Bit complexity for multi-homogeneous polynomial system solving
Application to polynomial minimization

Mohab Safey El Din
Sorbonne Universités, UPMC Univ Paris 06,
Inria, Paris Center, PolSys Project,
CNRS, LIP6 UMR 7606,
Mohab.Safey@lip6.fr

Éric Schost
University of Waterloo
David R. Cheriton School of Computer Science
eschost@uwaterloo.ca

May 19, 2016

Abstract

Multi-homogeneous polynomial systems arise in many applications. We provide bit complexity estimates for solving them which, up to a few extra other factors, are quadratic in the number of solutions and linear in the height of the input system under some genericity assumptions. The assumptions essentially imply that the Jacobian matrix of the system under study has maximal rank at the solution set and that this solution set if finite. The algorithm is probabilistic and a probability analysis is provided.

Next, we apply these results to the problem of optimizing a linear map on the real trace of an algebraic set. Under some genericity assumptions, we provide bit complexity estimates for solving this polynomial minimization problem.

1   Introduction

In this paper, we are interested in solving systems of polynomial equations with a multi-homogeneous structure (the polynomials we consider are actually affine, but can be seen as the dehomogenization of multi-homogeneous ones); we focus in particular on the bit

complexity aspects of this question. The main application we have in mind is the solution of some optimization problems, in particular for quadratic polynomials.

In all the paper, we use freely basic notions such as dimension, degree, reducibility and irreducibility, smoothness..., of algebraic sets, and we refer the reader to references such as [13, 39, 49, 53] for more details. In particular, given polynomials $\boldsymbol{f}$ with coefficients in a field $\mathbb{K}$, we denote by $V(\boldsymbol{f})$ their zero-set, over an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$.

We work with polynomials written in m groups of variables. Let thus $\boldsymbol{n} = (n_1, \ldots, n_m)$ be positive integers, and consider the variables $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_m)$, with $\mathbf{X}_1 = (X_{1,1}, \ldots, X_{1,n_1})$, $\ldots$, $\mathbf{X}_m = (X_{m,1}, \ldots, X_{m,n_m})$; we write $N = n_1 + \cdots + n_m$ for the total number of variables. With $\mathbb{K}$ as above, to a system $\boldsymbol{f} = (f_1, \ldots, f_N)$ in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ we associate the algebraic set $Z(\boldsymbol{f}) \subset V(\boldsymbol{f})$, defined as the set of all $\boldsymbol{x}$ in $\overline{\mathbb{K}}^N$ such that $\boldsymbol{f}(\boldsymbol{x}) = 0$ and such that the Jacobian matrix of $\boldsymbol{f}$ is invertible at $\boldsymbol{x}$ (remark that the system $\boldsymbol{f}$ has as many equations as unknowns). By the Jacobian criterion [13, Chapter 16], $Z(\boldsymbol{f})$ is a zero-dimensional (or empty) set, and it is defined over $\mathbb{K}$.

It is known that using the multi-degree structure of $\boldsymbol{f}$, that is, the partial degrees of these equations in $\mathbf{X}_1, \ldots, \mathbf{X}_m$, together with a multi-homogeneous Bézout bound, we can obtain finer estimates on the cardinality of $Z(\boldsymbol{f})$ than through the direct application of Bézout's theorem in many cases. In this paper, we focus on the case $\mathbb{K} = \mathbb{Q}$ and we show that the same phenomenon holds in terms of bit-size. From this, we deduce upper bounds on the cost of computing a representation of $Z(\boldsymbol{f})$.

Data structures. Let us first make our data representation explicit. Consider a zero-dimensional algebraic set $V \subset \overline{\mathbb{K}}^N$, defined over $\mathbb{K}$. A *zero-dimensional parametrization* $\mathscr{Q} = ((q, v_1, \ldots, v_N), \lambda)$ of V consists in polynomials $(q, v_1, \ldots, v_N)$, such that $q \in \mathbb{K}[T]$ is monic and squarefree, all v_i's are in $\mathbb{K}[T]$ and satisfy $\deg(v_i) < \deg(q)$, and in a $\mathbb{K}$-linear form λ in N variables, such that

- $\lambda(v_1, \ldots, v_N) = Tq' \bmod q$

- we have the equality $V = \left\{ \left(\frac{v_1(\tau)}{q'(\tau)}, \ldots, \frac{v_N(\tau)}{q'(\tau)} \right) \mid q(\tau) = 0 \right\}$;

the constraint on λ then says that the roots of q are precisely the values taken by λ on V. This definition implies that the linear form λ takes pairwise distinct values on the points of V; we call such linear forms *separating* and we say that $\mathscr{Q}$ is *associated to* λ.

This data structure has a long history, going back to work of Kronecker and Macaulay [30, 35], and has been used in a host of algorithms in effective algebra [1, 16, 17, 18, 19, 20, 34, 44]. The reason for using a rational parametrization with q' as a denominator is well-known [1, 20, 44]: when $\mathbb{K} = \mathbb{Q}$, and for systems without necessarily any kind of multi-homogeneous structure, it leads to a precise theoretical control on the size of the coefficients, which is verified in practice extremely accurately. A main purpose of this article is to show how such results, which are known for general systems, can be extended and refined to take into account multi-homogeneous situations.

Main result. Consider a polynomial f with coefficients in $\mathbb{Q}$. To measure its bit-size, we will use its *height*, defined as follows. First, for a in $\mathbb{Q} - \{0\}$, define the height of a, $\text{ht}(a)$, as $\max(\log(|n|), \log(d))$, with $n \in \mathbb{Z}$ and $d \in \mathbb{N}$ its minimal numerator and denominator. For $f = \sum_{\boldsymbol{c} \in C} f_{\boldsymbol{c}} X_1^{c_1} \cdots X_N^{c_N}$ non-zero in $\mathbb{Q}[X_1, \ldots, X_N]$, define $\text{ht}(f)$ as follows: let $d \in \mathbb{N}$ be the minimal common denominators of all coefficients $f_{\boldsymbol{c}}$, and let $\text{ht}(f)$ be the maximum of the logarithms of d and $\{d | f_{\boldsymbol{c}}|\}_{\boldsymbol{c} \in C}$ (which are integers).

When f has integer coefficients, this is simply the maximum of the logarithms of the absolute values of these coefficients. In general, knowing the degree and height of a polynomial with rational coefficients gives us an upper bound on the size of its binary representation.

The main results of this paper are stated in Section 3. Given polynomials $\boldsymbol{f} = (f_1, \ldots, f_N)$ in $\mathbb{Z}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, we show that $Z(\boldsymbol{f})$ admits a zero-dimensional parametrization where all polynomials have degree at most $\mathscr{C}$ and height $O\tilde{\ }(\mathscr{H} + N\mathscr{C})$, where $\mathscr{H}$ and $\mathscr{C}$ are respectively an arithmetic and a geometric measure of the "size" of $\boldsymbol{f}$, derived from its multi-degree and height; the $O\tilde{\ }$ indicates that we omit polylogarithmic factors. The quantity $\mathscr{C}$ is the usual multi-homogeneous Bézout number (so the degree bound is not new); $\mathscr{H}$ is an arithmetic analogue of it. In particular, the result above implies an upper bound of $O\tilde{\ }(N\mathscr{C}(\mathscr{H} + N\mathscr{C}))$ bits to represent the output. To establish this claim, we rely in a crucial manner on recent work by D'Andrea, Krick and Sombra [12].

From this we will deduce that such a representation can be computed by a randomized algorithm in boolean time that grows essentially like the product $\mathscr{C}\mathscr{H}$, up to a few extra other factors. Following references such as [17, 18, 19, 20, 34], we will represent the input polynomials $\boldsymbol{f}$ of our algorithm by means of a *straight-line program*, that is, a sequence of elementary operations $+, -, \times$ that computes the polynomials $\boldsymbol{f}$ from the input variables $X_1, \ldots, X_N$; the *length* E of such an objet is simply the number of operations it performs. The techniques used in the algorithm are not new: we first solve the system modulo a prime, using a symbolic homotopy algorithm that adapts to the multi-homogeneous case an algorithm given by Jeronimo *et al.* [26] for the sparse case; then, we use lifting techniques from [20] to recover the output over $\mathbb{Z}$. Taking into account our upper bound on the height of the output, this results in the first bound on the boolean cost of solving polynomial systems that involves their multi-homogeneous structure in such a manner.

Minimization problems. Let now $\boldsymbol{f} = (f_1, \ldots, f_p)$ be polynomials in $\mathbb{Z}[X_1, \ldots, X_n]$ and let $V \subset \mathbb{C}^n$ be the complex solution set of the system of equations $f_1 = \cdots = f_p = 0$. Consider the minimization problem $\min_{\boldsymbol{x} \in V \cap \mathbb{R}^n} \pi_1(\boldsymbol{x})$, where $\pi_1 : (x_1, \ldots, x_n) \mapsto x_1$ is the projection on the first coordinate axis. This question appears in many applications and has attracted a lot of attention from the scientific community, with methodologies ranging from approximate sums of squares [31, 32, 41], exact sums of squares [24, 40, 47], critical point methods [5, 21, 22], etc.

A particularly important situation is the *quadratic case*, where all equations have degree at most 2. As an illustration, one may mention the *Celis-Dennis-Tapia (CDT) problem* [9], to minimize a non-convex quadratic function over the intersection of two ellipsoids, which can be turned into an instance of the problem above by introducing a new dummy variable.

Such problems arise naturally in iterative non-linear optimization procedures where in one iteration step, the objective function and the constraints are approximated by quadratic models.

The quadratic case in polynomial optimization is known to be solvable in time polynomial in n, with an exponent that depends only on p [4, 23]. Still, general quadratic minimization problems, and the CDT likewise, still pose challenging difficulties, both from the theoretical and algorithmic perspective, and many articles have treated these and related problems [6, 7, 8, 10, 42, 52].

Prior works. Provided the algebraic set V is smooth, our minimization problem can be handled by computing the critical points of the restriction of π_1 to $V \cap \mathbb{R}^n$. If we let D be the maximum of the degrees of the input polynomials, it is known that these critical points can be computed in time $D^{O(n)}$ [5, Section 14.2] in an *algebraic complexity model*, counting arithmetic operations in the base field $\mathbb{Q}$ at unit cost.

More precisely, using Gröbner bases techniques, papers [14] and [51] establish that if the polynomials $f_1, \ldots, f_p$ are generic enough, this computation can done using

$$O\left(\binom{n + D_{\mathrm{reg}}}{n}^\omega + \left(D^p(D-1)^{n-p}\binom{n-1}{p-1}\right)^\omega\right)$$

operations in $\mathbb{Q}$, with $D_{\mathrm{reg}} = D(p-1) + (D-2)n + 2$, and where ω is such that computing the row echelon form of a matrix of size $k \times k$ is done in time $O(k^\omega)$. In the quadratic case, this becomes

$$O\left(\binom{n + 2p}{2p}^\omega + \left(2^p\binom{n-1}{p-1}\right)^\omega\right) \subset O((n + 2p)^{2p\omega})$$

operations in $\mathbb{Q}$. The best known value for ω is $\omega < 2.38$ [33]; in the often discussed case where p is constant, the cost is then $O(n^{4.76p})$. For the CDT problem, we have $p = 3$, so that generic instances of it can be solved using $O(n^{14.28})$ arithmetic operations.

As mentioned above, the quadratic case has actually been known to be solvable in $n^{O(p^2)}$ arithmetic operations since Barvinok's paper [4]; this was later improved to $n^{O(p)}$ in [23]. The algorithms are deterministic, and make no assumption on the input system, but the constant in the big-O exponent is not specified. In [27], Jeronimo and Perrucci give a randomized algorithm to compute the minimum of a function on a basic semi-algebraic set. In our setting, with $D = 2$ and p fixed, the running time is $O^\sim(n^{2p+5} + n^{3p})$ arithmetic operations.

Fewer references discuss bit complexity. When $p = 1$, [36, Prop. 3.8 and Lemma 4.1] give boolean complexity estimates of the form $O^\sim(\tau D^{3n})$ for critical point computation on a hypersurface, under some genericity assumptions on the input; here, τ is an upper bound on the height of the input polynomials. Height bounds on the minimum polynomial defining $\min_{\boldsymbol{x} \in V \cap \mathbb{R}^n} \pi_1(\boldsymbol{x})$ are given in [28]; as we will see, they turn out to be of the same order as the ones we will derive below, but no algorithm with bit complexity depending on these bounds is given. Finally, in the quadratic case, the results of Grigoriev and Pasechnik [23] carry over to the boolean case.

Our contributions. We will show how to handle *generic* instances of the optimization problem above using our algorithm for multi-homogeneous systems.

This is done by considering the Lagrange system in $N = n + p$ variables

$$f_1 = \cdots = f_p = 0, \qquad L_1 \frac{\partial f_1}{\partial X_j} + \cdots + L_p \frac{\partial f_p}{\partial X_j} = 0 \text{ for } 2 \le j \le n, \qquad u_1 L_1 + \cdots + u_p L_P = 1$$

where $\mathbf{L} = L_1, \ldots, L_p$ are new variables and $(u_1, \ldots, u_p) \ne \mathbf{0}$ are chosen at random. As we will see, in generic situations, the projection on the $(X_1, \ldots, X_n)$-space of the complex solution set of this system is finite, and coincides with the set of critical points of π_1 on V. Such a system possesses a bi-homogeneous structure, with p equations of degree at most D, resp. 0 in variables $\mathbf{X}$, resp. $\mathbf{L}$ (we will then speak of bidegree $(D, 0)$), $n - 1$ equations of bidegree at most $(D - 1, 1)$ and one equation of bidegree $(0, 1)$.

We prove in Section 4 that we can solve the bi-homogeneous system above in randomized time

$$O^\sim \left(p(E + n)\tau' + n^3 \binom{n-1}{p-1} \binom{n}{p} (\tau + D) D^{2p} (D - 1)^{2(n-p)} (pE + nD + n^2) \right),$$

where τ is the height of the input polynomials, E is the length of the straight-line program that computes them, and τ' is the height of the integers that appear in this straight-line program (in most cases, one expects $\tau' \le \tau$, in which case the first term disappears). The degree $\mathscr{C}$ of the output is at most $\binom{n-1}{p-1} D^p (D - 1)^{n-p}$, and its height $\mathscr{H}$ is $O^\sim \left(n \binom{n}{p} (\tau + D) D^p (D - 1)^{n-p} \right)$.

One can always construct a naive straight-line program for the input polynomials, simply by computing all monomials they involve and summing them. In this case, one can take $E \in O(p \binom{n+D}{n})$ and $\tau' = \tau$, which leads to a boolean runtime of the form

$$O^\sim \left(\binom{n-1}{p-1} \binom{n}{p} \binom{n+D}{n} (\tau + D) D^{2p} (D - 1)^{2(n-p)} \right).$$

Taking $p = 1$ as in [36], this is $O^\sim \left((\tau + D) D^{n+2} (D - 1)^{2(n-1)} \right)$. In this case, for large D, our result is hardly an improvement over the cost $O^\sim(\tau D^{3n})$ obtained in that reference.

The gain is much more significant in the case $D = 2$. In this case, we can take $E \in O(pn^2)$ and $\tau' = \tau$. As a result, we obtain a running time of $O^\sim(n^5 \binom{n-1}{p-1} \binom{n}{p} \tau 2^{2p})$ for the quadratic case, for an output of degree $\mathscr{C}$ at most $\binom{n-1}{p-1} 2^p$, and of height $\mathscr{H}$ in $O^\sim(n \binom{n}{p} \tau 2^p)$: when the codimension p is fixed, all these quantities are *polynomial* in n. This refines the complexity results in [23], which featured the same property but with no such precise control on the exponent, and those in [36], which would be $O^\sim(\tau 2^{3n})$ in this case. Remark that the bit-size bounds on the output are essentially the same as those obtained in [28] for related objects, namely the minimal polynomial of the algebraic number $\min_{\mathbf{x} \in C} \pi_1(\mathbf{x})$, for any compact connected component C of $V \cap \mathbb{R}^n$.

We end this section with an easy consequence of the above result, concerning the determination of an isolating interval for $\min_{\mathbf{x} \in V \cap \mathbb{R}^n} \pi_1(\mathbf{x})$. The output of our algorithm describes

a finite set in the $\mathbf{X}, \mathbf{L}$-space whose projection on the $\mathbf{X}$-space is the set of critical points of π_1 on V. From the zero-dimensional parametrization of this set, using root isolation algorithms as in [36, Section 3], we can then compute boxes of side $2^{-\kappa}$ around all roots of the system using $O\tilde{\ }(n\mathscr{C}^2\mathscr{H} + n\mathscr{C}\kappa)$ bit operations, with $\mathscr{C}$ and $\mathscr{H}$ the bounds on the output degree and height mentioned above. For instance, in the quadratic case, this is $O\tilde{\ }(n^2\binom{n-1}{p-1}^2\binom{n}{p}\tau 2^{3p} + n\binom{n-1}{p-1}2^p\kappa)$ bit operations, so the whole process is polynomial in n for fixed p. For instance, with $p = 3$ as in the CDT problem, the overall cost is $O\tilde{\ }(n^{10}\tau + n^3\kappa)$.

