ON THE BIT COMPLEXITY OF POLYNOMIAL SYSTEM SOLVING

NARDO GIMÉNEZ[1] AND GUILLERMO MATERA[1,2]

ABSTRACT. We exhibit a probabilistic algorithm which solves a polynomial system over the rationals defined by a reduced regular sequence. Its bit complexity is roughly quadratic in the Bézout number of the system and linear in its bit size. Our algorithm solves the input system modulo a prime number p and applies p–adic lifting. For this purpose, we establish a number of results on the bit length of a "lucky" prime p, namely one for which the reduction of the input system modulo p preserves certain fundamental geometric and algebraic properties of the original system. These results rely on the analysis of Chow forms associated to the set of solutions of the input system and effective arithmetic Nullstellensätze.

1. INTRODUCTION

Solving polynomial systems defined over $\mathbb{Q}$ is a fundamental task of computational algebraic geometry, which has been the subject of intensive work for at least 40 years. Symbolic approaches to this problem include Gröbner basis technology, triangular decomposition, resultants, Macaulay matrices and Kronecker–like algorithms (see, e.g., [35] and [36] for an overview of the existing methods). The corresponding *arithmetic complexity*, namely the number of arithmetic operations in $\mathbb{Q}$, has been analyzed in, e.g., [30], [16], [8], [13], [17], [20], [31] and [9], among others. The complexity paradigm arising from these works is that polynomial systems can be solved with a number of arithmetic operations which is *polynomial* in the Bézout number of the system. This conclusion nearly matches the lower bounds of [5], [15] and [1], under the assumption that the corresponding algorithms are "geometrically robust", namely they are universal and allow the solution of certain "limit" problems.

On the other hand, less work has been done to analyze the *bit complexity* of these algorithms. Concerning Gröbner bases, the work [22] by Hashemi and Lazard shows that zero–dimensional Gröbner bases can be computed essentially in polynomial time in the input size and D^n, where n is the number of unknowns and D is the mean value of the degrees of the defining polynomials. The bit complexity of Kronecker–like algorithms for complete intersections is analyzed in, e.g., [17] and [21], where it is shown that it is polynomial in the input size and certain invariant called the "system degree" (which is upper bounded by the Bézout number of the system). Further, the recent work by

Schost and Safey El Din [39] considers the bit complexity of multi–homogeneous zero–dimensional systems and proves that such systems can solved with quadratic complexity in the multi–homogeneous Bézout number and a corresponding arithmetic analogue of it. Finally, [17] provides a lower bound on the bit size of the output when "standard" representations are used.

This paper is devoted to analyze the bit complexity of a family of Kronecker–like algorithms originally due to [18] and [17]. We shall consider the improved version of this algorithm due to [20] (see also [9]), which we now discuss. Let $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials which form a reduced regular sequence, that is, $F_1, \ldots, F_r$ form a regular sequence and the ideal $(F_1, \ldots, F_s)$ is radical for $1 \le s \le r$. Denote by $\mathcal{V}_s := \mathcal{V}(F_1, \ldots, F_s)$ the affine subvariety of $\mathbb{C}^n$ defined by $F_1, \ldots, F_s$ and by $\delta_s := \deg \mathcal{V}_s$ its degree for $1 \le s \le r$. Let $\mathcal{V} := \mathcal{V}_r$ and $\delta := \max_{1 \le s \le r} \delta_s$. The algorithm outputs a suitable "parametrization" of a "lifting fiber" of $\mathcal{V}$, that is, a (zero–dimensional) fiber defined over $\mathbb{Q}$ of a general linear projection $\pi : \mathcal{V} \to \mathbb{C}^{n-r}$ defined over $\mathbb{Q}$. Such a parametrization is called a "Kronecker representation". Several works show that this constitutes a good representation of $\mathcal{V}$, namely a "solution" of the system $F_1 = 0, \ldots, F_r = 0$, both from the numeric and the symbolic point of view (see, e.g., [24], [41], [31], [4], [44]).

The computation of the Kronecker representation of such a lifting fiber proceeds in r stages. In the sth stage we compute a Kronecker representation of a lifting fiber of $\mathcal{V}_{s+1}$ from one of $\mathcal{V}_s$. Following a suggestion of [20], to keep the bit length of intermediate results under control, these computations are performed modulo a prime number p, followed by a step of p–adic lifting to recover the integers which define the Kronecker representation of $\mathcal{V}$. As a consequence, the determination of a prime number p with "good" modular reduction is crucial to estimate the bit complexity of the procedure.

For our purposes, the modular reduction defined by a prime number p is "good", and the corresponding prime p is called "lucky", if basic geometric and algebraic features of the variety $\mathcal{V}_s$ and its defining ideal $(F_1, \ldots, F_s)$ are preserved under modular reduction for $1 \le s \le r$. Among them, we may mention dimension, degree and generic smoothness. Further, our algorithm also requires that the modular reduction of the lifting fibers under consideration preserves dimension, degree and non–ramification. Partial results in this direction have been obtained in [40] (see also [34]), on modular reduction of smooth fibers of parametric families of zero–dimensional varieties, and [7], on modular reduction of zero–dimensional varieties defined over $\mathbb{Z}$. Unfortunately, these results are not enough for our purposes.

For the analysis of the bit length of lucky primes, we establish conditions on the coefficients of linear forms defining a projection $\pi_s : \mathcal{V}_s \to \mathbb{C}^{n-s}$, and the coordinates of a point $\boldsymbol{p} \in \mathbb{C}^{n-s}$, which imply that π is "general" in the sense above and $\boldsymbol{p}$ defines a lifting fiber for $1 \le s \le r$. As we need to analyze both conditions for projections and fibers defined over $\mathbb{Z}$, and their modular reductions, a natural framework for this analysis is that of an affine variety defined over a infinite perfect field $\mathbb{K}$. Our main result is the following (see Proposition 3.4 and Theorem 4.10).

Theorem 1.1. *Let $V \subset \overline{\mathbb{K}}^n$ be an equidimensional variety defined over $\mathbb{K}$ of dimension $n - s$ and degree δ_s. Let Λ_{ij} $(1 \le i \le n - s + 1, 1 \le j \le n)$ and $Z_1, \ldots, Z_{n-s}$ be indeterminates over $\mathbb{K}[V]$. Denote $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s})$, $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \le i \le n-s+1, 1 \le j \le n}$, $\boldsymbol{\Lambda}^* := (\Lambda_{ij})_{1 \le i \le n-s, 1 \le j \le n}$ and $\boldsymbol{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ for $1 \le i \le n - s + 1$. There exist*

polynomials $A_V \in \mathbb{K}[\boldsymbol{\Lambda}^*]$ and $\rho_V \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ such that $\deg_{\boldsymbol{\Lambda}_i} A_V = \delta_s$ $(1 \leq i \leq n - s)$, $\deg_{\boldsymbol{\Lambda}_i} \rho_V \leq \delta_s(2\delta_s - 1)$ $(1 \leq i \leq n - s + 1)$, $\deg_{\boldsymbol{Z}} \rho_V \leq \delta_s(2\delta_s - 1)$ and the following properties hold: for any $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} \in \mathbb{K}^{n-s}$ with $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, if $(Y_1, \ldots, Y_{n-s+1}) := \boldsymbol{\lambda}\boldsymbol{X}$, then

1. *the mapping $\pi : V \to \mathbb{A}^{n-s}$ defined by $\boldsymbol{Y} := (Y_1, \ldots, Y_{n-s})$ is a finite morphism;*
2. *Y_{n-s+1} induces a primitive element of the ring extension $\mathbb{K}[\boldsymbol{Y}] \hookrightarrow \mathbb{K}[V]$;*
3. *$\operatorname{rank}_{\mathbb{K}[\boldsymbol{Y}]} \mathbb{K}[V] = \delta_s$;*
4. *$\boldsymbol{p}$ is a lifting point of π and Y_{n-s+1} induces a primitive element of $\pi^{-1}(\boldsymbol{p})$.*

Our main technical tool is the analysis of the Chow form of V. A similar analysis is obtained in [4] under stronger assumptions, namely that $\mathbb{K}$ is a finite field $\mathbb{F}_q$ and V is an absolutely–irreducible complete intersection.

