

Degeneracy Loci and Polynomial Equation Solving

Bernd Bank · Marc Giusti · Joos Heintz ·
Grégoire Lecerf · Guillermo Matera ·
Pablo Solernó

Received: 19 June 2013 / Accepted: 10 December 2013 / Published online: 23 October 2014
© SFOCM 2014

Abstract Let V be a smooth, equidimensional, quasi-affine variety of dimension r over \mathbb{C} , and let F be a $(p \times s)$ matrix of coordinate functions of $\mathbb{C}[V]$, where $s \geq p + r$. The pair (V, F) determines a vector bundle E of rank $s - p$ over $W := \{x \in V \mid \text{rk } F(x) = p\}$. We associate with (V, F) a descending chain of degeneracy loci of E (the generic polar varieties of V represent a typical example of this situation). The maximal degree of these degeneracy loci constitutes the essential ingredient for the uniform, bounded-error probabilistic pseudo-polynomial-time algorithm that we will design and that solves a series of computational elimination problems that can be formulated in this framework. We describe applications to polynomial equation solving over the reals and to the computation of a generic fiber of a dominant endomorphism of an affine space.

Research partially supported by the following Argentinian, French and Spanish grants:
CONICET Res 4541-12, PIP 11220090100421 CONICET, UBACYT 20020100100945 and
20020110100063, PICT-2010-0525, Digiteo DIM 2009-36HD “MaGiX” grant of the Région
Ile-de-France, ANR-2010-BLAN-0109-04 “LEDA”, MTM2010-16051.

Dedicated to Mike Shub on the occasion of his 70th birthday.

Communicated by Teresa Krick and James Renegar.

B. Bank

Institut für Mathematik, Humboldt-Universität zu Berlin, 10099 Berlin, Germany
e-mail: bank@mathematik.hu-berlin.de

M. Giusti · G. Lecerf

Laboratoire d’informatique, LIX, UMR 7161 CNRS, Campus de l’École Polytechnique,
91128 Palaiseau Cedex, France
e-mail: Marc.Giusti@Polytechnique.fr

G. Lecerf

e-mail: gregoire.lecerf@math.cnrs.fr

Keywords Polynomial equation solving · Pseudo-polynomial complexity · Degeneracy locus · Degree of varieties

Mathematics Subject Classification 14M10 · 14M12 · 14Q20 · 14P05 · 68W30

1 Introduction

Let V be a smooth, equidimensional, quasi-affine variety over \mathbb{C} of dimension r , and let F be a $(p \times s)$ matrix of coordinate functions of $\mathbb{C}[V]$, where $s \geq p + r$. Then F determines a vector bundle E of rank $s - p$ over $W := \{x \in V \mid \text{rk } F(x) = p\}$. With E and a given *generic* matrix $a \in \mathbb{C}^{(s-p) \times s}$ we associate a descending chain of degeneracy loci of E . The generic polar varieties constitute a typical example of this situation.

We prove that these degeneracy loci are empty or equidimensional, normal, and Cohen–Macaulay. Moreover, if b is another generic matrix, the degeneracy loci associated with a and b are rationally equivalent, and their equivalence classes can be expressed in terms of the Chern classes of E . Not the rational equivalence classes, but the degeneracy loci themselves constitute a useful tool for solving efficiently certain computational elimination tasks associated with suitable quasi-affine varieties and matrices F . Such elimination tasks are, for example, real root finding in reduced complete intersection varieties with a smooth and compact real trace or the problem of efficiently describing a generic fiber of a given birational endomorphism of an affine space.

In a somewhat different context of effective elimination theory, rational equivalence classes of degeneracy loci were considered in [8].

J. Heintz (✉)

Departamento de Computación, Universidad de Buenos Aires,
Ciudad Univ., Pab.I, 1428 Buenos Aires, Argentina
e-mail: joos@dc.uba.ar

J. Heintz

CONICET, Ciudad Univ., Pab.I, 1428 Buenos Aires, Argentina

J. Heintz

Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias,
Universidad de Cantabria, 39071 Santander, Spain

G. Matera

Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento,
J. M. Gutierrez 1150, B1613GSX Los Polvorines, Buenos Aires, Argentina
e-mail: gmatera@ungs.edu.ar

G. Matera

CONICET, J. M. Gutierrez 1150, B1613GSX Los Polvorines, Buenos Aires, Argentina

P. Solernó

Instituto Matemático Luis Santaló, CONICET
Buenos Aires 1428, Argentina

P. Solernó

Departamento de Matemáticas, Facultad de Ciencias Exactas y Naturales,
Universidad de Buenos Aires, Buenos Aires 1428, Argentina
e-mail: psolerno@dm.uba.ar

1.1 Contributions

The main contribution of this paper is a new algorithm that solves the aforementioned and other elimination tasks in uniform, bounded-error probabilistic *pseudo-polynomial time*. In this sense it belongs to the pattern of elimination procedures introduced in symbolic seminumeric computation by the already classical Kronecker algorithm [9, 11, 17–19, 21]. Here we refer to procedures whose inputs are measured in the usual way by syntactic, extrinsic parameters; in addition to these, there is a semantic, intrinsic parameter that depends on the geometrical meaning of the input and may become exponential in terms of the syntactic parameters. A procedure is called *pseudo-polynomial* if its time complexity is polynomial in both the syntactic and semantic parameters. In this sense, the semantic parameter that controls the complexity of our main algorithm is the maximal degree of the degeneracy loci that we associate with the given elimination task.

The particular feature of this algorithm is that the input polynomials of the elimination task under consideration may be given by an essentially division-free arithmetic circuit (which means that only divisions by scalars are allowed) of size L . The complexity of the algorithm then becomes of order $L(snd)^{O(1)}\delta^2$, where n is the number of indeterminates of the input polynomials, d their maximal degree, s the number of columns of the given matrix, and δ essentially the maximal degree of the degeneracy loci involved. In the worst case, this complexity is of order $(s(nd)^n)^{O(1)}$. General degeneracy loci constitute an important instance of where we are able to achieve, as a generalization of [19], a complexity bound of order square δ . At present no other elimination procedure reaches such a sharp bound. In particular, we do not rely on equidimensional decomposition whose best known complexity is of order cube δ (see [28, Theorem 8] for an application to polar varieties). For comparisons with the complexity of Gröbner basis algorithms we refer the interested reader to [32]. Without going into the technical details we indicate also how our algorithm may be realized in the nonuniform deterministic complexity model by algebraic computation trees. We implemented our main algorithm within the C++ library `geomsolvex` of MATH-EMAGIX [33].

In Sect. 2 we present some of the basic mathematical facts concerning the geometry of our degeneracy loci that will be used in Sect. 4 to develop our main algorithm. The proofs, all of which except one are self-contained, require only some knowledge of classical algebraic geometry and commutative algebra, which can be found, for example, in [24, 25, 30], elementary properties of vector bundles over algebraic varieties [31], the Thom–Porteous formula [16, Chap. 14], and the notion of linear equivalence of cycles [16, Chap. 1]. The main algorithm requires some familiarity with the classical version of the Kronecker algorithm [11, 19] and with algebraic complexity [7].

1.2 Notions and Notations

We shall freely use standard notions, notations, and results of classic algebraic geometry, commutative algebra, and algebraic complexity theory, which can be found, for example, in [7, 24, 25, 30].

Let \mathbb{Q} and \mathbb{C} be the fields of rational and complex numbers, let X_1, \dots, X_n be indeterminates over \mathbb{C} , and let the following polynomials be given: G_1, \dots, G_q , and H in $\mathbb{C}[X_1, \dots, X_n]$. By \mathbb{A}^n we denote the n -dimensional affine space over \mathbb{C} . We shall use the following notations:

$$\{G_1 = 0, \dots, G_q = 0\} := \{x \in \mathbb{A}^n \mid G_1(x) = 0, \dots, G_q(x) = 0\}$$

and

$$\{G_1 = 0, \dots, G_q = 0\}_H := \{x \in \mathbb{A}^n \mid G_1(x) = 0, \dots, G_q(x) = 0, H(x) \neq 0\}.$$

Suppose $1 \leq q \leq n$ and that G_1, \dots, G_q form a regular sequence in the localized ring $\mathbb{C}[X_1, \dots, X_n]_H$. We call it *reduced* outside of $\{H = 0\}$ if for any index $1 \leq k \leq q$ the ideal $(G_1, \dots, G_k)_H$ is radical in $\mathbb{C}[X_1, \dots, X_n]_H$. Let V be the quasi-affine subvariety of the ambient space \mathbb{A}^n defined by $G_1 = 0, \dots, G_q = 0$ and $H \neq 0$, i.e.,

$$V := \{G_1 = 0, \dots, G_q = 0\}_H.$$

By $\mathbb{C}[V]$ we denote the coordinate ring of V whose elements we call the coordinate functions of V . We adopt the same notations of V as we did for $V := \mathbb{A}^n$.

Suppose for the moment that V is a closed subvariety of \mathbb{A}^n , i.e., V is of the form $V = \{G_1 = 0, \dots, G_q = 0\}$. For V irreducible we define its degree $\deg V$ as the maximal number of points we can obtain by cutting V with finitely many affine hyperplanes of \mathbb{C}^n such that the intersection is finite. Observe that this maximum is reached when we intersect V with dimension of V many *generic* affine hyperplanes of \mathbb{C}^n . If V is not irreducible, then let $V = C_1 \cup \dots \cup C_s$ be the decomposition of V into irreducible components. We define the degree of V as $\deg V := \sum_{1 \leq j \leq s} \deg C_j$. With this definition we can state the so-called *Bézout inequality*: if V and W are closed subvarieties of \mathbb{C}^n , then we have

$$\deg(V \cap W) \leq \deg V \cdot \deg W.$$

If V is a hypersurface of \mathbb{C}^n , then its degree equals the degree of its minimal equation. The degree of a point of \mathbb{C}^n is just one. For more details we refer the interested reader to [16, 20, 34].

2 Degeneracy Loci

We present the mathematical tools we need for the design of our main algorithm in Sect. 4. Proposition 3 and Theorem 5 below are not new. They can be extracted from existing results of modern algebraic geometry. Since we use the ingredients of our argumentation for these statements otherwise, we give new elementary proofs of them. This makes our exposition self-contained.

Let V be a quasi-affine variety, and suppose that V is smooth and equidimensional of dimension r . The following constructions, statements, and proofs generalize the basic arguments of [3–5]. Let p and s be natural numbers with $s \geq p + r$. We suppose that there is given a $(p \times s)$ matrix of coordinate functions of V , namely,

$$F := \begin{bmatrix} f_{1,1} & \cdots & f_{1,s} \\ \vdots & & \vdots \\ f_{p,1} & \cdots & f_{p,s} \end{bmatrix} \in \mathbb{C}[V]^{p \times s}.$$

For $x \in V$ we denote by $\text{rk } F(x)$ the rank of the complex $(p \times s)$ matrix $F(x)$. Let $W := \{x \in V \mid \text{rk } F(x) = p\}$, and observe that W is an open, not necessarily affine, subvariety of V that is covered by canonical affine charts given by the p minors of F .

