1
Kronecker's smart, little black boxes

Marc Giusti

UMS CNRS–Polytechnique MEDICIS
Laboratoire GAGE
École Polytechnique
F-91128 Palaiseau cedex, France
Email: Marc.Giusti@gage.polytechnique.fr

Joos Heintz

Depto. de Matemáticas, Est. y Comp.
Facultad de Ciencias Universidad de Cantabria
E-39071 Santander, Spain and
Depto. de Matemáticas
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria, Pab. I
(1428) Buenos Aires, Argentina
Email: heintz@hall.matesco.unican.es

Abstract

This paper is devoted to the complexity analysis of certain uniformity properties owned by all known symbolic methods of parametric polynomial equation solving (geometric elimination). It is shown that *any* parametric elimination procedure which is *parsimonious* with respect to *branchings* and *divisions* must necessarily have a non-polynomial sequential time complexity, even if highly efficient data structures (as e.g. the arithmetic circuit encoding of polynomials) are used.

1 Introduction

Origins, development and interaction of modern algebraic geometry and commutative algebra may be considered as one of the most illustrative examples of historical dialectics in mathematics. Still today, and more than ever before, timeless idealism (in form of modern commuta-

Research partially supported by the following Argentinian, Spanish, German and French grants : UBA-CYT TW 80, PIP CONICET 4571/96, ANPCyT PICT 03-00000-01593, DGICYT PB96–0671–C02–02, ARG 018/98 INF (BMBF), UMS 658 MEDICIS, ECOS A99E06, HF 1999–055

tive algebra) is bravely struggling whith secular materialism (in form of complexity issues in computational algebraic geometry).

Kronecker was doubtless the creator of this eternal battle field and its first war lord. In a similar way as Gauss did for computational number theory, Kronecker laid intuitively the mathematical foundations of modern computer algebra. He introduced 1882 in [24] his famous "elimination method" for polynomial equation systems and his "parametric representation" of (equidimensional) algebraic varieties. By the way, this parametric representation was until 10 years ago rediscovered again and again. It entered in modern computer algebra as "Shape Lemma" (see e.g. [36, 7, 10, 22]). Using his elimination method in a highly skillful, but unfortunately inimitable way, Kronecker was able to state and to prove a series of fundamental results on arbitrary algebraic varieties. He was able to define in a precise way the notion of dimension and to prove a corresponding dimension theorem for arbitrary algebraic varieties over an algebraically closed field, to estimate the number of equations needed to define any algebraic variety in affine or projective space and certainly he knew already the special form of "Hilbert's Nullstellensatz".

Not everything that came to Kronecker's mind was laid down by him in a explicit and written form. Nevertheless a careful interpretation of his work suggests his deep understanding of the general structure of algebraic varieties.

A particular result, proved by Kronecker, says that any algebraic variety can be defined by finitely many equations. Later Hilbert generalized this result to his seminal "Basissatz" introducing for its proof a new, nonconstructive method, far away from the traditional elimination-type arguments used by Kronecker and other contemporary mathematicians. It took some time to convince the mathematical world that "mystics" and "magicians" are able to produce (correct) mathematical results, but finally the new discipline of commutative algebra became legitimate.

Hilbert's discovery of the Basissatz was also the starting point for a long and huge conflict which dominated a considerable part of the history of modern algebraic geometry and which did not come to an end until today.

Classical algebraic geometry is motivated by the need – or the wish – to find tools which allow to "solve" or to "reduce" (whatever this means) systems of polynomial equations. This leads to the following questions:

- are commutative algebra and its modern derivate, namely todays scheme-theoretical algebraic geometry, able to absorb classical algebraic geometry?

- is the solution to Hilbert's "Hauptproblem der Idealtheorie" (the ideal membership problem) the key to all computational issues in classical algebraic geometry?

These questions, implicitly raised by the work of Hilbert and Macaulay, look very academic. However any attempt to answer them leads to deep consequences.

Let us here outline just one possible way to answer these questions.

If we consider the "Hauptproblem der Idealtheorie" as a question of pure theoretical computer science, this problem turns out to be computationally intractable, at least in worst case. More precisely, the "Hauptproblem der Idealtheorie" turns out to be complete in exponential (memory) space (see [33, 43, 8]). On the other hand, almost all of the most fundamental problems of computational classical algebraic geometry are proved to be solvable in polynomial space (see e.g. [32, 9, 30, 29, 25]). Thus computational complexity is able to distinguish between geometry and algebra and supports the viewpoint of Kronecker (geometry) against the viewpoint of Hilbert and Macaulay (algebra).

It is well known that Kronecker's personality was highly conflictive for his time. It is less known how much posthumous rejection Kronecker's personality was able to produce. Hilbert's writings are eloquent in this point ("die Kroneckersche Verbotsdiktatur", see [21]), whereas Macaulay's attack against Kronecker's work on elimination was a rather well educated one (see [28], Preface). In this context let us also remind André Weil's "elimination of the elimination theory". Kronecker's radical spirit did not recognise limitations. His radicalism was as universal as his spirit was. Of course he was right requiring that any mathematical reflection has to end up with finitely many and practically realizable computations which settle the concrete (e.g. application) problem under consideration. However declaring the natural numbers as the only mathematical objects created by god for mankind and declaring the "rest"(real, complex numbers, infinite cardinals and ordinals) as devils work, tempting humans to play with the infinite, he demonstrated that he was not able or willing to distinguish between syntaxis and semantics. He was right to require that mathematical expressions (algebra) have always to move within finitary limits, but he was wrong to exclude reflections about infinite mathematical objects (geometry) using a finitarian language. Of course his own work ended up to be godless enough to guarantee him mathematical recognition by his worst adversaries.

Kronecker's own formulation of his elimination method in [24] was imprecise and general enough to allow different interpretations of it, computationally efficient and inefficient ones. Possibly it was in his mind to leave open the door for future complexity issues of his method.

Hilbert's and Macaulay's attacks against Kronecker's method were based on the computationally inefficient interpretation. They noticed that under this interpretation Kronecker's elimination method leads to a hyperexponential swell of intermediate expression size and used this observation for the promotion of their own, more "simple" and "mathematical" point of view. Hilbert and Macaulay's position became finally predominant in the future development of algebraic geometry and commutative algebra (see e.g. [40]). Their ideas led to the modern, computer implemented tool of Gröbner basis algorithms for the symbolic resolution (simplification) of polynomial equation systems. This tool was introduced in the sixties by B. Buchberger (and his school) and represents today the core of all current computer algebra software packages.

The discovery of effective (affine) Nullstellensätze and their application to the complexity analysis of Gröbner basis algorithms for the solution of geometrical problems, represented at the end of the eighties the turning point for a process which led finally back to Kronecker's original ideas. This process was not a conscious motion with clear goals, but rather a slow emerging of mathematical insight and of algorithmic design within the scope of Kronecker's intuitions.

The first step in this direction was even made as part of a mathematical proof and not of an algorithmic design. In its standard interpretation, Kronecker's elimination method relies on an iterated use of resultants of suitable univariate polynomials with parametric coefficients. In fact, a resultant is nothing but the constant term of the characteristic polynomial of a suitable linear map determined by the polynomials under consideration. Replacing in this version of Kronecker's elimination algorithm the occuring resultants just by the constant terms of the corresponding minimal polynomials, one obtains an enormous reduction of degree, height and also of arithmetic circuit (straight-line program) complexity for the polynomials produced during the procedure (see e.g. [4, 5, 16]). By the way, let us remark that Kronecker applies in his method the mentioned simplification, however he omits to draw these important conclusions from his argument.

Other important ingredients of the emerging new algorithmic method were the parametric representation of equidimensional algebraic varieties (a rediscovery of Kronecker's old idea) and the arithmetic circuit (straight-line program) representation of polynomials (which was neither out of the scope of Kronecker's intuition nor clearly included in the main stream of his thinking). The combination of these ingredients produced a considerable effect upon the worst case complexity of symbolic elimination procedures (see e.g. [12, 23, 14]).

Nevertheless all this progress did not suffice to allow the design of practically efficient symbolic elimination algorithms and in particular of algorithms which were able to compete in complexity aspects with their numerical counterparts. The traditional huge gap between symbolic and numeric polynomial equation solving methods remained open. Whereas numeric algorithms are very efficient with respect to the number of arithmetical operations they require, they cannot be efficiently used in case of parametric, underdetermined, overdetermined or degenerate polynomial equation systems. Symbolic algorithms are free from these restrictions but they are also too inefficient for any reasonable use in practice. A way out of this dilemma became apparent in [13, 11] by a new interpretation of Newton's classical method. Interpreting Newton's approximation algorithm as a global procedure instead as a local one, allowed its use as a tool for data compression in the Kronecker–like elimination procedure of [14] (which relied on the arithmetic circuit representation of polynomials). It turns out that Newton's method is well adapted to exact symbolic computation if the correct (seminumerical) data structure is used. In this way a new algorithmic method finally emerged. This method is based on a combination of Kronecker's and Newton's ideas, and is able to distinguish dichotomically between "well behaved" and "badly behaved" polynomial equations systems. Moreover this algorithmic method is optimal for worst case (i.e. generic) systems.

Unlike Gröbner basis algorithms this new method avoids any significant computational overflow during its execution. Roughly speaking, the new algorithms are always polynomial in the output size and even polynomial in the input size, if the given polynomial equation system is "well behaved".

This view of algorithmic algebraic geometry produced also the following new insight:

elimination polynomials are always "smart"(i.e. not easy and not hard) to evaluate. How many variables they ever may contain, their evaluation complexity is always polynomial in their degree (whereas their number of monomials may be exponential in the number of their variables).

Although this insight is beyond of the scope of Kronecker's way of thinking, his formulation of the elimination method indicates that he might have intended to leave the door open for complexity issues.

A further development of this new algorithmic method was able to demonstrate its practical efficiency (see [27] and [31]). Moreover it turns out that the parameters which dominate the complexity of the new symbolic procedures determine also the efficiency of their numerical counterparts (at least if aspects of diophantine approximation are taken into account; see [34]). The new symbolic algorithms (and their numerical counterparts) have still a worst case complexity which is exponential in the (purely syntactical) input length. One may ask whether this fact is due to the algorithms and data structures employed or whether this is due to the intrinsic nature of geometric elimination.

