("correctness proof") that it meets its specification. The existence of such a proof necessarily restricts the syntactical form of the underlying program and hence the complexity model in which the running time of the program is measured.

A Appendix.

A.1 Universal correct test and identification sequences.

In this section we are going to formulate a slight generalization of the main results of Section 3.3 and 3.3.2 namely Lemma 4, Corollary 1 and Theorem 1. These generalizations are based on Baire's Theorem and lead to the concept of *universal* correct test and identification sequence.

Corollary 7 *Let $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ and let L, m, t be given natural numbers with $m > L$. Then there exists a subset $S \subset \mathbb{R}^{mt}$ satisfying the following conditions:*

(i) S is dense in the strong topology of $\mathbb{R}^{mt}$.

(ii) any element $\gamma = (\gamma_1, \ldots, \gamma_m) \in S$ with $\gamma_1, \ldots, \gamma_m \in \mathbb{R}^t$ is a correct test sequence for the $\mathbb{Q}$–Zariski closure of any $\mathbb{Q}$–constructible object class $\mathcal{O}$ of t–variate polynomial functions over $\mathbb{C}$ such that for $\mathcal{O}$ there exists a $\mathbb{Q}$–definable holomorphic encoding by a data structure of size L.

A correct test sequence as in Corollary 7, (ii) is called *universal* for the corresponding set of object classes.

Proof.– Observe that there are only countably many $\mathbb{Q}$–definable holomorphic encodings of $\mathbb{Q}$–constructible object classes of polynomial functions in t variables over $\mathbb{C}$ by data structures of size L. Therefore we may think these encodings enumerated as $\omega_1, \omega_2, \ldots$. From the second part of the proof of Lemma 4 of Section 3.3.1 we conclude that there exists for any $i \in \mathbb{N}$ a $\mathbb{Q}$–definable, Zariski open, dense subset $\mathcal{U}_i \subset \mathbb{C}^{mt}$ such that any element $\gamma = (\gamma_1, \ldots, \gamma_m)$ of $\mathcal{U}_i$ with $\gamma_1, \ldots, \gamma_m \in \mathbb{C}^t$ is a correct test sequence for the $\mathbb{Q}$–Zariski closure of the object class of t–variate polynomial functions over $\mathbb{C}$ encoded by ω_i. Observe now that $\mathcal{U}_i^* := \mathcal{U}_i \cap \mathbb{R}^{mt}$ is open and dense in the strong topology of $\mathbb{R}^{mt}$. Let $S := \cap_{i \in \mathbb{N}} \mathcal{U}_i^*$. From Baire's Theorem we deduce that the set S is still dense in the strong topology of $\mathbb{R}^{mt}$.

Let $\gamma = (\gamma_1, \ldots, \gamma_m)$ be an arbitrary element of S with $\gamma_1, \ldots, \gamma_m \in \mathbb{R}^t$ and let $\mathcal{O}$ be an arbitrary $\mathbb{Q}$–constructible object class of t–variate polynomials over $\mathbb{C}$ such that for $\mathcal{O}$ there exists a $\mathbb{Q}$–definable holomorphic encoding by a data structure of size L. Then there exist an index $i \in \mathbb{N}$ such that ω_i encodes $\mathcal{O}$. From $S \subset \mathcal{U}_i$ we deduce that γ is a correct test sequence for the object class $\overline{\mathcal{O}}$. In conclusion γ is a universal correct test sequence of length m for the set of object classes under consideration. ■

Corollary 8 *Let $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ and let L, m, t be given natural numbers with $m > 2L$. Then there exists a subset $S \subset \mathbb{R}^{mt}$ satisfying the following conditions:*

(*i*) *S is dense in the strong topology of $\mathbb{R}^{mt}$.*

(*ii*) *Any element $\gamma = (\gamma_1, \ldots, \gamma_m) \in S$ with $\gamma_1, \ldots, \gamma_m \in \mathbb{R}^t$ is an identification sequence for the $\mathbb{Q}$–Zariski closure of any $\mathbb{Q}$–constructible object class $\mathcal{O}$ of t–variate polynomial functions over $\mathbb{C}$ such that for $\mathcal{O}$ there exists a $\mathbb{Q}$–definable holomorphic encoding by a data structure of size L.*

An identification sequence as in Corollary 8, (*ii*) is called *universal* for the corresponding set of object classes.