Let $E := \{(x, y) \in W \times \mathbb{A}^s \mid F(x) \cdot y^T = 0\}$, and let $\pi : E \rightarrow W$ be the first projection (here y^T denotes the transposed vector of y). One sees easily that π is a vector bundle of rank $s - p$. We call π (or E) the vector bundle associated with the pair (V, F) . Let us fix for the moment a complex $((s - p) \times s)$ matrix:

$$a := \begin{bmatrix} a_{1,1} & \cdots & a_{1,s} \\ \vdots & & \vdots \\ a_{s-p,1} & \cdots & a_{s-p,s} \end{bmatrix} \in \mathbb{C}^{(s-p) \times s},$$

with $\text{rk } a = s - p$. For $1 \leq i \leq r + 1$, let

$$a_i := \begin{bmatrix} a_{1,1} & \cdots & a_{1,s} \\ \vdots & & \vdots \\ a_{s-p-i+1,1} & \cdots & a_{s-p-i+1,s} \end{bmatrix} \in \mathbb{C}^{(s-p-i+1) \times s}.$$

We have $\text{rk } a_i = s - p - i + 1$. Let

$$T(a_i) := \begin{bmatrix} F \\ a_i \end{bmatrix} \in \mathbb{C}[V]^{(s-i+1) \times s} \quad \text{and} \quad W(a_i) := \{x \in W \mid \text{rk } T(a_i)(x) < s - i + 1\}.$$

Applying [13, Theorem 3] or [24, Theorem 13.10] to each canonical affine chart of W we conclude that any irreducible component of $W(a_i)$ has codimension at most i in W . For $1 \leq i \leq r$, the locally closed algebraic varieties $W(a_i)$ form a descending chain

$$W \supseteq W(a_1) \supseteq \cdots \supseteq W(a_r).$$

We call the algebraic variety $W(a_i)$ the i th *degeneracy locus* of the pair (V, F) associated with a .

The vector bundle E is a subbundle of $W \times \mathbb{A}^s$. Fix $1 \leq i \leq r$. Then the matrix a_i defines a bundle map $W \times \mathbb{A}^s \rightarrow W \times \mathbb{A}^{s-p-i+1}$, which associates with each $(x, y) \in W \times \mathbb{A}^s$ the point $(x, a_i \cdot y^T) \in W \times \mathbb{A}^{s-p-i+1}$. By restriction we obtain a bundle map $\varphi_i : E \rightarrow W \times \mathbb{A}^{s-p-i+1}$ whose critical locus we are going to identify with $W(a_i)$. First we observe that $(x, y) \in E$ is a critical point of φ_i if and only if any point of the fiber E_x of E at x is critical for φ_i . Thus the property of being a critical point of φ_i depends only on the fiber. We say that $x \in W$ is *critical* for φ_i if this map is critical for E_x . One verifies easily by direct computation that the degeneracy locus $W(a_i)$ is the set of critical points of W for φ_i . In this sense, $W(a_i)$ is a degeneracy locus of φ_i [16, Chap. 14].

Example 1 We will visualize our setup by a simple example. Consider the polynomial $G := X_1^2 + X_2^2 + X_3^2 - 1 \in \mathbb{C}[X_1, X_2, X_3]$. Then $V := \{G = 0\}$ is an irreducible subvariety of \mathbb{A}^3 that is smooth of dimension $r := 2$. Let F be the gradient of G restricted to V , and let $p := 1$ and $s := 3$. Thus, $s = p + r$. For π_1, π_2, π_3 as the coordinate functions of $\mathbb{C}[V]$ induced by X_1, X_2, X_3 and for

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \end{bmatrix} \in \mathbb{C}^{2 \times 3}$$

generic, we have

$$F = [2\pi_1 \quad 2\pi_2 \quad 2\pi_3], \quad T(a_1) = \begin{bmatrix} 2\pi_1 & 2\pi_2 & 2\pi_3 \\ a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \end{bmatrix},$$

$$T(a_2) = \begin{bmatrix} 2\pi_1 & 2\pi_2 & 2\pi_3 \\ a_{1,1} & a_{1,2} & a_{1,3} \end{bmatrix}.$$

One verifies easily that $W = V$, $W(a_1) = \{x \in V \mid \det(T(a_1)) = 0\}$, and $W(a_2) = \{x \in V \mid x = (x_1, x_2, x_3), a_{1,2}x_1 - a_{1,1}x_2 = 0, a_{1,3}x_1 - a_{1,1}x_3 = 0, a_{1,3}x_2 - a_{1,2}x_3 = 0\}$ hold. Since the matrix $[a_{i,j}]_{1 \leq i \leq 2, 1 \leq j \leq 3}$ is generic by assumption, we conclude that $W(a_1)$ is equidimensional of dimension one and that $W(a_2)$ is the classical polar variety of the sphere V , which can be parameterized in the following way:

$$W(a_2) = \left\{ \left(\frac{a_{1,1}^2}{a_{1,3}^2} + \frac{a_{1,2}^2}{a_{1,3}^2} + 1 \right) X_3^2 - 1 = 0, X_1 - \frac{a_{1,1}}{a_{1,3}} X_3 = 0, X_2 - \frac{a_{1,2}}{a_{1,3}} X_3 = 0 \right\}.$$

2.1 Dimension of a Degeneracy Locus

We will now show that for a *generic* matrix a the degeneracy locus $W(a_i)$ is either empty or of expected pure codimension i in W (see Proposition 3 in what follows). Our considerations will only be local. Therefore, it suffices to consider the items to be introduced now. Let

$$\Delta := \det \begin{bmatrix} f_{1,1} & \cdots & f_{1,p} \\ \vdots & & \vdots \\ f_{p,1} & \cdots & f_{p,p} \end{bmatrix}.$$

For $1 \leq i \leq r$, let

$$m_i := \det \begin{bmatrix} f_{1,1} & \cdots & f_{1,s-i} \\ \vdots & & \vdots \\ f_{p,1} & \cdots & f_{p,s-i} \\ a_{1,1} & \cdots & a_{1,s-i} \\ \vdots & & \vdots \\ a_{s-p-i,1} & \cdots & a_{s-p-i,s-i} \end{bmatrix}.$$

Thus, m_i is the upper-left corner $(s - i)$ minor of the $((s - i + 1) \times s)$ matrix $T(a_i)$. Further, let

$$M_{s-i+1}, \dots, M_s$$

be the $(s - i + 1)$ minors of the matrix $T(a_i)$ given by the columns numbered $1, \dots, s - i$, to which we add, one by one, the columns numbered $s - i + 1, \dots, s$. Observe that

$$W(a_i)_\Delta := \{x \in W(a_i) \mid \Delta(x) \neq 0\}$$

is an affine chart of the degeneracy locus $W(a_i)$. The exchange lemma in [2] implies

$$W(a_i)_{\Delta \cdot m_i} = \{M_{s-i+1} = 0, \dots, M_s = 0\}_{\Delta \cdot m_i}.$$

Let Z_{s-i+1}, \dots, Z_s be new indeterminates and $\tilde{M}_{s-i+1}, \dots, \tilde{M}_s$ be the $(s - i + 1)$ minors of the matrix

$$\begin{bmatrix} f_{1,1} & \cdots & f_{1,s-i} & f_{1,s-i+1} & \cdots & f_{1,s} \\ \vdots & & \vdots & \vdots & & \vdots \\ f_{p,1} & \cdots & f_{p,s-i} & f_{p,s-i+1} & \cdots & f_{p,s} \\ a_{1,1} & \cdots & a_{1,s-i} & a_{1,s-i+1} & \cdots & a_{1,s} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{s-p-i,1} & \cdots & a_{s-p-i,s-i} & a_{s-p-i,s-i+1} & \cdots & a_{s-p-i,s} \\ a_{s-p-i+1,1} & \cdots & a_{s-p-i+1,s-i} & Z_{s-i+1} & \cdots & Z_s \end{bmatrix}$$

given by the columns numbered $1, \dots, s - i$, to which we add, one by one, the columns numbered $s - i + 1, \dots, s$. We consider now the morphism $\Phi_i : V_{m_i} \times \mathbb{A}^i \rightarrow \mathbb{A}^i$ of smooth algebraic varieties defined for $x \in V_{m_i}$ and $z \in \mathbb{A}^i$ by $(x, z) \mapsto \Phi_i(x, z) := (\tilde{M}_{s-i+1}(x, z), \dots, \tilde{M}_s(x, z))$.

Lemma 2 *The origin $(0, \dots, 0)$ of \mathbb{A}^i is a regular value of Φ_i .*

Proof Without loss of generality we may assume that $\Phi_i^{-1}(0, \dots, 0)$ is nonempty. Let $x \in V_{m_i}$ and $z \in \mathbb{A}^i$ with $\Phi_i(x, z) = (0, \dots, 0)$ be arbitrarily chosen. Observe that the Jacobian of Φ_i at (x, z) is a matrix with i rows of the following form:

$$\begin{bmatrix} * \cdots * m_i(x) & 0 & \cdots & 0 \\ * \cdots * & 0 & m_i(x) & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ * \cdots * & 0 & \cdots & 0 & m_i(x) \end{bmatrix}.$$

Since x belongs to V_{m_i} , we conclude that (x, z) is a regular point of Φ_i . The arbitrary choice of (x, z) in $\Phi_i^{-1}(0, \dots, 0)$ now implies Lemma 2. □

From the weak transversality theorem of Thom–Sard (e.g., [10, Theorem III.7.4]) we deduce now that there exists a nonempty Zariski open set Ω of \mathbb{A}^i such that for any point $z \in \Omega$ the equations $\tilde{M}_{s-i+1}(x, z) = 0, \dots, \tilde{M}_s(x, z) = 0$ intersect transversally at any common zero belonging to V_{m_i} . Henceforth we shall choose the complex $((s - p) \times s)$ matrix a generically proceeding step by step from row one until row $s - p$. With this choice in mind we may suppose without loss of generality that the equations $M_{s-i+1} = 0, \dots, M_s = 0$ intersect transversally at any of their common zeros belonging to V_{m_i} . In particular, $W(a_i)_{\Delta \cdot m_i} = \{M_{s-i+1} = 0, \dots, M_s = 0\}_{\Delta \cdot m_i}$ is either empty or of pure codimension i in $W_{\Delta \cdot m_i}$.

Proposition 3 ([26, Transversality Lemma 1.3 (i)]) *For $1 \leq i \leq r$ and a generic matrix $a \in \mathbb{C}^{(s-p) \times s}$, the i th degeneracy locus $W(a_i)$ is empty or of pure codimension i in W .*

Proof Let C be an irreducible component of $W(a_i)$ not contained in $W(a_{i+1})$. Without loss of generality we may assume that $\Delta \cdot m_i$ does not vanish identically on C . Therefore, $C_{\Delta \cdot m_i}$ is an irreducible component of $W(a_i)_{\Delta \cdot m_i}$. Hence, $C_{\Delta \cdot m_i}$ is of codimension i in $W_{\Delta \cdot m_i}$. This implies that the codimension of C in W is also i .

