Electronic Journal of SADIO
http://www.dc.uba.ar/sadio/ejs/
vol. 1, no. 1, pp. 37–51 (1998)

The intrinsic complexity of parametric elimination methods

J. Heintz[1,2] *G. Matera*[2,3] *L. M. Pardo*[1] *R. Wachenchauzer*[4]

[1] Depto. de Matemáticas, Est. y Comp., Facultad de Ciencias, Universidad de Cantabria, E-39071 SANTANDER, Spain.
heintz@matsun1.matesco.unican.es
[2] Depto. de Matemáticas, FCEyN, Universidad de Buenos Aires, Ciudad Universitaria, Pab. I, (1428) BUENOS AIRES, Argentina. gmatera@dm.uba.ar.
[3] Instituto de Ciencias, Universidad Nacional de Gral. Sarmiento, Roca 850, (1663) San Miguel - Pcia. de Buenos Aires, Argentina.
[4] Departamento de Computación, FCEyN, Universidad de Buenos Aires, Ciudad Universitaria, Pab. I, (1428) BUENOS AIRES, Argentina.
rosita@dc.uba.ar.

Abstract

This paper is devoted to the complexity analysis of a particular property, called *geometric robustness* owned by all known symbolic methods of parametric polynomial equation solving (geometric elimination). It is shown that *any* parametric elimination procedure which owns this property must necessarily have an exponential sequential time complexity even if highly performant data structures (as e.g. the straight–line program encoding of polynomials) are used. The paper finishes with the motivated introduction of a new non-uniform complexity measure for zero-dimensional polynomial equation systems, called *elimination complexity.*

Keywords. Polynomial system solving, elimination, complexity.

Research was partially supported by the following Argentinian and Spanish grants:UBA-CYT.EX.001, PIP CONICET 4571, DGICYT PB96–0671–C02–02.

1 Introduction

Modern algebraic geometry started about 200 years ago as *algorithmic* algebraic geometry, and, more precisely, as algorithmic elimination theory. The motivation for the creation of such a field was the search for methods which allow to find the *real* solutions of a polynomial equation system. Nevertheless, the very origin of algebraic geometry was given by the observation that real root finding is a rather infeasible task without a previous study of the behaviour of the *complex* solutions of polynomial equation systems. This observation was first made by Euler and Bézout and then extended to a general theory by a long list of geometers of the last century. This list includes names as Jacobi, Sylvester, Kronecker, M. Noether, Hilbert (the creator of modern commutative algebra), Castelnuovo, Bertini, Enriques.

Despite the orientation of modern algebraic geometry toward a new structural view of the field, in the last twenty years a new community of algebraic geometers doing symbolic computation splitted out of the mainstream. The intention of this community to bring back algebraic geometry to its origin (and to introduce also new aspects like efficient polynomial equation solving for industrial applications) must be praised highly. On the other hand the (mainly rewriting based) computational approach used by this community is far too simple minded for the difficult task of efficient, i.e. real world polynomial equation solving. An important drawback of this approach consists in the almost total absence of todays skill in algorithmics and data structure manipulation as well as the unawareness of modern programming techniques coming from software engineering. There is no place here to describe in detail the advances and weaknesses of symbolic computation (more precisely: computer algebra) techniques applied to elimination theory. For an overview about rewriting based methods (Gröbner basis techniques) we refer to the books [20], [15], [6] (these books include also motivations and historical considerations). The state of the art in sparse techniques can be found in [7]. Finally the seminumerical approach to elimination theory is described in the book [3] and the surveys [13], [17], [12] and in the research papers [11], [10] and [1].

It is well known that there exists no polynomial time geometric or algebraic elimination procedure if dense encoding of polynomials is used as basic data structure (see e.g. [14], [13], [17]). One may ask whether this conclusion remains still true for elimination procedures based on the more succinct straight–line program encoding of polynomials as fundamental data structure (see e.g. [13], [17], [4]).

In this paper we will give a partial answer to this question. We introduce and discuss the notion of a *geometrically robust parametric elimination procedure.* The main outcome is the observation that all known parametric elimination procedures are geometrically robust and that all geometrically robust parametric elimination procedures must necessarily have an exponential time complexity even if the highly performant encoding of polynomials by straight–line programs is used (Theorem 1). Therefore a revolutionary change of mathematical theory and algorithmics would be necessary in order to design a (possibly non-existent) highly performant general purpose elimination procedure. The rest of the paper is devoted to the motivated introduction of a new uniform complexity measure for zero-dimensional polynomial equation systems, called *elimination complexity.*