Plan of the paper. Section 2 proves degree bounds for systems defined by polynomial systems with a multi-homogeneous structure, and gives a symbolic homotopy deformation algorithm dedicated to these cases. Section 3 follows a similar pattern, but discusses height bounds and computation over the rationals, with a cost analysis in the boolean model. We finally apply this to our minimization problem in Section 4.

2 Degree bounds and the multi-homogeneous homotopy

In this section, we work over a perfect field $\mathbb{K}$, using N variables $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_m$ partitioned into m blocks, as explained in the introduction. Our goal here is to recall the multi-projective Bézout bound associated to a system $\boldsymbol{f} = (f_1, \ldots, f_N)$, and give a symbolic homotopy algorithm to compute $Z(\boldsymbol{f})$, for use in the next section. These results are for a substantial part not new. The algorithm can in particular be seen as a modification of that in [26]; we do however have to give a rather detailed presentation, for reasons explained in Subsection 2.2.

We will use a generalization of the notation $Z(\boldsymbol{f})$ introduced before to input systems $\boldsymbol{f} = (f_1, \ldots, f_M)$, with now $M \leq N$; this is defined as the union of the irreducible components of $V(\boldsymbol{f})$ over which the Jacobian matrix $\mathrm{jac}(\boldsymbol{f})$ has (generically) maximal rank. This algebraic set is either empty or $(N - M)$-equidimensional. We recall that the degree of an equidimensional algebraic set is the maximum (and generic) number of intersection points with a linear space of complementary dimension. In dimension zero, this is simply the cardinality.

Finally, in addition to algebraic sets in an affine space such as $\overline{\mathbb{K}}^n$, which are called affine, in the sequel we will also consider projective and multi-projective ones, which lie in a projective space $\mathbb{P}^n(\overline{\mathbb{K}})$, or product of projective spaces $\mathbb{P}^{n_1}(\overline{\mathbb{K}}) \times \cdots \times \mathbb{P}^{n_m}(\overline{\mathbb{K}})$.

2.1 Degree bounds

Consider the ring of truncated power series

$$A^*(\mathbb{P}^{\boldsymbol{n}}) = \mathbb{Z}[\vartheta_1, \ldots, \vartheta_m]/\langle \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1} \rangle;$$

this is the so-called *Chow ring* of the multi-projective space $\mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1}(\overline{\mathbb{K}}) \times \cdots \times \mathbb{P}^{n_m}(\overline{\mathbb{K}})$ over $\overline{\mathbb{K}}$, or any given algebraically closed field. Given an m-uple $d = (d_1, \ldots, d_m)$ in $\mathbb{N}^m$, we define the expression

$$\{d\} = d_1 \vartheta_1 + \cdots + d_m \vartheta_m.$$

To a sequence $\boldsymbol{d} = (d_1, \ldots, d_M)$ of such m-uples, we associate

$$\{\boldsymbol{d}\} = \{d_1\} \cdots \{d_M\} \bmod \langle \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1} \rangle \in A^*(\mathbb{P}^{\boldsymbol{n}});$$

note that all monomials appearing in this expression have total degree M; then, we define a useful quantity, $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$, as

$$\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = \sum_{(a_i)_{1 \le i \le m} \in \mathbb{N}^m, \ a_1 + \cdots + a_m = M} \operatorname{coeff}(\{\boldsymbol{d}\}, \vartheta_1^{a_1} \cdots \vartheta_m^{a_m});$$

remark that the coefficients appearing in this expression are the only (possibly) non-zero coefficients of $\{\boldsymbol{d}\}$.

Finally, to a polynomial f in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ we associate its *multi-degree* $\operatorname{mdeg}(f) = (d_1, \ldots, d_m) \in \mathbb{N}^m$, with $d_i = \deg(f, \mathbf{X}_i)$ for all i. When comparing multi-degrees, we use the (partial) componentwise order, so that saying that f has multi-degree at most $d = (d_1, \ldots, d_m)$ means that $\deg(f, \mathbf{X}_i) \le d_i$ holds for all i. Similarly, to a system $\boldsymbol{f} = (f_1, \ldots, f_M)$, we associate its multi-degree $\operatorname{mdeg}(\boldsymbol{f}) = (\operatorname{mdeg}(f_1), \ldots, \operatorname{mdeg}(f_M))$. Saying that $\boldsymbol{f}$ has multi-degree at most $\boldsymbol{d} = (d_1, \ldots, d_M)$, with now all $d_i = (d_{i,1}, \ldots, d_{i,m})$ in $\mathbb{N}^m$, means that $\deg(f_i, \mathbf{X}_j) \le d_{i,j}$ holds for all i, j. Then, the following degree inequality is proved in [46, Chapter 11].

Proposition 1. *Let* $\boldsymbol{f} = (f_1, \ldots, f_M)$ *be a polynomial system in* $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, *with* $\operatorname{mdeg}(\boldsymbol{f}) \le \boldsymbol{d}$. *Then,* $Z(\boldsymbol{f})$ *has degree at most* $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$.

In particular, if $M = N$, $Z(\boldsymbol{f})$ has degree (that is, cardinality) at most $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$, and thus all polynomials appearing in a zero-dimensional parametrization of it have degree at most $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$. This latter claim is not new; see for instance [37].

Finally, we will need the following notation below. Given $\boldsymbol{d} = (d_1, \ldots, d_M)$ as above, with $d_i = (d_{i,1}, \ldots, d_{i,m})$ for all i, we define the tuple $\boldsymbol{d}'$ as $\boldsymbol{d}' = (d_1', \ldots, d_M')$, with $d_i' = (1, d_{i,1}, \ldots, d_{i,m}) \in \mathbb{N}^{m+1}$ for all i, together with $\boldsymbol{n}' = (1, n_1, \ldots, n_m)$. Geometrically, this corresponds to adding one new variable (written t below) and considering polynomials of degree 1 in t and multi-degree $\boldsymbol{d}$ in $\mathbf{X}_1, \ldots, \mathbf{X}_m$.

2.2   The multi-homogeneous homotopy

Let us now consider polynomials $\boldsymbol{f} = (f_1, \ldots, f_N)$ in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ and show how to compute a zero-dimensional parametrization of the algebraic set $Z(\boldsymbol{f})$. For this, we use a symbolic adaptation of multi-homogeneous homotopy continuation algorithms. In the context of numerical continuation techniques, this approach is detailed in [50] and references therein; in a symbolic context, the algorithm underlying the following proposition is inspired by e.g. the one in [25], that applies in the bi-homogeneous case.

Proposition 2. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ has multi-degree at most $\boldsymbol{d} = (d_1, \ldots, d_N)$, with all d_i in $\mathbb{N}^m$, and that $\boldsymbol{f}$ is given by a straight-line program Γ of size L; suppose further that $\mathbb{K}$ has characteristic either zero or at least e, where*

$$e = \max\left(\max_{1 \leq j \leq m} d_{1,j} + \cdots + d_{N,j}, 8(N-1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2\right).$$

There exists an algorithm NonsingularSolutions *that takes Γ and $\boldsymbol{d}$ as input and that outputs one of the following:*

- *either a zero-dimensional parametrization of $Z(\boldsymbol{f})$,*

- *or a zero-dimensional parametrization of a subset of $Z(\boldsymbol{f})$,*

- *or* fail*.*

The first outcome occurs with probability at least $7/8$. In any case, the algorithm uses

$$O^{\sim}\left(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')\left(L + \sum_{1 \leq i \leq N, 1 \leq j \leq m} d_{i,j} + N^2\right)N\right)$$

operations in $\mathbb{K}$, where we write $\boldsymbol{d}' = (d_1', \ldots, d_N')$, with $d_i' = (1, d_{i,1}, \ldots, d_{i,m})$ for all i and $\boldsymbol{n}' = (1, n_1, \ldots, n_m)$.

In particular, running the algorithm k times, we obtain a zero-dimensional parametrization of $Z(\boldsymbol{f})$ among our k outputs with probability at least $1 - 1/8^k$; in that case, since all other possible outputs have degree less than $Z(\boldsymbol{f})$, we identify the correct outputs as the ones with highest degree.

As a matter of comparison, in the bi-homogeneous case, the algorithm in [25] has cost at least $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^5\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')^6$. Closer to us are two algorithms from [20] and [26]. The geometric resolution algorithm of [20] solves our questions in time quadratic in a particular geometric degree associated to the input system; however, in general, this degree cannot be controlled in terms of the quantities $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ and $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$ used in our analysis; in addition, we are not aware of a probability analysis for it, and we will need such an analysis in the next section.

The algorithm of [26] deals with symbolic homotopies for sparse systems, with a running time that would be comparable to ours in the case of multi-homogeneous systems. However, that algorithm requires a base field of characteristic zero (whereas we will need it over a finite field), and the system $\boldsymbol{f}$ must be zero-dimensional (which is not the case for us); in addition, the last step of that algorithm, specialization at $t = 1$ (Section 6.2 in [26]) appears to overlook issues that we discuss below, inspired by [45, Section 4]. For these reasons, lacking another reference, we decided to include a self-contained proof dedicated to our multi-homogeneous situation.

Without loss of generality, in what follows, we suppose that all polynomials f_i are non-constant

The start system. The following construction is from [25] (however, the cost estimates below are new). For any integers i, j, with j in $\{1, \ldots, m\}$, let us define the affine polynomial

$$L_i(\mathbf{X}_j) = X_{j,1} + iX_{j,2} + \cdots + i^{n_j-1}X_{j,n_j} + i^{n_j}.$$

Next, considering non-negative integers $d = (d_1, \ldots, d_m)$ and $e = (e_1, \ldots, e_m)$, we define the polynomial

$$g_{d,e} = \prod_{j=1}^{m} \prod_{\ell=0}^{d_j-1} L_{\ell+e_j}(\mathbf{X}_j).$$

The following result is straightforward, once one notices that for any i, $L_i(\mathbf{X}_j)$ has multi-degree $(0, \ldots, 0, 1, 0, \ldots, 0)$, with 1 at the j-th entry.

Lemma 3. *The polynomial $g_{d,e}$ has multi-degree d.*

Finally, given multi-degrees $\boldsymbol{d} = (d_1, \ldots, d_N)$, with each d_i in $\mathbb{N}^m$, we define the system $\mathbf{g} = (g_1, \ldots, g_N)$ by

$$g_i = g_{d_i, d_1 + \cdots + d_{i-1}} = \prod_{j=1}^{m} \prod_{\ell=0}^{d_{i,j}-1} L_{\ell+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j), \qquad 1 \le i \le N.$$

Lemma 4. *Suppose that $\mathbb{K}$ has characteristic zero, or at least $\max_{1 \le j \le m} d_{1,j} + \cdots + d_{N,j}$, and that for all i, d_i is different from $(0, \ldots, 0)$. Then the following holds:*

- *for i in $\{1, \ldots, N\}$, g_i has multi-degree d_i;*

- *one can compute $\mathbf{g}$ by means of a straight-line program of length $O^{\sim}(\sum_{i,j} d_{i,j})$;*

- *$\mathbf{g}$ has $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ roots, and one can compute all of them using $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$ operations in $\mathbb{K}$;*

- *the Jacobian matrix of $\mathbf{g}$ is invertible at all these roots.*

Proof. The first claim follows directly from Lemma 3. Recall next that $g_i(\mathbf{X})$ takes the form

$$g_i(\mathbf{X}) = \prod_{j=1}^{m} \prod_{\ell=0}^{d_{i,j}-1} L_{\ell+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j).$$

We actually start by fixing j in $\{1, \ldots, m\}$. For such a fixed j, we have to evaluate all linear forms $L_{\ell+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j)$, for $i = 1, \ldots, N$ and $\ell = 0, \ldots, d_{i,j} - 1$. Due to the shape of these linear forms, each such evaluation amounts to computing the value of the polynomial $X_{j,1} + X_{j,2}T + \cdots + X_{j,n_j}T^{n_j-1} + T^{n_j}$ at $\ell + d_{1,j} + \cdots + d_{i-1,j}$. This polynomial has degree less than n_j, and we have to evaluate it at $\sum_{i=1,\ldots,N} d_{i,j}$ points, so using fast multipoint evaluation [15, Chapter 10], this can be done in $O^{\sim}(n_j + \sum_i d_{i,j})$ operations.

Taking all j into account, the overall time for evaluating these linear forms is $O\tilde{}(N + \sum_{i,j} d_{i,j})$ operations. Because for all $i = 1, \ldots, N$, $\sum_{j=1,\ldots,m} d_{i,j}$ is at least equal to 1 (otherwise, we would have $d_i = (0, \ldots, 0)$), this is $O\tilde{}(\sum_{i,j} d_{i,j})$. The cost needed to deduce all $g_i(\mathbf{X})$ themselves is $O(\sum_{i,j} d_{i,j})$. This proves the second item.

For the third point, remark first that the solutions of the system $\mathbf{g} = 0$ are obtained by cancelling one factor in each g_i. For any given j in $\{1, \ldots, m\}$, our assumption on the characteristics of the base field implies that the affine forms $L_{\ell+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j)$ showing up in the definition of $g_1, \ldots, g_N$ are pairwise distinct, and thus (since they form a Vandermonde system) linearly independent. Thus, if we choose more than n_j forms involving $\mathbf{X}_j$, we obtain an inconsistent linear system for $\mathbf{X}_j$. As a result, the solutions are obtained by choosing n_1 linear equations for $\mathbf{X}_1, \ldots, n_m$ linear equations for $\mathbf{X}_m$. There are $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ such choices; for any of these choices, we recover the value of each $\mathbf{X}_j$ by solving a Vandermonde linear system; this can be done in quasi-linear time $O\tilde{}(N)$ [15, Chapter 10].

Finally, to prove that all solutions are multiplicity-free, remark that locally around any of these solutions, the system is equivalent to a linear system (since once we have chosen linear equations to define the values of $\mathbf{X}_1, \ldots, \mathbf{X}_m$, all other linear equations are non-zero). $\qquad\square$

The curve $\mathscr{Z}$. We now construct the homotopy itself. Given equations $\boldsymbol{f} = (f_1, \ldots, f_N)$ with multi-degrees $\boldsymbol{d} = (d_1, \ldots, d_N)$, with all d_i in $\mathbb{N}^m$, we define the system $\mathbf{g}$ as above, together with the equations

$$\boldsymbol{f}_t = t\boldsymbol{f} + (1-t)\mathbf{g} \in \mathbb{K}[t, \mathbf{X}],$$

for a new variable t. We make the same assumption on the characteristics of the base field as in the previous lemma (the assumptions on the d_i's is satisfied, since we assume that none of the f_i's is constant).

Remark that $\boldsymbol{f}_t(0, \mathbf{X}) = \mathbf{g}$ and $\boldsymbol{f}_t(1, \mathbf{X}) = \boldsymbol{f}$. Adding a new "block" of variables consisting only of t, the system $\boldsymbol{f}_t$ is seen to have multi-degree $\boldsymbol{d}' = (d'_1, \ldots, d'_N)$, with $d'_i = (1, d_{i,1}, \ldots, d_{i,m})$ for all i; as said above, we correspondingly define $\boldsymbol{n}' = (1, n_1, \ldots, n_m)$.

The system $\boldsymbol{f}_t$ may not necessarily define a curve in $\overline{\mathbb{K}}^{N+1}$ (for instance if $\boldsymbol{f} = -\mathbf{g}$, the fiber above $t = 1/2$ has dimension N). Let us then define the algebraic set $\mathscr{Z}$ as the Zariski closure of $V(\boldsymbol{f}_t) - V(D)$, where D is the determinant of the Jacobian matrix $\mathrm{jac}(\boldsymbol{f}_t, \mathbf{X})$ of $\boldsymbol{f}_t$ with respect to $\mathbf{X}_1, \ldots, \mathbf{X}_m$. Finally, let $\pi : \overline{\mathbb{K}}^{N+1} \to \overline{\mathbb{K}}$ denote the projection on the t-axis.

Lemma 5. *The algebraic set $\mathscr{Z}$ has dimension one, the image by π of each of its irreducible components is dense, and it has degree at most $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$.*

Proof. The so-called Lazard Lemma [38] implies the dimension claims; as a result, we can apply Proposition 1 to obtain the degree bound. $\qquad\square$

Let $\mathscr{I} \subset \mathbb{K}[t, \mathbf{X}]$ be the ideal $\langle \boldsymbol{f}_t \rangle : D^\infty$, so that $\mathscr{Z}$ is the zero-set of $\mathscr{I}$. Let us further denote by $\mathfrak{J}$ the extension of $\mathscr{I}$ to $\mathbb{K}(t)[\mathbf{X}]$, and by $\mathfrak{Z} \subset \overline{\mathbb{K}(t)}^N$ its zero-set; the Jacobian criterion implies that $\mathfrak{J}$ is radical, and that $\mathfrak{Z}$ has dimension zero. Let then λ be a linear form with coefficients in $\mathbb{K}$ that separates the points of $\mathfrak{Z}$ (we will discuss our choice for it further

on). To λ, we can associate a zero-dimensional parametrization $\mathscr{Q} = ((q, v_1, \ldots, v_N), \lambda)$ of $\mathfrak{Z}$, where all polynomials have coefficients in $\mathbb{K}(t)$. The previous lemma and Theorem 1 in [48] imply the following bound.

