

On the time–space complexity of geometric elimination procedures*

Joos Heintz^{1,2,3}, Guillermo Matera^{4,5}, Ariel Waissbein²

¹ Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, Avda. de Los Castros s/n, E-39071 Santander, España, heintz@matesco.unican.es

² Departamento de Matemáticas, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I, (1428) Buenos Aires, Argentina, {joos,awaisbe}@dm.uba.ar

³ Member of CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas), Argentina

⁴ Departamento de Computación, Universidad Favaloro, Belgrano 1723, (1093) Buenos Aires, Argentina, gmatera@favaloro.edu.ar

⁵ Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, Roca 850 (1663) San Miguel, Pcia. de Buenos Aires, Argentina, gmatera@ungs.edu.ar

Abstract In [25] and [22] a new algorithmic concept was introduced for the symbolic solution of a zero dimensional complete intersection polynomial equation system satisfying a certain generic smoothness condition. The main innovative point of this algorithmic concept consists in the introduction of a new geometric invariant, called the *degree of the input system*, and the proof that the most common elimination problems have time complexity which is *polynomial* in this degree and the length of the input.

In this paper we apply this algorithmic concept in order to exhibit an elimination procedure whose space complexity is only *quadratic* and its time complexity is only *cubic* in the degree of the input system.

Send offprint requests to: Guillermo Matera, Departamento de Computación, Universidad Favaloro, Belgrano 1723 (1093) Buenos Aires, Argentina

* Research was partially supported by the following Argentinian, French, German and Spanish grants : UBA–CyT TW80, PIP CONICET 4571, ANPCyT PICT 03–00000–01593, BMBF–SeTCIP AL/A97–EXI/09, DGICYT PB96–0671–C02–02, ECOS–SeTCIP A99E06.

Correspondence to: Guillermo Matera, Departamento de Computación, Universidad Favaloro, Belgrano 1723 (1093) Buenos Aires, Argentina

Key words Algorithmic elimination theory, polynomial equation solving, symbolic computation, algebraic complexity theory, time–space complexity, computation tree, straight–line program.

1 Introduction

The development of efficient algorithms for real–life purposes often requires the optimization of more than one resource at the same time. The two most significant resources for practical computing issues are *memory space* and *running time*. Generally, these two resources can not be minimized simultaneously (independently from each other), as they are linked by a time–space tradeoff function which is intrinsic to the problem treated. Our goal here is to analyze the intrinsic time–space complexity of multivariate polynomial elimination problems.

It is well known that algorithmic multivariate polynomial elimination faces serious complexity problems. As it was shown by E. Mayr and A. Meyer in [51], the typical *algebraic* elimination problems are computationally *infeasible* since they are EXPSPACE–complete (see also [50], [45] and [44]).

This fact is reflected by the complexity behaviour of the currently available software on the subject, mainly based on Gröbner basis computations (see [10]). The typical symptoms which can be observed when confronting these software packages with realistically sized problems, are out–of–memory errors.

This observation suggests the search for efficient *geometric* elimination procedures which may replace the known algebraic ones. This suggestion is also supported by the fact that all the most classical *geometric* elimination problems belong to the complexity class PSPACE (see [14], [13], [17], [24], [49], [48]).

On the other hand the limitation to geometric problems and algorithms does not suffice to settle the practical complexity issue of elimination. This is due to the impossibility to design general purpose elimination algorithms with polynomial time (and space) behaviour which are based on the classical dense encoding of multivariate polynomials. A well-known example due to D. Lazard, T. Mora, W. Masser and P. Philippon (see [9]) shows that exponential time behaviour is unavoidable while using dense representation of polynomials.

From these observations we infer the necessity of using alternative data structures for the representation of multivariate polynomials. One such possibility is the encoding of polynomials (and rational numbers) by arithmetic circuits and their related evaluation schemes or *straight–line programs* (see [53]).

Although geometric elimination algorithms based on straight–line program (*SLP*) encoding of multivariate polynomials improve drastically the complexity behaviour of their forerunners based on dense encoding (see [24], [28], [20], [41] or [42]), the complexity issue remains still unsatisfactory. From the main result of [37] one deduces that any *general purpose* elimination algorithm based on *SLP*–encoding of polynomials must necessarily have an exponential time complexity behaviour on infinitely many examples, provided the *SLP* representing the input polynomials is treated as a black box by the algorithm.

This insight leads in [26], [25], [22] and [27] to the consideration of a new intrinsic geometric invariant, associated to the input equation system, namely its

geometric degree (see also [47], [52], [32], [33], [36]). The new outcome consists in the conclusion that elimination has *polynomial time* character in the (syntactical) size of the input equation system (given by a straight–line program program or in sparse representation) *and* the (geometric) degree of the input system. Of course, this degree may be of exponential size in the number of variables to be eliminated (it is bounded by the Bezout number of the input system), but in case that this degree is considerably smaller than the Bézout number, the new algorithmic concept introduced in [25] and [22] becomes of practical interest. The main outcome of the mentioned work is the observation that elimination polynomials have only “small” circuit complexity. In fact, such a polynomial can be evaluated by a straight–line program whose length is roughly of the same order as its degree, even if the polynomial under consideration contains many variables. By the way, the classical elimination procedure of Kronecker [43] is vindicated by this work as the most powerful and efficient algorithm of all the times, although it received in the past a lot of negative criticism (see e.g. [46], [66]).

This was the starting point for the ongoing work of the TERA¹(=Turbo Evaluation and Rapid Algorithms) group on highly performant algorithms and computer programs for the design of an efficient solver for polynomial equation and inequality systems over the complex and real numbers (see [3] and [4] for progress in the real case).

These pages will be devoted to the design of an elimination algorithm which realizes the algorithmic concepts developed in [25] and [22] from a time–space tradeoff point of view. At the beginning we deduce, based on a result of J. Ja’Ja’ [38], that the algorithmic concepts of [25] and [22] cannot be realized using *sub-linear* space without causing a superpolynomial growth of the time–space tradeoff complexity.

Then, following Schönhage’s GOLDEN RULE NUMBER 1: *Do care about the constants!* [56], we develop an elimination algorithm which has *quadratic* space and *cubic* time complexity (in terms of the geometric degree of the input system). For this purpose we design a series of new algorithms for classical linear algebra tasks, for the manipulation of univariate polynomials and an effective Shape Lemma version which is particularly adapted to the special features of the main algorithm of [25] and [22].

1.1 Notations, assumptions and statement of the main result

Let X_1, \dots, X_n be indeterminates over the rational numbers \mathbf{Q} and let $\mathbf{Q}[X_1, \dots, X_n]$ denote the ring of n -variate polynomials over \mathbf{Q} . Let d be a natural number and let be given polynomials $F_1, \dots, F_n \in \mathbf{Q}[X_1, \dots, X_n]$ of degree at most d . Assume that F_1, \dots, F_n define a regular sequence in $\mathbf{Q}[X_1, \dots, X_n]$. Assume also that for $1 \leq r \leq n - 1$ the polynomials F_1, \dots, F_r span a *radical* ideal (F_1, \dots, F_r) in $\mathbf{Q}[X_1, \dots, X_n]$ and denote by V_r the equidimensional algebraic variety $V(F_1, \dots, F_r)$ defined by F_1, \dots, F_r in the complex n -dimensional

¹ Europe: <http://tera.medicis.polytechnique.fr/>
America: <http://www.dm.uba.ar/tera/>

affine space \mathbb{C}^n . Finally we assume that there is given a division-free straight-line program in $\mathbb{Q}[X_1, \dots, X_n]$ evaluating the polynomials F_1, \dots, F_n in space \mathcal{S} and time \mathcal{T} .

In the sequel we shall consider algorithms which “solve” symbolically the (input) equation system $F_1 = 0, \dots, F_n = 0$ over the complex numbers \mathbb{C} . As in [25] and [22] we associate to the equation system $F_1 = 0, \dots, F_n = 0$ a parameter δ , called the *geometric degree* of the system, which is defined as follows: for $1 \leq r \leq n$ let $\deg(V_r)$ denote the (geometric) degree of V_r , as introduced in [34]. The geometric degree of the system $F_1 = 0, \dots, F_n = 0$ is then defined as

$$\delta := \max_{1 \leq r \leq n} \deg(V_r).$$

In order to describe the geometric aspect of our procedure we need some more terminology, essentially borrowed from [22]. Let $2 \leq r \leq n$ and let us consider the $(n-r)$ -dimensional \mathbb{Q} -definable closed affine subvariety $V := V_r$ of \mathbb{C}^n . A *geometric solution* of the algebraic variety V consists of the following items:

- a \mathbb{Q} -linear change of variables, transforming the variables X_1, \dots, X_n into new ones, namely Y_1, \dots, Y_n , such that the linear map from \mathbb{C}^n to \mathbb{C}^{n-r} defined by the forms Y_1, \dots, Y_{n-r} induces a finite surjective morphism of affine varieties $\pi : V \rightarrow \mathbb{C}^{n-r}$. Such a variable transformation is called a *Noether normalization* of the variety V and we say that the variables Y_1, \dots, Y_n are in *Noether position* with respect to V , the variables Y_1, \dots, Y_{n-r} being *free*. The given Noether normalization induces an integral ring extension $R := \mathbb{Q}[Y_1, \dots, Y_{n-r}] \rightarrow \mathbb{Q}[V]$ (where $\mathbb{Q}[V]$ denotes the coordinate ring of the variety V). Observe that $\mathbb{Q}[V]$ is a free R -module whose rank we denote by $\text{rank}_R \mathbb{Q}[V]$. Notice that $\text{rank}_R \mathbb{Q}[V] \leq \deg V$ (see e.g. [28]) and $\mathbb{Q}[V] \cong \mathbb{Q}[X_1, \dots, X_n]/(F_1, \dots, F_r)$ holds.
- a \mathbb{Q} -linear form $U := \lambda_{n-r+1}Y_{n-r+1} + \dots + \lambda_n Y_n$ which induces a primitive element of the ring extension $R \rightarrow \mathbb{Q}[V]$, i.e. an element u of the coordinate ring $\mathbb{Q}[V]$ whose (monic) minimal polynomial $q \in R[T]$ over R satisfies the condition $\deg_T q = \text{rank}_R \mathbb{Q}[V]$ (here T is a new indeterminate and $\deg_T q$ denotes the partial degree of the polynomial $q \in R[T] = \mathbb{Q}[Y_1, \dots, Y_{n-r}][T]$ with respect to the variable T). Observe here that we always have $\deg q = \deg_T q \leq \deg V$ with $\deg q$ denoting the total degree of q .
- the minimal polynomial q of u over R .
- a generic “*parametrization*” of the variety V by the zeroes of q , given by polynomials of the form $\rho_{n-r+1}^{(u)} Y_{n-r+1} - v_{n-r+1}^{(u)}(T), \dots, \rho_n^{(u)} Y_n - v_n^{(u)}(T)$ with $\rho_{n-r+1}^{(u)}, \dots, \rho_n^{(u)} \in R \setminus \{0\}$ and $v_1^{(u)}, \dots, v_n^{(u)} \in R[T]$. We require that $\max\{\deg_T v_{n-r+1}^{(u)}, \dots, \deg_T v_n^{(u)}\} < \deg_T(q)$ and $\rho_{n-r+j}^{(u)} Y_{n-r+j} - v_{n-r+j}^{(u)}(T) \in I(V)$ holds for $1 \leq j \leq r$ (here $I(V)$ denotes the vanishing ideal of V , namely $I(V) = (F_1, \dots, F_r)$). Observe that this parametrization is unique up to scaling by nonzero elements of \mathbb{Q} .

Let us here remark that this notion of “geometric solution” has a long history, which goes back at least to L. Kronecker [43] (see also [46], [70]). One might

consider [15] and [30] as early references where this notion was implicitly used for the first time in modern symbolic computation.

Given a Noether normalization of the variety V as before, we call a point $P := (p_1, \dots, p_{n-r}) \in \mathbb{Z}^{n-r}$ a *lifting point* of V if the finite surjective morphism $\pi : V \rightarrow \mathbb{C}^{n-r}$ is unramified in P , i.e. if the equations $F_1 = 0, \dots, F_n = 0, Y_1 = p_1, \dots, Y_{n-r} = p_{n-r}$ define the fiber $\pi^{-1}(P)$ by transversal cuts. We call the zero–dimensional variety $V_P := \pi^{-1}(P)$ the *lifting fiber* of the point P .

Assume now that there is given as before a geometric solution of the $(n-r)$ –dimensional variety V and a lifting point P satisfying the condition $\rho_{n-r+1}(P) \neq 0, \dots, \rho_n(P) \neq 0$ and $\text{discr}_T q(P) \neq 0$, where $\text{discr}_T q$ denotes the discriminant of the polynomial q with respect to the variable T . Then the given geometric solution of the variety V induces a geometric solution of the lifting fiber V_P . This geometric solution of V_P is given by the linear form U , the polynomial $q(P, T) \in \mathbb{Q}[T]$ and the parametrization $\rho_{n-r+1}(P)Y_{n-r+1} - v_{n-r+1}^{(u)}(P, T), \dots, \rho_n(P)Y_n - v_n^{(u)}(P, T)$ (observe that all these entities are well defined because $\mathbb{Q}[V] \cong \mathbb{Q}[X_1, \dots, X_n]/(F_1, \dots, F_n)$ is a free R –module and because of our requirement $\rho_{n-r+1}(P) \neq 0, \dots, \rho_n(P) \neq 0$). We call such a geometric solution of the variety V *compatible* with the lifting point P .

Let us denote by $F_1(Y_1, \dots, Y_n), \dots, F_n(Y_1, \dots, Y_n)$ the elements of the polynomial ring $\mathbb{Q}[Y_1, \dots, Y_n]$ that we obtain if we rewrite the polynomials $F_1(X_1, \dots, X_n), \dots, F_n(X_1, \dots, X_n)$ in the variables Y_1, \dots, Y_n . Observe then that the unramifiedness of π in the lifting point P means that

$$(F_1(P, Y_{n-r}, \dots, Y_n), \dots, F_n(P, Y_{n-r}, \dots, Y_n))$$

is a radical ideal of $\mathbb{Q}[Y_{n-r+1}, \dots, Y_n]$. This is equivalent to saying that

$$\mathbb{Q}[V_P] \cong \mathbb{Q}[Y_{n-r+1}, \dots, Y_n]/(F_1(P, Y_{n-r}, \dots, Y_n), \dots, F_n(P, Y_{n-r}, \dots, Y_n))$$

holds.

The complexity of the procedure that we are going to design for the resolution of the system $F_1 = 0, \dots, F_n = 0$ will be described in terms of the following *syntactic* and *geometric* parameters:

- n , the number of variables,
- d , the maximum of the degrees of the polynomials F_1, \dots, F_n ,
- \mathcal{S} and \mathcal{T} , the space and time complexity of the given straight–line program in $\mathbb{Q}[X_1, \dots, X_n]$ which evaluates the polynomials F_1, \dots, F_n ,
- the geometric degree δ of the input system $F_1 = 0, \dots, F_n = 0$.

The algorithmic method proposed in [25] and [22] proceeds in $n-1$ stages, computing at each stage $2 \leq r \leq n$ a suitable finite projection π_r of the variety V_r onto the affine space \mathbb{C}^{n-r} , a suitable lifting point $P^{(r)} \in \mathbb{Z}^{n-r}$ and a geometric solution of the lifting fiber $V_{P^{(r)}} := (V_r)_{P^{(r)}}$ associated to the lifting point $P^{(r)}$ and the variety V_r . Then a geometric solution of the variety V_r is (re)constructed from the lifting fiber $V_{P^{(r)}}$ and the straight–line program representing the input polynomials F_1, \dots, F_r . For this purpose the idea of a division–free symbolic version of the Newton–Hensel algorithm is used. Then a Noether normalization of

the variety V_{r+1} and a new lifting point $P^{(r+1)}$ for V_{r+1} are determined. Finally a geometric solution of the lifting fiber $V_{P^{(r+1)}}$ is computed.

In this paper we realize the general algorithmic ideas of [25] and [22] by exhibiting a *practically efficient* (implementable) algorithm computing the geometric solution of the variety $V(F_1, \dots, F_n)$. For this purpose we introduce some modifications in the method of [25] and [22], we design a series of algorithms for specific linear algebra tasks and for the manipulation of univariate polynomials and we develop a new effective version of the so-called Shape Lemma (see [40], [14] or [30]).

The first modification consists roughly speaking in the determination of a simultaneous Noether normalization of all the varieties V_1, \dots, V_n and a simultaneous *a priori* determination of the corresponding lifting points $P^{(1)}, \dots, P^{(n-1)}$. The main purpose of this first modification is to obtain for $2 \leq r \leq n$ a lifting fiber $V_{P^{(r+1)}}$ with the following property: for any point $(x_1, \dots, x_n) \in V_{P^{(r+1)}}$, the morphism π_r is unramified in (x_1, \dots, x_{n-r}) . This property is crucial in order to avoid the introduction of additional (extraneous) points while computing the geometric solution of the lifting fiber $V_{P^{(r+1)}}$ from the geometric solution of $V_{P^{(r)}}$. The involuntary introduction of additional points in the procedure developed in [25] and [22] produces an unnecessary quadratic growth of the code size of the polynomials which appear during the algorithm (with the consequent undesired effect on the time and space complexity of the procedure).

A second modification of the algorithmic method designed in [25] and [22] consists in the development of an efficient subalgorithm which produces a geometric solution of the variety V_r from the geometric solution of the lifting fiber $V_{P^{(r)}}$. The symbolic Newton–Hensel algorithm used by this method requires to deal with very special matrices, which arise from the evaluation of a univariate polynomial in a Frobenius matrix. By means of simple duality techniques for univariate polynomials we obtain an efficient algorithm which computes the characteristic polynomial of such matrices, improving in this way considerably upon the time–space complexity of the main algorithm of [25] and [22].

Another important feature of the algorithmic method proposed by [25] and [22] is the use of a method — originally due to [42] — which reduces the general problem of finding a Shape Lemma–like representation of a given zero–dimensional complete intersection variety to the case of an algebraic variety defined by only two polynomials in two separate variables. We revise this method, replacing the generalistic linear algebra tools applied in [42] by more specific ones based on the manipulation of univariate polynomials. In this way we obtain a significant reduction of the time–space complexity of the corresponding subalgorithm of [42].

Finally we focus our attention on the subalgorithm which computes a geometric solution of the lifting fiber $V_{P^{(r+1)}}$ from a geometric solution of the lifting fiber $V_{P^{(r)}}$. The method used in [25] and [22] is divided in two stages. In the first stage a geometric solution of the variety V_r is obtained. Then a geometric solution of the intersection of the variety V_r with the hypersurface $\{F_{r+1} = 0\}$ is computed.

From this geometric solution one obtains a geometric solution of the lifting fiber $V_{P^{(r+1)}}$ just by specializing the remaining free variables of the given geometric solution of $V_r \cap \{F_{r+1} = 0\}$ into the coordinates of the point $P^{(r+1)}$. In this

paper we increase significantly the efficiency of this procedure reducing the task to the computation of a geometric solution of the intersection of the hypersurface $\{F_{r+1} = 0\}$ with a suitably introduced curve $W_{P(r+1)}$ which is contained in the $(n - r)$ -dimensional variety V_r . The technique of specializing the free variables represents a general method coming from theoretical computer science called *deforestation* (see [69]). In [23] this method is systematically applied in a computer algebra context. Our technique of lifting a projection from a zero-dimensional variety to a curve was independently discovered and applied in [29].

The final outcome is a *quadratic*-space and *cubic*-time procedure which computes the geometric solution of the given zero-dimensional algebraic variety $V(F_1, \dots, F_n)$. More precisely, we obtain the following complexity result:

Theorem 1 *Let notations and assumptions be as before. Then there exists a computation tree in $\mathbf{Q}[X_1, \dots, X_n]$ that computes a geometric solution of the algebraic variety $V = V(F_1, \dots, F_n)$ using space $O(Sdn\delta^2)$ and time $O((Tdn^2 + n^5)\delta^3 \log^3 \delta \log^2 \log \delta)$.*

In contrast to this result let us mention that a straightforward implementation of the algorithmic method proposed by [25] and [22] leads to an algorithm using space $O(Sdn\delta^4)$ and time $O(Tdn^6\delta^{16})$. Let us also remark that in the practical situations we have in mind, the quantity δ is expected to be much larger than the values of the parameters S , T , d and n . In this sense we are saying that our algorithm requires only *quadratic* space and *cubic* time.

The computational model we use in this paper is algebraic: we count operations at unit costs. One may argue that this is unrealistic. However, a practical implementation of the basic algorithmic ideas applied in this paper would necessarily rely on modular arithmetic. Nevertheless, for modular arithmetic our complexity model is suitable (compare the implementation work [29]).

2 On time–space tradeoffs

The efficient representation of multivariate polynomials and rational functions is of central importance for geometric elimination procedures (cf. [53]). Here we discuss the representation of multivariate polynomials by *arithmetic circuits* (see e.g. [67] or [68]).

Let $\mathbf{Q}(X_1, \dots, X_n)$ denote the field of rational functions over \mathbf{Q} in the variables X_1, \dots, X_n . An arithmetic circuit β in $\mathbf{Q}(X_1, \dots, X_n)$ is a *directed acyclic graph* (computation DAG for short), whose nodes have all bounded indegree of either 0 or 2. The nodes of indegree 0 are labeled by elements of the set $\mathbf{Q} \cup \{X_1, \dots, X_n\}$ and the nodes of indegree 2 (called *internal nodes*) are labeled by one of the arithmetic operations addition, subtraction, multiplication or division. The nodes of indegree 0 labeled by elements of $\{X_1, \dots, X_n\}$ are called *input nodes*. The nodes of indegree 0 labeled by elements of \mathbf{Q} are called *parameter nodes*. The elements of \mathbf{Q} occurring in that way are called *parameters* of the arithmetic circuit β . Finally, some nodes of the arithmetic circuit β are labeled as

output nodes (typically, the output nodes will be the nodes with out-degree 0). We denote the underlying computation *DAG* of β by $\Gamma(\beta)$.

When starting from the input nodes and proceeding along the computation *DAG*, to each node ρ there corresponds in a natural way a rational function Q_ρ computed as the result of all previous steps. Let be given s distinct rational functions $F_1, \dots, F_s \in \mathbf{Q}(X_1, \dots, X_n)$ and an arithmetic circuit β in $\mathbf{Q}(X_1, \dots, X_n)$ with s output nodes. We say that F_1, \dots, F_s are *represented* by β , if F_1, \dots, F_s are the rational functions associated to the output nodes of β .

In order to modelize the computation with arithmetic circuits, we introduce the notion of a *pebble game*. A pebble game converts a given arithmetic circuit β into a sequential algorithm (also called *straight-line program*) and associates to β natural time and space measures. On the computation graph $\Gamma(\beta)$ of the arithmetic circuit β we may play a pebble game subject to the following rules (see [7]):

- P1 any indegree 0 node of $\Gamma(\beta)$ can be pebbled,
- P2 if the predecessor nodes of a given node ρ of $\Gamma(\beta)$ are both pebbled, then ρ can be pebbled by a new pebble or just by moving a pebble from one of the predecessor nodes to ρ ,
- P3 a pebble can always be removed from a pebbled node of $\Gamma(\beta)$.

The pebble game finishes when all the output nodes of $\Gamma(\beta)$ are pebbled. Observe that the computation graph $\Gamma(\beta)$ does not determine a pebble game uniquely, i.e. different pebble games may be played on $\Gamma(\beta)$.

We associate to a given pebble game on the computation graph $\Gamma(\beta)$ the following complexity measures:

- C1 a *space* measure given by the maximum number of pebbles used at any moment of the game,
- C2 a *time* measure given by the number of pebble placements performed during the game following rules P1 and P2.

Any fixed pebble game on the computation graph $\Gamma(\beta)$ defines a strategy of evaluation of β which we call a *straight-line program*. A straight-line program in $\mathbf{Q}(X_1, \dots, X_n)$ which computes rational functions F_1, \dots, F_s is a sequence $\beta = (Q_1, \dots, Q_r)$ of elements of the field $\mathbf{Q}(X_1, \dots, X_n)$ with the following properties:

- i) $\{F_1, \dots, F_s\} \subseteq \{Q_1, \dots, Q_r\}$,
- ii) for any $1 \leq \rho \leq r$, the rational function Q_ρ belongs to $\mathbf{Q} \cup \{X_1, \dots, X_n\}$ or there exist $1 \leq \rho_1, \rho_2 < \rho$ and an arithmetic operation op_ρ belonging to the set $\{+, -, *, /\}$ such that $Q_\rho = Q_{\rho_1} op_\rho Q_{\rho_2}$ holds.

Straight-line programs have been extensively used to modelize algebraic computations (see for example [8], [65], [63], [35], [53], [11]). Since the late seventies the relevance of this concept for multivariate polynomial elimination became more and more evident (see e.g. [24], [28], [20], [19], [42], [26], [25], [22], [3]).

Our model of computation is based on the concept of arithmetic circuits and straight-line programs. However, a model of computation consisting *only* of arithmetic circuits and straight-line programs is not expressive enough for our purpose,

namely, the description of a general geometric elimination procedure. Therefore our model of computation has to include decisions and selections (subject to previous decisions). For this reason we shall consider *arithmetic–boolean circuits* (also called *arithmetic networks*) instead of arithmetic circuits and *computation trees* instead of straight–line programs. An arithmetic–boolean circuit is nothing but a *DAG* whose nodes are labeled either by arithmetic operations or by selections (pointing to other nodes) subject to previous equal–to–zero decisions. A pebble game on an arithmetic–boolean circuit gives rise to a computation tree, fixing thus a strategy of evaluation of the given arithmetic–boolean circuit. In other words, a computation tree is nothing but a straight–line program with *branchings*. Time and space of the evaluation of a given computation tree are defined analogously as in the case of straight–line programs (see. e.g. [67], [68] or [11] for more details on the notion of arithmetic–boolean circuits and computation trees).

From now on we shall tacitly assume that our arithmetic–boolean circuits and computation trees in $\mathbf{Q}[X_1, \dots, X_n]$ contain only *non–essential* divisions (i.e. only divisions by nonzero elements of \mathbf{Q}).

Let us now briefly discuss the time–space tradeoff complexity of the procedures in [25] and [22]. These procedures are described by arithmetic–boolean circuits of size $(nd\delta L)^{O(1)}$ and nonscalar depth $O((\log_2 n + \ell) \log_2 \delta)$, where as before n bounds the number of variables and d bounds the degree of the input polynomials, δ is the (affine) degree of the input system and finally, L and ℓ are the size and nonscalar depth of an arithmetic circuit representing the input polynomials.