Let us consider the case $i = r$. By induction on $1 \leq j \leq s - p - r$, we conclude in the same way as in the proof of Lemma 2 and the observations following it that for any point x of W_Δ there exists a $(p + j)$ minor corresponding to $p + j$ columns, including those numbered $1, \dots, p$, of the matrix

$$\begin{bmatrix} & F & \\ a_{1,1} & \cdots & a_{1,s} \\ \vdots & & \vdots \\ a_{j,1} & \cdots & a_{j,s} \end{bmatrix}$$

that does not vanish at x . This implies that $W(a_{r+1})_\Delta$ is empty. Thus, $W(a_r)_\Delta$ and, hence, $W(a_r)$ are empty or of pure codimension r in W . This proves Proposition 3 in the case $i = r$.

Suppose now that Proposition 3 is wrong, and let $1 \leq i < r$ be maximal such that there exists an irreducible component C of $W(a_i)$ with codimension different from i in W . Then C must be contained in $W(a_{i+1})$. There exists an irreducible component D of $W(a_{i+1})$ with $D \supseteq C$. From the maximal choice of i we deduce that the codimension of D in W is $i + 1$. This implies that the codimension of C in W is at least $i + 1$. On the other hand, we have seen that the codimension of C in W is at most i . This contradiction implies Proposition 3. □

By the way, we have proven that the variety $W(a_i) \setminus W(a_{i+1})$ is empty or equidimensional and smooth and that it can be defined locally by reduced complete intersections.

Corollary 4 ([16, Theorem 14.4 (c)]) *For $1 \leq i \leq r$ and a generic matrix $a \in \mathbb{C}^{(s-p) \times s}$, the degeneracy locus $W(a_i)$ is empty or equidimensional and Cohen–Macaulay.*

Proof The statement is local. Thus, we may, without loss of generality, restrict our attention to the affine variety $W(a_i)_\Delta$, and we may suppose $W(a_i)_\Delta \neq \emptyset$. Observe that the affine variety W_Δ is equidimensional and smooth and, therefore, Cohen–Macaulay. Furthermore, $W(a_i)_\Delta$ is a determinantal subvariety of W_Δ given by maximal minors, which is by Proposition 3 of pure codimension i in W_Δ .

Applying now [6, Theorem 2.7 and Proposition 16.19] to this situation we conclude that $W(a_i)_\Delta$ is Cohen–Macaulay (see also [12, 13] and [14, Section 18.5] for the general context of determinantal varieties). This implies Corollary 4. \square

Taking into account Corollary 4 we conclude that the $(s - i + 1)$ minors of $T(a_i)$ induce in the local ring of W at any point of $W(a_i)$ a radical ideal. Therefore, $W(a_i)$ considered as a scheme is reduced.

2.2 Normality and Rational Equivalence of Degeneracy Loci

Theorem 5 *For $1 \leq i \leq r$ and a generic matrix $a \in \mathbb{C}^{(s-p) \times s}$, the degeneracy locus $W(a_i)$ is empty or equidimensional, Cohen–Macaulay, and normal.*

Proof Again, because the statement of Theorem 5 is local, we may restrict our attention to the affine variety $W(a_i)_\Delta$, which we suppose to be nonempty. By Corollary 4, the variety $W(a_i)_\Delta$ is equidimensional and Cohen–Macaulay, and by Serre’s normality criterion (e.g., [24, Theorem 23.8]), it suffices therefore to prove the following statement.

Claim 6 *The singular points of $W(a_i)_\Delta$ form a subvariety of codimension at least two.*

Proof of the Claim We follow the general lines of the argumentation in [5, Sect. 3]. In the case where $i = r$, Proposition 3 implies the claim. Let us therefore suppose that there exists an index $1 \leq i < r$ such that the claim is wrong. Let

$$v := \det \begin{bmatrix} f_{1,1} & \cdots & f_{1,s-i-1} \\ \vdots & & \vdots \\ f_{p,1} & \cdots & f_{p,s-i-1} \\ a_{1,1} & \cdots & a_{1,s-i-1} \\ \vdots & & \vdots \\ a_{s-p-i-1,1} & \cdots & a_{s-p-i-1,s-i-1} \end{bmatrix}$$

be the $(s - i - 1)$ minor of the $((s - i - 1) \times s)$ matrix $T(a_{i+2}) = \begin{bmatrix} F \\ a_{i+2} \end{bmatrix}$ given by the columns numbered $1, \dots, s - i - 1$.

For $s - p - i \leq k \leq s - p - i + 1$ and $s - i \leq l \leq s$ let

$$m_{k,l} := \det \begin{bmatrix} f_{1,1} & \cdots & f_{1,s-i-1} & f_{1,l} \\ \vdots & & \vdots & \vdots \\ f_{p,1} & \cdots & f_{p,s-i-1} & f_{p,l} \\ a_{1,1} & \cdots & a_{1,s-i-1} & a_{1,l} \\ \vdots & & \vdots & \vdots \\ a_{s-p-i-1,1} & \cdots & a_{s-p-i-1,s-i-1} & a_{s-p-i-1,l} \\ a_{k,1} & \cdots & a_{k,s-i-1} & a_{k,l} \end{bmatrix}.$$

We consider now an arbitrary point x of $W(a_i)_{\Delta \cdot v}$. If there exists a pair (k, l) of indices with $s - p - i \leq k \leq s - p - i + 1$ and $s - i \leq l \leq s$ and $m_{k,l}(x) \neq 0$, then, by the generic choice of the complex $(r \times s)$ matrix a , the variety $W(a_i)_{\Delta \cdot v}$ must be smooth at x (compare to Lemma 2 and the comments following it).

Therefore, the singular locus of $W(a_i)_{\Delta \cdot v}$ is contained in

$$\mathcal{Z} := W_{\Delta \cdot v} \cap \{m_{k,l} = 0 \mid s - p - i \leq k \leq s - p - i + 1, s - i \leq l \leq s\}.$$

Again, the generic choice of a implies that \mathcal{Z} is empty or has pure codimension $2(i + 1)$ in $W_{\Delta \cdot v}$. Hence, the singular locus of $W(a_i)_{\Delta \cdot v}$ has at least codimension $2(i + 1)$ in $W_{\Delta \cdot v}$ and therefore at least codimension two in $W(a_i)_{\Delta \cdot v}$. This argumentation proves that the singular points of $W(a_i)_{\Delta} \setminus W(a_{i+2})_{\Delta}$ are contained in a subvariety of $W(a_i)_{\Delta}$ of codimension at least two. Since $W(a_{i+2})_{\Delta}$ is empty or has, by Proposition 3, codimension two in $W(a_i)_{\Delta}$, the claim follows. □

This ends our proof of Theorem 5. For more details we refer readers to [5]. □

Corollary 7 For $1 \leq i \leq r$, the irreducible components of $W(a_i)$ are exactly the Zariski connected components of $W(a_i)$ and are, hence, mutually disjoint.

Proof Corollary 7 follows immediately from Theorem 5 taking into account [24, Chap. 1, § 9, Remark]. □

Let $a \in \mathbb{C}^{(s-p) \times s}$ be generic and $1 \leq i \leq r$. Following the Thom–Porteous formula we may express the rational equivalence class of $W(a_i)$ in terms of the Chern classes of E (see [16, Theorem 14.4], and, in the case where $W(a_i)$ is a polar variety, the proof of [26, Proposition 1.2]). This argumentation yields the following statement.

Theorem 8 Let $a, b \in \mathbb{C}^{(s-p) \times s}$ be generic matrices, and let $1 \leq i \leq r$. Then the subvarieties $W(a_i)$ and $W(b_i)$ of W are rationally equivalent.

In the case of generic polar varieties Theorem 8 corresponds to [26, Proposition 1.2]. It is not too hard to prove by elementary techniques the algebraic equivalence of $W(a_i)$ and $W(b_i)$. However, the proof of their rational equivalence seems to be beyond the reach of direct arguments.

2.3 Geometric Tools

The following two technical statements will be used in Sect. 4, where we describe our main algorithm.

For $1 \leq k_1 < \dots < k_p \leq s$ we denote by Δ_{k_1, \dots, k_p} the p minor of F given by the columns numbered k_1, \dots, k_p , and for the columns numbered $1 \leq l_1 < \dots < l_{s-i} \leq s$ that contain k_1, \dots, k_p we denote by $m_{l_1, \dots, l_{s-i}}$ the $(s - i)$ minor of $T(a_{i+1})$ given by the columns numbered l_1, \dots, l_{s-i} (in the case where $s = r + p$ and $i = r$ we have $m_{l_1, \dots, l_p} = \Delta_{k_1, \dots, k_p}$). The following lemma is borrowed from [1, Sect. 4.3].

Lemma 9 *Let $1 \leq i \leq r$, and let C be an irreducible component of $W(a_i)_{\Delta_{k_1, \dots, k_p}}$. Then the polynomial $m_{l_1, \dots, l_{s-i}}$ does not vanish identically on C .*

Proof Fix $1 \leq i \leq r$. Without loss of generality we may assume $k_1 := 1, \dots, k_p := p$ and $l_1 := 1, \dots, l_{s-i} := s - i$, and hence, $\Delta_{k_1, \dots, k_p} := \Delta$ and $m_{l_1, \dots, l_{s-i}} := m_i$. By induction on $1 \leq i \leq r$, one deduces from the genericity of the complex matrix a that m_i does not vanish identically on any irreducible component of W_Δ . Therefore, the affine variety $\mathcal{Y} := W_\Delta \cap \{m_i = 0\}$ is empty or of pure codimension one in W_Δ .

Let $1 \leq l_1^* < \dots < l_{s-i}^* \leq s$ be arbitrary, and denote the $(s - i)$ minor $m_{l_1^*, \dots, l_{s-i}^*}$ of $T(a_{i+1})$ by m_i^* . Further, let $M_{s-i+1}^*, \dots, M_s^*$ be the $(s - i + 1)$ minors of $T(a_i)$ given by the columns numbered l_1^*, \dots, l_{s-i}^* , to which we add, one by one, the columns numbered by the elements of the index set $\{1, \dots, s\} \setminus \{l_1^*, \dots, l_{s-i}^*\}$. Again, the genericity of a implies that the intersection $\mathcal{Y}_{m_i^*} \cap \{M_{s-i+1}^* = 0, \dots, M_s^* = 0\}$ is empty or of pure codimension i in $\mathcal{Y}_{m_i^*}$ and, hence, of pure codimension $i + 1$ in $W_{\Delta \cdot m_i^*}$.

