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

Mohab Safey El Din, Éric Schost

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

M. Safey El Din[1], É. Schost[2]

December 9, 2017

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 is 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

1.1 Motivation and problem statement

In this paper, we are interested in exact algorithms 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 constrained optimization problems. This is used in many algorithms for studying real solutions to polynomial systems (see e.g. [2, 3, 42, 5, 43] and references therein). We will also pay particular attention to the situation when the constraints are given as quadratic equations.

We work with polynomials in m groups of variables. Let thus $\boldsymbol{n} = (n_1, \ldots, n_m)$ be positive integers, and consider 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.

Let $\mathbb{K}$ be a field and $\boldsymbol{f} = (f_1, \ldots, f_M)$ in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, for some $M \leq N$ (we will sometimes write $\boldsymbol{f}_M$ instead of $\boldsymbol{f}$, in order to highlight the length of the sequence). We associate to $\boldsymbol{f}$ the algebraic set $Z(\boldsymbol{f})$, 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 $\boldsymbol{f}$ has rank M at $\boldsymbol{x}$. By the Jacobian criterion [12, Chapter 16], $Z(\boldsymbol{f})$ is either empty, or equidimensional of dimension $N - M$, and it is defined over $\mathbb{K}$.

Suppose that $M = N$. 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 show how the same phenomenon holds in terms of bit complexity. Indeed, our goal is to obtain an algorithm for solving such systems whose bit complexity is, up to some extra factors, quadratic in the multi-homogeneous bound and linear in the *heights* of the polynomials in the input system (which is a measure of their bit size).

[1]Sorbonne Universités, UPMC Univ. Paris 06, CNRS, INRIA Paris Center, LIP6, PolSys Team, France
[2]David Cheriton School of Computer Science, University of Waterloo, ON, Canada

In the following paragraphs, we recall the notion of height and the data structure we use to represent $Z(\boldsymbol{f})$. We will also use these notions to describe related works on solving multi-homogeneous systems.

Let us first however describe how such results can be applied to the problem of minimizing the map $\pi_1 : (x_1, \ldots, x_n) \mapsto x_1$ subject to the constraints $h_1 = \cdots = h_p = 0$, with $\mathbf{h} = (h_1, \ldots, h_p) \subset \mathbb{Z}[X_1, \ldots, X_n]$. Assuming that $\mathbf{h}$ is a reduced regular sequence, that the minimizer exists and that the set of minimizers is finite, it is well-known that this problem can be tackled by solving the so-called Lagrange system

$$h_1 = \cdots = h_p = 0,\ [L_1, \ldots, L_p] \begin{bmatrix} \frac{\partial h_1}{\partial X_2} & \cdots & \frac{\partial h_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial h_p}{\partial X_2} & \cdots & \frac{\partial h_p}{\partial X_n} \end{bmatrix} = [0\ \cdots\ 0], u_1 L_1 + \cdots + u_p L_p = 1,$$

where $\mathbf{L} = (L_1, \ldots, L_p)$ are new variables (called Lagrange multipliers) and $(u_1, \ldots, u_p)$ are randomly chosen integers. Hence, using the notation introduced above, we have for this system $m = 2$, $\boldsymbol{n} = (n, p)$, $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2)$ with $\mathbf{X}_1 = (X_1, \ldots, X_n)$ and $\mathbf{X}_2 = \mathbf{L}$.

1.2 Bit size and data structures

1.2.1 Multi-degree, height and bit size

Let $\mathbb{K}$ be a field as above. To a polynomial f in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ we associate its *multi-degree* $\mathrm{mdeg}(f) = (d_1, \ldots, d_m) \in \mathbb{N}^m$, 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 $\underline{d} = (d_1, \ldots, d_m)$ means that $\deg(f, \mathbf{X}_i) \leq d_i$ holds for all i. Similarly, to a sequence of polynomials $\boldsymbol{f}_M$, we associate its multi-degree $\mathrm{mdeg}(\boldsymbol{f}_M) = (\mathrm{mdeg}(f_1), \ldots, \mathrm{mdeg}(f_M))$. Saying that $\boldsymbol{f}_M$ has multi-degree at most $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_M)$, with now all $\underline{d}_i = (d_{i,1}, \ldots, d_{i,m})$ in $\mathbb{N}^m$, means that $\deg(f_i, \mathbf{X}_j) \leq d_{i,j}$ holds for all i, j.

Consider a polynomial f with coefficients in $\mathbb{Q}$. To measure its bit size, we will use its *height*, defined as follows. First, for $a = u/v$ in $\mathbb{Q} - \{0\}$, define the height of a, $\mathrm{ht}(a)$, as $\max(\log(|u|), \log(v))$, with $u \in \mathbb{Z}$ and $v \in \mathbb{N}$ coprime . For a non-zero univariate or multivariate polynomial f with rational coefficients, we let $v \in \mathbb{N}$ be the minimal common denominator of all its non-zero coefficients; then $\mathrm{ht}(f)$ is defined as the maximum of the logarithms of v and of the absolute values of the coefficients of vf (which are integers).

When f has integer coefficients, this is simply the maximum of the logarithms of the absolute values of these coefficients. More generally, for f with rational coefficients, knowing the degree and height of a polynomial with rational coefficients gives us an upper bound on the size of its binary representation. As in the case of degrees, for polynomials $\boldsymbol{f}_M = (f_1, \ldots, f_M)$, we write that $\mathrm{ht}(\boldsymbol{f}_M) = (\mathrm{ht}(f_1), \ldots, \mathrm{ht}(f_M))$, and we say that $\mathrm{ht}(\boldsymbol{f}_M) \leq \boldsymbol{s}$, with $\boldsymbol{s} = (s_1, \ldots, s_M)$, if $\mathrm{ht}(f_i) \leq s_i$ holds for all i.

Given $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_M)$ in $\mathbb{R}^M$ and $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_M)$ with $\underline{d}_i = (d_{1,1}, \ldots, d_{i,m}) \in \mathbb{N}^m$, we denote by $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ the sum of the coefficients of the polynomial

$$\prod_{i=1}^{M} (d_{i,1}\vartheta_1 + \cdots + d_{i,m}\vartheta_m) \mod \langle \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1} \rangle$$

and by $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})$ the sum of the coefficients of the polynomial

$$\prod_{i=1}^{M} (\eta_i\zeta + d_{i,1}\vartheta_1 + \cdots + d_{i,m}\vartheta_m) \mod \langle \zeta^2, \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1} \rangle.$$

1.2.2 Zero-dimensional parametrizations

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

- $\lambda(v_1, \ldots, v_N) = Tq' \bmod q$, where $q' = \frac{\partial q}{\partial T}$;
- 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 [31, 34], and has been used in a host of algorithms in effective algebra [17, 19, 1, 20, 18, 40, 21, 33].

The reason for using a rational parametrization with q' as a denominator is well-known [1, 40, 21]: 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.

1.3 Main results

1.3.1 Algorithm for solving multi-homogeneous polynomial systems

The main result of the paper is a probabilistic algorithm for solving multi-homogeneous systems. Following references such as [19, 20, 18, 21, 33], 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 evaluates the polynomials $\boldsymbol{f}$ from the input variables $\mathbf{X}_1, \ldots, \mathbf{X}_m$; the *length* or *size* L of such an objet is simply the number of operations it performs.

The approach developed here is not new: we start by computing a zero-dimensional parametrization of $Z(\boldsymbol{f} \bmod p)$, for a well-chosen prime p, and lift it modulo powers of p to a zero-dimensional parametrization of $Z(\boldsymbol{f})$. The novelty of the theorem below lies in the use of multi-homogeneous height bounds proved hereafter to control the cost of the process.

The algorithm is randomized, and part of the randomness amounts to choosing the prime p. Constructing primes is a difficult question in itself, and not the topic of this paper; hence, 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 (for a randomized solution to this question, we refer the reader to [16, Section 18.4]). In all the paper, we use the soft-O notation $O^{\sim}$, in order to indicate that we omit polylogarithmic terms.

Theorem 1. *Suppose that* $\boldsymbol{f} = (f_1, \ldots, f_N)$ *satisfies* $\mathrm{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_m)$ *and* $\mathrm{ht}(\boldsymbol{f}) \leq \boldsymbol{s} = (s_1, \ldots, s_N)$*, 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*,* $\boldsymbol{d}$ *and* $\boldsymbol{s}$ *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*

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

boolean operations, with

$$\mathfrak{d} = \max_{1\le i\le N} d_{i,1} + \cdots + d_{i,m}, \quad s = \max_{1\le i\le N}(s_i) \quad \textit{and} \quad \boldsymbol{\eta} = \left(s_i + \sum_{j=1}^{m} \log(n_j+1) d_{i,j} \right)_{1\le i\le N}.$$

The algorithm calls the oracle $\mathscr{O}$ with an input parameter $B = s\mathfrak{d}^{O(N)}$ and the polynomials in the output have degree at most $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ and height $O^{\sim}(\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta},\boldsymbol{d}) + N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$.

A more detailed discussion on the probabilistic aspects and the choice of the prime p is given in Subsection 4.1. Here, we investigate an immediate consequence of Theorem 1, when for all $1 \le i \le N$, we have $\mathrm{mdeg}(f_i) \le \underline{d} = (d_1, \ldots, d_m)$ and $\mathrm{ht}(f_i) \le s$, that is, $\boldsymbol{d} = (\underline{d}, \ldots, \underline{d})$ and $\boldsymbol{s} = (s, \ldots, s)$. Technical but immediate computations show that in this case,

$$\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = d_1^{n_1} \cdots d_m^{n_m} \binom{N}{n_1 \cdots n_m}$$

where $\binom{N}{n_1\cdots n_m}$ is the multinomial coefficient $\frac{N!}{n_1!\cdots n_m!}$ (recall that $N = n_1 + \cdots + n_m$) and

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta},\boldsymbol{d}) \le m(s+\mathfrak{d}+1) d_1^{n_1} \cdots d_m^{n_m} \binom{N}{n_1 \cdots n_m}$$

where $\mathfrak{d} = d_1 + \cdots + d_m$. From this, we obtain the following corollary.