The proof of Corollary 8 combines the statement of Corollary 7 with the same arguments employed in the proof of Corollary 1 of Section 3.3.1 and is omitted here.

In a similar way one may combine Corollary 8 and Lemma 5 of Section 3.4 in order to prove the following statement:

Corollary 9 *Let $k := \mathbb{Q}$, $\overline{k} := \mathbb{C}$ and let L, m, t be given natural numbers with $m > 2L$. Then there exists a subset $S \subset \mathbb{R}^{mt}$ satisfying the following conditions:*

(*i*) *S is dense in the strong topology of $\mathbb{R}^{mt}$,*

(*ii*) *any element $\gamma = (\gamma_1, \ldots, \gamma_m) \in S$ with $\gamma_1, \ldots, \gamma_m \in \mathbb{R}^t$ has the following property:*

let $\mathcal{O}$ be an arbitrary $\mathbb{Q}$–constructible object class of t–variate polynomial functions over $\mathbb{C}$ such that for $\mathcal{O}$ there exists a $\mathbb{Q}$–definable holomorphic encoding by a data structure of size L and suppose that $\mathcal{O}$ is a cone. Let $\sigma : \overline{\mathcal{O}} \to \mathbb{A}^m(\mathbb{C})$ be the map defined by $\sigma(F) := \big(F(\gamma_1), \ldots, F(\gamma_m)\big)$ for $F \in \overline{\mathcal{O}}$ and let $\mathcal{D}^* := \sigma(\overline{\mathcal{O}})$. Then $\mathcal{D}^*$ is a cone of $\mathbb{A}^m(\mathbb{C})$ which is closed in the $\mathbb{C}$–Zariski topology of $\mathbb{A}^m(\mathbb{C})$ (and hence also in the strong topology) and σ defines a bijective finite morphism of $\mathcal{O}$ onto $\mathcal{D}^*$. For any $\mathbb{C}$–irreducible component $\mathcal{C}$ of $\overline{\mathcal{O}}$ the restriction map $\sigma : \mathcal{C} \to \sigma(\mathcal{C})$ is a birational (finite and bijective) morphism of $\mathcal{C}$ onto the $\mathbb{C}$–irreducible Zariski closed set $\sigma(\mathcal{C})$. The encoding of the object class $\overline{\mathcal{O}}$ by the data structure $\mathcal{D}^*$ defined by $\omega^* := \sigma^{-1}$ is continuous with respect to the $\mathbb{C}$–Zariski topologies of $\overline{\mathcal{O}}$ and $\mathcal{D}^*$. Moreover ω^* is holomorphic if and only if ω^* allows to answer holomorphically the value question about the object class $\overline{\mathcal{O}}$. Finally ω^* induces an encoding of the projective variety associated to the cone $\overline{\mathcal{O}}$ by the projective variety associated to the cone $\mathcal{D}^*$ which is continuous with respect to the strong topology.

A.2 The VC–dimension of a holomorphically encoded object class.

Let $\mathcal{O}$ be a k–constructible object class of polynomial functions. We say that a finite set $A \subset \mathbb{A}^t$ can be *shattered* by the object class $\mathcal{O}$ if for each subset $A' \subset A$ there exists an object $F \in \mathcal{O}$ such that any element $a \in A$ belongs to A' if and only if $F(a) = 0$ holds. We define the *Vapnik–Chervonenkis (VC) dimension* $dim_{VC}\mathcal{O}$ of $\mathcal{O}$ as infinite if there exist subsets A of $\mathbb{A}^t$ of arbitrary cardinality which can be shattered by $\mathcal{O}$. Otherwise we define $dim_{VC}\mathcal{O}$ as the maximal cardinality of such a set (see [Vap00, Chapter 3, 3.6] and [BCS97, Chapter 3, 3.5] for details). The following statement implies that the VC–dimension of the object class $\mathcal{O}$ is finite.