The procedures (algorithms) considered in this paper operate with division–free arithmetic circuits as basic data structure for the representation of inputs and outputs. In his turn such a circuit depends on certain input nodes, labeled by indeterminates over a given ground field k. These indeterminates are thought to be subdivided into two disjoint sets representing the *parameters* and *variables* of the given circuit. The output nodes of the circuit represent polynomials in the parameters and variables of the circuit. On the other hand the output nodes are labeled by sign marks of the form "$= 0$" or "$\neq 0$" or remain unlabeled. Thus the given circuit defines by means of its labeled output nodes a system of polynomial equations and inequations which determines in his turn a locally closed set with respect to the Zariski topology of the (affine) space of parameter and variable instances. The unlabeled nodes of the given circuit determine a polynomial map (in fact a morphism of algebraic varieties) which is defined on this locally closed set. We shall interpret the system of polynomial equations and inequations determined by the given circuit as a *parametric* system in the variables of the circuit. The same point of view is applied to the morphism determined by the unlabeled nodes of the circuit. We say that a given parameter point fixes an *input/output instance* of the procedure under consideration. Input and output instances will also be called *problem* and *solution instances* respectively.

In this paper we shall restrict our attention to input circuits which contain only output nodes labeled by "=0" and unlabeled output nodes and to output circuits having all output nodes labeled by the mark "=0". Such an input circuit represents a parametric polynomial equation system defining an algebraic variety and a morphism defined on this variety. Therefore any input circuit represents a parametric polynomial equation system defining an algebraic variety, and a morphism having this variety as domain. The corresponding output circuit will always represent an algebraic variety which describes the image of the given morphism (this image will be Zariski closed in all cases we shall consider).

All procedures we are going to consider are *geometric elimination procedures* in this sense. We modelize such a procedure by a family of arithmetic networks (arithmetic–boolean circuits, see [8], [9]). Let us observe that in principle such a procedure may contain branchings.

We call an elimination procedure *parametric* if it contains no branchings for any input equation system which represents a (geometrically or scheme–theoretically) flat family of input instances.

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

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

Finally let us refer to the books [5], [16] and [18] as a general background for notions of algebraic complexity theory and algebraic geometry we are going to use in this paper.

1.1 Flat families of elimination problems

Let k be an infinite and perfect field with algebraic closure $\bar{k}$ and let $T_1, \ldots, T_m$, $U_1, \ldots, U_r, X_1, \ldots, X_n, Y$ be indeterminates over k. Let $G_1, \ldots, G_n, F$ be polynomials belonging to the k-algebra $k[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$. Suppose that the polynomials $G_1, \ldots, G_n$ form a regular sequence in $k[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$ defining thus an equidimensional subvariety $V := \{G_1 = 0, \ldots, G_n = 0\}$ of the $(m + r + n)$-dimensional affine space $\mathbb{A}^{m+r+n}$ over the field $\bar{k}$. The algebraic variety V has dimension $m + r$. Let δ be the (geometric) degree of V. Suppose furthermore that the morphism of affine varieties $\pi : V \longrightarrow \mathbb{A}^{m+r}$, induced by the canonical projection of $\mathbb{A}^{m+r+n}$ onto $\mathbb{A}^{m+r}$, is finite and generically unramified (this implies that π is flat). Let $\tilde{\pi} : V \longrightarrow \mathbb{A}^{m+r+1}$ 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 $\mathbb{A}^{m+r+1}$ whose minimal equation is a polynomial of $k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ which we denote by P. Observe that P is monic in Y and that $\deg P \leq \delta$ holds. Furthermore $\deg_Y P$ is the cardinality of the image of the restriction of F to the set $\{w\} \times \pi^{-1}(w)$, where w is a typical point of $\mathbb{A}^{m+r}$. The polynomial $P(T_1, \ldots, T_m, U_1, \ldots, U_r, F)$ vanishes on the variety V.

Let us consider an arbitrary point $t = (t_1, \ldots, t_m)$ of $\mathbb{A}^m$. For arbitrary polynomials $B \in k[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$ and $C \in k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ we denote by $B^{(t)}$ and $C^{(t)}$ the polynomials $B(t_1, \ldots, t_m, U_1, \ldots, U_r, X_1, \ldots, X_n)$ and $C(t_1, \ldots, t_m, U_1, \ldots, U_r, Y)$ which belong to $k(t_1, \ldots, t_m)[U_1, \ldots, U_r, X_1, \ldots, X_n]$ and $k(t_1, \ldots, t_m)[U_1, \ldots, U_r, Y]$ respectively.