Corollary 2. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ satisfies $\mathrm{mdeg}(f_i) \le \underline{d} = (d_1, \ldots, d_m)$ and $\mathrm{ht}(f_i) \le s$ 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, $\underline{d}$ and s 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

$$O^{\sim}\left(Lb + \left(d_1^{n_1} \cdots d_m^{n_m} \binom{N}{n_1 \cdots n_m} \right)^2 m(s+\mathfrak{d}) \left(L + N\mathfrak{d} + N^2 \right) N(\log(s) + N) \right)$$

boolean operations, with $\mathfrak{d} = d_1 + \cdots + d_m$. The algorithm calls the oracle $\mathscr{O}$ with an input parameter $B = s\mathfrak{d}^{O(N)}$ and the polynomials in the output have degree at most $d_1^{n_1} \cdots d_m^{n_m} \binom{N}{n_1\cdots n_m}$ and height $O^{\sim}(d_1^{n_1} \cdots d_m^{n_m} \binom{N}{n_1\cdots n_m}(m(s+\mathfrak{d})+N))$.

1.3.2 Minimization problems

We describe now the main results on *generic instances* of the problem of minimizing the map $\pi_1 : (x_1, \ldots, x_n) \mapsto x_1$ subject to the constraints $h_1 = \cdots = h_p = 0$, with $\mathbf{h} = (h_1, \ldots, h_p) \subset \mathbb{Z}[X_1, \ldots, X_n]$, using our algorithm for multi-homogeneous systems.

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

$$h_1 = \cdots = h_p = 0, \qquad L_1 \frac{\partial h_1}{\partial X_j} + \cdots + L_p \frac{\partial h_p}{\partial X_j} = 0 \text{ for } 2 \le j \le n, \qquad u_1 L_1 + \cdots + u_p L_p = 1$$

where $\mathbf{L} = L_1, \ldots, L_p$ are new variables and $(u_1, \ldots, u_p)$ 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 $V = V(h_1, \ldots, h_p)$.

Let d be the maximum of the degrees of the polynomials in $\mathbf{h}$. The Lagrange system above possesses a bi-homogeneous structure, with p equations of total 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 5 that we can solve the bi-homogeneous system above in randomized time

$$O^{\sim}\left(p(E+n)s' + \binom{n-1}{p-1}\binom{n}{p}(s+d)d^{2p}(d-1)^{2(n-p)}(pE+nd+n^2)\right),$$

where s is the height of the input polynomials, E is the length of the straight-line program that computes them, and s' is the height of the integers that appear in this straight-line program (in most cases, one expects $s' \leq s$, 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 $O^{\sim}\left(n\binom{n}{p}(s+d)d^p(d-1)^{n-p}\right)$.

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 $s' = s$, which leads to a boolean runtime of the form

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

Taking $p = 1$ as in [35], this is $O^{\sim}\left((s+d)d^{n+2}(d-1)^{2(n-1)}\right)$. In this case, for large d, our result is hardly an improvement over the cost $O^{\sim}(d^{3n}s)$ 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 $s' = s$. As a result, we obtain a running time of $O^{\sim}(n^5\binom{n-1}{p-1}\binom{n}{p}s2^{2p})$ 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 $O^{\sim}(n\binom{n}{p}s2^p)$: when the codimension p is fixed, all these quantities are *polynomial* in n, with the runtime being $O^{\sim}(n^{2p+4}s)$.

We end this section with an easy consequence of the above result, concerning the determination of an isolating interval for $\min_{\boldsymbol{x}\in V\cap\mathbb{R}^n}\pi_1(\boldsymbol{x})$. 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 [35, Section 3], we can then compute boxes of side length $2^{-\sigma}$ around all roots of the system using $O^{\sim}(n\mathscr{C}^2\mathscr{H} + n\mathscr{C}\sigma)$ 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 $O^{\sim}(n^2\binom{n-1}{p-1}^2\binom{n}{p}s2^{3p} + n\binom{n-1}{p-1}2^p\sigma)$ bit operations. For fixed p, the cost of the root isolation step is $O^{\sim}(n^{2p+1}s + n^p\sigma)$, so the whole process is polynomial in n.

As an illustration/application, 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. Taking $p = 3$ as in the CDT problem, the overall cost for computing a zero-dimensional parametrization of the minimizers and computing isolating boxes is $O^{\sim}(n^{10}s + n^3\sigma)$.

1.4 Related work

1.4.1 Multi-homogeneous polynomial systems

As already said, 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 [21, 44], as well as techniques coming from [41, Section 4], 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 (that we are aware of) on the boolean cost of solving polynomial systems that involves their multi-homogeneous structure in such a manner. Our results on the heights of zero-dimensional parametrizations computed by our algorithm rely on objects introduced by, and results due to D'Andrea, Krick and Sombra [11].

Although we do not have boolean complexity bounds to compare with, several results are known in an arithmetic complexity model (where we count base field operations at unit cost). In the bi-homogeneous case, the algorithm in [24] has an arithmetic cost at least $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^5\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')^6$ with $\boldsymbol{n}' = (1, n_1, \dots n_m)$ and $\boldsymbol{d}' = (\underline{d}'_1, \dots, \underline{d}'_m)$, where for all i we set $\underline{d}'_i = (1, d_{i,1}, \dots, d_{i,m})$. Closer to us are two algorithms from [21] and [26]. The geometric resolution algorithm of [21] 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 (see for example those systems appearing in [25]); in addition, we are not aware of a probability analysis for it.

Another line of work exploits properties of resultant formulae to solve multi-homogeneous systems; we refer in particular to [29, 14, 22] among many others and we also mention [13] focusing on the particular case of bilinear systems. In this setting, solving multi-homogeneous polynomial systems mostly reduce to compute determinants of structured submatrices of the Macaulay matrix. The bit complexity results obtained this way are cubic in $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$; exploiting the structure of Macaulay submatrices, we do not know whether a result essentially linear in $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{d})$, such as the one in Theorem 1, could be obtained in this formalism.

1.4.2 Minimization problems

We comment now on related work on minimization problems. If we let d be the maximum of the degrees of the input polynomials, it is known that the critical point method runs in time $d^{O(n)}$ [7, 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 [15] and [47] establish that if the polynomials $h_1, \dots, h_p$ 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, with $d = 2$, 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 $\omega < 2.38$ [32]; 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.

The quadratic case has actually been known to be solvable in $n^{O(p^2)}$ bit operations since Barvinok's paper [6]; this was later improved to $n^{O(p)}$ by Grigoriev and Vorobjov 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 $s = 2$ and p fixed, the running time is $O^{\sim}(n^{2p+5} + n^{3p})$ arithmetic operations.

Fewer references discuss bit complexity. When $p = 1$, [35, Prop. 3.8 and Lemma 4.1] give boolean complexity estimates of the form $O^{\sim}(sd^{3n})$ for critical point computation on a hypersurface, under some genericity assumptions on the input; here, s 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]; they turn out to be of the same order as the ones we derive, but no algorithm with bit complexity depending on these bounds is given.

1.5 Plan of the paper

We start by recalling basic notions and fixing notation in Section 2. In particular, this section states height bounds for the output of our algorithms; the proof of these bounds is postponed to the end of the paper in Section 6. Section 3 gives a symbolic homotopy deformation algorithm dedicated to multi-homogeneous cases; in the main algorithm, we apply this result over a prime field. Section 4 discusses computations over the rationals, with a cost analysis in the boolean model. We finally apply this to our minimization problem in Section 5.

Acknowledgments. The first author is member of and supported by Institut Universitaire de France. The second author is supported by an NSERC Discovery Grant.

2 Notation and preliminaries

2.1 Basic notions

In the whole paper, we use freely basic notions such as dimension, degree, reducibility and irreducibility, smoothness..., of algebraic sets. We recall these basic notions below and we refer the reader to references such as [48, 38, 45, 12] for more details.

For a field $\mathbb{K}$ and an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, a $\mathbb{K}$-algebraic set $V \subset \overline{\mathbb{K}}^N$ is the set of common solutions in $\overline{\mathbb{K}}^N$ to N-variate polynomial equations with coefficients in $\mathbb{K}$. Usually, the base field $\mathbb{K}$ will be clear from the context; in this case we simply say *algebraic sets* for $\mathbb{K}$-algebraic sets.

For a sequence of polynomials $\boldsymbol{f}_M = (f_1, \ldots, f_M)$ in the ring of N-variate polynomials with coefficients in $\mathbb{K}$, $V(\boldsymbol{f}) \subset \overline{\mathbb{K}}^N$ denotes the algebraic set defined by $f_1 = \cdots = f_M = 0$. The ideal generated by $\boldsymbol{f}$ is denoted by $\langle \boldsymbol{f} \rangle$. The ideal associated to $V(\boldsymbol{f})$ is the set of polynomials that vanish at all points of $V(\boldsymbol{f})$.

For an algebraic set $V = V(\boldsymbol{f})$, the dimension $\dim(V)$ of V is the Krull dimension of the coordinate ring of V; zero-dimensional algebraic sets are non-empty finite algebraic sets. By convention, the empty algebraic set has dimension -1.

When V is an irreducible algebraic set, the degree of V is the number of points lying in the intersection of V with $\dim(V)$ generic hyperplanes. The degree of an arbitrary algebraic set is the sum of the degrees of its irreducible components. When the algebraic set under consideration has dimension zero, its degree is its cardinality.

An algebraic set $V = V(\boldsymbol{f}) \subset \overline{\mathbb{K}}^N$ is said to be equidimensional when all its irreducible components have the same dimension. In this case, assuming that $\boldsymbol{f}$ generates a radical ideal, the smooth points of V are those points at which the rank of the Jacobian matrix of $\boldsymbol{f}$ is the codimension of V, *i.e.*, $N - \dim(V)$. Those points which are not smooth are called singular.

2.2 Chow ring and arithmetic Chow ring

We recall hereafter definitions for Chow rings and arithmetic Chow rings; the latter ones are an arithmetic analogue to Chow rings due to D'Andrea, Krick and Sombra [11], on which most of our bit size estimates will rely.

For a field $\mathbb{K}$, an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, and an m-uple $\boldsymbol{n} = (n_1, \ldots, n_m)$, we denote by $\mathbb{P}^{\boldsymbol{n}}(\overline{\mathbb{K}})$ the multi-projective space $\mathbb{P}^{n_1}(\overline{\mathbb{K}}) \times \cdots \times \mathbb{P}^{n_m}(\overline{\mathbb{K}})$. Consider the ring of truncated power series

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

it is the *Chow ring* of the multi-projective space $\mathbb{P}^{\boldsymbol{n}}(\overline{\mathbb{K}})$. For $\mathbb{K} = \mathbb{Q}$, we also define

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

this is called the *arithmetic Chow ring* of $\mathbb{Q}$. Since the field we use will be clear from the context, we will use the simpler notations $A^*(\mathbb{P}^{\boldsymbol{n}})$ and $A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z})$ for Chow rings and arithmetic Chow rings.