Lemma 6. *The numerator and denominator of all coefficients of all polynomials $q, v_1, \ldots, v_N$ have degree at most $\mathscr{C}_{\boldsymbol{n'}}(\boldsymbol{d'})$.*

Specialization properties. In our main algorithm, we use a classical tool, *lifting techniques*: to compute $\mathscr{Q}$, we compute the specialization of it at $t = 0$, lift it to a sufficient precision in t, and recover $\mathscr{Q}$. Once we know $\mathscr{Q}$, we want to let $t = 1$ in it, in order to obtain a zero-dimenzional parametrization for $Z(\boldsymbol{f})$. In this paragraph, we give properties that underlie this process. First, we describe the situation at $t = 0$.

Lemma 7. *If a linear form λ with coefficients in $\mathbb{K}$ is a separating element for $Z(\mathbf{g})$, it is separating for $\mathfrak{Z}$. When it is the case, t divides no denominator in the corresponding zero-dimensional parametrization $\mathscr{Q} = ((q, v_1, \ldots, v_N), \lambda)$ of $\mathfrak{Z}$, and letting $t = 0$ in these polynomials yields a zero-dimensional parametrization of $Z(\mathbf{g})$.*

Proof. Consider the power series in $\overline{\mathbb{K}}[[t]]$ obtained by lifting the points of $Z(\mathbf{g})$ to solutions of $\boldsymbol{f}_t$ using Newton iteration; call them $\Gamma_1, \ldots, \Gamma_c$, with all Γ_i in $\overline{\mathbb{K}}[[t]]^N$ and $c = \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$.

Because there are $c = \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ such solutions, and $\mathfrak{I}$ can have at most c solutions (Proposition 1), these power series are the *only* solutions of the extension of $\mathfrak{I}$ to $\overline{\mathbb{K}}((t))[\mathbf{X}]$. The following well-known interpolation formulas

$$q = \prod_{\boldsymbol{x} \in \mathfrak{Z}} (T - \lambda(\boldsymbol{x})), \quad v_i = \sum_{\boldsymbol{x} = (x_1, \ldots, x_N) \in \mathfrak{Z}} x_i \prod_{\boldsymbol{x}' \in \mathfrak{Z}, \ \boldsymbol{x}' \neq \boldsymbol{x}} (T - \lambda(\boldsymbol{x})) \quad (1 \leq i \leq N). \qquad (1)$$

define $\mathscr{Q}$; they show that all polynomials q and $v_1, \ldots, v_N$ have non-negative valuation at $t = 0$ and prove our claims. $\qquad \square$

The situation at $t = 1$ is more complex, since $\boldsymbol{f}$ may have fewer than $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ roots. To state the relevant construction, we will need power series centered at $t = 1$ (and generalizations thereof). Thus, we let $\tau = t - 1$, and work with polynomials and power series written in τ (the system $\boldsymbol{f}_t$ written in terms of τ becomes $\boldsymbol{f}_\tau$). Let $\varphi_1, \ldots, \varphi_s$ be the points in $Z(\boldsymbol{f})$; they belong to $\overline{\mathbb{K}}^N$. Because the Jacobian matrix of $\boldsymbol{f}$ is invertible at these points, we can use Newton iteration to lift them to power series $\Phi_1, \ldots, \Phi_s$ in $\overline{\mathbb{K}}[[\tau]]^N$ that cancel $\boldsymbol{f}_\tau$.

We will in fact need to describe all solutions of $\boldsymbol{f}_\tau$; for this, we use a slight generalization of the presentation in [45]. That paper describes such solutions in characteristic zero, where this is done by means of Puiseux series; in arbitrary characteristic, this is not enough, so we will rely on the fact that the ring $\mathbb{L}$ of all "generalized power series" $F = \sum_{i \in I} f_i \tau^i$, where the index set $I \subset \mathbb{Q}$ (that depends on F) is well-ordered and all f_i's are in $\overline{\mathbb{K}}$, contains an algebraic closure of $\overline{\mathbb{K}}((\tau))$ [43].

Because the exponent support is well-ordered, we can define the *valuation* of such a (non-zero) F as the rational $\nu(F) = \min(i \in I, \ f_i \neq 0)$; this extends the τ-adic valuation

on $\overline{\mathbb{K}}((\tau))$. For such an element F, if $\nu(F) \geq 0$, we write $\ell_0(F)$ for the coefficient of τ^0 in the expansion of F (and we extend this notation to vectors).

We will ensure below that we can indeed apply Lemma 7; as a consequence, $\boldsymbol{f}_\tau$ has $c = \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ pairwise distinct roots in an algebraic closure of $\overline{\mathbb{K}}((\tau))$. These roots can then be written as $\Phi_1, \ldots, \Phi_c$, with all Φ_i in $\mathbb{L}^N$; up to reordering them, we can assume that the first s of them are the power series $\Phi_1, \ldots, \Phi_s$ defined previously. Let further $c' \geq s$ be such that $\Phi_1, \ldots, \Phi_{c'}$ have all their coordinates with non-negative valuations. We can then define $\varphi_1, \ldots, \varphi_{c'}$ as the vectors in $\overline{\mathbb{K}}^N$ obtained as $\varphi_i = \ell_0(\Phi_i)$ for all i. Although these vectors may not be pairwise distinct, the following lemma shows that $\varphi_1, \ldots, \varphi_s$ appear only once in that sequence.

Lemma 8. *For $i = 1, \ldots, s$ and $i' = s+1, \ldots, c'$, $\varphi_i \neq \varphi_{i'}$ holds.*

Proof. Take i and i' as above. By Newton iteration, we know that Φ_i is the unique vector of power series in $\overline{\mathbb{K}}[[\tau]]$ that cancels $\boldsymbol{f}_\tau$ and such that $\ell_0(\Phi_i) = \varphi_i$. Hence, the only case we have to exclude is $\Phi_{i'}$ being a vector in $\mathbb{L}^N - \overline{\mathbb{K}}[[\tau]]^N$ and with $\ell_0(\Phi_{i'}) = \varphi_i$.

Suppose it is the case. By assumption, $\Phi_{i'}$ is not in $\overline{\mathbb{K}}[[\tau]]^N$, so one of its entries, say $\Phi_{i',j}$, is not in $\overline{\mathbb{K}}[[\tau]]$. The well-ordered nature of the exponent set of $\Phi_{i',j}$ shows that there exists e in $\mathbb{Q}_{>0}$ such that τ^e is the smallest non-integer exponent appearing with non-zero coefficient in $\Phi_{i',j}$; if there are several such j's, assume we have chosen the one with smallest exponent e.

Write $\Phi_{i'} = \Phi_{i',0} + \Phi_{i',1}$, where $\Phi_{i',0}$ consists of all terms with exponent less than e; this is thus a vector of truncated power series, and all terms in $\Phi_{i',1}$ have valuation at least e. Since $\boldsymbol{f}_\tau(\Phi_{i'}) = 0$, Taylor expansion shows that $\boldsymbol{f}_\tau(\Phi_{i',0}) + \mathrm{jac}(\boldsymbol{f}_\tau, \mathbf{X})(\Phi_{i',0})\Phi_{i',1} = O(\tau^{2e})$, where the right-hand side consists of terms with valuation at least $2e$. The invertibility of $\mathrm{jac}(\boldsymbol{f}_\tau, \mathbf{X})(\varphi_i)$ implies that $\mathrm{jac}(\boldsymbol{f}_\tau, \mathbf{X})(\Phi_{i',0})$ is invertible too, so that $\mathrm{jac}(\boldsymbol{f}_\tau, \mathbf{X})(\Phi_{i',0})^{-1}\boldsymbol{f}_\tau(\Phi_{i',0}) + \Phi_{i',1} = O(\tau^{2e})$. The first term is a power series, whereas by assumption $\Phi_{i',1}$ has at least one term with non-integer exponent e. This term cannot be cancelled by the right-hand side, a contradiction. $\qquad\square$

Finally, in the discussion below, for $i = 1, \ldots, c$ and $j = 1, \ldots, N$, we write $\mu_{i,j} = \nu(\Phi_{i,j})$ and $\mu_i = \min_{1 \leq j \leq N} \mu_{i,j}$. In particular, $\mu_i \geq 0$ if and only if $i \leq c'$. Still inspired by [45], we will say that a linear form λ with coefficients in $\mathbb{K}$ is a *well-separating* element for $(\boldsymbol{f}, \mathbf{g})$ if:

1. λ is separating for $Z(\mathbf{g})$

2. λ is separating for $\{\varphi_1, \ldots, \varphi_{c'}\}$

3. $\nu(\lambda(\Phi_i)) = \mu_i$ for all $i = 1, \ldots, c$.

We will discuss later on how random choices can ensure these properties with high probability. For the moment, remark that by Lemma 7, the first condition implies that λ is separating for $\boldsymbol{3}$.

Let us extend ν to $\mathbb{L}[T]$, by letting $\nu(a_0 + \cdots + a_s T^s) = \min_{a_i \neq 0}(\nu(a_i))$. This applies in particular to polynomials in $\mathbb{K}((\tau))[T]$; in that case, note that for any f in $\mathbb{K}(\tau)[T]$ and e

in $\mathbb{Z}$, $\tau^e f$ is in $\mathbb{K}[[\tau]][T]$ if and only if $e + \nu(f) \geq 0$. This being said, we can state the main result in this paragraph; it follows closely [45], in our slightly different setting.

Lemma 9. *Suppose that λ is a well-separating element, let $\mathscr{Q} = ((q, v_1, \ldots, v_N), \lambda)$ be the corresponding zero-dimensional parametrization of $\mathfrak{Z}$ over $\mathbb{K}((\tau))$, and let $e = -\nu(q)$. Define the polynomials $q^\star = \tau^e q$ and $(v_j^\star = \tau^e v_j)_{1 \leq j \leq N}$. Then, these polynomials are in $\mathbb{K}[[\tau]][T]$.*

Defining further r_0 as the leading coefficient of $q^\star(0, T)$ and

$$r = \frac{1}{r_0} q^\star(0, T) \quad and \quad w_j = \frac{1}{r_0} v_j^\star(0, T) \bmod r \quad (1 \leq j \leq N),$$

the polynomials $r, w_1, \ldots, w_N$ are such that

$$r = \prod_{1 \leq i \leq c'} (T - \lambda(\varphi_i)) \quad and \quad w_j = \sum_{1 \leq i \leq c'} \varphi_{i,j} \prod_{1 \leq i' \leq c', \, i' \neq i} (T - \lambda(\varphi_{i'})).$$

Proof. To prove the first point, since all polynomials v_j and q have coefficients in $\mathbb{K}((\tau))$, it is enough to prove that $\nu(v_j) \geq \nu(q)$ holds for all j. In view of the interpolation formulas

$$q = \prod_{1 \leq i \leq c} (T - \lambda(\Phi_i)), \quad v_j = \sum_{1 \leq i \leq c} \Phi_{i,j} \prod_{1 \leq i' \leq c, \, i' \neq i} (T - \lambda(\Phi_{i'})),$$

we deduce first that $\nu(q) = \sum_{c' < i \leq c} \mu_i$, and that for all i, j,

$$\nu\left(\Phi_{i,j} \prod_{1 \leq i' \leq c, \, i' \neq i} (T - \lambda(\Phi_{i'}))\right) = \mu_{i,j} + \sum_{c' < i' \leq c, \, i' \neq i} \mu_{i'} \geq \sum_{c' < i' \leq c} \mu_{i'} = \nu(q).$$

Taking the sum, this implies that $\nu(v_j) \geq \nu(q)$, as claimed. Besides, since the definition of e gives $e = -\sum_{c' < i \leq c} \mu_i$, we obtain the factorization

$$q^\star = \prod_{1 \leq i \leq c'} (T - \lambda(\Phi_i)) \cdot \prod_{c' < i \leq c} (\tau^{-\mu_i} T - \tau^{-\mu_i} \lambda(\Phi_i)).$$

In particular, the polynomial $r = q^\star(0, T)$ satisfies

$$r = \gamma \prod_{1 \leq i \leq c'} (T - \ell_0(\lambda(\Phi_i))) = \gamma \prod_{1 \leq i \leq c'} (T - \lambda(\varphi_i)),$$

where γ is the scalar $\gamma = \prod_{c' < i \leq c} \ell_0(\tau^{-\mu_i} \lambda(\Phi_i))$; it is non-zero, as a consequence of the third condition in the definition of a well-separating element. Proceeding similarly with $v_j^\star$, we obtain the claim for w_j. $\qquad \square$

Recovering $Z(\boldsymbol{f})$. The polynomials r and $w_1, \ldots, w_N$ defined in the previous lemma do not necessarily form a zero-dimensional parametrization of $\{\varphi_1, \ldots, \varphi_{c'}\}$, since r may have multiple roots. We show here how to deduce a zero-dimensional parametrization of $Z(\boldsymbol{f}) = \{\varphi_1, \ldots, \varphi_s\}$.

Our starting point is that the minimal polynomial in the parametrization of $Z(\boldsymbol{f})$ associated to λ is $t = \prod_{1 \le i \le s}(T - \lambda(\varphi_i))$, and that this polynomial is a factor of r.

More precisely, because λ separates $\{\varphi_1, \ldots, \varphi_{c'}\}$, and because each φ_i, for i in $\{1, \ldots, s\}$, only appears once among $\varphi_1, \ldots, \varphi_{c'}$ (Lemma 8), $\lambda(\varphi_i)$ is a root of r of multiplicity 1, for all i as above. Thus, we can assume without loss of generality that the roots of r of multiplicity 1 are $\lambda(\varphi_1), \ldots, \lambda(\varphi_{c''})$, for some c'' in $\{s, \ldots, c'\}$, and let r_1 be the product $\prod_{1 \le i \le c''}(T - \lambda(\varphi_i))$, so that t divides r_1. Explicitly, we have (independently of the characteristic)

$$r_1 = \frac{\tilde{r}}{\gcd(\tilde{r}, r')} \quad \text{with} \quad \tilde{r} = \frac{r}{\gcd(r, r')}. \tag{2}$$

Let us write $r = r_1 r_{\ge 2}$, where $r_{\ge 2}$ is $\prod_{c'' < i < c'}(T - \lambda(\varphi(i)))$, and define

$$y_i = \frac{w_i}{r_2} \bmod r_1, \quad 1 \le i \le N;$$

one easily sees that

$$y_i = \sum_{1 \le i \le c''} \varphi_{i,j} \prod_{1 \le i' \le c'', \; i' \ne i} (T - \lambda(\varphi_i)).$$

In other words, $((r_1, y_1, \ldots, y_N), \lambda)$ is a zero-dimensional parametrization of $\{\varphi_1, \ldots, \varphi_{c''}\}$.

The set $\{\varphi_1, \ldots, \varphi_{c''}\}$ contains $Z(\boldsymbol{f}) = \{\varphi_1, \ldots, \varphi_s\}$ and is contained in $V(\boldsymbol{f})$. To conclude, we remove from this set all points where the Jacobian determinant of $\boldsymbol{f}$ vanishes. This is done as in Algorithm Clean of [20], with one small modification: in that result, zero-dimensional parametrizations did not involve rational expressions of the roots of the form $x_i = v_i(T)/q'(T)$, but polynomial ones of the form $x_i = v_i(T)$. This is harmless, since conversions between the two can be done in quasi-linear time.

The algorithm and its cost analysis. We can finally summarize the whole process in Algorithm 1 below. For the moment, we assume that a well-separaring element λ is part of the input.

Lemma 10. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ has multi-degree at most $\boldsymbol{d} = (d_1, \ldots, d_N)$, with all d_i in $\mathbb{N}^m$, and that $\boldsymbol{f}$ is given by a straight-line program Γ of size L; suppose further that $\mathbb{K}$ has characteristic either zero or at least equal to $\max_{1 \le j \le m} d_{1,j} + \cdots + d_{N,j}$. Given Γ, $\boldsymbol{d}$ and a linear form λ which is a well-separating element for $(\boldsymbol{f}, \mathbf{g})$, one can compute a zero-dimensional parametrization of $Z(\boldsymbol{f})$ using*

$$O^{\tilde{}}\left(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) \mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}') \left(L + \sum_{i,j} d_{i,j} + N^2 \right) N \right)$$

operations in $\mathbb{K}$.

Proof. The cost of Step 1 in NonsingularSolutions_aux follows from Lemma 4. Step 2 can be done in quasi-linear time $O\tilde{\ }(\mathscr{C}_n(d)N)$ using the algorithms of [15, Chapter 10].