We first observe, that using a standard *breadth–first search* scheme for the evaluation of the arithmetic–boolean circuits described in [25] and [22], we obtain a computation tree using space and time $(nd\delta L)^{O(1)}$.

Similarly, using a *depth–first search* scheme as in [6], we obtain a computation tree using space $O((\log_2 n + \ell) \log_2 \delta)^{O(1)}$ and time $Ln\delta^{O(\log_2 n + \ell)}$ for the same task (see [47]).

It would be desirable to combine the advantages of these two computation trees, namely, to construct a computation tree which uses only space $O((\log_2 n + \ell) \log_2 \delta)^{O(1)}$ and time $(nd\delta L)^{O(1)}$. Unfortunately, there seems to be little hope for the simultaneous optimization of both space and time requirements up to this level.

The main algorithm of [25] and [22] relies heavily on linear algebra tasks such as the computation of the characteristic polynomial or the determinant of matrices of size $\delta \times \delta$. As shown in [67] or [68], these tasks are of equal computational difficulty as the iterated matrix product of δ matrices of size $\delta \times \delta$. With respect to the latter task, the following result is known [38]:

Theorem 2 ([38], Theorem 5.3) *Let A_1, \dots, A_δ be δ matrices in $\mathbf{Q}^{\delta \times \delta}$. Then the time \mathcal{T} required to compute the product $A_1 \cdots A_\delta$ using space \mathcal{S} verifies:*

$$\mathcal{T} = \Omega \left(\frac{\delta^{l+1}}{\mathcal{S}^{l-2}} \right), \quad \text{where } l \geq \lceil \log \delta \rceil + 2.$$

From this theorem we deduce that using *sublinear* space algorithms (i.e. algorithms having for some constant $c < 1$ space complexity $O(\delta^c)$) in order to solve the linear algebra tasks posed by the main algorithm in [25] and [22] would produce an elimination procedure of superpolynomial $\delta^{O(\log \delta)}$ time complexity. Hence, sublinear space algorithms for linear algebra tasks do not produce the desired time–space tradeoff effect in our main algorithm.

In view of this conclusion, we see that *linear* space is the most space efficient alternative for linear algebra tasks if *practically feasible* procedures have to be designed. In the following sections we are going to revise the critical parts (in terms of memory usage) of the main algorithm in [25] and [22] which use linear algebra subroutines requiring *nonlinear* space. In this paper we replace these subroutines by *linear* space algorithms whose (polynomial) time complexity is as small as possible, i.e. asymptotically *quadratic*. Some more modifications of rather geometric nature of the main algorithm of [25] and [22] allow to reduce the exponent 4 of the space complexity of this algorithm to the exponent 2 announced in Theorem 1 (the simultaneous reduction of the time complexity is from exponent 16 to exponent 3).

3 Simultaneous Noether normalization

In this section we maintain the notations and assumptions established in the Introduction. The present section is devoted to the determination of a simultaneous Noether normalization of all varieties V_1, \dots, V_{n-1} and for any $1 \leq r \leq n - 2$ to the determination of a lifting point $P^{(r+1)}$ such that the corresponding lifting fiber $V_{P^{(r+1)}}$ has the following property: for any point $P := (x_1, \dots, x_n) \in V_{P^{(r+1)}}$, the morphism π_r is unramified in (x_1, \dots, x_{n-r}) . By a simultaneous Noether normalization we understand a linear change of variables given by a matrix $A \in \mathbf{Q}^{n \times n}$ such that for any $1 \leq r \leq n$ the new variables Y_1, \dots, Y_n are in Noether position with respect to the variety V_r , i.e. such that the canonical homomorphism

$$\mathbf{Q}[Y_1, \dots, Y_{n-r}] \hookrightarrow \mathbf{Q}[Y_1, \dots, Y_n]/(F_1, \dots, F_{n-r})$$

represents an integral extension of \mathbf{Q} -algebras.

In order to find the simultaneous Noether normalization and the lifting points we are looking for, we need suitable genericity conditions. The following lemma formalizes the well known fact that a generic linear change of coordinates yields a geometrically unramified Noether normalization of a given equidimensional algebraic variety. Moreover this lemma states an appropriate bound for the degree of certain polynomials whose nonvanishing expresses a suitable sufficient (and consistent) genericity condition for such a change of variables.

Lemma 1 *Let W be a nonempty and equidimensional Zariski closed subvariety of \mathbf{C}^n . Suppose that W is definable over \mathbf{Q} . Let $r := n - \dim(W)$, let $\Lambda := (\Lambda_{i,j})_{1 \leq i \leq n-r, 1 \leq j \leq n}$ be a matrix of indeterminates and let*

$$\begin{pmatrix} \tilde{Y}_1 \\ \vdots \\ \tilde{Y}_{n-r} \end{pmatrix} := \Lambda \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

Then there exists a nonzero polynomial $G \in \mathbf{Q}[A_{i,j} : 1 \leq i \leq n-r, 1 \leq j \leq n]$ such that the following conditions are satisfied:

- i) for any $(n-r) \times n$ matrix $\lambda := (\lambda_{i,j})_{1 \leq i \leq n-r, 1 \leq j \leq n} \in \mathbf{Q}^{(n-r) \times n}$ with $G(\lambda) \neq 0$, all $(n-r)$ -minors of λ are regular and the linear forms $Y_1 := \sum_{j=1}^n \lambda_{1,j} X_j, \dots, Y_{n-r} := \sum_{j=1}^n \lambda_{n-r,j} X_j$ define a finite morphism which maps the variety W onto the affine space \mathbf{C}^{n-r} ,
- ii) for $1 \leq i \leq n-r$ the polynomial G satisfies the degree estimate

$$\deg_{A_{i,1}, \dots, A_{i,n}}(G) \leq \deg W + 2(n-r)$$

(here $\deg_{A_{i,1}, \dots, A_{i,n}}(G)$ denotes the partial degree of G with respect to the variables $A_{i,1}, \dots, A_{i,n}$).

- iii) Finally, let $m \in \mathbf{Z}$, $m \geq 0$ and let Z_1, \dots, Z_m be new indeterminates. Let be given a polynomial

$$H \in \mathbf{Q}[A_{i,j}, X_j, Z_1, \dots, Z_m : 1 \leq i \leq n-r, 1 \leq j \leq n]$$

of degree at most D . Consider the Zariski closure \hat{W} of the set $(\mathbf{C}^{(n-r) \times n} \times \mathbf{C}^m \times W) \cap \{H = 0, G \neq 0\}$ and suppose that $\dim \hat{W} \leq (n-r)(n+1) + m - 1$ holds. Then the entries of the matrix Λ and the polynomials $Z_1, \dots, Z_m, \tilde{Y}_1, \dots, \tilde{Y}_{n-r}$ induce a morphism of affine spaces

$$\pi : \mathbf{C}^{(n-r) \times n} \times \mathbf{C}^m \times \mathbf{C}^n \rightarrow \mathbf{C}^{(n-r) \times n} \times \mathbf{C}^m \times \mathbf{C}^{n-r}$$

such that the Zariski closure of $\pi(\hat{W})$ is empty or a \mathbf{Q} -definable hypersurface of $\mathbf{C}^{(n-r) \times n} \times \mathbf{C}^m \times \mathbf{C}^{n-r}$ of degree at most $(n-r+1)D^2(\deg W)^3$.

Lemma 1 is a straightforward consequence of standard facts about equidimensional affine varieties and the Chow (Cayley) forms of their projective closures (compare [46], [60], [12]). We give therefore only a short account of its proof.

Proof of Lemma 1 (Sketch) Let U_1, \dots, U_n be new indeterminates. Let $\tilde{U} := U_1 X_1 + \dots + U_n X_n$ and consider $Y_1, \dots, Y_n, \tilde{U}$ as indeterminates. The Chow form P of the projective closure of the affine variety W can be interpreted as a polynomial of $\mathbf{Q}[A_{i,j}, \tilde{Y}_j, U_j, \tilde{U}, 1 \leq i \leq n-r, 1 \leq j \leq n]$ which is homogeneous of degree $\deg W$ in the variables $U_1, \dots, U_n, \tilde{U}$ and for any $1 \leq i \leq n-r$ in the variables $A_{i,1}, \dots, A_{i,n}, \tilde{Y}_i$. From the geometric properties of the Chow form P one deduces easily that the monomial $\tilde{U}^{\deg W}$ occurs in P with a nonzero coefficient \tilde{G} not containing any of the variables $\tilde{Y}_1, \dots, \tilde{Y}_n$. Thus we have

$$\tilde{G} \in \mathbf{Q}[A_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n],$$

$\tilde{G} \neq 0$ and $\deg_{A_{i,1}, \dots, A_{i,n}} \tilde{G} \leq \deg W$ for any $1 \leq i \leq n-r$. For any $1 \leq j \leq n$ we denote by ξ_j the coordinate function of W induced by the variable X_j . Let

$$\begin{pmatrix} Y_1^* \\ \vdots \\ Y_{n-r}^* \end{pmatrix} := \Lambda \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$$

and $U^* := U_1\xi_1 + \dots + U_n\xi_n$. Observe that Y_1^*, \dots, Y_{n-r}^* and U^* are algebraically independent over \mathbf{Q} ($A_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n$). From the geometric properties of the Chow form P one deduces immediately that in the \mathbf{Q} -algebra

$$\mathbf{Q}[A_{i,j}, U_j; 1 \leq i \leq n-r, 1 \leq j \leq n] \otimes_{\mathbf{Q}} \mathbf{Q}[W]$$

the algebraic identity

$$\begin{aligned} 0 &= P(\Lambda, Y_1^*, \dots, Y_{n-r}^*, U_1, \dots, U_n, U^*) = \\ &= P(\Lambda, Y_1^*, \dots, Y_{n-r}^*, U_1, \dots, U_n, U_1\xi_1 + \dots + U_n\xi_n) \end{aligned} \quad (1)$$

holds.

Moreover, $\frac{\partial P}{\partial U}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, U_1, \dots, U_n, U^*)$ is not a zero divisor of this \mathbf{Q} -algebra. Let $1 \leq j \leq n$ and let P_j be the polynomial obtained specializing in P all variables U_1, \dots, U_n , except the variable U_j , into the values zero and specializing the variable U_j into the value one. One verifies immediately that the nonzero polynomial \tilde{G} is still the coefficient of the monomial $\tilde{U}^{\deg W}$ in P_j .

From (1) one deduces now that in the \mathbf{Q} -algebra

$$\mathbf{Q}[A_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n] \otimes_{\mathbf{Q}} \mathbf{Q}[W]$$

the algebraic identity $P_j(\Lambda, Y_1^*, \dots, Y_{n-r}^*, \xi_j) = 0$ holds. This implies for

$$G := \tilde{G} \cdot \sum_{1 \leq j_1 < \dots < j_{n-r} \leq n-r} \det\left((A_{i,j_k})_{1 \leq i, k \leq n-r, 1 \leq j \leq n}\right)^2$$

statements (i) and (ii) of Lemma 1 (for more details see e.g. [62]).

We are now going to show statement (iii) of Lemma 1. As in [43] or [46, II.21] one deduces from (1) that in

$$\mathbf{Q}[A_{i,j}, U_j; 1 \leq i \leq n-r, 1 \leq j \leq n] \otimes_{\mathbf{Q}} \mathbf{Q}[W]$$

for any $1 \leq j \leq n$ the algebraic identity

$$\begin{aligned} \frac{\partial P}{\partial U}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, U_1, \dots, U_n, U^*)\xi_j + \\ + \frac{\partial P}{\partial U_j}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, U_1, \dots, U_n, U^*) = 0 \end{aligned} \quad (2)$$

holds.

We may now choose values $u_1, \dots, u_n \in \mathbf{Q}$ such that

$$\frac{\partial P}{\partial U}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, u_1, \dots, u_n, u_1\xi_1 + \dots + u_n\xi_n)$$

is still a nonzero divisor of the \mathbf{Q} -algebra

$$\mathbf{Q}[A_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n] \otimes_{\mathbf{Q}} \mathbf{Q}[W].$$

Let $\hat{P} := P(\Lambda, \tilde{Y}_1, \dots, \tilde{Y}_{n-r}, u_1, \dots, u_n, \tilde{U})$ and for $1 \leq j \leq n$ let $Q_j := \frac{\partial \hat{P}}{\partial \tilde{U}_j}(\Lambda, \tilde{Y}_1, \dots, \tilde{Y}_{n-r}, u_1, \dots, u_n, \tilde{U})$. Moreover let $\hat{U} := u_1 \xi_1 + \dots + u_n \xi_n$. Then we deduce from (2) that for any $1 \leq j \leq n$ in the \mathbf{Q} –algebra

$$\mathbf{Q}[A_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n] \otimes_{\mathbf{Q}} \mathbf{Q}[W]$$

the identity

$$\frac{\partial \hat{P}}{\partial \tilde{U}}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, \hat{U}) \xi_j + Q_j(\Lambda, Y_1^*, \dots, Y_{n-r}^*, \hat{U}) = 0 \quad (3)$$

holds.

Moreover, $\frac{\partial \hat{P}}{\partial \tilde{U}}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, \hat{U})$ is not a zero divisor of this algebra. Observe also that the nonzero polynomial \tilde{G} is the coefficient of the monomial $\tilde{U}^{\deg W}$ in \hat{P} . From (1) we deduce

$$\hat{P}(\Lambda, Y_1^*, \dots, Y_{n-r}^*, \hat{U}) = 0. \quad (4)$$

Let \hat{H} be the polynomial of

$$\mathbf{Q}[A_{i,j}, \tilde{Y}_i, Z_1, \dots, Z_m, \tilde{U}_j; 1 \leq i \leq n-r, 1 \leq j \leq n]$$

obtained by replacing in H for any $1 \leq j \leq n$ the variable X_j by $\frac{Q_j}{\frac{\partial \hat{P}}{\partial \tilde{U}}}$ and by clearing denominators. Observe that $\deg_{\tilde{U}} \hat{H} \leq D \deg W$ and that

$$\deg_{A_{i,j}, \tilde{Y}_1, \dots, \tilde{Y}_{n-r}, Z_1, \dots, Z_m} \hat{H} \leq (n-r+1)D \deg W$$

holds.

Let $R := \text{Res}_{\tilde{U}}(\hat{P}, \hat{H})$ be the resultant of the polynomials \hat{P} and \hat{H} with respect to the variable \tilde{U} . Observe that R is an element of $\mathbf{Q}[A_{i,j}, \tilde{Y}_i, Z_1, \dots, Z_m; 1 \leq i \leq n-r, 1 \leq j \leq n]$ of degree at most $(n-r+1)D^2(\deg W)^3$. From the identities (3), (4) and the properties of the resultant we deduce that $R(\Lambda, Y_1^*, \dots, Y_{n-r}^*, Z_1, \dots, Z_m)$ vanishes on the variety \hat{W} . The assumption $\dim \hat{W} \leq (n-r)(n+1) + m - 1$ implies $R(\Lambda, Y_1^*, \dots, Y_{n-r}^*, Z_1, \dots, Z_m) \neq 0$. Therefore R is a nonzero polynomial which vanishes on the set $\pi(\hat{W})$. \square

Now we are ready to prove the main theorem of this section. This result asserts that the coefficients of the linear forms Y_1, \dots, Y_n and the coordinates of the lifting points $P^{(r)}$ we are looking for can be randomly chosen in a suitable finite subset of \mathbb{Z} with high probability of success.

Theorem 3 *Let κ be a fixed natural number. There exist linear forms $Y_1 := \sum_{j=1}^n \lambda_{1,j} X_j, \dots, Y_n := \sum_{j=1}^n \lambda_{n,j} X_j$ of $\mathbb{Z}[X_1, \dots, X_n]$ and a point $P = (p_1, \dots, p_n) \in \mathbb{Z}^n$ of (absolute) height at most $8\kappa n^8 d^4 \delta^9$ such that for $1 \leq r \leq n-1$ the following conditions are satisfied:*

- i) the linear forms Y_1, \dots, Y_{n-r} are in Noether position with respect to the variety V_r ,*

- ii) the point $P^{(r)} := (p_1, \dots, p_{n-r})$ is a lifting point of V_r , i.e. the morphism $\pi_r : V_r \rightarrow \mathbf{C}^{n-r}$ induced by the linear forms Y_1, \dots, Y_{n-r} is unramified in $P^{(r)}$,
- iii) $r = n - 1$ or the π_r -fiber of any point $Q \in \pi_r(\pi_{r+1}^{-1}(P^{(r+1)}))$ is unramified, i.e. for any point $x \in \pi_r^{-1}(Q)$ the condition

$$\det \left(\frac{J(F_1, \dots, F_r)}{\partial(X_{n-r+1}, \dots, X_n)} \right) (x) \neq 0$$

is satisfied.

Furthermore, we can choose the coefficients of the linear forms Y_1, \dots, Y_n and the coordinates of the point P randomly and uniformly in the set $S := \{1, 2, \dots, 8\kappa n^8 d^4 \delta^9\}$ with a probability of success of at least

$$\left(1 - \frac{1}{2\kappa}\right)^2 > \frac{1}{4}.$$

Proof Let $\Lambda := (\Lambda_{i,j})_{1 \leq i, j \leq n}$ be a matrix of indeterminates and let

$$\begin{pmatrix} \tilde{Y}_1 \\ \vdots \\ \tilde{Y}_n \end{pmatrix} := \Lambda \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

Let us fix for the moment an arbitrary index $1 \leq r \leq n - 1$.

Let $\Lambda_r := (\Lambda_{i,j})_{1 \leq i \leq n-r, 1 \leq j \leq n}$ and let

$$H_r := \det \begin{pmatrix} \Lambda_{1,1} & \dots & \Lambda_{1,n} \\ \vdots & & \vdots \\ \Lambda_{n-r,1} & \dots & \Lambda_{n-r,n} \\ \frac{\partial F_1}{\partial X_1} & \dots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1} & \dots & \frac{\partial F_r}{\partial X_n} \end{pmatrix}.$$

Thus we have $H_r \in \mathbf{C}[\Lambda_{i,j}, X_j; 1 \leq i \leq n-r, 1 \leq j \leq n]$ and $\deg H_r \leq n - r + rd \leq nd$. Let $x \in \mathbf{C}^n$ an arbitrary point. Observe that the Jacobian matrix

$$\begin{pmatrix} \frac{\partial F_1}{\partial X_1}(x) & \dots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1}(x) & \dots & \frac{\partial F_r}{\partial X_n}(x) \end{pmatrix}$$

has maximal rank r if and only if $H_r(\Lambda_r, x) \neq 0$ holds in $\mathbf{C}[\Lambda_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n]$ (or equivalently if there exists a matrix $\lambda \in \mathbf{Q}^{(n-r) \times n}$ with $H_r(\lambda, x) \neq 0$).

Let \mathcal{C} be an arbitrary irreducible component of the variety V_r . Then $\dim(\mathcal{C}) = n - r$ and $\mathbf{C}^{(n-r) \times n} \times \mathcal{C}$ is an irreducible component of dimension $(n-r)(n+1)$ of the variety $\mathbf{C}^{(n-r) \times n} \times V_r$ and all irreducible components of $\mathbf{C}^{(n-r) \times n} \times V_r$ have this cylindric form.

Since by hypothesis the ideal (F_1, \dots, F_r) is radical, there exists a point $x \in C$ such that the matrix

$$\begin{pmatrix} \frac{\partial F_1}{\partial X_1}(x) & \cdots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1}(x) & \cdots & \frac{\partial F_r}{\partial X_n}(x) \end{pmatrix}$$

has maximal rank r in x . Therefore we have $H_r(A_r, x) \neq 0$. Thus there exists a matrix $\lambda_r \in \mathbf{Q}^{(n-r) \times n}$ with $H_r(\lambda_r, x) \neq 0$. On the other hand, the null matrix $0_r \in \mathbf{Q}^{(n-r) \times n}$ satisfies the condition $H_r(0_r, x) = 0$. This implies that $(\mathbf{C}^{(n-r) \times n} \times \mathcal{C}) \cap \{H_r = 0\}$ is an equidimensional variety of dimension $(n-r)(n+1) - 1$ and that the same for $(\mathbf{C}^{(n-r) \times n} \times V_r) \cap \{H_r = 0\}$ holds.

Let $\varphi_r : \mathbf{C}^{(n-r) \times n} \times \mathbf{C}^n \rightarrow \mathbf{C}^{(n-r) \times n} \times \mathbf{C}^{n-r}$ be the morphism of affine spaces induced by the entries of the matrix A_r and the polynomials $\tilde{Y}_1, \dots, \tilde{Y}_{n-r}$. We are now able to apply Lemma 1 to V_r and to φ_r and H_r . Observing $\deg V_r \leq \delta$ we deduce from Lemma 1 (i) and (ii) that there exists a nonzero polynomial

$$G_r \in \mathbf{Q}[A_{i,j}; 1 \leq i \leq n-r, 1 \leq j \leq n]$$

with

$$\deg G_r \leq 2(n-r) + \deg V_r \leq 2n + \delta$$

such that for any $\lambda_r \in \mathbf{Q}^{(n-r) \times n}$ with $G_r(\lambda_r) \neq 0$ all $(n-r)$ -minors of λ_r are

regular and such that for $\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} := \lambda_r \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ the linear forms Y_1, \dots, Y_{n-r}

induce a Noether normalization of the variety V_r . Taking into account $\deg H_r \leq nd$ we deduce from Lemma 1 (iii) that there exists a nonzero polynomial

$$R_r \in \mathbf{Q}[A_{i,j}, \tilde{Y}_i; 1 \leq i \leq n-r, 1 \leq j \leq n]$$

with

$$\deg R_r \leq (n-r+1)(nd)^2(\deg V_r)^3 \leq n^3 d^2 \delta^3$$

such that R_r vanishes on the φ_r -image of the set

$$(\mathbf{C}^{(n-r) \times n} \times V_r) \cap \{H_r = 0, G_r \neq 0\}.$$

Considering R_r as a polynomial in the variables $\tilde{Y}_1, \dots, \tilde{Y}_{n-r}$ we may choose a nonzero coefficient of a suitable monomial of $\tilde{Y}_1, \dots, \tilde{Y}_{n-r}$ occurring in R_r . Multiplying G_r by this coefficient, we may assume without loss of generality that for any matrix $\lambda_r \in \mathbf{C}^{(n-r) \times n}$ with $G_r(\lambda_r) \neq 0$ the polynomial $R_r(\lambda_r, \tilde{Y}_1, \dots, \tilde{Y}_{n-r})$ is not identically zero and that $\deg G_r \leq 2n^3 d^2 \delta^3$ holds.

Let now D be an arbitrary irreducible component of the variety V_{r+1} . As before one may choose a point $x \in D$ such that the matrix

$$\begin{pmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_{r+1}}{\partial X_1} & \cdots & \frac{\partial F_{r+1}}{\partial X_n} \end{pmatrix}$$

has maximal rank $r + 1$ in x . Therefore also the matrix

$$\begin{pmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1} & \cdots & \frac{\partial F_r}{\partial X_n} \end{pmatrix}$$

has maximal rank, namely r , in x . Therefore there exists a matrix $\lambda_r \in \mathbf{Q}^{(n-r) \times n}$ such that $H_r(\lambda_r, x) \neq 0$. This implies that the coordinate function of the \mathbf{Q} -algebra $\mathbf{Q}[\mathbf{C}^{(n-r) \times n} \times D]$, induced by the polynomial H_r , does not vanish identically. Since D was an arbitrary irreducible component of V_{r+1} we conclude that the coordinate function of

$$\mathbf{Q}[\mathbf{C}^{(n-r) \times n} \times V_{r+1}] \cong \mathbf{Q}[A_{i,j}, X_j; 1 \leq i \leq n-r, 1 \leq j \leq n]/(F_1, \dots, F_{r+1}),$$

induced by the polynomial H_r , is not a zero divisor.

Consider now the \mathbf{Q} -algebra extension

$$\begin{aligned} A &:= \mathbf{Q}[A_{i,j}, \tilde{Y}_i; 1 \leq i \leq n-r, 1 \leq j \leq n] \subset \\ &\subset B := \mathbf{Q}[A_{i,j}, X_j; 1 \leq i \leq n-r, 1 \leq j \leq n]/(F_1, \dots, F_r) \end{aligned}$$

and denote by $\overline{F_{r+1}}$ and $\overline{H_r}$ the residue class of F_{r+1} and H_r in B . Observe that B is a equidimensional and reduced \mathbf{Q} -algebra of Krull dimension $(n-r)(n+1)$, that $\overline{F_{r+1}}$ is not a zero divisor of B , that $\overline{H_r}$ does not belong to any (isolated) prime component of the principal ideal $B\overline{F_{r+1}}$ and that A is a polynomial ring over \mathbf{Q} in $(n-r)(n+1)$ variables (namely in the entries of the matrix A_r and in $\tilde{Y}_1, \dots, \tilde{Y}_r$). The nonzero polynomials G_r and R_r belong to A and the localization A_{G_r} is integrally closed. From the geometric properties of the polynomial G_r we deduce that the map φ_r induces a finite, surjective morphism of varieties which maps $(\mathbf{C}^{(n-r) \times n} \cap \{G_r \neq 0\}) \times V_r$ onto $(\mathbf{C}^{(n-r) \times n} \cap \{G_r \neq 0\}) \times \mathbf{C}^{n-r}$.

Thus the \mathbf{Q} -algebra extension $A_{G_r} \rightarrow B_{G_r}$ is integral. Since the polynomial R_r vanishes on the φ_r -image of the locally closed variety

$$(\mathbf{C}^{(n-r) \times n} \times V_r) \cap \{H_r = 0, G_r \neq 0\}$$

we may suppose without loss of generality (replacing the polynomial R_r by a suitable factor) that the radical of the principal ideal generated by R_r in A_{G_r} coincides with the radical ideal of $A_{G_r} \cap (B_{G_r} \overline{H_r})$ in A_{G_r} .

From the cylindric structure of the irreducible components of $\mathbf{C}^{(n-r) \times n} \times V_{r+1}$ one deduces immediately that no (isolated) prime component of the ideal $B\overline{F_{r+1}}$ contains the polynomial G_r .

If there exists an (isolated) prime component of $B\overline{F_{r+1}}$ which contains the polynomial R_r we have the same situation for $B_{G_r} \overline{F_{r+1}}$. Considering now the integral ring extension $A_{G_r} \rightarrow B_{G_r}$ and taking into account that A_{G_r} is integrally closed, one concludes by standard arguments of commutative algebra (as e.g. in [13]) that there exists an isolated prime component of $B_{G_r} \overline{F_{r+1}}$ which contains $\overline{H_r}$ and therefore we have the same situation for $B\overline{F_{r+1}}$. As we have seen before, this is impossible. Thus we have shown that no (isolated) prime component of

$\overline{BF_{r+1}}$ contains the polynomial R_r . By the way, let us observe that we did not make use of the Cohen–Macaulayness of the \mathbf{Q} –algebra B .