Now, given a multi-degree $\underline{d} = (d_1, \ldots, d_m)$ and a non-negative real number η, we set

$$\chi(\underline{d}) = d_1\vartheta_1 + \cdots + d_m\vartheta_m \in A^*(\mathbb{P}^{\boldsymbol{n}})$$

and

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

Given vectors $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_M)$ and $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_M)$, with all $\underline{d}_i$ in $\mathbb{N}^m$ and all η_i in $\mathbb{R}_{\geq 0}$, we set

$$\boldsymbol{\chi}(\boldsymbol{d}) = \chi(\underline{d}_1) \cdots \chi(\underline{d}_M) \in A^*(\mathbb{P}^{\boldsymbol{n}}).$$

and

$$\boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d}) = \chi(\eta_1, \underline{d}_1) \cdots \chi(\eta_M, \underline{d}_M) \in A^*(\mathbb{P}^{\boldsymbol{n}}, \mathbb{Z}).$$

For $\boldsymbol{c} = (c_1, \ldots, c_m) \in \mathbb{N}^m$, we denote in the sequel $\vartheta_1^{c_1} \cdots \vartheta_m^{c_m}$ by $\vartheta^{\boldsymbol{c}}$. Note that all monomials appearing in $\boldsymbol{\chi}(\boldsymbol{d})$ and $\boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d})$ have total degree M; then, we define the quantities

$$\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = \sum_{\boldsymbol{c} \in \mathbb{N}^m} \operatorname{coeff}(\boldsymbol{\chi}(\boldsymbol{d}), \vartheta^{\boldsymbol{c}})$$

and

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) = \sum_{\boldsymbol{c} \in \mathbb{N}^m,\ |\boldsymbol{c}| = M-1} \operatorname{coeff}(\boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d}), \zeta\ \vartheta^{\boldsymbol{c}}) + \sum_{\boldsymbol{c} \in \mathbb{N}^m,\ |\boldsymbol{c}| = M} \operatorname{coeff}(\boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d}), \vartheta^{\boldsymbol{c}}).$$

Note that they coincide with the quantities defined in Subsection 1.2. Observe also that all coefficients of $\boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d})$ not taken into account in the above sums are necessarily zero.

The quantities $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ and $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})$ play a crucial role for bounding the degree and the height of the output of the algorithms described in the sequel. As an illustration, the following degree inequality is proved in [43, Proposition I.1, electronic appendix]. In what follows, we let $\mathbf{X}_1, \ldots, \mathbf{X}_m$ be blocks of variables of respective lengths $n_1, \ldots, n_m$, as defined in the introduction.

Proposition 3. *Let $\boldsymbol{f} = (f_1, \ldots, f_M)$ be polynomials in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, with $\operatorname{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d}$. Then, the $(N - M)$-equidimensional component of $V(\boldsymbol{f})$ 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 [36].

All these definitions being written, we can state the new result of this paragraph. Its proof is given in Section 6.

Proposition 4. *Let $\boldsymbol{f} = (f_1, \ldots, f_N)$ be polynomials in $\mathbb{Z}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, with $\operatorname{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_N)$ and $\underline{d}_i = (d_{i,1}, \ldots, d_{i,m})$ for all i, and $\operatorname{ht}(\boldsymbol{f}) \leq \boldsymbol{s} = (s_1, \ldots, s_N)$; let also 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 of $Z(\boldsymbol{f})$ associated to λ have height at most $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + (b + 4\log(N+2))\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$, with*

$$\boldsymbol{\eta} = \left(s_i + \sum_{j=1}^{m} \log(n_j + 1) d_{i,j} \right)_{1 \leq i \leq N}.$$

3 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 of respective lengths $(n_1, \ldots, n_m)$, as explained in the introduction. Our goal here is to give a symbolic homotopy algorithm to compute $Z(\boldsymbol{f})$, where $\boldsymbol{f} = (f_1, \ldots, f_N)$ has coefficients in $\mathbb{K}$, 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 3.1.

3.1 Main statement

In order to compute a zero-dimensional parametrization of the algebraic set $Z(\boldsymbol{f})$, we use a symbolic adaptation of multi-homogeneous homotopy continuation algorithms. In the context of numerical continuation techniques, this approach is detailed in [46] and references therein; in a symbolic context, the algorithm underlying the following proposition is inspired by e.g. the algorithm in [24], that applies in the bi-homogeneous case.

We need here to introduce the following notation. Given a vector $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_M)$, with $\underline{d}_i = (d_{i,1}, \ldots, d_{i,m})$ for all i, we define the tuple $\boldsymbol{d}'$ as $\boldsymbol{d}' = (\underline{d}'_1, \ldots, \underline{d}'_M)$, with $\underline{d}'_i = (1, d_{i,1}, \ldots, d_{i,m}) \in \mathbb{N}^{m+1}$ for all i, together with $\boldsymbol{n}' = (1, n_1, \ldots, n_m)$. If we see $\boldsymbol{d}$ as being a vector of multi-degrees, this corresponds to adding one new variable (written t below) and considering polynomials of degree 1 in t and multi-degree $\boldsymbol{d}$ in $\mathbf{X}_1, \ldots, \mathbf{X}_m$. This allows us to introduce the integer $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$, which we define as we did for $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ above. Our convention was to use variables $\vartheta_1, \ldots, \vartheta_m$ for $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$; to define $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$, we introduce a new variable ϑ_0 and let $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$ be the sum of the coefficients of the polynomial

$$\prod_{i=1}^{M} (\vartheta_0 + d_{i,1}\vartheta_1 + \cdots + d_{i,m}\vartheta_m) \mod \langle \vartheta_0^2, \vartheta_1^{n_1+1}, \ldots, \vartheta_m^{n_m+1} \rangle.$$

Proposition 5. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ has multi-degree at most $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_N)$, with all $\underline{d}_i$ 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*

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

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 degree less than that of $Z(\boldsymbol{f})$,*
- *or* fail.

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

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

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 $\boldsymbol{n}' = (1, n_1, \ldots, n_m)$.

A discussion on probabilistic aspects and cases where the algorithm fails is given in Remark 15.

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 [41, 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.

3.2 The start system

The following construction is from [24, 29] (however, the cost estimates below are new). For any integers i, j, with j in $\{1, \ldots, m\}$, let us define the affine polynomial

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

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

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

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

Lemma 6. *The polynomial $g_{\underline{d},\underline{e}}$ has multi-degree $\underline{d}$.*

Finally, given multi-degrees $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_N)$, with each $\underline{d}_i$ in $\mathbb{N}^m$, we define the system $\mathbf{g} = (g_1, \ldots, g_N)$ by

$$g_i = g_{\underline{d}_i, \underline{d}_1+\cdots+\underline{d}_{i-1}} = \prod_{j=1}^{m} \prod_{k=0}^{d_{i,j}-1} \kappa_{k+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j), \qquad 1 \le i \le N.$$

Lemma 7. *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, $\underline{d}_i$ is different from $(0, \ldots, 0)$. Then the following holds:*

- *for i in $\{1, \ldots, N\}$, g_i has multi-degree $\underline{d}_i$;*
- *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 6. In order to build a straight-line program for the polynomials $\mathbf{g}$, recall that $g_i(\mathbf{X})$ takes the form

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

We actually start by fixing j in $\{1, \ldots, m\}$. For such a fixed j, we have to evaluate all linear forms $\kappa_{k+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j)$, for $i = 1, \ldots, N$ and $k = 0, \ldots, d_{i,j} - 1$. 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 $k + d_{1,j} + \cdots + d_{i-1,j}$. 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 [16, 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 $O^{\sim}(N + \sum_{i,j} d_{i,j})$ 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 $\underline{d}_i = (0, \ldots, 0)$), this is $O^{\sim}(\sum_{1\le i\le N, 1\le j\le m} d_{i,j})$. 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 $\kappa_{k+d_{1,j}+\cdots+d_{i-1,j}}(\mathbf{X}_j)$ 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 $\mathbf{X}_1$, ..., 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 $O^{\sim}(N)$ [16, 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). □

3.3 The homotopy curve $\mathscr{Z}$

We now construct the homotopy itself. Given polynomials $\boldsymbol{f} = (f_1, \ldots, f_N)$ with multi-degrees $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_N)$, with all $\underline{d}_i$ in $\mathbb{N}^m$, we define the system $\mathbf{g}$ as above, together with the equations

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

for a new variable t. We make the same assumption on the characteristics of the base field as in the Lemma 7 (the assumptions on the d_i's is satisfied, since we assume that none of the f_i's is constant).

Remark that $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, 0) = \mathbf{g}$ and $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, 1) = \boldsymbol{f}$. Adding a new "block" of variables consisting only of t, the system $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)$ is seen to have multi-degree at most $\boldsymbol{d}' = (d'_1, \ldots, d'_N)$, 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 $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)$ 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 $V(\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)) - V(D)$, where D is the determinant of the Jacobian matrix $\mathbf{J}(\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t))$ of $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)$ 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 8. *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 [37, Proposition 3.4] implies the dimension claims; as a result, we can apply Proposition 3 to obtain the degree bound. □

Let $\mathscr{I} \subset \mathbb{K}[t, \mathbf{X}]$ be the ideal $\langle \mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t) \rangle : D^{\infty}$, so that $\mathscr{Z}$ is the zero-set of $\mathscr{I}$. Let us further denote by $\mathfrak{I}$ 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 $\mathfrak{I}$ 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 [44] imply the following bound.

Lemma 9. *The numerator and denominator of all coefficients of all polynomials $q, v_1, \ldots, v_N$ have degree at most $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$.*

3.4 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 10. *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 $\mathbb{K}[[t]]$ obtained by lifting the points of $Z(\mathbf{g})$ to solutions of $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)$ using Newton iteration; call them $\Gamma_1, \ldots, \Gamma_c$, with all Γ_i in $\mathbb{K}[[t]]^N \subset \overline{\mathbb{K}}[[t]]^N$ and $c = \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$. In the sequel, $\mathbb{K}((t))$ denotes the field of fractions of $\mathbb{K}((t))$.