Then we compare the conditions underlying Theorem 1.1 for $\mathbb{K} = \mathbb{Q}$ and $\mathbb{K} = \overline{\mathbb{F}}_p$, where $\mathbb{F}_p$ is a given prime field. This yields an integer multiple $\mathfrak{N}$ of all primes p which are not lucky in the sense above. We upper bound the bit length of this integer $\mathfrak{N}$ using estimates for heights of equidimensional varieties of [6], and then obtain a lucky prime p with "low" bit length. The following statement summarizes our results on modular reduction (see Theorems 5.9 and A.13).

Theorem 1.2. *Let $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials of degree at most d with coefficients of bit length at most h. Assume that $F_1, \ldots, F_r$ form a reduced regular sequence and denote $\mathcal{V}_s := V(F_1, \ldots, F_s) \subset \mathbb{C}^n$ and $\delta_s := \deg \mathcal{V}_s$ for $1 \leq s \leq r$. Let $\delta := \max_{1 \leq s \leq r} \delta_s$. Let $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ and $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathbb{Z}^{n-1}$ be randomly chosen elements with entries of bit length $\mathcal{O}(n^2\delta^3)$. Let $(Y_1, \ldots, Y_n) := \boldsymbol{\lambda}\boldsymbol{X}$ and $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ for $1 \leq s \leq r$.*

Let p be a random prime number of bit length $\mathcal{O}^{\sim}\big(\log(nd^r h)\big)$. Denote by $F_{1,p}, \ldots, F_{r,p}$, $Y_{1,p}, \ldots, Y_{n,p}$ and $\boldsymbol{p}_p$ the corresponding reductions modulo p. Then the following conditions are satisfied for $1 \leq s \leq r$ with probability at least $2/3$:

1. *the polynomials $F_{1,p}, \ldots, F_{s,p}$ generate a radical ideal in $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ and define an equidimensional variety $V_{s,p} \subset \overline{\mathbb{F}}_p^n$ of dimension $n - s$ and degree δ_s;*
2. *the mapping $\pi_{s,p} : V_{s,p} \to \overline{\mathbb{F}}_p^{n-s}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism, $\boldsymbol{p}_p^s \in \mathbb{F}_p^{n-s}$ is a lifting point of $\pi_{s,p}$, and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{p}_p^s)$;*
3. *any $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^{s+1})\big)$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{q})$.*

We observe that the analysis of lucky primes becomes much simpler if only conditions (1) and (2) above are required. An analysis along these lines can be deduced from [40] (compare with [34]). Nevertheless, condition (3), which is critical to prove the correctness of our algorithm for solving the system $F_1 = 0, \ldots, F_r = 0$, requires a significant extension of these techniques.

Finally, we combine the algorithm of [4] with p–adic lifting, as in [20], to obtain an algorithm for solving the system $F_1 = 0, \ldots, F_r = 0$ with good bit complexity. We prove the following result (see Theorem 6.8 for a precise statement).

Theorem 1.3. *Let $F_1, \ldots, F_r$ be polynomials of $\mathbb{Z}[X_1, \ldots, X_n]$ as in the statement of Theorem 1.2. There exists a probabilistic algorithm that takes as input an algorithm evaluating $F_1, \ldots, F_r$ with at most L arithmetic operations, and outputs a parametrization of a lifting fiber of $\mathcal{V}(F_1, \ldots, F_r)$ with $\mathcal{O}^{\sim}\big(n^{\mathcal{O}(1)} L\delta(d\delta + d^r h)\big)$ bit operations.*

The paper is organized as follows. In Section 2 we recall the notions and results of algebraic geometry and commutative algebra we shall use, and discuss the representation of multivariate polynomials by straight–line programs and algebraic varieties by Kronecker representations. In Section 3 we recall the notion of Chow form of an equidimensional variety, discuss its basic properties and obtain conditions (1)–(3) of Theorem 1.1. In Section 4 we discuss the notion of lifting point and finish the proof of Theorem 1.1. In Section 5 we prove Theorem 1.2. For sake of readability, all estimates on heights of varieties underlying the proof of this result are postponed to Appendix A. Finally, in Section 6 we describe our algorithm for solving the input system $F_1 = 0, \ldots, F_r = 0$ and analyze its bit complexity, showing thus Theorem 1.3.

2. NOTIONS AND NOTATIONS

We use standard notions and notations of commutative algebra and algebraic geometry as can be found in, e.g., [29], [10], [42].

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ its algebraic closure. Let $\mathbb{K}[X_1, \ldots, X_n]$ denote the ring of n–variate polynomials in indeterminates $X_1, \ldots, X_n$ and coefficients in $\mathbb{K}$. Let $\mathbb{A}^n := \mathbb{A}^n(\overline{\mathbb{K}})$ be the affine n–dimensional space over $\overline{\mathbb{K}}$. A subset of $\mathbb{A}^n$ is called a $\mathbb{K}$–*definable affine subvariety* of $\mathbb{A}^n$ (a $\mathbb{K}$–*variety* for short) if it is the set of common zeros in $\mathbb{A}^n$ of a set of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$. We will use the notations $\mathcal{V}(F_1, \ldots, F_s)$ and $\{F_1 = 0, \ldots, F_s = 0\}$ to denote the $\mathbb{K}$–variety defined by $F_1, \ldots, F_s$. Further, if $\mathcal{I}$ is an ideal of $\mathbb{K}[X_1, \ldots, X_n]$, then $\mathcal{V}(\mathcal{I})$ denotes the $\mathbb{K}$–variety of $\mathbb{A}^n$ defined by the elements of $\mathcal{I}$. On the other hand, we shall denote by $\mathcal{I}(V)$ the vanishing ideal of a $\mathbb{K}$–variety $V \subset \mathbb{A}^n$ in $\mathbb{K}[X_1, \ldots, X_n]$ and by $\mathbb{K}[V]$ its coordinate ring, namely the quotient ring $\mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$.

Let $V \subseteq \mathbb{A}^n$ be a $\mathbb{K}$–variety. We denote by $\dim V$ its dimension with respect to the Zariski topology over $\mathbb{K}$ (which agrees with the Krull dimension of $\mathbb{K}[V]$). More generally, if R is a ring, then $\dim R$ denotes its Krull dimension. Suppose further that V is irreducible with respect to the Zariski topology over $\mathbb{K}$. We define its *degree* as the maximum number of points lying in the intersection of V with an affine linear $\overline{\mathbb{K}}$–variety L of $\mathbb{A}^n$ of codimension $\dim V$ for which $\#(V \cap L) < \infty$. Now, if $V = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_N$ is the decomposition of V into irreducible $\mathbb{K}$–components, we define the degree of V as $\deg V = \sum_{i=1}^{N} \deg \mathcal{C}_i$ (cf. [23]). This definition of degree satisfies the following *Bézout inequality* ([23]; see also [14]): if V and W are $\mathbb{K}$–varieties of $\mathbb{A}^n$, then

$$(2.1) \qquad\qquad\qquad \deg(V \cap W) \le \deg V \deg W.$$

2.1. **Notions and results of commutative algebra.** A proper ideal $\mathcal{I}$ of $\mathbb{K}[X_1, \ldots, X_n]$ is *unmixed* if the codimensions of its associated primes are all equal. A classical result asserts that the *unmixedness theorem* holds for $\mathbb{K}[X_1, \ldots, X_n]$, namely an ideal $\mathcal{I}$ of $\mathbb{K}[X_1, \ldots, X_n]$ of codimension r generated by r elements is unmixed for any $r \ge 0$ (see, e.g., [33, Theorems 17.6 and 17.7]).