Let C be an irreducible component of $W(a_i)_\Delta$. From Proposition 3 we deduce that C is not contained in $W(a_{i+1})_\Delta$. This implies that there exists an $(s - i)$ minor m_i^* of $T(a_{i+1})$, with $C_{m_i^*} \neq \emptyset$. The corresponding $(s - i + 1)$ minors $M_{s-i+1}^*, \dots, M_s^*$ of $T(a_i)$ define in $W_{\Delta \cdot m_i^*}$ a variety that contains $C_{m_i^*}$ as an irreducible component. Hence, $C_{m_i^*}$ is a subset of $\{M_{s-i+1}^* = 0, \dots, M_s^* = 0\}$. Suppose now that m_i vanishes identically on C . Then $\mathcal{Y}_{m_i^*}$ contains $C_{m_i^*}$ and is in particular nonempty. Since $C_{m_i^*}$ is contained in $\mathcal{Y}_{m_i^*} \cap \{M_{s-i+1}^* = 0, \dots, M_s^* = 0\}$, we conclude that the codimension of $C_{m_i^*}$ in $W_{\Delta \cdot m_i^*}$ is at least $i + 1$.

On the other hand, Proposition 3 implies that the codimension of $C_{m_i^*}$ in $W_{\Delta \cdot m_i^*}$ is i . This contradiction proves that m_i cannot vanish identically on C . \square

Suppose that the quasi-affine variety V is embedded in the affine space \mathbb{A}^n and that the Zariski closure of V in \mathbb{A}^n can be defined by the polynomials of $\mathbb{C}[X_1, \dots, X_n]$ of degree at most d . Furthermore, suppose that for each $1 \leq i \leq p$ and $1 \leq j \leq s$ there is given a polynomial $F_{i,j} \in \mathbb{C}[X_1, \dots, X_n]$ of degree at most d such that the entry $f_{i,j}$ of matrix F is the restriction of $F_{i,j}$ to V .

Let $b_1, \dots, b_{r+1} \in \mathbb{C}^{s \times s}$ be regular matrices. We call (b_1, \dots, b_{r+1}) a *hit-ting sequence* for V and F if the following property holds: there exist p minors $\Delta_1, \dots, \Delta_{r+1}$ of the matrices $F \cdot b_1, \dots, F \cdot b_{r+1} \in \mathbb{C}[V]^{p \times s}$, respectively, such that for any point x of W at least one of the minors Δ_t ($1 \leq t \leq r + 1$) does not vanish at x . The following lemma is reminiscent of [22, Theorem 4.4].

Lemma 10 *Let $\kappa := (4pd)^{2n}$, and let $\mathcal{K} := \{1, \dots, \kappa\}$. Then the set $(\mathcal{K}^{s \times s})^{r+1}$ contains at least $\kappa^{s^2(r+1)}(1 - 4^{-n})$ hitting sequences for V and F .*

Proof For $1 \leq t \leq r + 1$ and $1 \leq k, l \leq s$ let $B_{k,l}^t$ be new indeterminates over \mathbb{C} , and let $\mathbf{B}_t := (B_{k,l}^t)_{1 \leq k, l \leq s}$. Furthermore, let $\Delta_t \in \mathbb{C}[V][\mathbf{B}_t]$ be the p minor of $F \cdot \mathbf{B}_t$ given by the first p columns of $F \cdot \mathbf{B}_t$.

Consider an arbitrary point x of W . Without loss of generality we may suppose $\Delta(x) \neq 0$. Fix for the moment $1 \leq t \leq r + 1$, and consider the matrix \mathbf{C}_t obtained from \mathbf{B}_t by substituting zero for $B_{k,l}^t$ for any (k, l) , with $p + 1 \leq k \leq s$ and $1 \leq l \leq p$, namely,

$$\mathbf{C}_t := \begin{bmatrix} B_{1,1}^t & \cdots & B_{1,p}^t & B_{1,p+1}^t & \cdots & B_{1,s}^t \\ \vdots & & \vdots & \vdots & & \vdots \\ B_{p,1}^t & \cdots & B_{p,p}^t & B_{p,p+1}^t & \cdots & B_{p,s}^t \\ 0 & \cdots & 0 & B_{p+1,p+1}^t & \cdots & B_{p+1,s}^t \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & B_{s,p+1}^t & \cdots & B_{s,s}^t \end{bmatrix}.$$

It is easy to see that the left p minor $\Delta_t(x, \mathbf{C}_t)$ of the matrix $F \cdot \mathbf{C}_t$ is of the form $\Delta(x)$ times a nonzero polynomial of $\mathbb{C}[\mathbf{B}_t]$. In particular, $\Delta_t(x, \mathbf{C}_t)$ is a polynomial of positive degree. We conclude now a fortiori that for any $x \in W$ the polynomial $\Delta_t(x, \mathbf{B}_t)$ is of positive degree.

We consider now the incidence variety $\mathcal{H} \subset W \times (\mathbb{A}^{s \times s})^{r+1}$ defined by the vanishing of $\Delta_1, \dots, \Delta_{r+1}$. Let π be the projection of \mathcal{H} into $(\mathbb{A}^{s \times s})^{r+1}$. It is not difficult to see that \mathcal{H} is equidimensional of dimension $s^2(r + 1) - 1$. To show this, we proceed recursively. Let W_0 be an arbitrary irreducible component of W . Since the polynomial $\Delta_1(x, \mathbf{B}_1)$ has positive degree in the variables \mathbf{B}_1 for any point $x \in W$, the variety $(W_0 \times (\mathbb{A}^{s \times s})^{r+1}) \cap \{\Delta_1 = 0\}$ must be equidimensional of dimension $r + s^2(r + 1) - 1$. Moreover, each irreducible component of this variety has the form $W_1 \times (\mathbb{A}^{s \times s})^r$, where W_1 is an irreducible component of $(W_0 \times \mathbb{A}^{s \times s}) \cap \{\Delta_1 = 0\}$. Applying this argument recursively for each polynomial Δ_t we conclude that $\Delta_1, \dots, \Delta_{r+1}$ constitute a secant family for the variety $W \times (\mathbb{A}^{s \times s})^{r+1}$ (recall that $\Delta_1, \dots, \Delta_{r+1}$ are polynomials in disjoint groups of indeterminates). Hence, the incidence variety \mathcal{H} is equidimensional of dimension $r + s^2(r + 1) - (r + 1) = s^2(r + 1) - 1$.

In particular, we infer that the Zariski closure of $\pi(\mathcal{H})$ in $(\mathbb{A}^{s \times s})^{r+1}$ has dimension at most $s^2(r + 1) - 1$, and therefore it is a proper closed subvariety of $(\mathbb{A}^{s \times s})^{r+1}$. Observe that the zero-dimensional variety $\pi(\mathcal{H}) \cap (\mathcal{K}^{s \times s})^{r+1}$ contains all sequences of $(\mathcal{K}^{s \times s})^{r+1}$ that are not hitting for V and F .

Claim 11 $\#(\pi(\mathcal{H}) \cap (\mathcal{K}^{s \times s})^{r+1}) \leq (2pd)^{2n} \kappa^{s^2(r+1)-1}$.

Proof of the Claim Observe $\pi^{-1}(\pi(\mathcal{H}) \cap (\mathcal{K}^{s \times s})^{r+1}) = \mathcal{H} \cap (\mathbb{A}^n \times (\mathcal{K}^{s \times s})^{r+1})$. Let C_1, \dots, C_m be the irreducible components of $\mathcal{H} \cap (\mathbb{A}^n \times (\mathcal{K}^{s \times s})^{r+1})$. Because the image under π of each component C_j of $\mathcal{H} \cap (\mathbb{A}^n \times (\mathcal{K}^{s \times s})^{r+1})$ is a point of $\pi(\mathcal{H}) \cap (\mathcal{K}^{s \times s})^{r+1}$, we conclude

$$\#(\pi(\mathcal{H}) \cap (\mathcal{K}^{s \times s})^{r+1}) \leq m \leq \sum_{i=1}^m \deg \overline{C}_i = \deg(\overline{\mathcal{H}} \cap (\mathbb{A}^n \times (\mathcal{K}^{s \times s})^{r+1})) \tag{1}$$

[here, \overline{C}_i denotes the Zariski closure of C_i in $\mathbb{A}^n \times (\mathbb{A}^{s \times s})^{r+1}$]. It is easy to see that the affine variety $\mathbb{A}^n \times (\mathcal{K}^{s \times s})^{r+1}$ can be defined by the vanishing of $s^2(r + 1)$ univariate polynomials of degree κ . Therefore, by [22, Proposition 2.3], it follows that

$$\deg(\overline{\mathcal{H}} \cap (\mathbb{A}^n \times (\mathcal{K}^{s \times s})^{r+1})) \leq \deg \overline{\mathcal{H}} \cdot \kappa^{s^2(r+1)-1} \tag{2}$$

holds. On the other hand, the Bézout inequality implies

$$\deg \overline{\mathcal{H}} \leq \deg \overline{V} \cdot (p(d + 1))^{r+1} \leq (2pd)^{2n}. \tag{3}$$

Combining (1), (2), and (3) we easily deduce the statement of the claim. □

Following the previous claim the probability of finding a nonhitting sequence for V and F in $(\mathcal{K}^{s \times s})^{r+1}$ is at most

$$\frac{(2pd)^{2n} \kappa^{s^2(r+1)-1}}{\kappa^{s^2(r+1)}} = \frac{(2pd)^{2n}}{\kappa} = \frac{(2pd)^{2n}}{(4pd)^{2n}} = \frac{1}{4^n}.$$

This implies Lemma 10. □

2.4 Algebraic Characterization of Degeneracy Loci

Let U_2, \dots, U_s be new indeterminates. For $1 \leq i \leq r$ let $U^{(i)}$ be the $(s \times (s - i + 1))$ matrix

$$U^{(i)} := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ U_2 & 1 & \ddots & \vdots \\ U_3 & U_2 & \ddots & 0 \\ \vdots & U_3 & \ddots & 1 \\ U_i & \vdots & \ddots & U_2 \\ \vdots & U_i & & U_3 \\ U_{s-1} & \vdots & \ddots & \vdots \\ U_s & U_{s-1} & \cdots & U_i \end{bmatrix},$$

and let $U := U^{(s-p+1)}$. With these notations the following assertion holds.

Lemma 12 *Let $1 \leq i \leq r$. Any point $x \in V$ belongs to $W(a_i)$ if and only if the conditions*

$$\det(F(x) \cdot U) \neq 0 \text{ and } \det(T(a_i)(x) \cdot U^{(i)}) = 0$$

are satisfied identically.

Proof Let x be any point of V that satisfies the condition $\det(F(x) \cdot U) \neq 0$. Then $F(x)$ must be of maximal rank p , and hence x belongs to W .

Suppose now that x belongs to W . Let K run over all subsets of $\{1, \dots, s\}$ of cardinality p . Denote by $F(x)_K$ and U_K the p minors of $F(x)$ and U corresponding to the columns of $F(x)$ and rows U indexed by the elements of K . The Binet–Cauchy formula yields

$$\det(F(x) \cdot U) = \sum_{\substack{K \subseteq \{1, \dots, s\} \\ \#K=p}} F(x)_K U_K.$$

From the proof of [23, Theorem 2] we deduce that for $K \subseteq \{1, \dots, s\}, \#K = p$, all the minors U_K are linearly independent over \mathbb{C} . Since x belongs to W , there exists a subset K of $\{1, \dots, s\}$ of cardinality p , with $F(x)_K \neq 0$. This implies $\det(F(x) \cdot U) \neq 0$.