The new results presented in this paper address this question. In order to discuss this point, let us turn back to our interpretation of Kronecker's ideas behind geometric elimination. Kronecker's elimination method (and theory) behaves well under specialisation of the input equations. In fact, at any moment of the procedure one may consider the (parametric) input equations as given by their coefficients and these coefficients may be considered as purely algebraic objects, determined only by their algebraic relations. A given equation system may even be "generalized", i.e. the coefficients of the given input equations may be replaced by indeterminates and the discussion of the solvability of the generalized systems answers all imaginable questions about the solvability of the original system. This concept of specialisation–generalisation reveals an idea of universality (or uniformity) behind Kronecker's elimination theory. This philosophical idea of universality became one of the corner stones of modern algebraic geometry and commutative algebra. Since we are (still) unable to think in a different way, we shall consider the input equations of a parametric elimination problem as functions which may be called by their values in the variables to be eliminated (black-box representation) or simply as being given by their coefficients (formal representation).

Any elimination algorithm we are able to imagine today starts from this kind of data. In other words, the black box representation constitutes today the most general way we may think the equations of our input system to be given. Of course each evaluation of the input equations has its costs and these costs may be measured by the size of a division-free arithmetic circuit which represents the input equations.

In this paper we shall show that any sufficiently uniform elimination procedure (which avoids superfluous branchings) becomes necessarily exponential in worst case, if the input equations are given in black-box representation and if the required output is a canonical elimination polynomial (a "resolvent" in the terminology of Kronecker and Macaulay). This is a general and provable fact for any symbolic as well as for any numerical elimination procedure. We shall also show, that even in case that the input equations are not given by a black box, but by an explicit arithmetic circuit, the same conclusion holds true for any sufficiently universal and uniform elimination procedure which is able to compute efficiently Zariski closures and (generically squarefree) *parametric* greatest common divisors for circuit represented algebraic families of polynomials.

Below we shall give a precise definition of the meaning of a "sufficiently universal and uniform elimination procedure" for the case of a flat family of elimination problems. Such an elimination procedure will be called *parametric.*

If an elimination procedure is used in order to assign "coordinates" (i.e. in order to parametrise) suitable and easy-to-represent families of algebraic varieties the same conclusion holds again, without any further restriction on the input representation (see [6] and [18]). Summing up, we may say: the vision of elimination theory initiated by Kronecker hides a concept of universality and uniformity which obstructs its general efficiency. The question what happens with complexity when we drop this universality and uniformity requirement, exceeds the horizon of todays mathematical thinking and is equivalent to the question whether $P \neq NP$ holds over the complex numbers (in the sense of the BSS complexity model; see [2]).

2 Parametric elimination

2.1 Parametric elimination procedures

The procedures (algorithms) considered in this paper operate with *essentially division-free arithmetic circuits* (straight-line programs) as basic data structures for the representation of inputs and outputs. Such a circuit depends on certain input nodes, labelled by indeterminates over a given ground field k (in the sequel we shall suppose that k is infinite and perfect with algebraic closure $\bar{k}$). These indeterminates are thought to be subdivided into two disjoint sets representing the *parameters* and *variables* of the given circuit. The circuit nodes of indegree zero which are not inputs are labelled 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 labelled by arithmetic operations (addition, subtraction, multiplication and division). The internal nodes of the circuit represent polynomials in the variables of the circuit. The coefficients of these polynomials belong to the *parameter field* K, generated over the ground field k by the parameters of the circuit. This is achieved by allowing in a 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 variables. A circuit which contains only divisions by nonzero elements of k is called *totally division-free.* The output nodes of an essentially division-free circuit may occur labelled by sign marks of the form "$= 0$" or "$\neq 0$" or may remain unlabelled (by sign marks). Thus the given circuit *represents* by means of its labelled output nodes a system of polynomial equations and inequations which determine in their turn a locally closed set (i.e. an embedded affine variety) with respect to the Zariski topology of the affine space of parameter and variable instances. The unlabelled output nodes of the given circuit represent a polynomial application (in fact a morphism of algebraic varieties) which maps this locally closed set into a suitable affine space. We shall interprete 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 an *parametric family of varieties.* The same point of view is applied to the morphism determined by the unlabelled 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 mainly concerned with *sequential* computing *time*, measured by the *size* of the circuit. Occasionally we will also refer to *parallel time*, measured by the *depth* of the circuit. In our main complexity model is the *total* one, where we take into account *all* arithmetic operations (additions, subtractions, multiplications and possibly occuring divisions) at *unit costs.* For purely technical reasons we shall also consider two *non-scalar* complexity models, one over the ground field k and the other one over the parameter 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 only 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. For more details about complexity measures and models we refer to [3].

Given an essentially division-free arithmetic circuit as input, an *elimination problem* consists in the task of finding an essentially division-free output circuit which describes the Zariski closure of the image of the morphism determined by the input circuit. The output circuit and the corresponding algebraic variety are also called a *solution* of the given elimination problem. We say that a given parameter point fixes an *instance* of the elimination problem under consideration. In this sense a problem instance is described by an input and an output (solution) instance.

In this paper we restrict our attention to input circuits which are totally division-free and contain only output nodes labelled by "=0" and unlabelled output nodes. Mostly our output circuits will also be totally division-free and will contain only one output node, labelled by the mark "=0". This output node will always represent a canonical elimination polynomial associated to the elimination problem under consideration (see Section 2.2 for more details).

In case that our output circuit contains divisions (depending only on parameters but not on variables), we require to be able to perform these divisions for any problem instance. In order to make this requirement sound, we admit in our algorithmic model certain limit processes in the spirit of de l'Hôpital's rule (below we shall modelise these limit processes algebraically, in terms of places and valuations). The restriction we impose on the possible divisions in an output circuit represents a *first* fundamental geometric *uniformity requirement* for our algorithmic model.

An algorithm which solves a given elimination problem may be considered as a (geometric) elimination procedure. However this simple minded notion is too restrictive for our purpose of showing lower complexity bounds for elimination problems. It is thinkable that there exists for every individual elimination problem an efficient ad hoc algorithm, but that there is no universal way to find and to represent all these ad hoc procedures. Therefore, a *geometric elimination procedure* in the sense of this paper will satisfy certain uniformity and universality requirements which we are going to explain now.

We modelise our elimination procedures by families of *arithmetic networks* (also called arithmetic-boolean circuits) which solve entire classes of elimination problems of *arbitrary* input size (see [41], [42]). In this sense we shall require the *universality* of our geometric elimination procedures. Moreover, we require that our elimination procedures should be essentially division-free.

In a universal geometric elimination procedure, branchings and divisions by intermediate results (that involve only parameters, but not variables) cannot be avoided. From our elimination procedures we shall require to be *parsimonious* with respect to *branchings* (and divisions). In particular we shall require that our elimination procedures do not introduce branchings and divisions for the solution of a given elimination problem when traditional algorithms do not demand this (an example of such a situation is given by the flat families of elimination problems we are going to consider in the sequel). This restriction represents a *second* fundamental *uniformity requirement* for our algorithmic model.

We call a universal elimination procedure *parametric* if it satisfies our first and second uniformity requirement, i.e. if the procedure does not contain branchings which otherwise could be avoided and if all possibly occurring divisions can be performed on all problem instances, in the way we have explained before. In this paper we shall only consider parametric elimination procedures.

We call a parametric elimination procedure *geometrically robust* if it produces for any input instance an output circuit which depends only on the mathematical objects "input equation system" and "input morphism" but not on their circuit representation. We shall apply this notion only to elimination problems given by (geometrically or scheme-theoretically) flat families of algebraic varieties. This means informally that a parametric elimination procedure is geometrically robust if it produces for flat families of problem instances "continuous" solutions.

Of course, our notion of geometric robustness depends on the (geometric or scheme-theoretical) context, i.e. it is not the same for schemes or varieties. In Section 2.2 we shall explain our idea of geometric robustness in the typical situation of flat families of algebraic varieties given by reduced complete intersections.

Traditionally, the size of a system of polynomial equations (and inequations) is measured in purely extrinsic, syntactic terms (e.g. number of parameters and variables, degree of the input polynomials, size and depth of the input circuit etc). However, there exists a new generation of symbolic and numeric algorithms which take also into account intrinsic, semantic (e.g. geometric or arithmetic) invariants of the input equation system in order to measure the complexity of elimination procedure under consideration more accurately (see e.g. [13, 11, 15] and [38, 39]).

In this paper we shall turn back to the traditional point of view. In Theorem 5 we shall show that, under our universality and uniformity restrictions, *no parametric elimination procedure which includes efficient computation of Zariski closures and of generically squarefree parametric greatest common divisors for circuit represented algebraic families of polynomials, is able to solve an arbitrary elimination problem in polynomial (sequential) time, if time is measured in terms of circuit size and input length is measured in syntactical terms only.*

Finally let us refer to the books [3], [35] and [37] as a general background for notions of algebraic complexity theory and algebraic geometry we are going to use in this paper.

2.2 Flat families of 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 $G_1, \ldots, G_n$ and F be polynomials belonging to the k-algebra $k[U_1, \ldots, U_r, X_1, \ldots, X_n]$. Suppose that the polynomials $G_1, \ldots, G_n$ form a regular sequence in $k[U_1, \ldots, U_r, X_1, \ldots, X_n]$ defining thus an equidimensional subvariety $V := \{G_1 = 0, \ldots, G_n = 0\}$ of the $(r+n)$-dimensional affine space $\mathbb{A}^r \times \mathbb{A}^n$ over the field $\bar{k}$. The algebraic variety V has dimension r. Let δ be the (geometric) degree of V as defined in [17] (this degree does not take into account multiplicities or components at infinity). Suppose furthermore that the morphism of affine varieties $\pi : V \longrightarrow \mathbb{A}^r$, 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 $k[U_1, \ldots, U_r, X_1, \ldots, X_n]$ is radical). Let $\tilde{\pi} : V \longrightarrow \mathbb{A}^{r+1}$ 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 $k[U_1, \ldots, U_r, Y]$ 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 $P(U_1, \ldots, U_r, F)$ vanishes on the variety V.