For the main step, computing the parametrization $\mathscr{Q}$ with coefficients in $\mathbb{K}(t)$, we use the lifting algorithm in [48]. The main factor determining the cost of this algorithm is the required precision needed in t, that is, the degree of the coefficients in the output: Lemma 5 shows that it is at most $\mathscr{C}_{n'}(d')$. The other important quantity is the size of the straight-line program that evaluates $\boldsymbol{f}_t$: using Lemma 4, we see that it is $O(L + \sum_{i,j} d_{i,j})$.

Step 4 involves exponent comparisons, setting some variable to zero and computing a remainder; it can be done in quasi-linear time $O\tilde{\ }(\mathscr{C}_n(d)N)$. Step 5 requires computing the polynomial r_1 using (2), and some computations modulo r_1; all of this can be done in time $O\tilde{\ }(\mathscr{C}_n(d)N)$.

Finally, Step 6 takes $O(\mathscr{C}_n(d)(L + N^2)N)$ to reduce D modulo $(r_1, u_1, \ldots, y_N)$, where the term $(L + N^2)N$ is the size of the straight-line program that computes the Jacobian determinant D. The other operations at this stage take quasi-linear time $O(\mathscr{C}_n(d)N)$. $\square$

Algorithm 1 (NonsingularSolutions_aux): Solving $\boldsymbol{f}$ by symbolic homotopy

---

Input: Γ, $\boldsymbol{d}$, a well-separating element λ
Output: a zero-dimensional parametrization of $Z(\boldsymbol{f})$
1: Define $\mathbf{g}$ and compute $Z(\mathbf{g})$ using Lemma 4
   Cost: $O\tilde{\ }(\mathscr{C}_n(d)N)$
2: Compute a zero-dimensional parametrization $\mathscr{Q}_{\mathbf{g}}$ for $Z(\mathbf{g})$ using interpolation formulas (1)
   Cost: $O\tilde{\ }(\mathscr{C}_n(d)N)$
3: Apply the lifting algorithm of [48] to $\mathscr{Q}_{\mathbf{g}}$ and $\boldsymbol{f}_t$, to recover a zero-dimensional parametrization $\mathscr{Q}$ for $\mathfrak{Z}$ with coefficients in $\mathbb{K}(t)$
   Cost: $O\tilde{\ }(\mathscr{C}_n(d)\mathscr{C}_{n'}(d')(L + \sum_{i,j} d_{i,j} + N^2)N)$
4: Compute r and $w_1, \ldots, w_N$ as in Lemma 9
   Cost: $O\tilde{\ }(\mathscr{C}_n(d)N)$
5: Compute r_1 and $y_1, \ldots, y_N$ as in Subsection 2.2
   Cost: $O\tilde{\ }(\mathscr{C}_n(d)N)$
6: Compute and return $\mathsf{Clean}(r_1, y_1, \ldots, y_N, D)$
   Cost: $O\tilde{\ }(\mathscr{C}_n(d)(L + N^2)N)$

Finding a well-separating element. Our last question is how to ensure that with high probability, a randomly chosen λ is well-separating. For this, we can follow the analysis of [45, Lemma 4.2]: for a linear form λ to be well-separating, λ must assume non-zero values at most c^2 non-zero vectors in $\overline{\mathbb{K}}^N$ (with $c = \mathscr{C}_n(d)$), namely the differences $\boldsymbol{x} - \boldsymbol{x}'$, for distinct $\boldsymbol{x}, \boldsymbol{x}'$ in $Z(\mathbf{g})$, the differences $\varphi_i - \varphi_{i'}$, for i, i' in $\{1, \ldots, c'\}$ such that $\varphi_i \neq \varphi_{i'}$, and the coefficient vectors $(\mathrm{coeff}(\Phi_{i,j}, \tau^{\mu_i}))_{1 \le j \le N}$, for i in $\{1, \ldots, c\}$.

The following classical result shows that a random choice of λ is well-separating with high probability, provided we pick it in a large enough set.

Lemma 11. *Let $\mathbb{A}$ be a domain containing a field $\mathbb{K}$, let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ be non-zero vectors in $\mathbb{A}^N$, and suppose that $\mathbb{K}$ has characteristic either zero or at least $8(N-1)k$. Consider the set of linear forms*

$$u^{(i)} = X_1 + iX_2 + \cdots + i^{N-1}X_N,$$

for i in $\{1, \ldots, 8(N-1)k\}$. Then at least $7/8$ of these linear forms vanish on none of $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$.

Proof. For any i in $\{1, \ldots, k\}$, write $\boldsymbol{x}_i = (x_{i,1}, \ldots, x_{i,N})$ and consider the polynomial $P_i = x_{i,1} + x_{i,2}T + \cdots + x_{i,N}T^{N-1}$. This is a non-zero polynomial, so it has at most $N-1$ roots, and thus at most $N-1$ roots in $\{1, \ldots, 8(N-1)k\}$. Taking all i's into account, we see that at least $7/8$ of the elements in $\{1, \ldots, 8(N-1)k\}$ cancel none of the polynomials P_i. $\qquad\square$

We can then state our main algorithm, together with its probablity analysis (obviously, the cost is the same as that of NonsingularSolutions_aux). Remark first that in any case, the output is a subset of $Z(\boldsymbol{f})$; this is ensured by our call to Clean in the last step of NonsingularSolutions_aux. If λ is a well-separating element, which occurs with probability at least $7/8$, the output is $Z(\boldsymbol{f})$ itself; otherwise we may obtain a subset of it, or fail, when for instance the assumptions of Lemma 9 are not satisfied. This analysis establishes Proposition 2.

Algorithm 2 (NonsingularSolutions): Solving $\boldsymbol{f}$ by symbolic homotopy

---

Input: $\Gamma, \boldsymbol{d}$
Output: a zero-dimensional parametrization of $Z(\boldsymbol{f})$
  1: Set $\lambda = u^{(i)}$, for a randomly chosen i in $\{1, \ldots, 8(N-1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2\}$
  2: Return NonsingularSolutions_aux$(\Gamma, \boldsymbol{d}, \lambda)$

---

3 Height bounds, and the main algorithm

In this section, we work over $\mathbb{K} = \mathbb{Q}$ and we give bounds on the height of polynomials appearing in a zero-dimensional parametrization of a set $Z(\boldsymbol{f})$ as before, using the multi-degree structure of $\boldsymbol{f}$; as for the degree bounds, this gives finer results than using the total degree in many cases. These height bounds are derived in a manner similar to the degree ones, using the recent introduction of an arithmetic version of multiprojective intersection theory in [12]. Then, we show how to use this result in the context of a lifting algorithm following that of [20].

Concrete example of the bounds derived here are given in the next section.

3.1 Bounds

Supposing that $\boldsymbol{f} = (f_1, \ldots, f_N)$ are polynomials with integer coefficients, we want to give an estimate for the bit size of a zero-dimensional parametrization of $Z(\boldsymbol{f})$, taking into account

the multi-degree of $\boldsymbol{f}$. To this effect, we use an arithmetic analogue of the ring $A^*(\mathbb{P}^{\boldsymbol{n}})$ seen above, due to D'Andrea, Krick and Sombra [12]; here, since we work over $\mathbb{Q}$, we write $\mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1}(\overline{\mathbb{Q}}) \times \cdots \times \mathbb{P}^{n_m}(\overline{\mathbb{Q}})$. Following that reference, let us define the *arithmetic Chow ring*

$$A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z}) = \mathbb{R}[\zeta, \vartheta_1, \ldots, \vartheta_m]/\langle \zeta^2, \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1}\rangle.$$

Continuing the analogy with the previous section, let us define the following symbols: given a non-negative real number η and a multi-degree $d = (d_1, \ldots, d_m)$, set

$$\{\eta, d\} = \eta\zeta + d_1\vartheta_1 + \cdots + d_m\vartheta_m \in \mathbb{A}^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z});$$

given vectors $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_M)$ and $\boldsymbol{d} = (d_1, \ldots, d_M)$, with all η_i in $\mathbb{R}_{\geq 0}$ and all d_i in $\mathbb{N}^m$, write

$$\{\boldsymbol{\eta}, \boldsymbol{d}\} = \{\eta_1, d_1\} \cdots \{\eta_M, d_M\} \bmod \langle \zeta^2, \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1}\rangle \in A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z}).$$

This can be seen as a polynomial of total degree M, so as before, we define

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) = \sum_{\boldsymbol{c} \in \mathbb{N}^m, \ |\boldsymbol{c}| = M-1} \mathrm{coeff}(\{\boldsymbol{\eta}, \boldsymbol{d}\}, \zeta \ \vartheta_1^{c_1} \cdots \vartheta_m^{c_m}) + \sum_{\boldsymbol{c} \in \mathbb{N}^m, \ |\boldsymbol{c}| = M} \mathrm{coeff}(\{\boldsymbol{\eta}, \boldsymbol{d}\}, \vartheta_1^{c_1} \cdots \vartheta_m^{c_m});$$

again, all coefficients of $\{\boldsymbol{\eta}, \boldsymbol{d}\}$ not taken into account in this sum are necessarily zero. Given a system of polynomials $\boldsymbol{f} = (f_1, \ldots, f_M)$ in $\mathbb{Z}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, we write $\eta(\boldsymbol{f}) = (\eta_1, \ldots, \eta_M)$, with

$$\eta_i = \mathrm{ht}(f_i) + \sum_{j=1}^{m} \log(n_j + 1) \deg_{\mathbf{X}_j}(f_i), \tag{3}$$

and use the same conventions for inequalities as for multi-degrees. All these definitions being written, we can state the main proposition of this paragraph. Its proof occupies the rest of this subsection.

Proposition 12. *Let $\boldsymbol{f} = (f_1, \ldots, f_N)$ be a polynomial system in $\mathbb{Z}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, with $\mathrm{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d}$ and $\eta(\boldsymbol{f}) \leq \boldsymbol{\eta}$, and let λ be a separating linear form for $Z(\boldsymbol{f})$ with integer coefficients of height at most b. Then all polynomials in the zero-dimensional parametrization $\mathscr{Q}$ of $Z(\boldsymbol{f})$ associated to λ have height at most $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + (b + 4\log(N+2))\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$.*

The Chow forms. As a preliminary, we recall the definition of the Chow form of an algebraic set. Let $V \subset \overline{\mathbb{Q}}^N$ be a zero-dimensional algebraic set. We call *Chow form* of V any polynomial of the form

$$C_{V,a} = a \prod_{\boldsymbol{x} = (x_1, \ldots, x_N) \in V} (T_0 - x_1 T_1 - \cdots - x_N T_N),$$

for some nonzero a in $\overline{\mathbb{Q}}$. If V is defined over $\mathbb{Q}$, then for a in $\mathbb{Q}$, $C_{V,a}$ is in $\mathbb{Q}[T_0, \ldots, T_N]$. Clearing denominators and removing contents, we see that only two of them are primitive polynomials in $\mathbb{Z}[T_0, \ldots, T_N]$ (they differ by a sign): we call them the *primitive* Chow forms of V.

The arithmetic Chow ring. The proof of the above proposition will rely on objects introduced by, and results due to, D'Andrea, Krick and Sombra [12]. We give here a quick overview of the main features of their construction.

Introducing new variables $X_{1,0}, \ldots, X_{m,0}$ as homogenization variables, we will use $\mathbf{X}' = (\mathbf{X}'_1, \ldots, \mathbf{X}'_m)$, with $\mathbf{X}'_j = (X_{j,0}, \ldots, X_{j,n_j})$ for all j, to describe multi-homogeneous polynomials. To any r-equidimensional algebraic set $V \subset \mathbb{P}^{\boldsymbol{n}}$ defined over $\mathbb{Q}$, we associate its class $[V]_{\mathbb{Z}} \in A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z})$, which takes the form of an homogeneous expression of degree $N - r$:

$$[V]_{\mathbb{Z}} = \sum_{\boldsymbol{c} \in \mathbb{N}^m, \ |\boldsymbol{c}|=r+1, \boldsymbol{c} \leq \boldsymbol{n}} \widehat{h}_{\boldsymbol{c}}(V) \, \zeta \, \vartheta_1^{n_1-c_1} \cdots \vartheta_m^{n_m-c_m} + \sum_{\boldsymbol{c} \in \mathbb{N}^m, \ |\boldsymbol{c}|=r, \boldsymbol{c} \leq \boldsymbol{n}} \deg_{\boldsymbol{c}}(V) \vartheta_1^{n_1-c_1} \cdots \vartheta_m^{n_m-c_m},$$

where $\widehat{h}_{\boldsymbol{c}}(V)$ and $\deg_{\boldsymbol{c}}(V)$ are families of non-negative real numbers. For $\boldsymbol{c} = (c_1, \ldots, c_m)$, the degree $\deg_{\boldsymbol{c}}(V)$ is defined as the generic number of intersection points between V and c_1 linear forms in $\mathbf{X}'_1$, $\ldots$, c_m linear forms in $\mathbf{X}'_m$. The height component $\widehat{h}_{\boldsymbol{c}}(V)$ is harder to define, and we refer to [12] for a precise statement (the properties given below will be sufficient for our purposes). When V has dimension zero, using a slight re-indexing of the height components, we can write

$$[V]_{\mathbb{Z}} = \sum_{1 \leq i \leq m} \widehat{h}_i(V) \, \zeta \, \vartheta_1^{n_1} \cdots \vartheta_i^{n_i-1} \cdots \vartheta_m^{n_m} + \deg(V) \vartheta_1^{n_1} \cdots \vartheta_m^{n_m},$$

where $\widehat{h}_i(V)$ is defined as $\widehat{h}_{\boldsymbol{c}_i}(V)$, with $\boldsymbol{c}_i$ the ith unit vector, and where $\deg(V)$ is simply its cardinality.

We now list a few properties which will be central for our purposes.

A_1. For any V as above, $\widehat{h}_{\boldsymbol{c}}(V) \geq 0$ holds for all $\boldsymbol{c}$ [12, Proposition 2.51.2]. In other words, we have $[V]_{\mathbb{Z}} \geq 0$, where here, and in all that follows, inequalities between elements of arithmetic Chow rings are to be understood coefficientwise.

A_2. If V and V' are both r-equidimensional and without irreducible components in common, $[V \cup V']_{\mathbb{Z}} = [V]_{\mathbb{Z}} + [V']_{\mathbb{Z}}$ (this is clear for the degree and follows from [12, Definition 2.40] for the height). We could remove the assumption above, but this would require us to talk about cycles, for which we will have no use below.

A_3. If V is a hypersurface given as $V = V(f)$, with $f \in \mathbb{Z}[\mathbf{X}'_1, \ldots, \mathbf{X}'_m]$ multi-homogeneous, squarefree and primitive, we have from [12, Proposition 2.53]

$$[V]_{\mathbb{Z}} = m(f)\zeta + \deg_{\mathbf{X}'_1}(f)\vartheta_1 + \cdots + \deg_{\mathbf{X}'_m}(f)\vartheta_m,$$

where $m(f) = \int_{S_1^{N+m}} \log(|f|) d\mu^{N+m}$ is the *Mahler measure* of f with respect to the Haar measure μ of mass 1 on the complex unit circle S_1.

A_4. If V is an r-equidimensional algebraic subset of $\mathbb{P}^{\boldsymbol{n}}$ defined over $\mathbb{Q}$ and f is multi-homogeneous in $\mathbb{Z}[\mathbf{X}'_1, \ldots, \mathbf{X}'_m]$, we have from [12, Corollary 2.61]

$$[W]_{\mathbb{Z}} \leq [V]_{\mathbb{Z}} \cdot [f]_{\sup},$$

where W is the $(r-1)$-dimensional part of $V \cap V(f)$, $|f|_{\sup} = \sup_{\boldsymbol{x} \in S_1^{N+m}} |f(\boldsymbol{x})|$ and

$$[f]_{\sup} = \log(|f|_{\sup})\zeta + \deg_{\mathbf{X}'_1}(f)\vartheta_1 + \cdots + \deg_{\mathbf{X}'_m}(f)\vartheta_m.$$

Using the Bézout inequality. Let $\boldsymbol{f}^h = (f_1^h, \ldots, f_N^h)$ be the polynomials in $\mathbb{Z}[\mathbf{X}'_1, \ldots, \mathbf{X}'_m]$ obtained by multi-homogenizing the input $f_1, \ldots, f_N$ with respect to all groups of variables $\mathbf{X}_1, \ldots, \mathbf{X}_m$, let $S \subset \mathbb{P}^{\boldsymbol{n}}$ be the zero-dimensional component of $V(\boldsymbol{f}^h)$, and let $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_N)$ and $\boldsymbol{d} = (d_1, \ldots, d_N)$ be upper bounds on respectively $\eta(\boldsymbol{f})$ and $\mathrm{mdeg}(\boldsymbol{f})$.