Translated into geometry our conclusion means that

$$\dim \left((\mathbf{C}^{(n-r) \times n} \times V_{r+1}) \cap \{R_r = 0\} \right) \leq (n-r)(n+1) - 2$$

holds.

Consider now the morphism of affine spaces

$$\psi_{r+1} : \mathbf{C}^{(n-r) \times n} \times \mathbf{C}^n \rightarrow \mathbf{C}^{(n-r) \times n} \times \mathbf{C}^{n-r-1}$$

induced by the entries of the matrix A_r and the polynomials $\tilde{Y}_1, \dots, \tilde{Y}_{n-r-1}$. Applying now Lemma 1 (iii) to V_{r+1} , ψ_r and R_r , we conclude that there exists a nonzero polynomial

$$A_r \in \mathbf{Q} [A_{i,j}, \tilde{Y}_1, \dots, \tilde{Y}_{n-r-1}; 1 \leq i \leq n-r, 1 \leq j \leq n]$$

with $\deg A_r \leq (n-r)(\deg R_r)^2(\deg V_{r+1})^3 \leq n^7 d^4 \delta^9$ such that A_r vanishes on the ψ_r –image of the locally closed variety

$$\mathbf{C}^{(n-r) \times n} \times V_{r+1} \cap \{R_r = 0, G_{r+1} \neq 0\}.$$

Considering A_r as a polynomial in the variables $\tilde{Y}_1, \dots, \tilde{Y}_{n-r-1}$, we may choose a nonzero coefficient of a suitable monomial of $\tilde{Y}_1, \dots, \tilde{Y}_{n-r-1}$ occurring in A_r . Multiplying G_r by this coefficient we may assume without loss of generality that for any matrix $\lambda_r \in \mathbf{C}^{(n-r) \times n}$ with $G_r(\lambda_r) \neq 0$ the polynomial $A_r(\lambda_r, \tilde{Y}_1, \dots, \tilde{Y}_{n-r-1})$ is not identically zero and that $\deg G_r \leq 3n^7 d^4 \delta^9$ holds.

Let $G := \det(A) \cdot \prod_{r=1}^{n-1} G_r$ and $R := \prod_{r=1}^{n-1} A_r R_r$. Then G is a nonzero polynomial of $\mathbf{Q} [A_{i,j}; 1 \leq i, j \leq n]$ with $\deg G \leq 4n^8 d^4 \delta^9$ and R is a nonzero polynomial of $\mathbf{Q} [A_{i,j}, \tilde{Y}_j; 1 \leq i, j \leq n]$ with $\deg R \leq 2n^8 d^4 \delta^9$. Recall that the statement of Theorem 3 depends on a parameter $\kappa \in \mathbb{N}$. We suppose now that this parameter is fixed.

Let $S := \{1, \dots, 6\kappa n^8 d^4 \delta^9\}$. Observe that the cardinality $\#S$ of the set S is strictly larger than $\deg G$ and $\deg R$. Therefore, we may find, by a random choice, a matrix $\lambda \in S^{n \times n}$ and a point $P \in S^n$ such that the conditions $G(\lambda) \neq 0$ and $R(\lambda, P) \neq 0$ are satisfied. By the Zippel–Schwartz test (see [71], [57] or [72]) the probability of success of such a random choice is at least

$$\left(1 - \frac{\deg(G)}{\#(S)}\right) \left(1 - \frac{\deg(R)}{\#(S)}\right) \geq \left(1 - \frac{4n^8 d^4 \delta^9}{\#(S)}\right)^2 = \left(1 - \frac{1}{2\kappa}\right)^2 \geq \frac{1}{4}.$$

Suppose that there is given a matrix $\lambda = (\lambda_{i,j})_{1 \leq i, j \leq n} \in S^{n \times n}$ and a point $P = (p_1, \dots, p_n) \in S^n$ such that $G(\lambda) \neq 0$ and $R(\lambda, P) \neq 0$ holds. From $G(\lambda) \neq 0$ we deduce that $\det(\lambda) \neq 0$ and this implies that for

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} := \lambda \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

the condition $\mathbf{Q}[Y_1, \dots, Y_n] = \mathbf{Q}[X_1, \dots, X_n]$ is satisfied.

Consider an arbitrary index $1 \leq r \leq n-1$. Let $\lambda_r := (\lambda_{i,j})_{1 \leq i \leq n-r, 1 \leq j \leq n}$, $P^{(r)} := (p_1, \dots, p_{n-r})$ and $P^{(r+1)} := (p_1, \dots, p_{n-r-1})$. Observe that we have

with this notation $\begin{pmatrix} Y_1 \\ \vdots \\ Y_{n-r} \end{pmatrix} := \lambda_r \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$. Denote by $\pi_r : V_r \rightarrow \mathbf{C}^{n-r}$ and

$\pi_{r+1} : V_{r+1} \rightarrow \mathbf{C}^{n-r-1}$ the morphisms of affine varieties induced by the linear forms Y_1, \dots, Y_{n-r} and Y_1, \dots, Y_{n-r-1} . From $G(\lambda) \neq 0$ we deduce $G_r(\lambda_r) \neq 0$. Therefore all $(n-r)$ -minors of λ_r are regular. This implies $\mathbf{Q}[Y_1, \dots, Y_{n-r}, X_{i_1}, \dots, X_{i_r}] = \mathbf{Q}[X_1, \dots, X_n]$ for any choice of r indices $1 \leq i_1 < \dots < i_r \leq n$. Moreover, from $G_r(\lambda_r) \neq 0$ we infer that the linear forms Y_1, \dots, Y_{n-r} induce a Noether normalization of the variety V_r . Thus Y_1, \dots, Y_{n-r} satisfy condition (i) of Theorem 3. We conclude in particular that $\pi_r : V_r \rightarrow \mathbf{C}^{n-r}$ and $\pi_{r+1} : V_{r+1} \rightarrow \mathbf{C}^{n-r-1}$ are finite surjective morphisms of affine varieties. Since by construction the polynomial R_r vanishes on the φ_r -image of the locally closed variety

$$(\mathbf{C}^{(n-r) \times n} \times V_r) \cap \{H_r = 0, G_r \neq 0\},$$

we conclude that for any point $x \in V_r$ with $H_r(\lambda_r, x) = 0$ the condition

$$R_r(\lambda_r, \pi_r(x)) = R_r(\lambda_r, Y_1(x), \dots, Y_{n-r}(x)) = 0$$

is satisfied. On the other hand we have by assumption $R(\lambda, P) \neq 0$. This implies $R_r(\lambda_r, P^{(r)}) \neq 0$. From $R_r(\lambda_r, P^{(r)}) \neq 0$ we deduce now that the polynomial $H_r(\lambda_r, X_1, \dots, X_n)$ vanishes nowhere on $\pi_r^{-1}(P^{(r)})$. Let x be an arbitrary point of $\pi_r^{-1}(P^{(r)})$. Then we have

$$0 \neq H_i(\lambda_r, x) = \det \begin{pmatrix} \lambda_{1,1} & \dots & \lambda_{1,n} \\ \vdots & & \vdots \\ \lambda_{n-r,1} & \dots & \lambda_{n-r,n} \\ \frac{\partial F_1}{\partial X_1}(x) & \dots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1}(x) & \dots & \frac{\partial F_r}{\partial X_n}(x) \end{pmatrix}.$$

Since all $(n-r)$ -minors of λ_r are regular we conclude that there exist r indices $1 \leq i_1 < \dots < i_r \leq n$ such that the linear forms $Y_1, \dots, Y_{n-r}, X_{i_1}, \dots, X_{i_r}$ are \mathbf{Q} -linearly independent and such that

$$\det \begin{pmatrix} \frac{\partial F_1}{\partial X_{i_1}}(x) & \dots & \frac{\partial F_1}{\partial X_{i_r}}(x) \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_{i_1}}(x) & \dots & \frac{\partial F_r}{\partial X_{i_r}}(x) \end{pmatrix} \neq 0$$

holds. Since $x \in \pi_r^{-1}(P^{(r)})$ was arbitrary, this means that the finite morphism $\pi_r : V_r \rightarrow \mathbf{C}^{n-r}$ is unramified in the point $P^{(r)}$. Thus $P^{(r)}$ is a lifting point of V_r . Therefore, Y_1, \dots, Y_{n-r} and $P^{(r)}$ satisfy condition (ii) of Theorem 3.

Observe now that $G(\lambda) \neq 0$ and $R(\lambda, P) \neq 0$ implies $G_{r+1}(\lambda_r) = G_r(\lambda_r) \neq 0$ and $A_r(\lambda_r, P^{(r+1)}) \neq 0$.

Let us consider an arbitrary point $Q \in \pi_r(\pi_{r+1}^{-1}(P^{(r+1)}))$. Then there exists a point $z \in \pi_{r+1}^{-1}(P^{(r+1)})$ such that

$$Q = (Y_1(z), \dots, Y_{n-r}(z)) = (p_1, \dots, p_{n-r-1}, Y_{n-r}(z))$$

holds. Suppose now

$$0 = R_r(\lambda_r, Q) = R_r(\lambda_r, Y_1(z), \dots, Y_{n-r}(z)).$$

Since by construction the polynomial A_r vanishes on the ψ_{r+1} -image of the locally closed variety

$$(\mathbb{C}^{(n-r) \times n} \times V_{r+1}) \cap \{R_r = 0, G_{r+1} \neq 0\}$$

and since we have $G_{r+1}(\lambda_r) \neq 0$, we conclude

$$\begin{aligned} 0 &= A_r(\lambda_r, Y_1(z), \dots, Y_{n-r-1}(z)) \\ &= A_r(\lambda_r, p_1, \dots, p_{n-r-1}) \\ &= A_r(\lambda_r, P^{(r+1)}). \end{aligned}$$

However, as we have seen before, our choice of λ and P implies $A_r(\lambda_r, P^{(r+1)}) \neq 0$. Therefore we have $R_r(\lambda_r, Q) \neq 0$.

Following our previous reasoning, this means that the morphism π_r is unramified in the point Q . Therefore Y_1, \dots, Y_{n-r} and $P^{(r+1)}$ satisfy condition (iii) of Theorem 3. \square

From now on we shall suppose that κ is fixed and that we have already chosen linear forms $Y_1, \dots, Y_n \in \mathbb{Z}[X_1, \dots, X_n]$ and a point $P = (p_1, \dots, p_n) \in \mathbb{Z}^n$ satisfying the conditions (i), (ii), and (iii) of Theorem 3 and having coordinates in $S = \{1, \dots, 8\kappa n^8 d^4 \delta^9\}$.

4 Algorithmic tools

In this section we are going to exhibit efficient algorithms for some specific geometric tasks. These tasks are crucial for the design of our main algorithm which computes a geometric solution of the algebraic variety $V_n := V(F_1, \dots, F_n)$. Fix $1 \leq r \leq n - 1$. We are going to consider the following tasks:

- lifting of a projection: given a geometric solution of the lifting fiber $V_{P^{(r)}}$ of the morphism $\pi_r : V_r \rightarrow \mathbb{C}^{n-r}$ and a polynomial $F \in \mathbb{Q}[X_1, \dots, X_n]$, compute the minimal polynomial of F over $\mathbb{Q}[V_r]$,

- the following effective variant of the Shape Lemma: let K be a field of characteristic zero with algebraic closure \bar{K} . Let be given three nonconstant and square-free polynomials $f, g, h \in K[T]$ by their coefficients and let be given a nonzero element $\alpha \in K$. Suppose that the linear form $\alpha X + Y$ separates points of the zero-dimensional variety $\{(x, y) \in \bar{K}^2; f(x) = 0, g(x) = 0\}$ and that the variety $W := \{(x, y) \in \bar{K}^2; f(x) = 0, g(x) = 0, h(\alpha x + y) = 0\}$ is nonempty. The task consists in the computation of a geometric solution of the zero-dimensional algebraic variety W .
- lifting of a zero-dimensional fiber: given a geometric solution of the lifting fiber $V_{P^{(r)}}$ of the morphism $\pi_r : V_r \rightarrow \mathbb{C}^{n-r}$, compute a geometric solution of V_r ,
- computation of a projection: given a geometric solution of the lifting fiber $V_{P^{(r)}}$ of the morphism $\pi_r : V_r \rightarrow \mathbb{C}^{n-r}$, compute the minimal equation satisfied by the linear form Y_{n-r} over the lifting fiber $V_{P^{(r+1)}}$ of the morphism $\pi_{r+1} : V_{r+1} \rightarrow \mathbb{C}^{n-r-1}$.

4.1 Newton–Hensel lifting of a projection

Fix again $1 \leq r \leq n-1$. In this subsection we shall develop an efficient algorithm for the following task:

Given a polynomial $F \in \mathbb{Q}[Y_1, \dots, Y_n]$, compute a polynomial $q_F \in \mathbb{Q}[Y_1, \dots, Y_{n-r}][T]$ such that the condition $q_F(Y_1, \dots, Y_{n-r}, F) \in (F_1, \dots, F_r)$ is satisfied.

This task is a fundamental problem for geometric elimination procedures and was considered by several authors (see for example [24], [42], [26], [25], [22], [52]). Our approach is inspired by [22], where the authors describe an algorithm which solves this task starting from a geometric solution of the lifting fiber $V_{P^{(r)}}$ as input.

Let notations and assumptions be as before. Assume that there is given a geometric solution of the variety V_r and assume that this geometric solution is compatible with the given lifting point $P^{(r)} \in \mathbb{Z}^{n-r}$. In view of the notation introduced in Section 1 let this geometric solution be given by the following items:

- a linear form $U \in \mathbb{Q}[Y_{n-r+1}, \dots, Y_n]$ inducing a primitive element u of the integral ring extension $\mathbb{Q}[Y_{n-r+1}, \dots, Y_n] \hookrightarrow \mathbb{Q}[V_r]$ with minimal polynomial $q(T) \in \mathbb{Q}[Y_1, \dots, Y_{n-r}][T]$
- primitive polynomials

$$\rho_{n-r+1}Y_{n-r+1} - v_{n-r+1}(T) \quad \dots, \quad \rho_n Y_n - v_n(T)$$

with $v_{n-r+1}(T), \dots, v_n(T)$ belonging to $\mathbb{Q}[Y_1, \dots, Y_{n-r}][T]$ and $\rho_{n-r+1}, \dots, \rho_n$ being nonzero elements of $\mathbb{Q}[Y_1, \dots, Y_{n-r}]$.

These items satisfy by assumption the following conditions:

- i) $\deg_T q = \text{rank}_{\mathbf{Q}[Y_1, \dots, Y_{n-r}]} \mathbf{Q}[V_r]$
- ii) $\rho_{n-r+1} Y_{n-r+1} - v_{n-r+1}(T), \dots, \rho_n Y_n - v_n(T)$ form a generic “parametrization” of the variety V_r by the zeroes of $q(T)$ (see Section 1 for details)
- iii) $\rho_{n-r+1}(P^{(r)}) \neq 0, \dots, \rho_n(P^{(r)}) \neq 0$ and $\text{discr}_T q(P^{(r)}) \neq 0$

In order to simplify notations, we assume without loss of generality $\delta_r = \deg_T q = \text{rank}_{\mathbf{Q}[Y_1, \dots, Y_{n-r}]} \mathbf{Q}[V_r]$.

The given geometric solution of V_r induces a geometric solution of the lifting fiber $V_{P^{(r)}}$. This geometric solution is given by a primitive element $u^{(r)} \in \mathbf{Q}[V_r]$, namely the coordinate function defined by the linear form U , and by the polynomials

$$\begin{aligned} q^{(P^{(r)})}(T) &:= q(P^{(r)}, T) \\ Y_{n-r+1} - v_{n-r+1}^{(P^{(r)})}(T) &:= Y_{n-r+1} - \frac{1}{\rho(P^{(r)})} v_{n-r+1}(P^{(r)}, T) \\ &\vdots \\ Y_n - v_n^{(P^{(r)})}(T) &:= Y_n - \frac{1}{\rho(P^{(r)})} v_n(P^{(r)}, T) \end{aligned}$$

with $v_{n-r+1}^{(P^{(r)})}(T), \dots, v_n^{(P^{(r)})}(T) \in \mathbf{Q}[T]$. Here $q^{(P^{(r)})}(T)$ is the minimal polynomial of the primitive element $u^{(r)}$ in $\mathbf{Q}[V_{P^{(r)}}]$ and the polynomials $Y_{n-r+1} - v_{n-r+1}^{(P^{(r)})}(T), \dots, Y_n - v_n^{(P^{(r)})}(T)$ parametrize the points of $V_{P^{(r)}}$ by the zeroes of the polynomial $q^{(P^{(r)})}(T)$. Denote by $M \in \mathbf{Q}^{\delta_r \times \delta_r}$ the companion matrix of the polynomial $q^{(P^{(r)})}(T)$. Considering F_1, \dots, F_r as polynomials in the variables Y_{n-r+1}, \dots, Y_n with coefficients in the polynomial ring $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ let us write

$$h_0 := \det \begin{pmatrix} \frac{\partial F_1}{\partial Y_{n-r+1}} & \cdots & \frac{\partial F_1}{\partial Y_n} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial Y_{n-r+1}} & \cdots & \frac{\partial F_r}{\partial Y_n} \end{pmatrix}.$$

Observing that the vanishing ideal $I(V_{P^{(r)}})$ of the lifting fiber $V_{P^{(r)}}$ is generated in $\mathbf{Q}[Y_{n-r+1}, \dots, Y_n]$ by the polynomials $F_1(P^{(r)}, Y_{n-r+1}, \dots, Y_n), \dots, F_r(P^{(r)}, Y_{n-r+1}, \dots, Y_n)$ we easily deduce from conditions (i)–(iii) above that the rational $\delta_r \times \delta_r$ matrix $h_0(P^{(r)}, v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M))$ is invertible.

The algorithm of [22] relies on a symbolic iteration of the following Newton–Hensel operator:

$$\begin{aligned} N(Y_{n-r+1}, \dots, Y_n)^t &:= \\ &= \begin{pmatrix} Y_{n-r+1} \\ \vdots \\ Y_n \end{pmatrix} - \begin{pmatrix} \frac{\partial F_1}{\partial Y_{n-r+1}} & \cdots & \frac{\partial F_1}{\partial Y_n} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial Y_{n-r+1}} & \cdots & \frac{\partial F_r}{\partial Y_n} \end{pmatrix}^{-1} \cdot \begin{pmatrix} F_1(Y_{n-r+1}, \dots, Y_n) \\ \vdots \\ F_r(Y_{n-r+1}, \dots, Y_n) \end{pmatrix}. \end{aligned}$$

Here $N(Y_{n-r+1}, \dots, Y_n)^t$ denotes the transposition of the row vector $N(Y_{n-r+1}, \dots, Y_n)$ to the corresponding column vector. The approach of [22] is

based on the observation that any *generic* 0-dimensional fiber $V_{P^{(r)}}$ provides all necessary information for the reconstruction of a geometric solution of the *positive* dimensional variety V_r .

Let D be the total degree of F and let $\sigma := \lceil \log(D\delta_r) \rceil + 1$. Let us denote by $(\frac{g_{n-r+1}}{h}, \dots, \frac{g_n}{h})$ the vector of rational functions

$$\frac{g_k}{h} \in \mathbf{Q}(Y_1, \dots, Y_{n-r})[Y_{n-r+1}, \dots, Y_n],$$

$n-r \leq k \leq n$, obtained by iterating the Newton–Hensel operator σ times. Since the rational $\delta_r \times \delta_r$ matrix $h_0(P^{(r)}, v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M))$ is invertible, we may assume without loss of generality that the same holds for $h(P^{(r)}, v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M))$. Thus we see that the matrix $h(v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M))$, that we obtain from the polynomial $h(Y_1, \dots, Y_n)$ by specializing the variables Y_{n-r+1}, \dots, Y_n into the rational $\delta_r \times \delta_r$ matrices $v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M)$, is an invertible element of the matrix ring

$$\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}^{\delta_r \times \delta_r}$$

and hence of the matrix rings $\mathbf{Q}(Y_1, \dots, Y_{n-r})_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}^{\delta_r \times \delta_r}$ and $\mathbf{Q}[[Y_1-p_1, \dots, Y_{n-r}-p_{n-r}]]^{\delta_r \times \delta_r}$ (here $\mathbf{Q}[[Y_1-p_1, \dots, Y_{n-r}-p_{n-r}]]$ denotes the formal power series ring over \mathbf{Q} in the variables $Y_1-p_1, \dots, Y_{n-r}-p_{n-r}$). With all these notations we have the following result:

Theorem 4 ([22], Lemma 29) *Suppose that $F(Y_1, \dots, Y_n)$ is a polynomial of $\mathbf{Q}[Y_1, \dots, Y_n]$ having degree at most D . Suppose that F is given by a straight-line program using space \mathcal{S} and time \mathcal{T} . The coordinate function of V_r defined by the polynomial F has a monic minimal polynomial $q_F(T) \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ with respect to the ring extension $\mathbf{Q}[Y_1, \dots, Y_{n-r}] \hookrightarrow \mathbf{Q}[V_r]$. For $1 \leq k \leq r$ let us introduce the following $\delta_r \times \delta_r$ matrix:*

$$\mathcal{N}_{n-r+k} := g_{n-r+k} \left(v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M) \right).$$

$$h \left(v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M) \right)^{-1}$$

(observe that \mathcal{N}_{n-r+k} is an element of $\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}^{\delta_r \times \delta_r}$). Finally, let $\mathcal{M}_F \in \mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}^{\delta_r \times \delta_r}$ be the $\delta_r \times \delta_r$ matrix defined by the formula $\mathcal{M}_F := F(Y_1, \dots, Y_{n-r}, \mathcal{N}_{n-r+1}, \dots, \mathcal{N}_n)$ and let $\tilde{q}_F(T) \in \mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}[T]$ be the minimal polynomial of \mathcal{M}_F . Suppose that $\deg_T q_F = \deg_T \tilde{q}_F$ holds. Then we have that in

$$\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}[T]$$

(and hence in $\mathbf{Q}[[Y_1-p_1, \dots, Y_{n-r}-p_{n-r}]](T)$) the polynomials q_F and \tilde{q}_F are congruent modulo the ideal $(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})^{D\delta_r+1}$. In symbols we have:

$$q_F \equiv \tilde{q}_F \text{ modulo } (Y_1-p_1, \dots, Y_{n-r}-p_{n-r})^{D\delta_r+1}.$$

By means of this theorem and of the estimation $\deg q_F \leq D\delta_r$ ([55]) it is possible to design a computation tree which produces a straight–line program representing every coefficient of the polynomial $q_F(T)$ with respect to the variable T . This computation tree (and the corresponding straight–line program for the coefficients of $q_F(T)$) uses space $O(SrD\delta_r^3)$ and time $O(Tr^4D^2\delta_r^6)$.

Sketch of the construction of the computation tree: First we compute the Jacobian matrix

$$\begin{pmatrix} \frac{\partial F_1}{\partial Y_{n-r+1}} & \cdots & \frac{\partial F_1}{\partial Y_n} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial Y_{n-r+1}} & \cdots & \frac{\partial F_r}{\partial Y_n} \end{pmatrix}$$

and its inverse using neither divisions nor branchings (by means, e.g., of the Samuelson algorithm [18]). Then, we compute the polynomials g_{n-r+1}, \dots, g_n, h , only using non–essential divisions, by means of a suitable homogenization procedure (see [22], Lemma 27). Afterwards, we evaluate the given parametrization polynomials $v_{n-r+1}^{(P^{(r)})}(T), \dots, v_n^{(P^{(r)})}(T)$ in the companion matrix M . Now we substitute in the given straight–line program for the polynomial $F(Y_1, \dots, Y_n)$ the input nodes Y_{n-r+1}, \dots, Y_n by the rational functions $\frac{g_{n-r+1}}{h}, \dots, \frac{g_n}{h}$ and compute numerator and denominator of the resulting rational function $F(Y_1, \dots, Y_{n-r}, \frac{g_{n-r+1}}{h}, \dots, \frac{g_n}{h})$ separately. To this numerator and denominator we apply the same procedure as before, replacing the input nodes Y_{n-r+1}, \dots, Y_n by the matrices $v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M)$. In this way we easily obtain a straight–line program representation of the entries of the matrix \mathcal{M}_F , dividing only by units in

$$\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}.$$

Then we represent each coefficient of the characteristic polynomial $\tilde{q}_F(T)$ of the matrix \mathcal{M}_F as the quotient of two polynomials, the denominator being a unit in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}$. These polynomials are given by a division–free straight–line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ and we obtain this straight–line program adding only division–free linear algebra routines ([18]) to the previously computed straight–line program representation of the entries of the matrix \mathcal{M}_F . Applying to this numerator–denominator representation of each coefficient of $\tilde{q}_F(T)$ the *Vermeidung von Divisionen* procedure [64], we obtain a division–free straight–line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ which computes the coefficients of a polynomial of $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ which is in $\mathbf{Q}[[Y_1 - p_1, \dots, Y_{n-r} - p_{n-r}]] [T]$ congruent to \tilde{q}_F modulo the ideal $(Y_1 - p_1, \dots, Y_{n-r} - p_{n-r})^{D\delta_r+1}$. From this polynomial it is now easy to read–off the coefficients of q_F with respect to the variable T .

Since the quantity δ_r may be large in many practical situations, the $O(\delta_r^3)$ space requirement for the evaluation of this computation tree seems to be prohibitive for an efficient implementation. Moreover we would also like to reduce the time requirement of $O(\delta_r^6)$ of this procedure, in order to increase the range of practical problems which can be treated by our algorithmic approach.

For this reason we are now going to develop several linear algebra procedures that profit from the fact that all the matrices we have to deal with are in some sense “structured” ones. This will allow us to reduce the time–space complexity of the subroutine we are considering here. We are now going to show that the geometric sub–problem under consideration can be solved in space *quadratic* and time *cubic* in δ_r .

4.1.1 Time–space economy in linear algebra We start this subsection with the formulation of a preliminary result concerning modular computation with straight–line programs.