Because there are $c = \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ such solutions, and $\mathfrak{I}$ can have at most c solutions (Proposition 3), 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

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

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. □

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 $\mathbf{homot}(\boldsymbol{f},\mathbf{g},t)$ written in terms of τ becomes $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)$). 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 $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)$.

We will in fact need to describe all solutions of $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)$; for this, we use a slight generalization of the presentation in [41]. 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 $\overline{\mathbb{K}}((\tau))$ [39].

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 $\nu(F)\ge 0$, 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 apply Lemma 10; as a consequence, $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)$ 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.

Lemma 11. *Let c' in $\{s,\ldots,c\}$ be such that $\Phi_1,\ldots,\Phi_{c'}$ have all their coordinates with non-negative valuations. 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. Then, 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 $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)$ 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 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 $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)(\Phi_{i'})=0$, Taylor expansion shows that $\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)(\Phi_{i',0})+\mathbf{J}(\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau))(\Phi_{i',0})\Phi_{i',1}=O(\tau^{2e})$, where the right-hand side consists of terms with valuation at least $2e$. The invertibility of $\mathbf{J}(\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau))(\varphi_i)$ implies that the matrix $\mathbf{J}(\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau))(\Phi_{i',0})$ is invertible too, so that

$$\mathbf{J}(\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau))(\Phi_{i',0})^{-1}\mathbf{homot}(\boldsymbol{f},\mathbf{g},\tau)(\Phi_{i',0})+\Phi_{i',1}=O(\tau^{2e}).$$

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. □

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 $\mu_i=\min_{1\le j\le N}\mu_{i,j}$. In particular, $\mu_i\ge 0$ if and only if $i\le c'$. Still inspired by [41], 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 10, the first condition implies that λ is separating for $\mathfrak{Z}$.

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 [41], in our slightly different setting.

Lemma 12. *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

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

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

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

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. ∎

3.5 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 11), $\lambda(\varphi_i)$ 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

$$y_i = \frac{w_i}{r_{\ge 2}} \bmod r_1, \quad 1 \le i \le N;$$

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 [21], 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.

3.6 The algorithm and proof of Proposition 5

We can finally summarize the whole process in Algorithm 1 below. For the moment, we assume that a well-separating element λ is part of the input.

Lemma 13. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ has multi-degree at most $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_N)$, with all $\underline{d}_i$ 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*

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

operations in $\mathbb{K}$.

Proof. The cost of Step 1 in NonsingularSolutions_aux follows from Lemma 7. Step 2 can be done in quasi-linear time $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$ using the algorithms of [16, Chapter 10].

For the main step, computing the parametrization $\mathscr{Q}$ with coefficients in $\mathbb{K}(t)$, we use the lifting algorithm in [44]. 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 8 shows that it is at most $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$. The other important quantity is the size of the straight-line program that evaluates $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)$: using Lemma 7, we see that it is $O(L + \sum_{i,j} d_{i,j})$. We deduce that this step has cost $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')(L + \sum_{i,j} d_{i,j} + N^2)N)$.

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

Finally, Step 6 takes $O(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})(L+N^2)N)$ 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 $O(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$. □

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 7
   Cost: $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$
2: Compute a zero-dimensional parametrization $\mathscr{Q}_{\mathbf{g}}$ for $Z(\mathbf{g})$ using interpolation formulas (1)
   Cost: $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$
3: Apply the lifting algorithm of [44] to $\mathscr{Q}_{\mathbf{g}}$ and $\mathbf{homot}(\boldsymbol{f}, \mathbf{g}, t)$, to recover a zero-dimensional parametrization $\mathscr{Q}$ for $\mathfrak{Z}$ with coefficients in $\mathbb{K}(t)$
   Cost: $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')(L + \sum_{i,j} d_{i,j} + N^2)N)$
4: Compute r and $w_1, \ldots, w_N$ as in Lemma 12
   Cost: $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$
5: Compute r_1 and $y_1, \ldots, y_N$ as in Subsection 3.5
   Cost: $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})N)$
6: Compute and return $\mathsf{Clean}(r_1, y_1, \ldots, y_N, D)$
   Cost: $O^{\sim}(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})(L + N^2)N)$

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 [41, Lemma 4.2]: for a linear form λ to be well-separating, λ must assume non-zero values on at most c^2 non-zero vectors in $\overline{\mathbb{K}}^N$ (with $c = \mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$), 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 $(\mathrm{coeff}(\Phi_{i,j}, \tau^{\mu_i}))_{1 \leq j \leq N}$, 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 14. *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. □

We can then state the main algorithm of this section, together with its probablity analysis (obviously, the cost is the same as that of NonsingularSolutions_aux), which will finish the proof of Proposition 5.

Remark 15. *We do not know how to verify the output of our algorithm with an admissible cost (that is, similar to the cost of running the algorithm itself). 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. *However, we may miss some solutions.*

More precisely, 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 12 are not satisfied (this analysis establishes Proposition 5).*

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

Input: Γ, $\boldsymbol{d}$

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$(\Gamma, \boldsymbol{d}, \lambda)$

Running the algorithm k times, we obtain k outputs, and a zero-dimensional parametrization of $Z(\boldsymbol{f})$ lies among these k outputs with probability at least $1 - 1/8^k$. If it is the case, since all other outputs have degree less than that of $Z(\boldsymbol{f})$, the correct outputs are the ones with highest degree.

3.7 Example

To illustrate the algorithm, let us consider a simple example. In this example, we work over $\mathbb{Q}$ (later on, the algorithm of this section will be applied over a prime field, but it is of course valid over $\mathbb{Q}$ as well). We take $m = 2$ and $\boldsymbol{n} = (1, 2)$, so that $N = 3$, and that our variables are $\mathbf{X}_1 = (X_{1,1})$ and $\mathbf{X}_2 = (X_{2,1}, X_{2,2})$. We take polynomials $\boldsymbol{f} = (f_1, f_2, f_3)$ having respective multi-degrees $\boldsymbol{d} = (\underline{d}_1, \underline{d}_2, \underline{d}_3)$, with $\underline{d}_1 = \underline{d}_2 = \underline{d}_3 = (1, 1)$ (that is, they are bilinear). Explicitly,

$$\begin{aligned} f_1 &= -16X_{1,1}X_{2,1} + 8X_{1,1}, \\ f_2 &= -8X_{1,1}X_{2,1} - 16X_{1,1}X_{2,2} - 4X_{1,1}, \\ f_3 &= 3X_{1,1}X_{2,1} + 4X_{1,1}X_{2,2} + X_{1,1} + 2X_{2,1} + 4. \end{aligned}$$

The quantity $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ is the coefficient of $\vartheta_1\vartheta_2^2$ in $(\vartheta_1 + \vartheta_2)^3 \bmod \langle \vartheta_1^2, \vartheta_2^3 \rangle$, that is, 3; similarly, with $\boldsymbol{d}' = (\underline{d}'_1, \underline{d}'_2, \underline{d}'_3)$, all $\underline{d}'_i$ being equal to $(1, 1, 1)$, and $\boldsymbol{n}' = (1, 1, 1)$, we see that $\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')$ is the sum of the coefficients of $(\vartheta_0 + \vartheta_1 + \vartheta_3)^3 \bmod \langle \vartheta_0^2, \vartheta_1^2, \vartheta_2^3 \rangle$, that is, 12.

The system $\mathbf{g}$ is given by

$$\begin{aligned} g_1 &= X_{1,1}X_{2,1} \\ g_2 &= (X_{1,1} + 1)(X_{2,1} + X_{2,2} + 1) \\ g_3 &= (X_{1,1} + 2)(X_{2,1} + 2X_{2,2} + 4), \end{aligned}$$

its solutions being $(-2, 0, -1), (-1, 0, -2), (0, 2, -3)$ (so it has $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = 3$ solutions, as claimed). Using $\lambda = X_{1,1} + 2X_{2,1} + 4X_{2,2}$, the corresponding zero-dimensional parametrization is

$$\mathscr{Q}_{\mathbf{g}} = ((T^3 + 23T^2 + 174T + 432,\ -3T^2 - 48T - 192,\ 2T^2 + 30T + 108,\ -6T^2 - 90T - 330), \lambda).$$

Applying Newton iteration, we deduce a zero-dimensional parametrization with coefficients in $\mathbb{Q}(t)$ of the form $\mathscr{Q} = ((q, v_1, v_2, v_3), \lambda)$ that describes the solutions of $t\boldsymbol{f} + (1-t)\mathbf{g}$; the coefficients that appear have numerators and denominators of degree at most $8 \leq \mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}') = 12$. For instance, the first two terms of q are

$$T^3 + \frac{9561314t^7 - 35955867t^6 + 43077203t^5 - 18750948t^4 + 2544440t^3 - 152707t^2 + 4291t - 46}{1081710t^7 - 3054661t^6 + 2913623t^5 - 1066868t^4 + 133524t^3 - 7525t^2 + 199t - 2}T^2 + \cdots,$$

where as a sanity check, we can verify that letting $t = 0$ gives back the polynomial $T^3 + 23T^2 + \cdots$ that we started from.

The $(t-1)$-adic valuation of q is -1, which means that the integer e of Lemma 12 is 1. Hence, we multiply q and v_1, v_2, v_3 by $(t-1)$, to obtain polynomials $q^\star, v_1^\star, v_2^\star, v_3^\star$, in which we can evaluate t at 1. In particular, we obtain $q^\star(1, T) = -80/17T^2 - 880/17T$, whose leading coefficient is $r_0 = -80/17$ (remark that Lemma 12 uses evaluation at 0, since we work in variable $\tau = t - 1$ in that paragraph). Still following Lemma 12, we can then define $r = 1/r_0\, q^\star(1, T)$ and $w_j = 1/r_0\, v_j^\star(1, T) \bmod r$, for $j = 1, 2, 3$; explicitly, they are given by

$$r = T^2 + 11T,\ w_1 = -10T,\ w_2 = -\frac{3}{2}T - 22,\ w_3 = \frac{1}{2}T + 11.$$

The roots of r are $T = 0$ and $T = -11$ (both with multiplicity 1, so we do not need to clean multiple roots); evaluating $(w_1/r', w_2/r', w_3/r')$ at $T = 0$ and $T = -11$, we find the points $\boldsymbol{x} = (-10, 1/2, -1/2)$ and $\boldsymbol{x}' = (0, -2, 1)$.