Lemma 7 *Let notations and assumptions be as in Lemma 4 of Section 3.3.1. Then $dim_{VC}\mathcal{O}$ satisfies the following estimate:*

$$(dim_{VC}\mathcal{O})^{\frac{1}{2}} \leq \frac{dim_{VC}\mathcal{O}}{\log dim_{VC}\mathcal{O}} \leq L(1 + \log \Delta_2)$$

(here log *denotes the logarithm to the base 2).*

Proof.– We shall freely use the notations of the proof of Lemma 4. Let $s \in \mathbb{N}$ with $s \leq dim_{VC}\mathcal{O}$. Then there exists a finite set $A \subset \mathbb{A}^t$ of cardinality s which can be shattered by $\mathcal{O}$. Let $A = \{a_1, \ldots, a_s\}$ with $a_1, \ldots, a_s \in \mathbb{A}^t$. From the construction of the ambient space $\mathbb{A}^N$ of $\mathcal{O}$ we deduce that there exists a k–definable (evaluation) map $eval : \mathbb{A}^N \times \mathbb{A}^t \to \mathbb{A}^1$ which satisfies the condition $eval(F, y) = F(y)$ for any polynomial $F \in \mathcal{O}$ and any point $y \in \mathbb{A}^t$. This implies that for any $a \in A$ there exists a polynomial $\Omega_a \in \overline{k}[Z_1, \ldots, Z_L]$ of degree at most Δ_2 such that for any $D \in \mathcal{D}$ the identity $\Omega_a(D) = eval(\Omega(D), a) = \omega(D)(a)$ holds.

Let A' be an arbitrary subset of A. By hypothesis there exists a polynomial $F \in \mathcal{O}$ with $A' = \{a \in A; F(a) = 0\}$. Consider

$$\mathcal{D}_{A'} := \{D \in \mathcal{D}; \Omega_a(D) = 0 \text{ for } a \in A', \ \Omega_a(D) \neq 0 \text{ for } a \in A \setminus A'\}.$$

Any code $D \in \mathcal{D}$ with $\omega(D) = F$ belongs to $\mathcal{D}_{A'}$. Therefore $\mathcal{D}_{A'}$ is nonempty. Thus $\mathcal{D}_{A'}$ is a $\Omega_{a_1}, \ldots, \Omega_{a_s}$–cell in the sense of [Hei83]. From [JS00, Theorem 2] or [Hei83, Corollary 1] one deduces that the number of $\Omega_{a_1}, \ldots, \Omega_{a_s}$–cells is bounded by $(1 + s\Delta_2)^L$. Since the set A can be shattered by $\mathcal{O}$ and different subsets of A define disjoint $\Omega_{a_1}, \ldots, \Omega_{a_s}$–cells we conclude

$$2^s \leq (1 + s\Delta_2)^L.$$

This implies $\frac{s}{\log s} \leq L(1 + \log \Delta_2)$. From $s \leq dim_{VC}\mathcal{O}$ we deduce now

$$(dim_{VC}\mathcal{O})^{\frac{1}{2}} \leq \frac{dim_{VC}\mathcal{O}}{\log dim_{VC}\mathcal{O}} \leq L(1 + \log \Delta_2).$$

■

Let $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$. We are going to consider the data structure $\mathcal{D}_{real} := \mathcal{D} \cap \mathbb{R}^L$ and the object class $\mathcal{O}_{real} := \omega(\mathcal{D}_{real})$. Observe that $\mathcal{O}_{real}$ is a $\mathbb{Q}$–definable semialgebraic subset of $\mathbb{R}^N$. The standard definition of the VC–dimension of $\mathcal{O}_{real}$ is slightly different from our definition of the VC–dimension of $\mathcal{O}$ (see [Vap00, Chapter 3, 3.6]). Taking into account the number of different real cells of a system of s real polynomials of degree at most Δ_2 in $L+1$ variables is of order $O\left(\left(\frac{s\Delta_2}{L+1}\right)^{L+1}\right)$ (see [PR93]), one concludes in the same way as in the proof of Lemma 7 that

$$(dim_{VC}\mathcal{O}_{real})^{\frac{1}{2}} \leq \frac{dim_{VC}\mathcal{O}_{real}}{\log dim_{VC}\mathcal{O}_{real}} \leq (L+1)\log\Delta_2 + O\left(\frac{1}{\log dim_{VC}\mathcal{O}_{real}}\right) \tag{13}$$

holds.