Let us consider an arbitrary point $u = (u_1, \ldots, u_r)$ of $\mathbb{A}^r$. For arbitrary polynomials $A \in k[U_1, \ldots, U_r, X_1, \ldots, X_n]$ and $B \in k[U_1, \ldots, U_r, Y]$ 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 $k(u_1, \ldots, u_r)[X_1, \ldots, X_n]$ and $k(u_1, \ldots, u_r)[Y]$ respectively. Similarly we denote for an arbitrary polynomial $C \in k[U_1, \ldots, U_r]$ by $C^{(u)}$ the value $C(u_1, \ldots, u_r)$ which belongs to the field $k(u_1, \ldots, u_r)$. 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 (cardinality) of $V^{(u)}$ is bounded by δ. Denote by $\tilde{\pi}^{(u)} : V^{(u)} \longrightarrow \mathbb{A}^1$ the morphisms 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 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* (see Section 2.1). 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.

The *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 $A \in k[U_1, \ldots, U_r, X_1, \ldots, X_n]$, $B \in k[U_1, \ldots, U_r, Y]$ and $C \in k[U_1, \ldots, U_r]$ *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.

An arithmetic circuit in $k[U_1, \ldots, U_r, Y]$ *with scalars in* $k[U_1, \ldots, U_r]$ is a totally division-free arithmetic circuit in $k[U_1, \ldots, U_r, Y]$, say β, modelised in the following way: β is given by a directed acyclic graph whose internal nodes are labelled as before by arithmetic operations. There is only one input node of β, labelled by the variable Y. The other nodes of indegree zero the circuit β may contain, are labelled by arbitrary elements of $k[U_1, \ldots, U_r]$. These elements are considered as the *scalars of* β. We call such an arithmetic circuit β *invariant* (with respect to the equivalence relation $\sim$) if all its scalars are invariant polynomials of $k[U_1, \ldots, U_r]$. Considering instead of Y the variables $X_1, \ldots, X_n$ as inputs, one may analogously define the notion of an arithmetic circuit in $k[U_1, \ldots, U_r, X_1, \ldots, X_n]$ with scalars in $k[U_1, \ldots, U_r]$ and the meaning of its invariance. However, typically we shall limit ourselves to circuits in $k[U_1, \ldots, U_r, Y]$ with scalars in $k[U_1, \ldots, U_r]$.

We are now ready to characterise in the given situation what we mean by a *geometrically robust parametric elimination procedure.* Suppose that the polynomials $G_1, \ldots, G_n$ and F are given by a totally division-free arithmetic circuit β in $k[U_1, \ldots, U_r, X_1, \ldots, X_n]$. A geometrically robust parametric elimination procedure accepts the circuit β as input and produces as output an *invariant* circuit Γ in $k[U_1, \ldots, U_r, Y]$ with scalars in $k[U_1, \ldots, U_r]$, such that Γ represents the polynomial P. Observe that in our definition of geometric robustness we did not require that β is an invariant circuit because this would be too restrictive for the modelling of concrete situations in computational elimination theory.

The invariance property required for the output circuit Γ means the following: let $u = (u_1, \ldots, u_r)$ be a parameter point of $\mathbb{A}^r$ and let $\Gamma^{(u)}$ be the arithmetic circuit in $k(u_1, \ldots, u_r)[Y]$ obtained from the circuit Γ evaluating in the point u the elements of $k[U_1, \ldots, U_r]$ which occur as scalars of Γ. Then the invariance of Γ means that the circuit $\Gamma^{(u)}$ depends only on the particular *problem instance* determined by the parameter point u but not on u itself. Said otherwise, a geometrically robust 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.

By definition, a geometrically robust parametric elimination procedure produces always the *general* solution of the flat family of elimination problems under consideration. This means that for flat families, geometrically robust parametric elimination procedures do not introduce branchings in the output circuits. In Section 3.1 we shall exhibit a complexity result which may be paraphrased as follows: *within the standard philosophy of commutative algebra, none of the known (exponential time) parametric elimination procedures can be improved to a polynomial time algorithm.* For this purpose it is important to remark that the known *parametric* elimination procedures (which are without exception based on linear algebra as well as on comprehensive Gröbner basis techniques) are all geometrically robust.

The invariance property of these procedures is easily verified in the situation of a flat family of elimination problems. One has only to observe that all known elimination procedures accept the input polynomials $G_1, \ldots, G_n$ and F in their dense or sparse *coefficient representation* or as *evaluation black box* with respect to the variables $X_1, \ldots, X_n$.

Finally we are going to explain what we mean by a *(generically squarefree) parametric greatest common divisor of an algebraic family of polynomials* and by the problem of the computation of this greatest common divisor (in case of a circuit represented family).

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 thet there exists an index $1 \leq k \leq s$ with $b_k \neq 0$. Without loss of generality we may suppose that for some index $1 \leq m \leq s$ the polynomials $b_1, \ldots, b_m$ are exactly the non–zero elements of $b_1, \ldots, b_s$. Observe that each polynomial $b_1, \ldots, b_s$ has positive degree (in the variable Y).

We consider $b_1, \ldots, b_m$ as an *algebraic family of polynomials* (in the variable Y) and $B_1, \ldots, B_m$ as their representatives. The polynomials $b_1, \ldots, b_m$ have in $k(S)[Y]$ a well defined *normalised* (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 $b_1, \ldots, b_m$.

Our first requirement is $D \geq 1$.

Let us fix for the moment an arbitrary point $u \in S$. The evaluation in u determines a canonical k–algebra homomorphism $\phi_u : k[S] \longrightarrow \bar{k}$. Let $\phi : k(S) \longrightarrow \bar{k} \cup \{\infty\}$ be any *place* which extends the homomorphism ϕ_u (this means that the valuation ring of ϕ contains the local ring of the point u in the variety S and that the residue class of ϕ is contained in $\bar{k}$).

We require now that the place ϕ takes only *finite* values (i.e. values of

$\bar{k}$) in the coefficients of the polynomial h (recall that these coefficients belong to the field $k(S)$).

Moreover we require that the values of the place ϕ in these coefficients *depend only on the point* u and not on the particular choice of the place ϕ extending the homomorphism ϕ_u.

In this way the place ϕ maps the polynomial h to a monic polynomial of degree D in Y with coefficients in $\bar{k}$. 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 $1 \leq k \leq m$.

Finally we require that the polynomials $b_1(u)(Y), \ldots, b_m(u)(Y)$ of $\bar{k}(Y)$ are not all zero and that their (normalized) greatest common divisor is divisible by $h(u)(Y)$.

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 coefficienst of h (with respect to the varable 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 call h a *parametric greatest common divisor of the algebraic family of polynomials* $b_1, \ldots, b_m \in k[S][Y]$. 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 $\hat{h} \in k(S)[Y]$ with the same zeroes as h in an algebraic closure of $k(S)$, is called a *generically squarefree* parametric greatest common divisor of the algebraic family $b_1, \ldots, b_m \in k[S][Y]$.

If the characteristic of the ground field k is zero, such a generically squarefree parametric greatest common divisor $\hat{h}$ always exists and has the same properties as h with respect to the places $\phi : k(S) \longrightarrow \bar{k} \cup \{\infty\}$ considered before.

If the characteristic of k is positive, this general conclusion is not true anymore. However, in the purely geometric context of the present paper, we may always arrange the polynomials $B_1, \ldots, B_s$ and their arithmetic circuits in order to assure the existence of a generically squarefree greatest common divisor. For this purpose we need that k is a perfect field.

In case that a generically squarefree greatest common divisor $\hat{h}$ exists, the notion of a representative of $\hat{h}$ is defined in the same way as for h.

Suppose now that the polynomials $B_1, \ldots, B_s$ are given by a totally division–free arithmetic circuit β_* in $k[U_1, \ldots, U_r, Y]$.

We are now going to formulate the algorithmic problem of computing the (generically square–free) parametric greatest common divisor h (or $\hat{h}$) of the algebraic family of polynomials $b_1, \ldots, b_m \in k[S][Y]$.

We consider Y as variable and $U_1, \ldots, U_r$ as parameters. We are looking for an essentially division–free arithmetic circuit Γ_* in $k(U_1, \ldots, U_r)[Y]$ which computes a representative of the (generically square–free) parametric greatest common divisor h (or $\hat{h}$), associated to the polynomials $B_1, \ldots, B_s$.

We require that the scalars of Γ_* induce well–defined rational functions of the variety S and that for any point $u \in S$ and any place $\phi : k(S) \longrightarrow \bar{k} \cup \{\infty\}$ extending the homomorphism $\phi_u : k[S] \longrightarrow \bar{k}$ the following condition is satisified:

any scalar of the arithmetic circuit Γ_* induces a rational function of the variety S, which is mapped by ϕ into a *finite* value of $\bar{k}$. This value is *uniquely* determined by the point $u \in S$.

The problem of computing the (generically square–free) parametric greatest common divisor of the algebraic family of polynomials $b_1, \ldots, b_m \in k[S][Y]$ consists now in producing from the input circuit β_* a (smallest possible) circuit Γ_* which satisfies the requirement above.

Observe that the scalars of such a circuit Γ_*, as well as the coefficients of h, are rational functions of the variety S which belong to the integral closure of $k[S]$ in the function field $k(S)$. This property of Γ_* is conserved under specialisations of the k–algebra $k[S]$.

In the proof of Theorem 5 we shall make substantial use of this observation.

For general background and details about places and valuation rings we refer to [26].

3 The intrinsic complexity of parametric elimination procedures

3.1 A particular flat family of elimination problems

Let n be a fixed natural number and let T, $U_1, \ldots, U_n$, $X_1, \ldots, X_n$ and Y be indeterminates over $\mathbb{Q}$. In the sequel we are going to 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 be the following polynomial of $\mathbb{Q}[T, U_1, \ldots, U_n, Y]$:

$$P(T, U_1, \ldots, U_n, Y) := \prod_{j=0}^{2^n-1} \big(Y - (j + T \prod_{i=1}^{n} U_i^{[j]_i})\big). \tag{3.1}$$

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

$$P(T, U_1, \ldots, U_n, Y) = Y^{2^n} + A_1 Y^{2^n-1} + \cdots + A_{2^n},$$

where $A_1, \ldots, A_{2^n}$ are suitably defined polynomials of $\mathbb{Q}[T, U_1, \ldots, U_n]$.