Both cancel $\boldsymbol{f} = (f_1, f_2, f_3)$; on the other hand, the Jacobian determinant of $\boldsymbol{f}$ vanishes at $\boldsymbol{x}'$, but not at $\boldsymbol{x}$. We can then conclude that $Z(\boldsymbol{f}) = \{\boldsymbol{x}\}$.

4 The main algorithm: proof of Theorem 1

In this section, we work over $\mathbb{K} = \mathbb{Q}$ and we use the bounds on the height of polynomials appearing in a zero-dimensional parametrization of a set $Z(\boldsymbol{f})$ given before in the context of a lifting algorithm following that of [21].

4.1 The lifting algorithm

Our goal is now to give boolean complexity statements for the computation of a zero-dimensional representation of $Z(\boldsymbol{f})$. Given a well-chosen prime p, we start by computing a zero-dimensional parametrization of $Z(\boldsymbol{f} \bmod p)$, which is then lifted to a zero-dimensional parametrization of $Z(\boldsymbol{f})$.

Recall that we 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 [16, Section 18.4]. Recall as well the statement of Theorem 1.

Suppose that $\boldsymbol{f} = (f_1, \ldots, f_N)$ *satisfies* $\mathrm{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_m)$ *and* $\mathrm{ht}(\boldsymbol{f}) \leq \boldsymbol{s} = (s_1, \ldots, s_N)$, *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, $\boldsymbol{d}$ *and* $\boldsymbol{s}$ *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*

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

boolean operations, with

$$\mathfrak{d} = \max_{1 \leq i \leq N} d_{i,1} + \cdots + d_{i,m}, \quad s = \max_{1 \leq i \leq N}(s_i) \quad \text{and} \quad \boldsymbol{\eta} = \left(s_i + \sum_{j=1}^{m} \log(n_j + 1) d_{i,j}\right)_{1 \leq i \leq N}.$$

The algorithm calls the oracle $\mathscr{O}$ *with an input parameter* $B = s\mathfrak{d}^{O(N)}$ *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 5, 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 $1 - (11/32)^k$; observe also that all incorrect answers have degree less than that of $Z(\boldsymbol{f})$.

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 $N, d, \log(s), L$, 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.

In order to quantify primes of "bad reduction", we need to introduce several quantities related to $Z(\boldsymbol{f})$. In addition to $\boldsymbol{d}$, $\boldsymbol{\eta}$ and s as given above, we define

- $\mu_1 = N \log(8N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2)$,
- $\mu_2 = \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + 2\log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$,
- $\mu_3 = \mu_2 + \mu_1\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) + \log(N+2)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) + (N+1)\log(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$,
- $H = 6N(\mathfrak{d}+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\,(\mu_3 + s + \log(N+1)\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$,
- $H' = \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + (\mu_1 + 4\log(N+2))\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$,
- $e = \max_{1\le j\le m} d_{1,j} + \cdots + d_{N,j}$,
- $B = \max\,(8\lceil H\rceil, e)$.

Here is how these quantities come into play. 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 it has height at most μ_1.

Next, using Lemmas 8 and 9 in [10], we deduce that there is a positive integer A such that we have

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

Now, remark the following:

- there are at least $B/2\log(B)$ primes in $\{B+1, \ldots, 2B\}$, by [16, Theorem 18.8];
- there are at most $\log(A)/\log(B) \le H/\log(B)$ primes in $\{B+1, \ldots, 2B\}$ that divide A.

Let p be a prime in $\{B+1, \ldots, 2B\}$, which we obtain by calling the oracle $\mathscr{O}$ with input parameter B. By the discussion above, the probability that p 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 $s\mathfrak{d}^{O(N)}$, so that $\log(B)$ is $O(\log(s) + N\log(\mathfrak{d}))$.

As in the algorithm in [21], we start by solving the system modulo p, then lift this solution to a zero-dimensional parametrization of $Z(\boldsymbol{f})$. By definition of B, the field $\mathbb{F}_p$ satisfies the assumptions of Proposition 5, 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 $O^{\sim}(L(\log(B)+b)) = O^{\sim}(L(\log(s) + N\log(\mathfrak{d}) + b))$). Recall that we obtain

- either a zero-dimensional parametrization of $Z(\boldsymbol{f} \bmod p)$,
- or a zero-dimensional parametrization of degree less than that 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 $O^{\sim}(\log(s) + N\log(\mathfrak{d}))$ bit operations, the running time is

$$O^{\sim}\left(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{C}_{\boldsymbol{n}'}(\boldsymbol{d}')\left(L + \sum_{1\le i\le N, 1\le j\le m} d_{i,j} + N^2\right) N(\log(s) + N\log(\mathfrak{d}))\right) \tag{3}$$

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 coefficients; as said previously, the way λ_0 is chosen implies that λ has height at most $\mu_1 = N \log(8N\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})^2)$. Using Newton iteration [21, 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 [21, Section 4.3] up to a precision at least equal to $2H'$, 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 μ_1, Proposition 4 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 $\mathscr{Q}_0$ describes a proper subset of $Z(\boldsymbol{f} \bmod p)$. 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 [16, Chapter 11]. Using the cost analysis from [21], we deduce that the cost is

$$O^{\tilde{}}\left(\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) H' \left(L + N^2\right) N\right) \tag{4}$$

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 (3) and (4) the following upper bound on the total boolean cost of our algorithm:

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

5 Application to polynomial minimization

We finally turn to the last question mentioned in the introduction: given polynomials $\mathbf{h} = (h_1, \ldots, h_p) \subset \mathbb{Z}[X_1, \ldots, X_n]$, that define an algebraic set $V = V(\mathbf{h}) \subset \mathbb{C}^n$, 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 $\mathbf{h}$. The assumptions on $\mathbf{h}$ are discussed in the first subsection, which also contains the statement of the main result of this section (Theorem 16). Next, we discuss the Lagrangian reformulation of our minimization problem; this allows us prove Theorem 16 in the last subsection.

5.1 Genericity assumptions

Let $\mathbf{h} = (h_1, \ldots, h_p)$ 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 [3, 4], we denote this set by $W(\pi_1, V)$.

Let $\mathrm{jac}(\mathbf{h})$ be the Jacobian matrix of $\mathbf{h}$ and let $\mathrm{jac}(\mathbf{h}, 1)$ denote the truncated jacobian matrix (which in general is rectangular)

$$\begin{bmatrix} \frac{\partial h_1}{\partial X_2} & \cdots\cdots & \frac{\partial h_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial h_p}{\partial X_2} & \cdots\cdots & \frac{\partial h_p}{\partial X_n} \end{bmatrix}.$$

Following again the construction of [4], if m is a $(p-1)$-minor of $\mathrm{jac}(\mathbf{h}, 1)$, $\mathsf{Minors}(\mathbf{h}, m)$ denotes the vector of p-minors of $\mathrm{jac}(\mathbf{h}, 1)$ obtained by adding the missing row and the missing column to m; there are $n - p$ such minors. Then, we say that $(h_1, \ldots, h_p)$ satisfies assumption G if the following conditions hold:

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

This implies that if not empty, V is smooth and $(n-p)$-equidimensional and $\mathbf{h}$ 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

$$h_1(\boldsymbol{x}) = \cdots = h_p(\boldsymbol{x}) = 0, \qquad \mathrm{rank}(\mathrm{jac}_{\boldsymbol{x}}(\mathbf{h}, 1)) \leq p - 1,$$

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 $\mathrm{jac}(\mathbf{h}, 1)$ 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 $\mathrm{jac}(\mathbf{h}, 1)$, the polynomials $\mathbf{h}, \mathsf{Minors}(\mathbf{h}, m)$ 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 $W(\pi_1, V) \cap \mathcal{O}(m)$.

We can now state the main result of this section.

Theorem 16. *Let $\mathbf{h} = (h_1, \ldots, h_p) \subset \mathbb{Z}[X_1, \ldots, X_n]$, and assume that all h_i's have degree at most d and height at most s. Assume further that $\mathbf{h}$ satisfies G and is given by a straight-line program Γ of length E, that uses integers of height at most s'.*

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

$$O^{\sim}\left(p(E+n)s' + n^3\binom{n-1}{p-1}\binom{n}{p}(s+d)d^{2p}(d-1)^{2(n-p)}(pE + nd + n^2)\right).$$

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

We now prove that assumption G is generic. The proof of this proposition occupies the rest of this subsection. In what follows, we 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 $\binom{n+d}{n}$.

Proposition 17. *Let d be a positive integer. There exists a nonempty Zariski open set $\mathscr{O} \subset \mathbb{C}[X_1, \ldots, X_n]_d^p$ such that any $\mathbf{h} \in \mathscr{O}$ satisfies G.*

Let $\mathcal{N} = \binom{n+d}{n}$ be the number of monomials of degree at most d in $\mathbb{C}[X_1, \ldots, X_n]$ and denote these monomials by $1 = \mathfrak{m}_1, \ldots, \mathfrak{m}_{\mathcal{N}}$; 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 $\mathfrak{h}_i$ the polynomial $\sum_{j=1}^{\mathcal{N}} \gamma_{i,j}\mathfrak{m}_j$, where the $\gamma_{i,j}$'s are new indeterminates, and by $\mathbb{K}$ the field of rational fractions $\mathbb{C}(\gamma_{1,1}, \ldots, \gamma_{p,\mathcal{N}})$. We consider the sequence $\mathfrak{H} = (\mathfrak{h}_1, \ldots, \mathfrak{h}_p)$; it is seen as a sequence of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$.

Polynomials in $\mathbb{C}[X_1,\dots,X_n]_d$ are obtained by instantiating the indeterminates $\gamma_{i,j}$ to elements of $\mathbb{C}$, so we can we identify a polynomial f with the sequence of coefficients of $\mathfrak{m}_1,\dots,\mathfrak{m}_{\mathcal{N}}$ in it. In a similar way, a sequence of polynomials in $\mathbb{C}[X_1,\dots,X_n]_d^p$ is identified with elements of $\mathbb{C}^{\mathcal{N}p}$ and, by abuse of notation, given a subset $A \subset \mathbb{C}^{\mathcal{N}p}$ we may use the notation "$\mathbf{h} = (h_1,\dots,h_p) \in A$" to denote a family of polynomials in $\mathbb{C}[X_1,\dots,X_n]_d^p$ whose sequence of coefficients belongs to A.