By [12, Proposition 2.51.3], $[\mathbb{P}^{\boldsymbol{n}}]_{\mathbb{Z}} = 1$. Applying A_4 repeatedly, we obtain that

$$[S]_{\mathbb{Z}} \le [f_1^h]_{\sup} \cdots [f_N^h]_{\sup}.$$

By [12, Lemma 2.32], for all i, we have the inequality

$$[f_i]_{\sup} \le \eta_i \zeta + d_{i,1}\vartheta_1 + \cdots + d_{i,m}\vartheta_m,$$

or equivalently $[f_i]_{\sup} \le \{\eta_i, d_i\}$. This implies that

$$[S]_{\mathbb{Z}} \le \{\eta_1, d_1\} \cdots \{\eta_N, d_N\} = \{\boldsymbol{\eta}, \boldsymbol{d}\}. \tag{4}$$

From multi-projective to affine. Let now $S' \subset \mathbb{P}^{\boldsymbol{n}}$ be the subset of S consisting of all those points $\boldsymbol{x}' = (\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m)$ in S, with $\boldsymbol{x}'_i$ in $\mathbb{P}^{n_i}(\overline{\mathbb{Q}})$ for all i, such that

- $\boldsymbol{x}'_i$ does not belong to the hyperplane at infinity in $\mathbb{P}^{n_i}(\overline{\mathbb{Q}})$;

- the multi-homogeneous polynomial J^h obtained by multi-homogenizing the Jacobian determinant $J = \det(\mathrm{jac}(\boldsymbol{f}))$ with respect to all groups of variables $\mathbf{X}_1, \ldots, \mathbf{X}_m$ does not vanish at $\boldsymbol{x}'$.

Because we obtain S' by removing algebraic subsets from S, and these subsets are defined over $\mathbb{Q}$, S' itself is defined over $\mathbb{Q}$. Using A_1 and A_2, we deduce from (4) that we have

$$[S']_{\mathbb{Z}} \le \{\boldsymbol{\eta}, \boldsymbol{d}\}. \tag{5}$$

Our goal is now to compute the Chow form of the related algebraic $Z(\boldsymbol{f})$ in $\overline{\mathbb{Q}}^N$. For $(\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m)$ in S', our definition shows that each block-coordinate $\boldsymbol{x}'_i$ can be written as $\boldsymbol{x}'_i = (1, x_{i,1}, \ldots, x_{i,n_i})$. We use this notation in the lemma below — whose proof is a direct consequence of our construction.

Lemma 13. *The following equality holds*

$$Z(\boldsymbol{f}) = \{(x_{1,1}, \ldots, x_{1,n_1}, \ldots, x_{m,1}, \ldots, x_{m,n_m}) \mid \boldsymbol{x} \in S'\} \subset \overline{\mathbb{Q}}^N.$$

Letting $T_0, \ldots, T_N$ be new variables, the Chow forms of $Z(\boldsymbol{f})$ are thus of the form

$$C_{Z(\boldsymbol{f}),c} = c \prod_{\boldsymbol{x} \in S'} (T_0 - x_{1,1}T_1 - \cdots - x_{m,n_m-1}T_{N-1} - x_{m,n_m-1}T_N), \tag{6}$$

for some constant c.

Let us next describe a classical geometric way to construct these Chow forms starting from S'. We start by considering the product $T = S' \times \mathbb{P}^N(\overline{\mathbb{Q}})$, which is an algebraic subset of $\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}})$; we use $T_0, \ldots, T_N$ as our coordinates in $\mathbb{P}^N(\overline{\mathbb{Q}})$. Next, define T' as the intersection of T and $Z(L^h)$, where L is given by

$$L = T_0 - (X_{1,1}T_1 + X_{1,2}T_2 + \cdots + X_{m,n_m-1}T_{N-1} + X_{m,n_m}T_N)$$

and L^h is obtained by multi-homogenizing L with respect to the groups of variables $\mathbf{X}_1, \ldots, \mathbf{X}_m$, using respectively $X_{1,0}, \ldots, X_{m,0}$ (L is already homogeneous with respect to $T_0, \ldots, T_N$).

Lemma 14. *The intersection $T' = T \cap V(L^h)$ is proper.*

Proof. Since S' is finite, it is sufficient to consider the case where S' is a single point of the form $(\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m)$. In that case, the set T' is isomorphic to the zero-set of the linear form $L^h(\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m, T_0, \ldots, T_N)$ in $\mathbb{P}^N(\overline{\mathbb{Q}})$. Our construction of S' implies that the coefficient of T_0 in this linear form is non-zero, so we are done. $\square$

Finally, call π the projection on the last factor $\mathbb{P}^N(\overline{\mathbb{Q}})$, and let us define Y as the image of T' by this projection.

Lemma 15. *The image of each $\overline{\mathbb{Q}}$-irreducible component of T' by π is a hypersurface and each squarefree polynomial in $\mathbb{Q}[T_0, \ldots, T_N]$ defining Y is a Chow form of $Z(\boldsymbol{f})$.*

Proof. Continuing the proof of the previous lemma, we see that the $\overline{\mathbb{Q}}$-irreducible components of T' are finite unions of sets of the form $(\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m) \times H$, where, writing $\boldsymbol{x}'_i = (1, x_{i,1}, \ldots, x_{i,n_i})$, H is the hyperplane of $\mathbb{P}^N(\overline{\mathbb{Q}})$ defined by

$$L = T_0 - (x_{1,1}T_1 + x_{1,2}T_2 + \cdots + x_{m,n_m-1}T_{N-1} + x_{m,n_m}T_N).$$

The conclusion follows from (6). $\square$

Explicit bounds. We can now give quantitative estimates for the classes of the objects introduced so far. By [12, Proposition 2.66], we have the equality $[T]_{\mathbb{Z}} = \iota([S']_{\mathbb{Z}})$, where $[T]_{\mathbb{Z}}$ lies in $A^*(\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}}), \mathbb{Z})$ and ι is the canonical injection

$$A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z}) = \mathbb{R}[\zeta, \vartheta_1, \ldots, \vartheta_m] / \langle \zeta^2, \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1} \rangle$$
$$\to A^*(\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}}), \mathbb{Z}) = \mathbb{R}[\zeta, \vartheta_1, \ldots, \vartheta_m, \mu] / \langle \zeta^2, \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1}, \mu^{N+1} \rangle.$$

Since S' has dimension zero, its class in $A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z})$ has the form

$$[S']_{\mathbb{Z}} = \sum_{1 \leq i \leq m} \widehat{h}_i(S') \, \zeta \, \vartheta_1^{n_1} \cdots \vartheta_i^{n_i-1} \cdots \vartheta_m^{n_m} + \deg(S')\vartheta_1^{n_1} \cdots \vartheta_m^{n_m}. \tag{7}$$

We deduce that $[T]_{\mathbb{Z}}$ has the same form, but in $A^*(\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}}), \mathbb{Z})$. Remark next that the element $[L^h]_{\sup} \in A^*(\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}}), \mathbb{Z})$ satisfies

$$[L^h]_{\sup} = \log(N+1)\zeta + \vartheta_1 + \cdots + \vartheta_m + \mu.$$

Hence, because the intersection defining T' is proper, we deduce from the Bézout inequality A_4 that

$$[T']_{\mathbb{Z}} \leq [T]_{\mathbb{Z}} \cdot (\log(N+1)\zeta + \vartheta_1 + \cdots + \vartheta_m + \mu).$$

Using the formula for $[T]_{\mathbb{Z}}$ given above, we obtain

$$[T']_{\mathbb{Z}} \leq \sum_{1 \leq i \leq m} \widehat{h}_i(S') \zeta \, \vartheta_1^{n_1} \cdots \vartheta_m^{n_m} + \sum_{1 \leq i \leq m} \widehat{h}_i(S') \zeta \, \vartheta_1^{n_1} \cdots \vartheta_i^{n_i-1} \cdots \vartheta_m^{n_m} \mu$$

$$+ \log(N+1) \deg(S')\zeta \, \vartheta_1^{n_1} \cdots \vartheta_m^{n_m} + \deg(S')\vartheta_1^{n_1} \cdots \vartheta_m^{n_m} \mu.$$

Finally, we consider the projection on $\mathbb{P}^N(\overline{\mathbb{Q}})$. The arithmetic Chow ring of this projective space is $\mathbb{R}[\zeta, \mu]/\langle \zeta^2, \mu^{N+1} \rangle$, and [12, Proposition 2.64] shows that

$$\vartheta_1^{n_1} \cdots \vartheta_m^{n_m}[Y]_{\mathbb{Z}} \leq [T']_{\mathbb{Z}}.$$

Considering the possible monomial support of $[Y]_{\mathbb{Z}}$, we deduce that we have the inequality

$$[Y]_{\mathbb{Z}} \leq \sum_{1 \leq i \leq m} \widehat{h}_i(S') \, \zeta + \log(N+1) \deg(S')\zeta + \deg(S')\mu.$$

Hence, if C is a primitive polynomial in $\mathbb{Z}[T_0, \ldots, T_N]$ defining Y, we deduce from A_3 that

$$m(C) \leq \sum_{1 \leq i \leq m} \widehat{h}_i(S') + \log(N+1) \deg(S').$$

This leads us to the following lemma.

Lemma 16. *Any primitive Chow form C of $V(\boldsymbol{f})$ satisfies*

$$m(C) \leq \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + \log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}).$$

Proof. In view of the previous discussion, it is enough to prove that the inequality

$$\sum_{1 \leq i \leq m} \widehat{h}_i(S') + \log(N+1) \deg(S') \leq \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + \log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$$

holds. We saw in (5) the inequality $[S']_{\mathbb{Z}} \leq \{\boldsymbol{\eta}, \boldsymbol{d}\}$, which is to be understood coefficient-wise. Take the sum of coefficients on both sides. From (7), we deduce that the left-hand side adds up to $\sum_{1 \leq i \leq m} \widehat{h}_i(S') + \deg(S')$, which is an upper bound on $\sum_{1 \leq i \leq m} \widehat{h}_i(S')$, whereas the right-hand side gives $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})$. To conclude, we add $\log(N+1) \deg(S')$ on both sides, and we use the fact that $\deg(S') = \deg(Z(\boldsymbol{f})) \leq \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$, as pointed out after Proposition 1. $\square$

Conclusion. Finally, we can conclude the proof of Proposition 12. Lemma 16 shows that for any primitive Chow C form of $Z(\boldsymbol{f})$, we have $m(C) \leq \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + \log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$; using the inequality $|m(C) - \mathrm{ht}(C)| \leq \log(N+2)\deg(C)$ (see [12, Lemma 2.30]), we deduce that such a Chow form has height at most $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + 2\log(N+2)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$. Using Lemma 17 below (which is itself a standard result), we deduce that all polynomials appearing in the zero-dimensional parametrization of $Z(\boldsymbol{f})$ associated to a linear form λ of height b have height at most

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + (b + 4\log(N+2))\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}),$$

which proves the proposition.

Lemma 17. *Suppose that $V \subset \overline{\mathbb{Q}}^N$ is a zero-dimensional algebraic set defined over $\mathbb{Q}$ and that λ is a separating linear form for V with integer coefficients of height at most b. Suppose as well that the primitive Chow forms of V have height at most h. Then, all polynomials that appear in the zero-dimensional parametrization $\mathscr{Q} = ((q, v_1, \ldots, v_N), \lambda)$ of V have height at most $h + \log(\deg(V)) + \deg(V)(b + \log(N+1))$.*

Proof. Let C be a primitive Chow form of V, written $C = aC_0$, with C_0 monic in T_0. It is well-known (see for instance [1]) that we obtain q and $v_1, \ldots, v_n$ as

$$q = \frac{1}{a}C(T, \lambda_1, \ldots, \lambda_n), \quad v_i = -\frac{1}{a}\frac{\partial C}{\partial T_i}(T, \lambda_1, \ldots, \lambda_n).$$

Since C has degree $\deg(V)$ and height h, its partial derivatives have height at most $h + \log(\deg(V))$. The conclusion then follows from (for instance) Lemma 1.2.1.c in [29]. $\square$

3.2 The lifting algorithm

Our goal is now to give boolean complexity statements for the computation of a zero-dimensional representation of $Z(\boldsymbol{f})$. The approach is not new: we lift a zero-dimensional parametrization of $Z(\boldsymbol{f} \bmod p)$, for a well-chosen prime p, to a zero-dimensional parametrization of $Z(\boldsymbol{f})$; the novelty of the proposition below lies in the use of our multi-homogeneous height bounds to control the cost of the process.

The algorithm is randomized, and part of the randomness amounts to choosing primes. This is a delicate question in itself, and not the topic of this paper, so we will assume that we are given an oracle $\mathscr{O}$, which takes as input an integer B, and returns a prime number in $\{B+1, \ldots, 2B\}$, uniformly distributed within the set of primes in this interval [15, Section 18.4].

Proposition 18. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ satisfies $\mathrm{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d} = (d_1, \ldots, d_m)$, $\eta(\boldsymbol{f}) \leq \boldsymbol{\eta}$ and $\mathrm{ht}(f_i) \leq h$ for all i, and that $\boldsymbol{f}$ is given by means of a straight-line program Γ of size L, that uses integer constants of height at most b.*

There exists an algorithm NonsingularSolutionsOverZ *that takes Γ, $\boldsymbol{d}$, $\boldsymbol{\eta}$ and h as input, and that produces one of the following outputs:*

- *either a zero-dimensional parametrization of $Z(\boldsymbol{f})$,*

- *or a zero-dimensional parametrization of degree less than that of $Z(\boldsymbol{f})$,*

- *or* fail.

The first outcome occurs with probability at least $21/32$. In any case, the algorithm uses

$$O^\sim\left(Lb + \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})\left(L + Nd + N^2\right)N(\log(h) + N)\right)$$

boolean operations, with $d = \max_{1 \leq i \leq N} d_{i,1} + \cdots + d_{i,m}$. The algorithm calls the oracle $\mathscr{O}$ with an input parameter $B = hd^{O(N)}$ and the polynomials in the output have degree at most $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ and height $O^\sim(\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$.

As in the case of Proposition 2, running the algorithm k times gives a list of outputs among which is at least one zero-dimensional parametrization of $Z(\boldsymbol{f})$ with probability at least $1 - (11/32)^k$; the fact that all incorrect answers have degree less than that of $Z(\boldsymbol{f})$ allows us to find a correct one by degree considerations only.

The input size of the algorithm is $O(Lb)$ bits, whereas the output size is $O^\sim(N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})(\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})))$ bits; thus, up to polynomial factors in $N, d, \log(h), L$, the cost of the algorithm is close to our upper bound on the combined size of its input and output. We are not aware of previous results that would take multi-homogeneous bit-size bounds into account in such a manner.

Some useful quantities. In order to quantify primes of "bad reduction", we need to define a few quantities related to $Z(\boldsymbol{f})$. In addition to d and h as defined above, we let

$$e = \max_{1 \leq j \leq m} d_{1,j} + \cdots + d_{N,j}.$$

We will run Algorithm NonsingularSolutions with input $\boldsymbol{f}$ mod p, for a prime p. The separating element used in this algorithm has coefficients in $\mathbb{F}_p$; once lifted back to $\mathbb{Z}$ in the canonical manner, the construction used in that algorithm shows that is has height at most $\eta_1 = N\log(8N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2)$.

Next, recall from Lemma 16 that any primitive Chow form C of $Z(\boldsymbol{f})$ satisfies

$$m(C) \leq \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + \log(N + 1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}),$$

where m is the Mahler measure. We will actually use $h(Z(\boldsymbol{f}))$, the *affine height of $Z(\boldsymbol{f})$*, defined in [29] as

$$h(Z(\boldsymbol{f})) = m(C, S_{N+1}) + |Z(\boldsymbol{f})| \sum_{i=1}^{N} \frac{1}{2i},$$

where $m(C, S_{N+1})$ is the Mahler measure on the unit sphere S_{N+1} in $\mathbb{C}^{N+1}$, namely

$$m(g, S_{N+1}) = \int_{S_{N+1}} \log|g(x)|\mu(x),$$

where μ is the Haar measure of mass 1 on S_{N+1}. We will mainly use this through the inequality $m(g, S_{N+1}) \leq m(g)$ of [29, Eq. (1.2)], where $m(g)$ is its usual Mahler measure; hence, we have $h(Z(\boldsymbol{f})) \leq \eta_2$, with

$$\eta_2 = \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + 2\log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}).$$

Finally, define

$$\eta_3 = \eta_2 + \eta_1 \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) + \log(N+2)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) + (N+1)\log(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$$

and

$$H = 6N(d+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\left(\eta_3 + h + \log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\right). \tag{8}$$

Then, using Lemmas 8 and 9 in [11], we deduce that there is a positive integer A such that we have

- $\log(A) \leq H$

- for any prime p that does not divide A, $Z(\boldsymbol{f})$ and $Z(\boldsymbol{f} \bmod p)$ have the same cardinality.

Define

$$B = \max\left(8\lceil H \rceil, e\right)$$

and remark the following:

- there are at least $B/2\log(B)$ primes in $\{B+1, \ldots, 2B\}$ [15, Th. 18.8];

- there are at most $\log(A)/\log(B) \leq H/\log(B)$ primes in $\{B+1, \ldots, 2B\}$ that divide A.