Let $1 \leq k \leq 2^n$. In order to determine the polynomial A_k, we observe, by expanding the right hand side of (3.1), that A_k 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 A_k can be expressed as follows:

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

Observe that for $0 \leq j_1 < \cdots < j_k \leq 2^n - 1$ 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 A_k has the form:

$$\begin{aligned} A_k = & \sum_{0 \leq j_1 < \cdots < j_k \leq 2^n-1} j_1 \cdots j_k \\ & + T \left(\sum_{0 \leq j_1 < \cdots < j_k \leq 2^n-1} \sum_{h=1}^{k} j_1 \cdots \widehat{j_h} \cdots j_k \prod_{i=1}^{n} U_i^{[j_h]_i} \right) \qquad (3.2) \\ & + \text{terms of higher degree in } T. \end{aligned}$$

Let us denote by L_k the coefficient of T in the representation (3.2), namely:

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

For later use we are now going to show the following result, for whose proof we are indebted to G. Matera.

Lemma 1 *The polynomials $L_1, \ldots, L_{2^n}$ are $\mathbb{Q}$-linearly independent in $\mathbb{Q}[U_1, \ldots, U_n]$.*

Proof Let us abbreviate $N := 2^n - 1$. 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

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

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 1. By our claim there exist for arbitrary $1 \leq k \leq N+1$ integers $c_0^{(k)}, \cdots, c_{k-1}^{(k)}$ with $c_{k-1}^{(k)} \neq 0$ 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 $P_k := \sum_{0\leq j\leq N} j^k \prod_{i=1}^n U_i^{[j]_i}$ 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 $P_0, \ldots, P_N$ are $\mathbb{Q}$-linearly independent. Therefore the $\mathbb{Q}$-vector space generated by $L_1, \ldots, L_{N+1}$ in $\mathbb{Q}[U_1, \ldots, U_n]$ has dimension $N+1 = 2^n$. This implies that $L_1, \ldots, L_{2^n}$ are $\mathbb{Q}$-linearly independent. □

With the notations of Section 2.2, put now $r := n+1$, $T := U_{n+1}$ and let us consider the following polynomials of $\mathbb{Q}[T, U_1, \ldots, U_n, X_1, \ldots, X_n]$:

$$G_1 := {X_1}^2 - X_1, \ldots, G_n := {X_n}^2 - X_n \quad \text{and}$$
$$F := \sum_{i=1}^n 2^{i-1}X_i + T\prod_{i=1}^n (1 + (U_i - 1)X_i). \tag{3.3}$$

It is clear from their definition that the polynomials $G_1, \ldots, G_n$ and F can be evaluated by a (non-invariant) totally division-free arithmetic circuit β of size $O(n)$ in $\mathbb{Q}[T, U_1, \ldots, U_n, X_1, \ldots, X_n]$. Observe that the polynomials $G_1, \ldots, G_n$ do not depend on the $T, U_1, \ldots, U_n$ and that their degree is two. The polynomial F is of degree $2n + 1$. More precisely, we have $\deg_{X_1,\dots,X_n} F = n$, $\deg_{U_1,\dots,U_n} F = n$, and $\deg_T F = 1$. Although the polynomial F can be evaluated using $O(n)$ arithmetic operations, the sparse representation of F, as a polynomial in the variables $T, U_1, \dots, U_n, X_1, \dots, X_n$, contains asymptotically 2^n non-zero monomial terms.

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

The variety $V := \{G_1 = 0, \dots, G_n = 0\}$ 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 any 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 generically unramified. In particular π has constant fibres which are all canonically isomorphic to the hypercube $\{0,1\}^n$. Let $(j_1, \dots, j_n)$ be an arbitrary point of $\{0,1\}^n$ and let $j := \sum_{1 \le i \le n} j_i 2^{i-1}$ be the integer $0 \le j < 2^n$ whose bit representation is $j_n j_{n-1} \cdots j_1$. One verifies immediately the identity

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

Therefore for any point $(t, u_1, \dots, u_n, j_1, \dots, j_n) \in V$ with $j := \sum_1^n j_i 2^{i-1}$ we have

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

¿From this observation we deduce easily that the polynomial

$$P \in \mathbb{Q}[T, U_1, \dots, U_n, Y]$$

we are looking for (as the elimination polynomial associated to the flat family $G_1, \dots, G_n, F$) is in fact

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

With the notations of the beginning of this section, this polynomial has the form

$$P = Y^{2^n} + \sum_{1 \le k \le 2^n} A_k Y^{2^n - k} \equiv Y^{2^n} + \sum_{1 \le k \le 2^n} (a_k + T L_k) Y^{2^n - k} \text{ modulo } T^2, \tag{3.4}$$

with $a_k := \sum_{1\leq j_1<\ldots<j_k\leq 2^n-1} j_1\cdots j_k$ for $1 \leq k \leq 2^n$.

Suppose now that there is given a geometrically robust parametric elimination procedure. This procedure produces from the input circuit β an invariant arithmetic circuit Γ in $\mathbb{Q}[T, U_1, \ldots, U_n, Y]$, with scalars in $\mathbb{Q}[T, U_1, \ldots, U_n]$, which evaluates the polynomial P. Recall that the invariance of Γ means that the scalars of Γ are invariant polynomials of $\mathbb{Q}[T, U_1, \ldots, U_n]$, say $\Omega_1, \ldots, \Omega_N$.

Let $\mathcal{L}(\Gamma)$ be the total and $L(\Gamma)$ the non-scalar size of the arithmetic circuit Γ over $\mathbb{Q}[T, U_1, \ldots, U_n]$. Without loss of generality we have $L(\Gamma) \leq \mathcal{L}(\Gamma)$ and $N \leq (L(\Gamma) + 3)^2$.

Let $Z_1, \ldots, Z_N$ be new indeterminates. From the graph structure of the circuit Γ we deduce that there exists for each $1 \leq k \leq 2^n$ a polynomial $Q_k \in \mathbb{Q}[Z_1, \ldots, Z_N]$ satisfying the condition

$$Q_k(\Omega_1, \ldots, \Omega_N) = A_k \tag{3.5}$$

(see [3] for details). Let us now consider two arbitrary elements $u, u' \in \mathbb{A}^n$. Observe that the parameter points $(0, u)$ and $(0, u')$ of $\mathbb{A}^{n+1}$ are equivalent (in symbols: $(0, u) \sim (0, u')$). From the invariance of $\Omega_1, \ldots, \Omega_N$ we deduce therefore that $\Omega_j(0, u) = \Omega_j(0, u')$ holds for any $1 \leq j \leq N$. This means that the polynomials

$$\omega_1 = \Omega_1(0, U_1, \ldots, U_n), \ldots, \omega_N := \Omega_N(0, U_1, \ldots, U_n)$$

are independent from the variables $U_1, \ldots, U_n$ and therefore elements of $\mathbb{Q}$. From identity (3.4) we conclude that the same is true for $\alpha_1 := A_1(0, U_1, \ldots, U_n), \ldots, \alpha_{2^n} := A_{2^n}(0, U_1, \ldots, U_n)$. We shall abbreviate $\omega := (\omega_1, \ldots, \omega_N)$ and $\alpha := (\alpha_1, \ldots, \alpha_{2^n})$.

Let us consider the morphisms of affine spaces $\mu : \mathbb{A}^{n+1} \longrightarrow \mathbb{A}^N$ and $\psi : \mathbb{A}^N \longrightarrow \mathbb{A}^{2^n}$ given by $\mu := (\Omega_1, \ldots, \Omega_N)$ and $\psi := (Q_k)_{1\leq k\leq 2^n}$.

Observe that

$$\psi \circ \mu = (Q_k(\Omega_1, \ldots, \Omega_N))_{1\leq k\leq 2^n} = (A_k)_{1\leq k\leq 2^n}$$

holds. From our previous considerations we deduce the identities

$$\begin{aligned} &(\psi \circ \mu)(0, U_1, \ldots, U_n) \\ &= (Q_k(\Omega_1(0, U_1, \ldots, U_n), \ldots, \Omega_N(0, U_1, \ldots, U_n)))_{1\leq k\leq 2^n} \\ &= (Q_k(\omega))_{1\leq k\leq 2^n}. \end{aligned}$$

In particular we have $\psi(\omega) = \alpha$.

We analyse now the local behaviour of the morphism ψ in the point

$\omega \in \mathbb{A}^N$. Let E_ω and E_α be the tangent spaces of the points $\omega \in \mathbb{A}^N$ and $\alpha \in \mathbb{A}^{2^n}$. Let us denote the differential of the map ψ in the point ω by $(D\psi)_\omega : E_\omega \longrightarrow E_\alpha$. Taking the canonical projections of $\mathbb{A}^N$ and $\mathbb{A}^{2^n}$ as local coordinates in the points ω and α respectively, we identify E_ω with $\mathbb{A}^N$ and E_α with $\mathbb{A}^{2^n}$.

For any point $u \in \mathbb{Q}^n$ we consider the parametric algebraic curves $\gamma_u : \mathbb{A}^1 \longrightarrow \mathbb{A}^N$ and $\delta_u : \mathbb{A}^1 \longrightarrow \mathbb{A}^{2^n}$ defined as

$$\gamma_u := (\Omega_1(T,u),\dots,\Omega_N(T,u)) \text{ and } \delta_u := (A_k(T,u))_{1\le k\le 2^n}.$$

Observe that $\psi \circ \gamma_u = \delta_u$ and that $\gamma_u(0) = \omega$, $\delta_u(0) = \alpha$ holds (independently of the point u).

Now fix $u \in \mathbb{Q}^n$ and consider

$$\gamma_u'(0) = (\frac{\partial\Omega_1}{\partial T}(0,u),\dots,\frac{\partial\Omega_N}{\partial T}(0,u)) \text{ and } \delta_u'(0) = (\frac{\partial A_k}{\partial T}(0,u))_{1\le k\le 2^n}.$$

We have $\gamma_u'(0) \in E_\omega$ and $\delta'(0) \in E_\alpha$. ¿From (3.4) we deduce that for any $1 \le k \le 2^n$ the identity $\frac{\partial A_k}{\partial T}(0,u)) = L_k(u)$ holds. Therefore we have $\delta_u'(0) = (L_k(u))_{1\le k\le 2^n}$. This implies

$$(D\psi)_\omega(\gamma_u'(0)) = \delta_u'(0) = (L_k(u))_{1\le k\le 2^n}. \tag{3.6}$$

holds. From Lemma 1 we deduce that there exist for $1 \le l \le 2^n$ rational points $u_l \in \mathbb{Q}^n$ such that the matrix $(L_k(u_l))_{1\le k,l\le 2^n}$ is regular. From (3.6) we deduce now that the $2^n \times N$-matrix built by the row vectors $\gamma_{u_1}'(0),\dots,\gamma_{u_{2^n}}'(0)$ has rank at least 2^n. This implies the lower bound $N \ge 2^n$.