Using the same kinds of arguments one shows that, for $x \in V$, the condition $\det(T(a_i)(x) \cdot U^{(i)}) = 0$ is equivalent to $\text{rk } T(a_i)(x) < s - i + 1$. Lemma 12 follows now easily. □

We define the *point-finding problem associated with the pair (V, F)* as the problem of deciding whether $W(a_r)$ is empty, and if not, to find all the points of the zero-dimensional degeneracy locus $W(a_r)$.

The degree of this problem is the maximal degree of the Zariski closures of all degeneracy loci $W(a_i)$, for $1 \leq i \leq r$, in the ambient space \mathbb{A}^n of V . Observe that this degree does not depend on the particular generic choice of the $((s - p) \times s)$ matrix a (compare to [5, Section 4]).

3 Examples

3.1 Polar Varieties

Let X_1, \dots, X_n be indeterminates over \mathbb{C} , $1 \leq p \leq n$, and let G_1, \dots, G_p be a reduced regular sequence of polynomials in $\mathbb{C}[X_1, \dots, X_n]$. We denote the Jacobian of G_1, \dots, G_p by

$$J(G_1, \dots, G_p) := \begin{bmatrix} \frac{\partial G_1}{\partial X_1} & \dots & \frac{\partial G_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial G_p}{\partial X_1} & \dots & \frac{\partial G_p}{\partial X_n} \end{bmatrix}.$$

Fix a p minor Δ of $J(G_1, \dots, G_p)$, and let

$$V := \{G_1 = 0, \dots, G_p = 0\}_\Delta.$$

Then V is a smooth, equidimensional, quasi-affine subvariety of \mathbb{A}^n of dimension $r := n - p$. Let $s := r + p = n$, and let $F \in \mathbb{C}[V]^{p \times s}$ be the $(p \times s)$ matrix induced by $J(G_1, \dots, G_p)$ on V .

For a given generic complex $((s - p) \times s)$ matrix a and for $1 \leq i \leq r$ the degeneracy locus $W(a_i)$ is the i th generic (classic) polar variety of V associated with the complex $((s - p - i + 1) \times s)$ matrix a_i (see details in [5]).

Proposition 3, Corollary 4, and Theorem 5, given previously, say that the i th generic (classic) polar variety of V is empty or a normal Cohen–Macaulay subvariety of V of pure codimension i (compare to [5, Theorem 2]). From [5, Sect. 3.1] we deduce that such a generic polar variety is not necessarily smooth. Hence, the smoothness of our degeneracy loci cannot be expected in general. If the coefficients of G_1, \dots, G_p and the entries of the $((n - p) \times n)$ matrix a are real, and if the real trace of $\{G_1 = 0, \dots, G_p = 0\}$ is smooth and compact, then there exists a p minor Δ of $J(G_1, \dots, G_p)$ such that the polar varieties associated with a contain real points and are therefore nonempty. The generic polar varieties then form a strictly descending chain ([3] and [4, Proposition 1]).

3.2 Composition of Polynomial Maps

Let $1 \leq p \leq n$, and let Q_1, \dots, Q_n and P_1, \dots, P_p be polynomials of $\mathbb{C}[X_1, \dots, X_n]$ such that P_1, \dots, P_p form a reduced regular sequence. Moreover, let

$$(G_1, \dots, G_p) := (P_1, \dots, P_p) \circ (Q_1, \dots, Q_n)$$

be the composition map defined for $1 \leq k \leq p$ by

$$G_k(X_1, \dots, X_n) := P_k(Q_1(X_1, \dots, X_n), \dots, Q_n(X_1, \dots, X_n)).$$

Suppose that G_1, \dots, G_p constitute a reduced regular sequence in $\mathbb{C}[X_1, \dots, X_n]$. Fix a p minor Δ of the Jacobian $J(G_1, \dots, G_p)$. Then

$$V := \{G_1 = 0, \dots, G_p = 0\}_\Delta$$

is a smooth, quasi-affine subvariety of \mathbb{A}^n of dimension $r := n - p$. The morphism defined by (Q_1, \dots, Q_n) maps V into

$$\mathcal{V} := \{P_1 = 0, \dots, P_p = 0\}.$$

We suppose that this morphism of affine varieties is dominant, i.e.,

$$\overline{(Q_1, \dots, Q_n)(V)} = \mathcal{V}.$$

Observe that for any point $x \in V$ the variety \mathcal{V} is smooth at $y = (Q_1(x), \dots, Q_n(x))$.

Let $s := r + p = n$, and let F be the $(p \times s)$ matrix induced by $J(P_1, \dots, P_p) \circ (Q_1, \dots, Q_n)$ on V . Let $a \in \mathbb{C}^{(s-p) \times s}$ be a generic complex matrix, and denote by $\tilde{W}(a_i)$ the i th polar variety of \mathcal{V} associated with a_i , for $1 \leq i \leq r$. Then we have

$W = V$, and the i th degeneracy locus $W(a_i)$ of W , namely,

$$\begin{aligned}
 W(a_i) &= \left\{ x \in V \mid \text{rk} \begin{bmatrix} F(x) \\ a_i \end{bmatrix} < s - i + 1 \right\} \\
 &= \left\{ x \in V \mid \text{rk} \begin{bmatrix} J(P_1, \dots, P_p) \circ (Q_1, \dots, Q_n)(x) \\ a_i \end{bmatrix} < s - i + 1 \right\},
 \end{aligned}$$

is the (Q_1, \dots, Q_n) preimage of $\tilde{W}(a_i)$.

3.3 Dominant Endomorphisms of Affine Spaces

Let $F_1, \dots, F_n \in \mathbb{C}[X_1, \dots, X_n]$, $V := \mathbb{A}^n$, $p := 1$, $s := p + r = 1 + n$, $F := [F_1, \dots, F_n, 1] \in \mathbb{C}^{1 \times s}$, and let $a \in \mathbb{C}^{n \times s}$ be a generic complex matrix. Observe $W = V = \mathbb{A}^n$ and that, for any $1 \leq i \leq n$, the degeneracy locus $W(a_i)$ is a closed affine subvariety of \mathbb{A}^n . We will now analyze the n th degeneracy locus $W(a_n)$.

Lemma 13 *The degeneracy locus $W(a_n)$ is nonempty if and only if the endomorphism $\Psi : \mathbb{A}^n \rightarrow \mathbb{A}^n$ defined by $\Psi(x) := (F_1(x), \dots, F_n(x))$ is dominant. In this case, the cardinality $\#W(a_n)$ of $W(a_n)$ equals the cardinality of a generic fiber of Ψ .*

Proof Suppose that $W(a_n)$ is nonempty, and let x be a point of $W(a_n)$. Then there exists a $\lambda \in \mathbb{C}$ such that $(F_1(x), \dots, F_n(x), 1) = \lambda(a_{1,1}, \dots, a_{1,n}, a_{1,n+1})$. This implies $(F_1(x), \dots, F_n(x)) = \frac{1}{a_{1,n+1}}(a_{1,1}, \dots, a_{1,n})$. The right-hand side of this equation is therefore a generic point of \mathbb{A}^n with a zero-dimensional (F_1, \dots, F_n) fiber. Hence, the endomorphism Ψ of \mathbb{A}^n is dominant.

Suppose now that Ψ is dominant. Then we may assume without loss of generality that there exists a point $x \in \mathbb{A}^n$ with $(F_1(x), \dots, F_n(x)) = \frac{1}{a_{1,n+1}}(a_{1,1}, \dots, a_{1,n})$. This implies the equation $(F_1(x), \dots, F_n(x), 1) = \lambda(a_{1,1}, \dots, a_{1,n}, a_{1,n+1})$, with $\lambda = \frac{1}{a_{n+1}}$. Hence, x belongs to $W(a_n)$, and thus $W(a_n)$ is not empty. Moreover, $\#W(a_n)$ equals the cardinality of the (F_1, \dots, F_n) fiber of $\frac{1}{a_{1,n+1}}(a_{1,1}, \dots, a_{1,n})$. \square

Suppose now that the morphism Ψ is dominant. Then the degeneracy loci of (\mathbb{A}^n, F) form a descending chain

$$\mathbb{A}^n \supseteq W(a_1) \supseteq \dots \supseteq W(a_n) \neq \emptyset,$$

where, for $1 \leq i < n$, the $(i + 1)$ th degeneracy locus $W(a_{i+1})$ is a closed affine subvariety of $W(a_i)$ of pure codimension one in $W(a_i)$.

3.4 Homotopy

Let F_1, \dots, F_n and G_1, \dots, G_n be reduced regular sequences of $\mathbb{C}[X_1, \dots, X_n]$. We consider the algebraic family

$$\{\lambda F_1 + \mu G_1 = 0, \dots, \lambda F_n + \mu G_n = 0\}, \quad (\lambda, \mu) \in \mathbb{C}^2 \setminus \{(0, 0)\}$$

as a homotopy between the zero-dimensional varieties $\{F_1 = 0, \dots, F_n = 0\}$ and $\{G_1 = 0, \dots, G_n = 0\}$.

We will analyze this homotopy. For this purpose let $V := \mathbb{A}^n, p := 2, s := n + p = n + 2$, and

$$F := \begin{bmatrix} F_1 & \cdots & F_n & 1 & 0 \\ G_1 & \cdots & G_n & 0 & 1 \end{bmatrix}.$$

Furthermore, let $a \in \mathbb{C}^{(s-p) \times s}$ be generically chosen. Then we have $W = V = \mathbb{A}^n$, and for any $1 \leq i \leq n$ the degeneracy locus $W(a_i)$ is a closed affine subvariety of \mathbb{A}^n . From the exchange lemma of [2] we deduce

$$\#W(a_n) = \#\{a_{1,n+1}F_1 + a_{1,n+2}G_1 = a_{1,1}, \dots, a_{1,n+1}F_n + a_{1,n+2}G_n = a_{1,n}\}.$$

Thus, $W(a_n)$ may be interpreted as a deformation of

$$\{a_{1,n+1}F_1 + a_{1,n+2}G_1 = 0, \dots, a_{1,n+1}F_n + a_{1,n+2}G_n = 0\}.$$

4 Algorithms

We will present two procedures, our main algorithm, which computes an algebraic description of the set $W(a_r)$, and a procedure to check membership in a degeneracy locus.

4.1 Notations

Let n, d, p, r, q, s, L be integers with $r = n - q$ and $s \geq p + r$, and let $G_1, \dots, G_q, H, F_{k,l}$, for $1 \leq k \leq p$ and $1 \leq l \leq s$, be polynomials of $\mathbb{Q}[X_1, \dots, X_n]$ given as outputs of an essentially division-free arithmetic circuit β of size L . This means that β contains divisions only by elements of \mathbb{Q} (for details about arithmetic circuits we refer the reader to [7]).