Lemma 2 *Let R be the polynomial ring $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ and let K be its quotient field. Let be given polynomials $q(T)$, $f(T)$ and $g(T)$ of $R[T]$. Assume that $q(T)$ is separable and monic with respect to the variable T and let $\delta := \deg_T q(T)$. Assume furthermore that $q(T)$ and $g(T)$ are coprime in $K[T]$ and that there is given a division–free straight–line program β in $R[T]$ which computes the coefficients of the polynomial $q(T)$ with respect to the variable T and which evaluates the polynomials $f(T)$ and $g(T)$ with respect to all variables (including T) in space \mathcal{S} and time \mathcal{T} . Then there exists a division–free straight–line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}] = R$ computing a nonzero element α of R and the coefficients of a polynomial $h(T)$ of $R[T]$ with $\deg_T h \leq \delta - 1$ such that in $R[T]$ the condition $g(T)h(T) \equiv \alpha f(T)$ modulo $q(T)$ is satisfied. This straight–line program uses space $O(\mathcal{S}\delta)$ and time $O((\mathcal{T} + \delta)\delta \log \delta \log \log \delta) = O(\mathcal{T}\delta^2 \log \log \delta)$.*

Proof First we compute the coefficients of the remainders of the division of $f(T)$ and $g(T)$ by $q(T)$ and call them $\tilde{f}(T)$ and $\tilde{g}(T)$ respectively. For this purpose, we execute the straight–line program β performing polynomial arithmetic modulo $q(T)$ in each step. Each intermediate result of the computation is a polynomial of $R[T]$ of degree at most $\delta - 1$, which we represent by a vector of R^δ .

We are now going to see how β can be transformed into a division–free straight–line program $\tilde{\beta}$ in $\mathbf{Q}[Y_1, \dots, Y_{n-r}] = R$ which computes the coefficients of $\tilde{f}(T)$ and $\tilde{g}(T)$ with respect to the variable T . This transformation is performed step by step along the straight–line program β . Each addition node of β is transformed in the most obvious way into δ addition nodes of $\tilde{\beta}$.

We are now going to describe the transformation of a multiplication node of β . Let $u(T)$ and $v(T)$ be intermediate results of β and let us suppose that the coefficients of $u(T)$ modulo $q(T)$ and $v(T)$ modulo $q(T)$ are already computed by the straight–line program $\tilde{\beta}$. We compute then the coefficients of the polynomial $(u \cdot v)(T)$ by means of a FFT–based algorithm (see [5]) and divide afterwards $(u \cdot v)(T)$ by $q(T)$ using the Sieveking–Kung algorithm which is based on the inversion of formal power series (see [61], [8] or [5]). This single transformation step can be performed in space $O(\delta)$ and time $O(\delta \log \delta \log \log \delta)$.

This first part of the computation, which produces the coefficients of $\tilde{f}(T)$ and $\tilde{g}(T)$ with respect to the variable T , can therefore be performed in space $O(\mathcal{S}\delta)$ and time $O(\mathcal{T}\delta \log \delta \log \log \delta)$. Now suppose that the coefficients of $\tilde{f}(T)$ and of $\tilde{g}(T)$ are already computed. Observe that these coefficients can be stored in space $O(\delta)$.

Then, we apply the algorithms based on Hankel matrices of [58] and [59] in order to produce a nonzero element $\alpha \in R$ and a polynomial $\tilde{h}(T) \in R[T]$ which satisfy in $R[T]$ the condition $\tilde{h}(T)\tilde{g}(T) \equiv \alpha$ modulo $q(T)$. This can be done in additional space $O(\delta)$ and time $O(\delta^2 \log \delta \log \log \delta)$. Finally, multiplying $\tilde{f}(T)$ and $\tilde{h}(T)$ and dividing the result by $q(T)$ in the same way as before, we obtain the coefficients of a polynomial $h(T) \in R[T]$ which satisfies the requirements of the statement of Lemma 2. The complexity bounds of the lemma are obtained by adding up the complexities of the different steps of the algorithm just described. \square

Now we state the fundamental result of this subsection (compare [2] and [54]).

Lemma 3 *Let notations and assumptions be as in Lemma 2. Let M be the companion matrix of the polynomial $q(T)$. Thus $g(M)$ is a $\delta \times \delta$ matrix with entries from R , which is invertible in the matrix ring $K^{\delta \times \delta}$. Let N be the matrix $N := f(M)g(M)^{-1}$. Then there exists a straight–line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}] = R$ which computes in space $O(\mathcal{S}\delta)$ and time $O((\mathcal{T} + \delta)\delta \log \delta \log \log \delta) = O(\mathcal{T}\delta^2 \log \delta \log \log \delta)$ the element $\alpha \in R$ of the statement of Lemma 2 and the α^δ –multiples of the coefficients of the characteristic polynomial $\chi_N(Y)$ of N . In particular, these α^δ –multiples of the coefficients of $\chi_N(Y)$ are elements of R (here Y is a new variable).*

Proof From Lemma 2 we deduce that $h(M) = \alpha f(M)g^{-1}(M) = \alpha N$ holds and therefore the $\delta \times \delta$ matrix αN has its entries from R .

The algorithm underlying the statement of Lemma 3 runs as follows: we compute first the traces of the matrices $\alpha N, \dots, (\alpha N)^\delta$ and use then the Newton relations in order to produce the coefficients of the characteristic polynomial $\chi_{\alpha N}(Y)$ of the matrix αN . Finally we compute the coefficients of the polynomial $\chi_{\alpha N}(\alpha Y)$ which are in fact the α^δ –multiples of the coefficients of the polynomial $\chi_N(Y)$.

Let T be a new variable. In order to compute for $1 \leq k \leq \delta$ the trace $tr((\alpha N)^k)$ of the matrix $(\alpha N)^k$ time–space–efficiently (i.e. avoiding the explicit computation of the matrices $(\alpha N)^k$ which requires space $O(\delta^2)$), we consider the decomposition of the polynomial $q(T)$ into linear factors over an algebraic closure \bar{K} of the field K , namely the decomposition $q(T) = \prod_{1 \leq i \leq \delta} (T - \alpha_i)$ with $\alpha_i \in \bar{K}$.

We shall use the following representation for the derivative $q'(T) := \frac{\partial q(T)}{\partial T}$ of the polynomial $q(T)$:

$$q'(T) = \sum_{i=1}^{\delta} \prod_{j \neq i} (T - \alpha_j).$$

From the given decomposition of $q(T)$ in linear factors we infer that in $\bar{K}[T]$ for any $1 \leq i \leq \delta$ the congruence relation

$$T \prod_{j \neq i} (T - \alpha_j) \equiv \alpha_i \prod_{j \neq i} (T - \alpha_j) \quad \text{modulo } q(T)$$

holds. Summing up these congruence relations, we obtain

$$T \sum_{i=1}^{\delta} \prod_{j \neq i} (T - \alpha_j) \equiv \sum_{i=1}^{\delta} \alpha_i \prod_{j \neq i} (T - \alpha_j) \pmod{q(T)} .$$

This implies that for any polynomial $p(T) \in R[T]$ the congruence relation

$$\begin{aligned} p(T)q'(T) &= p(T) \sum_{i=1}^{\delta} \prod_{j \neq i} (T - \alpha_j) \\ &\equiv \sum_{i=1}^{\delta} p(\alpha_i) \prod_{j \neq i} (T - \alpha_j) \pmod{q(T)} \end{aligned} \quad (5)$$

holds in $R[T]$.

This means that $\text{tr}(p(M)) = \sum_{1 \leq i \leq \delta} p(\alpha_i)$ appears as the leading coefficient of the remainder of the division of the polynomial $(p \cdot q')(T)$ by the polynomial $q(T)$.

In particular, we deduce from the congruence relation (5) that for any $1 \leq k \leq \delta$ the value $\text{tr}((\alpha N)^k) = \text{tr}(h(M)^k)$ appears as the $(\delta - 1)$ -th coefficient of the remainder of the division of $(h^k q')(T)$ by $q(T)$ (here $h(T)$ is the polynomial of the statement of Lemma 2).

By assumption, the given straight-line program β produces the coefficients of the polynomial $q(T)$ and therefore, without loss of generality, also the coefficients of the derivative $q'(T)$. Now, applying Lemma 2, we compute in space $O(\mathcal{S}\delta)$ and time $O((\mathcal{T} + \delta)\delta \log \delta \log \log \delta)$ the element α and the coefficients of the polynomial $h(T)$ with respect to the variable T . At this moment we store only the element $\alpha \in R$ and the coefficients of $q(T)$, of $q'(T)$ modulo $q(T)$ and of $h(T)$. This can be done in space $O(\delta)$.

From these data we compute now in the same way as at the beginning of the proof the following items: first we compute the coefficients of the polynomial $(h \cdot q')(T)$ modulo $q(T)$ and store them for the next step, while we clear from our memory space the coefficients of $q'(T)$. Next we compute from the coefficients of $(h \cdot q')(T)$ modulo $q(T)$, $h(T)$ and $q(T)$ the coefficients of $(h^2 \cdot q')(T)$ modulo $q(T)$, while we clear from our memory space all coefficients of $(h \cdot q')(T)$, except the $(\delta - 1)$ -th one. We proceed in this way during δ successive steps, the computation of the coefficients of $(h \cdot q')(T)$ modulo $q(T)$ and of $(h^2 \cdot q')(T)$ modulo $q(T)$ being the first and second one. Let $1 < k \leq \delta$. In the k -th step we compute the coefficients of $(h^k \cdot q')(T)$ modulo $q(T)$ from the coefficients of $(h^{k-1} \cdot q')(T)$ modulo $q(T)$. Then we clear from our memory space all coefficients of $(h^{k-1} \cdot q')(T)$ modulo $q(T)$, except the $(\delta - 1)$ -th one. In case $1 < k < \delta$ we proceed to compute then in the same way the coefficients of $(h^{k+1} \cdot q')(T)$ modulo $q(T)$.

During this procedure only the element α and the coefficients of the polynomials $h(T)$, $q(T)$ are stored permanently, while for $1 \leq k \leq \delta$ only the $(\delta - 1)$ -th coefficient of the polynomial $(h^k q)(T)$ modulo $q(T)$ is computed (and stored). As we have seen before, these coefficients are the elements $\text{tr}(\alpha N), \dots, \text{tr}((\alpha N)^\delta)$. Obviously this procedure can be performed in additional space $O(\delta)$ and time $O(\delta^2 \log \delta \log \log \delta)$.

From $\text{tr}(\alpha N), \dots, \text{tr}((\alpha N)^\delta)$ we obtain the coefficients of $\chi_{\alpha N}(T)$ in additional constant space and time $O(\delta)$ by means of the Newton relations. The coefficients of $\chi_{\alpha N}(\alpha T)$ are now easily computed multiplying the coefficients of $\chi_{\alpha N}(T)$ by suitable powers of α . Again this can be done in constant space and in time $O(\delta)$. Summing up the complexities of all these steps, we see that our procedure yields a straight–line program for the desired output, which can be evaluated in space $O(\mathcal{S}\delta)$ and time $O((\mathcal{T} + \delta)\delta \log \delta \log \log \delta) = O(\mathcal{T}\delta^2 \log \delta \log \log \delta)$. \square

4.1.2 The Newton–Hensel iteration The just proved Lemma 3 is the key algorithmic result we are going to apply to the Newton–Hensel iteration procedure described at the beginning of this section. First of all, we establish a suitable version of the *Vermeidung von Divisionen* procedure of [64], with the following refined complexity bounds:

Lemma 4 *Let $\mathcal{F} := \{F_0, \dots, F_m\}$ be a finite set of polynomials of $\mathbf{Q}[Y_1, \dots, Y_n]$ of degree at most δ , computed by a straight–line program β in space \mathcal{S} and time \mathcal{T} . Assume $F_0 \neq 0$ and that F_0 divides F_i in $\mathbf{Q}[Y_1, \dots, Y_n]$ for any $1 \leq i \leq m$. Then there exists a straight–line program that computes the polynomials*

$$P_1 := \frac{F_1}{F_0}, \dots, P_m := \frac{F_m}{F_0}$$

in space $O(\mathcal{S}\delta)$ and time $O((\mathcal{T} + \log \delta)\delta \log \delta \log \log \delta) = O(\mathcal{T}\delta \log^2 \delta \log \log \delta)$.

Proof This proof is an adaptation of an idea of [42]. Let be given an integer point $\gamma := (\gamma_1, \dots, \gamma_n) \in \mathbb{Z}^n$ such that $\rho := F_0(\gamma) \neq 0$ holds (observe that, using the Zippel–Schwartz test, such a point can be found, e.g. in the hypercube $[1, 2\delta]^n \cap \mathbb{Z}^n$, at an average cost of space \mathcal{S} and time $2\mathcal{T}$).

For $1 \leq i \leq m$, let us write $G_i(Y_1, \dots, Y_n) := F_i(Y_1 + \gamma_1, \dots, Y_n + \gamma_n)$. One easily sees that the polynomial $P_i(Y_1 + \gamma_1, \dots, Y_n + \gamma_n) = \frac{F_i(Y_1 + \gamma_1, \dots, Y_n + \gamma_n)}{F_0(Y_1 + \gamma_1, \dots, Y_n + \gamma_n)}$ can be computed as the sum of the first $\delta + 1$ homogeneous components of the polynomial $\frac{G_i}{\rho} \sum_{k=0}^{\delta} \left(\frac{\rho - G_0}{\rho}\right)^k$. Note that this latter polynomial can be evaluated by means of a straight–line program in space $O(\mathcal{S})$ and time $O(\mathcal{T} + \log \delta)$.

For the decomposition of a polynomial given by a straight–line program into its homogeneous components we follow an idea of [47], which reduces the task to polynomial arithmetic in $\mathbf{Q}[Y_1, \dots, Y_n][T]$ modulo $T^{\delta+1}$. Applying FFT–based polynomial multiplication (see [5]), we obtain a straight–line program that performs the *Vermeidung von Divisionen* procedure using space $O(\mathcal{S}\delta)$ and time $O((\mathcal{T} + \log \delta)\delta \log \delta \log \log \delta)$, just as claimed in the statement of Lemma 4. \square

We are now going to show a technical lemma which we need for our analysis of the Newton–Hensel iteration.

Lemma 5 *Let R be the polynomial ring $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ and let K be its quotient field. Let β be a straight–line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}] = R$ that computes the*

coefficients of two univariate polynomials $p(T), q(T) \in R[T]$ with $q(T) \neq 0$ in space \mathcal{S} and time \mathcal{T} . Let $u(T), v(T)$ be two coprime polynomials of $K[T]$ and assume that $\frac{p}{q} = \frac{u}{v}$ and $\deg_T u = \delta$ and $\deg_T v < \delta$ holds and that $u(T)$ is monic in T . Then, there exists a straight-line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}] = R$ that computes a nonzero element $\gamma \in R$ and a γ -multiple of the coefficients of u in space $O(\mathcal{S} + \delta)$ and time $O(\mathcal{T} + \delta^2 \log \delta \log \log \delta)$.

Proof Using the Zippel–Schwartz test we may assume by the same argument as in the proof of Lemma 4 that there is given an element t of \mathbf{Q} with $q(t) \neq 0$. Let $u(T) = T^\delta + u_{\delta-1}T^{\delta-1} + \dots + u_0$ with $u_{\delta-1}, \dots, u_0 \in K$. Following [5, Remark 2.9.1] we consider the power series representation of the rational function $\frac{v((T-t)^{-1})}{(T-t)u((T-t)^{-1})}$ with respect to the variable $(T-t)$, namely

$$\frac{v((T-t)^{-1})}{(T-t)u((T-t)^{-1})} = \frac{q((T-t)^{-1})}{(T-t)p((T-t)^{-1})} = \sum_{i=0}^{+\infty} h_i(T-t)^i. \quad (6)$$

Then, by [5, Proposition 2.9.1], we have the following identity:

$$\begin{pmatrix} h_0 & h_1 & \dots & h_{\delta-1} \\ h_1 & h_2 & \dots & h_\delta \\ \vdots & \vdots & & \vdots \\ h_{\delta-1} & h_\delta & \dots & h_{2\delta-2} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\delta-1} \end{pmatrix} = - \begin{pmatrix} h_\delta \\ h_{\delta+1} \\ \vdots \\ h_{2\delta-1} \end{pmatrix} \quad (7)$$

Without loss of generality we may assume $p \neq 0$ and hence $(h_0, \dots, h_{2\delta-1}) \neq 0$. Now we apply the algorithm of Sieveking–Kung in order to compute in additional space $O(\delta)$ and time $O(\delta \log^2 \delta \log \log \delta)$ an element $\rho \in R$ and for $\gamma := \rho^\delta$ a γ -multiple of the first 2δ coefficients $h_0, \dots, h_{2\delta-1}$ of (6). Notice that the solution $(u_0, \dots, u_{\delta-1})$ of the linear equation system (7) does not change if we substitute the elements $h_0, \dots, h_{2\delta-1}$ by their nonzero multiples $\gamma h_0, \dots, \gamma h_{2\delta-1}$. Since the matrix appearing in (7) is of Hankel type, we can solve the system (7) applying the technique of linear recurring sequences in additional space $O(\delta)$ and additional time $O(\delta^2 \log \delta \log \log \delta)$ (see e.g. [59]). In order to avoid divisions by elements of R we can modify slightly this classical algorithm and obtain as result a nonzero element γ of R such that $\gamma u_0, \dots, \gamma u_{\delta-1}$ are elements of R forming a solution of the system (7). \square

Let us now turn back to the situation at the beginning of this section. We re-take the notation and the assumptions introduced at this place. We attack now the main task of this subsection by the design of an algorithm which performs $\sigma = \lfloor \log(D\delta_r) \rfloor + 1$ iterations of the Newton–Hensel operator in space and time which are, roughly speaking, only quadratic and cubic in δ_r .

Theorem 5 *Let notations and assumptions be as at the beginning of this section. The coefficients of the minimal polynomial $q_F \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ satisfying the condition $q_F(Y_1, \dots, Y_{n-r}, F) \in (F_1, \dots, F_r)$ can be computed from a*

given geometric solution of the lifting fiber $V_{P^{(r)}}$, by a straight–line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ using space $O(SrD\delta_r^2)$ and time $O((TrD + r^4)D\delta_r^3 \log^3 \delta_r \log^2 \log \delta_r)$.

Proof We follow the strategy of [22] as outlined in the Introduction, applying for this purpose the procedures described in the proofs of Lemma 3 and Lemma 4.

Using a linear space straight–line program version of Samuelson’s algorithm for the computation of the determinant (see [18] or [1]), we first compute without divisions numerators g_{n-r+1}, \dots, g_n and a denominator h of the rational functions $\frac{g_{n-r+1}}{h}, \dots, \frac{g_n}{h}$ which represent the $\sigma = \lfloor \log(D\delta_r) \rfloor + 1$ iterations of the Newton–Hensel operator. Following the general lines of [22, Lemma 27] this can be done in space $O(Sr)$ and time $O((Tr + r^4) \log(D\delta_r))$.

Let us denote by $g_{n-r+1}^{(r)}(T), \dots, g_n^{(r)}(T), h^{(r)}(T)$ the polynomials of $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ resulting from the specialization of the variables Y_{n-r+1}, \dots, Y_n occurring in the polynomials g_{n-r+1}, \dots, g_n, h into the “parametrizing” polynomials $v_{n-r+1}^{(P^{(r)})}(T), \dots, v_n^{(P^{(r)})}(T)$ of the lifting fiber $V_{P^{(r)}}$. In Subsection 4.1 we have shown that the matrix $h(v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M))$ we obtain specializing in $h(Y_1, \dots, Y_n)$ the variables Y_{n-r+1}, \dots, Y_n into the matrices $v_{n-r+1}^{(P^{(r)})}(M), \dots, v_n^{(P^{(r)})}(M)$ represents an invertible element of the matrix ring $\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}^{\delta_r \times \delta_r}$ (recall that M denotes the companion matrix of the polynomial $q^{(P^{(r)})}(T)$). This implies that $h^{(r)}(T)$ is a unit in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}[T]/q^{(P^{(r)})}(T)$.

Now we consider in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}[T]$ the rational function

$$f^{(r)} := F \left(Y_1, \dots, Y_{n-r}, \frac{g_{n-r+1}^{(r)}(T)}{h^{(r)}(T)}, \dots, \frac{g_n^{(r)}(T)}{h^{(r)}(T)} \right)$$

modulo the polynomial $q^{(P^{(r)})}(T)$. For this purpose, we compute the homogeneous decomposition

$$\sum_{k=0}^d F_k(Y_1, \dots, Y_{n-r}, Y_{n-r+1}, \dots, Y_n)$$

of $F(Y_1, \dots, Y_n)$, which we consider as a polynomial in the variables Y_{n-r+1}, \dots, Y_n with coefficients from $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$. This decomposition can be computed by means of the procedure described in the proof of Lemma 4 using space $O(SD)$ and time $O(TD \log D \log \log D)$. Considering in

$$\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}[T]$$

the following identities:

$$\begin{aligned}
f^{(r)} &= F \left(Y_1, \dots, Y_{n-r}, \frac{g_{n-r+1}^{(r)}(T)}{h^{(r)}(T)}, \dots, \frac{g_n^{(r)}(T)}{h^{(r)}(T)} \right) \\
&= \sum_{k=0}^D F_k \left(Y_1, \dots, Y_{n-r}, \frac{g_{n-r+1}^{(r)}(T)}{h^{(r)}(T)}, \dots, \frac{g_n^{(r)}(T)}{h^{(r)}(T)} \right) \\
&= \sum_{k=0}^D \frac{F_k \left(Y_1, \dots, Y_{n-r}, g_{n-r+1}^{(r)}(T), \dots, g_n^{(r)}(T) \right)}{(h^{(r)}(T))^k} \\
&= \frac{\sum_{k=0}^D F_k \left(Y_1, \dots, Y_{n-r}, g_{n-r+1}^{(r)}(T), \dots, g_n^{(r)}(T) \right) (h^{(r)}(T))^{D-k}}{(h^{(r)}(T))^D},
\end{aligned}$$

we conclude that the numerator and denominator of the rational function $f^{(r)}$ can be computed in space $O(\mathcal{S}(r+D))$ and time $O((TrD+r^4)\log(D\delta_r))$ using only divisions by nonzero elements of \mathbf{Q} .

Since by construction the polynomials $h^{(r)}(T)$ and $q^{(P^{(r)})}(T)$ are coprime in $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ we are able to apply the procedure described at the beginning of the proof of Lemma 2 in order to compute a polynomial $\tilde{f}^{(r)}(T) \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ of degree in T at most $\delta_r - 1$ and an element $\alpha \in \mathbf{Q}[Y_1, \dots, Y_{n-r}]$ satisfying in $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ the condition $h^{(r)}(T)^D f^{(r)}(T) \equiv \alpha g(T)$ modulo $q^{(P^{(r)})}(T)$, with

$$g(T) := \sum_{1 \leq k \leq D} F_k(Y_1, \dots, Y_{n-r}, g_{n-r+1}^{(r)}(T), \dots, g_n^{(r)}(T)) \cdot h^{(r)}(T)^{D-k}.$$

Thus we have in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]_{(Y_1-p_1, \dots, Y_{n-r}-p_{n-r})}[T]$ the congruence relation $\tilde{f}^{(r)}(T) \equiv \alpha f^{(r)}(T)$ modulo $q^{(P^{(r)})}(T)$.

Since M is the companion matrix of the polynomial $q^{(P^{(r)})}(T)$, this implies with the notations of Theorem 4:

$$\begin{aligned}
\tilde{f}^{(r)}(M) &= \alpha f^{(r)}(M) \\
&= \alpha F(Y_1, \dots, Y_{n-r}, \mathcal{N}_{n-r+1}, \dots, \mathcal{N}_n) \cdot \\
&= \alpha \mathcal{M}_F
\end{aligned}$$

The polynomial $\tilde{f}^{(r)}(T)$ and the element α can be computed by means of a straight-line program in space $O(\mathcal{S}\delta_r(r+D))$ and time $O((TrD+r^4)\delta_r^2 \log^2 \delta_r \log \log \delta_r)$.

We have shown that $\alpha \mathcal{M}_F = \tilde{f}^{(r)}(M)$ holds. Therefore using a similar procedure as in the proof of Lemma 3, we are able to compute the α_r^δ -multiples of the coefficients of the characteristic polynomial $\chi(T) := \chi_{\mathcal{M}_F}(T)$ of \mathcal{M}_F in space

$O(\mathcal{S}\delta_r(r+D))$ and time $O((TrD+r^4)\delta_r^2\log^2\delta_r\log\log\delta_r)$. Thus, let us assume that the coefficients of the polynomial $\alpha^\delta\chi_F(T)$ are now computed.

Since the matrix \mathcal{M}_F is diagonalizable, it suffices to clear from the characteristic polynomial $\chi(T)$ of \mathcal{M}_F the multiple factors in order to obtain the minimal polynomial \tilde{q}_F of \mathcal{M}_F (recall the notations of Theorem 4). Therefore the monic numerator of the irreducible representation of the rational function $\frac{\chi(T)}{\chi'(T)} = \frac{\alpha^\delta\chi(T)}{\alpha^\delta\chi'(T)}$ is in fact the minimal polynomial $\tilde{q}_F(T)$ of the matrix \mathcal{M}_F . Now, applying Lemma 5 to the rational function $\frac{\alpha^\delta\chi(T)}{\alpha^\delta\chi'(T)}$ we compute an element $\gamma \in R$ and a γ -multiple of the coefficients $a_0, \dots, a_{\deg(q_F)}$ of the minimal polynomial \tilde{q}_F of \mathcal{M}_F , such that $\gamma a_0, \dots, \gamma a_{\deg(q_F)}$ are elements of R . This can be done in space $O(\mathcal{S}r\delta_r)$ and time $O((TrD+r^4)\delta_r^2\log^2\delta_r\log\log\delta_r)$.

Taking into account the congruence relation

$$q_F \equiv \tilde{q}_F \text{ modulo } (Y_1 - p_1, \dots, Y_{n-r} - p_{n-r})^{D\delta_r}$$

in $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ (see Theorem 4) and the fact that $\deg q_F \leq D\delta_r$ holds (see [55]), we deduce that for $1 \leq k \leq \deg q_F$ the power series expansion of the k -th coefficient a_k of the polynomial \tilde{q}_F equals to the k -th coefficient of the polynomial q_F . Since the polynomials $\gamma a_0, \dots, \gamma a_{\deg(q_F)}, \gamma \in \mathbf{Q}[Y_1, \dots, Y_{n-r}]$ are already computed by a division-free straight-line program, we are finally able to compute the polynomials $a_0, \dots, a_{\deg(q_F)} \in \mathbf{Q}[Y_1, \dots, Y_{n-r}]$ by means of Lemma 4. This can be done in space $O(\mathcal{S}Dr\delta_r)$ and time $O((TrD+r^4)D\delta_r^3\log^3\delta_r\log^2\log\delta_r)$. \square

Remark 1 In case $r := n - 1$, when the algebraic variety $V_r = V_{n-1}$ is a curve, the algorithm underlying Theorem 5 outputs in fact the dense representation of the polynomial $q_F(T) \in \mathbf{Q}[Y_1, T]$.