Therefore we have $2^n \le N \le (L(\Gamma)+3)^2$ and hence the estimate $2^{\frac{n}{2}} - 3 \le L(\Gamma) \le \mathcal{L}(\Gamma)$. *We have therefore shown that any geometrically robust parametric elimination procedure applied to the flat family of elimination problems (3.3) produces a solution circuit of size at least* $2^{\frac{n}{2}} - 3$*, i.e. a circuit of exponential size in the length* $O(n)$ *of the input.*

¿From the previous example we deduce that the goal of a polynomial time procedure for geometric (or algebraic) elimination can not be reached just by means of an improvement of known, commutative algebra-based elimination methods.

On the other hand, our proof method is not very specific for elimination problems. This can be visualised by the following example:

let $\mathcal{A}$ be the $\mathbb{Q}$–subalgebra of $\mathbb{Q}[T,U_1,\dots,U_n]$ generated by the coefficients of the polynomial F of (3.3) with respect to the variables $X_1,\dots,X_n$. In the same manner as above, one may show that in the non–scalar complexity model with respect to $\mathcal{A}$, any totally division–free arithmetic circuit which evaluates the polynomial F using only scalars from the $\mathbb{Q}$–algebra $\mathcal{A}$, has necessarily exponential size in n.

On the other hand, the polynomial F can be evaluated by a totally division–free arithmetic circuit in $\mathbb{Q}[T, U_1, \ldots, U_n, X_1, \ldots, X_n]$ of size $O(n)$.

Therefore we see that in the non-scalar model the (sequential time) complexity of a polynomial depends strongly on the structure of the algebra of scalars.

It was fundamental for our argumentation above that our notion of a *geometrically robust parametric elimination procedure* excludes branchings and divisions in the output program. We resume the conclusions from the complexity discussion of our example in the following form.

Theorem 2 (**[18]**) *For any $n \in \mathbb{N}$ there exists a flat family of elimination problems depending on $n+1$ parameters and n variables over $\mathbb{Q}$ and having input length $O(n)$, such that the following holds: any geometrically robust parametric elimination procedure which solves this problem produces an output circuit of size at least $2^{\frac{n}{2}} - 3$ (i.e. of exponential size in the input length).*

3.2 Circuit encoding of polynomials

We are now going to explain how we may encode polynomials of a certain complexity class by their values in suitable test sequences.

Let L and n be given natural numbers which we think fixed for the moment and let $X_1, \ldots, X_n$ be indeterminates over $\bar{k}$. In this section we shall only consider totally division-free arithmetic circuits in $\bar{k}[X_1, \ldots, X_n]$ and we shall only consider the non-scalar sequential complexity model over $\bar{k}$.

By $\mathcal{H} := \mathcal{H}_{L,n}$ we denote the *complexity class* of all polynomials $H \in \bar{k}[X_1, \ldots, X_n]$ which can be evaluated by a totally division-free arithmetic circuit in $\bar{k}[X_1, \ldots, X_n]$ of size at most L.

For any polynomial $H \in \mathcal{H}$ we have $\deg H \leq 2^L$. On the other hand we have e.g. $X_1^{2^L} \in \mathcal{H}$. This implies that 2^L is an *exact* degree bound for the elements of $\mathcal{H}$. Let $D := 2^L + 1$. Since the elements of $\mathcal{H}$ are contained in the D-dimensional $\bar{k}$-linear subspace of $\bar{k}[X_1, \ldots, X_n]$ consisting of the polynomials of degree at most $2^L = D - 1$, we may consider $\mathcal{H}$ as a subset of $\mathbb{A}^D$. Observe that for any $H \in \mathcal{H}$ and any $\alpha \in \bar{k}$ the element αH belongs to $\mathcal{H}$. Let $\mathcal{W} := \mathcal{W}_{L,n}$ be the Zariski closure of $\mathcal{H} := \mathcal{H}_{L,n}$ in $\mathbb{A}^D$. Since $\mathcal{H}$ is a cone over $\bar{k}$, the same is true for $\mathcal{W}$. On the other hand,

$\mathcal{H}$ is the image of a k-definable morphism of affine spaces $\mathbb{A}^{(L+3)^2} \longrightarrow \mathbb{A}^D$. Thus, in conclusion, W is an *irreducible* algebraic variety of $\mathbb{A}^D$, definable by *homogeneous* polynomials belonging to $k[X_1, \ldots, X_n]$ (see [3], Chapter 9 for details).

In the sequel we shall interprete the points of $\mathbb{A}^D$ as polynomials of $\bar{k}[X_1, \ldots, X_n]$ having degree at most $D-1$ and viceversa. In particular we shall interprete the points of $\mathcal{W}$ as polynomials.

Definition 1 *Let be given a sequence of points $\gamma_1, \ldots, \gamma_m \in k^n$ and let $\gamma := (\gamma_1, \ldots, \gamma_m)$. Let us call m the length of γ.*

(i) *We call γ a correct test sequence for the polynomials of*

$$\bar{k}[X_1, \ldots, X_n]$$

of non-scalar complexity at most L (i.e. for $\mathcal{H}_{L,n}$), if for any $H \in \mathcal{W}_{L,n}$ the following implication holds:

$$H(\gamma_1) = 0, \ldots, H(\gamma_m) = 0 \Longrightarrow H = 0.$$

(ii) *We call γ an identification sequence for the polynomials of*

$$\bar{k}[X_1, \ldots, X_n]$$

of non-scalar complexity at most L (i.e. for $\mathcal{H}_{L,n}$), if for any two elements H_1, H_2 of $\mathcal{W}_{L,n}$ the following implication holds:

$$H_1(\gamma_1) = H_2(\gamma_1), \ldots, H_1(\gamma_m) = H_2(\gamma_m) \Longrightarrow H_1 = H_2.$$

Although the polynomials of the complexity class $\mathcal{H}_{L,n}$ may have exponential degree 2^L, there exist short identification sequences for $\mathcal{H}_{L,n}$. This is the content of the next result.

Lemma 3 ([20, 23]) *Let the notation be as before. Let $M \subseteq k$ be a finite set of cardinality at least $4LD^2$ and let $m := 6(2L+n+1)^2$. The there exist points $\gamma_1, \ldots, \gamma_m \in M^n$ such that $\gamma := (\gamma_1, \ldots, \gamma_m)$ is an identification sequence for $\mathcal{H}_{L,n}$. Suppose that the points of M^n are equidistributed. The probability of finding by a random choice such an identification sequence is at least $(1 - 4LD^{-12(2L+n+1)^2}) > 1/2$.*

Proof From [20, 23] we deduce that there exist in M^n correct test sequences of length $m := 6(2L+n+1)^2$ for $\mathcal{H}_{2L,n}$ and that such a correct test sequence can be found with probability of success $(1 - 4LD^{-12(2L+n+1)^2})$ by a random choice in M^n.

Let $\gamma := (\gamma_1, \ldots, \gamma_m) \in k^{m \times n}$ be a correct test sequence for $\mathcal{H}_{2L,n}$. Let $H_1, H_2 \in \mathcal{W}_{L,n}$ and suppose that

$$H_1(\gamma_1) = H_2(\gamma_1), \ldots, H_1(\gamma_m) = H_2(\gamma_m)$$

holds. Observe that $H := H_2 - H_1$ belongs to $\mathcal{W}_{2L,n}$. Therefore we have $H(\gamma_1) = 0, \ldots, H(\gamma_m) = 0$, and, since γ is a correct test sequence for $\mathcal{H}_{2L,n}$, we may conclude $H = H_2 - H_1 = 0$. □

Let now $m := 6(2L + n + 1)^2$. Then, by Lemma 3, we may fix an identification sequence $\gamma := (\gamma_1, \ldots, \gamma_m) \in k^{m \times n}$ for the complexity class $\mathcal{H} = \mathcal{H}_{L,n}$. Let $S_1, \ldots, S_m$ be new indeterminates denoting the canonical coordinate functions of $\mathbb{A}^m$. We are going to consider the morphism $\sigma_{L,n}^{(\gamma)} : \mathcal{W}_{L,n} \longrightarrow \mathbb{A}^m$, defined for $H \in \mathcal{W}_{L,n}$ by $\sigma_{L,n}^{(\gamma)}(H) := (H(\gamma_1), \ldots, H(\gamma_m))$. Let $\mathcal{S}_{L,n}^{(\gamma)}$ be the Zariski closure of the image of the morphism $\sigma_{L,n}^{(\gamma)}$ and let us abbreviate $\sigma := \sigma_{L,n}^{(\gamma)}$ and $\mathcal{S} := \mathcal{S}_{L,n}^{(\gamma)}$.

Since the variety $\mathcal{W}$ and the morphism $\sigma : \mathcal{W} \longrightarrow \mathcal{S}$ are k-definable, we conclude that $\mathcal{S}$ is k-definable too. Moreover for any polynomial $H \in \mathcal{W}$ and any value $\alpha \in \bar{k}$ we have

$$\sigma(\alpha H) = (\alpha H(\gamma_1), \ldots, \alpha H(\gamma_m)) = \alpha \sigma(H)$$

and from this *homogeneity* property of σ we conclude that $\mathcal{S}$ is a *cone* over the field $\bar{k}$. Therefore $\mathcal{S}$ is definable by *homogeneous* polynomials belonging to $k[S_1, \ldots, S_m]$. Since the variety $\mathcal{W}$ is irreducible and $\mathcal{S}$ is the closure of the image of σ, we conclude that $\mathcal{S}$ is irreducible too.