Let d be an upper bound for the degrees of G_1, \dots, G_q and $F_{k,l}$, for $1 \leq k \leq p$ and $1 \leq l \leq s$. We suppose that G_1, \dots, G_q and H satisfy the following two conditions:

- G_1, \dots, G_q form a reduced regular sequence outside of $\{H = 0\}$;
- $V := \{G_1 = 0, \dots, G_q = 0\}_H$ is a smooth quasi-affine variety.

For $1 \leq k \leq p$ and $1 \leq l \leq s$, let $f_{k,l} \in \mathbb{C}[V]$ be the restriction of $F_{k,l}$ to V , and let $F := [f_{k,l}]_{1 \leq k \leq p, 1 \leq l \leq s}$. Let δ^* be the degree of the point-finding problem associated with the pair (V, F) , which was previously introduced as the maximal degree of the Zariski closures of all degeneracy loci $W(a_i)$, $1 \leq i \leq r$, in the ambient space \mathbb{A}^n of V . We write

$$\delta_G := \max\{\deg \overline{\{G_1 = 0, \dots, G_j = 0\}_H} \mid 1 \leq j \leq q\}$$

and $\delta := \max\{\delta_G, \delta^*\}$. We call δ the *system degree* of $G_1, \dots, G_q = 0, H \neq 0$, and $[F_{k,l}]_{1 \leq k \leq p, 1 \leq l \leq s}$.

Fix a generic matrix $a \in \mathbb{Q}^{(s-p) \times s}$. We will design a uniform, bounded-error probabilistic procedure that takes β as input and decides whether $W(a_r)$ is empty and, if not, computes a description of $W(a_r)$ in terms of a primitive element. More precisely, for a new indeterminate T , the procedure outputs the coefficients of univariate polynomials $P, Q_1, \dots, Q_n \in \mathbb{Q}[T]$ such that P is separable, $\deg Q_1 < \deg P, \dots, \deg Q_n < \deg P$, and such that

$$W(a_r) = \{(Q_1(t), \dots, Q_n(t)) \mid t \in \mathbb{C} : P(t) = 0\}$$

holds. Following [19, Section 3.2], such a description is called a *geometric resolution* of $W(a_r)$.

In the sequel we refer freely to terminology, mathematical results, and subroutines of [19], where the first streamlined version of the classical Kronecker algorithm was described. To simplify the exposition, we shall refrain from the presentation of details that merely serve to ensure the appropriate genericity properties for the procedure. The following account requires some familiarity with technical aspects of the classical Kronecker algorithm. A standalone presentation of the algorithm from a mathematical point of view is contained in [11].

4.2 Main Algorithm

As our first task, we compute a description of the variety V . For this purpose, we use the main tools of [19, Algorithm 12] in the following way. As input we take the representation of G_1, \dots, G_q and H by the circuit β . Although the system $G_1 = 0, \dots, G_q = 0$ contains $n \geq q$ variables, we may execute just the q first steps of the main loop of [19, Algorithm 12] to obtain a *lifting fiber* for V [19, Definition 4]. This lifting fiber consists of the following items:

- The *lifting system* G_1, \dots, G_q ;
- An invertible $n \times n$ square matrix M with rational entries such that the new coordinates $Y := M^{-1}X$ are in *Noether position* with respect to V ;
- A rational *lifting point* $z = (z_1, \dots, z_r)$ for V and the lifting system G_1, \dots, G_q ;
- Rational coefficients $\lambda_{r+1}, \dots, \lambda_n$ defining a *primitive element* $u := \lambda_{r+1}Y_{r+1} + \dots + \lambda_n Y_n$ of $V^{(z)} := V \cap \{Y_1 - z_1 = 0, \dots, Y_r - z_r = 0\}$;
- A polynomial $Q \in \mathbb{Q}[T]$ of minimal degree such that $Q(u)$ vanishes on $V^{(z)}$;
- $n - r$ polynomials v_{r+1}, \dots, v_n of $\mathbb{Q}[T]$, of degree strictly smaller than $\deg Q$, such that the equations $Y_1 - z_1 = 0, \dots, Y_r - z_r = 0, Y_{r+1} - v_{r+1}(T) = 0, \dots, Y_n - v_n(T) = 0, Q(T) = 0$ define a *parameterization* of $V^{(z)}$ by the zeros of Q .

The computation of these items depends on the choice of at most $O(n^2)$ parameters in \mathbb{Q} . If the parameters are chosen correctly, then the algorithm returns these items. Otherwise, the algorithm fails. The incorrect choices of these parameters are contained in a hypersurface whose degree is a priori bounded ([19]). Therefore, the whole procedure yields a bounded-error probabilistic algorithm (compare [29, 35]). The error can

be bounded uniformly with respect to the input parameters, whatever they are (e.g., dimension of the ambient space n , degree and coefficients of the input equations). We summarize the outcome in the following statement.

Lemma 14 *Let the notations and assumptions be as previously. There exists a uniform, bounded-error probabilistic algorithm over \mathbb{Q} that computes a lifting fiber of V in time $L(nd)^{O(1)}\delta_G^2$.*

Proof Apply [19, Theorem 1], taking care to perform products of univariate polynomials in quasilinear time. The Bézout inequality implies $\delta_G = O(d^n)$. The complexity bound of Lemma 14 follows now from $\delta_G^2 \log^{O(1)}(\delta_G) = (nd)^{O(1)}\delta_G^2$. \square

By Lemma 10, we may choose with a high probability of success a hitting sequence (b_1, \dots, b_{r+1}) of regular integer $(s \times s)$ matrices and p minors $\Delta_1, \dots, \Delta_{r+1}$ of the matrices $F \cdot b_1, \dots, F \cdot b_{r+1}$ such that $W = V_{\Delta_1} \cup \dots \cup V_{\Delta_{r+1}}$ holds.

Lemma 15 *Let the notations and assumptions be as previously, and let a lifting fiber of V be given. There exists a uniform, bounded-error probabilistic algorithm over \mathbb{Q} that computes lifting fibers for $V_{\Delta_1}, \dots, V_{\Delta_{r+1}}$ in time $L(pnd)^{O(1)}\delta_G^2$.*

Proof Let us fix $1 \leq j \leq r + 1$. The given lifting point of V may be changed by means of [19, Algorithm 5] in time $L(nd)^{O(1)}\delta_G^2$. We call [19, Algorithm 10] with input the lifting fiber of V and the polynomial representing Δ_j (observe that this polynomial can be evaluated using $L + O(p^4)$ arithmetic operations). This yields, with a high probability of success, a lifting fiber of V_{Δ_j} in time $L(pnd)^{O(1)}\delta_G$ (compare [19, Lemmas 14 and 15]). \square

If the varieties $V_{\Delta_1}, \dots, V_{\Delta_{r+1}}$ are empty, then $W(a_r)$ is empty, and the algorithm stops. We suppose that this is not the case. We are now going to describe how we decide whether $W(a_r)_{\Delta_j}$ is empty and, if not, how we compute a lifting fiber of $W(a_r)_{\Delta_j}$. To simplify the notations, we make, without loss of generality, the following assumptions. Let $j := 1, b_1$ be the identity matrix, $\Delta_1 := \Delta$, and $V_\Delta = W_\Delta \neq \emptyset$.

Lemma 16 *Let the notations and assumptions be as previously. For a given lifting fiber of $V_\Delta = W_\Delta$ there exists a uniform, bounded-error probabilistic algorithm over \mathbb{Q} that computes a lifting fiber of $W(a_1)_{\Delta \cdot m_1}$ in time $L(snd)^{O(1)}\delta^2$.*

Proof Observe that $W(a_1) = V_\Delta \cap \{\det(T(a_1)) = 0\}$ holds. By Proposition 3, the polynomial representing $\det(T(a_1))$ does not vanish identically on any irreducible component of V_Δ . Thus, we may use [19, Algorithms 2, 4, 5, 6, and 11] to compute a lifting fiber of $W(a_1)_{\Delta \cdot m_1}$. Since the polynomials representing Δ and m_1 have degrees bounded by pd and can be evaluated in time $L + O(s^4)$, Lemma 16 follows from [19, Lemmas 6, 14, and 16]. \square

From Lemma 9 we deduce that the emptiness of $W(a_1)_{\Delta \cdot m_1}$ implies that of $W(a_1)_\Delta$ and, hence, that of $W(a_r)_\Delta$.

Let $1 \leq i < r$, and assume that we have computed a lifting fiber of $W(a_i)_{\Delta \cdot m_i}$.

Lemma 17 *Let the notations and assumptions be as previously. There exists a uniform, bounded-error probabilistic algorithm over \mathbb{Q} that decides whether $W(a_{i+1})_\Delta$ is empty and, if not, computes a lifting fiber of $W(a_{i+1})_{\Delta \cdot m_{i+1}}$ in time $L(snd)^{O(1)}\delta^2$.*

Proof In Sect. 2.1 we saw that the equations $M_{s-i+1} = 0, \dots, M_s = 0$ intersect transversally at any of their common zeros belonging to V_{m_i} . Therefore, G_1, \dots, G_q and the polynomials representing M_{s-i+1}, \dots, M_s form a reduced regular sequence outside of $\{\Delta \cdot m_i = 0\}$. From Lemma 9 we deduce that m_i does not vanish identically on any irreducible component of $W(a_i)_\Delta$. Hence, the given lifting fiber of $W(a_i)_{\Delta \cdot m_i}$ is also a lifting fiber of $W(a_i)_\Delta$, and $G_1, \dots, G_q, M_{s-i+1}, \dots, M_s$ can be used as a lifting system of the lifting fiber of $\overline{W(a_i)_{\Delta \cdot m_i}}$.

Applying successively [19, Algorithms 4, 5, and 6] we produce a Kronecker parameterization of a suitable curve C in $\overline{W(a_i)_{\Delta \cdot m_i}}$ on which $\Delta \cdot m_i$ does not vanish identically.

Then we apply [19, Algorithm 2] to C, m_i , and $H \cdot \Delta \cdot m_{i+1}$ to obtain a lifting fiber of $(C \cap \{m_i = 0\})_{\Delta \cdot m_{i+1}}$.

Let N_{s-i}, \dots, N_s be the polynomials representing the $(s - i)$ minors of $T(a_{i+1})$ given by the columns numbered $1, \dots, s - i - 1$, to which we add, one by one, the columns $s - i, \dots, s$. In a way very similar to [19, Algorithm 10] we can remove the points of the given lifting fiber $(C \cap \{m_i = 0\})_{\Delta \cdot m_{i+1}}$ that are not zeros of N_{s-i}, \dots, N_s to obtain a lifting fiber of $\overline{W(a_{i+1})_{\Delta \cdot m_{i+1}}}$. The time cost of the whole procedure is a consequence of [19, Lemmas 3, 6, 14, and 16] □

We apply Lemma 16 and then 17 iteratively to obtain a lifting fiber of the zero-dimensional variety $W(a_r)_{\Delta \cdot m_r}$ and, hence, of $W(a_r)_\Delta$ by Lemma 9. Combining all previously described procedures we obtain the proposed main algorithm.