Similarly we denote for an arbitrary polynomial $A \in k[T_1, \ldots, T_m]$ by $A^{(t)}$ the value $A(t_1, \ldots, t_m)$ which belongs to the field $k(t_1, \ldots, t_m)$. The polynomials $G_1^{(t)}, \ldots, G_n^{(t)}$ form a regular sequence in $k(t_1, \ldots, t_m)[U_1, \ldots, U_r, X_1, \ldots, X_n]$ and define an equidimensional subvariety $V^{(t)} := \{G_1^{(t)} = 0, \ldots, G_n^{(t)} = 0\}$ of $\mathbb{A}^{r+n}$ whose degree is bounded by δ. Let $\pi^{(t)} : V^{(t)} \longrightarrow \mathbb{A}^r$ and $\tilde{\pi}^{(t)} : V^{(t)} \longrightarrow \mathbb{A}^{r+1}$ be the morphisms induced by π and $\tilde{\pi}$ on the variety $V^{(t)}$. Then the morphism $\pi^{(t)}$ is finite and flat but not necessarily generically unramified. Furthermore the image of $\tilde{\pi}^{(t)}$ is a hypersurface of $\mathbb{A}^{r+1}$ on which the polynomial $P^{(t)}$ vanishes (however $P^{(t)}$ is not necessarily the minimal equation of this hypersurface). We call the equation system $G_1 = 0, \ldots, G_n = 0$ and the polynomial F *a flat family of r-dimensional elimination problems depending on the parameters* $T_1, \ldots, T_m$. An element $t \in \mathbb{A}^m$ is considered as a *parameter point* which determines a *particular problem instance*. The equation system $G_1 = 0, \ldots, G_n = 0$ together with the polynomial F is called the *general instance* of the given elimination problem and the polynomial P is called its *general solution*.

The problem instance determined by the parameter point $t \in \mathbb{A}^m$ is given by the equations $G_1^{(t)} = 0, \ldots, G_n^{(t)} = 0$ and the polynomial $F^{(t)}$. The polynomial $P^{(t)}$ is called the *solution* of this particular problem instance. We call two parameter points $t, t' \in \mathbb{A}^m$ *equivalent* (in symbols $t \sim t'$) if $G_1^{(t)} = G_1^{(t')}, \ldots, G_n^{(t)} = G_n^{(t')}$ and $F^{(t)} = F^{(t')}$ holds. Observe that $t \sim t'$ implies also $P^{(t)} = P^{(t')}$. We call polynomials $A \in k[T_1, \ldots, T_m]$, $B \in k[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$ and $C \in k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ invariant (with respect to $\sim$) if for any two parameter points t, t' of $\mathbb{A}^m$ with $t \sim t'$ the identities $A^{(t)} = A^{(t')}$, $B^{(t)} = B^{(t')}$ and $C^{(t)} = C^{(t')}$ hold.

A straight-line program in $k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ *with parameters in* $k[T_1, \ldots, T_m]$ is an arithmetic circuit in $k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$, say γ, modelized in the following way: γ is given by a directed acyclic graph whose internal nodes are labeled as usual by arithmetic operations. The input nodes of γ are labeled by the variables $U_1, \ldots, U_r$ and the nodes of γ of indegree 0 which are not input nodes (i.e. the parameter nodes of γ) are labeled by arbitrary elements of $k[T_1, \ldots, T_m]$ called *parameters of* γ. We call such a straight-line program γ *invariant* (with respect to the equivalence relation $\sim$) if all its parameters are invariant polynomials of $k[T_1, \ldots, T_m]$. Let us observe that in an absolutely analogous way one may extend the notion of a straight-line program with parameters in $k[T_1, \ldots, T_m]$ and the notion of an invariant straight-line program to arithmetic circuits defined in $k[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$ or in $k[T_1, \ldots, T_m, U_1, \ldots, U_r]$ (however we shall make almost exclusive use of the corresponding notion for circuits in
$k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$).

We are now ready to characterize 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 straight-line program β in $k[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$. A geometrically robust parametric elimination procedure produces from the circuit β as input an *invariant* straight–line program Γ in $k[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ as output such that Γ represents the polynomial P. Observe that in our definition of geometric robustness we did not require that β is an invariant straight–line program because this would be too restrictive for the modeling of real situations in computational elimination theory. However in all known practical situations β always satisfies the following (weak) invariance condition: any specialization of the input variables $X_1, \ldots, X_n$ in β into arbitrary values of k transforms the circuit β in a invariant straight–line program in $k[T_1, \ldots, T_m, U_1, \ldots, U_r]$.