By assumption $\gamma := (\gamma_1, \ldots, \gamma_m)$ is an identification sequence for the complexity class $\mathcal{H} = \mathcal{H}_{L,n}$. Therefore we conclude that $\sigma : \mathcal{W} \longrightarrow \mathcal{S}$ is an *injective,* dominant morphism. Hence σ is *birational.*

Let $\sigma = (\sigma_1, \ldots, \sigma_m)$ where $\sigma_1, \ldots, \sigma_m$ are suitable coordinate functions of the affine variety $\mathcal{W}$. Let us consider $\mathcal{W}$ as a closed subvariety of the affine space $\mathbb{A}^D$. We recall that the points of $\mathbb{A}^D$ correspond to the polynomials of $\bar{k}[X_1, \ldots, X_n]$ of degree at most D and that the morphism σ is defined by means of the evaluation of the polynomials of $\mathcal{W}$ in the points $\gamma_1, \ldots, \gamma_m$. This implies that there exist *linear forms* in the coordinate ring of $\mathbb{A}^D$ such that $\sigma_1, \ldots, \sigma_m$ are the restrictions of these linear forms to the variety $\mathcal{W}$. From the injectivity of σ we deduce that $\mathcal{W} \cap \{\sigma_1 = 0, \ldots, \sigma_m = 0\}$ contains only the origin of $\mathbb{A}^D$. This implies that the homogeneous map σ induces a finite morphism between the projective varieties associated to the cones $\mathcal{W}$ and $\mathcal{S}$. In fact, the standard proof of this classical result implies something more, namely that also the morphism $\sigma : \mathcal{W} \longrightarrow \mathcal{S}$ is *finite* (see [37] I.5.3, Theorem

8 and proof of Theorem 7). In particular, σ is a surjective, closed map and hence a homeomorphism with respect to the Zariski topologies of $\mathcal{W}$ and $\mathcal{S}$.

Thus we have shown the following result:

Lemma 4 *Let notations be as before and let* $m := 6(2L + n + 1)^2$. *Suppose that there is given an identification sequence* $\gamma := (\gamma_1, \ldots, \gamma_m) \in k^{m \times n}$ *for the complexity class* $\mathcal{H}_{L,n}$ *and let* $\sigma_{L,n}^{(\gamma)} : \mathcal{W}_{L,n} \longrightarrow \mathcal{S}_{L,n}^{(\gamma)}$ *be the morphism of affine varieties associated to the identification sequence* γ. *Then* $\sigma_{L,n}^{(\gamma)}$ *is a finite, bijective and birational morphism of algebraic varieties and in particular* $\sigma_{L,n}^{(\gamma)}$ *is a homeomorphism with respect to the Zariski topologies of* $\mathcal{W}_{L,n}$ *and* $\mathcal{S}_{L,n}^{(\gamma)}$

Since the varieties $\mathcal{W}_{L,n}$ and $\mathcal{S}_{L,n}^{(\gamma)}$ are irreducible, we conclude that their coordinate rings $k[\mathcal{W}_{L,n}]$ and $k[\mathcal{S}_{L,n}^{(\gamma)}]$ are domains with function fields $k(\mathcal{W}_{L,n})$ and $k(\mathcal{S}_{L,n}^{(\gamma)})$. The morphism $\sigma_{L,n}^{(\gamma)}$ induces an embedding of the coordinate ring $k[\mathcal{S}_{L,n}^{(\gamma)}]$ into $k[\mathcal{W}_{L,n}]$ (and the same is true for the corresponding function fields). Moreover, the finiteness of the morphism $\sigma_{L,n}^{(\gamma)}$ means that $k[\mathcal{W}_{L,n}]$ is an *integral* ring extension of $k[\mathcal{S}_{L,n}^{(\gamma)}]$.

Disregarding the complexity aspect, Lemma 4 says that it is possible to reconstruct the coefficients of a polynomial $H \in \mathcal{H}_{L,n}$ from the values of H in a given identification sequence γ, even if the sequence γ is short in comparison with the degree of H. Lemma 4 says further that this reconstruction is rational (i.e. it uses only arithmetical operations) and that possibly occuring divisions may always be performed by limit processes in the spirit of de l'Hôpital's rule. These processes produce only *finite* limits, because the coefficients of H are integrally dependent on the values of H in the given identification sequence γ. In algebraic terms, we may modelise these limit processes by *places* (corresponding to valuation rings) which map the function field $k(\mathcal{S}_{L,n}^{(\gamma)})$ of the variety $\mathcal{S}_{L,n}^{(\gamma)}$ into the set of values $\bar{k} \cup \{\infty\}$ and take only finite values on $k[\mathcal{S}_{L,n}^{(\gamma)}]$. The finiteness of the limits mentioned before is modelised by the requirement that any extension of such a place to the function field $k(\mathcal{W}_{L,n})$ takes finite values on $k[\mathcal{W}_{L,n}]$. This requirement is satisfied, because $k[\mathcal{W}_{L,n}]$ is integral over $k[\mathcal{S}_{L,n}^{(\gamma)}]$ (see [26] for details about places and integral extensions).

3.3 The complexity of parametric elimination procedures

In this section we suppose that the ground field k is of characteristic zero. Let n be a fixed natural number, $m(n) := 6(3n+1)^2, N(n) := (n+3)^2$ and $X_1, \dots, X_n, Z_1, \dots, Z_{N(n)}$ and $Y, S_1, \dots, S_{m(n)}$ indeterminates over k.

Let us fix an identification sequence $\gamma := (\gamma_1, \dots, \gamma_{m(n)}) \in k^{m(n)\times n}$ for the polynomials of $\bar{k}[X_1, \dots, X_n]$ having non-scalar complexity at most n (i.e. for the complexity class $\mathcal{H}_{n,n}$).

¿From [3], Chapter 9, Theorem 9.9 we deduce that there exists a polynomial

$$R_n \in k[Z_1, \dots, Z_{N(n)}, X_1, \dots, X_n]$$

satisfying the following conditions,

- R_n can be evaluated by a totally division-free arithmetic circuit in $k[Z_1, \dots, Z_{N(n)}, X_1, \dots, X_n]$ of non-scalar size $N(n)$
- for any $H \in \mathcal{H}_{n,n}$ and any totally division-free arithmetic circuit β in $\bar{k}[X_1, \dots, X_n]$, such that β has non-scalar size n, scalars $\zeta_1, \dots, \zeta_{N(n)} \in \bar{k}$ and such that β evaluates the polynomial H, we have

$$H = R_n(\zeta_1, \dots, \zeta_{N(n)}, X_1, \dots, X_n).$$

Let us consider the following existential formula $\Phi_n(S_1, \dots, S_{m(n)}, Y)$ in the free indeterminates ("free variables" in the terminology of mathematical logic) $S_1, \dots, S_{m(n)}, Y$,

$$(\exists X_1), \dots, (\exists X_n)(\exists Z_1), \dots, (\exists Z_{N(n)}))(\bigwedge_{1\le i\le n} {X_i}^2 - X_i = 0 \wedge$$

$$\bigwedge_{1\le k\le m(n)} S_k = R_n(Z_1, \dots, Z_{N(n)}, \gamma_k) \wedge Y = R_n(Z_1, \dots, Z_{N(n)}, X_1, \dots, X_n)).$$

Observe that the existential formula $(\exists Y)\Phi_n(S_1, \dots, S_{m(n)}, Y)$ describes the set $\sigma_{n,n}^{(\gamma)}(\mathcal{H}_{n,n})$. Thus the formula $\Phi_n(S_1, \dots, S_{m(n)}, Y)$ introduces an implicit semantical dependence between the indeterminates $S_1, \dots, S_{m(n)}$. In the sequel we shall consider the inteterminates $S_1, \dots, S_{m(n)}$ as parameters and Y as variable.

Let us finally remark that the formula $\Phi_n(S_1, \dots, S_{m(n)}, Y)$ may be represented by a totally division-free circuit in

$$k[X_1, \dots, X_n, Z_1, \dots, Z_{N(n)}, S_1, \dots, S_{m(n)}, Y]$$

of size $O(n^4)$.

Let us now consider an arbitrary (universal) *parametric* elimination procedure Π with associated sequential time complexity measure $\mathcal{T}$ and suppose that Π and $\mathcal{T}$ satisfy the following conditions:

(i) For any totally division-free arithmetic input network β of total size $\mathcal{L}(\beta)$ such that β represents an existential input formula Φ in the elementary language of algebraic geometry over the field k, the elimination procedure Π is able to produce a totally division-free arithmetic output network Γ with $\mathcal{L}(\Gamma) \leq \mathcal{T}(\mathcal{L}(\beta))$, such that Γ represents a quantifier-free formula which is semantically equivalent to Φ.

(ii) For any totally division-free arithmetic input network β_1 representing a constructible subset $\mathcal{X}$ of an appropriate affine space, the procedure Π is able to produce a totally division-free arithmetic output circuit Γ_1 with $\mathcal{L}(\Gamma_1) \leq \mathcal{T}(\mathcal{L}(\beta_1))$, such that Γ_1 represents a suitable polynomial equation system for the Zariski closure of the constructible set $\mathcal{X}$.

(iii) Let $U_1, \ldots, U_r$ and Y be indeterminates and let be 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. Consider 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 assume that S is an irreducible closed subvariety of $\mathbb{A}^r$. Suppose that the polynomials $B_1, \ldots, B_s$ are given by a totally division–free arithmetic circuit β_2 in $k[U_1, \ldots, U_r, Y]$ and suppose that they satisfy all our requirements at the end of Section 2.2. Hence there exists a well–defined parametric greatest common divisor $h \in k(S)[Y]$ associated to the polynomials $B_1, \ldots, B_s$.

Then the procedure Π is able to produce an essentially division-free arithmetic circuit Γ_2 in $k(U_1, \ldots, U_r)[Y]$ with $\mathcal{L}(\Gamma_2) \leq \mathcal{T}(\mathcal{L}(\beta_2))$ such that Γ_2 computes a representative $H \in k(U_1, \ldots, U_r)[Y]$ of the (generically squarefree) parametric greatest common divisor $h \in k(S)[Y]$ and such that Γ_2 satisfies the requirements formulated at the end of Section 2.2 for such a circuit. Moreover, the same holds true for the generically squarefree parametric greatest common divisor associated to the polynomials $B_1, \ldots, B_s$.

In view of conditions (*ii*) and (*iii*) above, we say that the parametric elimination procedure Π *computes efficiently Zariski closures and (generically squarefree) greatest common divisors.*

The requirement that Γ_1 and Γ_2 are *circuits* (and not arithmetic networks) contains implicitly the meaning that the procedure Π is *branching parsimonious* (see Section 2). Similarly, the behaviour of the circuit Γ_2 under specialisation by places expresses the requirement that the procedure Π is *division parsimonious.*

Let us finally observe that, after a suitable adaption of the data structures, all known universal elimination procedures satisfy with respect to appropriate sequential time complexity measures our conditions $(i), (iii)$ and (iii) (see Section 3.4 for more details).