Proof In case $r := n - 1$, when $V_r = V_{n-1}$ has dimension one (i.e. V_r is a curve), we have a Noether normalization of the form $\mathbf{Q}[Y_1] \hookrightarrow \mathbf{Q}[V_{n-1}]$. We observe that the algorithm underlying the proof of Theorem 5 computes the elements $\gamma a_0, \dots, \gamma a_{\deg(q_F)}, \gamma$, which are in fact univariate polynomials of $\mathbf{Q}[Y_1]$. Then the *Vermeidung von Divisionen* procedure computes the power series expansion of the rational expressions $\frac{\gamma a_0}{\gamma}, \dots, \frac{\gamma a_{\deg(q_F)}}{\gamma}$ up to degree $D\delta_{n-1}$, producing thus the dense representation of the coefficients of the polynomial $q_F(T)$ with respect to the variable T . Therefore, the algorithm underlying Theorem 5 outputs the dense representation of the polynomial $q_F \in \mathbf{Q}[Y_1, T]$. \square

We apply now Theorem 5 and Remark 1 to a particular case. This application will be used again in Subsection 5.1.

Remark 2 Let us consider the curve

$$W_{P(r+1)} := V_r \cap \{Y_1 = p_1, \dots, Y_{n-r-1} = p_{n-r-1}\}$$

as a subvariety of \mathbf{C}^{r+1} . Let $\ell \in \mathbf{Q}[Y_1, \dots, Y_n]$ be a linear form such that $\ell, Y_{n-r+1}, \dots, Y_n$ are in Noether position with respect to the curve $W_{P(r+1)}$ and

such that ℓ plays the rôle of the free variable. Assume that there is given an element $a \in \mathbf{Q}$ such that the variety $V_{\ell,a} := W_{P^{(r+1)}} \cap \{\ell = a\}$ is a lifting fiber of $W_{P^{(r+1)}}$. Assume furthermore that there is given a geometric solution of the variety $V_{\ell,a}$, represented by polynomials $q^{(\ell,a)}, v_{n-r}^{(\ell,a)}, \dots, v_n^{(\ell,a)} \in \mathbf{Q}[T]$, i.e. we assume that the following identity holds:

$$V_{\ell,a} = \left\{ \left(v_{n-r}^{(\ell,a)}(u), \dots, v_n^{(\ell,a)}(u) \right) \in \mathbf{C}^{r+1} : q^{(\ell,a)}(u) = 0 \right\}.$$

Let be given a polynomial $F \in \mathbf{Q}[Y_1, \dots, Y_n]$ of total degree D by a straight-line program γ in $\mathbf{Q}[Y_1, \dots, Y_n]$. Let f be the coordinate function induced by the polynomial F on the curve $W_{P^{(r+1)}}$. Then we can apply Theorem 5 in order to compute the projection of f along the “line” ℓ , i.e. the minimal (integral) dependence relation $m_F \in \mathbf{Q}[\ell][T]$ satisfied by the coordinate function f . This can be done using as input the straight-line program γ computing F and the given geometric solution of $V_{\ell,a}$. We shall call this procedure *lifting the projection of F from $V_{\ell,a}$ to $W_{P^{(r+1)}}$* .

Since $W_{P^{(r+1)}}$ is a curve, we deduce from Remark 1 that the procedure of Theorem 5 outputs the *dense* representation of the polynomial $m_F \in \mathbf{Q}[\ell, T]$.

The technique of lifting a projection from a zero-dimensional variety to a curve is fundamental for the main algorithm of this paper. This technique was independently discovered and applied in [29].

4.2 An efficient Shape Lemma

This subsection will be devoted to the description of an efficient algorithm for the following task:

Let be given a natural number δ and let be given (by their coefficients) three nonconstant and separable polynomials $f, g, h \in \mathbf{Q}[T]$ of degree at most δ . Moreover, let be given a nonzero element $\alpha \in \mathbf{Q}$. Suppose that the linear form $u(X, Y) := \alpha X + Y$ separates the points of the zero-dimensional variety $\{(x, y) \in \mathbf{C}^2 : f(x) = 0, g(y) = 0\}$ and that the variety $W := \{(x, y) \in \mathbf{C}^2 : f(x) = 0, g(y) = 0, h(\alpha x + y) = 0\}$ is nonempty. The task consists in the computation of a geometric solution of the zero-dimensional variety W .

In many elimination procedures this task appears only for the special case $h := 0$, while the required output is the geometric solution of the variety W induced by the linear form $u(X, Y)$ (see e.g. [24], [42]). In [42] for instance, this task is solved by linear algebra computations.

From a practical point of view, this approach has the drawback of introducing additional (extraneous) points, producing in this way a quadratic growth of the size of the appearing matrices and hence also a quadratic excess of the space and time complexity of the algorithm. In this way, the corresponding subroutine of the elimination procedure under consideration contributes with an additional quadratic growth to the overall complexity of the procedure.

In order to overcome this undesirable effect, we reformulate the original algorithmic task in the above indicated way: instead of considering zero–dimensional varieties given only by two polynomials $f(X)$ and $g(Y)$ in two separate variables and a linear form $u(X, Y)$ as in [42], we introduce an additional condition given by the polynomial $h(u(X, Y))$, which eliminates the extraneous points.

In order to solve the task described above, it suffices to find a polynomial $v(T) \in \mathbf{Q}[T]$ of degree at most $\delta - 1$, such that $X - v(u(X, Y))$ vanishes on the whole variety W . Let us remark that the procedure of [42] computing such a polynomial $v(T)$ requires space $O(\delta^4)$ and time $O(\delta^8)$, and this is unfeasible for our algorithmic aim. Therefore, we redesign the effective Shape Lemma version of [42] in such a way that a quadratic complexity growth can be avoided. The following result represents the effective Shape lemma version we are going to use in the sequel (see Theorem 6 and Proposition 1 below).

Lemma 6 *Let R be an integrally closed domain of characteristic zero which contains the field \mathbf{Q} of rational numbers. Let K be the fraction field of R and let \bar{K} be an algebraic closure of K . Let $W \subset \bar{K}^2$ be a zero–dimensional variety and let $\delta := \deg W = \#W$. Let $f \in R[T]$ and $g \in R[T]$ be two nonconstant and square–free polynomials of degree at most δ . Moreover, let be given a nonzero element $\alpha \in \mathbf{Q}$ and assume that the linear form $u := \alpha X + Y$ separates the points of the variety $W_0 := \{(x, y) \in \bar{K}^2 : f(x) = 0, g(y) = 0\}$. Suppose furthermore $W \subset W_0$. Finally let $h \in R[T]$ be the minimal polynomial of the coordinate function of W induced by the linear form u . Assume that the polynomials $f(T), g(T)$ and $h(T)$ are given by their coefficients in R . Then there exists a nonzero element $\rho \in R$ and a polynomial $v(T) \in R[T]$ of degree strictly smaller than δ , such that $\rho X - v(u(X, Y))$ vanishes on the whole variety W and such that ρ and the coefficients of $v(T)$ can be computed by means of an essentially division–free straight–line program β in R using space $O(\delta^2)$ and time $O(\delta^3 \log^2 \delta \log^2 \log \delta)$.*

Here by “essentially division–free” we mean that β contains only divisions by nonzero elements of \mathbf{Q} . Furthermore let us observe that the polynomial $v(T)$ of the statement of Lemma 6 is uniquely determined up to scaling by nonzero elements of R . This means that there exists exactly one polynomial $\tilde{v}(T) \in K[T]$ of degree strictly smaller than δ with $X - \tilde{v}(u(X, Y))$ vanishing on the whole variety W and that this polynomial is precisely $\tilde{v}(T) := \frac{1}{\rho}v(T)$.

Proof of Lemma 6.– Let $W := \{\gamma_1, \dots, \gamma_\delta\}$ with $\gamma_i = (\alpha_i, \beta_i) \in \bar{K}^2$ for $1 \leq i \leq \delta$. By assumption the polynomial $h(u(X, Y))$ vanishes on the whole variety W and $h(T)$ is the polynomial in T of minimal degree having this property. Since $u(X, Y)$ separates the points of the variety W_0 (and hence also the points of W) and from the minimality of the degree of $h(T)$, we conclude $h(T) = \prod_{1 \leq i \leq \delta} (T - u(\gamma_i))$ and $\deg h = \deg W = \delta$.

From the assumption that the linear form $u(X, Y)$ separates the points of the variety W and from $\delta = \deg W$ one easily deduces the existence of a uniquely determined polynomial $\tilde{v}(T) \in K[T]$ of degree strictly less than δ such that $X -$

$\tilde{v}(u(X, Y))$ vanishes on the whole variety W (this is the standard form of the Shape–Lemma, see e.g. [43], [46] and [30]).

Fix for the moment an arbitrary index $1 \leq i \leq \delta$. We show first the following statement:

Claim: *The greatest common divisor (gcd) of the polynomials $f(X)$ and $g(u(\gamma_i) - \alpha X)$ of $\bar{K}[X]$ is the linear form $X - \tilde{v}(u(\gamma_i))$ (in symbols: $X - \tilde{v}(u(\gamma_i)) = \gcd(f(X), g(u(\gamma_i) - \alpha X))$).*

Proof of the Claim Since the polynomial $X - \tilde{v}(u(X, Y))$ vanishes on the variety W , we deduce from $(\alpha_i, \beta_i) = \gamma_i \in W$ the identity $\alpha_i - \tilde{v}(u(\gamma_i)) = \alpha_i - \tilde{v}(u(\alpha_i, \beta_i)) = 0$. Moreover we have $f(\alpha_i) = 0$ and by $u(\gamma_i) = \alpha\alpha_i + \beta_i$ also $g(u(\gamma_i) - \alpha\alpha_i) = g(\beta_i) = 0$.

The identity $\alpha_i = \tilde{v}(u(\gamma_i))$ implies now that $\tilde{v}(u(\gamma_i))$ is a common root of $f(X)$ and $g(u(\gamma_i) - \alpha X)$. Therefore the linear form $X - \tilde{v}(u(\gamma_i))$ divides the greatest common divisor of these polynomials. In order to finish the proof of the Claim, it suffices to show that $\tilde{v}(u(\gamma_i))$ is the unique common root of $f(X)$ and $g(u(\gamma_i) - \alpha X)$ (recall that $f(X)$ is by assumption square–free).

Let $\mu \in \bar{K}$ be any common root of these polynomials. Then, the point $\tilde{\gamma} := (\mu, u(\gamma_i) - \alpha\mu)$ belongs to the variety W_0 , defined by the polynomials $f(X)$ and $g(Y)$. Since by assumption the linear form $u(X, Y) = \alpha X + Y$ separates the points of the variety W_0 we deduce from the identity $u(\tilde{\gamma}) = u(\gamma_i)$ that $\tilde{\gamma} = \gamma_i$ holds. This finishes the proof of the Claim.

From the statement of the Claim we deduce immediately that in $\bar{K}[T]$ the identity

$$\begin{aligned} f(T) &= \prod_{1 \leq i \leq \delta} (T - v(u(\gamma_i))) \\ &= \prod_{1 \leq i \leq \delta} \gcd(f(T), g(u(\gamma_i) - \alpha T)) \end{aligned}$$

holds.

This implies that the first principal subresultant $P_1(u) \in K[u]$ of the Sylvester matrix of the polynomials $f(T)$ and $g(u - \alpha T)$ does not vanish on any root of $h(u)$ (here we treat the linear form u as an indeterminate). Therefore the residue class of $P_1(u)$ in $K[u]/(h(u))$ is a unit.

Taking into account that the variety W is contained in the variety W_0 (defined by $f(X)$ and $g(Y)$), that the linear form $u(X, Y)$ separates the points of W_0 and that by definition $h(T)$ is the minimal polynomial of the coordinate function of W induced by the linear form u , one easily sees that the variety W is definable by the equations $f(X) = 0, g(Y) = 0, h(u(X, Y)) = 0$. Let $I := (f(X), g(Y), h(u(X, Y)))$ be the ideal generated by these polynomials in $K[X, Y]$. Since by assumption $f(X)$ and $g(Y)$ are square–free, I is radical and hence the vanishing ideal of the variety W .

Therefore the polynomial $X - \tilde{v}(u(X, Y))$ belongs to the ideal $I = (f(X), g(Y), h(u(X, Y)))$ (recall that this polynomial vanishes on the variety W). This implies that there exist polynomials $r(X), s(X)$ of $K[u]/(h(u))[X]$ such that in

this polynomial ring the identity

$$X - \tilde{v}(u) = r(X)f(X) + s(X)g(u - \alpha X) \quad (8)$$

holds. Without loss of generality we may assume

$$\deg_X r \leq \deg_X(g(u - \alpha X)) - 1 \text{ and } \deg_X s \leq \deg_X(f(X)) - 1 \quad (9)$$

Since the residue class of $P_1(u)$ in $K[u]/(h(u))$ is a unit, the coefficients of $r(X)$ and $s(X)$ are uniquely determined by the identities (8) and (9).

If we are able to find polynomials $r(X), s(X) \in K[u]/(h(u))[X]$ satisfying the identities (8) and (9) we easily obtain $\tilde{v}(u)$ as the constant term of the polynomial

$$r(X)f(X) + s(X)g(u - \alpha X)$$

in $K[u]/(h(u))[X]$.

In order to compute the Bezout identity (8) subject to condition (9) we use the algorithms of [59] or [16]. These algorithms return as output a multiple $w(u)$ of the Bezout identity (8), namely a representation

$$w(u)X - \hat{v}(u) = \tilde{r}(X)f(X) + \tilde{s}(X)g(u - \alpha X), \quad (10)$$

with polynomials $\tilde{r}, \tilde{s} \in K[u]/(h(u))[X]$ having degree at most $\deg_X(g(u - \alpha X)) - 1$ and $\deg_X(f(X)) - 1$ respectively and $w(u), \hat{v}(u)$ belonging to $K[u]/(h(u))$. Without loss of generality we may assume that $w(u)$ and $\hat{v}(u)$ are polynomials in the variable u (i.e. elements of $K[u]$) which are reduced modulo $h(u)$. If $\gcd(w(u), h(u)) = 1$ holds, we can invert $w(u)$ modulo $h(u)$ in order to satisfy conditions (8) and (9) with $w(u)\tilde{v}(u) \equiv \hat{v}(u)$ modulo $h(u)$. If $\gcd(w(u), h(u))$ is a nonconstant polynomial $w_1(u)$ of $K[u]$, we claim that $w_1(T)$ divides $\hat{v}(T)$. Since the polynomial $h(T)$ is separable and $w_1(T)$ divides this polynomial, we conclude that $w_1(T)$ is separable too. Thus, if $w_1(T)$ does not divide $\hat{v}(T)$, there exists a root τ of $w_1(T)$ with $\hat{v}(\tau) \neq 0$. Since $w_1(T)$ divides $h(T) = \prod_{1 \leq i \leq \delta} (T - u(\gamma_i))$ there exists $1 \leq i \leq \delta$ such that the root τ is of the form $u(\gamma_i)$. Thus, we have $w(u(\gamma_i)) = 0$ and $\hat{v}(u(\gamma_i)) \neq 0$. Since $u(\gamma_i)$ is a root of $h(T)$ we may “specialize” in identity (10) the residue class of u modulo $h(u)$ into the value $u(\gamma_i)$. Doing this we deduce from (10) that the polynomials $f(X)$ and $g(u(\gamma_i) - \alpha X)$ are coprime, which contradicts the statement of the Claim above. Thus $w_1(T) = \gcd(w(T), h(T))$ divides $\hat{v}(T)$. This allows to compute the polynomial $\tilde{v}(u)$ of the identity (8) in an analogous way as before from the polynomial $\frac{\hat{v}(u)}{w_1(u)}$.

The computation of the polynomial $\tilde{v}(u)$ satisfying conditions (8) and (9) above can be done by $O(\delta^2 \log \delta \log \log \delta)$ arithmetic operations in $K[u]/(h(u))$ using space $O(\delta)$. Performing these arithmetic operations by FFT–based algorithms as in [5], we obtain a straight–line program $\tilde{\beta}$ in K (containing divisions) which computes the coefficients of the polynomial $\tilde{v}(T)$. Computing numerators and denominators in $\tilde{\beta}$ separately, we get an essentially division–free straight–line program β in R which computes a nonzero element $\rho \in R$ and the coefficients of a polynomial $v(T) \in R[T]$ of the same degree as $\tilde{v}(T)$ such that $\frac{1}{\rho}v(T) = \tilde{v}(T)$

holds. It is now clear that $\rho X - v(u(X, Y))$ vanishes on the whole variety W , and that β has essentially the same space and time complexity as $\tilde{\beta}$. Thus β satisfies the requirements of Lemma 6. \square

4.3 Lifting of a zero-dimensional fiber

In this subsection we shall develop an algorithm which, given a geometric solution of the lifting fiber $V_{P^{(r)}}$ as input, computes a geometric solution of the algebraic variety V_r as output. For this purpose we shall follow the strategy of [42], in combination with our tools developed in Subsections 4.1 and 4.2.

In the sequel we shall use the following notations and conventions: let be given the linear form $U^{(r)} := \lambda_{n-r+1}^{(r)} Y_{n-r+1} + \cdots + \lambda_n^{(r)} Y_n$ which induces a primitive element of $V_{P^{(r)}}$ (and hence of the integral \mathbf{Q} -algebra extension $\mathbf{Q}[Y_1, \dots, Y_{n-r}] \hookrightarrow \mathbf{Q}[V_r]$) and let be given the coefficients of the polynomials $q^{(P^{(r)})}, v_{n-r+1}^{(P^{(r)})}, \dots, v_n^{(P^{(r)})} \in \mathbf{Q}[T]$ introduced in Subsection 4.1 for the representation of a geometric solution of the lifting fiber $V_{P^{(r)}}$. Following [42], we define for $1 \leq j \leq r$ linear form $Z_j^{(r)} := U^{(r)} - \lambda_{n-r+j}^{(r)} Y_{n-r+j}$ and denote by $\tilde{q}_j^{(r)} \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ the minimal polynomial of the coordinate function of V_r induced by Z_j . Furthermore, let us denote by $q^{(r)}$ and $q_1^{(r)}, \dots, q_r^{(r)} \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ the minimal polynomials of the coordinate functions of V_r induced by the linear forms $U^{(r)}$ and Y_{n-r+1}, \dots, Y_n . With the notations of Lemma 6 above, let $R := \mathbf{Q}[Y_1, \dots, Y_{n-r}]$, $K := \mathbf{Q}(Y_1, \dots, Y_{n-r})$ and let \bar{K} be an algebraic closure of K . In the proof of Theorem 6 below we are going to apply for each $1 \leq j \leq r$ the algorithm underlying the statement of Lemma 6 to the zero-dimensional algebraic variety $W_j^{(r)} := \{(y, z) \in \bar{K}^2 : q_j^{(r)}(y) = 0, \tilde{q}_j^{(r)}(z) = 0\}$.

Under the assumption that the coefficient vector of the linear form $U^{(r)}$ satisfies a certain genericity condition, it was shown in [42, Proposition 29] that a Shape-Lemma-like representation of each algebraic variety $W_1^{(r)}, \dots, W_r^{(r)}$ produces “parametrizing” polynomials $\rho_{n-r+1}^{(r)} Y_{n-r+1} - v_{n-r+1}^{(r)}(T), \dots, \rho_n^{(r)} Y_n - v_n^{(r)}(T)$ of $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ required for a geometric solution of the variety V_r (here we use the coordinate function of V_r induced by the linear form $U^{(r)}$ as a primitive element with minimal polynomial $q^{(r)}(T)$).

Therefore, the problem of computing a geometric solution of V_r is reduced to the following two tasks: the lifting of a projection (in the sense of Subsection 4.1) and the computation of a Shape-Lemma-like representation (in the sense of Subsection 4.2). These two tasks are solved in Theorem 5 and in Lemma 6. The next result will illustrate this idea.

Theorem 6 *Let notations and assumptions be as before. In particular, let be given a linear form $U^{(r)} \in \mathbf{Q}[Y_{n-r+1}, \dots, Y_n]$ inducing a primitive element of the lifting fiber $V_{P^{(r)}}$. Then there exists a straight-line program in $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$, computing from (the coefficients of) a given geometric solution of the lifting fiber $V_{P^{(r)}}$ and the given linear form $U^{(r)}$ the coefficients of a geometric solution of*

the algebraic variety V_r . This straight–line program uses space $O(Sr\delta_r^2)$ and time $O((\mathcal{T}r^2 + r^5)\delta_r^3 \log^3 \delta_r \log^2 \log \delta_r)$.

Proof Assume that there is given as before a geometric solution of the lifting fiber $V_{P^{(r)}}$. Applying Theorem 5 we are then able to compute the coefficients of the minimal integral dependence relations $q^{(r)}(T), q_1^{(r)}(T), \dots, q_r^{(r)}(T), \tilde{q}_1^{(r)}(T), \dots, \tilde{q}_r^{(r)}(T)$ of the coordinate functions of V_r induced by the linear forms $U^{(r)}, Y_{n-r+1}, \dots, Y_n$ and $Z_1^{(r)}, \dots, Z_r^{(r)}$. Then, for $1 \leq j \leq r$, we apply Lemma 6 to the zero–dimensional variety $W_j^{(r)}$ and the polynomials $q^{(r)}, q_j^{(r)}$ and $\tilde{q}_j^{(r)}$ in order to compute the coefficients of a polynomial having the form $\rho_{n-r+j}^{(r)} Y_{n-r+j} - v_{n-r+j}^{(r)}(T) \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ with $\rho_{n-r+j}^{(r)} \neq 0$ and $\deg_T v_{n-r+j}^{(r)}(T) < \delta_r$, such that $U^{(r)}, q^{(r)}(T)$ and $\rho_{n-r+1}^{(r)} Y_{n-r+1} - v_{n-r+1}^{(r)}(T), \dots, \rho_n^{(r)} Y_n - v_n^{(r)}(T)$ form a geometric solution of the variety V_r .

From the complexity estimates of Theorem 5 and Lemma 6 we deduce now easily the complexity statement of Theorem 6. \square

Theorem 6 has its own interest. Unfortunately, in the sequel we shall not be able to apply Theorem 6 directly since we have no control over the coefficients $\rho_{n-r+1}^{(r)}, \dots, \rho_n^{(r)}$ produced by the application of Lemma 6 in the proof of Theorem 6. Therefore, we shall only apply Lemma 6 and not Theorem 6 in the future.

4.4 Minimal equations: stepping downwards on the lifting fibers

In Subsection 4.1 we have already met the task of computing a minimal integral dependence relation in $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ for the coordinate function of V_r induced by a given polynomial $F \in \mathbf{Q}[Y_1, \dots, Y_n]$. In the present subsection we describe an efficient algorithm for the following task:

Let $1 \leq r < n$. Given a geometric solution of the lifting fiber $V_{P^{(r)}}$ of V_r , compute the coefficients of the minimal equation in $\mathbf{Q}[T]$ of the coordinate function of the lifting fiber $V_{P^{(r+1)}}$ induced by the linear form Y_{n-r} .

Below we present two lemmas deducing finally from them Proposition 1 which says that, under the assumptions of Theorem 3, the coefficients of the minimal equation $m_{Y_{n-r}} \in \mathbf{Q}[T]$ of the coordinate function of $V_{P^{(r+1)}}$ induced by the linear form Y_{n-r} can be computed by a straight–line program in space $O(Srd\delta_r^2)$ and time $O((\mathcal{T}dr + r^4)d\delta_r^3 \log^3 \delta_r \log^2 \log \delta_r)$.

Applying the Zippel–Schwartz test in the same way as in Section 3, we deduce from Theorem 3, that by a random choice of the coefficients $\lambda_{n-r+1}^{(r)}, \dots, \lambda_n^{(r)}$, the linear form $U^{(r)} = \lambda_{n-r+1}^{(r)} Y_{n-r+1} + \dots + \lambda_n^{(r)} Y_n$ happens to separate the points of the π_r –fiber of the π_r –image of each point of the lifting fiber $V_{P^{(r+1)}}$. Assume from now on that the linear form $U^{(r)}$ has this property.

Let us consider again the curve

$$W_{P^{(r+1)}} := V_r \cap \{Y_1 = p_1, \dots, Y_{n-r-1} = p_{n-r-1}\}$$

introduced in Remark 2 and observe that $W_{P^{(r+1)}}$ is defined by the polynomials $F_1(Y_1, \dots, Y_n), \dots, F_r(Y_1, \dots, Y_n), Y_1 - p_1^{(r+1)}, \dots, Y_{n-r-1} - p_{n-r-1}^{(r+1)}$ which form a regular sequence in $\mathbf{Q}[Y_1, \dots, Y_n]$.

The variables Y_1, \dots, Y_n are in Noether position with respect to this complete intersection curve, the variable Y_{n-r} being free. Therefore the canonical homomorphism $\mathbf{Q}[Y_{n-r}] \hookrightarrow \mathbf{Q}[W_{P^{(r+1)}}]$ represents an integral \mathbf{Q} -algebra extension. Moreover $\mathbf{Q}[W_{P^{(r+1)}}]$ is a free $\mathbf{Q}[Y_{n-r}]$ -module of rank δ_r .

Let us denote by $u^{(r)}$ and y_{n-r} the coordinate functions of the curve $W_{P^{(r+1)}}$ induced by the linear forms $U^{(r)}$ and Y_{n-r} . Let us fix for the moment an arbitrary point $P = (p_1, \dots, p_{n-r-1}, \alpha_{n-r}, \dots, \alpha_n) \in \mathbf{C}^n$ of the (nonempty) lifting fiber $\pi_{r+1}^{-1}(P^{(r+1)}) = V_{P^{(r+1)}}$. Let us consider the fiber

$$\begin{aligned} \pi_r^{-1}(\pi_r(P)) &= \pi_r^{-1}\left((p_1, \dots, p_{n-r-1}, \alpha_{n-r})\right) \\ &= V_r \cap \{Y_1 = p_1, \dots, Y_{n-r-1} = p_{n-r-1}, Y_{n-r} = \alpha_{n-r}\} \end{aligned}$$

which is defined by the polynomials $F_1(Y_1, \dots, Y_n), \dots, F_r(Y_1, \dots, Y_n), Y_1 - p_1, \dots, Y_{n-r-1} - p_{n-r-1}, Y_{n-r} - \alpha_{n-r}$ of $\mathbf{C}[Y_1, \dots, Y_n]$.