Let $\overline{W}_{L,t}$ be the set of all polynomials $F \in \overline{k}[Y_1, \ldots, Y_t]$ which have approximative nonscalar (sequential) complexity over $\overline{k}$ at most L. From Corollary 2 and its proof we conclude that $\overline{W}_{L,t}$ is a k–constructible object class which has a k–definable, holomorphic encoding of size $4(L+t+1)^2+2$ by means of polynomials over k of degree at most $L2^{L+1}+2$. Thus Lemma 7 implies the estimate

$$dim_{VC}\overline{W}_{L,t} \leq 8(L+t+1)^{3+\varepsilon}$$

for any $\varepsilon > 0$. From [BCS97, Chapter 9, Proposition 9.1] we infer that any univariate polynomial of $\overline{k}[Y_1, \ldots, Y_t]$ of degree at most $\frac{L^2}{4}$ belongs to $W_{L,t}$ and hence to $\overline{W}_{L,t}$.

Let $A \subset \mathbb{A}^t$ be a subset of $s := \lfloor \frac{L^2}{4} \rfloor$ elements of the form $A := \{(a_i, 0, \ldots, 0); a_i \in k, 1 \leq i \leq s\}$ (here $\lfloor \frac{L^2}{4} \rfloor$ denotes the largest integer below $\frac{L^2}{4}$). Then for any subset A' of A there exists a polynomial $F \in k[Y_1]$ of degree $\#A'$ such that $A' := \{a \in A; F(a) = 0\}$ holds. From $\deg F = \#A' \leq \frac{L^2}{4}$ we deduce $F \in \overline{W}_{L,t}$. This consideration implies finally

$$\frac{L^2}{4} - 1 < dim_{VC}\overline{W}_{L,t} \leq 8(L+t+1)^{3+\varepsilon}$$

for any $\varepsilon > 0$.

Let $k := \mathbb{Q}$ and $\overline{k} := \mathbb{C}$. We consider the set $W^{real}_{L,t}$ of all polynomials of $\mathbb{R}[Y_1, \ldots, Y_t]$ which can be evaluated by a totally division–free arithmetic circuit of nonscalar size at most L using only scalars from $\mathbb{R}$. Thus we have $W^{real}_{L,t} = (W_{L,t})_{real}$. Taking into account the estimate (13), we conclude in a similar way as before that

$$\frac{L^2}{4} - 1 < dim_{VC}\overline{W}^{real}_{L,t} \leq 8(L+t+1)^{3+\varepsilon} + O\left(\frac{1}{\log dim_{VC}\overline{W}^{real}_{L,t}}\right)$$

holds for any $\varepsilon > 0$.

Analogous considerations lead to an upper bound for the set of polynomials of $\mathbb{R}[Y_1, \dots, Y_t]$ which have approximative complexity at most L in terms of essentially division–free arithmetic circuits using only parameters from $\mathbb{R}(\varepsilon)$.

Acknowledgment. The authors wish to thank Rosa Wachenchauzer who pointed to us the relation between complexity theory and program specification and generation. They are especially grateful to the anonymous referees for many useful suggestions which helped to improve considerably the presentation of the results of this paper. J. Heintz and G. Matera thank to the Facultad de Ingeniería, Ciencias Exactas y Naturales, Universidad Favaloro, where they did part of this work.