We are now ready to state the main result of this paper.

Theorem 5 *Assume that the ground field k is of characteristic zero. Let Π be an arbitrary parametric elimination procedure with associated sequential time complexity measure $\mathcal{T}$ and suppose that Π and $\mathcal{T}$ satisfy conditions $(i), (iii)$ and (iii) above. There exists a family of totally division-free arithmetic input circuits $\beta = (\beta_n)_{n \in \mathbb{N}}$ such that each β_n has total size $n^{O(1)}$ and represents a parametric family of polynomial equation systems with a well defined, canonical elimination polynomial P_n. The elimination procedure Π produces for each $n \in \mathbb{N}$ from the input circuit β_n an essentially division-free output circuit Γ_n which represents the elimination polynomial P_n. The total size of the output circuit Γ_n cannot be polynomial in the parameter n. Therefore $\mathcal{T}$ is not a polynomial function.*

Proof Let be given a parametric elimination procedure Π with associated sequential time complexity measure $\mathcal{T}$, as in the statement of the theorem. Let $n \in \mathbb{N}$. We apply first the procedure Π to any totally division-free arithmetic circuit β_n of size $O(n^4)$ which represents the formula $\Phi_n(S_1, \ldots, S_{m(n)}, Y)$. In virtue of condition (i) above, we obtain as output a totally division-free arithmetic network $\beta_1^{(n)}$ of size $\mathcal{T}(O(n^4))$ representing a quantifier-free formula which is semantically equivalent to $\Phi_n(S_1, \ldots, S_{m(n)}, Y)$. Applying now the procedure Π to the network $\beta_1^{(n)}$, we obtain in virtue of condition (ii) above a totally division-free circuit $\beta_2^{(n)}$ of size $\mathcal{T}^2(O(n^4))$ which represents a positive number s of polynomials, say $B_1, \ldots, B_s \in k[S_1, \ldots, S_{m(n)}, Y]$, such that $B_1 = 0, \ldots, B_s = 0$ forms a polynomial equation system for the Zariski closure of the constructible subset of the affine space $\mathbb{A}^{m(n)} \times \mathbb{A}^1$, defined by the formula $\Phi_n(S_1, \ldots, S_{m(n)}, Y)$. This equation system contains polynomials of $k[S_1, \ldots, S_{m(n)}]$ which determine the Zariski closed subset $\mathcal{S} := \mathcal{S}_{n,n}^{(\gamma)}$ of $\mathbb{A}^{m(n)}$ (recall that the existential formula

$$(\exists Y)\Phi_n(S_1, \ldots, S_{m(n)}, Y)$$

describes the set $\sigma_{n,n}^{(\gamma)}(\mathcal{H}_{n,n})$ and that $\mathcal{S}_{n,n}^{(\gamma)}$ is its Zariski closure).

Let $b_1, \ldots, b_s \in k[\mathcal{S}][Y]$ be the polynomials in Y with coefficients in $k[\mathcal{S}]$ induced by $B_1, \ldots, B_s$ and observe that not all polynomials $b_1, \ldots, b_s$ are zero. We consider now an arbirary point

$$u = (u_1, \ldots, u_{m(n)}) \in \sigma_{n,n}^{(\gamma)}(\mathcal{H}_{n,n}).$$

There exists a point $\zeta = (\zeta_1, \ldots, \zeta_{N(n)}) \in \mathbb{A}^{N(n)}$ such that

$$E := R_n(\zeta, X_1, \ldots, X_n) := R_n(\zeta_1, \ldots, \zeta_{N(n)}, X_1, \ldots, X_n)$$

satisfies the condition $u = \sigma_{n,n}^{(\gamma)}(E) = (R_n(\zeta, \gamma_1), \ldots, R_n(\zeta, \gamma_{m(n)}))$.

¿From Lemma 4 we deduce that the polynomial $E \in \bar{k}[X_1, \ldots, X_n]$ depends only on the point u and not on the particular choice of $\zeta \in \mathbb{A}^{N(n)}$. Let us therefore write $E_u := E$. Let $P_u := \prod_{(\epsilon_1, \ldots, \epsilon_n) \in \{0,1\}^n}(Y - E_u(\epsilon_1, \ldots, \epsilon_n))$.

Interpreting now the formula $\Phi_n(S_1, \ldots, S_{m(n)}, Y)$ semantically, we see that $\Phi_n(u_1, \ldots, u_{m(n)}, Y)$ is equivalent to $P_u(Y) = 0$.

For a suitable choice of $u \in \sigma_{n,n}^{(\gamma)}(\mathcal{H}_{n,n})$ (e.g. choosing u with $H_u = \sum_{i=1}^{n} 2^{i-1}X_i$) we obtain a *separable* polynomial P_u.

There exists therefore a nonempty Zariski open subset $\mathcal{U} \subset \mathcal{S}$, contained in $\sigma_{n,n}^{(\gamma)}(\mathcal{H}_{n,n})$, such that for $u \in \mathcal{U}$ the greatest common divisor of the non–zero elements of $b_1(u, Y) := B_1(u, Y), \ldots, b_s(u, Y) := B_s(u, Y)$ has the same zeroes in $\bar{k}$ as the polynomial $P_u(Y)$ and such that $P_u(Y)$ is separable.

Let $h \in k(\mathcal{S})[Y]$ be the (normalised) greatest common divisor of the non–zero elements between the polynomials $b_1, \ldots, b_s$ and let $\hat{h} \in k(\mathcal{S})[Y]$ be the unique monic sparable polynomial with the same roots as h in an algebraic closure of $k(\mathcal{S})$. Without loss of generality we may assume that for any point $u \in \mathcal{U}$ the specialised polynomial $\hat{h}(u, Y)$ is a well–defined element of $\bar{k}[Y]$ with $\hat{h}(u, Y) = P_u(Y)$.

Let $\mathcal{A}$ be the integral closure of the coordinate ring $k[\mathcal{S}]$ in its fraction field $k(\mathcal{S})$. From Lemma 4 we deduce now that $\hat{h}$ and h belong to the polynomial ring $\mathcal{A}[Y]$ and that the polynomials $B_1, \ldots, B_s$ satisfy the requirements of the end of Section 2.2. In other words,the polynomial h is the parametric greatest common divisor associated to $B_1, \ldots, B_s$ and $\hat{h}$ is its generically squarefree counterpart.

Let us now consider $S_1, \ldots, S_{m(n)}$ as parameters and Y as variable.

Applying finally the procedure Π to the circuit $\beta_2^{(n)}$ we obtain by virtue of condition (*iii*) above an essentially division-free arithmetic circuit ${\Gamma_n}^*$ in $k(S_1, \ldots, S_{m(n)})[Y]$ which computes a representative of the generically squarefree greatest common divisor $\hat{h} \in \mathcal{A}[Y]$. The size of ${\Gamma_n}^*$ is $\mathcal{T}^3(O(n^4))$ and the circuit ${\Gamma_n}^*$ satisfies the requirements of the end of Section 2.2. From condition (*iii*) above we deduce that all scalars of ${\Gamma_n}^*$ are rational functions of $k(S_1, \ldots, S_{m(n)})$ which represent elements of the ring $\mathcal{A}$.

We consider now the polynomial $F := \sum_{i=1}^n 2^{i-1}X_i + T\prod_{i=1}^n(1+(U_i-1)X_i)$ introduced in Section 3.1. This polynomial can be represented by a totally division-free circuit of non-scalar size n over $k[U_1, \ldots, U_n, T]$.

Let $A_1 := F(U_1, \ldots, U_n, T, \gamma_1), \ldots, A_{m(n)} := F(U_1, \ldots, U_n, T, \gamma_{m(n)})$. Then $A_1, \ldots, A_{m(n)}$ are invariant polynomials of $k[U_1, \ldots, U_n, T]$. Specialising now the parameters $S_1, \ldots, S_{m(n)}$ into the polynomials
$A_1, \ldots, A_{m(n)}$, we obtain a k–algebra homomorphism

$$k[\mathcal{S}] \longrightarrow k[A_1, \ldots, A_{m(n)}].$$

We consider this homomorphism as a specialization of the coordinate ring $k[\mathcal{S}]$.

Since the circuit ${\Gamma_n}^*$ satisfies the requirements of the end of Section 2.2, the scalars of ${\Gamma_n}^*$ become now specialised into elements of the field $k(A_1, \ldots, A_{m(n)})$. These elements belong to the integral closure of the k–algebra $k[A_1, \ldots, A_{m(n)}]$ in its fraction field $k(A_1, \ldots, A_{m(n)})$. Since $k[A_1, \ldots, A_{m(n)}]$ is a k–subalgebra of the (integrally closed) polynomial ring $k[U_1, \ldots, U_r, T]$, we conclude that the above specialisation maps the scalars of the circuit ${\Gamma_n}^*$ into elements of $k[U_1, \ldots, U_r, T]$ which are integral over $k[A_1, \ldots, A_{m(n)}]$. This implies that the scalars of ${\Gamma_n}^*$ are specialised into *invariant* polynomials of $k[U_1, \ldots, U_r, T]$.

Denote now by Γ_n the totally division–free invariant circuit of
$k[U_1, \ldots, U_r, T, Y]$ obtained by specializing in ${\Gamma_n}^*$ the scalars as explained before. Let $L(\Gamma_n)$ be the non–scalar size of the circuit Γ_n over $k[U_1, \ldots, U_r, T]$. Then we have $L(\Gamma_n) \geq \mathcal{L}({\Gamma_n}^*) \geq \mathcal{T}^3(O(n^4))$ and Γ_n computes the image of $\hat{h}$ under the above specialisation, namely the elimination polynomial $P := \prod_{j=0}^{2^n-1}(Y - (j + T\prod_{i=1}^n {U_i}^{[j]_i}))$ of Section 3.1.

¿From the invariance of the circuit Γ_n and Theorem 2 and its proof we deduce now the estimate $L(\Gamma_n) \geq 2^{\frac{n}{2}} - 3$. On the other hand we have $\mathcal{T}^3(O(n^4)) \geq L(\Gamma_n)$. This implies that $\mathcal{T}$ cannot be a polynomial function. □

3.4 State of the art in circuit-based elimination

Let us now analyse from a general non-uniform point of view how the seminumerical elimination procedure designed in [13] and [11] works on a given flat family of zero-dimensional elimination problems.