The invariance property required for the output circuit Γ means the following: let $t = (t_1, \ldots, t_m)$ be a parameter point of $\mathbb{A}^m$ and let $\Gamma^{(t)}$ be the straight–line program in $k(t_1, \ldots, t_m)[U_1, \ldots, U_r, Y]$ obtained from the circuit Γ evaluating in t the elements of $k[T_1, \ldots, T_m]$ which occur as parameters of Γ. Then the straight–line program $\Gamma^{(t)}$ depends only on the particular problem instance determined by the parameter point t but not on t 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 elimination problem under consideration. In other words this means that geometrically robust parametric elimination procedures do not contain branchings. Now we are going to show a complexity result which can be paraphrased as follows: *none of the known (exponential time) parametric elimination procedures can be transformed into 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 for flat families of elimination problems.

The invariance property of these procedures is easily verified in the situation of the flat family of r-dimensional elimination problems introduced before. One has only to observe that all known elimination procedures accept the input polynomials $G_1, \ldots, G_n, F$ in their dense or sparse coefficient representation or as evaluation black box with respect to the variables $U_1, \ldots, U_r, X_1, \ldots, X_n$.

1.2 A particular flat family of 1-dimensional elimination problems

Let $S, T, U, X_1, \ldots, X_{2n}, Y$ be indeterminates over $\mathbb{Q}$. We consider the following flat family of one-dimensional elimination problems depending on the parameters S and T. Let

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

$$G_{n+1} := X_{n+1} - \sum_{1 \le k \le n} 2^{k-1} X_k, G_{n+2} := X_{n+2} - X_{n+1}^2, G_{2n} := X_{2n} - X_{2n-1}^2$$

and

$$F := (1 + S \prod_{1 \le i \le n} (T^{2^{i-1}} + X_{n+i})) \prod_{1 \le j \le n} ((U^{2^{j-1}} - 1)X_j + 1).$$

We interpret $G_1, \ldots, G_{2n}$ and F as elements of the polynomial ring $\mathbb{Q}[S, T, U, X_1, \ldots, X_{2n}]$. Thus we have $m := 2$ and $r := 1$ in this situation.

It is clear from this representation that the polynomials $G_1, \ldots, G_{2n}$ and F can be evaluated by a straight–line program β in $\mathbb{Q}[S, T, U, X_1, \ldots, X_{2n}]$ of nonscalar length $O(n)$ (which satisfies the invariance condition for input circuits mentioned before). The degree in $X_1, \ldots, X_{2n}$ of the polynomials $G_1, \ldots, G_{2n}$ and F is bounded by $2n$. The variety $V := \{G_1 = 0, \ldots, G_n = 0\}$ is the union of 2^n affine linear subspaces of $\mathbb{A}^{3+2n}$ of the form $\mathbb{A}^3 \times \{\xi\}$, where ξ is a solution of the equation system $G_1 = 0, \ldots, G_{2n} = 0$ in $\mathbb{Z}^{2n}$. The morphism $\pi : V \to \mathbb{A}^3$ is obtained by gluing together the canonical projections onto $\mathbb{A}^3$ of these affine linear spaces. Obviously the morphismπ is finite an generically unramified. In particular π has constant fibers. Let $(l_1, \ldots, l_n)$ be a point of $\{0, 1\}^n$ and let $l := \sum_{1 \le j \le n} l_j 2^{j-2}$ be the integer $0 \le l < 2^n$ with bit representation $l_n l_{n-1} \ldots l_1$. Put $l_{n+1} := l, l_{n+2} := l^2, \ldots, l_{2n} := l^{2^{n-1}}$. One verifies immediately that with the convention $0^0 := 1$ the identity

$$F(S, T, U, l_1, \ldots, l_{2n}) = U^l (1 + S \sum_{\substack{0 \le p, q < 2^n \\ p+q = 2^n - 1}} T^p l^q)$$

holds. Therefore for any point $(s, t, u, l_1, \ldots, l_{2n}) \in V$ with $l := \sum_{1 \le j \le n} l_j 2^{j-1}$ we have

$$F(s, t, u, l_1, \ldots, l_{2n}) = u^l (1 + s \sum_{\substack{0 \le p, q < 2^n \\ p+q = 2^n - 1}} t^p l^q).$$

From this we deduce easily that the elimination polynomial $P \in \mathbb{Q}[S, T, U, Y]$ we are looking for is

$$P := \prod_{0 \le l < 2^n} \left(Y - U^l (1 + S \sum_{\substack{0 \le p, q < 2^n \\ p+q = 2^n - 1}} T^p l^q) \right).$$

This polynomial has the form

$$P = Y^{2^n} - \left(\sum_{0 \leq l < 2^n} U^l (1 + S \sum_{\substack{0 \leq p,q < 2^n \\ p+q = 2^n - 1}} T^p l^q) \right) Y^{2^n - 1} + \text{ lower degree terms in } Y.$$

Suppose now that there is given a geometrically robust parametric elimination procedure. This procedure produces from the input circuit β an invariant straight–line program Γ in $\mathbb{Q}\,[S, T, U, Y]$, which evaluates the polynomial P. Recall that the invariance of Γ means that the parameters of Γ are invariant polynomials of $\mathbb{Q}\,[S, T]$, say $A_1, \ldots, A_N$.