References

[AHM$^+$98] M. Aldaz, J. Heintz, G. Matera, J. L. Montaña, and L.M. Pardo. Combinatorial hardness proofs for polynomial evaluation. In L. Brim *et al.*, editor, *Proceedings 23rd. International Symposium on Mathematical Foundations of Computer Science, MFoCS'98*, volume 1450 of *Lecture Notes in Computer Science*, pages 167–175, Berlin Heidelberg New York, 1998. Springer.

[Ald84] A. Alder. *Grenzrang und Grenzkomplexität aus algebraischer und topologischer Sicht.* PhD thesis, Universität Zürich, Philosophische Fakultät II, 1984.

[AM69] M.F. Atiyah and J.G. MacDonald. *Introduction to Commutative Algebra.* Addison–Wesley, Reading, Massachusetts, 1969.

[AM$^+$01] M. Aldaz, G. Matera, J.L. Montaña, and L.M. Pardo. A new method to obtain lower bounds for polynomial evaluation. *Theoretical Computer Science*, 259(1–2):577–596, 2001.

[BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften.* Springer, Berlin Heidelberg New York, 1997.

[BCSS98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer, New York Berlin Heidelberg, 1998.

[BGHM97] B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties and efficient real equation solving: The hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[BGHM01] B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[BHMW02] N. Bruno, J. Heintz, G. Matera, and R. Wachenchauzer. Functional programming concepts and straight–line programs in computer algebra. *Mathematics and Computers in Simulation*, 60(6): 423–473, 2002.

[BM93] D. Bayer and D. Mumford. What can be computed in algebraic geometry ? In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Symposia Matematica*, pages 1–49, Cambridge, 1993. Instituto Nazionale di Alta Matematica, Cambridge University Press.

[Bor48] E. Borel. La définition en mathématiques. In *Les Grands Courants de la Pensée Mathématique*, pages 24–34. Cahiers du Sud, Paris, 1948.

[Bor93] A. Borodin. Time space tradeoffs (getting closer to the barriers?). In *4th International Symposium on Algorithms and Computation, ISAAC '93, Hong Kong, December 15-17, 1993*, volume 762 of *Lecture Notes in Computer Science*, pages 209–220, Berlin Heidelberg New York, 1993. Springer.

[Can88] J. Canny. Some algebraic and geometric problems in PSPACE. In *Proceedings 20th. Annual ACM Symposium on Theory of Computing, Chicago, Illinois, 2–4 May 1988*, pages 460–467, New York, 1988. ACM Press.

[CG83] A.L. Chistov and D.Y. Grigoriev. Subexponential time solving systems of algebraic equations. I, II. LOMI preprints E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[CGH89] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora et al., editor, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-6*, volume 357 of *Lecture Notes in Computer Science*, pages 131–152, Berlin Heidelberg New York, 1989. Springer.

[CHLM00] B. Castaño, J. Heintz, J. Llovet, and R. Martínez. On the data structure straight–line program and its implementation in symbolic computation. *Mathematics and Computers in Simulation*, 51:497–528, 2000.

[CHMP01] D. Castro, K. Hägele, J.E. Morais, and L.M. Pardo. Kronecker's and newton's approaches to solving: a first comparison. *Journal of Complexity*, 17(1):212–303, 2001.

[CMPS02] D. Castro, J.L. Montaña, L.M. Pardo, and J. San Martín. The distribution of condition numbers of rational data of bounded bit length. *Foundations of Computational Mathematics*, 2(1):1–52, 2002.

[CS99] F. Cucker and S. Smale. Complexity estimates depending on condition and round–off error. *Journal of the Association for Computing Machinery*, 46(1):113–184, 1999.

[DFGS91] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33:73–94, 1991.

[DH88] J.H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5:29–35, 1988.

[FGM90a] N. Fitchas, A. Galligo, and J. Morgenstern. Algorithmes rapides en sequentiel et en parallele pour l'élimination des quantificateurs en Géométrie élementaire. In F. Delon, M. Dickmann, and D. Gondard, editors, *Seminaire sur les structures algébriques ordonnées*, volume 32 of *Pub. Math. Univ. Paris VII*, pages 103–145. Paris, 1990.