Let $\mathcal{I} := (F_1, \ldots, F_r) \subset \mathbb{K}[X_1, \ldots, X_n]$ be an ideal of dimension $n - r$. Then $\mathcal{I}$ is un-mixed and defines an equidimensional $\mathbb{K}$–variety $V \subset \mathbb{A}^n$. Let $Y_1, \ldots, Y_n \in \mathbb{K}[X_1, \ldots, X_n]$ be linearly–independent linear forms such that the mapping $\pi : V \to \mathbb{A}^{n-r}$ defined by $Y_1, \ldots, Y_{n-r}$ is a finite morphism. The change of variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$ is called a *Noether normalization* of V (or $\mathcal{I}$) and we say that the variables $Y_1, \ldots, Y_n$ are in *Noether position* with respect to V (or $\mathcal{I}$), the variables $Y_1, \ldots, Y_{n-r}$ being *free*. Let $R := \mathbb{K}[Y_1, \ldots, Y_{n-r}]$ and let R' denote the field of fractions of R. Denote $B := \mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}$ and let $B' := R' \otimes_{\mathbb{K}} B := R'[Y_{n-r+1}, \ldots, Y_n]/\mathcal{I}^e$, where $\mathcal{I}^e$ is the extension of $\mathcal{I}$ to $R'[Y_{n-r+1}, \ldots, Y_n]$. We consider B as an R–module and B' as an R'–vector space respectively. Since B is a finitely generated, B' is a finite–dimensional R'–vector space, whose dimension we denote by $\dim_{R'} B'$. In particular, for any $F \in \mathbb{K}[X_1, \ldots, X_n]$ we may consider the characteristic polynomial $\chi \in R'[T]$ (respectively the minimal polynomial $\mu \in R'[T]$) of the homothety of multiplication by F in B'. In this situation we have that χ and μ belong to $R[T]$ (see, e.g., [9, Theorem 1.27]). We shall call χ and μ respectively the *characteristic* and the *minimal* polynomials of F modulo $\mathcal{I}$.

Now assume further that $\mathbb{K}$ is an infinite perfect field. Then B is a free R–module of finite rank $\operatorname{rank}_R B$ (see, e.g. [19, Lemma 3.3.1]). Since any basis of B as an R–module induces a basis of B' as an R'–vector space, we have $\operatorname{rank}_R B = \dim_{R'} B'$. In this case, we say that $G \in \mathbb{K}[X_1, \ldots, X_n]$ induces a *primitive element* for $\mathcal{I}$ if the powers of the image g of G in B' generate the R'–vector space B'. We shall also say that G induces a primitive element of the ring extension $R \hookrightarrow B$.

The following criterion for deciding radicality of an ideal, probably well–known, is stated and proved here for lack of a suitable reference.

Lemma 2.1. *Let $\mathbb{K}$ be a perfect field, $\mathcal{I} := (F_1, \ldots, F_s) \subset \mathbb{K}[X_1, \ldots, X_n]$ an ideal of dimension $n - s$, and $\mathcal{J}$ the ideal of $\mathbb{K}[X_1, \ldots, X_n]$ generated by $\mathcal{I}$ and the $(s \times s)$–minors of the Jacobian matrix $(\partial F_i/\partial X_j)_{1 \leq i \leq s, 1 \leq j \leq n}$. Then the following conditions are equivalent:*

- $\mathcal{I}$ *is radical;*
- $\mathcal{J}$ *is not contained in any minimal prime of $\mathcal{I}$.*

Proof. Let $B := \mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}$. By [10, Exercise 11.10], it suffices to show that the second condition is equivalent to the following ones:

(1) the localization of B at each prime of codimension 0 is regular;
(2) all primes associated to zero in B have codimension 0.

To prove this equivalence, we observe that the canonical homomorphism $\mathbb{K}[X_1, \ldots, X_n] \to B$ induces a bijection between the set of primes associated to $\mathcal{I}$ and the set of primes associated to 0 in B. This bijection maps the minimal primes over $\mathcal{I}$ to the minimal primes over 0 in B, which are precisely the primes of codimension 0 in B. Now, since the unmixedness theorem holds in $\mathbb{K}[X_1, \ldots, X_n]$, the ideal $\mathcal{I}$ is unmixed, and thus the set of primes associated to $\mathcal{I}$ coincides with the set of minimal primes over $\mathcal{I}$, which implies that (2) is satisfied. Next, the second condition of the lemma can be rephrased by saying that the image $\overline{\mathcal{J}}$ of $\mathcal{J}$ in B is not contained in any prime of B of codimension 0. By [10, Corollary 16.20], this is equivalent to (1), which finishes the proof. □

2.2. **Kronecker representations.** Let $V \subset \mathbb{A}^n$ be an equidimensional $\mathbb{K}$–variety of dimension $n - s$, and let $\mathcal{I} \subset \mathbb{K}[X_1, \ldots, X_n]$ be its vanishing ideal. For a change of variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$, denote $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$, $B := \mathbb{K}[V]$ and $R' := \mathbb{K}(Y_1, \ldots, Y_{n-s})$. Consider $B' := R'[Y_{n-s+1}, \ldots, Y_n]/\mathcal{I}^e$ as an R'-vector space, where $\mathcal{I}^e$ is the extended ideal $\mathcal{I}R[Y_{n-s+1}, \ldots, Y_n]$, and let $\delta := \dim_{R'} B'$.

Definition 2.2. *A* Kronecker representation *of $\mathcal{I}$ (or V) consists of the following items:*
- *a Noether normalization of $\mathcal{I}$, defined by a linear change of variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$ such that Y_{n-s+1} induces a* primitive element *for $\mathcal{I}$;*
- *the minimal (monic) polynomial $Q \in R[T]$ of Y_{n-s+1} modulo $\mathcal{I}$;*
- *the (unique) polynomials $W_{n-s+2}, \ldots, W_n \in R'[T]$ of degree at most $\delta - 1$ such that the following identity of ideals holds in $R'[Y_{n-s+1}, \ldots, Y_n]$:*

(2.2)
$$\mathcal{I}^e = \big(Q(Y_{n-s+1}), Q'(Y_{n-s+1})Y_{n-s+2} - W_{n-s+2}(Y_{n-s+1}), \ldots, Q'(Y_{n-s+1})Y_n - Q_n(Y_{n-s+1}) \big),$$

where Q' denotes the first derivative of Q with respect to T.

Considering instead polynomials $V_{n-s+2}, \ldots, V_n$ of degree at most $\delta - 1$ such that

$$\mathcal{I}^e = \big(Q(Y_{n-s+1}), Y_{n-s+2} - V_{n-s+2}(Y_{n-s+1}), \ldots, Y_n - V_n(Y_{n-s+1}) \big),$$

we have a univariate representation *of $\mathcal{I}$ (or V).*

If $Q' \neq 0$, identity (2.2) may be interpreted in geometric terms as we now explain. Let $\ell : \mathbb{A}^n \to \mathbb{A}^n$ be the linear mapping defined by $Y_1, \ldots, Y_n$ and $W := \ell(V)$. We interpret $Y_1, \ldots, Y_n$ as new indeterminates and consider the mapping $\Pi : W \to \mathbb{A}^{n-s+1}$ defined by the projection on the first $n - s + 1$ coordinates. Considering Q as an element of $\mathbb{K}[Y_1, \ldots, Y_{n-s+1}]$, it turns out that Π defines a birational isomorphism between W and the hypersurface $\{Q = 0\}$ of $\mathbb{A}^{n-s+1}$, whose inverse is the rational mapping $\Phi : \{Q = 0\} \to W$ defined in the following way:

$$\Phi(\boldsymbol{y}) := \left(\boldsymbol{y}, \frac{W_{n-s+2}(\boldsymbol{y})}{Q'(\boldsymbol{y})}, \ldots, \frac{W_n(\boldsymbol{y})}{Q'(\boldsymbol{y})} \right).$$

2.3. **Model of computation.** Besides the Big–Oh notation $\mathcal{O}$, we also use the standard Soft–Oh notation $\mathcal{O}^\sim$ which does not take into account logarithmic terms. We remark that the cost of certain basic operations (such as addition, multiplication, division, and gcd) with integers of bit length m is in $\mathcal{O}^\sim(m)$. In particular, arithmetic operations in the prime finite field $\mathbb{F}_p$ of p elements can be performed with $\mathcal{O}^\sim(\log p)$ bit operations.