Hence, the probability that a randomly chosen prime among those in $\{B+1, \ldots, 2B\}$ divides A is at most $2H/B$, which is at most $1/4$ by construction; on the other hand, B has been chosen small enough to be $hd^{O(N)}$, so that that $\log(B)$ is $O(\log(h) + N\log(d))$.

The last quantity we introduce is

$$H' = \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + \left(\eta_1 + 4\log(N+2)\right)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}); \tag{9}$$

as we will see, this will control the height of the output of our algorithm.

The main algorithm. Following the algorithm given [20], we start by solving the system modulo a prime p, then lift this solution to a zero-dimensional parametrization of $Z(\boldsymbol{f})$. As input, we take a straight-line program Γ of size L that evaluates $\boldsymbol{f}$, using only integer constants; we define b as the maximum of the heights of the constants in Γ.

Let p be a prime in $\{B+1, \ldots, 2B\}$, which we obtain by calling the oracle $\mathscr{O}$ with input parameter B. By construction of B, the field $\mathbb{F}_p$ satisfies the assumptions of Proposition 2, since B is at least $\max(e, 8(N-1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2)$. Thus, we can call Algorithm NonsingularSolutions, with input the straight-line program Γ' obtained by reducing all constants appearing in Γ modulo p (computing these constants takes time $O\tilde{\ }(L(\log(B) + b)) = O\tilde{\ }(L(\log(h) + N\log(d) + b)))$. Recall that we obtain

- either a zero-dimensional parametrization of $Z(\boldsymbol{f} \bmod p)$,

- or a zero-dimensional parametrization of a subset of $Z(\boldsymbol{f} \bmod p)$,

- or fail,

with the first outcome arising with probability at least $7/8$. In all cases, since operations modulo p take $O\tilde{\ }(\log(h) + N\log(d))$ bit operations, the running time is

$$O\tilde{\ }\left(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{C}_{\boldsymbol{n'}}(\boldsymbol{d'})\left(L + \sum_{1 \leq i \leq N, 1 \leq j \leq m} d_{i,j} + N^2\right)N(\log(h) + N\log(d))\right) \qquad (10)$$

bit operations. If this computation fails, our main algorithm will return fail as well. Else, we have obtained a zero-dimensional parametrization $\mathscr{Q}_0 = ((q_0, v_{1,0}, \ldots, v_{N,0}), \lambda_0)$.

Let then λ be the canonical lift of λ_0 to a linear form with non-negative integer co-efficients; as said previously, the way λ_0 is chosen implies that λ has height at most $\eta_1 = N\log(8N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2)$. Using Newton iteration [20, Section 4.3], we deduce the existence of a zero-dimensional parametrization $\mathscr{Q}_\infty = ((q_\infty, v_{1,\infty}, \ldots, v_{N,\infty}), \lambda)$ with coefficients in the p-adic integers $\mathbb{Z}_p$, that describes a subset of $Z(\boldsymbol{f})$ over an algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. We run the lifting algorithm of [20, Section 4.3] up to a precision at least equal to $2H'$, where H' as defined in (9), from which we reconstruct a rational parametrization with rational coefficients.

- Suppose that $Z(\boldsymbol{f})$ and $Z(\boldsymbol{f} \bmod p)$ have the same cardinality, and that $\mathscr{Q}_0$ describes $Z(\boldsymbol{f} \bmod p)$; this is the case in particular when p does not divide A, and $\mathscr{Q}_0$ is a zero-dimensional parametrization of $Z(\boldsymbol{f} \bmod p)$, so it occurs with probability at least $7/8 \times 3/4 = 21/32$, as claimed.

  Then, by reasons of cardinality, the zero-dimensional parametrization $\mathscr{Q}_\infty$ actually describes all of $Z(\boldsymbol{f})$, over an algebraic closure of $\mathbb{Q}_p$. Since $Z(\boldsymbol{f})$ is defined over $\mathbb{Q}$, and since λ has coefficients in $\mathbb{Z}$, we deduce that all coefficients in $\mathscr{Q}_\infty$ actually belong to $\mathbb{Q}$: indeed, these polynomials show up as a Gröbner basis in $\mathbb{Q}_p[X_1, \ldots, X_N, T]$ of the ideal generated by the defining ideal of $Z(\boldsymbol{f})$, together with $T - \lambda$.

  Since the separating element constructed by NonsingularSolutions has coefficients of height at most η_1, Proposition 12 shows that all coefficients in $\mathscr{Q}_\infty$ are rational numbers of height at most H'. Hence, knowing them modulo a number greater than $\exp(2H')$ is sufficient to reconstruct them.

- Otherwise, either $Z(\boldsymbol{f})$ and $Z(\boldsymbol{f} \bmod p)$ do not have the same cardinality, or $\mathscr{Q}_0$ de-scribes a proper subset $Z(\boldsymbol{f} \bmod p)$. Since the lifting argument above shows that $Z(\boldsymbol{f} \bmod p)$ must have cardinality at most equal to that of $Z(\boldsymbol{f})$, in all cases, $\mathscr{Q}_0$ has degree less than that of $Z(\boldsymbol{f})$, and similarly for the output of the lifting algorithm.

In any case, the dominant part of this process is lifting, since reconstructing rational numbers from their p-adic expansion can be done in quasi-linear time [15, Chapter 11]. Using the

cost analysis from [20], we deduce that the cost is

$$O^{\tilde{}}\left(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})H'\left(L+N^2\right)N\right) \qquad (11)$$

bit operations.

Up to logarithmic factors, the height bound H' on the output is $O^{\tilde{}}(\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta},\boldsymbol{d})+N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$. Remark now that the definitions of $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta},\boldsymbol{d})$ and $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$ are very similar, and imply that we have $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) \leq \mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}') \leq \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta},\boldsymbol{d})$. Thus, we deduce from (10) and (11) the following upper bound on the total boolean cost of our algorithm:

$$O^{\tilde{}}\left(Lb+\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta},\boldsymbol{d})\left(L+Nd+N^2\right)N(\log(h)+N\log(d))\right).$$

4   Application to polynomial minimization

We finally turn to the last question mentioned in the introduction: given polynomials $\boldsymbol{f} = (f_1,\ldots,f_p) \subset \mathbb{Z}[X_1,\ldots,X_n]$, that define an algebraic set $V = V(\boldsymbol{f}) \subset \mathbb{C}^n$, determine $\min_{\boldsymbol{x}\in V\cap\mathbb{R}^n}\pi_1(\boldsymbol{x})$, where π_1 is the canonical projection $(x_1,\ldots,x_n) \mapsto x_1$.

Our goal is to give boolean complexity estimates for the computation of this minimum, under some genericity assumptions on $\boldsymbol{f}$; we will pay a particular attention to the quadratic case, where all input polynomials have degree at most 2. The assumptions on $\boldsymbol{f}$ are discussed in the first subsection; we will say that $\boldsymbol{f}$ satisfies G when they hold, and we will prove below that they are indeed satisfied for a generic choice of $\boldsymbol{f}$ for the Zariski topology. Then, our main result is the following.

Theorem 19. *Let $\boldsymbol{f} = (f_1,\ldots,f_p) \subset \mathbb{Z}[X_1,\ldots,X_n]$, and assume that all f_i's have degree at most D and height at most τ. Assume further that $\boldsymbol{f}$ satisfies G and is given by a straight-line program Γ of length E, that uses integers of height at most τ'.*

Then, there exists a randomized algorithm that takes Γ, D and τ as input, and computes a zero-dimensional parametrization of the set of critical points of π_1 on $V(\boldsymbol{f})$ with probability at least $147/256 \geq 0.57$ and using

$$O^{\tilde{}}\left(p(E+n)\tau' + n^3\binom{n-1}{p-1}\binom{n}{p}(\tau+D)D^{2p}(D-1)^{2(n-p)}(pE+nD+n^2)\right).$$

boolean operations. Moreover, the output polynomials have degree at most $\binom{n-1}{p-1}D^p(D-1)^{n-p}$ and height $O^{\tilde{}}(n\binom{n}{p}(\tau+D)D^p(D-1)^{n-p})$.

4.1   Genericity assumptions

Let $\boldsymbol{f} = (f_1,\ldots,f_p)$ be our input polynomials and let $V \subset \mathbb{C}^n$ be their zero-set. In general, in cases where we may not necessarily assume V smooth, the *critical points* of π_1 on V are those points $\boldsymbol{x} \in V$ that do not belong to the singular locus of V and at which $T_{\boldsymbol{x}}V$ is "vertical", in the sense that $\pi_1(T_{\boldsymbol{x}}V) = \{0\}$; following [2, 3], we denote this set by $W(\pi_1, V)$.

Let $\mathrm{jac}(\boldsymbol{f})$ be the Jacobian matrix of $\boldsymbol{f}$ and let $\mathrm{jac}(\boldsymbol{f},1)$ denote the truncated jacobian matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_2} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial X_2} & \cdots & \frac{\partial f_p}{\partial X_n} \end{bmatrix}.$$

Following again the construction of [3], if m is a $(p-1)$-minor of $\mathrm{jac}(\boldsymbol{f},1)$, $\mathsf{Minors}(\boldsymbol{f},m)$ denotes the vector of p-minors of $\mathrm{jac}(\boldsymbol{f},1)$ obtained by adding the missing row and the missing column to m; there are $n-p$ such minors. Then, we say that $(f_1,\ldots,f_p)$ satisfies assumption G if the following conditions hold:

(1) At any point of V, the jacobian matrix $\mathrm{jac}(\boldsymbol{f})$ has full rank p.

This implies that if not empty, V is smooth and $(n-p)$-equidimensional and $\boldsymbol{f}$ generates its vanishing ideal. As a further consequence, the set $W(\pi_1,V)$ of critical points of π_1 on V consists exactly of those points $\mathbf{x}$ that satisfy the conditions

$$f_1(\boldsymbol{x}) = \cdots = f_p(\boldsymbol{x}) = 0, \qquad \mathrm{rank}(\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f},1)) \leq p-1,$$

and the minimizers of π_1 on $V \cap \mathbb{R}^n$ form a subset of $W(\pi_1,V)$.

(2) The truncated jacobian matrix $\mathrm{jac}(\boldsymbol{f},1)$ has rank $p-1$ at all $\boldsymbol{x} \in W(\pi_1,V)$.

(3) The set $W(\pi_1,V)$ is finite.

(4) For any $(p-1)$-minor m of $\mathrm{jac}(\boldsymbol{f},1)$, the polynomials $\boldsymbol{f}, \mathsf{Minors}(\boldsymbol{f},m)$ define $W(\pi_1,V)$ in the Zariski open set $\mathcal{O}(m)$ defined by $m \neq 0$ and their jacobian matrix has full rank n at any point of $W(\pi_1,V) \cap \mathcal{O}(m)$.

Let $\mathbb{C}[X_1,\ldots,X_n]_D$ denote the subset of polynomials in $\mathbb{C}[X_1,\ldots,X_n]$ of degree at most D; we can see this as an affine space of dimension $\binom{n+D}{n}$. We will prove that assumption G is generic, in the following sense; the proof of this proposition occupies the rest of this subsection.

Proposition 20. *Let D be a positive integer. There exists a nonempty Zariski open set $\mathcal{O} \subset \mathbb{C}[X_1,\ldots,X_n]_D^p$ such that any $\boldsymbol{f} \in \mathcal{O}$ satisfies G.*

Let $N = \binom{n+D}{n}$ be the number of monomials of degree $\leq D$ in $\mathbb{C}[X_1,\ldots,X_n]$ and denote these monomials by $1 = m_1,\ldots,m_N$; they form a $\mathbb{C}$-vector space basis of $\mathbb{C}[X_1,\ldots,X_n]_D$. For $1 \leq i \leq p$, denote by $\mathfrak{f}_i$ the polynomial $\sum_{j=1}^N \gamma_{i,j} m_j$, where the $\gamma_{i,j}$'s are new indeterminates, and by $\mathbb{K}$ the field of rational fractions $\mathbb{C}(\gamma_{1,1},\ldots,\gamma_{p,N})$. We consider the sequence $\mathfrak{F} = (\mathfrak{f}_1,\ldots,\mathfrak{f}_p)$; it is seen as a sequence of polynomials in $\mathbb{K}[X_1,\ldots,X_n]$.

Polynomials in $\mathbb{C}[X_1,\ldots,X_n]_D$ are obtained by instantiating the indeterminates $\gamma_{i,j}$ to elements of $\mathbb{C}$, so we can we identify a polynomial f to the sequence of coefficients of $m_1,\ldots,m_N$ in it. In a similar way, a sequence of polynomials in $\mathbb{C}[X_1,\ldots,X_n]_D^p$ is identified to elements of $\mathbb{C}^{Np}$ and, by abuse of notation, given a subset $A \subset \mathbb{C}^{Np}$ we may use the notation "$\boldsymbol{f} = (f_1,\ldots,f_p) \in A$" to denote a family of polynomials in $\mathbb{C}[X_1,\ldots,X_n]_D^p$ whose sequence of coefficients belongs to A.

Genericity of $\mathsf{G}(1)$. We first prove that for a generic choice of $\boldsymbol{f}$, at any point of $V(\boldsymbol{f})$, the jacobian matrix $\mathrm{jac}(\boldsymbol{f})$ of $\boldsymbol{f}$ has full rank p.

In this paragraph, we consider the polynomials $\mathfrak{h}_i = \mathfrak{f}_i - \gamma_{i,1}$ for $1 \leq i \leq p$; hence $\mathfrak{h}_i$ has no constant term, and belongs to $\mathbb{K}'[X_1, \ldots, X_n]$, where $\mathbb{K}' \subset \mathbb{K}$ is the field of rational fractions $\mathbb{C}((\gamma_{i,j})_{1 \leq i \leq p, 2 \leq j \leq N})$. Let ψ denote the mapping

$$\psi : \overline{\mathbb{K}'}^n \longrightarrow \overline{\mathbb{K}'}^p$$
$$\mathbf{c} \longmapsto (\mathfrak{h}_1(\mathbf{c}), \ldots, \mathfrak{h}_p(\mathbf{c})).$$

Let $K_0 \subset \overline{\mathbb{K}'}^p$ be the set of critical values of ψ. By Sard's Theorem [49, Chap. 2, Sec. 6.2, Thm 2], K_0 is contained in a proper closed subset of the closure of the image of ψ, and thus of $\overline{\mathbb{K}'}^p$.

We use $\gamma_{1,1}, \ldots, \gamma_{p,1}$ as coordinates in the target space. Then, the ideal of $\mathbb{K}'[\mathbf{X}, \gamma_{1,1}, \ldots, \gamma_{p,1}]$ generated by $\mathfrak{h}_1 + \gamma_{1,1}, \ldots, \mathfrak{h}_p + \gamma_{p,1}$ and the maximal minors of $\mathrm{jac}(\mathfrak{h}_1, \ldots, \mathfrak{h}_p)$ contains a non-zero polynomial $P \in \mathbb{K}'[\gamma_{1,1}, \ldots, \gamma_{p,1}]$. Up to multiplying P by a suitable denominator, we can then assume that P lies in $\mathbb{C}[(\gamma_{i,j})_{1 \leq i \leq p, 1 \leq j \leq N}]$ and belongs to the ideal generated by the above polynomials in $\mathbb{C}[(\gamma_{i,j})_{1 \leq i \leq p, 1 \leq j \leq N}, \mathbf{X}]$.

Remark now that the generators we consider can be rewritten as $\mathfrak{f}_1, \ldots, \mathfrak{f}_p$ and the maximal minors of $\mathrm{jac}(\mathfrak{f}_1, \ldots, \mathfrak{f}_p)$. Thus, if we define $\mathscr{O}_1 \subset \mathbb{C}^{Np}$ as the non-empty Zariski open $\mathbb{C}^{Np} - V(P)$, we deduce that for any $\boldsymbol{f} \in \mathscr{O}_1$, $\mathsf{G}(1)$ holds.

Genericity of $\mathsf{G}(2)$. For the remaining genericity properties, we will use the fact that for any system $\boldsymbol{f}$ that satisfies $\mathsf{G}(1)$, these properties are known to hold in generic coordinates. From this, we will deduce our claims using several times the following arguments.

Let $\mathfrak{A}$ be the $n \times n$ matrix $(\alpha_{k,\ell})_{1 \leq k, \ell \leq n}$, where the $\alpha_{k,\ell}$'s are new indeterminates. We denote by $\mathbb{F}$ the field of rational fractions in the indeterminates $\gamma_{i,j}$ and $\alpha_{k,\ell}$ (for $1 \leq i \leq p$, $1 \leq j \leq N$ and $1 \leq k, \ell \leq n$) with coefficients in $\mathbb{C}$; we will also consider its subfield $\mathbb{F}' = \mathbb{C}(\alpha_{1,1}, \ldots, \alpha_{n,n})$. For $f \in \mathbb{F}[X_1, \ldots, X_n]$, we denote by $f^{\mathfrak{A}}$ the polynomial $f(\mathfrak{A}\mathbf{X})$; for a subset $F \subset \mathbb{F}[X_1, \ldots, X_n]$, $F^{\mathfrak{A}}$ denotes the set $\{f^{\mathfrak{A}} \mid f \in F\}$. These notations are naturally extended to the situation where we let a matrix $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$ act on $(X_1, \ldots, X_n)$

We prove here that for a generic choice of $\boldsymbol{f}$, the matrix $\mathrm{jac}(\boldsymbol{f}, 1)$ has rank at least $p - 1$ at any $\boldsymbol{x}$ in $V(\boldsymbol{f})$; this will prove that it has rank exactly $p-1$ at the points of $W(\pi_1, V(\boldsymbol{f}))$.