[FGM90b] N. Fitchas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *Journal of Pure and Applied Algebra*, 67(1):1–14, 1990.

[FGS95] N. Fitchas, M. Giusti, and F. Smietanski. Sur la complexité du théorème des zéros. In J. Guddat et al, editor, *Approximation and Optimization in the Caribbean II, Proceedings 2nd International Conference on Non–Linear Optimization and Approximation*, volume 8 of *Approximation and Optimization*, pages 247–329. Peter Lange Verlag, Frankfurt am Main, 1995.

[Ful84] W. Fulton. *Intersection Theory.* Springer, Berlin Heidelberg New York, 1984.

[GH91] M. Giusti and J. Heintz. Algorithmes - disons rapides - pour la décomposition d' une variété algébrique en composantes irréductibles et équidimensionelles. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry, Proceedings of MEGA'90*, volume 94 of *Progress in Mathematics*, pages 169–194, Basel, 1991. Birkhäuser.

[GH93] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Symposia Matematica*, pages 216–256, Cambridge, 1993. Cambridge University Press.

[GH01] M. Giusti and J. Heintz. Kronecker's smart, little black–boxes. In A. Iserles R. Devore and E. Süli, editors, *Proceedings of Foundations of Computational Mathematics, FoCM'99, Oxford 1999*, volume 284 of *London Mathematical Society Lecture Notes Series*, pages 69–104, Cambridge, 2001. Cambridge University Press.

[GHH$^+$97] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, and L.M. Pardo. Lower bounds for diophantine approximation. *Journal of Pure and Applied Algebra*, 117,118:277–317, 1997.

[GHM$^+$98] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo. Straight–line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.

[GHMP95] M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo. When polynomial equation systems can be solved fast ? In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, ' Proceedings AAECC-11*, volume 948 of *Lecture Notes in Computer Science*, pages 205–231, Berlin Heidelberg New York, 1995. Springer.

[GHMP97] M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *Comptes Rendus de l'Academie de Sciences de Paris*, 325:1223–1228, 1997.

[GHS93] M. Giusti, J. Heintz, and J. Sabia. On the efficiency of effective Nullstellensätze. *Computational Complexity*, 3:56–95, 1993.

[GKZ94] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants.* Birkhäuser, Boston, 1994.

[GLS01] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[GM89] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using gröbner bases. In L. Huguet and A. Poli, editors, *Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, Proceedings of AAECC–5, Menorca, Spain, June 15-19, 1987*, volume 356 of *Lecture Notes in Computer Science*, pages 247–257, Berlin Heidelberg New York, 1989. Springer.

[GS99] M. Giusti and E. Schost. Solving some over–determined systems. In S. Dooley, editor, *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation, ISSAC'99, July 28–31, 1999, Vancouver, Canada*, pages 1–8, New York, 1999. ACM Press.

[GV88] D. Grigoriev and N.N. Vorobjov, Jr. Solving systems of polynomial inequalities in sub–exponential time. *Journal of Symbolic Computation*, 5(1-2):37–64, 1988.

[Hei79] J. Heintz. Definability bounds of first order theories of algebraically closed fields (extended abstract). In L. Budach, editor, *Proceedings of Fundamentals of Computation Theory, FCT'79, Berlin/ Wendisch- Rietz, 1979*, pages 160–166, Berlin, 1979. Akademie Verlag.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.

[Hei89] J. Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. In L. Huguet and A. Poli, editors, *Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, Proceedings of AAECC–5, Menorca, Spain, June 15-19, 1987*, volume 356 of *Lecture Notes in Computer Science*, pages 269–300, Berlin Heidelberg New York, 1989. Springer.

[HKP$^+$00] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *Journal of Complexity*, 16(1):70–109, 2000.

[HMPS00] K. Hägele, J.E. Morais, L.M. Pardo, and M. Sombra. On the intrinsic complexity of the arithmetic Nullstellensatz. *Journal of Pure and Applied Algebra*, 146(2):103–183, 2000.