From Theorem 3 iv) we deduce that the Jacobian of these polynomials vanishes nowhere on $\pi_r^{-1}(\pi_r(P))$. This implies that the canonical \mathbf{C} -algebra homomorphism

$$\begin{aligned} \mathbf{C}[Y_1, \dots, Y_{n-r}]_{(Y_1 - p_1, \dots, Y_{n-r-1} - p_{n-r-1}, Y_{n-r} - \alpha_{n-r})} \\ \downarrow \\ \mathbf{C}[Y_1, \dots, Y_{n-r}]_{(Y_1 - p_1, \dots, Y_{n-r-1} - p_{n-r-1}, Y_{n-r} - \alpha_{n-r})}[Y_{n-r+1}, \dots, Y_n] / \\ (F_1, \dots, F_r) \end{aligned} \quad (11)$$

is unramified and hence étale (recall that $\mathbf{C}[Y_1, \dots, Y_n]/(F_1, \dots, F_r)$ is a free $\mathbf{C}[Y_1, \dots, Y_{n-r}]$ -module of rank δ_r). Therefore we conclude that $\#\pi_r^{-1}(\pi_r(P)) = \delta_r$ holds.

Observe that the set $\pi_r^{-1}(\pi_r(P))$ is contained in the curve $W_{P^{(r+1)}}$, and that $\pi_r^{-1}(\pi_r(P))$ is the fiber of the finite morphism $y_{n-r} : W_{P^{(r+1)}} \rightarrow \mathbf{C}^1$ in the point $\alpha_{n-r} \in \mathbf{C}$ (in symbols: $\pi_r^{-1}(\pi_r(P)) = y_{n-r}^{-1}(\alpha_{n-r})$). Recall that, by construction, the linear form $U^{(r)}$ separates the δ_r points of the fiber $y_{n-r}^{-1}(\alpha_{n-r}) = \pi_r^{-1}(\pi_r(P))$ and that $\mathbf{Q}[W_{P^{(r+1)}}]$ is a free $\mathbf{Q}[Y_{n-r}]$ -module of rank δ_r . This implies that $u^{(r)}$ is a primitive element of the integral \mathbf{Q} -algebra extension $\mathbf{Q}[Y_{n-r}] \rightarrow \mathbf{Q}[W_{P^{(r+1)}}]$.

Let, as in Subsection 4.3, the polynomial $q^{(r)} \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ represent the minimal integral dependence relation of the coordinate function of V_r induced by the linear form $U^{(r)}$ and let us denote by $\rho^{(r)} \in \mathbf{Q}[Y_1, \dots, Y_{n-r}]$ the discriminant of $q^{(r)}(T)$ with respect to the variable T . Let $q^{(r, P^{(r+1)})}(Y_{n-r}, T) := q^{(r)}(p_1, \dots, p_{n-r-1}, Y_{n-r}, T)$. Then the polynomial $q^{(r, P^{(r+1)})}$ belongs to $\mathbf{Q}[Y_{n-r}][T]$ and represents the minimal integral dependence relation of the primitive element $u^{(r)} \in \mathbf{Q}[W_{P^{(r+1)}}]$ over $\mathbf{Q}[Y_{n-r}]$. Observe $\deg q^{(r, P^{(r+1)})} = \deg_T q^{(r, P^{(r+1)})} = \delta_r$.

Observe furthermore that the coordinate functions $y_{n-r}, u^{(r)} \in \mathbf{Q}[W_{P^{(r+1)}}]$ define a morphism of algebraic varieties which maps $W_{P^{(r+1)}}$ onto the plane curve defined by the polynomial $q^{(r, P^{(r+1)})}(Y_{n-r}, T)$. This morphism is finite and has a rational inverse which may be given by a geometric solution of the curve $W_{P^{(r+1)}}$, with the free variable Y_{n-r} and primitive element induced by the linear form $U^{(r)}$. In the proofs of the next two lemmas we shall make a *purely mathematical* use of a particular geometric solution of $W_{P^{(r+1)}}$, which we shall *not* compute.

Observe first that $\rho^{(r, P^{(r+1)})}(Y_{n-r}) := \rho^{(r)}(p_1, \dots, p_{n-r-1}, Y_{n-r}) \in \mathbf{Q}[Y_{n-r}]$ is the discriminant of the polynomial $q^{(r, P^{(r+1)})}(Y_{n-r}, T)$ with respect to the variable T . Let us now consider (but not compute) polynomials $v_{n-r+1}^{(r, P^{(r+1)})}, \dots, v_n^{(r, P^{(r+1)})} \in \mathbf{Q}[Y_{n-r}, T]$ which are uniquely determined by the condition

$$\begin{aligned} & \left(F_1(p_1^{(r+1)}, \dots, p_{n-r-1}^{(r+1)}, Y_{n-r}, \dots, Y_n), \dots, \right. \\ & \quad \left. F_r(p_1, \dots, p_{n-r-1}, Y_{n-r}, \dots, Y_n) \right)_{\rho^{(r, P^{(r+1)})}(Y_{n-r})} = \\ & = \left(q^{(r, P^{(r+1)})}(Y_{n-r}, U^{(r)}), \rho^{(r, P^{(r+1)})}(Y_{n-r}) Y_{n-r+1} - v_{n-r+1}^{(r, P^{(r+1)})}(U^{(r)}), \right. \\ & \quad \left. \dots, \rho^{(r, P^{(r+1)})}(Y_{n-r}) Y_n - v_n^{(r, P^{(r+1)})}(U^{(r)}) \right)_{\rho^{(r, P^{(r+1)})}(Y_{n-r})} \quad (12) \end{aligned}$$

Thus, the linear form $U^{(r)}$ and the polynomials $\rho^{(r, P^{(r+1)})} \in \mathbf{Q}[Y_{n-r}]$ and $q^{(r, P^{(r+1)})}(T), v_{n-r+1}^{(r, P^{(r+1)})}(T), \dots, v_n^{(r, P^{(r+1)})}(T) \in \mathbf{Q}[Y_{n-r}][T]$ represent a *particular* geometric solution of the curve $W_{P^{(r+1)}}$ in the sense of the Introduction. This geometric solution induces in the most obvious way a “reduction” isomorphism which maps the “rational function $\mathbf{Q}(Y_{n-r})$ –algebra” $\mathbf{Q}(Y_{n-r}) \otimes \mathbf{Q}[Y_{n-r}]$ $\mathbf{Q}[W_{P^{(r+1)}}]$ of $W_{P^{(r+1)}}$ onto the “rational function $\mathbf{Q}(Y_{n-r})$ –algebra” $\mathbf{Q}(Y_{n-r})[T]/(q^{(r, P^{(r+1)})}(Y_{n-r}, T))$ of the curve $\{q^{(r, P^{(r+1)})}(Y_{n-r}, T) = 0\}$ contained in \mathbf{C}^2 . This isomorphism leaves the field $\mathbf{Q}(Y_{n-r})$ fixed.

We are now going to analyze this isomorphism more closely. For any polynomial $F \in \mathbf{Q}[Y_1, \dots, Y_n]$ inducing a coordinate function φ of $\mathbf{Q}[W_{P^{(r+1)}}]$ let us write

$$\begin{aligned} \hat{F} := F & \left(p_1, \dots, p_{n-r-1}, Y_{n-r}, \frac{v_{n-r-1}^{(r, P^{(r+1)})}(Y_{n-r}, T)}{\rho^{(r, P^{(r+1)})}(Y_{n-r})}, \right. \\ & \quad \left. \dots, \frac{v_n^{(r, P^{(r+1)})}(Y_{n-r}, T)}{\rho^{(r, P^{(r+1)})}(Y_{n-r})} \right) \in \mathbf{Q}[Y_{n-r}]_{\rho^{(r, P^{(r+1)})}(Y_{n-r})}[T] \end{aligned}$$

and let us write $\hat{\varphi}$ for the residue class of \hat{F} in

$$\mathbf{Q}[Y_{n-r}]_{\rho^{(r, P^{(r+1)})}(Y_{n-r})}[T]/(q^{(r, P^{(r+1)})}(Y_{n-r}, T)).$$

Observe that $\hat{F}(y_{n-r}, u^{(r)})$ and $\hat{\varphi}$ define rational functions of the curves $W_{P^{(r+1)}}$ and $\{q^{(r, P^{(r+1)})}(Y_{n-r}, T) = 0\}$ respectively.

In the sequel we shall denote by φ_{r+1} the coordinate function of $\mathbf{Q}[W_{P^{(r+1)}}]$ induced by the polynomial $F_{r+1} \in \mathbf{Q}[Y_1, \dots, Y_n]$ and we shall write $f_{r+1}(Y_{n-r},$

$T) := \hat{F}_{r+1}(Y_{n-r}, T)$. Thus $f_{r+1}(y_{n-r}, u^{(r+1)})$ and $\hat{\varphi}_{r+1}$ define rational functions of the curves $W_{P^{(r+1)}}$ and $\{q^{(r, P^{(r+1)})}(Y_{n-r}, T) = 0\}$ respectively.

Let us observe

$$\begin{aligned} V_{P^{(r+1)}} &= V_{r+1} \cap \{Y_1 = p_1, \dots, Y_{n-r-1} = p_{n-r-1}\} \\ &= V_r \cap \{F_{r+1}(Y_1, \dots, Y_n) = 0, Y_1 = p_1, \dots, Y_{n-r-1} = p_{n-r-1}\} \\ &= W_{P^{(r+1)}} \cap \{F_{r+1}(Y_1, \dots, Y_n) = 0\}. \end{aligned}$$

In particular $V_{P^{(r+1)}}$ is a zero-dimensional variety contained in the curve $W_{P^{(r+1)}}$ and the polynomials $\rho^{(r)}(Y_1, \dots, Y_n)$ and $\rho^{(r, P^{(r+1)})}(Y_{n-r})$ induce the same coordinate function of $V_{P^{(r+1)}}$.

We are going to show that this coordinate function is a unit of $\mathbf{Q}[V_{P^{(r+1)}}]$ (this implies then that the rational function $f_{r+1}(y_{n-r}, u^{(r)})$ is well defined in all points of $V_{P^{(r+1)}}$). Assume on the contrary that there exists a point $P = (p_1, \dots, p_{n-r-1}, \alpha_{n-r}, \dots, \alpha_n) \in V_{P^{(r+1)}}$ such that $\rho^{(r)}(p_1, \dots, p_{n-r-1}, \alpha_{n-r}) = \rho^{(r, P^{(r+1)})}(\alpha_{n-r}) = 0$ holds. Since $\rho^{(r)}$ is the discriminant of the polynomial $q^{(r)} \in \mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$ with respect to the variable T , we deduce that $q^{(r)}(p_1, \dots, p_{n-r-1}, \alpha_{n-r}, T) = q^{(r, P^{(r)})}(\alpha_{n-r}, T)$ has a multiple root.

From (11) we deduce $\#\pi_r^{-1}((p_1, \dots, p_{n-r-1}, \alpha_{n-r})) = \#\pi_r^{-1}(\pi_r(P)) = \delta_r$. Moreover, by construction, the linear form $U^{(r)}$ separates the δ_r points of $\pi_r^{-1}(\pi_r(P))$. Let $\pi_r^{-1}(\pi_r(P)) = \{\gamma_1, \dots, \gamma_{\delta_r}\}$. Then we have $\#\{U^{(r)}(\gamma_1), \dots, U^{(r)}(\gamma_{\delta_r})\} = \delta_r$ and since the point $P = (p_1, \dots, p_{n-r-1}, \alpha_{n-r}, \dots, \alpha_n)$ belongs to $V_{P^{(r+1)}} \subset V_r$ and since $q^{(r)}(Y_1, \dots, Y_{n-r}, U^{(r)})$ vanishes on V_r we conclude that

$$q^{(r)}(p_1, \dots, p_{n-r-1}, \alpha_{n-r}, U^{(r)}(\gamma_j)) = q^{(r, P^{(r)})}(\alpha_{n-r}, U^{(r)}(\gamma_j)) = 0$$

holds for any $1 \leq j \leq \delta_r$. Moreover we have $\deg q^{(r, P^{(r+1)})}(\alpha_{n-r}, T) = \delta_r$. Putting all this together, we see that $q^{(r, P^{(r+1)})}(\alpha_{n-r}, T)$ is a separable polynomial of $\mathbf{C}[T]$. This contradicts the conclusion that $q^{(r, P^{(r+1)})}(\alpha_{n-r}, T)$ has a multiple root. Therefore the polynomial $\rho^{(r, P^{(r+1)})}(Y_{n-r})$ induces a unit of $\mathbf{Q}[V_{P^{(r+1)}}]$ and the rational function $f_{r+1}(y_{n-r}, u^{(r)})$ is well defined (and finite) in all points of $V_{P^{(r+1)}}$.

With these definitions, notions and notations we are now ready to expose the procedure which computes the minimal polynomial $m_{Y_{n-r}} \in \mathbf{Q}[Y_{n-r}]$ of the coordinate function of $V_{P^{(r+1)}}$ induced by the variable Y_{n-r} . We show in Lemma 7 below that the polynomial

$$g(Y_{n-r}) := \text{Res}_T \left(q^{(r, P^{(r+1)})}(Y_{n-r}, T), (\rho^{(r, P^{(r+1)})})^N(Y_{n-r}) f_{r+1}(Y_{n-r}, T) \right)$$

vanishes on all roots of the minimal polynomial $m_{Y_{n-r}}(Y_{n-r})$ (here N denotes a suitable positive integer, not exceeding $d\delta_r$, which satisfies the condition $(\rho^{(r, P^{(r)})})^N f_{r+1}(Y_{n-r}, T) \in \mathbf{Q}[Y_{n-r}, T]$). Perhaps the polynomial $g(Y_{n-r})$ vanishes also on certain roots of $\rho^{(r, P^{(r+1)})}(Y_{n-r})$ and might have high degree.

The exact relationship between the polynomials $g(Y_{n-r})$ and $m_{Y_{n-r}}(Y_{n-r})$ is clarified in Lemma 8 below. This lemma says that the square–free representation $a(Y_{n-r}) \in \mathbf{Q}[Y_{n-r}]$ of the roots of $g(Y_{n-r})$ satisfies the condition

$$m_{Y_{n-r}}(Y_{n-r}) = \frac{a(Y_{n-r})}{\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), a(Y_{n-r}))}.$$

Lemma 7 *Let $m_{Y_{n-r}} \in \mathbf{Q}[Y_{n-r}]$ be the minimal equation satisfied by the coordinate function of $V_{P^{(r+1)}}$ induced by the variable Y_{n-r} and let $g \in \mathbf{Q}[Y_{n-r}]$ be defined as*

$$g(Y_{n-r}) := \text{Res}_T \left(q^{(r,P^{(r+1)})}(Y_{n-r}, T), (\rho^{(r,P^{(r+1)})})^N(Y_{n-r}) f_{r+1}(Y_{n-r}, T) \right)$$

where N is a positive integer, not exceeding $d\delta_r$, such that $(\rho^{(r,P^{(r+1)})})^N(Y_{n-r}) f_{r+1}(Y_{n-r}, T)$ belongs to the polynomial ring $\mathbf{Q}[Y_{n-r}, T]$. Then the polynomial g vanishes on all roots of the polynomial $m_{Y_{n-r}}$. Moreover the polynomials $m_{Y_{n-r}}$ and $\rho^{(r,P^{(r+1)})}$ are coprime and the roots of the polynomial g where $\rho^{(r,P^{(r+1)})}$ does not vanish are also roots of the polynomial $m_{Y_{n-r}}$.

Proof Let $\alpha \in \mathbf{C}$ be a root of g with $\rho^{(r,P^{(r+1)})}(\alpha) \neq 0$. Then $f_{r+1}(\alpha, T)$ is a well defined polynomial of $\mathbf{C}[T]$ and there exists a complex number u_α satisfying the conditions $q^{(r,P^{(r+1)})}(\alpha, u_\alpha) = 0$ and $f_{r+1}(\alpha, u_\alpha) = 0$.

For $1 \leq j \leq r$ let $\alpha_{n-r+j} := \frac{v_{n-r+j}^{(r,P^{(r+1)})}(\alpha, u_\alpha)}{\rho^{(r,P^{(r+1)})}(\alpha)}$. We claim that the point

$$(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n) = (p_1, \dots, p_{n-r-1}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n)$$

belongs to the lifting fiber $V_{P^{(r+1)}}$.

Specializing in the right hand side of the identity (12) the “variables” $U^{(r)}$, $Y_{n-r}, Y_{n-r-1}, \dots, Y_n$ into the values $u_\alpha, \alpha, \alpha_{n-r+1}, \dots, \alpha_n$ and observing $\rho^{(r,P^{(r+1)})}(\alpha) \neq 0$ we deduce that $F_j(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n) = 0$ holds for every $1 \leq j \leq r$ (here we use the fact that the affine curves $W_{P^{(r+1)}} \cap \{\rho^{(r,P^{(r+1)})}(Y_{n-r}) \neq 0\}$ and $\{q^{(r,P^{(r+1)})}(Y_{n-r}) = 0, \rho^{(r,P^{(r+1)})}(Y_{n-r}) \neq 0\}$ are isomorphic, while the corresponding isomorphism is ideal–theoretically expressed by the identity (12)).

Therefore the point $(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n)$ belongs to the curve $W_{P^{(r+1)}}$. From the definition of f_{r+1} , namely $f_{r+1}(Y_{n-r}, T) = \hat{F}_{r+1}(Y_{n-r}, T) =$

$$= F \left(P^{(r+1)}, Y_{n-r}, \frac{v_{n-r-1}^{(r,P^{(r+1)})}(Y_{n-r}, T)}{\rho^{(r,P^{(r+1)})}(Y_{n-r})}, \dots, \frac{v_n^{(r,P^{(r+1)})}(Y_{n-r}, T)}{\rho^{(r,P^{(r+1)})}(Y_{n-r})} \right)$$

we deduce $0 = f_{r+1}(\alpha, u_\alpha) = F_{r+1}(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n)$ and this finally implies that the point $(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n)$ belongs to the variety $V_{P^{(r+1)}} = W_{P^{(r+1)}} \cap \{F_{r+1}(Y_1, \dots, Y_n) = 0\}$.

From $(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n) \in V_{P^{(r+1)}}$ we deduce that $m_{Y_{n-r}}(\alpha) = 0$ holds. Thus any root of the polynomial g , where $\rho^{(r,P^{(r+1)})}$ does not vanish, is a root of $m_{Y_{n-r}}$.

Let now $\alpha \in \mathbf{C}$ be a root of $m_{Y_{n-r}}$ with $\rho^{(r, P^{(r+1)})}(\alpha) \neq 0$. Then there exist complex numbers $\alpha_{n-r+1}, \dots, \alpha_n$ such that the point $(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n)$ belongs to the lifting fiber $V_{P^{(r+1)}}$. Consider $u_\alpha := U^{(r)}(\alpha_{n-r+1}, \dots, \alpha_n) = \lambda_{n-r+1}^{(r)} \alpha_{n-r+1} + \dots + \lambda_n^{(r)} \alpha_n$. Using again identity (12) and observing that by hypothesis $\rho^{(r, P^{(r+1)})}(\alpha) \neq 0$ we conclude that $q^{(r, P^{(r+1)})}(\alpha, u_\alpha) = 0$ and $\alpha_{n-r+j} = \frac{v_j^{(r, P^{(r+1)})}(\alpha, u_\alpha)}{\rho^{(r, P^{(r+1)})}(\alpha)}$ holds for any $1 \leq j \leq r$. In the same manner as before, we deduce from the definition of f_{r+1} that $f_{r+1}(\alpha, u_\alpha)$ is well defined and that $f_{r+1}(\alpha, u_\alpha) = F_{r+1}(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n) = 0$ holds (recall that $(P^{(r+1)}, \alpha, \alpha_{n-r+1}, \dots, \alpha_n)$ belongs to $V_{P^{(r+1)}}$). Thus u_α is a common root of $q^{(r, P^{(r+1)})}(\alpha, T)$ and $\rho^{(r, P^{(r+1)})}(\alpha)^N f_{r+1}(\alpha, T)$. This implies $g(\alpha) = 0$. Therefore any root of $m_{Y_{n-r}}$ where $\rho^{(r, P^{(r+1)})}$ does not vanish is a root of the polynomial g .

Finally recall that we have shown that the coordinate function of $\mathbf{Q}[V_{P^{(r+1)}}]$ induced by the polynomial $\rho^{(r, P^{(r+1)})}(Y_{n-r})$ is a unit of $\mathbf{Q}[V_{P^{(r+1)}}]$. Thus the polynomial $\rho^{(r, P^{(r+1)})}(Y_{n-r})$ vanishes nowhere on the lifting fiber $V_{P^{(r+1)}}$. In particular there is no root of $m_{Y_{n-r}}$ where $\rho^{(r, P^{(r+1)})}$ vanishes. This implies that $m_{Y_{n-r}}$ and $\rho^{(r, P^{(r+1)})}$ are coprime and therefore g vanishes on *all* roots of $m_{Y_{n-r}}$. \square

For the statement of the next Lemma we need the following considerations: we have seen before that the “rational function $\mathbf{Q}(Y_{n-r})$ -algebras” $\mathbf{Q}(Y_{n-r}) \otimes \mathbf{Q}[Y_{n-r}]$, $\mathbf{Q}[W_{P^{(r+1)}}]$ and $\mathbf{Q}(Y_{n-r})[T]/(q^{(r, P^{(r+1)})}(Y_{n-r}, T))$ are isomorphic. The canonical isomorphism of these algebras maps $1 \otimes \varphi_{r+1}$ to $\hat{\varphi}_{r+1}$, where φ_{r+1} is the coordinate function of $W_{P^{(r+1)}}$ induced by the polynomial $F_{r+1}(Y_1, \dots, Y_n)$ and $\hat{\varphi}_{r+1}$ is the residue class of f_{r+1} in $\mathbf{Q}(Y_{n-r})[T]/(q^{(r, P^{(r+1)})}(Y_{n-r}, T))$.

The homotheties $\eta_{F_{r+1}}$ and $\eta_{f_{r+1}}$ defined by multiplication by φ_{r+1} and $\hat{\varphi}_{r+1}$ in the $\mathbf{Q}[Y_{n-r}]$ -algebra $\mathbf{Q}[W_{P^{(r+1)}}]$ and the $\mathbf{Q}(Y_{n-r})$ -algebra $\mathbf{Q}(Y_{n-r})[T]/(q^{(r, P^{(r+1)})}(Y_{n-r}, T))$ have the same characteristic and minimal polynomials. We denote the minimal polynomial of $\eta_{f_{r+1}}$ by $m_{f_{r+1}}$. The coefficients of the minimal polynomial $m_{f_{r+1}}$ belong to $\mathbf{Q}[Y_{n-r}]$ and the *total* degree of $m_{f_{r+1}}$ is bounded by $d\delta_r$ (see [55]). Let us denote by $a(Y_{n-r}) \in \mathbf{Q}[Y_{n-r}]$ the square-free representation of the roots of the constant term of $m_{f_{r+1}}$ (with respect to the main variable) and observe that $\deg a(Y_{n-r}) \leq d\delta_r$ holds. Then we have the following result:

Lemma 8 *With the notations and assumptions introduced before, we have the identity:*

$$m_{Y_{n-r}} = \frac{a(Y_{n-r})}{\gcd(\rho^{(r, P^{(r+1)})}(Y_{n-r}), a(Y_{n-r}))}.$$

Proof Let $g(Y_{n-r}) \in \mathbf{Q}[Y_{n-r}]$ be the polynomial of Lemma 7 and let $\tilde{a}(Y_{n-r}) \in \mathbf{Q}[Y_{n-r}]$ be the square-free representation of the roots of $g(Y_{n-r})$. By Lemma 7, the roots of g and of $m_{Y_{n-r}}$ which are not roots of $\rho^{(r, P^{(r+1)})}$ coincide. Thus the polynomials \tilde{a} and $m_{Y_{n-r}}$ vanish on the same non-roots of $\rho^{(r, P^{(r+1)})}$.

On the other hand the polynomials $m_{Y_{n-r}}$ and $\rho^{(r,P^{(r+1)})}$ are coprime. Since $m_{Y_{n-r}}$ is square–free we have therefore the identity

$$m_{Y_{n-r}}(Y_{n-r}) = \frac{\tilde{a}(Y_{n-r})}{\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), \tilde{a}(Y_{n-r}))}.$$

From the definition of the polynomial g we deduce that in $\mathbf{Q}(Y_{n-r})[T]$ the identity

$$g(Y_{n-r}) = \rho^{(r,P^{(r+1)})}(Y_{n-r})^{N\delta_r} \text{Res}_T\left(q^{(r,P^{(r+1)})}(Y_{n-r}, T), f_{r+1}(Y_{n-r}, T)\right)$$

holds.

Applying in the same way as in [31] Stickelberger’s Theorem, we see that $\frac{g(Y_{n-r})}{\rho^{(r,P^{(r+1)})}(Y_{n-r})^{N\delta_r}} = \text{Res}_T\left(q^{(r,P^{(r+1)})}(Y_{n-r}, T), f_{r+1}(Y_{n-r}, T)\right)$ is in fact the constant term of the characteristic polynomial of the homothesy $\eta_{f_{r+1}}$. Since the homothesies $\eta_{f_{r+1}}$ and $\eta_{\varphi_{r+1}}$ have the same characteristic polynomial we deduce that $\frac{g(Y_{n-r})}{\rho^{(r,P^{(r+1)})}(Y_{n-r})^{N\delta_r}}$ is a polynomial of $\mathbf{Q}[Y_{n-r}]$. Since the constant terms of the characteristic and of the minimal polynomial of $\eta_{f_{r+1}}$ (and of $\eta_{\varphi_{r+1}}$) have the same roots, we conclude that the polynomial $a(Y_{n-r}) \in \mathbf{Q}[Y_{n-r}]$ is the square–free representation of the roots of both of them. Taking into account that the polynomial $\frac{g(Y_{n-r})}{\rho^{(r,P^{(r+1)})}(Y_{n-r})^{N\delta_r}}$ is the constant term of the characteristic polynomial of the homothesy $\eta_{f_{r+1}}$ we deduce that the identity

$$\begin{aligned} \frac{a(Y_{n-r})}{\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), a(Y_{n-r}))} &= \frac{\tilde{a}(Y_{n-r})}{\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), \tilde{a}(Y_{n-r}))} \\ &= m_{Y_{n-r}}(Y_{n-r}) \end{aligned}$$

holds. This implies the statement of the lemma. \square

We now exhibit an efficient procedure for the computation of the minimal polynomial $m_{Y_{n-r}}$.