Let $\Delta(\mathfrak{F}, \mathfrak{A})$ be the vector of $(p-1)$-minors of $\mathrm{jac}(\mathfrak{F}^{\mathfrak{A}}, 1)$ and $\mathfrak{S}(\mathfrak{F}, \mathfrak{A}) \subset \mathbb{F}[X_1, \ldots, X_n]$ be the polynomial sequence

$$\mathfrak{F}^{\mathfrak{A}}, \Delta(\mathfrak{F}, \mathfrak{A});$$

remark that the polynomials $\Delta(\mathfrak{F}, \mathfrak{A})$ are *not* obtained by applying the change of variables $\mathfrak{A}$ to the $(p-1)$-minors of $\mathrm{jac}(\mathfrak{F}, 1)$. For $\boldsymbol{f} \in \mathbb{C}^{Np}$ and/or $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$, we denote by $\mathfrak{S}(\boldsymbol{f}, \mathfrak{A}) \subset \mathbb{F}'[X_1, \ldots, X_n]$, $\mathfrak{S}(\mathfrak{F}, \mathbf{A}) \subset \mathbb{K}[X_1, \ldots, X_n]$ and $\mathfrak{S}(\boldsymbol{f}, \mathbf{A}) \subset \mathbb{C}[X_1, \ldots, X_n]$ the polynomial sequences obtained by instantiating $\mathfrak{F}$ to $\boldsymbol{f}$ and/or $\mathfrak{A}$ to $\mathbf{A}$.

Let r be the dimension of the zero-set of $\mathfrak{S}(\mathfrak{F}, \mathfrak{A})$ over an algebraic closure of $\mathbb{F}$. We first prove that this dimension is -1.

Indeed, there exists a non-polynomial Λ in $\mathbb{C}[(\gamma_{i,j})_{1 \leq i \leq p, 1 \leq j \leq N}, (\alpha_{k,\ell})_{1 \leq k, \ell \leq n}]$ such that for any $\boldsymbol{f}, \mathbf{A}$ that do not cancel Λ, the zero-set of the system $\mathfrak{S}(\boldsymbol{f}, \mathbf{A})$ has dimension r as well.

28

Fix $\boldsymbol{f}$ such that $\Lambda(\boldsymbol{f}, \mathfrak{A})$ is not zero and such that $\boldsymbol{f}$ belongs to $\mathscr{O}_1$ (such an $\boldsymbol{f}$ exists). Since $\boldsymbol{f}$ then satisfies $\mathsf{G}(1)$, using the third item in [46, Proposition 4.1.1], we deduce that there exists a non-empty Zariski open set $\mathscr{A}_{\boldsymbol{f}}$ of $\mathbb{C}^{n \times n}$ such that for $\mathbf{A} \in \mathscr{A}_{\boldsymbol{f}}$, the zero-set of $\mathfrak{S}(\boldsymbol{f}, \mathbf{A})$ has dimension -1. On the other hand, by assumption on $\boldsymbol{f}$, for a generic $\mathbf{A}$, the value $\Lambda(\boldsymbol{f}, \mathbf{A})$ is not zero; in that case, the zero-set of $\mathfrak{S}(\boldsymbol{f}, \mathbf{A})$ has dimension r. Thus, our claim $r = -1$ is proved.

Repeating the specializing argument, but with respect to the variables $\alpha_{k,\ell}$, we choose $\mathbf{A} \in \mathscr{A}$ such that $\Lambda_{\mathbf{A}} = \Lambda((\gamma_{i,j})_{1 \le i \le p, 1 \le j \le N}, \mathbf{A})$ is non zero. Letting $\mathscr{O}_{\mathbf{A}} \subset \mathbb{C}^{Np}$ be the complement of $V(\Lambda_{\mathbf{A}})$, we deduce that for $\boldsymbol{f} \in \mathscr{O}_{\mathbf{A}}$, the system $\mathfrak{S}(\boldsymbol{f}, \mathbf{A})$ is inconsistent, which means that the polynomials $\boldsymbol{f}^{\mathbf{A}}$ satisfy $\mathsf{G}(2)$. The transformation $\varphi : \boldsymbol{f} \in \mathbb{C}[X_1, \ldots, X_n]_D^p \mapsto \boldsymbol{f}^{\mathbf{A}} = \boldsymbol{f}(\mathbf{A}\mathbf{X}) \in \mathbb{C}[X_1, \ldots, X_n]_D^p$ is linear and invertible. The image $\mathscr{O}_2 = \varphi(\mathscr{O}_{\mathbf{A}})$ is thus still Zariski open and satisfies our requirements.

Genericity of $\mathsf{G}(3)$. We next prove that for a generic choice of $\boldsymbol{f}$, the polar variety $W(\pi_1, V(\boldsymbol{f}))$ is finite. The proof is similar to the one above, with a few modifications. This time, we define $\Delta'(\mathfrak{F}, \mathfrak{A})$ be the vector of p-minors of $\mathrm{jac}(\mathfrak{F}^{\mathfrak{A}}, 1)$, and let $\mathfrak{S}'(\mathfrak{F}, \mathfrak{A}) \subset \mathbb{F}[X_1, \ldots, X_n]$ be system of the polynomials $(\mathfrak{F}^{\mathfrak{A}}, \Delta'(\mathfrak{F}, \mathfrak{A}))$. The polynomials $\mathfrak{S}'(\boldsymbol{f}, \mathfrak{A})$ and $\mathfrak{S}'(\boldsymbol{f}, \mathbf{A})$ are defined as above.

Then, we proceed as before, noticing that there exists a non-zero polynomial Λ' in $\mathbb{C}[(\gamma_{i,j})_{1 \le i \le p, 1 \le j \le N}, (\alpha_{k,\ell})_{1 \le k, \ell \le n}]$ such that for any $\boldsymbol{f}, \mathbf{A}$ that do not cancel Λ', the zero-sets of the systems $\mathfrak{S}'(\mathfrak{F}, \mathfrak{A})$ and $\mathfrak{S}'(\boldsymbol{f}, \mathbf{A})$ have the same dimension r', the former being over an algebraic closure of $\mathbb{F}$. Fix an $\boldsymbol{f}$ such that $\Lambda'(\boldsymbol{f}, \mathfrak{A})$ is not zero and that satisfies $\mathsf{G}(1)$. The second item of [46, Proposition 4.1.1] shows that for $\mathbf{A}$ in a suitable Zariski open subset of $\mathbb{C}^{n \times n}$, $W(\pi_1, V(\boldsymbol{f}^{\mathbf{A}}))$ is finite, or equivalently $\mathfrak{S}'(\boldsymbol{f}, \mathbf{A})$ is finite. As for the previous property, this now implies that r' is either 0 or -1.

In particular, there exists $\mathbf{A}$ such that $\mathfrak{S}'(\mathfrak{F}, \mathbf{A})$ has dimension r' as well; thus, this $\mathbf{A}$ being fixed, we deduce that there exists an open set $\mathscr{O}'_{\mathbf{A}}$ of $\mathbb{C}^{Np}$ such that for $\boldsymbol{f}$ in $\mathscr{O}'_{\mathbf{A}}$, $W(\pi_1, V(\boldsymbol{f}^{\mathbf{A}}))$ is finite. The conclusion follows as in the previous paragraph, by defining $\mathscr{O}_3 = \varphi(\mathscr{O}'_{\mathbf{A}})$.

Genericity of $\mathsf{G}(4)$. We first prove that for $\boldsymbol{f} = (f_1, \ldots, f_p) \in \mathscr{O}_1$, the first claim in $\mathsf{G}(4)$ holds. Let m be a $(p-1)$-minor of $\mathrm{jac}(\boldsymbol{f}, 1)$; without loss of generality, we assume that this minor is the upper left minor.

Take $\boldsymbol{x}$ that cancels all of $\boldsymbol{f}, \mathsf{Minors}(\boldsymbol{f}, m)$, and such that $m(\boldsymbol{x}) \ne 0$; we prove that $\boldsymbol{x}$ belongs to $W(\pi_1, V(\boldsymbol{f}))$. Indeed, by elementary linear algebra (using Cramer's rules), we deduce that there exists a non-zero row vector $[\lambda_1, \ldots, \lambda_p]$ such that

$$f_1(\boldsymbol{x}) = \cdots = f_p(\boldsymbol{x}) = 0, \qquad [\lambda_1, \ldots, \lambda_p] \cdot \mathrm{jac}(\boldsymbol{f}, 1) = [0, \ldots, 0]^t.$$

We deduce that $\mathrm{jac}(\boldsymbol{f}, 1)$ is rank deficient at $\boldsymbol{x}$, and as pointed out in the statement of $\mathsf{G}(1)$ given above, this implies that $\boldsymbol{x}$ belongs to $W(\pi_1, V(\boldsymbol{f}))$. For the reverse inclusion, take now $\boldsymbol{x} \in W(\pi_1, V(\boldsymbol{f})) \cap \mathcal{O}(m)$. This implies that $\mathrm{jac}(\boldsymbol{f}, 1)$ is rank deficient at $\boldsymbol{x}$, so that

all minors in $\mathsf{Minors}(\boldsymbol{f}, m)$ vanish at $\boldsymbol{x}$. Hence, we proved that in the open set defined by $m \neq 0$, $W(\pi_1, V(\boldsymbol{f}))$ is the zero-set of $\boldsymbol{f}, \mathsf{Minors}(\boldsymbol{f}, m)$.

Finally, we have to prove that for a generic choice of $\boldsymbol{f}$, the Jacobian matrix of the polynomials $\boldsymbol{f}, \mathsf{Minors}(\boldsymbol{f}, m)$ has full rank n at every point in $W(\pi_1, V(\boldsymbol{f}))$ where m does not vanish. The proof is again modeled on the pattern of our proof of $\mathsf{G}(2)$.

Consider the polynomials $\mathfrak{S}''(\mathfrak{F}, \mathfrak{A})$, consisting of $\mathfrak{F}^{\mathfrak{A}}, \mathsf{Minors}(\mathfrak{F}^{\mathfrak{A}}, m_{\mathfrak{A}})$, where $m_{\mathfrak{A}}$ denotes the top-left $(p-1)$-minor of $\mathrm{jac}(\mathfrak{F}^{\mathfrak{A}}, 1)$, together with their Jacobian determinant $C_{\mathfrak{A}}$ and the polynomials $m_{\mathfrak{A}} T - 1$, where T is a new variable. We first prove that this system has no solution, over an algebraic closure of $\mathbb{F}$.

As we did before, we notice that there exists a non-zero polynomial Λ'' in $\mathbb{C}[(\gamma_{i,j})_{1 \leq i \leq p, 1 \leq j \leq N}, (\alpha_{k,\ell})_{1 \leq k, \ell \leq n}]$ such that for any $\boldsymbol{f}, \mathbf{A}$ that do not cancel Λ'', the zero-sets of the systems $\mathfrak{S}''(\mathfrak{F}, \mathfrak{A})$ and $\mathfrak{S}''(\boldsymbol{f}, \mathbf{A})$ have the same dimension r''. Again, we choose $\boldsymbol{f}$ in $\mathscr{O}_1$ and such that $\Lambda''(\boldsymbol{f}, \mathfrak{A})$ is not zero.

For such an $\boldsymbol{f}$, because $V(\boldsymbol{f})$ is smooth, the third and fourth item of [46, Proposition 4.1.1] prove that for a generic choice of $\mathbf{A}$, the Jacobian matrix of $\boldsymbol{f}^{\mathbf{A}}, \mathsf{Minors}(\boldsymbol{f}^{\mathbf{A}}, m_{\mathbf{A}})$ has full rank n at every point of $W(\pi_1, V(f^{\mathbf{A}})) \cap \mathcal{O}(m_{\mathbf{A}})$; as a result, for such an $\mathbf{A}$, $\mathfrak{S}''(\boldsymbol{f}, \mathbf{A})$ defines the empty set. As before, this implies that $\mathfrak{S}''(\mathfrak{F}, \mathfrak{A})$ defines the empty set as well. This in turn implies that for a generic choice of $\mathbf{A}$, the system $\mathfrak{S}''(\mathfrak{F}, \mathbf{A})$ defines the empty set. Fixing such an $\mathbf{A}$, we deduce that for a generic choice of $\boldsymbol{f}$, $\mathfrak{S}''(\boldsymbol{f}, \mathbf{A})$ defines the empty set as well; in other words, $\boldsymbol{f}^{\mathbf{A}}$ satisfies $\mathsf{G}(4)$. Undoing the change of variables as we did before proves the last point in $\mathsf{G}(4)$.

4.2   A Lagrangian reformulation

Suppose in all that follows that $\boldsymbol{f}$ satisfies G and let $V = V(\boldsymbol{f})$. We now show that under assumption G, we can derive a Lagrangian formulation for $W(\pi_1, V)$ that still satisfies regularity properties. In particular, by $\mathsf{G}(3)$, $W(\pi_1, V)$ is finite. For any $\boldsymbol{x}$ in this set, by $\mathsf{G}(2)$, there exists a non-zero vector $\boldsymbol{\ell_x} = [\ell_{\boldsymbol{x},1}, \ldots, \ell_{\boldsymbol{x},p}]$ in the left nullspace of $\mathrm{jac}(\boldsymbol{f}, 1)$, and this vector is unique up to a multiplicative constant.

Proposition 21. *Suppose that $\boldsymbol{u} = (u_1, \ldots, u_p) \in \mathbb{C}^n$ is such that $u_1 \ell_{\boldsymbol{x},1} + \cdots + u_p \ell_{\boldsymbol{x},p} \neq 0$ for all $\boldsymbol{x}$ in $W(\pi_1, V)$. Then the system in variables $X_1, \ldots, X_n, L_1, \ldots, L_p$*

$$\mathcal{W}_{\boldsymbol{u}} = \big(\boldsymbol{f}, \quad [L_1 \ \cdots \ L_p] \cdot \mathrm{jac}(\boldsymbol{f}, 1), \quad u_1 L_1 + \cdots + u_p L_p - 1\big)$$

is such that

$$Z(\mathcal{W}_{\boldsymbol{u}}) = \left(\boldsymbol{x}, \frac{1}{u_1 \ell_{\boldsymbol{x},1} + \cdots + u_p \ell_{\boldsymbol{x},p}} \ell_{\boldsymbol{x}}\right)_{\boldsymbol{x} \in W(\pi_1, V)} \subset \mathbb{C}^{n+p}.$$

Proof. First, take $(\boldsymbol{x}, \boldsymbol{\ell})$ in $V(\mathcal{W}_{\boldsymbol{u}})$. The fact that $\boldsymbol{x}$ and $\boldsymbol{\ell}$ cancel both $\boldsymbol{f}$ and $[L_1 \ \cdots \ L_p] \cdot \mathrm{jac}(\boldsymbol{f}, 1)$ implies that $\boldsymbol{x}$ is in $W(\pi_1, V)$ and that $\boldsymbol{\ell} = \lambda \boldsymbol{\ell_x}$ for some non-zero constant λ. The fact that $u_1 \ell_1 + \cdots + u_p \ell_p = 1$ implies that $(u_1 \ell_{\boldsymbol{x},1} + \cdots + u_p \ell_{\boldsymbol{x},p})\lambda = 1$. Thus, we have proved that $V(\mathcal{W}_{\boldsymbol{u}})$ is contained in the right-hand side.