[HMPW98] J. Heintz, G. Matera, L.M. Pardo, and R. Wachenchauzer. The intrinsic complexity of parametric elimination methods. *Electronic Journal of SADIO*, 1(1):37–51, 1998.

[HMW01] J. Heintz, G. Matera, and A. Waissbein. On the time–space complexity of geometric elimination procedures. *Applicable Algebra in Engineering, Communication and Computing*, 11(4):239–296, 2001.

[HRS89] J. Heintz, M.-F. Roy, and P. Solernó. On the complexity of semialgebraic sets. In G. Ritter, editor, *Information Processing 89, Proceedings of the IFIP 11th World Computer Congress, San Francisco, USA, August 28 – September 1, 1989*, pages 293–298. North-Holland/IFIP, 1989.

[HRS90] J. Heintz, M.-F. Roy, and P. Solernó. Sur la complexité du principe de Tarski–Seidenberg. *Bulletin de la Societé Mathématique de France*, 118(1):101–126, 1990.

[HS81] J. Heintz and M. Sieveking. Absolute primality of polynomials is decidable in random polynomial–time in the number of variables. In Shimon Even and Oded Kariv, editors, *ICALP 81: Proceedings 8th International Colloquium on Automata, Languages and Programming, Acre (Akko), Israel, July 13-17, 1981*, volume 115 of *Lecture Notes in Computer Science*, pages 16–28. Springer, 1981.

[HS82] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *International Symposium on Logic and Algorithmic, Zurich 1980*, volume 30 of *Monographie de l'Enseignement Mathématique*, pages 237–254, 1982.

[Ier89] D. Ierardi. Quantifier elimination in the theory of an algebraically closed field. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, Seattle, Washington, 15–17 May 1989*, pages 138–147, New York, 1989. ACM Press.

[Ive73] B. Iversen. *Generic local structure of the morphisms in Commutative Algebra*, volume 310 of *Lecture Notes in Mathematics*. Springer, 1973.

[JS00] G. Jerónimo and J. Sabia. On the number of sets definable by polynomials. *Journal of Algebra*, 227(2):633–644, 2000.

[Kal88] E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *Journal of the Association for Computing Machinery*, 35(1):231–264, 1988.

[Kol99] J. Kollár. *Rational curves on algebraic varieties*. Springer Verlag, 1999.

[KP94] T. Krick and L.M. Pardo. Une approche informatique pour l'approximation diophantienne. *Comptes Rendus de l'Académie des Sciences de Paris*, 318(1):407–412, 1994.

[KP96] T. Krick and L.M. Pardo. A computational method for diophantine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 193–254, Basel, 1996. Birkhäuser.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen theorie de algebraischen grössen. *Journal für die Reine und Angewandte Mathematik*, 92:1–122, 1882.

[Lan58] S. Lang. *Introduction to Algebraic Geometry.* Interscience, 1958.

[Lan93] S. Lang. *Algebra.* Addison–Wesley Publishing Co., Reading, Massachusetts, third edition, 1993.

[Lec00] G. Lecerf. *Kronecker 0.16beta-2. Reference Manual.* Laboratoire GAGE, École Polytechnique, Palaiseau, France, 2000. `http://kronecker.medicis.polytechnique.fr/`.

[Lec01] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *Proceedings 2000 ACM-SIGSAM International Symposium on Symbolic and Algebraic Computation ISSAC'2000 (August 6 - 10, 2000, St. Andrews, United Kingdom)*, pages 209–216, New York, 2001. ACM Press.

[LV93] M. Li and P. Vitányi. *Introduction to Kolmogorov Complexity and its Applications.* Springer, Berlin Heidelberg New York, 1993.

[Mat80] H. Matsumura. *Commutative Algebra.* Benjamin, 1980.

[Mat99] G. Matera. Probabilistic algorithms for geometric elimination. *Applicable Algebra in Engineering, Communication and Computing*, 9(6):463–520, 1999.

[MP93] J.L. Montaña and L.M. Pardo. Lower bounds for arithmetic networks. *Applicable Algebra in Engineering, Communication and Computing*, 4(1):1–24, 1993.