Let $\mathcal{L}(\Gamma)$ be the total and $L(\Gamma)$ the non-scalar length of the straight–line program Γ. 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 exist for $0 \leq l < 2^n$ polynomials $Q_l \in \mathbb{Z}[Z_1, \ldots, Z_N]$ such that $Q_l(A_1, \ldots, A_N)$ is the coefficient of the monomial $U^l Y^{2^n - 1}$ of P. This means that we have for $0 \leq l < 2^n$ the identity

$$Q_l(A_1, \ldots, A_N) = 1 + S \sum_{\substack{0 \leq p,q < 2^n \\ p+q = 2^n - 1}} T^p l^q. \tag{1}$$

Observe now that for any two values $t, t' \in \mathbb{A}^1$ the points $(0, t)$ and $(0, t')$ of $\mathbb{A}^2$ are equivalent (in symbols: $(0, t) \sim (0, t')$). From the invariance of $A_1, \ldots, A_N$ we deduce therefore that $A_j(0, t) = A_j(0, t')$ holds for $1 \leq j \leq N$. This means that $\alpha_1 := A_1(0, T), \ldots, \alpha_N := A_N(0, T)$ are constant values of $\mathbb{Q}$. From identity (1) we deduce that $Q_l(\alpha_1, \ldots, \alpha_N) = 1$ holds for any $0 \leq l < 2^n$.

Let us consider the morphisms of affine spaces $\mu : \mathbb{A}^2 \longrightarrow \mathbb{A}^N$ and $\psi : \mathbb{A}^N \longrightarrow \mathbb{A}^{2^n}$ given by $\mu := (A_1, \ldots, A_N)$ and $\psi := (Q_l)_{0 \leq l < 2^n}$.

Observe that

$$\psi \circ \mu = (Q_l(A_1, \ldots, A_N))_{0 \leq l < 2^n} = (1 + S \sum_{\substack{0 \leq p,q < 2^n \\ p+q = 2^n - 1}} T^p l^q)_{0 \leq l < 2^n}$$

holds. Furthermore let us consider the points $\alpha := (\alpha_1, \ldots, \alpha_N) \in \mathbb{A}^N$ and $\omega := (1, \ldots, 1) \in \mathbb{A}^{2^n}$. From our previous considerations we deduce the identities

$$\begin{aligned} (\psi \circ \mu)(0, T) = &\quad (Q_l(A_1(0, T), \ldots, A_N(0, T)))_{0 \leq l < 2^n} = \\ = &\quad (Q_l(\alpha_1, \ldots, \alpha_N))_{0 \leq l < 2^n} = (Q_l(\alpha))_{0 \leq l < 2^n} \quad = (1, \ldots, 1) = \omega. \end{aligned}$$

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

For any value $t \in \mathbb{Q}$ we consider the parametric curves $\gamma_t : \ \mathbb{A}^1 \longrightarrow \mathbb{A}^N$ and $\delta_t : \ \mathbb{A}^1 \longrightarrow \mathbb{A}^{2^n}$ defined by

$$\gamma_t := (A_1(S,t), \ldots, A_N(S,t)) \text{ and } \delta_t := (1 + S \sum_{\substack{0 \le p,q < 2^n \\ p+q = 2^n - 1}} t^p l^q)_{0 \le l < 2^n}$$

respectively. Observe that $\psi \circ \gamma_t = \delta_t$ and that $\gamma_t(0) = \alpha$, $\delta_t(0) = \omega$ holds (independently of the value t).

We consider γ_t and δ_t as one-parameter subgroups of $\mathbb{A}^N$ and A^{2^n} respectively.