Conversely, consider a point $(\boldsymbol{x}, 1/(u_1\ell_{\boldsymbol{x},1} + \cdots + u_p\ell_{\boldsymbol{x},p})\ell_{\boldsymbol{x}})$, for some $\boldsymbol{x}$ in $W(\pi_1, V)$; one easily sees that it satisfies the defining equations of the zero-set $\mathcal{V}_{\boldsymbol{u}}$, so we have proved that

$$V(\mathcal{W}_{\boldsymbol{u}}) = \left(\boldsymbol{x}, \frac{1}{u_1\ell_{\boldsymbol{x},1} + \cdots + u_p\ell_{\boldsymbol{x},p}}\ell_{\boldsymbol{x}}\right)_{\boldsymbol{x} \in W(\pi_1, V)} \subset \mathbb{C}^{n+p}.$$

We next prove that all solutions are simple. Take $\boldsymbol{x}$ in $W(\pi_1, V)$, together with the corresponding ℓ such that $(\boldsymbol{x}, \ell)$ is in $\mathcal{W}_{\boldsymbol{u}}$. By $\mathsf{G}(3)$, there exists a minor $m_{\boldsymbol{x}}$ of $\mathrm{jac}(\boldsymbol{f}, 1)$ such that $m_{\boldsymbol{x}}(\boldsymbol{x})$ is non-zero; let ι be the index of the missing row. Using Proposition 3.2.7 of [46], we deduce the existence of rational functions $(\rho_j)_{j=1,\dots,p,j\neq\iota}$ in $\mathbb{Q}[\mathbf{X}]$ such that we have equality between ideals

$$\langle \boldsymbol{f}, \quad [L_1 \; \cdots \; L_p] \cdot \mathrm{jac}(\boldsymbol{f}, 1)\rangle = \langle \boldsymbol{f}, \quad L_\iota \mathsf{Minors}(\boldsymbol{f}, m_{\boldsymbol{x}}), \quad (L_j - \rho_j L_\iota)_{j=1,\dots,p,j\neq\iota}\rangle$$

in the localization $\mathbb{Q}[\mathbf{X}, \mathbf{L}]_{m_{\boldsymbol{x}}}$. Add the equation $u_1 L_1 + \cdots + u_p L_p - 1$ to both sides. On the left, we obtain the equations for $\mathcal{W}_{\boldsymbol{u}}$. On the right, we obtain

$$\langle \boldsymbol{f}, \quad L_\iota \mathsf{Minors}(\boldsymbol{f}, m_{\boldsymbol{x}}), \quad (L_j - \rho_j L_\iota)_{j=1,\dots,p,j\neq\iota}, \quad u_1 L_1 + \cdots + u_p L_p - 1\rangle,$$

which is equal to

$$\langle \boldsymbol{f}, \quad L_\iota \mathsf{Minors}(\boldsymbol{f}, m_{\boldsymbol{x}}), \quad (L_j - \rho_j L_\iota)_{j=1,\dots,p,j\neq\iota}, \quad (u_1\rho_1 + \cdots + u_p\rho_p)L_\iota - 1\rangle,$$

provided we write $\rho_\iota = 1$; this is in turn the same ideal as

$$\langle \boldsymbol{f}, \quad \mathsf{Minors}(\boldsymbol{f}, m_{\boldsymbol{x}}), \quad (L_j - \rho_j L_\iota)_{j=1,\dots,p,j\neq\iota}, \quad (u_1\rho_1 + \cdots + u_p\rho_p)L_\iota - 1\rangle.$$

Since $(\boldsymbol{x}, \ell)$ is in $\mathcal{W}_{\boldsymbol{u}}$, and $m_{\boldsymbol{x}}(\boldsymbol{x})$ is non-zero, $(\boldsymbol{x}, \ell)$ must cancel all equations above. In particular, $(u_1\rho_1 + \cdots + u_p\rho_p)(\boldsymbol{x})$ is non-zero.

Now, $\mathsf{G}(3)$ states that the Jacobian matrix of $(\boldsymbol{f}, \mathsf{Minors}(\boldsymbol{f}, m_{\boldsymbol{x}}))$ has full rank at $\boldsymbol{x}$. Writing down that Jacobian of the system above in $\mathbb{Q}[\mathbf{X}, \mathbf{L}]_{m_{\boldsymbol{x}}}$, and using the fact that $(u_1\rho_1 + \cdots + u_p\rho_p)(\boldsymbol{x})$ does not vanish, one sees that this larger Jacobian matrix has full rank $n + p$ at $(\boldsymbol{x}, \ell)$. The equality between ideals seen above implies that it is also the case for the polynomials defining $\mathcal{W}_{\boldsymbol{u}}$. $\qquad\square$

The following lemma shows that one can find a suitable $\boldsymbol{u}$ with small bit-size. The proof is a direct application of Lemma 11.

Proposition 22. *Let δ be an upper bound on the cardinality of $W(\pi_1, V)$ and consider the set of linear forms*

$$u^{(i)} = L_1 + iL_2 + \cdots + i^{p-1}L_p,$$

for i in $\{1, \dots, 8(p-1)\delta\}$. Then at least $7/8$ of these linear forms satisfy the assumptions of Proposition 21.

4.3 Explicit bound for Lagrange systems: proof of Theorem 19

We continue with the notation introduced at the begining of this section and let τ be an upper bound on the height of all f_i, $i = 1, \ldots, p$. Assume that $\boldsymbol{f}$ satisfies the genericity assumptions G defined in the previous subsection. As in the previous subsection, let $\mathcal{W}_{\boldsymbol{u}}$ be the system
$$\left(\boldsymbol{f}, \quad [L_1 \ \cdots \ L_p] \cdot \mathrm{jac}(\boldsymbol{f}, 1), \quad u_1 L_1 + \cdots + u_p L_p - 1\right)$$
with $\mathbf{u}$ chosen as in Proposition 22; we write $\mathbf{g} = (g_1, \ldots, g_{n-1})$ for the equations $[L_1 \ \cdots \ L_p] \cdot \mathrm{jac}(\boldsymbol{f}, 1)$ and $\ell = u_1 L_1 + \cdots + u_p L_p - 1$.

The proof of Theorem 19 simply consists in applying Proposition 18 to $\mathcal{W}_{\boldsymbol{u}}$. Let us review the quantities that appear in that proposition, and adapt them to our present context.

- We have here $m = 2$ and $\boldsymbol{n} = (n, p)$.

- The multi-degrees of the input polynomials are bounded by $\boldsymbol{d} = (d_1, \ldots, d_1, d_2, \ldots, d_2, d_3)$, with $d_1 = (D, 0)$ appearing p times, $d_2 = (D - 1, 1)$ appearing $n - 1$ times and $d_3 = (0, 1)$ appearing once. Expanding the product
$$\{\boldsymbol{d}\} = (D\vartheta_1)^p((D - 1)\vartheta_1 + \vartheta_2)^{n-1}\vartheta_2 \bmod \langle \vartheta_1^{n+1}, \vartheta_2^{p+1} \rangle,$$
we deduce that $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = \binom{n-1}{p-1} D^p (D - 1)^{n-p}$. Proposition 1 then implies that $Z(\mathcal{W}_{\boldsymbol{u}})$ is a finite set of cardinality bounded by this quantity. In the particular case $D = 2$, the expression above becomes $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = \binom{n-1}{p-1} 2^p$.

- The polynomials $\boldsymbol{f}$, $\mathbf{g}$ and ℓ have heights bounded by respectively τ, $\tau + \log(n) + \log(D)$ and $p\log(8p\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$. Using the notation introduced in Eq. (3) of Section 3.1, we now define
$$\begin{aligned} h_1 &= \tau + D\log(n + 1), \\ h_2 &= \tau + \log(n) + \log(D) + (D - 1)\log(n + 1) + \log(p + 1), \\ h_3 &= p\log(8p\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})) + \log(p + 1). \end{aligned}$$

We can then let $\boldsymbol{\eta} = (h_1, \ldots, h_1, h_2, \ldots, h_2, h_3)$, with h_1 appearing p times and h_2 appearing $n - 1$ times. The corresponding arithmetic Chow ring is $\mathbb{R}[\eta, \vartheta_1, \vartheta_2]/\langle \eta^2, \vartheta_1^{n+1}, \vartheta_2^{p+1} \rangle$, and we have

$$\{\boldsymbol{\eta}, \boldsymbol{d}\} = (h_1\eta + D\vartheta_1)^p(h_2\eta + (D - 1)\vartheta_1 + \vartheta_2)^{n-1}(h_3\eta + \vartheta_2) \bmod \langle \eta^2, \vartheta_1^{n+1}, \vartheta_2^{p+1} \rangle.$$

We deduce that

$$\begin{aligned}
\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) = \ & h_1 D^{p-1}(D - 1)^{n-p}\left(\binom{n - 1}{p - 1} + (D - 1)\binom{n - 1}{p - 2}\right) + \\
& h_2 D^p (D - 1)^{n-p-1}\left(\binom{n - 2}{p - 1} + (D - 1)\binom{n - 2}{p - 2}\right) + \\
& h_3 D^p (D - 1)^{n-p-1}\left(\binom{n - 1}{p} + (D - 1)\binom{n - 1}{p - 1}\right) + \\
& D^p (D - 1)^{n-p}\binom{n - 1}{p - 1}.
\end{aligned}$$

Letting $N_1 = \binom{n-1}{p-1} + \binom{n-1}{p-2} = \binom{n}{p-1}$, $N_2 = \binom{n-2}{p-1} + \binom{n-2}{p-2} = \binom{n-1}{p-1}$ and $N_3 = \binom{n-1}{p} + \binom{n-1}{p-1} = \binom{n}{p}$, we deduce that

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \leq D^p (D-1)^{n-p} \left(h_1 N_1 + (h_2 + 1) N_2 + h_3 N_3 \right).$$

Observing that $N_1 + N_2 + N_3 \leq (n+2) N_3$, we obtain the upper bound

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \leq D^p (D-1)^{n-p} \max(h_1, h_2 + 1, h_3)(n+2) N_3.$$

This implies that

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \in O^\tilde{} \left(n \binom{n}{p} (\tau + D) D^p (D-1)^{n-p} \right).$$

In the particular case $D = 2$, we obtain

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \in O^\tilde{} \left(n \binom{n}{p} \tau 2^p \right).$$

- For a general value of D, we will assume that $\boldsymbol{f}$ is given by a straight-line program of length E with constants of height bounded by τ'. Using Baur-Strassen's algorithm, one can deduce a straight-line program with constants of bit size in $O(\tau')$ evaluating $\boldsymbol{f}$ and $\mathrm{jac}(\boldsymbol{f})$ in time $O(pE)$. Hence, one can deduce a straight-line program with constants of bit size in $O(\tau')$ evaluating $\boldsymbol{f}$ and $\mathbf{g}$ in time $O(pE + pn)$.

  Altogether, the system $\mathcal{W}_{\boldsymbol{u}}$ can be evaluated by straight-line program Γ of length $L \in O(pE + pn)$ with constants of height at most $b = \max(\tau', p \log(8p\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})))$.

  When $D = 2$, we use the obvious construction to construct the straight-line program for $\boldsymbol{f}$ (simply expanding all polynomials on the monomial basis), with in this case $E \in O(pn^2)$ and $\tau' = \tau$.

Proposition 22 ensures that $\mathbf{u}$ is well-chosen with probability at least $7/8$. Using the fact that the total number of variables N is at most $2n$, Proposition 18 shows that on input Γ, $\boldsymbol{d}$ and $\boldsymbol{\eta}$, Algorithm NonSingularSolutionsOverZ runs within

$$O^\tilde{} \left(p(E+n)\tau' + \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \left(pE + nD + n^2 \right) n^2 \right)$$

boolean operations (the expression given in that proposition also involves a term of the form $\log(\max(h_1, h_2, h_3))$, but it is polylogarithmic in terms of $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})$). It returns the correct output with probability at least $21/32$, so the overall probability of success is at least $147/256$, as claimed. Using the equalities and inequalities

$$\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = \binom{n-1}{p-1} D^p (D-1)^{n-p}, \quad \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \in O^\tilde{} \left(n \binom{n}{p} (\tau + D) D^p (D-1)^{n-p} \right),$$

the bound on the running time becomes

$$O^\sim\left(p(E+n)\tau' + n^3\binom{n-1}{p-1}\binom{n}{p}(\tau+D)D^{2p}(D-1)^{2(n-p)}(pE+nD+n^2)\right).$$

In the special case $D = 2$, with $E \in O(pn^2)$ and $\tau' = \tau$, this is

$$O^\sim\left(n^5\binom{n-1}{p-1}\binom{n}{p}2^{2p}\tau\right).$$

The height bound on the coefficients in the output follows immediately from Proposition 18 and the bounds on $\mathscr{C}_n(\boldsymbol{d})$ and $\mathscr{H}_n(\boldsymbol{\eta},\boldsymbol{d})$.

References

[1] 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. Birkhaüser, 1996.

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

[3] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: geometry and algorithms. *Journal of Complexity*, 21(4):377–412, 2005.

[4] A. Barvinok. Feasibility testing for systems of real quadratic equations. *Discrete & Computational Geometry*, 10(1):1–13, 1993.

[5] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets (extended abstract). In *STOC*, pages 168–173. ACM, 1996.

[6] D. Bienstock. A note on polynomial solvability of the CDT problem. *SIAM Journal on Optimization*, 26(1):488–498, 2016.

[7] D. Bienstock and A. Michalka. Polynomial solvability of variants of the trust-region subproblem. In *SODA'14*, pages 380–390. SIAM, 2014.

[8] I. Bomze and M. Overton. Narrowing the difficulty gap for the Celis–Dennis–Tapia problem. *Mathematical Programming*, 151(2):459–476, 2014.

[9] M. Celis, J. Dennis, and R. Tapia. A trust region strategy for nonlinear equality constrained optimization. *Numerical optimization*, 1984:71–82, 1985.

[10] X. Chen and Y. Yuan. Strong duality for the cdt subproblem: a necessary and sufficient condition. *J. Comput. Math*, 19(2):113–124, 2009.

[11] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, 2005.

[12] C. D'Andrea, T. Krick, and M. Sombra. Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze. *Annales scientifiques de l'ENS*, 46(4):549–627, 2013.

[13] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[14] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Critical points and gröbner bases: the unmixed case. In *ISSAC*, pages 162–169. ACM, 2012.

[15] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[16] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Groebner bases. In *AAECC*, volume 356 of *LNCS*, pages 247–257. Springer, 1989.

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

[18] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

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

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

[21] A. Greuet and M. Safey El Din. Deciding reachability of the infimum of a multivariate polynomial. In *ISSAC'11*, pages 131–138. ACM, 2011.

[22] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. *SIAM Journal on Optimization*, 24(3):1313–1343, 2014.

[23] D. Grigoriev and D. Pasechnik. Polynomial time computing over quadratic maps I. sampling in real algebraic sets. *Computational complexity*, 14:20–52, 2005.

[24] Q. Guo, M. Safey El Din, and L. Zhi. Computing rational solutions of linear matrix inequalities. In *ISSAC'13*, pages 197–204. ACM, 2013.

[25] J. Heintz, G. Jeronimo, J. Sabia, and P. Solerno. Intersection theory and deformation algorithms: the multi-homogeneous case. Manuscript, 2002.

[26] G. Jeronimo, G. Matera, P. Solerno, and A. Waissbein. Deformation techniques for sparse systems. *Foundations of Computational Mathematics*, 9(1):1–50, 2009.

[27] G. Jeronimo and D. Perrucci. A probabilistic symbolic algorithm to find the minimum of a polynomial function on a basic closed semialgebraic set. *Discrete and Computational Geometry*, 52(2):260–277, 2014.

[28] G. Jeronimo, D. Perrucci, and E. Tsigaridas. On the minimum of a polynomial function on a basic closed semialgebraic set and applications. *SIAM Journal on Optimization*, 23(1):241–255, 2013.

[29] T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109:521–598, 2001.

[30] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die reine und angewandte Mathematik*, 92:1–122, 1882.

[31] J.-B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

[32] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, pages 157–270. Springer, 2009.

[33] F. Le Gall. Powers of tensors and fast matrix multiplication. In *ISSAC'14*, pages 296–303. ACM, 2014.

[34] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *ISSAC'00*, pages 209–216. ACM, 2000.

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

[36] S. Melczer and B. Salvy. Symbolic-numeric tools for analytic combinatorics in several variables. Submitted to ISSAC'16, 2016.

[37] A. Morgan and A. J. Sommese. A homotopy for solving general polynomial systems that respects m-homogeneous structures. *Applied Mathematics and Computations*, 24:101–113, 1987.

[38] S. Morrison. The differential ideal $[P] : M^\infty$. *J. Symb Comp.*, 28:631–656, 1999.

[39] D. Mumford. *Algebraic Geometry I, Complex projective varieties*. Classics in Mathematics. Springer Verlag, 1976.

[40] S. Naldi. Solving rank-constrained semidefinite programs in exact arithmetic. *ArXiv e-prints*, February 2016.

[41] P. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical programming*, 96(2):293–320, 2003.

[42] J. Peng and Y.-X. Yuan. Optimality conditions for the minimization of a quadratic with two quadratic constraints. *SIAM J. Optim.*, 7(3):579–594, 1997.

[43] F. J. Rayner. An algebraically closed field. *Glasgow Mathematical Journal*, 9:146–151, 1968.

[44] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1999.

[45] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a re al algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.

[46] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. arXiv:1307.7836, 2013.

[47] M. Safey El Din and L. Zhi. Computing rational points in convex semialgebraic sets and sum of squares decompositions. *SIAM Journal on Optimization*, 20(6):2876–2889, 2010.

[48] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003.

[49] I. Shafarevich. *Basic Algebraic Geometry 1*. Springer Verlag, 1977.

[50] A. J. Sommese and C. W. Wampler. *The numerical solution of systems of polynomials arising in engineering and science*. World Scientific, 2005.

[51] P.-J. Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM Journal on Optimization*, 24(3):1382–1401, 2014.

[52] Y.-X. Yuan. On a subproblem of trust region algorithms for constrained optimization. *Math. Program. (Ser. A)*, 47(1):53–63, 1990.

[53] O. Zariski and P. Samuel. *Commutative algebra*. Van Nostrand, 1958.