[MP97] B. Mourrain and V. Pan. Solving special polynomial systems by using structural matrices and algebraic residues. In F. Cucker and M. Shub, editors, *Proceedings Foundations of Computational Mathematics (FOCM'97)*, pages 287–304, Berlin Heidelberg New York, 1997. Springer.

[Mum88] D. Mumford. *The Red Book of Varieties and Schemes*, volume 1358 of *Lecture Notes in Mathematics.* Springer, Berlin Heidelberg New York, 1st edition, 1988.

[Par95] L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC–11*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69, Berlin Heidelberg New York, 1995. Springer.

[PR93] R. Pollack and M.-F. Roy. On the number of cells defined by a set of polynomials. *Comptes Rendus de l'Academie des Sciences de Paris*, 316(6):573–577, 1993.

[PS98] S. Puddu and J. Sabia. An effective algorithm for quantifier elimination over algebraically closed fields using straight–line programs. *Journal of Pure and Applied Algebra*, 129(2):173–200, 1998.

[Ren92] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. Part I: Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals. *Journal of Symbolic Computation*, 13(3):255–300, 1992.

[Roj00] J.M. Rojas. Computing complex dimension faster and deterministically (extended abstract). Preprint arXiv:math.AG/0005028, 2000.

[Sch76] A. Schönhage. An elementary proof for Strassen's degree bound. *Theoretical Computer Science*, 3:267–272, 1976.

[Sch78] C.P. Schnorr. Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials. *Theoretical Computer Science*, 7:251–261, 1978.

[Sch00] E. Schost. Computing parametric geometric resolutions. Accepted for publication in *Applicable Algebra in Engineering, Communication and Computing*, 2002.

[Sha84] I.R. Shafarevich. *Basic algebraic geometry.* Graduate Texts in Mathematics. Springer, 1984.

[SS93a] M. Shub and S. Smale. Complexity of Bézout's Theorem I: Geometric aspects. *Journal of the AMS*, 6(2):459–501, 1993.

[SS93b] M. Shub and S. Smale. Complexity of Bézout's Theorem II: Volumes and probabilities. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 267–285, Basel, 1993. Birkhäuser.

[SS93c] M. Shub and S. Smale. Complexity of Bézout's Theorem III: Condition number and packing. *Journal of Complexity*, 9:4–14, 1993.

[SS94] M. Shub and S. Smale. Complexity of Bézout's Theorem V: Polynomial time. *Theoretical Computer Science*, 133:141–164, 1994.

[SS96] M. Shub and S. Smale. Complexity of Bézout's Theorem IV: Probability of success. *SIAM Journal of Numerical Analysis*, 33:141–164, 1996.

[Str73a] V. Strassen. Die berechnungskomplexität von elementarsymmetrischen funktionen und von interpolationspolynomen. *Numerische Mathematik*, 2:238–251, 1973.

[Str73b] V. Strassen. Vermeidung von Divisionen. *Crelle J. Reine Angew. Math,*, 264:182–202, 1973.

[Vap00] V.N. Vapnik. *The nature of statistical learning theory.* Statistics for Engineering and Information Science. Springer, New York, 2nd edition, 2000.

[Vog84] W. Vogel. *Results on Bezout's Theorem.* Tata Institute of Fundamental Research. Springer, 1984.

[vzG86] J. von zur Gathen. Parallel arithmetic computations: A survey. In B. Rovan J. Gruska and J. Wiedermann, editors, *Proceedings of the 12th Symposium on Mathematical Foundations of Computer Science, Bratislava, Czechoslovakia, August 25–29, 1996*, volume 233 of *Lecture Notes in Computer Science*, pages 93–112, Berlin Heidelberg New York, August 1986. Springer.

[vzG93] J. von zur Gathen. Parallel linear algebra. In John H. Reif, editor, *Synthesis of Parallel Algorithms.* Morgan Kaufmann, Los Altas, CA, 1993.

[Wei88] V. Weispfennig. The complexity of linear problems in fields. *Journal of Symbolic Computation*, 5:3–27, 1988.