Proposition 1 *Let notations and assumptions be as before. Suppose that there is given a geometric solution of the lifting fiber $V_{P^{(r)}}$. Then it is possible to compute in space $O(Sr\delta_r^2)$ and time $O((Tdr^2 + r^5)d\delta_r^3 \log^3 \delta_r \log^3 \log^2 \delta_r)$ the coefficients of the minimal polynomial $m_{Y_{n-r}}$ of the coordinate function of $V_{P^{(r+1)}}$ induced by the variable Y_{n-r} .*

Proof First of all, we observe that the discriminant $\rho^{(r,P^{(r+1)})}(Y_{n-r})$ of the polynomial $q^{(r,P^{(r+1)})}(Y_{n-r}, T) \in \mathbf{Q}[Y_{n-r}][T]$ with respect to the variable T is a nonzero polynomial of $\mathbf{Q}[Y_{n-r}]$ of degree at most δ_r^2 . Let κ be a fixed natural number. Applying the Zippel–Schwartz test in the same way we did in the proof of Theorem 3, we may choose an element η of the set $\{1, \dots, 2\kappa\delta^2\}$ such that with probability of success at least $1 - \frac{1}{2\kappa}$, the condition $\rho^{(r,P^{(r+1)})}(\eta) \neq 0$ is satisfied.

It is clear that η is a lifting point of the curve $W_{P^{(r+1)}}$ and that the zero-dimensional variety $V_{Y_{n-r}, \eta}^{(r+1)} := W_{P^{(r+1)}} \cap \{Y_{n-r} = \eta\}$ is the lifting fiber of the lifting point η .

We have seen before that the coordinate function $u^{(r)}$ of the curve $W_{P^{(r+1)}}$, induced by the linear form $U^{(r)}$, is a primitive element of the integral \mathbf{Q} -algebra extension $\mathbf{Q}[Y_{n-r}] \hookrightarrow \mathbf{Q}[W_{P^{(r+1)}}]$. Since $q^{(r, P^{(r+1)})}(Y_{n-r}, T)$ is the minimal integral dependence relation satisfied by $u^{(r)}$ over $\mathbf{Q}[Y_{n-r}]$ and since $\rho^{(r, P^{(r+1)})}(Y_{n-r})$ is the discriminant of $q^{(r, P^{(r+1)})}$ we deduce from $\rho^{(r, P^{(r+1)})}(\eta) \neq 0$ that the coordinate function of the zero-dimensional variety $V_{Y_{n-r}, \eta}^{(r+1)}$, induced by the linear form $U^{(r)}$, is also a primitive element of $\mathbf{Q}[V_{Y_{n-r}, \eta}^{(r+1)}]$.

Observe that $V_{Y_{n-r}, \eta}^{(r+1)} = W_{P^{(r+1)}} \cap \{Y_{n-r} = \eta\}$ is isomorphic to the zero-dimensional subvariety $\{F_1(P^{(r+1)}, \eta, Y_{n-r+1}, \dots, Y_n) = 0, \dots, F_r(P^{(r+1)}, \eta, Y_{n-r+1}, \dots, Y_n) = 0\}$ of \mathbf{C}^{n-r} . Observe also that $q^{(r, P^{(r+1)})}(\eta, Y_{n-r})$ is the minimal polynomial equation of $V_{Y_{n-r}, \eta}^{(r+1)}$ induced by the linear form $U^{(r)}$. Applying Theorem 5 to the linear forms $U^{(r)}, Y_{n-r+1}, \dots, Y_n, Z_1^{(r)}, \dots, Z_r^{(r)}$ introduced in Subsections 4.3 and 4.4 we compute, as in the proof of Theorem 6, the coefficients of the minimal integral dependence relations $q^{(r)}(T), q_1^{(r)}(T), \dots, q_r^{(r)}(T), \tilde{q}_1^{(r)}(T), \dots, \tilde{q}_r^{(r)}(T)$ of the coordinate functions of V_r induced by these linear forms. These polynomials belong to $\mathbf{Q}[Y_1, \dots, Y_{n-r}][T]$. We specialize now in all these polynomials the variables Y_1, \dots, Y_{n-r} into the values $p_1, \dots, p_{n-r-1}, \eta$. In this way we obtain the polynomial

$$q^{(r)}(p_1, \dots, p_{n-r-1}, \eta, T) = q^{(r)}(P^{(r+1)}, \eta, T) = q^{(r, P^{(r+1)})}(\eta, T)$$

and certain polynomials

$$\begin{aligned} q_1^{(r, P^{(r+1)})}(T) &:= q_1^{(r)}(p_1, \dots, p_{n-r-1}, \eta, T) \\ &\vdots \\ q_r^{(r, P^{(r+1)})}(T) &:= q_r^{(r)}(p_1, \dots, p_{n-r-1}, \eta, T) \\ \tilde{q}_1^{(r, P^{(r+1)})}(T) &:= \tilde{q}_1^{(r)}(p_1, \dots, p_{n-r-1}, \eta, T) \\ &\vdots \\ \tilde{q}_r^{(r, P^{(r+1)})}(T) &:= \tilde{q}_r^{(r)}(p_r, \dots, p_{n-r-1}, \eta, T). \end{aligned}$$

All these polynomials belong to $\mathbf{Q}[T]$ and the polynomials $q_1^{(r, P^{(r+1)})}, \dots, q_r^{(r, P^{(r+1)})}$ and $\tilde{q}_1^{(r, P^{(r+1)})}, \dots, \tilde{q}_r^{(r, P^{(r+1)})}$ represent nontrivial equations satisfied by the coordinate functions of $V_{Y_{n-r}, \eta}^{(r+1)}$ induced by the linear forms Y_{n-r+1}, \dots, Y_n and $Z_1^{(r)}, \dots, Z_r^{(r)}$.

We have already shown that the coordinate function of $V_{Y_{n-r}, \eta}^{(r+1)}$ induced by the linear form $U^{(r)}$ is a primitive element of $\mathbf{Q}[V_{Y_{n-r}, \eta}^{(r+1)}]$ (thus $U^{(r)}$ separates the elements of $V_{Y_{n-r}, \eta}^{(r+1)}$) and that $q^{(r, P^{(r+1)})}(T)$ is the minimal polynomial of this coordinate function.

As in the proof of Theorem 6 we apply now Lemma 6 to these data, obtaining thus a geometric solution of the zero–dimensional variety $V_{Y_{n-r},\eta}^{(r+1)}$. All this can be done in space $O(Sr\delta_r^2)$ and time $O((Tr^2 + r^5)\delta_r^3 \log^2 \delta_r \log^2 \log \delta_r)$.

Since we have at our disposal a geometric solution of the zero–dimensional variety $V_{Y_{n-r},\eta}^{(r+1)}$, we are now able to apply Theorem 5 to the lifting fiber $V_{Y_{n-r},\eta}^{(r+1)}$ of the curve $W_{P^{(r+1)}}$ and to the polynomial F_{r+1} . In this way we compute the coefficients of the minimal integral dependence relation satisfied over $\mathbf{Q}[Y_{n-r}]$ by the coordinate function φ_{r+1} of $W_{P^{(r+1)}}$, which is induced by the polynomial F_{r+1} . This can be done in additional space $O(Sd\delta_r^2)$ and in additional time $O((Tdr + r^4)d\delta_r^3 \log^3 \delta_r \log^2 \log \delta_r)$.

The minimal integral dependence relation over $\mathbf{Q}[Y_{n-r}]$ satisfied by φ_{r+1} is also the minimal polynomial over the field $\mathbf{Q}(Y_{n-r})$ of the homothesy $\eta_{\varphi_{r+1}}$ of the rational function $f_{r+1} \in \mathbf{Q}(Y_{n-r})[T]/(q^{(r,P^{(r+1)})}(Y_{n-r}, T))$ and of the homothesy $\eta_{f_{r+1}}$. We denote this minimal polynomial by $m_{f_{r+1}}(T)$. Observe that the polynomial $m_{f_{r+1}}$ belongs to $\mathbf{Q}[Y_{n-r}, T]$ and from Remark 1 we deduce that our algorithm computes in fact the *dense* representation of $m_{f_{r+1}}$. Moreover, we have $\deg m_{f_{r+1}} \leq d\delta_r$ (see [55]).

Therefore, the constant term $b(Y_{n-r})$ of the minimal polynomial $m_{f_{r+1}}$ is a polynomial of $\mathbf{Q}[Y_{n-r}]$ of degree at most $d\delta_r$ given in dense representation. Applying e.g. the main procedure of [39], we obtain the square–free representation $a(Y_{n-r})$ of the roots of the polynomial $b(Y_{n-r})$ in additional space $O(d\delta_r)$ and time $O(d\delta_r \log(d\delta_r) \log \log(d\delta_r))$.

Now we compute from the already determined coefficients of the polynomial $q^{(r,P^{(r+1)})}(T) \in \mathbf{Q}[Y_{n-r}][T]$ its discriminant $\rho^{(r,P^{(r+1)})}$ with respect to the variable T . This can be done by [59] in additional space $O(d\delta_r)$ and time $O((d\delta_r)^2 \log \delta_r \log \log \delta_r)$. By means of the procedure introduced at the beginning of the proof of Lemma 2 we compute the dense representation of the remainder $c(Y_{n-r})$ of the division of $\rho^{(r,P^{(r+1)})}(Y_{n-r})$ by the polynomial $a(Y_{n-r})$, which itself is given in its dense representation. This can be done using additional space $O(d\delta_r^2)$ and time $O(d\delta_r^3 \log^2 \delta_r \log^2 \log \delta_r)$.

Using the identity $\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), a(Y_{n-r})) = \gcd(c(Y_{n-r}), a(Y_{n-r}))$ we compute the dense representation of the polynomial $\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), a(Y_{n-r}))$ in additional space $O(d\delta_r)$ and time $O(d\delta_r \log^2 \delta_r \log \log \delta_r)$ (see [39]). Finally we divide the polynomial $a(Y_{n-r})$ by $\gcd(\rho^{(r,P^{(r+1)})}(Y_{n-r}), a(Y_{n-r}))$ obtaining in this way the dense representation of the polynomial $m_{Y_{n-r}}$ (see Lemma 8). Using the algorithm of Sieveking–Kung, this can be done in additional space $O(d\delta_r)$ and time $O(d\delta_r \log^2 \delta_r \log \log \delta_r)$. Adding up the complexities of every step in this algorithm we obtain the complexity estimate of Proposition 1. \square

5 The main algorithm

In this section we collect the algorithmic tools developed before and describe the main algorithm of this paper, concluding thus the proof of Theorem 1.

In the introduction of this paper we announced this algorithm as a recursive procedure which produces in $n-1$ steps a geometric solution of the zero-dimensional variety V_n defined by the given polynomials $F_1, \dots, F_n \in \mathbb{Q}[X_1, \dots, X_n]$.

From now on we shall use freely all notations and assumptions introduced in the previous sections, and in particular those of Subsections 4.3 and 4.4.

Recall that we have already chosen linear forms $Y_1, \dots, Y_n \in \mathbb{Z}[X_1, \dots, X_n]$ and a point $P = (p_1, \dots, p_n) \in \mathbb{Z}^n$ such that for $1 \leq r \leq n-1$ the conditions (i), (ii) and (iii) of Theorem 3 are satisfied. In particular, the linear forms Y_1, \dots, Y_n represent a simultaneous Noether normalization of the varieties V_1, \dots, V_n and for $1 \leq r \leq n-1$ the finite surjective morphism $\pi_r : V_r \rightarrow \mathbb{C}^{n-r}$ induced by the linear forms Y_1, \dots, Y_{n-r} is unramified in the point $P^{(r)} = (p_1, \dots, p_{n-r})$. In other words, $P^{(r)}$ is a lifting point of the variety V_r with lifting fiber $V_{P^{(r)}} := \pi_r^{-1}(P^{(r)})$.

For the presentation of our main algorithm we shall focus our attention on its recursive character. Let us fix $1 \leq r \leq n-1$. In the next subsection we are going to describe the r -th step of our main algorithm. This step starts with a (previously computed) geometric solution of the lifting fiber $V_{P^{(r)}}$ and produces a geometric solution of the next lifting fiber $V_{P^{(r+1)}}$.

5.1 The recursion

As before, let $1 \leq r \leq n-1$ be fixed. We suppose that there is given a geometric solution of the lifting fiber $V_{P^{(r)}}$. This geometric solution is represented by the (rational) coefficients of the univariate polynomials occurring in it. Our goal is to compute the coefficients of a geometric solution of the lifting fiber $V_{P^{(r+1)}}$.

For this purpose we consider again the curve

$$W_{P^{(r+1)}} = V_r \cap \{Y_1 = p_1, \dots, Y_{n-r-1} = p_{n-r-1}\}.$$

Recall that lifting any projection from a zero-dimensional variety to this curve produces a bivariate polynomial in *dense* representation (see Remark 2).

We sketch now how we compute from a given geometric solution of $V_{P^{(r)}}$ a geometric solution of the lifting fiber $V_{P^{(r+1)}}$:

applying Proposition 1 we compute first the coefficients of the minimal polynomial $m_{Y_{n-r}}$ of the coordinate function of $W_{P^{(r+1)}}$ induced by the linear form Y_{n-r} . At this point we introduce two linear forms $\ell_1 := \alpha_1 Y_{n-r} + U^{(r)}$ and $\ell_2 := \alpha_2 Y_{n-r} + U^{(r)}$, where α_1 and α_2 are suitably chosen nonzero integers. Modifying slightly the algorithm underlying Proposition 1 we compute the coefficients of the minimal polynomials m_{ℓ_1} and m_{ℓ_2} of the coordinate functions of $W_{P^{(r+1)}}$

induced by the linear forms ℓ_1 and ℓ_2 . Interpreting the linear forms Y_{n-r} and $U^{(r)}$ as indeterminates, we consider now the zero–dimensional variety

$$W := \{m_{\ell_1}(\alpha_1 Y_{n-r} + U^{(r)}) = 0, m_{\ell_2}(\alpha_2 Y_{n-r} + U^{(r)}) = 0, m_{Y_{n-r}}(Y_{n-r}) = 0\}$$

which is contained in the affine space \mathbb{C}^2 . The linear form $\ell_1 = \alpha_1 Y_{n-r} + U^{(r)}$ separates the points of the variety W . Using ℓ_1 as separating linear form, we apply now Lemma 6 to the variety W . In this way we obtain a suitable “parametrizing” polynomial $v_{n-r}^{(P^{(r+1)})}(T)$ such that $Y_{n-r} - v_{n-r}^{(P^{(r+1)})}(\alpha_1 Y_{n-r} + U^{(r)})$ vanishes on the whole variety W . This polynomial is now used for the computation of a suitable birational morphism which maps the zero–dimensional variety W to the lifting fiber $V_{P^{(r+1)}}$. From the coordinates of this morphism we obtain a geometric solution of $V_{P^{(r+1)}}$.

We are now going to describe the details of the procedure sketched just before.

Let us consider the linear form $Y_{n-r} + \alpha U^{(r)}$, where α is an integer which will be determined later. We claim that for a generic choice of the parameter α , the linear form $Y_{n-r} + \alpha U^{(r)}$ induces a finite morphism which maps the curve $W_{P^{(r+1)}}$ onto the affine space \mathbb{C}^1 .

In order to prove this claim, let us consider the minimal polynomial $q^{(r, P^{(r+1)})}(Y_{n-r}, T) \in \mathbb{Q}[Y_{n-r}, T]$ of the element $u^{(r)}$ of $\mathbb{Q}[W_{P^{(r+1)}}]$ (recall that $u^{(r)}$ is the coordinate function of $W_{P^{(r+1)}}$ induced by the linear form $U^{(r)}$). Let A be a new indeterminate and let $\mathcal{L} := Y_{n-r} + AT$. Specializing in the polynomial $q^{(r, P^{(r+1)})}(Y_{n-r}, T)$ the variable Y_{n-r} into the value $\mathcal{L} - AT$ we obtain a new polynomial $\hat{q}^{(r, P^{(r+1)})}(A, \mathcal{L}, T)$ in the indeterminates A , \mathcal{L} and T . This polynomial can be written as

$$\hat{q}^{(r, P^{(r+1)})}(A, \mathcal{L}, T) = c_{\delta_r, 0}(A)T_r^\delta + \cdots + c_{0, \delta_r}(A)\mathcal{L}_r^\delta,$$

with $c_{\delta_r, 0}(A), \dots, c_{0, \delta_r}(A)$ being elements of $\mathbb{Q}[A]$ (observe that this representation is possible since $\deg_T \hat{q}^{(r, P^{(r+1)})} = \deg \hat{q}^{(r, P^{(r+1)})} = \delta_r$ holds and since the expression $\mathcal{L} - AT$ is linear in \mathcal{L} and T). Specializing again in $\hat{q}^{(r, P^{(r+1)})}$ the parameter A into the value zero, we obtain $q^{(r, P^{(r+1)})}(\mathcal{L}, T)$ which is a monic polynomial in the variable T of degree δ_r . This implies $c_{\delta_r, 0}(0) = 1$ and therefore we have $c_{\delta_r, 0}(A) \neq 0$. Observe also that $\deg c_{\delta_r, 0} \leq \delta_r$ holds.

Therefore, specializing the indeterminate A into any value $\alpha \in \mathbb{Z}$ satisfying $c_{\delta_r, 0}(\alpha) \neq 0$, we obtain from $\hat{q}^{(r, P^{(r+1)})}(A, \mathcal{L}, T)$ a new polynomial $\hat{q}^{(r, P^{(r+1)})}(\alpha, \mathcal{L}, T) \in \mathbb{Q}[\mathcal{L}, T]$ of partial degree δ_r in the variable T . We consider now the coordinate function $\ell = y_{n-r} + \alpha u^{(r)}$ of the curve $W_{P^{(r+1)}}$ and the subalgebra $\mathbb{Q}[\ell]$ of $\mathbb{Q}[W_{P^{(r+1)}}]$.

From the identity $q^{(r, P^{(r+1)})}(y_{n-r}, u^{(r)}) = 0$ we deduce that in the \mathbb{Q} –algebra $\mathbb{Q}[W_{P^{(r+1)}}]$ the identity $\hat{q}^{(r, P^{(r+1)})}(\alpha, \ell, u^{(r)}) = 0$ holds. This means that in $\mathbb{Q}[W_{P^{(r+1)}}]$ the polynomial $\hat{q}^{(r, P^{(r+1)})}(\alpha, \ell, T)$ represents an integral dependence relation for the coordinate function $u^{(r)}$ over the subalgebra $\mathbb{Q}[\ell]$.

From the identities $\mathbf{Q}[W_{P^{(r+1)}}] = \mathbf{Q}[y_{n-r}, u^{(r)}]$ and $y_{n-r} = \ell - \alpha u^{(r)}$ we deduce now that $\mathbf{Q}[\ell] \hookrightarrow \mathbf{Q}[W_{P^{(r+1)}}]$ is an integral \mathbf{Q} -algebra extension and therefore the morphism $\ell : W_{P^{(r+1)}} \rightarrow \mathbf{C}^1$ is finite and surjective.

We claim now that for a generic choice of the parameter $\alpha \in \mathbb{Z}$ the linear form $Y_{n-r} + \alpha U^{(r)}$ induces a primitive element of the zero-dimensional variety $V_{P^{(r+1)}}$.

In order to show this claim, let us consider the linear form $\mathcal{L} := Y_{n-r} + AU^{(r)} \in \mathbf{Q}[A][X_1, \dots, X_n]$. The polynomial

$$P(A) = \prod_{\substack{x^{(1)}, x^{(2)} \in V_{P^{(r+1)}} \\ x^{(1)} \neq x^{(2)}}} (\hat{\mathcal{L}}(x^{(1)}) - \hat{\mathcal{L}}(x^{(2)}))$$

belongs to $\mathbf{Q}[A]$. By construction, the linear form Y_{n-r} separates the points of the lifting fiber $V_{P^{(r+1)}}$ (see Fact in the proof of Theorem 3). This implies $P(0) \neq 0$. One sees now immediately that P is a nonzero polynomial of $\mathbf{Q}[A]$ of degree at most δ_{r+1}^2 which expresses a genericity condition saying that for any $\alpha \in \mathbb{Z}$ with $P(\alpha) \neq 0$ the linear form $\ell = Y_{n-r} + \alpha U^{(r)}$ induces a primitive element of the lifting fiber $V_{P^{(r+1)}}$.

For an arbitrary integer α , let us write $\ell_\alpha = Y_{n-r} + \alpha U^{(r)}$ and m_{ℓ_α} for the minimal polynomial of the coordinate function of $V_{P^{(r+1)}}$ induced by the linear form ℓ_α . Furthermore let us write $\rho_{\ell_\alpha}^{(r, P^{(r+1)})}$ for the discriminant of the minimal polynomial $q_{\ell_\alpha}^{(r, P^{(r+1)})}(\ell_\alpha, T)$ of the coordinate function $u^{(r)} \in W_{P^{(r+1)}}$ over the \mathbf{Q} -algebra $\mathbf{Q}[\ell_\alpha]$. We finally claim that for a generic choice of the parameter $\alpha \in \mathbb{Z}$, the linear form $\ell := \ell_\alpha = Y_{n-r} + \alpha U^{(r)}$ satisfies the condition:

$$\gcd(\rho_\ell^{(r, P^{(r+1)})}, m_\ell) = 1. \quad (13)$$

In order to prove this claim, we consider again the linear form $\mathcal{L} = Y_{n-r} + AT$ and the polynomial $\hat{q}^{(r, P^{(r+1)})}(A, \mathcal{L}, T)$ introduced above. Let $\rho_{\mathcal{L}}(A, \mathcal{L})$ be the discriminant of the polynomial $\hat{q}^{(r, P^{(r+1)})}(A, \mathcal{L}, T)$ with respect to the variable T . Specializing again in $\hat{q}^{(r, P^{(r+1)})}(A, \mathcal{L}, T)$ the parameter A into the value zero, we obtain the polynomial $q^{(r, P^{(r+1)})}(\mathcal{L}, T)$ which is separable and monic. This implies $\rho_{\mathcal{L}}(0, \mathcal{L}) \neq 0$. Moreover the total degree of $\rho_{\mathcal{L}}$ is bounded by δ_r^2 . Let $m_{\mathcal{L}} \in \mathbf{Q}[A][T]$ be the minimal polynomial of the image of the linear form $Y_{n-r} + AU^{(r)}$ in the $\mathbf{Q}[A]$ -algebra $\mathbf{Q}[A] \otimes_{\mathbf{Q}} \mathbf{Q}[V_{P^{(r+1)}}]$. One immediately verifies $\deg_T m_{\mathcal{L}} \leq \delta_{r+1}$. Let $R(A) \in \mathbf{Q}[A]$ be the resultant of the polynomials $\rho_{\mathcal{L}}(A, \mathcal{L})$ and $m_{\mathcal{L}}(A, \mathcal{L})$ with respect to the indeterminate \mathcal{L} . From Lemma 7 we deduce $R(0) \neq 0$. Therefore we have $R(A) \neq 0$. Moreover, the estimates $\deg_{\mathcal{L}} \rho_{\mathcal{L}} \leq \delta_r^2$ and $\deg_{\mathcal{L}} m_{\mathcal{L}}(A, \mathcal{L}) \leq \delta_{r+1}$ imply $\deg R \leq \delta_r^2 \delta_{r+1}$. Therefore for any integer α satisfying $R(\alpha) \neq 0$ we see that the linear form $\ell := \ell_\alpha = Y_{n-r} + \alpha U^{(r)}$ satisfies condition (13).

We are now going to describe how we can find effectively an integer $\alpha \in \mathbb{Z}$ which satisfies the genericity conditions of the three claims just proved. For this purpose we consider the polynomial $H \in \mathbf{Q}[A]$ defined by the formula

$H(A) := c_{\delta_r,0}(A)P(A)R(A)$. One sees immediately that $H \neq 0$ and $\deg H \leq 2\delta^3$ hold. Let κ be a fixed natural number as in Theorem 3. Applying the Zippel–Schwartz test we choose now randomly two distinct elements α_1 and α_2 of the set $\{1, \dots, 4\kappa\delta^3\}$ satisfying the conditions $H(\alpha_1) \neq 0$ and $H(\alpha_2) \neq 0$. The probability of success is at least $(1 - \frac{1}{2\kappa})^2$. We suppose from now on that we have already found such integers α_1 and α_2 . Let $\ell_1 := Y_{n-r} + \alpha_1 U^{(r)}$ and $\ell_2 := Y_{n-r} + \alpha_2 U^{(r)}$. Observe that the linear forms ℓ_1 and ℓ_2 have the properties formulated in the three claims just before.

Our next aim is to compute the coefficients of the minimal polynomials $m_{Y_{n-r}}$, m_{ℓ_1} and m_{ℓ_2} of the coordinate functions of the lifting fiber $V_{P^{(r+1)}}$ induced by the linear forms Y_{n-r} , ℓ_1 and ℓ_2 . First we compute the coefficients of the minimal polynomial $m_{Y_{n-r}}$ applying directly the procedure underlying Proposition 1.

For the computation of the coefficients of the minimal polynomials m_{ℓ_1} and m_{ℓ_2} we modify this procedure in the way we are going to explain now. Recall first the following notations:

by $q^{(r,P^{(r+1)})} \in \mathbf{Q}[Y_{n-r}][T]$ we denote the minimal polynomial of the coordinate function $u^{(r)} \in \mathbf{Q}[W_{P^{(r+1)}}]$ over the \mathbf{Q} –algebra $\mathbf{Q}[Y_{n-r}]$ and by $\rho^{(r,P^{(r+1)})} \in \mathbf{Q}[Y_{n-r}]$ we denote the discriminant of $q^{(r,P^{(r+1)})}(Y_{n-r}, T)$ with respect to the variable T . Moreover φ_{r+1} denotes the coordinate function of the curve $W_{P^{(r+1)}}$ induced by the polynomial F_{r+1} . Observe that to the coordinate function $\varphi_{r+1} \in \mathbf{Q}[W_{P^{(r+1)}}]$ there corresponds an element f_{r+1} of the quotient algebra $\mathbf{Q}[Y_{n-r}][T]/(q^{(r,P^{(r+1)})}(Y_{n-r}, T))$ which has the same minimal polynomial over $\mathbf{Q}[Y_{n-r}]$ as the coordinate function φ_{r+1} over $\mathbf{Q}[W_{P^{(r+1)}}]$. This minimal polynomial belongs to $\mathbf{Q}[Y_{n-r}][T]$ and is denoted by $m_{f_{r+1}}$.

The procedure underlying Proposition 1 requires the computation of the dense representation of the minimal polynomials $m_{f_{r+1}}$ and $q^{(r,P^{(r+1)})}$ which belong to $\mathbf{Q}[Y_{n-r}][T]$.

Let us fix $1 \leq i \leq 2$. Observe that the minimal polynomial $m_{f_{r+1}}^{(i)} \in \mathbf{Q}[\ell_i][T]$ of the coordinate function φ_{r+1} with respect to the integral \mathbf{Q} –algebra extension $\mathbf{Q}[\ell_i] \hookrightarrow \mathbf{Q}[W_{P^{(r+1)}}]$ can be obtained from $m_{f_{r+1}}$ in the following simple way :

$$m_{f_{r+1}}^{(i)}(\ell_i, T) = m_{f_{r+1}}(\ell_i - \alpha_i T, T).$$

This identity implies that the coefficients of the constant term $a^{(i)} \in \mathbf{Q}[\ell_i]$ (with respect to the variable T) of the minimal polynomial $m_{f_{r+1}}^{(i)}$ can be determined from the (already computed) dense representation of the polynomial $m_{f_{r+1}}$. This can be done in additional time $O(\delta_{r+1}^2)$ using constant additional space.