Algorithms in computer algebra usually consider the standard dense (or sparse) representation model, where multivariate polynomials are encoded by means of the vector of all (or of all nonzero) coefficients. However, since a generic n–variate polynomial of degree d has $\binom{n+d}{n} = \mathcal{O}(d^n)$ nonzero coefficients, its dense or sparse representation requires an exponential size in d and n, and their manipulation usually requires an exponential number of arithmetic operations with respect to d and n. To avoid this phenomenon we will use an alternative representation for multivariate polynomials by means of straight–line programs (cf. [3]). A *(division–free) straight–line program β* in $\mathbb{K}[X_1, \ldots, X_n]$ which *represents* or *evaluates* polynomials $F_1, \ldots, F_s \in \mathbb{K}[X_1, \ldots, X_n]$ is a sequence $(Q_1, \ldots, Q_r)$ of elements of $\mathbb{K}[X_1, \ldots, X_n]$ satisfying the following conditions:
- $\{F_1, \ldots, F_s\} \subseteq \{Q_1, \ldots, Q_r\}$;

- there exists a finite subset $\mathcal{T} \subset \mathbb{K}$, called the set of *parameters* of β, such that for every $1 \leq \rho \leq r$, the polynomial Q_ρ either is an element of $\mathcal{T} \cup \{X_1, \ldots, X_n\}$, or there exist $1 \leq \rho_1, \rho_2 < \rho$ such that $Q_\rho = Q_{\rho_1} \circ_\rho Q_{\rho_2}$, where $\circ_\rho$ is one of the arithmetic operations $+, -, \times$.

The *length* of β is defined as the total number of arithmetic operations performed during the evaluation process defined by β.

Our algorithm is probabilistic, of *Monte Carlo* type (see, e.g., [45]). One of the probabilistic aspects is related to random choices of points outside certain Zariski open sets. A basic tool for estimating the corresponding probability of success is the following well–known result (see, e.g., [45, Lemma 6.44]).

Lemma 2.3. *Let R be an integral domain, $U_1, \ldots, U_k$ indeterminates over R, $S \subseteq R$ a finite set with $s := \#S$ elements, and $F \in R[U_1, \ldots, U_k]$ a nonzero polynomial of degree at most d. Then F has at most ds^{k-1} zeros in S^k.*

We shall interpret Lemma 2.3 in terms of probabilities: for an element $\boldsymbol{u}$ chosen uniformly at random in S^k, the probability that $F(\boldsymbol{u}) \neq 0$ is greater than $1 - d/s$.

The second probabilistic aspect concerns the choice of a "lucky" prime number p. In connection with this matter, we have the following result (see, e.g., [45, Section 18.4]).

Lemma 2.4. *Let B, m be positive integers and M a nonzero integer such that $\log |M| \leq \frac{B}{m}$. There is a probabilistic algorithm which, from the integer B and any positive integer k, returns a prime p between $B + 1$ and $2B$ not dividing M. It performs $\mathcal{O}^\sim(k \log^2 B)$ bit operations and returns the right result with probability at least*

$$\left(1 - \frac{\log B}{2^{k-1}}\right)\left(1 - \frac{2}{m}\right).$$

Proof. According to, e.g., [45, Theorem 18.8], there is a probabilistic algorithm which computes a random prime p such that $B < p \leq 2B$ with $\mathcal{O}^\sim(k \log^2 B)$ bit operations and probability of success at least $1 - \log B / 2^{k-1}$. On the other hand, if p is a random prime with $B < p \leq 2B$, then p does not divide M with probability at least $1 - 2/m$. Combining both assertions the lemma follows. $\square$

3. On Noether normalizations

Let $\mathbb{K}$ be a perfect field and $V \subset \mathbb{A}^n$ an equidimensional $\mathbb{K}$–variety of dimension $n - s \geq 0$ and degree δ. In this section we obtain a condition on the coefficients of linear forms $Y_1, \ldots, Y_{n-s+1} \in \mathbb{K}[X_1, \ldots, X_n]$ which implies that $Y_1, \ldots, Y_{n-s}$ define a Noether normalization of V and Y_{n-s+1} is a primitive element of the ring extension $\mathbb{K}[Y_1, \ldots, Y_{n-s}] \hookrightarrow \mathbb{K}[V]$ (Proposition 3.4). As these conditions rely heavily on properties of the Chow form of V, we also recall the notion of Chow form of an equidimensional variety and some of its basic properties.

3.1. **The Chow form of an equidimensional variety.** Let $\boldsymbol{\Lambda}^h := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 0 \leq j \leq n}$ be a matrix of indeterminates over $\mathbb{K}[V]$, let $\boldsymbol{\Lambda}_i^h := (\Lambda_{i0}, \ldots, \Lambda_{in})$ and $\boldsymbol{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ for $1 \leq i \leq n - s + 1$. A Chow form of V is a square–free polynomial F_V of $\mathbb{K}[\boldsymbol{\Lambda}^h]$ such that $F_V(\boldsymbol{\lambda}^h) = 0$ if and only if $\overline{V} \cap \{\lambda_{i0} + \sum_{j=1}^n \lambda_{ij} X_j = 0 \ (1 \leq i \leq n - s + 1)\}$ is nonempty, where $\overline{V} \subset \mathbb{P}^n$ is the projective closure of V with respect to the canonical

inclusion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ (see [25, Chapter X, Section 6]). We observe that F_V is multiho-
mogeneous of degree δ in each group of variables $\mathbf{\Lambda}_i^h$ for $1 \leq i \leq n - s + 1$, and is
uniquely determined up to nonzero multiples in $\mathbb{K}$. Let $\mathbf{\Lambda} := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$ and
let $Z_1, \ldots, Z_{n-s+1}$ be new indeterminates. Let $P_V \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$ be the unique
polynomial such that

$$P_V(\mathbf{\Lambda}, \Lambda_{10}, \ldots, \Lambda_{n-s+1,0}) = F_V(\mathbf{\Lambda}_1^h, \ldots, \mathbf{\Lambda}_{n-s+1}^h).$$

By abuse of language we also call P_V a Chow form of V.

Let $\xi_1, \ldots, \xi_n$ be the coordinate functions of V induced by $X_1, \ldots, X_n$. Set $\boldsymbol{\xi} := (\xi_1, \ldots, \xi_n)$ and let $\mathbf{\Lambda}_i \cdot \boldsymbol{\xi} \in \mathbb{K}[V][\mathbf{\Lambda}]$ be defined by

$$\mathbf{\Lambda}_i \cdot \boldsymbol{\xi} := \sum_{j=1}^n \Lambda_{ij} \xi_j \quad (1 \leq i \leq n - s + 1).$$

A fundamental property of the Chow form is that P_V is uniquely determined, up to
multiplication by nonzero elements of $\mathbb{K}$, by the following two conditions:

- if $\mathbf{\Lambda}\boldsymbol{\xi} := (\mathbf{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \mathbf{\Lambda}_{n-s+1} \cdot \boldsymbol{\xi})$, then the following identity holds in $\mathbb{K}[V][\mathbf{\Lambda}]$:

(3.1) $$P_V(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi}) = 0.$$

  Equivalently, let $\mathbf{\Lambda}_i \cdot \boldsymbol{X} := \sum_{j=1}^n \Lambda_{ij} X_j$ for $1 \leq i \leq n - s + 1$ and $\mathbf{\Lambda}\boldsymbol{X} := (\mathbf{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \mathbf{\Lambda}_{n-s+1} \cdot \boldsymbol{X})$. Then the polynomial $P_V(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{X}) \in \mathbb{K}[\mathbf{\Lambda}, \boldsymbol{X}]$ vanishes
  on the variety $\mathbb{A}^{(n-s+1)n} \times V$.
- If $G \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$ is any polynomial such that $G(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi}) = 0$, then P_V
  divides G in $\mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$.