Genericity of $\mathsf{G}(1)$. We first prove that for a generic choice of $\mathbf{h}$, at any point of $V(\mathbf{h})$, the jacobian matrix $\mathrm{jac}(\mathbf{h})$ of $\mathbf{h}$ has full rank p. In this paragraph, we consider the polynomials $\mathfrak{l}_i = \mathfrak{h}_i - \gamma_{i,1}$ for $1 \le i \le p$; hence $\mathfrak{l}_i$ has no constant term, and belongs to $\mathbb{K}'[X_1,\dots,X_n]$, where $\mathbb{K}' \subset \mathbb{K}$ is the field of rational fractions $\mathbb{C}((\gamma_{i,j})_{1\le i\le p, 2\le j\le \mathcal{N}})$. Let ψ denote the mapping

$$\begin{array}{rccc} \psi : & \overline{\mathbb{K}'}^n & \longrightarrow & \overline{\mathbb{K}'}^p \\ & \mathbf{c} & \longmapsto & (\mathfrak{l}_1(\mathbf{c}),\dots,\mathfrak{l}_p(\mathbf{c})). \end{array}$$

Let $K_0 \subset \overline{\mathbb{K}'}^p$ be the set of critical values of ψ. By Sard's Theorem [45, 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 $\gamma_{1,1},\dots,\gamma_{p,1}$ as coordinates in the target space. Then, the ideal of $\mathbb{K}'[\mathbf{X},\gamma_{1,1},\dots,\gamma_{p,1}]$ generated by $\mathfrak{l}_1+\gamma_{1,1},\dots,\mathfrak{l}_p+\gamma_{p,1}$ and the maximal minors of $\mathrm{jac}(\mathfrak{l}_1,\dots,\mathfrak{l}_p)$ contains a non-zero polynomial $P \in \mathbb{K}'[\gamma_{1,1},\dots,\gamma_{p,1}]$. Up to multiplying P by a suitable denominator, we can then assume that P lies in $\mathbb{C}[(\gamma_{i,j})_{1\le i\le p,1\le j\le\mathcal{N}}]$ and belongs to the ideal generated by the above polynomials in $\mathbb{C}[(\gamma_{i,j})_{1\le i\le p,1\le j\le\mathcal{N}},\mathbf{X}]$.

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

Genericity of $\mathsf{G}(2)$. For the remaining genericity properties, we will use the fact that for any system $\mathbf{h}$ 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 $(\alpha_{k,\ell})_{1\le k,\ell\le n}$, 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 $1\le i\le p$, $1\le j\le\mathcal{N}$ and $1\le k,\ell\le n$) with coefficients in $\mathbb{C}$; we will also consider its subfield $\mathbb{F}' = \mathbb{C}(\alpha_{1,1},\dots,\alpha_{n,n})$. For $f \in \mathbb{F}[X_1,\dots,X_n]$, we denote by $f^{\mathfrak{A}}$ the polynomial $f(\mathfrak{A}\mathbf{X})$; for a subset $F \subset \mathbb{F}[X_1,\dots,X_n]$, $F^{\mathfrak{A}}$ 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 $(X_1,\dots,X_n)$.

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

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

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

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

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

Indeed, there exists a non-zero polynomial Λ in $\mathbb{C}[(\gamma_{i,j})_{1\le i\le p,1\le j\le\mathcal{N}},(\alpha_{k,\ell})_{1\le k,\ell\le n}]$ such that for any $\mathbf{h},\mathbf{A}$ that do not cancel Λ, the zero-set of the system $\mathfrak{S}(\mathbf{h},\mathbf{A})$ has dimension r as well. Fix $\mathbf{h}$ such that $\Lambda(\mathbf{h},\mathfrak{A})$ is not zero and such that $\mathbf{h}$ belongs to $\mathscr{O}_1$ (such an $\mathbf{h}$ exists). Since $\mathbf{h}$ then satisfies $\mathsf{G}(1)$, using the third item in [43, Proposition B.1 (elec. appendix)], we deduce that there exists a non-empty Zariski open set $\mathscr{A}_{\mathbf{h}}$ of $\mathbb{C}^{n\times n}$ such that for $\mathbf{A} \in \mathscr{A}_{\mathbf{h}}$, the zero-set of $\mathfrak{S}(\mathbf{h},\mathbf{A})$ has dimension -1. On the other hand, by assumption on $\mathbf{h}$, for a generic $\mathbf{A}$, the value $\Lambda(\mathbf{h},\mathbf{A})$ is not zero; in that case, the zero-set of $\mathfrak{S}(\mathbf{h},\mathbf{A})$ 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 $\Lambda_{\mathbf{A}} = \Lambda((\gamma_{i,j})_{1\le i\le p, 1\le j\le \mathcal{N}}, \mathbf{A})$ is non zero. Letting $\mathscr{O}_{\mathbf{A}} \subset \mathbb{C}^{\mathcal{N}p}$ be the complement of $V(\Lambda_{\mathbf{A}})$, we deduce that for $\mathbf{h} \in \mathscr{O}_{\mathbf{A}}$, the system $\mathfrak{S}(\mathbf{h}, \mathbf{A})$ is inconsistent, which means that the polynomials $\mathbf{h}^{\mathbf{A}}$ satisfy $\mathsf{G}(2)$. The transformation $\varphi : \mathbf{h} \in \mathbb{C}[X_1, \ldots, X_n]_d^p \mapsto \mathbf{h}^{\mathbf{A}} = \mathbf{h}(\mathbf{A}\mathbf{X}) \in \mathbb{C}[X_1, \ldots, X_n]_d^p$ 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 $\mathbf{h}$, the polar variety $W(\pi_1, V(\mathbf{h}))$ is finite. The proof is similar to the one above, with a few modifications. This time, we define $\Delta'(\mathfrak{H}, \mathfrak{A})$ to be the vector of p-minors of $\mathrm{jac}(\mathfrak{H}^{\mathfrak{A}}, 1)$, and let $\mathfrak{S}'(\mathfrak{H}, \mathfrak{A}) \subset \mathbb{F}[X_1, \ldots, X_n]$ be system of the polynomials $(\mathfrak{H}^{\mathfrak{A}}, \Delta'(\mathfrak{H}, \mathfrak{A}))$. The polynomials $\mathfrak{S}'(\mathbf{h}, \mathfrak{A})$ and $\mathfrak{S}'(\mathbf{h}, \mathbf{A})$ are defined as above.

Then, we proceed as before, noticing that there exists a non-zero polynomial Λ' in $\mathbb{C}[(\gamma_{i,j})_{1\le i\le p, 1\le j\le \mathcal{N}}, (\alpha_{k,\ell})_{1\le k,\ell\le n}]$ such that for any $\mathbf{h}, \mathbf{A}$ that do not cancel Λ', the zero-sets of the systems $\mathfrak{S}'(\mathfrak{H}, \mathfrak{A})$ and $\mathfrak{S}'(\mathbf{h}, \mathbf{A})$ have the same dimension r', the former being over an algebraic closure of $\mathbb{F}$. Fix an $\mathbf{h}$ such that $\Lambda'(\mathbf{h}, \mathfrak{A})$ is not zero and that satisfies $\mathsf{G}(1)$. [43, Proposition 3.7] shows that for $\mathbf{A}$ in a suitable Zariski open subset of $\mathbb{C}^{n\times n}$, $W(\pi_1, V(\mathbf{h}^{\mathbf{A}}))$ is finite, or equivalently $\mathfrak{S}'(\mathbf{h}, \mathbf{A})$ 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 $\mathfrak{S}'(\mathfrak{H}, \mathbf{A})$ has dimension r' as well; thus, this $\mathbf{A}$ being fixed, we deduce that there exists an open set $\mathscr{O}'_{\mathbf{A}}$ of $\mathbb{C}^{\mathcal{N}p}$ such that for $\mathbf{h}$ in $\mathscr{O}'_{\mathbf{A}}$, $W(\pi_1, V(\mathbf{h}^{\mathbf{A}}))$ 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 $\mathbf{h} = (h_1, \ldots, h_p) \in \mathscr{O}_1$, the first claim in $\mathsf{G}(4)$ holds. Let m be a $(p-1)$-minor of $\mathrm{jac}(\mathbf{h}, 1)$; without loss of generality, we assume that this minor is the upper left minor.

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

$$h_1(\boldsymbol{x}) = \cdots = h_p(\boldsymbol{x}) = 0, \qquad [\lambda_1, \ldots, \lambda_p] \cdot \mathrm{jac}(\mathbf{h}, 1) = [0, \ldots, 0].$$

We deduce that $\mathrm{jac}(\mathbf{h}, 1)$ 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 $W(\pi_1, V(\mathbf{h}))$. For the reverse inclusion, take now $\boldsymbol{x} \in W(\pi_1, V(\mathbf{h})) \cap \mathcal{O}(m)$. This implies that $\mathrm{jac}(\mathbf{h}, 1)$ is rank deficient at $\boldsymbol{x}$, so that all minors in $\mathsf{Minors}(\mathbf{h}, m)$ vanish at $\boldsymbol{x}$. Hence, we proved that in the open set defined by $m \neq 0$, $W(\pi_1, V(\mathbf{h}))$ is the zero-set of $\mathbf{h}, \mathsf{Minors}(\mathbf{h}, m)$.

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

Consider the polynomials $\mathfrak{S}''(\mathfrak{H}, \mathfrak{A})$, consisting of $\mathfrak{H}^{\mathfrak{A}}, \mathsf{Minors}(\mathfrak{H}^{\mathfrak{A}}, m_{\mathfrak{A}})$, where $m_{\mathfrak{A}}$ denotes the top-left $(p-1)$-minor of $\mathrm{jac}(\mathfrak{H}^{\mathfrak{A}}, 1)$, 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 $\mathbb{C}[(\gamma_{i,j})_{1\le i\le p, 1\le j\le \mathcal{N}}, (\alpha_{k,\ell})_{1\le k,\ell\le n}]$ such that for any $\mathbf{h}, \mathbf{A}$ that do not cancel Λ'', the zero-sets of the systems $\mathfrak{S}''(\mathfrak{H}, \mathfrak{A})$ and $\mathfrak{S}''(\mathbf{h}, \mathbf{A})$ have the same dimension r''. Again, we choose $\mathbf{h}$ in $\mathscr{O}_1$ and such that $\Lambda''(\mathbf{h}, \mathfrak{A})$ is not zero.