In the same way, the minimal polynomial $q_{\ell_i} := q_{\ell_i}^{(r,P^{(r+1)})} \in \mathbf{Q}[\ell_i, T]$ of the coordinate function $u^{(r)}$ with respect to the \mathbf{Q} –algebra extension $\mathbf{Q}[\ell_i] \hookrightarrow \mathbf{Q}[W_{P^{(r+1)}}]$ can be obtained by means of the identity :

$$q_{\ell_i}(\ell_i, T) = q^{(r,P^{(r+1)})}(\ell_i - \alpha_i T, T).$$

Let $\rho_i := \rho_{\ell_i}^{(r, P^{(r+1)})} \in \mathbf{Q}[\ell_i]$ be the discriminant of the polynomial $q_{\ell_i} \in \mathbf{Q}[\ell_i][T]$ with respect to the variable T . From the generic choice of the integer α_i and the third (and last) claim proved at the beginning of this subsection we deduce in the same manner as in Lemma 8 the identity:

$$m_{\ell_i} = \frac{a^{(i)}}{\gcd(a^{(i)}, \rho_i)}.$$

Using the same argumentation as in the proof of Proposition 1 we deduce from this identity that the dense representation of the polynomials m_{ℓ_1} and m_{ℓ_2} can be computed in additional space $O(Sr\delta_r^2)$ and time $O((\mathcal{T}dr + r^5)d\delta_r^3 \log^3 \delta_r \log^2 \log \delta_r)$.

Consider now the zero-dimensional variety

$$W := \{(\lambda, \eta) \in \mathbf{C}^2; m_{\ell_2}(\lambda) = 0, m_{Y_{n-r}}(\eta) = 0, m_{\ell_1}(\lambda + (\alpha_1 - \alpha_2)\eta) = 0\}$$

which is contained in the affine plane \mathbf{C}^2 .

Taking into account the identity $\ell_1 = \ell_2 + (\alpha_1 - \alpha_2)Y_{n-r}$ we may consider ℓ_1 as a linear form in the indeterminates ℓ_2 and Y_{n-r} . Thus for any point $(\lambda, \eta) \in \mathbf{C}^2$ let $\ell_1(\lambda, \eta) := \lambda + (\alpha_1 - \alpha_2)\eta$. In this sense, the linear form ℓ_1 separates the points of the variety W .

Applying now Lemma 6 to the zero-dimensional variety W and the linear form ℓ_1 we compute from the dense representation of the polynomials $m_{Y_{n-r}}$, m_{ℓ_2} and m_{ℓ_1} the coefficients of a polynomial $v_{n-r}^{(P^{(r+1)})} \in \mathbf{Q}[T]$ of degree at most $\delta_{r+1} - 1$, which satisfies for any point $(\lambda, \eta) \in W$ the condition

$$\eta = v_{n-r}^{(P^{(r+1)})}(\lambda + (\alpha_1 - \alpha_2)\eta) = v_{n-r}^{(P^{(r+1)})}(\ell_1(\lambda, \eta)).$$

From [42, Proposition 29] we conclude now that the polynomial $Y_{n-r} - v_{n-r}^{(P^{(r+1)})}(\ell_1)$ vanishes on the whole lifting fiber $V_{P^{(r+1)}}$. The computation of the coefficients of the polynomial $v_{n-r}^{(P^{(r+1)})}$ can be done in additional space $O(\delta_{r+1}^2)$ and time $O(\delta_{r+1}^3 \log^2 \delta_{r+1} \log^2 \log \delta_{r+1})$.

Taking into account the estimation $\delta_{r+1} \leq d\delta_r$ and summing up all complexities we obtain the following result:

Lemma 9 *Let notations and assumptions be as before. In particular suppose that there is given a geometric solution of the lifting fiber $V_{P^{(r)}}$ and a linear form $\ell_1 = Y_{n-r} + \alpha_1 U^{(r)}$, where α_1 is a sufficiently generic integer. Then it is possible to compute in space $O(Sr\delta_r^2)$ and time $O((\mathcal{T}dr + r^5)d\delta_r^3 \log^3 \delta_r \log^2 \log \delta_r)$ the following items:*

- the coefficients of the minimal polynomial m_{ℓ_1} of the coordinate function of the lifting fiber $V_{P^{(r+1)}}$ induced by the linear form ℓ_1 ,
- the coefficients of a univariate polynomial $v_{n-r}^{(P^{(r+1)})} \in \mathbf{Q}[T]$ of degree at most $\delta_{r+1} - 1$ such that $Y_{n-r} - v_{n-r}^{(P^{(r+1)})}(\ell_1)$ vanishes on the whole lifting fiber $V_{P^{(r+1)}}$.

It remains now to compute the coefficients of certain suitable polynomials $v_{n-r+1}^{(P^{(r+1)})}, \dots, v_n^{(P^{(r+1)})}$ of $\mathbf{Q}[T]$ having degree at most $\delta_{r+1} - 1$, which, together with the polynomial $v_{n-r}^{(P^{(r+1)})}$, parametrize the lifting fiber $V_{P^{(r+1)}}$ in terms of the linear form ℓ_1 and its minimal polynomial m_{ℓ_1} . This is the content of the next result.

Theorem 7 *Let notations and assumptions be in Lemma 9. Then it is possible to compute in space $O(Sdr\delta^2)$ and time $O((\mathcal{T}dr^2 + r^5)\delta^3 \log^2 \delta \log^2 \log \delta)$ the coefficients of certain (univariate) polynomials representing a geometric solution of the lifting fiber $V_{P^{(r+1)}}$.*

Proof As in Theorem 3, let us fix a natural number κ and let us fix an integer η such that η is a lifting point of the curve $W_{P^{(r+1)}}$. The corresponding lifting fiber is $V_{Y_{n-r}, \eta}^{(r+1)} := W_{P^{(r+1)}} \cap \{Y_{n-r} = \eta\}$. We have seen at the beginning of the proof of Proposition 1 that such an integer η can be chosen randomly in the set $\{1, \dots, 2\kappa\delta^2\}$ with probability of success at least $1 - \frac{1}{2\kappa}$. Applying now Proposition 1 we compute the coefficients of the minimal polynomial $m_{Y_{n-r}}$ of the coordinate function of $V_{P^{(r+1)}}$ induced by the linear form Y_{n-r} . This can be done by means of a computation tree using space $O(Srd\delta_r^2)$ and time $O((\mathcal{T}dr^2 + r^5)\delta_r^3 \log^2 \delta_r \log^2 \log \delta_r)$.

Then we choose randomly two distinct elements α_1 and α_2 of the set $\{1, \dots, 2\kappa\delta^3\}$. Let $\ell_1 := Y_{n-r} + \alpha_1 U^{(r)}$ and $\ell_2 := Y_{n-r} + \alpha_2 U^{(r)}$. With probability at least $(1 - \frac{1}{\kappa})^2$ the linear forms ℓ_1 and ℓ_2 have the properties formulated in the three claims shown at the beginning of this subsection. Then we compute as in the proof of Lemma 9 the coefficients of the minimal polynomials m_{ℓ_1} and m_{ℓ_2} of the coordinate functions of the lifting fiber $V_{P^{(r+1)}}$ induced by the linear forms ℓ_1 and ℓ_2 in. Moreover we compute for $1 \leq i \leq 2$ the dense representation of $q_{\ell_i} \in \mathbf{Q}[\ell_i][T]$, which is the minimal polynomial of the coordinate function $u^{(r)}$ of $W_{P^{(r+1)}}$ over the \mathbf{Q} -algebra $\mathbf{Q}[\ell_i]$.

Now we use the already determined dense representation of the minimal polynomials $m_{Y_{n-r}}, m_{\ell_1}$ and m_{ℓ_2} in order to compute the coefficients of a polynomial $v_{n-r}^{(P^{(r+1)})} \in \mathbf{Q}[T]$ having degree at most $\delta_{r+1} - 1$, such that $Y_{n-r} - v_{n-r}^{(P^{(r+1)})}(\ell_1)$ vanishes on the whole lifting fiber $V_{P^{(r+1)}}$. This can be done by means of a computation tree using space $O(Srd\delta_r^2)$ and time $O((\mathcal{T}dr + r^5)\delta_r^3 \log^2 \delta_r \log^2 \log \delta_r)$.

For $1 \leq k \leq r$ let $\tilde{Z}_k^{(r)}$ be the linear form $\tilde{Z}_k^{(r)} := \frac{1}{\alpha_1} \ell_1 - \lambda_{n-r+k}^{(r)} Y_{n-r+k}$ and let us consider the integral \mathbf{Q} -algebra extension $\mathbf{Q}[\ell_1] \hookrightarrow \mathbf{Q}[W_{P^{(r+1)}}]$. Our aim is to compute for $1 \leq k \leq r$ the minimal polynomials $\tilde{f}_k^{(r+1)}$ and $\tilde{g}_k^{(r+1)}$ over $\mathbf{Q}[\ell_1]$ of the coordinate functions of $W_{P^{(r+1)}}$ induced by the linear forms Y_{n-r+k} and $\tilde{Z}_k^{(r)}$. For this purpose we compute first a geometric solution of an appropriate lifting fiber of the curve $W_{P^{(r+1)}}$ and determine then the polynomials $\tilde{f}_k^{(r+1)}$ and $\tilde{g}_k^{(r+1)}$ by a suitable lifting process.

We start choosing randomly an element ξ in the set $\{1, \dots, \kappa\delta^2\}$. As at the beginning of the proof of Proposition 1 we conclude that with probability at least $1 - \frac{1}{\kappa}$ the finite morphism $W_{P^{(r+1)}} \rightarrow \mathbf{C}^1$ defined by the linear form ℓ_1 is unramified

in the point ξ . Hence ξ is a lifting point of the curve $W_{P^{(r+1)}}$ with lifting fiber $V_{\ell_1, \xi}^{(r+1)} := W_{P^{(r+1)}} \cap \{\ell_1 = \xi\}$.

Now we proceed to compute the coefficients of certain suitable polynomials representing a geometric solution of the zero-dimensional variety $V_{\ell_1, \xi}^{(r+1)}$. Observe that the coordinate function of $V_{\ell_1, \xi}^{(r+1)}$ induced by the linear form $U^{(r)}$ is a primitive element of $\mathbf{Q}[V_{\ell_1, \xi}^{(r+1)}]$ (compare with the argumentation at the beginning of the proof of Proposition 1).

Since $V_{\ell_1, \xi}^{(r+1)}$ is the fiber of the lifting point ξ of the curve $W_{P^{(r+1)}}$, the minimal polynomial of the coordinate function of $V_{\ell_1, \xi}^{(r+1)}$ induced by the linear form $U^{(r)}$ can be obtained just by specializing in the polynomial $q_{\ell_1} \in \mathbf{Q}[\ell_1][T]$ the variable ℓ_1 into the value ξ .

From the already computed dense representation of the polynomial q_{ℓ_1} we obtain therefore the minimal polynomial of the primitive element of $\mathbf{Q}[V_{\ell_1, \xi}^{(r+1)}]$ induced by the linear form $U^{(r)}$.

At the beginning of Subsection 4.3 we considered for each $1 \leq k \leq r$ the linear forms Y_{n-r+k} and $Z_k^{(r)} := U^{(r)} - \lambda_{n-r+k}^{(r)} Y_{n-r+k}$. In the same way as in the proof of Proposition 1 we compute first the minimal integral dependence relations $q_1^{(r)}(T), \dots, q_r^{(r)}(T)$ and $\tilde{q}_1^{(r)}, \dots, \tilde{q}_r^{(r)}(T)$ over $\mathbf{Q}[Y_1, \dots, Y_{n-r}]$ of the coordinate functions of V_r induced by the linear forms Y_{n-r+1}, \dots, Y_n and $Z_1^{(r)}, \dots, Z_r^{(r)}$. Then we specialize in these integral dependence relations the variables Y_1, \dots, Y_{n-r-1} into the values p_1, \dots, p_{n-r-1} and the variable Y_{n-r} into the value $\xi - \alpha_1 U^{(r)}$. In this manner we obtain for any $1 \leq k \leq r$ two polynomials $q_k^{(r, \xi)}(U^{(r)}, T)$ and $\tilde{q}_k^{(r, \xi)}(U^{(r)}, T)$ which belong to $\mathbf{Q}[U^{(r)}][T]$ and which have the property that $q_k^{(r, \xi)}(U^{(r)}, Y_{n-r+k})$ and $\tilde{q}_k^{(r, \xi)}(U^{(r)}, Z_k^{(r)})$ vanish on the whole zero-dimensional variety $V_{\ell_1, \xi}^{(r+1)}$. We apply now Lemma 6 (in a slightly modified form) to the zero-dimensional variety defined in the affine plane \mathbf{C}^2 by the polynomials $q_k^{(r, \xi)}(U^{(r)}, Y_{n-r+k}), \tilde{q}_k^{(r, \xi)}(U^{(r)}, Z_k^{(r)})$ and $q_{\ell_1}(\xi, U^{(r)})$ and to the (separating) linear form $U^{(r)}$. As output of the algorithm underlying Lemma 6 we obtain the coefficients of a certain univariate polynomial $\tilde{v}_{n-r+k}^{(r, \xi)} \in \mathbf{Q}[T]$ having degree at most $\delta_r - 1$, such that $Y_{n-r+k} - \tilde{v}_{n-r+k}^{(r, \xi)}(U^{(r)})$ vanishes on the whole variety $V_{\ell_1, \xi}^{(r+1)}$.

In the same way as in the proof of Proposition 1 we conclude that the coefficients of the (univariate) polynomials $q_{\ell_1}(\xi, T)$ and $\tilde{v}_{n-r+1}^{(r, \xi)}(T), \dots, \tilde{v}_n^{(r, \xi)}(T)$ can be computed in space $O(Sr d \delta_r^2)$ and time $O((\mathcal{T} d r^2 + r^5) \delta_r^3 \log^2 \delta_r \log^2 \log \delta_r)$. These polynomials represent a geometric solution of the zero-dimensional variety $V_{\ell_1, \xi}^{(r+1)}$.

Next we apply Theorem 6 in order to lift for each $1 \leq k \leq r$ the projections of the linear forms Y_{n-r+k} and $\tilde{Z}_k^{(r)} = \frac{1}{\alpha_1} \ell_1 - \lambda_{n-r+k}^{(r)} Y_{n-r+k}$ from the zero-dimensional variety $V_{\ell_1, \xi}^{(r+1)}$ to the curve $W_{P^{(r+1)}}$. This lifting procedure computes the dense representation of the polynomials $\tilde{f}_k^{(r+1)}$ and $\tilde{g}_k^{(r+1)}$ which

belong to $\mathbf{Q}[\ell_1, T]$ (see Remark 2). It can be performed in space $O(Srd\delta_r^2)$ and time $O((Tdr^2 + r^5)\delta_r^3 \log^2 \delta_r \log^2 \log \delta_r)$.

Let $1 \leq k \leq r$. We consider now the zero–dimensional subvariety of the affine plane \mathbf{C}^2 defined by the polynomials $\tilde{f}_k^{(r+1)}(\ell_1, Y_{n-r+k}), \tilde{g}_k^{(r+1)}(\ell_1, \tilde{Z}_k^{(r)}) = \tilde{g}_k^{(r+1)}(\frac{1}{\alpha_1}\ell_1 - \lambda_{n-r+k}^{(r)}Y_{n-r+k})$ and $m_{\ell_1}(\ell_1)$. Applying as before Lemma 6 in a slightly modified form to this zero–dimensional variety, we obtain the coefficients of a certain univariate polynomial $v_{n-r+k}^{(P(r+1))} \in \mathbf{Q}[T]$ having degree at most $\delta_{r+1} - 1$, such that $Y_{n-r+k} - v_{n-r+k}^{(P(r+1))}(\ell_1)$ vanishes on the whole lifting fiber $V_{P(r+1)}$. The coefficients of the polynomials $v_{n-r+1}^{(P(r+1))}, \dots, v_n^{(P(r+1))}$ can be computed in additional space $O(\delta_{r+1}^2)$ and time $O(\delta_{r+1}^3 \log^2 \delta_{r+1} \log^2 \log \delta_{r+1})$.

These polynomials and the already computed univariate polynomials $v_{n-r}^{(P(r))}$ and m_{ℓ_1} represent a geometric solution of the lifting fiber $V_{P(r+1)}$.

Adding up the complexities of each step in the argument we obtain finally the complexity estimate of Theorem 7. \square

The proof of Theorem 7 makes precise the computational model in which our main algorithm works, namely the model of computation trees, whose correctness depends on the random choice of certain not too big integers. The computation tree underlying the proof of Theorem 7 is reliable with probability at least $(1 - \frac{1}{\kappa})^4$.

Applying Theorem 7 recursively, we obtain now easily a proof of Theorem 1.

Acknowledgements The authors thank to M. Giusti, G. Lecerf, T. Krick, L.M. Pardo and M. Sombra for their helpful commentaries about this paper.

References

1. J. Abdeljaoued. *Algorithmes rapides pour le Calcul du Polynôme Caractéristique*. PhD thesis, Université de Franche Compte, Besançon, France, 1997.
2. M.E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.
3. B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties, real equation solving and data structures: The hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.
4. B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties and efficient real elimination. To appear in *Math. Zeitschrift*, 2000.
5. D. Bini and V. Pan. *Polynomial and matrix computations*. Progress in Theoretical Computer Science. Birkhäuser Boston–Basel–Berlin, 1994.
6. A. Borodin. On relating time and space to size and depth. *SIAM J. on Comp.*, 6:733–744, 1977.
7. A. Borodin. Time space tradeoffs (getting closer to the barrier ?). In *Algorithms and Computation, Proceedings 4th ISAAC*, volume 762 of *Lecture Notes in Computer Science*, pages 209–220. Springer, 1993.

8. A. Borodin and J. Munro. *The Computational Complexity of Algebraic and Numeric Problems*. Elsevier, 1972.
9. D.W. Brownawell. Bounds for the degree in the Nullstellensatz. *Annals of Math.*, 126:577–591, 1987.
10. B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N. K. Bose et al, editor, *Multidimensional System Theory*, pages 374–383. Reidel, Dordrecht, 1985.
11. P. Bürgisser, M. Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1997.
12. L. Caniglia. How to compute the Chow Form of an unmixed Polynomial Ideal in Single Exponential Time. *Applicable Algebra in Engineering, Communication and Computing*, 1(1):25–41, 1990.
13. L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora et al, editor, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAEECC-6*, volume 357 of *LNCS*, pages 131–152. Springer, 1989.
14. J. Canny. Some algebraic and geometric problems in PSPACE. In *Proceedings 20th. ACM STOC*, pages 460–467, 1988.
15. 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.
16. G.E. Collins. Subresultants and reduced polynomial sequences. *Journal of the Association for Computing Machinery*, 14:128–142, 1967.
17. A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33:73–94, 1991.
18. D.K. Faddeev and V.N. Faddeeva. *Computational methods of linear algebra*. W.H. Freeman, San Francisco, 1963.
19. N. Fitchas and A. Galligo. Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel. *Math. Nachr.*, 149:231–253, 1990.
20. N. Fitchas, M. Giusti, and F. Smietanski. Sur la complexité du théorème des zéros. In J. Guddat et al, editor, *Approximation and Optimization in the Caribbean II, Proceedings 2nd Int. Conf. on Non-Linear Optimization and Approximation*, volume 8 of *Approximation and Optimization*, pages 247–329. Peter Lange Verlag, Frankfurt am Main, 1995.
21. W. Fulton. *Intersection Theory*, volume 3 of *Ergebnisse der Mathematik*. Springer, 1984.
22. M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, and L.M. Pardo. Lower bounds for diophantine approximation. *Journal of Pure and Applied Algebra*, 117,118: 277–317, 1997.
23. M. Giusti, K. Hägele, G. Lecerf, J. Marchand, and B. Salvy. The Projective Noether Maple Package: Computing the dimension of a projective variety. To appear in *Journal of Symbolic Computation*, 2000.
24. 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.

25. M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo. Straight–line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.
26. 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.
27. M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo. Le rôle des structures de données dans les problèmes d’élimination. *Comptes Rendus de l’Academie de Sciences de Paris*, 325:1223–1228, 1997.
28. M. Giusti, J. Heintz, and J. Sabia. On the efficiency of effective Nullstellensätze. *Computational Complexity*, 3:56–95, 1993.
29. M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. To appear in *Journal of Complexity*, 2000.
30. P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Gröbner Bases. In *Proceedings AAECC-5*, volume 356 of LNCS, pages 247–257. Springer–Verlag, 1989.
31. L. Gonzalez-Vega, F. Rouillier, and M.-F. Roy. Symbolic recipes for polynomial system solving. In *Some Tapas of Computer algebra*, pages 34–65. Springer–Verlag, 1997.
32. K. Hägele. *Intrinsic height estimates for the Nullstellensatz*. PhD thesis, Universidad de Cantabria, Santander, Spain, 1998.
33. K. Hägele, J.E. Morais, L.M. Pardo, and M. Sombra. On the intrinsic complexity of the arithmetic Nullstellensatz. *Journal of Pure and Applied Algebra*, 146:103–183, 2000.
34. J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.
35. J. Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. In *Proceedings AAECC-5*, volume 356 of *Lecture Notes in Computer Science*, pages 269–300. Springer–Verlag, 1989.
36. J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Weissbein. Deformation techniques for efficient polynomial equation solving. *Journal of Complexity*, 16(1):70–109, 2000.
37. J. Heintz, G. Matera, L.M. Pardo, and R. Wachenchauser. The intrinsic complexity of parametric elimination methods. *Electronic Journal of SADIO*, 1(1):37–51, 1998.
38. J. Ja’Ja’. Time–space tradeoffs for some algebraic problems. *Journal of the Association for Computing Machinery*, 30(3):657–667, 1983.
39. E. Kaltofen. Asymptotically fast solution of Toeplitz–like singular linear systems. In J. von zur Gathen and M. Giesbrecht, editors, *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation, ISSAC’94 (Oxford, July 20–22 1994)*, ACM Press, pages 297–304, New York, 1994. ACM.
40. H. Kobayashi, T. Fujise, and A. Furukawa. Solving systems of algebraic equations by general elimination method. *J. of Symb. Comp.*, 5:303–320, 1988.
41. T. Krick and L.M. Pardo. Une approche informatique pour l’approximation diophantienne. *C. R. Acad. Sci. Paris*, 318(1):407–412, 1994.
42. 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.

43. L. Kronecker. Grundzüge einer arithmetischen theorie de algebraischen grössen. *J. reine angew. Math.*, 92:1–122, 1882.
44. K. Kühnle. *Space optimal computation of normal forms of polynomials*. PhD thesis, Technischen Universität München, München, Germany, 1998.
45. K. Kühnle and E. Mayr. Exponential space computation of Gröbner bases. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, ISSAC'96 (Zürich, 24–26 July 1996)*, volume 358 of *ACM Press*, pages 63–71, New York, 1996. ACM.
46. F.S. Macaulay. *The Algebraic Theory of Modular Systems*. Cambridge University Press, 1916.
47. G. Matera. *Sobre la complejidad en espacio y tiempo de la eliminación geométrica*. PhD thesis, Universidad de Buenos Aires, Argentina, 1997.
48. G. Matera. Probabilistic algorithms for geometric elimination. *Applicable Algebra in Engineering Communications and Computing*, 9(6):476–521, 1999.
49. G. Matera and J.M. Turull Torres. The space complexity of elimination: Upper bounds. In F.Cucker and M.Shub, editors, *Proceedings Foundations of Computational Mathematics (FOCM'97)*, pages 267–276. Springer, 1997.
50. 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.
51. E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups. *Adv. in Math.*, 46:305–329, 1982.
52. J.E. Morais. *Resolución eficaz de sistemas de ecuaciones polinomiales*. PhD thesis, Universidad de Cantabria, Santander, Spain, 1997.
53. L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAEECC-11*, volume 948 of *Lecture Notes in Computer Science*. Springer-Verlag, 1995.
54. F. Rouillier. Solving zero-dimensional systems through rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1997.
55. J. Sabia and P. Solernó. Bounds for traces in complete intersections and degrees in the Nullstellensatz. *Applicable Algebra in Engineering, Communication and Computing*, 6(6):353–376, 1996.
56. A. Schönhage, F.W. Grotfeld, and E. Vetter. *Fast Algorithms: A Multitape Turing Machine Implementation*. B.I. Wissenschaftsverlag, 1994.
57. J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.
58. J.R. Sendra. *Algoritmos simbólicos de Hankel en álgebra computacional*. PhD thesis, Universidad de Alcalá de Henares, Madrid, Spain, 1990.
59. R. Sendra and J. Llovet. An extended polynomial gcd algorithm using Hankel matrices. *Journal of Symbolic Computation*, 13:25–39, 1992.
60. I.R. Shafarevich. *Basic algebraic geometry*. Springer-Verlag, 1974.
61. M. Sieveking. An algorithm for division of power series. *Computing*, 10:153–156, 1972.
62. M. Sombra. *Estimaciones para el Teorema de Ceros de Hilbert*. PhD thesis, Universidad de Buenos Aires, Argentina, 1998.
63. H.-J. Stoß. Lower bounds for the complexity of polynomials. *Theoretical Computer Science*, 64:15–23, 1989.

64. V. Strassen. Vermeidung von Divisionen. *Crelle J. Reine Angew. Math.*, 264:182–202, 1973.
65. V. Strassen. Algebraic complexity theory. In *Handbook of Theoretical Computer Science*, chapter 11, pages 634–671. Elsevier, 1990.
66. B.L. van der Waerden. *Moderne Algebra II*. Springer Verlag, Berlin, 1931.
67. J. von zur Gathen. Parallel arithmetic computations: a survey. In B. Rován 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.
68. J. von zur Gathen. Parallel linear algebra. In John H. Reif, editor, *Synthesis of Parallel Algorithms*. Morgan Kaufmann, 1993.
69. P. Wadler. Deforestation: transforming programs to eliminate trees. *Theoretical Computer Science*, 73:231–248, 1990. (Special issue of selected papers from 2nd. ESOP).
70. O. Zariski. *Algebraic surfaces*. Classics in Mathematics. Springer–Verlag, 1995.
71. R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings EUROSAM' 79*, volume 72 of *LNCS*, pages 216–226, 1979.
72. R. Zippel. *Effective Polynomial Computation*. ECS 241. Kluwer Academic Publishers, 1993.