Let $U_1, \dots, U_m, X_1, \dots, X_n, Y$ be indeterminates over the ground field k and let $G_1, \dots, G_n, F$ be polynomials belonging to the k-algebra

$$k[U_1, \dots, U_m, X_1, \dots, X_n].$$

Let $d := \max\{\deg G_1, \dots, \deg G_n\}$ and suppose that $G_1, \dots, G_n$ and F are given by straight-line programs in $k[U_1, \dots, U_m X_1, \dots, X_n]$ of length L and K respectively. Suppose that the polynomials $G_1, \dots, G_n$ form a regular sequence in $k[U_1, \dots, U_m, X_1, \dots, X_n]$ defining thus an equidimensional subvariety $V = \{G_1 = 0, \dots, G_n = 0\}$ of $\mathbb{A}^{m+n}$ of dimension m.

Assume that the morphism $\pi : V \longrightarrow \mathbb{A}^m$, induced by the canonical projection of $\mathbb{A}^{m+n}$ onto $\mathbb{A}^m$ is finite and generically unramified. Let δ be the degree of the variety V and let $D \leq \delta$ be the degree of the morphism π. Furthermore let $\tilde{\pi} : V \longrightarrow \mathbb{A}^{m+1}$ be the morphism of affine varieties defined by $\tilde{\pi}(z) := (\pi(z), F(z))$ for any point z of V. Let $P \in k[U_1, \dots, U_m, Y]$ be the minimal polynomial of the image of $\tilde{\pi}$. The polynomial P is monic in Y and one sees immediately that $\deg P \leq \delta \deg F$ and $\deg_Y P \leq D$ holds. Let us write $\delta_* := \deg_{U_1, \dots, U_m} P$.

Let us consider as Algorithm 1 and Algorithm 2 two non-uniform variants of the basic elimination method designed in [13] and [11].

- Algorithm 1 is represented by an arithmetic network of size $K\delta^{O(1)} + L(nd\Delta)^{O(1)}$ where Δ is the degree of the equation system $G_1 = 0, \dots, G_n = 0$ (observe that always $\delta \leq \Delta \leq \deg G_1 \cdots \deg G_n$ holds). The output is a straight-line program Γ_1 in $k[U_1, \dots, U_m, Y]$ of length $(K + L)(n\delta)^{O(1)}$ which represents the polynomial P.
- Algorithm 2 starts from the geometric description of a unramified parameter (and lifting) point $u = (u_1, \dots, u_m)$ of k^m which has the additional property that the image of F restricted to the set $\{u\} \times \pi^{-1}(u)$ has cardinality $D_* = \deg_Y P$. The algorithm produces then an arithmetic circuit Γ_2 in $k[U_1, \dots, U_m, Y]$ of length

  $$O(KD^{O(1)} \log \delta_*) + \delta_*^{O(1)} = K(\delta \deg F)^{O(1)}$$

  which represents the polynomial P.

We observe that $K\delta^{O(1)}$ is a characteristic quantity which appears in the length of both circuits Γ_1 and Γ_2. One may ask whether a complexity of type $K\delta^{O(1)}$ is intrinsic for the elimination problem under consideration.

In view of Bézout's Theorem and the lower complexity bound of Theorem 5, one may guess that a quantity of asymptotic order $K\delta$ may be characteristic for the intrinsic sequential time complexity of universal parametric elimination procedures.

4 Conclusions

It was fundamental for our argumentation in Section 3 that our notion of *parametric elimination procedure* restricts severely the possibility of branchings in the output circuit or network. This suggests that any polynomial time elimination algorithm (if there exists one) must have a huge topological complexity. Thus hypothetical efficiency in geometric elimination seems to imply complicated casuistics.

Let us also mention that the proof method of Section 3 contributes absolutely *nothing* to the elucidation of the fundamental thesis of algebraic complexity theory, which says that geometric elimination produces elimination polynomials which are intrinsically hard to evaluate (i.e. these polynomials need asymptotically degree–much sequential time for their evaluation). A good example for this thesis is the Pochhammer–Wilkinson polynomial which can be obtained easily as the solution of a suitable elimination problem but which is conjecturally hard to evaluate (see e.g. [19, 1]) Similarly no advance is obtained by our method with respect to the question whether $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$ holds in the BSS complexity model, see [2], Chapter7.

In fact our contribution consists only in the discovery of a very limiting uniformity property present in all known elimination procedures. This uniformity property inhibits the transformation of these elimination procedures into polynomial time algorithms.

In conclusion, when treating with algorithmic elimination problems, one should not expect too much from the output: as observed already by Hilbert, a strong limitation to *specific* elimination problems (with additional a priori information or additional semantical structure) is necessary in order to avoid huge difficulties and one should also renounce to compute the whole elimination object, if this is not required in advance. In particular, canonical elimination polynomials contain the complete information about the elimination problem under consideration, they are "co–versal", and this makes necessarily intricate their representation in any reasonable data–structure (for more details see [6]). A way out of this dilemma should be found in analysing which information about elimination objects is really relevant, avoiding in this way to struggle with enormous objects which encode a lot of spurious knowledge.

Acknowlegment.

The authors wish to express their gratitude to Guillermo Matera and Rosa Wachenchauzer (Buenos Aires, Argentina) and to David Castro and Luis Miguel Pardo (Santander, Spain) for many fruitful discussions and ideas. They are deeply indepted to Jacques Morgenstern (Nice, France), who suggested this research and made together with the authors the first and most fundamental steps toward the complexity model and results of this paper.

Bibliography

[1] Blum, Cucker, Shub, and Smale. Algebraic settings for the problem "$P \neq NP$?". In Renegar, Shub, and Smale, editors, *The Mathematics of Numerical Analysis: 1995 (25th) AMS-SIAM Summer Seminar in Applied Mathematics (Lectures in Applied Mathematics, Volume 32), American Mathematical Society.* 1996.

[2] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and real computation.* Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.

[3] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.

[4] L. Caniglia, A. Galligo, and J. Heintz. Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de charactéristique quelconque. *C. R. Acad. Sci. Paris*, 307:255–258, 1988.

[5] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora, editor, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAECC-6*, volume 357 of *LNCS*, pages 131–152. Springer, 1989.

[6] D. Castro, M. Giusti, J. Heintz, G. Matera, and L. M. Pardo. Data structures and smooth interpolation procedures in elimination theory. Manuscript, 1999.

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

[8] M. Demazure. Le théorème de complexité de mayr–meyer. Manuscript Ecole Polytechnique, 1985.

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

[10] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using gröbner bases. In *Applied Algebra, Algebraic Algorithms*

and Error Correcting Codes, Proceedings of AAECC-5, volume 356 of *LNCS*, pages 247–257. Springer, 1989.

[11] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for diophantine approximation. In *Proceedings of MEGA'96*, volume 117,118, pages 277–317. Journal of Pure and Applied Algebra, 1997.

[12] 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 University Press, 1993.

[13] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight–line programs in geometric elimination theory. *J. of Pure and App. Algebra*, 124:101–146, 1998.

[14] 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 *LNCS*, pages 205–231. Springer, 1995.

[15] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *C. R. Acad. Sci. Paris*, 325:1223–1228, 1997.

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

[17] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, 24(3):239–277, 1983.

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

[19] J. Heintz and J. Morgenstern. On the intrinsic complexity of elimination theory. *J. of Complexity*, 9:471–498, 1993.

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

[21] D. Hilbert. Neubegründung der mathematik. erste mitteilung. *Abhandl. aus dem Math. Seminar d. Hamb. Univ.*, 1:157–177, 1922.

[22] Hidetsune Kobayashi, Shuichi Moritsugu, and Robert W. Hogan. Solving systems of algebraic equations. In *Symbolic and algebraic computation (Rome, 1988)*, pages 139–149. Springer, Berlin, 1989.

[23] 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. Birkhäuser Verlag, 1996.

[24] L. Kronecker. Grundzüge einer arithmetischen theorie der algebraischen grössen. *J. reine angew. Math.*, 92:1–122, 1882.

[25] Klaus Kühnle. *Space Optimal Computation of Normal Forms of Polynomials.* PhD thesis, Universität München, 1998.

[26] Serge Lang. *Algebra.* Addison-Wesley Publishing Co., Reading, Mass., second edition, 1984.

[27] M. Giusti G. Lecerf and B. Salvy. A gröbner free alternative for polynomial systems solving. *to appear in J. Complexity*, 2000.

[28] F. S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.

[29] Guillermo Matera. Probabilistic algorithms for geometric elimination. *Appl. Algebra Engrg. Comm. Comput.*, 9(6):463–520, 1999.

[30] Guillermo Matera and Jose Maria Turull Torres. The space complexity of elimination theory: upper bounds. In *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 267–276. Springer, Berlin, 1997.

[31] J. Heintz G. Matera and A. Waissbein. On the time–space complexity of geometric elimination procedures. *to appear in Appl. Algebra Engrg. Comm. Comput.*, 2000.

[32] E. Mayr. Membership in polynomial ideals over Q is exponential space complete. In B. Monien et al, editor, *Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (STACS'89), Paderborn (FRG) 1989*, number 349 in Lecture Notes in Computer Science, pages 400–406. Springer, 1989.

[33] E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups. *Adv. in Math.*, 46:305–329, 1982.

[34] D. Castro K. Hägele J.E. Morais and L.M. Pardo. Kronecker's and newton's approaches to solving : a first comparison. *to appear in J. of Complexity*, 2000.

[35] David Mumford. *The Red Book of Varieties and Schemes*, volume 1358 of *LNM.* Springer, Berlin, 1 edition, 1988.

[36] Raghavan Narasimhan. *Introduction to the theory of analytic spaces.* Springer-Verlag, Berlin, 1966. Lecture Notes in Mathematics, No. 25.

[37] I. R. Shavarevich. *Basic Algebraic Geometry : Varieties in Projective Space.* Springer, 1994.

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

[39] M. Shub and S. Smale. Complexity of Bézout's theorem V: Polynomial time. *Theor. Comp. Sci.*, 133:141–164, 1994.

[40] B. L. van der Waerden. *Moderne Algebra II.* Springer Verlag,Berlin, 1931.

[41] 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*, volume 233 of *LNCS*, pages 93–112, Bratislava, Czechoslovakia, August 1986. Springer.

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

[43] Chee-K. Yap. A new lower bound construction for commutative Thue systems with applications. *J. Symbolic Comput.*, 12(1):1–27, 1991.