Furthermore, F_V has the following features (see [25, Chapter X, Sections 7 and 9]):

(1) F_V is homogeneous of degree δ in the $(n - s + 1) \times (n - s + 1)$–minors of $\mathbf{\Lambda}^h$;
(2) $\deg_{(\Lambda_{10}, \ldots, \Lambda_{n-s+1,0})} F_V = \deg_{\Lambda_{n-s+1,0}} F_V = \delta$;
(3) if V is an irreducible $\mathbb{K}$–variety, then F_V is an irreducible polynomial of $\mathbb{K}[\mathbf{\Lambda}^h]$.
    More generally, if $V = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_N$ is the decomposition of V into irreducible
    $\mathbb{K}$–components, and $F_{\mathcal{C}_i}$ is a Chow form of $\mathcal{C}_i$ for $1 \leq i \leq N$, then $\prod_{1 \leq i \leq s} F_{\mathcal{C}_i}$ is
    a Chow form of V.

Remark 3.1. *Let $A_V \in \mathbb{K}[\mathbf{\Lambda}_1^h, \ldots, \mathbf{\Lambda}_{n-s}^h]$ be the (nonzero) polynomial which arises
as the coefficient of the monomial $\Lambda_{n-s+1,0}^\delta$ in F_V, considering F_V as an element of
$\mathbb{K}[\mathbf{\Lambda}][\Lambda_{10}, \ldots, \Lambda_{n-s+1,0}]$. Then (2) implies that A_V is independent of $\Lambda_{10}, \ldots, \Lambda_{n-s\,0}$,
that is, $A_V \in \mathbb{K}[\mathbf{\Lambda}_1, \ldots, \mathbf{\Lambda}_{n-s}]$. In particular, A_V is homogeneous of degree δ in the
$(n - s) \times (n - s)$–minors of the $(n - s) \times n$–matrix $\mathbf{\Lambda}^* = (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$.*

Let $\rho_V \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}]$ be the discriminant of P_V with respect to Z_{n-s+1}, namely

$$\rho_V := \mathrm{Res}_{Z_{n-s+1}} \left(P_V, \frac{\partial P_V}{\partial Z_{n-s+1}} \right).$$

Lemma 3.2. *ρ_V and $\partial P_V / \partial Z_{n-s+1}$ are both nonzero.*

Proof. We have that $A := \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]/(P_V)$ is a reduced $\mathbb{K}$–algebra. Since $\mathbb{K}$
is perfect, by [32, Corollary, page 194] it follows that A is a separable $\mathbb{K}$–algebra. Let $\mathbb{K}'$
denote the algebraic closure of $\mathbb{K}(\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s})$. By [32, 27.G], we deduce that the

$\mathbb{K}'$–algebra $A \otimes_{\mathbb{K}} \mathbb{K}' = \mathbb{K}'[Z_{n-s+1}]/(P_V)$ is reduced. Since $\mathbb{K}'$ is a perfect field, this implies that $\partial P_V / \partial Z_{n-s+1} \neq 0$. Now, by (2) and (3) above, each irreducible factor of P_V is a Chow form of an irreducible component $\mathcal{C}_i$ of V, of positive degree $\deg \mathcal{C}_i$ in Z_{n-s+1}. Then the previous argument shows that the partial derivative with respect to Z_{n-s+1} of each irreducible factor of P_V does not vanish, which in turn implies that P_V and $\partial P_V / \partial Z_{n-s+1}$ are relatively prime polynomials of $\mathbb{K}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$. Since $\mathbb{K}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ is a factorial ring, this implies that the resultant ρ_V of these polynomials does not vanish. $\square$

Further, ρ_V satisfies the following degree estimates:

$$\deg_{(Z_1, \ldots, Z_{n-s})} \rho_V \leq (2\delta - 1)\delta, \quad \deg_{\boldsymbol{\Lambda}_i} \rho_V \leq (2\delta - 1)\delta \quad (1 \leq i \leq n - s + 1).$$

In particular, for its total degree we have $\deg \rho_V \leq (n - s + 2)(2\delta^2 - \delta)$.

Let $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s+1})$. Further, for any $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n} \in \mathbb{A}^{(n-s+1)n}$, we write $\boldsymbol{\lambda}_i := (\lambda_{i1}, \ldots, \lambda_{in})$ and $\boldsymbol{\lambda}_i \cdot \boldsymbol{\xi} := \sum_{j=1}^{n} \lambda_{ij} \xi_j$ for $1 \leq i \leq n - s + 1$. We consider $\mathbb{K}[V][\boldsymbol{\Lambda}]$ as a $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–algebra through the ring homomorphism $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[V][\boldsymbol{\Lambda}]$ which maps any $F \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ to $F(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})$. In these terms, we have the following result.

Lemma 3.3. $\partial P_V / \partial Z_{n-s+1}$ is not a zero divisor of the $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–algebra $\mathbb{K}[V][\boldsymbol{\Lambda}]$.

Proof. Let $G \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{X}]$ be any polynomial such that

$$(3.2) \qquad \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) \cdot G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$$

in $\mathbb{K}[V][\boldsymbol{\Lambda}]$. We have $\rho_V \in (P_V, \partial P_V / \partial Z_{n-s+1}) \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Since $P_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) = 0$, we deduce that $\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi})$ is a multiple of $\partial P_V / \partial Z_{n-s+1}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})$ in the ring $\mathbb{K}[V][\boldsymbol{\Lambda}]$. Combining this with (3.2), we deduce that

$$\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) \cdot G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$$

in $\mathbb{K}[V][\boldsymbol{\Lambda}]$. Suppose that there exists an irreducible $\mathbb{K}$–component $\mathcal{C}$ of V such that $G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) \neq 0$ in $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. Then

$$\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) \cdot G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$$

in $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. Since $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$ is an integral domain, we conclude that $\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) = 0$ in $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. This implies that

$$(3.3) \qquad \rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) = 0$$

in $\overline{\mathbb{K}}[\mathcal{C}][\boldsymbol{\Lambda}]$, where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$. On the other hand, by Lemma 3.2 the polynomial ρ_V is nonzero. Then, for a generic choice of $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$, the ring extension $\overline{\mathbb{K}}[\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}] \hookrightarrow \overline{\mathbb{K}}[V]$ is integral and $\rho_V(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s})$ is a nonzero polynomial in $\overline{\mathbb{K}}[Z_1, \ldots, Z_{n-s}]$. By (3.3) we deduce that $\rho_V(\boldsymbol{\lambda}, \boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}) = 0$ in $\overline{\mathbb{K}}[\mathcal{C}]$, which shows that $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ are algebraically dependent over $\overline{\mathbb{K}}$. Since $\overline{\mathbb{K}}[\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}] \hookrightarrow \overline{\mathbb{K}}[\mathcal{C}]$ is also integral, it follows that $\dim \mathcal{C} \leq n - s - 1$, which is a contradiction. Therefore, $G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$ in $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$ for every irreducible component $\mathcal{C}$ of V. We conclude that $G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$ in $\mathbb{K}[V][\boldsymbol{\Lambda}]$, which finishes the proof. $\square$

3.2. **A generic condition for a Noether normalization.** In the sequel, for $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n} \in \mathbb{K}^{(n-s+1)n}$ we write $\boldsymbol{\lambda}^* := (\lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$.