Theorem 18 *Let $n, d, p, r, q, s, L, \delta \in \mathbb{N}$, with $r = n - q$ and $s \geq p + r$, be arbitrary, and let G_1, \dots, G_q, H and $F_{k,l}$, for $1 \leq k \leq p, 1 \leq l \leq s$, be polynomials of $\mathbb{Q}[X_1, \dots, X_n]$ of degree at most d . Suppose that G_1, \dots, G_q form a reduced regular sequence outside of $\{H = 0\}$, the variety $V := \{G_1 = 0, \dots, G_q = 0\}_H$ is smooth, and the system degree of $G_1 = 0, \dots, G_q = 0, H \neq 0$, and $[F_{k,l}]_{1 \leq k \leq p, 1 \leq l \leq s}$ is at most δ .*

Furthermore, suppose that these polynomials are given as outputs of an essentially division-free arithmetic circuit β in $\mathbb{Q}[X_1, \dots, X_n]$ of size at most L . Let $a \in \mathbb{Q}^{(s-p) \times s}$ be a generic matrix. Then there exists a uniform, bounded-error probabilistic algorithm over \mathbb{Q} that decides from the input β in time $L(snd)^{O(1)}\delta^2 = (s(nd)^n)^{O(1)}$ whether $W(a_r)$ is empty and, if not, computes a geometric resolution of $W(a_r)$ (here, arithmetic operations and comparisons in \mathbb{Q} are taken into account at unit costs).

Proof This result is essentially a consequence of Lemmas 14, 15, 16, and 17. In fact, first we obtain for all $1 \leq j \leq r + 1$ lifting fibers of $W(a_r)_{\Delta_j}$. Then we change back the variables of the lifting fibers and find a primitive element common to all the fibers by means of [19, Algorithm 6] at a total cost of $O((snd)^{O(1)}\delta^2)$.

By means of classical greatest-common-divisor computations, we remove the points of $W(a_r)_{\Delta_2}$ that belong already to $W(a_r)_{\Delta_1}$. Then we remove the points of $W(a_r)_{\Delta_3}$ that belong already to $W(a_r)_{\Delta_1}$ and $W(a_r)_{\Delta_2}$. Recursively we remove the points of

$W(a_r)_{\Delta_j}$ that belong already to $W(a_r)_{\Delta_k}$ for $k < j$. The total cost of these operations remains bounded by $O((nd)^{O(1)}\delta)$. □

Remark 19 For any $n, d, p, r, q, s, L, \delta \in \mathbb{N}$, with $r = n - q$ and $s \geq p + r$, the probabilistic algorithm of Theorem 18 may be realized by an algebraic computation tree of depth $L(snd)^{O(1)}\delta^2 = (s(nd)^n)^{O(1)}$ that depends on parameters that may be chosen randomly. The proof of this statement requires a suitable refinement of Lemma 10 given earlier in the spirit of [22, Theorem 4.4], which exceeds the scope of this paper.

4.3 Checking Membership in a Degeneracy Locus

Finally, we will consider the computational task of deciding for any $x \in \mathbb{A}^n$ and any $1 \leq i \leq r$ whether x belongs to $W(a_i)$.

Proposition 20 *Let the notations and assumptions be as previously, let $1 \leq i \leq r$, and let $\mathbb{Q}[\alpha]$ be an algebraic extension of \mathbb{Q} of degree e , given by the minimal polynomial of α . Then there exists a bounded-error probabilistic algorithm \mathcal{B} that, for any point $x \in \mathbb{Q}[\alpha]^n$, decides in sequential time $O(e(L + s^{O(1)}) \log^{O(1)} e) = (esd^n)^{O(1)}$ whether x belongs to $W(a_i)$.*

For any $n, d, p, r, q, s, L \in \mathbb{N}$, with $r = n - q$ and $s \geq p + r$, the probabilistic algorithm \mathcal{B} may be realized by an essentially division-free arithmetic circuit of size $O(e(L + s^{O(1)} + n)^2 \log^{O(1)} e) = (esd^n)^{O(1)}$ that depends on parameters that may be chosen randomly.

Proof Checking the membership of x in V takes $O(L)$ operations in $\mathbb{Q}[\alpha]$. Each field operation in $\mathbb{Q}[\alpha]$ can be performed by $e \log^{O(1)} e$ operations in \mathbb{Q} . Lemma 12 now justifies the following probabilistic test whether $x \in V$ belongs to $W(a_i)$. With a high probability of success we can choose values u_i for the variables U_i , so that if we write $u^{(i)}$ (resp. u) for the corresponding specialization of $U^{(i)}$ (resp. of U), then the test becomes the verification of the conditions

$$\det(F(x) \cdot u) \neq 0 \quad \text{and} \quad \det(T(a_i)(x) \cdot u^{(i)}) = 0. \tag{4}$$

This leads to an additional cost of $e(L + s^{O(1)}) \log^{O(1)} e$.

The second part of Proposition 20 is a direct consequence of [22, Theorem 4.4]. □

4.4 Example

We will exemplify how our main algorithm runs on the following example. Let $n := 3$, $q := 1$, $G_1 := X_1^2 + X_2^2 + X_3^2$, $H := X_1X_2X_3$, $p := 1$, $s := 3$, $F_{1,1} := X_1$, $F_{1,2} := X_1X_2 + X_2^2$, $F_{1,3} := X_1X_3$, and $a := \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$. The variety $V = \{G_1 = 0\}_H$ is smooth of dimension $r := 2$. The algorithm starts representing a lifting fiber for V in the following way:

- G_1 as lifting system;
- $Y_1 := X_1 - X_2, Y_2 := X_2, Y_3 := X_3$ as new coordinates;
- $(-1, -1)$ as lifting point;
- $u := Y_3$ as primitive element;
- $Q := T^2 + 5$ as the minimal polynomial of u ;
- $v_3 := T$ as parameterization.

For the sake of simplicity, all the random choices made by the Kronecker routines are kept simple throughout this example. We took care to verify that they are generic enough to ensure the correctness of the computations.

As hitting sequence $b_1, b_2,$ and b_3 we choose the identity matrix and take $\mathbf{\Delta}_1 = X_1, \mathbf{\Delta}_2 = X_1X_2 + X_2^2, \mathbf{\Delta}_3 = X_1X_3$. Since $V_{\mathbf{\Delta}_1} = V_{\mathbf{\Delta}_3} = V$ holds, it is sufficient to carry out the computations for V_{Δ} , where $\Delta := \mathbf{\Delta}_1$. Hence, our lifting fiber is also a lifting fiber for V_{Δ} .

The lifting curve $V_{\Delta} \cap \{Y_1 = -1\}$ is described by the following equations: $T^2 + 2Y_2^2 - 2Y_2 + 1 = 0, Y_3 = T, Y_1 = 1$. The intersection of this curve with $\det(T(a_1)) = 3X_1 + 3X_1X_2 + 3X_2^2 - 3X_1X_3 = 3(Y_1 + Y_2)(1 + Y_2 - Y_3) + 3Y_2^2$ leads to the following lifting fiber for $W(a_1)$:

- $G_1, \det(T(a_1))$ as lifting system;
- $Y_1 := X_1 - X_2, Y_2 := X_2, Y_3 := X_3$ as new coordinates;
- (-1) as lifting point;
- $u := Y_2$ as primitive element;
- $Q := 6T^4 - 6T^3 + 3T^2 - 4T + 2$ as the minimal polynomial;
- $v_2 := T, v_3 := -6T^3 - T + 3$ as parameterization.

We verify that none of the points of this fiber annihilates $H, \Delta,$ or $m_1 := 2X_1 - X_1X_2 - X_2^2$. Hence, this lifting fiber is also a lifting fiber for $W(a_1)_{\Delta \cdot m_1}$.

The lifting curve for $W(a_1)_{\Delta \cdot m_1}$ is described by the following equations: $P(T) := 6T^4 + (10Y_1 + 4)T^3 + (8Y_1^2 + 6Y_1 + 1)T^2 + (4Y_1^3 + 2Y_1^2 + 2Y_1)T + Y_1^4 + Y_1^2 = 0, Y_2 = T, P'(T)Y_3 = (-8Y_1 + 4)T^3 + (-14Y_1^2 + 10Y_1)T^2 + (-10Y_1^3 + 8Y_1^2)T - 2Y_1^4 + 2Y_1^3$. The intersection of this curve with the hypersurface $\{m_1 = 0\}$ yields the following set of points:

$$\begin{aligned} \{Y_1^5 + 4Y_1^4 + 31Y_1^3 + 72Y_1^2 + 198Y_1 = 0, \\ Y_2 = \frac{-1}{198}Y_1^4 + \frac{7}{198}Y_1^3 - \frac{1}{22}Y_1^2 + \frac{3}{22}Y_1, \\ Y_3 = \frac{-1}{66}Y_1^4 - \frac{2}{33}Y_1^3 - \frac{31}{66}Y_1^2 - \frac{12}{11}Y_1\}. \end{aligned}$$

We observe that $(0, 0, 0)$ is the only point of this set that annihilates Δ or H . Therefore, the lifting fiber for $W(a_2)_{\Delta \cdot m_2}$ we find is represented by the following items:

- $G_1, \det(T(a_1)), m_1$ as lifting system;
- $Y_1 := X_1 - X_2, Y_2 := X_2, Y_3 := X_3$ as new coordinates;
- $u := Y_1$ as primitive element;
- $Q := T^4 + 4T^3 + 31T^2 + 72T + 198$ as the minimal polynomial;
- $v_1 := T, v_2 := \frac{1}{18}T^3 + \frac{1}{9}T^2 + \frac{1}{2}T + 1, v_3 := 3$ as parameterization.

We have implemented our main algorithm within the C++ library `geomsolvex` of `MATHEMAGIX` [33]. In fact, this implementation uses the strategy described in [19, Sect. 7.3]: we first choose a suitable prime number p that fits a machine word, compute the degeneracy locus modulo p , and then lift the geometric resolution to recover the solutions over the rational numbers.

5 Applications

In this section we complete the examples of Sects. 3.1 and 3.4. The other two examples of Sect. 3 may be adapted in a straightforward way to the context of Theorem 18. We refrain from presenting the details.

5.1 Polar Varieties

We consider first a somewhat modified version of the example of Sect. 3.1. Let $n \in \mathbb{N}$, $1 \leq p \leq n$, and $r := n - p$, and let G_1, \dots, G_p be a reduced regular sequence of polynomials of $\mathbb{Q}[X_1, \dots, X_n]$. We suppose that these polynomials are given by an essentially division-free arithmetic circuit in $\mathbb{Q}[X_1, \dots, X_n]$ of size L . From Lemma 10 we deduce that we may choose a hitting sequence (b_1, \dots, b_{r+1}) of regular matrices of $\mathbb{Z}^{n \times n}$ for $\{G_1 = 0, \dots, G_p = 0\}$ and the restriction of the Jacobian $J(G_1, \dots, G_p)$ to this variety. This yields p minors $\Delta_1, \dots, \Delta_{r+1}$ of $J(G_1, \dots, G_p) \cdot b_1, \dots, J(G_1, \dots, G_p) \cdot b_{r+1}$ such that

$$\bigcup_{1 \leq j \leq r+1} \{G_1 = 0, \dots, G_p = 0\}_{\Delta_j}$$

is the regular locus of $\{G_1 = 0, \dots, G_p = 0\}$.