Now fix $t \in \mathbb{Q}$ and consider

$$\gamma_t'(0) = (\frac{\partial A_1}{\partial S}(0,t), \ldots, \frac{\partial A_N}{\partial S}(0,t)) \text{ and } \delta_t'(0) = (\sum_{\substack{0 \le p,q < 2^n \\ p+q = 2^n - 1}} t^p l^q)_{0 \le l < 2^n}.$$

We have $\gamma_t'(0) \in E_\alpha$ and $\delta'(0) \in E_\omega$. Moreover one sees easily that

$$(D\psi)_\alpha(\gamma_t'(0)) = \delta_t'(0) = (\sum_{\substack{0 \le p,q < 2^n \\ p+q = 2^n - 1}} t^p l^q)_{0 \le l < 2^n}$$

holds. Choosing now 2^n different values $t_0, \ldots, t_{2^n-1}$ of $\mathbb{Q}$ we obtain 2^n tangent vectors $v_l := \gamma_{t_l}'(0)$ of E_α with $0 \le l < 2^n$. Let M be the $2^n \times 2^n$ matrix whose row vectors are $(D\psi)_\alpha(v_0), \ldots, (D\psi)_\alpha(v_{2^n-1})$. Observe that M has the form

$$M = (t_h^{2^n - p - 1})_{0 \le h,p < 2^n} \cdot (l^q)_{0 \le l,q < 2^n}.$$

Thus M is the product of two non-singular Vandermonde matrices and therefore itself non-singular. This means that in E_ω the tangent vectors $(D\psi)_\alpha(v_0), \ldots, (D\psi)_\alpha(v_{2^n-1})$ are linearly independent. Hence in E_α the tangent vectors $v_0, \ldots, v_{2^n-1}$ are linearly independent too.

Therefore we have $2^n \le \dim E_\alpha = N$ which implies $2^n \le N \le (L(\Gamma) + 3)^2$. From this we deduce the estimation $2^{\frac{n}{2}} - 3 \le L(\Gamma) \le \mathcal{L}(\Gamma)$.

We have therefore shown that any geometrically robust parametric elimination procedure applied to our flat family of one-dimensional elimination problems *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.*

The discussion of the previous example shows that the objective of a polynomial time procedure for geometric (or algebraic) elimination can not be reached following a evolutionary way, i.e. constructing improvements of known elimination methods.

It was fundamental in our argumentation above that our notion of *geometrically robust parametric elimination procedure* excludes branchings in the output program. 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.

This idea is worth to be discussed further. One may also ask whether admitting divisions in the output circuit helps to lower its minimal size. To some limited extent divisions in the output circuit are compatible with our proof method. However one has to take care of the way how these divisions may affect the dependence of the coefficients of the output polynomial on the parameters of the circuit representing it.

The formulation of a condition which guarantees the generalization of our method to output circuits with divisions seems to be cumbersome. In our example one has to make sure that even in presence of divisions for any value $t \in \mathbb{Q}$ the one-parameter subgroup γ_t still converges to one and the same point of $\mathbb{A}^N$.

Finally let us mention that our proof method above contributes absolutely *nothing* to the elucidation of the fundamental thesis of algebraic complexity theory, which says that geometric elimination is non-polynomial in the (unrestricted) non-uniform complexity model. 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 [3, Chapter 7].

In fact our contribution consists only in the discovery of a very limiting uniformity property (geometric robustness) present in all known elimination procedures. This uniformity property inhibits the transformation of these elimination procedures into polynomial time algorithms. We resume the conclusions from the complexity discussion of our example in the following form:

Theorem 1 *For any $n \in \mathbb{N}$ there exists a one-dimensional elimination problem depending on one parameter and $2n+1$ variables, 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).*

2 On the complexity of geometric elimination procedures in the unrestricted non-uniform model

Let us now analyze from a general non-uniform point of view how the seminumerical elimination procedure designed in [11] and [10] works on a given flat family of zero-dimensional elimination problems.

Let $T_1,\ldots,T_m,X_1,\ldots,X_n,Y$ be indeterminates over the ground ground field k and let $G_1,\ldots,G_n,F$ be polynomials belonging to the k-algebra $k[T_1,\ldots,T_m,X_1,\ldots,X_n]$. Let $d := \max\{\deg G_1,\ldots,\deg G_n\}$ and suppose that $G_1,\ldots,G_n$ and F are given by straight–line programs in $k[T_1,\ldots,T_m X_1,\ldots,X_n]$ of length L and K respectively. Suppose that the polynomials $G_1,\ldots,G_n$ form a regular sequence in $k[T_1,\ldots,T_m,X_1,\ldots,X_n]$ defining thus an equidimensional subvariety $V=\{G_1=0,\ldots,G_n=0\}$ 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 $D\le\delta$ 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 $P\in k[T_1,\ldots,T_m,Y]$ be the minimal polynomial of the image of $\tilde\pi$. The polynomial P is monic in Y and one sees immediately that $\deg P\le\delta\deg F$ and $\deg_Y P\le D$ holds. Let us write $\delta_* := \deg_{T_1,\ldots,T_m} P$.