Proposition 3.4. *With hypotheses and notations as before, let $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ be such that $A_V(\boldsymbol{\lambda}^*) \neq 0$. Let $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n - s + 1$, $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$, $B := \mathbb{K}[V]$, $R' := \mathbb{K}(Y_1, \ldots, Y_{n-s})$ and $B' := R' \otimes_{\mathbb{K}} B$. Then the mapping $\pi : V \to \mathbb{A}^r$ defined by $Y_1, \ldots, Y_{n-s}$ is a finite morphism. Further, if $\rho_V(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s}) \neq 0$, then Y_{n-s+1} induces a primitive element of the ring extension $R \hookrightarrow \mathbb{K}[V]$ and $\dim_{R'} B' \leq \delta$.*

Proof. Let $\boldsymbol{\Lambda}^* = (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$. Recall that A_V is homogeneous of degree δ in the $(n-s) \times (n-s)$–minors of $\boldsymbol{\Lambda}^*$. Since $A_V(\boldsymbol{\lambda}^*) \neq 0$, at least one of the minors of the $(n-s) \times n$ matrix $\boldsymbol{\lambda}^*$ is nonzero. We deduce that the linear forms $Y_1, \ldots, Y_{n-s}$ are linearly independent. Thus there exist linear forms $Y_{n-s+1}, \ldots, Y_n \in \mathbb{K}[\boldsymbol{X}]$ such that $Y_1, \ldots, Y_{n-s}, Y_{n-s+1}, \ldots, Y_n$ are linearly independent. Let $\boldsymbol{w}_k := (w_{k1}, \ldots, w_{kn}) \in \mathbb{K}^n$ be such that $Y_{n-s+k} = \boldsymbol{w}_k \cdot \boldsymbol{X}$ for $1 \leq k \leq s$. Let $Q_k \in \mathbb{K}[Z_1, \ldots, Z_{n-s+1}]$ be the polynomial obtained by replacing in P_V the matrix $\boldsymbol{\Lambda}$ for $(\boldsymbol{\lambda}^*, \boldsymbol{w}_k)$. From (3.1) we deduce that

$$(3.4) \qquad Q_k(Y_1, \ldots, Y_{n-s}, \boldsymbol{w}_k \cdot \boldsymbol{\xi}) = 0$$

in the R–algebra B for $1 \leq k \leq s$, where $\boldsymbol{\xi} := (\xi_1, \ldots, \xi_n)$ denotes the n–tuple of coordinate functions in B induced by $X_1, \ldots, X_n$. Observe that $\deg_{Z_{n-s+1}} Q_k \leq \delta$ and that $A_V(\boldsymbol{\lambda}^*)$ is the coefficient of Z_{n-s+1}^δ in Q_k. Since $A_V(\boldsymbol{\lambda}^*) \neq 0$, we have that $\deg_{Z_{n-s+1}} Q_k = \delta$ and (3.4) may be interpreted as a relation of integral dependence for the image $\boldsymbol{w}_k \cdot \boldsymbol{\xi}$ of Y_{n-s+k} in B over R for $1 \leq k \leq s$. Moreover, $\mathbb{K}[Y_1, \ldots, Y_n] = \mathbb{K}[\boldsymbol{X}]$ because the linear forms $Y_1, \ldots, Y_n$ are linearly independent. This implies that $R \to B$ is an integral ring extension.

To prove that π is finite, let $\mathcal{C}$ be any irreducible $\mathbb{K}$–component of V and let $\pi_{\mathcal{C}}$ be the restriction of π to $\mathcal{C}$. It suffices to prove that $\pi_{\mathcal{C}}$ is dominant or, equivalently, that its dual ring homomorphism $\pi_{\mathcal{C}}^* : \mathbb{K}[\mathbb{A}^{n-s}] \to \mathbb{K}[\mathcal{C}]$ is injective. Let t_i denote the i–th coordinate function of $\mathbb{A}^{n-s}$ for $1 \leq i \leq n-s$. With a slight abuse of notation denote also by $\boldsymbol{\xi}$ the n–tuple of coordinate functions of $\mathbb{K}[\mathcal{C}]$ induced by $X_1, \ldots, X_n$. Then $\pi_{\mathcal{C}}^*(t_i) = \boldsymbol{\lambda}_i \cdot \boldsymbol{\xi}$ for $1 \leq i \leq n-s$. Since $\mathbb{K}[\mathcal{C}]$ is integral over $\mathbb{K}[\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}]$ and $\dim \mathcal{C} = r$, we deduce that $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ are algebraically independent over $\mathbb{K}$. This implies the injectivity of $\pi_{\mathcal{C}}^*$, which concludes the proof of the first assertion of the proposition.

Next, taking partial derivatives with respect to the variable $\Lambda_{n-s+1,k}$ at both sides of (3.1), we obtain the following identity in $\mathbb{K}[V][\boldsymbol{\Lambda}]$ for $1 \leq k \leq n$:

$$(3.5) \qquad \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})\,\xi_k + \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) = 0.$$

From (3.1) and (3.5) we deduce that there exists $R_k \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ such that

$$(3.6) \qquad \rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi})\,\xi_k = R_k(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})$$

in $\mathbb{K}[V][\boldsymbol{\Lambda}]$ for $1 \leq k \leq n$. By substituting $\boldsymbol{\lambda}$ for $\boldsymbol{\Lambda}$ in (3.6) we deduce that

$$\rho_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})\xi_k = R_k(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}, \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi})$$

in $\mathbb{K}[V]$ for $1 \leq k \leq n$. By the choice of $\boldsymbol{\lambda}$, the polynomial $\rho_V(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s})$ is nonzero. Since $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ are algebraically independent over $\mathbb{K}$, we deduce that $\rho_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})$ is a nonzero element of R. Then the previous identities show that

the powers of $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}$ generate the R'–vector space B'. In other words, Y_{n-s+1} induces a primitive element of the ring extension $R \hookrightarrow \mathbb{K}[V]$.

Now, let $Q \in R[Z_{n-s+1}]$ be the polynomial obtained by substituting $\boldsymbol{\lambda}$ for $\boldsymbol{\Lambda}$ and $Y_1, \ldots, Y_{n-s}$ for $Z_1, \ldots, Z_{n-s}$ in P_V. From (3.1) we deduce that $Q(\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}) = 0$ in B'. Taking into account that $\deg_{Z_{n-s+1}} Q = \delta$ we conclude that $\dim_{R'} B' \leq \delta$. $\qquad\square$

4. LIFTING POINTS AND LIFTING FIBERS

Assume as in Section 3 that $\mathbb{K}$ is perfect field and $V \subset \mathbb{A}^n$ is an equidimensional $\mathbb{K}$–variety of dimension $n - s$ and degree δ. Let $F_1, \ldots, F_s \in \mathbb{K}[\boldsymbol{X}]$ be polynomials that generate the vanishing ideal $\mathcal{I}$ of V. Assume further that we are given linear forms $Y_1, \ldots, Y_{n-s} \in \mathbb{K}[\boldsymbol{X}]$ defining a finite morphism $\pi : V \to \mathbb{A}^{n-s}$, and let $J \in \mathbb{K}[\boldsymbol{X}]$ be the Jacobian determinant of $Y_1, \ldots, Y_{n-s}, F_1, \ldots, F_s$ with respect to the variables $X_1, \ldots, X_n$. A point $\boldsymbol{p} \in \mathbb{K}^{n-s}$ is called a *lifting point* of π with respect to the system $F_1 = 0, \ldots, F_s = 0$ if $J(\boldsymbol{x}) \neq 0$ for every $\boldsymbol{x} \in \pi^{-1}(\boldsymbol{p})$. We call the zero–dimensional variety $\pi^{-1}(\boldsymbol{p})$ the *lifting fiber* of $\boldsymbol{p}$. According to Proposition 4.6 below, the notions of lifting point and lifting fiber are independent of the choice of the polynomials $F_1, \ldots, F_s$ generating $\mathcal{I}(V)$. Consequently, in the sequel we shall simply say that $\boldsymbol{p}$ is a lifting point of π and $\pi^{-1}(\boldsymbol{p})$ is a lifting fiber without reference to $F_1, \ldots, F_s$.