For such an $\mathbf{h}$, because $V(\mathbf{h})$ is smooth, the third and fourth item of [43, Proposition B.1] prove that for a generic choice of $\mathbf{A}$, the Jacobian matrix of $\mathbf{h}^{\mathbf{A}}, \mathsf{Minors}(\mathbf{h}^{\mathbf{A}}, m_{\mathbf{A}})$ has full rank n at every point of $W(\pi_1, V(\mathbf{h}^{\mathbf{A}})) \cap \mathcal{O}(m_{\mathbf{A}})$; as a result, for such an $\mathbf{A}$, $\mathfrak{G}''(\mathbf{h}, \mathbf{A})$ defines the empty set. As before, this implies that $\mathfrak{G}''(\mathfrak{H}, \mathfrak{A})$ defines the empty set as well. This in turn implies that for a generic choice of $\mathbf{A}$, the system $\mathfrak{S}''(\mathfrak{H}, \mathbf{A})$ defines the empty set. Fixing such an $\mathbf{A}$, we deduce that for a generic choice of $\mathbf{h}$, $\mathfrak{S}''(\mathbf{h}, \mathbf{A})$ defines the empty set as well; in other words, $\mathbf{h}^{\mathbf{A}}$ satisfies $\mathsf{G}(4)$. Undoing the change of variables as we did before proves the last point in $\mathsf{G}(4)$.

5.2 A Lagrangian reformulation

Suppose in all that follows that $\mathbf{h}$ satisfies G and let $V = V(\mathbf{h})$. 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. Also, by $\mathsf{G}(1)$, V is smooth, $(n-p)$-equidimensional and $\mathbf{h}$ generates its vanishing ideal. As previously noticed, this implies that $W(\pi_1, V)$ is defined by

$$h_1 = \cdots = h_p = 0, \qquad \operatorname{rank}(\operatorname{jac}_{\boldsymbol{x}}(\mathbf{h}, 1)) \leq p - 1.$$

For any $\boldsymbol{x}$ in this set, by $\mathsf{G}(2)$, there exists a non-zero vector $\boldsymbol{\ell}_{\boldsymbol{x}} = [\ell_{\boldsymbol{x},1}, \ldots, \ell_{\boldsymbol{x},p}]$ in the left nullspace of $\operatorname{jac}(\mathbf{h}, 1)$, and this vector is unique up to a multiplicative constant.

Proposition 18. *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 sequence of polynomials in variables $X_1, \ldots, X_n, L_1, \ldots, L_p$*

$$\mathcal{W}_{\boldsymbol{u}} = \big(\mathbf{h}, \quad [L_1 \ \cdots \ L_p] \cdot \operatorname{jac}(\mathbf{h}, 1), \quad u_1L_1 + \cdots + u_pL_p - 1\big)$$

is such that

$$Z(\mathcal{W}_{\boldsymbol{u}}) = \{(\boldsymbol{x}, \boldsymbol{\ell}_{\boldsymbol{x}}) \in \mathbb{C}^{n+p} \mid \boldsymbol{x} \in W(\pi_1, V), (\boldsymbol{x}, \boldsymbol{\ell}_{\boldsymbol{x}}) \in V(\mathcal{W}_{\mathbf{u}})\}.$$

Proof. First, take $(\boldsymbol{x}, \boldsymbol{\ell})$ in $V(\mathcal{W}_{\boldsymbol{u}})$. The fact that $\boldsymbol{x}$ and $\boldsymbol{\ell}$ cancel both $\mathbf{h}$ and $[L_1 \ \cdots \ L_p] \cdot \operatorname{jac}(\mathbf{h}, 1)$ implies that $\boldsymbol{x}$ is in $W(\pi_1, V)$ and that $\boldsymbol{\ell} = \lambda\boldsymbol{\ell}_{\boldsymbol{x}}$ 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 $\boldsymbol{\ell}$ such that $(\boldsymbol{x}, \boldsymbol{\ell})$ is in $\mathcal{W}_{\boldsymbol{u}}$. By $\mathsf{G}(2)$, there exists a $(p-1)$-minor $m_{\boldsymbol{x}}$ of $\operatorname{jac}(\mathbf{h}, 1)$ such that $m_{\boldsymbol{x}}(\boldsymbol{x})$ is non-zero; let ι be the index of the missing row. Using Proposition 5.3 of [43], we deduce the existence of rational functions $(\rho_j)_{j=1,\ldots,p,j\neq\iota}$ in $\mathbb{Q}[\mathbf{X}]$ such that we have equality between ideals

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

in the localization $\mathbb{Q}[\mathbf{X}, \mathbf{L}]_{m_{\boldsymbol{x}}}$. Add the equation $u_1L_1 + \cdots + u_pL_p - 1$ to both sides. On the left, we obtain the equations for $\mathcal{W}_{\boldsymbol{u}}$. On the right, we obtain

$$\langle \mathbf{h}, \quad L_\iota \mathsf{Minors}(\mathbf{h}, m_{\boldsymbol{x}}), \quad (L_j - \rho_j L_\iota)_{j=1,\ldots,p,j\neq\iota}, \quad u_1L_1 + \cdots + u_pL_p - 1\rangle,$$

which is equal to

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

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

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

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

Now, $\mathsf{G}(4)$ states that the Jacobian matrix of $(\mathbf{h}, \mathsf{Minors}(\mathbf{h}, m_{\boldsymbol{x}}))$ 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 $(\boldsymbol{x}, \boldsymbol{\ell})$. The equality between ideals seen above implies that it is also the case for the polynomials defining $\mathcal{W}_{\boldsymbol{u}}$. ∎

The following lemma shows that one can find a suitable $\boldsymbol{u}$ with small bit-size. The proof is a direct application of Lemma 14.

Proposition 19. *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 $\{1, \ldots, 8(p-1)\delta\}$. Then at least $7/8$ of these linear forms satisfy the assumptions of Proposition 18.

5.3 Explicit bound for Lagrange systems: proof of Theorem 16

We continue with the notation introduced at the begining of this section and let s be an upper bound on the height of all h_i, $i = 1, \ldots, p$. Assume that $\mathbf{h}$ satisfies the genericity assumptions G defined previously. As in the previous subsection, let $\mathcal{W}_{\boldsymbol{u}}$ be the system

$$\big(\mathbf{h}, \quad [L_1 \ \cdots \ L_p] \cdot \mathrm{jac}(\mathbf{h}, 1), \quad u_1L_1 + \cdots + u_pL_p - 1\big)$$

with $\mathbf{u}$ chosen as in Proposition 19; we write $\mathbf{g} = (g_1, \ldots, g_{n-1})$ for the polynomials $[L_1 \ \cdots \ L_p] \cdot \mathrm{jac}(\mathbf{h}, 1)$ and $\ell = u_1L_1 + \cdots + u_pL_p - 1$.

The proof of Theorem 16 simply consists in applying Theorem 1 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 in $\mathcal{W}_{\boldsymbol{u}}$ are bounded by the multi-degree vector $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_1, \underline{d}_2, \ldots, \underline{d}_2, \underline{d}_3)$, with $\underline{d}_1 = (d, 0)$ appearing p times, $\underline{d}_2 = (d-1, 1)$ appearing $n-1$ times and $\underline{d}_3 = (0, 1)$ appearing once. Expanding the product

  $$\boldsymbol{\chi}(\boldsymbol{d}) = (d\vartheta_1)^p((d-1)\vartheta_1 + \vartheta_2)^{n-1}\vartheta_2 \bmod \langle \vartheta_1^{n+1}, \vartheta_2^{p+1}\rangle,$$

  we deduce that $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) = \binom{n-1}{p-1}d^p(d-1)^{n-p}$. Proposition 3 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 $\mathbf{h}$, $\mathbf{g}$ and ℓ have heights bounded by respectively s, $s + \log(n) + \log(d)$ and $p\log(8p\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}))$. Using the notation introduced in Section 2.2, we now define

  $$\begin{aligned}
  \eta_1 &= s + d\log(n+1),\\
  \eta_2 &= s + \log(n) + \log(d) + (d-1)\log(n+1) + \log(p+1),\\
  \eta_3 &= p\log(8p\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})) + \log(p+1).
  \end{aligned}$$

  We can then let $\boldsymbol{\eta} = (\mu_1, \ldots, \mu_1, \mu_2, \ldots, \mu_2, \mu_3)$, with μ_1 appearing p times and μ_2 appearing $n-1$ times. The corresponding arithmetic Chow ring is $\mathbb{R}[\xi, \vartheta_1, \vartheta_2]/\langle \xi^2, \vartheta_1^{n+1}, \vartheta_2^{p+1}\rangle$, and we have

  $$\boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d}) = (\mu_1\xi + d\vartheta_1)^p(\mu_2\xi + (d-1)\vartheta_1 + \vartheta_2)^{n-1}(\mu_3\xi + \vartheta_2) \bmod \langle \xi^2, \vartheta_1^{n+1}, \vartheta_2^{p+1}\rangle.$$

  We deduce that

  $$\begin{aligned}
  \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \quad = \quad & \mu_1 d^{p-1}(d-1)^{n-p}\left(\binom{n-1}{p-1} + (d-1)\binom{n-1}{p-2}\right) +\\
  & \mu_2 d^p(d-1)^{n-p-1}\left(\binom{n-2}{p-1} + (d-1)\binom{n-2}{p-2}\right) +\\
  & \mu_3 d^p(d-1)^{n-p-1}\left(\binom{n-1}{p} + (d-1)\binom{n-1}{p-1}\right) +\\
  & d^p(d-1)^{n-p}\binom{n-1}{p-1}.
  \end{aligned}$$

Letting $B_1 = \binom{n-1}{p-1} + \binom{n-1}{p-2} = \binom{n}{p-1}$, $B_2 = \binom{n-2}{p-1} + \binom{n-2}{p-2} = \binom{n-1}{p-1}$ and $B_3 = \binom{n-1}{p} + \binom{n-1}{p-1} = \binom{n}{p}$, we deduce that

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \leq d^p(d-1)^{n-p}\left(\mu_1 B_1 + (\mu_2+1)B_2 + \mu_3 B_3\right).$$

Observing that $B_1 + B_2 + B_3 \leq (n+2)B_3$, we obtain the upper bound

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \leq d^p(d-1)^{n-p}\max(\mu_1, \mu_2+1, \mu_3)(n+2)B_3.$$

This implies that

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

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

$$\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \in O^{\sim}\left(n\binom{n}{p}s2^p\right).$$

- For a general value of d, we will assume that $\mathbf{h}$ is given by a straight-line program of length E with constants of height bounded by s'. Using Baur-Strassen's algorithm [8], one can deduce a straight-line program with constants of bit size in $O(s')$ evaluating $\mathbf{h}$ and $\mathrm{jac}(\mathbf{h})$ in time $O(pE)$. Hence, one can deduce a straight-line program with constants of bit size in $O(s')$ evaluating $\mathbf{h}$ 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 $b = \max(s', p\log(8p\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})))$.