Let us consider as Algorithm 1 and Algorithm 2 two non-uniform variants of the basic elimination method designed in [11] and [10].

- 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 $G_1=0,\ldots,G_n=0$ (observe that always $\delta\le\Delta\le\deg G_1\cdots\deg G_n$ holds). The output is a straight–line program Γ_1 in $k[T_1,\ldots,T_m,Y]$ 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 $t=(t_1,\ldots,t_m)$ of k^m which has the additional property that the image of F restricted to the set $\{t\}\times\pi^{-1}(t)$ has cardinality $D_*=\deg_Y P$. The algorithm produces then a straight–line program Γ_2 in $k[T_1,\ldots,T_m,Y]$ 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 straight–line programs Γ_1 and Γ_2. We are going now to analyze the question whether a complexity of type $K\delta^{O(1)}$ is intrinsic for the elimination problem under consideration.

In the next subsection we are going to exhibit an example of a particular zero-dimensional elimination problem for which the quantity $K\delta$ appears as a lower bound for the nonscalar size of the output polynomial in the *unrestricted non-uniform* complexity model.

2.1 A particular flat family of zero-dimensional elimination problems

Let $S, T_1, \ldots, T_\delta, X, Y$ be indeterminates over $\mathbb{Q}$ and let
$G := \prod_{1 \leq l \leq \delta}(X - T_l)$ and $F := SX^{2^K}$. Let $V := \{G = 0\}$ be the hypersurface of $\mathbb{A}^{\delta+2}$ defined by the polynomial G and let $\pi : V \longrightarrow \mathbb{A}^{\delta+1}$ be the finite, generically unramified morphism induced by the canonical projection of $\mathbb{A}^{\delta+2}$ onto $\mathbb{A}^{\delta+1}$.

Observe that δ is the degree of the hypersurface V of $\mathbb{A}^{\delta+2}$ and of the morphism π (in fact V is the union of δ distinct hyperplanes of $\mathbb{A}^{\delta+2}$).

The polynomials G and F have a nonscalar complexity δ and $K+1$ respectively. They represent a flat family of zero-dimensional elimination problems with $m := \delta + 1, n := 1, \deg V = \delta$ and $\deg \pi = \delta$ (see Subsection 1.1). The general solution of this elimination problem is represented by the polynomial

$$P := \prod_{1 \leq l \leq \delta} (Y - ST_l^{2^K}) = Y^\delta - Y^{\delta-1} S \sum_{1 \leq l \leq \delta} T_l^{2^K} + \text{ higher degree terms in } S$$

which belongs to $\mathbb{Q}[S, T_1, \ldots, T_\delta, Y]$. Let Γ be straight–line program of nonscalar length $L(\Gamma)$ in $k[S, T_1, \ldots, T_\delta, Y]$ which computes the polynomial P. We transform the circuit Γ into a straight–line program Γ^* in $\mathbb{Q}[T_1, \ldots, T_\delta]$ of nonscalar length $L(\Gamma^*) \leq 3L(\Gamma)$ which computes the polynomial $R := \sum_{1 \leq l \leq \delta} T_l^{2^K}$.

This can be done as follows: first we derive the straight–line program Γ with respect to the variable S and then we specialize S and the variable Y into the values 0 and 1 respectively.

Analyzing the complexity of the polynomial R by means of Strassen's degree method as in [2], [19] we find that $L(\Gamma^*) \geq (K-1)\delta$ holds. This implies $L(\Gamma) \geq \frac{1}{3}(K-1)\delta = \Omega(K\delta)$.

Unfortunately the meaning of the parameter δ is ambiguous: δ is the degree of the variety V and the degree of the morphism π as well as the nonscalar complexity of the polynomial G. Nevertheless our example shows that any optimal elimination procedure which produces the general solution of a given flat family of zero-dimensional elimination problems has an inherent complexity which depends linearly on the nonscalar length of the polynomial which defines the projection we are considering. The factor of proportionality of this linear dependence appears as an invariant of the equational part of our elimination problem. For the moment we are not able to interpret unambiguously this factor of proportionality. It is always bounded from above by a polynomial function of the straight–line program size, of the number of variables eliminated and of the degree of the input variety and appears in some cases as bounded from below by a quantity which may be interpreted alternatively as the degree of the input system or as its nonscalar length. This leads us to the following notion of *elimination complexity* of a given flat family of zero-dimensional elimination problems. This notion is the subject of the next subsection.