Let $H := \sum_{1 \leq j \leq r+1} \Delta_j^2$, and assume that

$$\Gamma := \{G_1 = 0, \dots, G_p = 0\} \cap \mathbb{R}^n$$

is nonempty, smooth, and compact. Let $V := \{G_1 = 0, \dots, G_p = 0\}_H$, and let F be the restriction of $J(G_1, \dots, G_p)$ to V . Then V is nonempty, smooth, equidimensional of dimension r , and contains Γ . From [3, Proposition 1] or [4, Proposition 1] we conclude that, for $a \in \mathbb{Q}^{r \times n}$ generic, $W(a_r)$ contains for each connected component of Γ a real point. Let δ be the system degree of $G_1 = 0, \dots, G_p = 0$, $H \neq 0$, and $J(G_1, \dots, G_p)$. Then Theorem 18 implies that we can compute a sample point for any connected component of Γ in time $L(nd)^{O(1)}\delta^2 = (nd)^{O(n)}$. This result improves the complexity bound of [3, Theorem 11] and [4, Theorem 13] by a factor of $\binom{n}{p}$.

5.2 Dominant Endomorphisms of Affine Spaces

We treat now the example of Sect. 3.3 in the spirit of Theorem 18. Let F_1, \dots, F_n be in $\mathbb{Q}[X_1, \dots, X_n]$ such that (F_1, \dots, F_n) defines a birational endomorphism of \mathbb{A}^n .

Suppose that F_1, \dots, F_n are given by an essentially division-free arithmetic circuit in $\mathbb{Q}[X_1, \dots, X_n]$ of size L . Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Q}^n$ be generic. Then Theorem 18 can be used to compute a geometric solution of the polynomial equation system $F_1 - \alpha_1 = 0, \dots, F_n - \alpha_n = 0$ in time $L(nd)^{O(1)}\delta^2 = (nd)^{O(n)}$, where δ is the degree of the point-finding problem associated with $(\mathbb{A}^n, [F_1, \dots, F_n, 1])$. The main outcome of this result is that we may consider this degree as a natural invariant of the endomorphism of \mathbb{A}^n defined by (F_1, \dots, F_n) .

5.3 Timings

In this final subsection, we report on timings obtained with our software `geomsolvex`. For $n := 3$ we consider the following infinite family of examples, which are parameterized by an integer $N \geq 1$. For any $1 \leq j \leq N$, let $S_j := (X_1 - 4j)^2 + X_2^2 + X_3^2 - 1$, $p := 1$, and $G_1 := S_1 \cdots S_N - \epsilon$, where $\epsilon := 1/1000000$. It is clear that $\Gamma := \{G_1 = 0\} \cap \mathbb{R}^n$ is compact. On the other hand, the gradient of G_1 is given by

$$\begin{aligned} \frac{\partial G_1}{\partial X_1} &= 2(G_1 + \epsilon) \left(\frac{X_1 - 4}{S_1} + \frac{X_1 - 8}{S_2} + \dots + \frac{X_1 - 4N}{S_N} \right), \\ \frac{\partial G_1}{\partial X_2} &= 2X_2(G_1 + \epsilon) \left(\frac{1}{S_1} + \frac{1}{S_2} + \dots + \frac{1}{S_N} \right), \\ \frac{\partial G_1}{\partial X_3} &= 2X_3(G_1 + \epsilon) \left(\frac{1}{S_1} + \frac{1}{S_2} + \dots + \frac{1}{S_N} \right). \end{aligned}$$

We observe that $\frac{1}{S_1} + \frac{1}{S_2} + \dots + \frac{1}{S_N}$ does not vanish on Γ . In fact, the terms of this sum are necessarily positive on Γ since the open balls defined by $S_j < 0, 1 \leq j \leq N$, are all disjoint and $S_1 S_2 \cdots S_N$ is positive on Γ . Hence, Γ is smooth at any point $(x_1, x_2, x_3) \in \Gamma$, with $x_2 \neq 0$ or $x_3 \neq 0$. Thus, on singular points of Γ , the discriminant of the univariate polynomial $G_1(X_1, 0, 0)$ vanishes. Keeping this in mind we verified by a simple computation that Γ has no singular point for the values of N considered in our timings.

To make the equation $G_1 = 0$ dependent on generic coordinates, we replaced the variables X_1, X_2 , and X_3 with $3X_1 + 5X_2 + 7X_3, X_1 - X_2 + X_3$, and $-X_1 + 2X_2 + 5X_3$, respectively. Finally, for a we took $\begin{pmatrix} 1 & 17 & 7 \\ 11 & 23 & 13 \end{pmatrix}$. We used our software `geomsolvex` described in Sect. 5.1 and computed at least one point per connected component of Γ . Timings are reported in Table 1. We used the SVN revision number 8738 of `MATHEMAGIX` and compared it with version 3.21 of the `RAGLIB` library developed in

Table 1 Timings for polar varieties, in seconds

N	3	4	5	6	7	8	9
MATHEMAGIX	30	79	174	383	729	1,380	2,250
RAGLIB	1.2	3.1	19	126	748	3,202	13,021

MAPLE (TM) by M. Safey El Din [27], which in its turn relies on the FGB version 1.58 of J.-C. Faugère [15]. Our platform uses one core of an Intel Xeon CPU X5650 at 2.67 GHz with 48 GB. We observed that RAGLIB was much faster in small input sizes. Nevertheless, its cost increases faster than that of our probabilistic algorithm.

Acknowledgments The authors wish to thank Antonio Campillo (Valladolid, Spain) for stimulating conversations on the subject of this paper.

References

1. B. Bank, M. Giusti, J. Heintz, L. Lehmann, and L. M. Pardo, *Algorithms of intrinsic complexity for point searching in compact real singular hypersurfaces*, Found. Comput. Math. **12** (2012), no. 1, 75–122.
2. B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop, *Polar varieties and efficient real elimination*, Math. Z. **238** (2001), no. 1, 115–144.
3. B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Generalized polar varieties and an efficient real elimination*, Kybernetika **40** (2004), no. 5, 519–550.
4. B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Generalized polar varieties: geometry and algorithms*, J. Complexity **21** (2005), no. 4, 377–412.
5. B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and É. Schost, *On the geometry of polar varieties*, Appl. Algebra Eng. Commun. Comput. **21** (2010), no. 1, 33–83.
6. W. Bruns and U. Vetter, *Determinantal rings*, Lecture Notes in Mathematics, vol. 1327, Springer Berlin Heidelberg, 1988.
7. P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der mathematischen Wissenschaften, vol. 315, Springer Berlin Heidelberg, 1997.
8. P. Bürgisser and M. Lotz, *The complexity of computing the Hilbert polynomial of smooth equidimensional complex projective varieties*, Found. Comput. Math. **7** (2007), no. 1, 59–86.
9. A. Cafure and G. Matera, *Fast computation of a rational point of a variety over a finite field*, Math. Comp. **75** (2006), no. 256, 2049–2085.
10. M. Demazure, *Catastrophes et bifurcations*, Ellipses, Paris, 1989.
11. C. Duryve and G. Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Exp. Math. **26** (2008), no. 2, 101–139.
12. J. A. Eagon and M. Hochster, *R-sequences and indeterminates*, Quart. J. Math. Oxford Ser. (2) **25** (1974), 61–71.
13. J. A. Eagon and D. G. Northcott, *Ideals defined by matrices and a certain complex associated with them*, Proc. Roy. Soc. Ser. A **269** (1962), 188–204.
14. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.
15. J.-C. Faugère, *Fgb: A Library for Computing Gröbner Bases*, Mathematical Software - ICMS 2010 (K. Fukuda, J. van der Hoeven, M. Joswig, and N. Takayama, eds.), Lecture Notes in Comput. Sci., vol. 6327, Springer-Verlag, 2010, pp. 84–87.
16. W. Fulton, *Intersection theory*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 2, Springer-Verlag, Berlin, 1998.
17. M. Giusti, J. Heintz, K. Hägele, J. E. Morais, L. M. Pardo, and J. L. Montaña, *Lower bounds for Diophantine approximations*, J. Pure Appl. Algebra **117/118** (1997), 277–317.
18. M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo, *Straight-line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), no. 1-3, 101–146.
19. M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211.
20. J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277.
21. J. Heintz, G. Matera, and A. Weissbein, *On the time-space complexity of geometric elimination procedures*, Appl. Algebra Eng. Comm. Comput. **11** (2001), no. 4, 239–296.
22. J. Heintz and C.-P. Schnorr, *Testing polynomials which are easy to compute*, International Symposium on Logic and Algorithmic (Zurich, 1980) (Geneva), Monograph. Enseign. Math., vol. 30, Univ. Genève, 1982, pp. 237–254.

23. E. Kaltofen and B. D. Saunders, *On Wiedemann's method of solving sparse linear systems*, Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991), Lecture Notes in Comput. Sci., vol. 539, Springer, Berlin, 1991, pp. 29–38.
24. H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986, Translated from the Japanese by M. Reid.
25. D. Mumford, *The red book of varieties and schemes*, Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1988.
26. R. Piene, *Polar classes of singular varieties*, Ann. Sci. École Norm. Sup. (4) **11** (1978), no. 2, 247–276.
27. M. Safey El Din, *RAGLib (Real Algebraic Geometry Library)*, Maple (TM) package, from 2007, <http://www.polsys.lip6.fr/~safey/RAGLib>.
28. M. Safey El Din and Ph. Trébuchet, *Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry*, Tech. Report 6001, INRIA, 2006, <http://hal.inria.fr/inria-00105204>.
29. J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. Assoc. Comput. Mach. **27** (1980), no. 4, 701–717.
30. I. R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.
31. I. R. Shafarevich, *Basic algebraic geometry. 2*, second ed., Springer-Verlag, Berlin, 1994, Schemes and complex manifolds, Translated from the 1988 Russian edition by Miles Reid.
32. M. Turrel Bardet, *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*, Ph.D. thesis, Université Paris 6, 2004, <http://tel.archives-ouvertes.fr/tel-00449609>.
33. J. van der Hoeven, G. Lecerf, B. Mourain, et al., *Mathemagix*, from 2002, <http://www.mathemagix.org>.
34. W. Vogel, *Lectures on results on Bezout's theorem*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 74, Published for the Tata Institute of Fundamental Research, Bombay, 1984, Notes by D. P. Patil.
35. R. Zippel, *Probabilistic algorithms for sparse polynomials*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin, 1979, pp. 216–226.