The notion of lifting fiber in this framework was first introduced in [17]. The concept was isolated in [24], where it was shown how one can use a Kronecker representation of a lifting fiber of a given equidimensional variety to tackle certain fundamental algorithmic problems associated to it (see also [20], [41], [2], [38] and [27] for extensions, refinements and algorithmic aspects related to lifting fibers). The notion is also important in numerical algebraic geometry, where it is known under the name of *witness set* (see, e.g., [44]; see [43] for a dictionary between lifting fibers and witness sets).

As expressed in the introduction, the output of the main algorithm of this paper will be a lifting fiber of the variety defined by the input system. For this reason, we devote Section 4.1 to discuss a number of properties of lifting points and lifting fibers which are important for the algorithm. Then in Section 4.2 we obtain a condition on the coordinates of a point $\boldsymbol{p} \in \mathbb{K}^{n-s}$ which implies that $\boldsymbol{p}$ is a lifting point of π (Theorem 4.10). Finally, in Section 4.3 we show that, taking partial derivatives and specializing a Chow form of V at the coordinates of linear forms $Y_1, \ldots, Y_{n-s+1}$ as above and a lifting point $\boldsymbol{p}$ of π, we obtain a Kronecker representation of the lifting fiber $\pi^{-1}(\boldsymbol{p})$ and a related object, called a lifting curve (Propositions 4.13 and 4.14).

4.1. **Properties of lifting points.** Let $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ be a point as above. Then $\pi^{-1}(\boldsymbol{p}) = V \cap \{Y_1 - p_1 = 0, \ldots, Y_{n-s} - p_{n-s} = 0\}$. We shall prove that $\boldsymbol{p}$ is a lifting point of π if and only if the ideal

$$(4.1) \qquad \mathcal{J} := (F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}) \subset \mathbb{K}[\boldsymbol{X}]$$

is radical. To this aim, we start with a technical result.

Lemma 4.1. *With hypotheses and notations as above, assume further that $\mathbb{K}[V]$ is a free R–module of finite rank D, where $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$. Fix j with $0 \leq j \leq n - s$ and let $\mathcal{J}_j \subseteq \mathbb{K}[\boldsymbol{X}]$ be the ideal $\mathcal{J}_j := (F_1, \ldots, F_s) + (Y_1 - p_1, \ldots, Y_j - p_j)$. Then $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ is a free $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–module of rank equal to D. Moreover, if the coordinate functions*

of V defined by $G_1, \ldots, G_D \in \mathbb{K}[\boldsymbol{X}]$ form a basis of $\mathbb{K}[V]$ as R–module, then they also induce a basis of $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ as $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–module.

Proof. It suffices to prove the last assertion. Let $F \in \mathbb{K}[\boldsymbol{X}]$. There exist $A_1, \ldots, A_D \in R$ such that $F = A_1 G_1 + \cdots + A_D G_D$ in $\mathbb{K}[V]$. Note that

$$A_i \equiv A_i(p_1, \ldots, p_j, Y_{j+1}, \ldots, Y_{n-s}) \qquad \mod (Y_1 - p_1, \ldots, Y_j - p_j)$$

for $1 \leq i \leq D$. Hence, if $B_i := A_i(p_1, \ldots, p_j, Y_{j+1}, \ldots, Y_{n-s})$ for $1 \leq i \leq D$, then $F = B_1 G_1 + \cdots + B_D G_D$ in $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$. This shows that $G_1, \ldots, G_D$ generate $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ as a $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–module. Next, suppose that $B_1 G_1 + \cdots + B_D G_D = 0$ in $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ for certain $B_1, \ldots, B_D \in \mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$. It follows that there exist $H_1, \ldots, H_j \in \mathbb{K}[\boldsymbol{X}]$ such that $B_1 G_1 + \cdots + B_D G_D = H_1(Y_1 - p_1) + \cdots + H_j(Y_j - p_j)$ in $\mathbb{K}[V]$. We can write $H_i = \sum_{k=1}^{D} C_{ik} G_k$ in $\mathbb{K}[V]$ with $C_{ik} \in R$ for $1 \leq i \leq j$ and $1 \leq k \leq D$. As a consequence, we obtain the following identity in $\mathbb{K}[V]$:

$$\left(B_1 - \sum_{k=1}^{j} C_{k1}(Y_k - p_k) \right) G_1 + \cdots + \left(B_D - \sum_{k=1}^{j} C_{kD}(Y_k - p_k) \right) G_D = 0.$$

Since $G_1, \ldots, G_D$ induce a basis of $\mathbb{K}[V]$ as R–module, we see that $B_i = \sum_{k=1}^{j} C_{ki}(Y_k - p_k)$ for $1 \leq i \leq D$. By substituting p_k for Y_k in these identities for $1 \leq k \leq j$, we conclude that $B_i = 0$ for $1 \leq i \leq D$. This shows that $G_1, \ldots, G_D$ define $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–linearly independent elements of $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$, which finishes the proof of the lemma. $\square$

Now we are able to prove that the ideal $\mathcal{J}$ above is radical if $\boldsymbol{p}$ is a lifting point of π.

Lemma 4.2. *With hypotheses and notations as in Lemma 4.1, assume further that $\boldsymbol{p}$ is a lifting point of π. Then $\mathcal{J}_j$ is a radical, equidimensional ideal of dimension $n - s - j$. Further, if $W_j \subseteq \mathbb{A}^n$ is the $\mathbb{K}$–variety defined by $\mathcal{J}_j$, then the mapping $\pi_j : W_j \to \mathbb{A}^{n-s-j}$ defined by $Y_{j+1}, \ldots, Y_{n-s}$ is a finite morphism.*

Proof. Since $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ is a finite $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–module by Lemma 4.1, we deduce that $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ is integral over $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$. This implies that $\dim W_j \leq n - s - j$. On the other hand, the Principal Ideal theorem (see, e.g., [10, Theorem 10.2]) shows that $\dim W_j \geq n - s - j$, from which we conclude that $\dim W_j = n - s - j$. By the unmixedness theorem it follows that $\mathcal{J}_j$ is unmixed. Next, let $\mathcal{C}$ be an irreducible $\mathbb{K}$–component of W_j. We claim that the restriction $\pi_{\mathcal{C}} : \mathcal{C} \to \mathbb{A}^{n-s-j}$ of π_j to $\mathcal{C}$ is a finite morphism. Indeed, since $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}] \hookrightarrow \mathbb{K}[W]$ is an integral extension of rings, so is the extension $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}] \to \mathbb{K}[\mathcal{C}]$ induced by the dual ring homomorphism $\pi_{\mathcal{C}}^*$. Moreover, since $\dim \mathcal{C} = n - s - j$, it follows that $\pi_{\mathcal{C}}^*$ is injective and therefore $\pi_{\mathcal{C}}$ is dominant. This proves the claim, which implies that π_j is a finite morphism.