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

Proposition 19 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 $2n$, Theorem 1 shows that on input Γ, $\boldsymbol{d}$ and $\boldsymbol{\eta}$, Algorithm NonSingularSolutionsOverZ runs within

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

boolean operations (the expression given in that proposition also involves a term of the form $\log(\max(\mu_1, \mu_2, \mu_3))$, 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

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

the bound on the running time becomes

$$O^{\sim}\left(p(E+n)s' + n^3\binom{n-1}{p-1}\binom{n}{p}(s+d)d^{2p}(d-1)^{2(n-p)}(pE+nd+n^2)\right).$$

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

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

The height bound on the coefficients in the output follows immediately from Theorem 1 and the bounds on $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$ and $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})$.

6 Proof of Proposition 4

We conclude with the proof of Proposition 4, which reads as follows: *Let* $\boldsymbol{f} = (f_1, \dots, f_N)$ *be polynomials in* $\mathbb{Z}[\mathbf{X}_1, \dots, \mathbf{X}_m]$, *with* $\mathrm{mdeg}(\boldsymbol{f}) \leq \boldsymbol{d} = (\underline{d}_1, \dots, \underline{d}_N)$ *and* $\underline{d}_i = (d_{i,1}, \dots, d_{i,m})$ *for all* i, *and* $\mathrm{ht}(\boldsymbol{f}) \leq \boldsymbol{s} = (s_1, \dots, s_N)$; *let also* 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 of* $Z(\boldsymbol{f})$ *associated to* λ *have height at most* $\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) + (b + 4\log(N+2))\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})$, *with*

$$\boldsymbol{\eta} = \left(s_i + \sum_{j=1}^{m} \log(n_j + 1) d_{i,j} \right)_{1 \leq i \leq N}.$$

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

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

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 $\mathbb{Q}[T_0, \dots, T_N]$. Clearing denominators and removing contents, we see that only two of them are primitive polynomials in $\mathbb{Z}[T_0, \dots, T_N]$ (they differ by a sign): we call them the *primitive* Chow forms of V.

The arithmetic Chow ring. The proof of Proposition 4 will rely on objects introduced by, and results due to, D'Andrea, Krick and Sombra [11]. We give here a quick overview of the main features of their construction.

Introducing new variables $X_{1,0}, \dots, X_{m,0}$ as homogenization variables, we will use $\mathbf{X}' = (\mathbf{X}'_1, \dots, \mathbf{X}'_m)$, with $\mathbf{X}'_j = (X_{j,0}, \dots, X_{j,n_j})$ 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 $\boldsymbol{c} = (c_1, \dots, c_m)$, the degree $\deg_{\boldsymbol{c}}(V)$ is defined as the generic number of intersection points between V and c_1 linear forms in $\mathbf{X}'_1$, …, c_m linear forms in $\mathbf{X}'_m$. The height component $\widehat{h_{\boldsymbol{c}}}(V)$ is harder to define, and we refer to [11] 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 $\boldsymbol{c}$ [11, 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 [11, 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 [11, 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 [11, 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 $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_N)$ and $\mathbf{s} = (s_1, \ldots, s_N)$ be upper bounds on respectively $\mathrm{mdeg}(\boldsymbol{f})$ and $\mathrm{ht}(\boldsymbol{f})$; as in the proposition, we define

$$\boldsymbol{\eta} = (\eta_1, \ldots, \eta_N) = \left(s_i + \sum_{j=1}^{m} \log(n_j + 1) d_{i,j} \right)_{1 \leq i \leq N}.$$

By [11, Proposition 2.51.3], $[\mathbb{P}^{\boldsymbol{n}}]_{\mathbb{Z}} = 1$. Applying A_4 repeatedly, we obtain that

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

By [11, Lemma 2.32], for all i, we have the inequality

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

or equivalently $[f_i]_{\sup} \leq \chi'(\eta_i, \underline{d}_i)$. This implies that

$$[S]_{\mathbb{Z}} \leq \chi'(\eta_1, \underline{d}_1) \cdots \chi'(\eta_N, \underline{d}_N) = \boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d}). \tag{5}$$

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 $D = \det(jac(\boldsymbol{f}))$ 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 (5) that we have

$$[S']_{\mathbb{Z}} \leq \boldsymbol{\chi}'(\boldsymbol{\eta}, \boldsymbol{d}). \tag{6}$$

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 20. *The following equality holds*

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

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

$$C_{Z(\boldsymbol{f}),c} = c \prod_{\boldsymbol{x} \in S'} (T_0 - x_{1,1}T_1 - \cdots - x_{m,n_m-1}T_{N-1} - x_{m,n_m-1}T_N), \tag{7}$$

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 $\mathscr{T} = S' \times \mathbb{P}^N(\overline{\mathbb{Q}})$, which is an algebraic subset of $\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}})$; we use $T_0, \dots, T_N$ as our coordinates in $\mathbb{P}^N(\overline{\mathbb{Q}})$. Next, define $\mathscr{T}'$ as the intersection of $\mathscr{T}$ and $Z(K^h)$, where K is given by

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

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

Lemma 21. *The intersection $\mathscr{T}' = \mathscr{T} \cap V(K^h)$ is proper.*

Proof. Since S' is finite, it is sufficient to consider the case where S' is a single point of the form $(\boldsymbol{x}'_1, \dots, \boldsymbol{x}'_m)$. In that case, the set $\mathscr{T}'$ is isomorphic to the zero-set of the linear form $K^h(\boldsymbol{x}'_1, \dots, \boldsymbol{x}'_m, T_0, \dots, T_N)$ 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. □

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

Lemma 22. *The image of each $\overline{\mathbb{Q}}$-irreducible component of $\mathscr{T}'$ by π is a hypersurface and each squarefree polynomial in $\mathbb{Q}[T_0, \dots, T_N]$ defining $\mathscr{Y}$ 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 $\mathscr{T}'$ are finite unions of sets of the form $(\boldsymbol{x}'_1, \dots, \boldsymbol{x}'_m) \times H$, where, writing $\boldsymbol{x}'_i = (1, x_{i,1}, \dots, x_{i,n_i})$, H is the hyperplane of $\mathbb{P}^N(\overline{\mathbb{Q}})$ defined by

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

The conclusion follows from (7). □

Explicit bounds. We can now give quantitative estimates for the classes of the objects introduced so far. By [11, Proposition 2.66], we have the equality $[\mathscr{T}]_{\mathbb{Z}} = \iota([S']_{\mathbb{Z}})$, where $[\mathscr{T}]_{\mathbb{Z}}$ lies in $A^*(\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}}), \mathbb{Z})$ and ι is the canonical injection

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

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

$$[S']_{\mathbb{Z}} = \sum_{1 \le i \le m} \widehat{h}_i(S')\, \zeta\, \vartheta_1^{n_1} \cdots \vartheta_i^{n_i - 1} \cdots \vartheta_m^{n_m} + \deg(S') \vartheta_1^{n_1} \cdots \vartheta_m^{n_m}. \tag{8}$$

We deduce that $[\mathscr{T}]_{\mathbb{Z}}$ 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 $[K^h]_{\sup} \in A^*(\mathbb{P}^{\boldsymbol{n}} \times \mathbb{P}^N(\overline{\mathbb{Q}}), \mathbb{Z})$ satisfies

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

Hence, because the intersection defining $\mathscr{T}'$ is proper, we deduce from the Bézout inequality A_4 that

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

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

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

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 [11, Proposition 2.64] shows that

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

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

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

Hence, if C is a primitive polynomial in $\mathbb{Z}[T_0,\ldots,T_N]$ defining $\mathscr{Y}$, 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 23. *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 (6) the inequality $[S']_{\mathbb{Z}} \leq \boldsymbol{\chi}(\boldsymbol{\eta},\boldsymbol{d})$, which is to be understood coefficient-wise. Take the sum of coefficients on both sides. From (8), 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 3. □

Conclusion. Finally, we can conclude the proof of Proposition 4. Lemma 23 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 [11, 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 24 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 24. *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 [30]. □

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 equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

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

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

[5] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. *Journal of Complexity*, 30(4):430–443, 2014.

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

[7] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, second edition, 2006. http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted2.pdf.

[8] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22:317–330, 1983.

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

[11] 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.

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

[13] I. Emiris, A. Mantzaflaris, and E. Tsigaridas. On the bit complexity of solving bilinear polynomial systems. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, pages 215–222. ACM, 2016.

[14] I. Z Emiris and A. Mantzaflaris. Multihomogeneous resultant formulae for systems with scaled support. *Journal of Symbolic Computation*, 47(7):820–842, 2012.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] B. Grenet, P. Koiran, and N. Portier. On the complexity of the multivariate resultant. *Journal of Complexity*, 29(2):142–157, 2013.

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

[25] D. Henrion, S. Naldi, and M. Safey El Din. Exact algorithms for linear matrix inequalities. *SIAM Journal on Optimization*, 26(4):2512–2539, 2016.

[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] G. Jeronimo and J. Sabia. Computing multihomogeneous resultants using straight-line programs. *Journal of Symbolic Computation*, 42(12):218 – 235, 2007. Effective Methods in Algebraic Geometry (MEGA 2005).

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

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

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

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

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

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

[36] 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.

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

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

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

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

[41] 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.

[42] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *ISSAC'03*, pages 224–231. ACM, 2003.

[43] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM*, 63(6):48:1–48:37, January 2017.

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

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

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

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

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