2.2 The elimination complexity of a zero-dimensional polynomial equation system

Let $T_1, \ldots, T_m, X_1, \ldots, X_n, Y$ be indeterminates over k and let $G_1, \ldots, G_n \in k[T_1, \ldots, T_m, X_1, \ldots, X_n]$ be polynomials forming a regular sequence in $k[T_1, \ldots, T_m, X_1, \ldots, X_n]$. Let $V = \{G_1 = 0, \ldots, G_n = 0\}$ be the equidimensional variety defined by the polynomials $G_1, \ldots, G_n$ and let $\pi: V \longrightarrow \mathbb{A}^m$ be the morphism of affine varieties induced by the canonical projections of $\mathbb{A}^{m+n}$ onto $\mathbb{A}^m$. Suppose that π is finite and generically unramified and observe that V has dimension m.

For any polynomial $F \in k[T_1, \ldots, T_m, X_1, \ldots, X_n]$ we consider the flat family of zero-dimensional elimination problems given by the equations $G_1 = 0, \ldots, G_n = 0$ and the polynomial F. Let $P_F \in k[T_1, \ldots, T_m, Y]$ be the general solution of this problem. Let $L(F)$ and $L(P_F)$ be the nonscalar complexity of the polynomials F and P_F respectively. Observe that the set of values

$$N_{G_1,\ldots,G_n} := \{\frac{L(P_F)}{L(F)}; F \in K[T_1, \ldots, T_m, X_1, \ldots, X_n]\}$$

is bounded by a quantity which depends polynomially on the degree of V and the number n of variables to be eliminated (compare this with the length of the straight–line program Γ_1 in Algorithm 1 in this section).

We define now the supremum $\sup N_{G_1,\ldots,G_n}$ as the *elimination complexity* of the equation system $G_1 = 0, \ldots, G_n = 0$. In the example of the previous subsection the nonscalar straight–line program length of the equational part of the input system equals the quantity $\deg V$ and this quantity represents a lower bound for the elimination complexity of the given equation system.

References

[1] B. Bank, M. Giusti, J. Heintz, and G. Mbakop. Polar Varieties and Efficient Real Equation Solving: The Hypersurface Case. *J. of Complexity*, **vol. 13 (1)**:pp. 5–27, 1997.

[2] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comp. Sci.*, **vol. 22**:pp. 317–330, 1983.

[3] L. Blum, F. Cucker, M. Shub, and S. Smale. Complexity and Real Computation. preprint, 1997.

[4] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. of the AMS*, **vol. 21 (1)**:pp. 1–46, 1989.

[5] P. Bürgisser, M. Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory*, vol. 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.

[6] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: an introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer Verlag, Berlin, 1992.

[7] I. Emiris. On the Complexity of Sparse Elimination. *J. Complexity*, **vol. 12**:pp. 134–166, 1996.

[8] J. von zur Gathen. Parallel arithmetic computations: a survey. In B. R. J. Gruska and J. Wiedermann, eds., *Proceedings of the 12th Symposium on Mathematical Foundations of Computer Science*, vol. 233 of *LNCS*, pp. 93–112. Springer, Bratislava, Czechoslovakia, August 1986.

[9] J. von zur Gathen. Parallel Linear Algebra. In J. H. Reif, ed., *Synthesis of Parallel Algorithms*. Morgan Kaufmann, 1993.

[10] 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*, vol. 117,118, pp. 277–317. Journal of Pure and Applied Algebra, 1997.

[11] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight–Line Programs In Geometric Elimination Theory. *to appear in J. of Pure and App. Algebra*, pp. 1–46, 1997.

[12] J. Heintz. The Project TERA: the Comeback of Oblomov in Computer Science. *SAC Newsletter*, **vol. 1**, nov 1996.

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

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

[15] B. Mishra. *Algorithmic Algebra*. Springer Verlag, New York, 1993. ISBN 0-387-94090-1.

[16] D. Mumford. *The Red Book of Varieties and Schemes*, vol. 1358 of *LNM*. Springer, Berlin, first edition, 1988.

[17] L. M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, eds., *Applied Algebra, Algebraic Algorithms and Error Corecting Codes. Proceedings of AAECC-11*, vol. 948 of *LNCS*. Springer, 1995.

[18] I. Shafarevich. *Basic algebraic geometry*. Graduate Texts in Mathematics. Springer-Verlag, 1984.

[19] V. Strassen. Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationspolynomen. *Numer. Math.*, **vol. 2**:pp. 238–251, 1973.

[20] V. Weispfenning and T. Becker. *Groebner bases: a computational approach to commutative algebra*, vol. 141 of *Graduate Texts in Mathematics: readings in mathematics*. Springer, 1993.