It remains to prove that $\mathcal{J}_j$ is radical. Let $\mathcal{C}$ be any irreducible $\mathbb{K}$–component of W_j. Since the restriction $\pi_{\mathcal{C}}$ of π_j to $\mathcal{C}$ is a finite morphism, it is surjective, and there exists $\boldsymbol{x} \in \pi_{\mathcal{C}}^{-1}(p_{j+1}, \ldots, p_{n-s}) = \mathcal{C} \cap \{Y_{j+1} - p_{j+1} = 0, \ldots, Y_{n-s} - p_{n-s} = 0\}$. Let J be the Jacobian determinant of $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ with respect to $X_1, \ldots, X_n$ and M_j the Jacobian matrix of $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_j - p_j$ with respect to $X_1, \ldots, X_n$. Since $\boldsymbol{p}$ is a lifting point of π and $\boldsymbol{x} \in \pi^{-1}(\boldsymbol{p})$, we have $J(\boldsymbol{x}) \neq 0$, which implies that $M_j(\boldsymbol{x})$ has rank $s + j$. As a consequence, there exists an $(s + j) \times (s + j)$–minor m of M_j such that $m(\boldsymbol{x}) \neq 0$. It follows that the ideal generated by $\mathcal{J}_j$ and all

the $(s+j) \times (s+j)$–minors of M_j is not contained in $\mathcal{I}(\mathcal{C})$. Then Lemma 2.1 shows that $\mathcal{J}_j$ is radical. $\qquad\square$

Let $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ be a lifting point of π. In the sequel we shall interpret $Y_1, \ldots, Y_{n-s}$ either as linear forms in $X_1, \ldots, X_n$ or as indeterminates over $\mathbb{K}$, each interpretation being clear from the context. By Lemma 4.2, the zero–dimensional ideal $\mathcal{J} := (F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}) \subset \mathbb{K}[\boldsymbol{X}]$ is radical and therefore it is the vanishing ideal of the lifting fiber $V_{\boldsymbol{p}} := \pi^{-1}(\boldsymbol{p})$. Now, for the main algorithm of this paper we shall consider certain curve associated to $\boldsymbol{p}$ and V, which we now introduce. Let $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$ and let $W_{\boldsymbol{p}^*} \subset \mathbb{A}^n$ be the $\mathbb{K}$–variety defined by the ideal

$$\mathcal{K} := (F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1}) \subseteq \mathbb{K}[\boldsymbol{X}].$$

According to Lemma 4.2, $\mathcal{K}$ is a radical, equidimensional ideal of dimension 1 and the mapping $\pi_1 : W_{\boldsymbol{p}^*} \to \mathbb{A}^1$ defined by Y_{n-s} is a finite morphism. We call $W_{\boldsymbol{p}^*}$ the *lifting curve* defined by $\boldsymbol{p}^*$.

We shall identify $V_{\boldsymbol{p}}$ with a zero–dimensional subvariety of $\mathbb{A}^s$ and $W_{\boldsymbol{p}^*}$ with a curve of $\mathbb{A}^{s+1}$ as follows. For simplicity of notations, we shall denote by $F_i(Y_1, \ldots, Y_n)$ or $F_i(\boldsymbol{Y})$ the element of $\mathbb{K}[Y_1, \ldots, Y_n]$ obtained by rewriting $F_i(X_1, \ldots, X_n)$ in the variables $Y_1, \ldots, Y_n$.

Lemma 4.3. *With hypotheses as in Lemma 4.2, the following assertions hold:*

- *the polynomials $F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ generate a radical, zero–dimensional ideal $\overline{\mathcal{J}}$ of $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$, and the $\mathbb{K}$–variety $\mathcal{V}(\overline{\mathcal{J}}) \subset \mathbb{A}^s$ is isomorphic to $V_{\boldsymbol{p}}$. Further, $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$ is a $\mathbb{K}$–vector space of dimension $\mathrm{rank}_R \mathbb{K}[V]$;*
- *the polynomials $F_1(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n)$ generate a radical, equidimensional ideal $\overline{\mathcal{K}}$ of $\mathbb{K}[Y_{n-s}, \ldots, Y_n]$ of dimension 1, and the $\mathbb{K}$–variety $\mathcal{V}(\overline{\mathcal{K}}) \subset \mathbb{A}^{s+1}$ is isomorphic to $W_{\boldsymbol{p}^*}$. Further, $Y_{n-s}, \ldots, Y_n$ are in Noether position with respect to $\overline{\mathcal{K}}$ and $\mathbb{K}[Y_{n-s}, \ldots, Y_n]/\overline{\mathcal{K}}$ is a free $\mathbb{K}[Y_{n-s}]$–module of rank equal to $\mathrm{rank}_R \mathbb{K}[V]$.*

Proof. Clearly, we have an isomorphism of $\mathbb{K}$–algebras

$$\mathbb{K}[Y_1, \ldots, Y_n]/\mathcal{J} \cong \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}},$$

which maps $F(Y_1, \ldots, Y_n) \mod \mathcal{J}$ to $F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) \mod \overline{\mathcal{J}}$. It follows that $\overline{\mathcal{J}}$ is radical and zero–dimensional, since so is $\mathcal{J}$. Therefore, this is an isomorphism between the coordinate rings of $V_{\boldsymbol{p}}$ and $\mathcal{V}(\overline{\mathcal{J}})$, and proves that $V_{\boldsymbol{p}}$ and $\mathcal{V}(\overline{\mathcal{J}})$ are isomorphic. Similarly, we have an isomorphism of $\mathbb{K}$–algebras

$$\mathbb{K}[Y_1, \ldots, Y_n]/\mathcal{K} \cong \mathbb{K}[Y_{n-s}, \ldots, Y_n]/\overline{\mathcal{K}},$$

which maps $F(Y_1, \ldots, Y_n) \mod \mathcal{K}$ to $F(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n) \mod \overline{\mathcal{K}}$. Arguing as before we conclude that $\overline{\mathcal{K}}$ is radical and $W_{\boldsymbol{p}^*}$ and $\mathcal{V}(\overline{\mathcal{K}})$ are isomorphic. Further, we have that Y_j is integral over $\mathbb{K}[Y_{n-s}]$ modulo $\overline{\mathcal{K}}$ for $n - s + 1 \leq j \leq n$, which proves that $Y_{n-s}, \ldots, Y_n$ are in Noether position with respect to $\overline{\mathcal{K}}$. Finally, the assertions concerning freeness and ranks follow by Lemma 4.1, which completes the proof of the lemma. $\qquad\square$

A critical step in our main algorithm is to obtain a Kronecker representation of a lifting curve $W_{\boldsymbol{p}^*}$ from one of a lifting fiber $V_{\boldsymbol{p}}$. This will be achieved by considering a symbolic version of the Newton method, which requires that the polynomials $F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ define all points of $V_{\boldsymbol{p}}$ by transversal cuts. Further, in Section 6.2 we shall lift a Kronecker representation of the output lifting fiber modulo a prime number p, which also requires such a transversality condition. As the next result shows, this is guaranteed if $\boldsymbol{p}$ is a lifting point π.

Lemma 4.4. *With hypotheses as in Lemma 4.2, the Jacobian determinant $\overline{J}$ of the polynomials $F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ with respect to $Y_{n-s+1}, \ldots, Y_n$ is invertible in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$.*

Proof. Let $\mathcal{P}_1, \ldots, \mathcal{P}_N$ be the minimal prime ideals of $\overline{\mathcal{J}}$. Since $\overline{\mathcal{J}}$ is radical, by Lemma 2.1 we deduce that $\overline{J} \notin \mathcal{P}_i$ for $1 \leq i \leq N$. As $\overline{\mathcal{J}}$ is of dimension zero, each $\mathcal{P}_i$ is a maximal ideal of $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$, which implies that $\overline{J}$ is a unit in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\mathcal{P}_i$ for $1 \leq i \leq N$. By the Chinese remainder theorem we conclude that $\overline{J}$ is a unit in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$, which finishes the proof of the lemma. $\qquad\square$

Finally, assuming that $F_1, \ldots, F_s$ form a regular sequence, we shall need to see that this is preserved when specializing $(Y_1, \ldots, Y_{n-s})$ at a lifting point $\boldsymbol{p}$. We have the following result.

Lemma 4.5. *Assume that $F_1, \ldots, F_s$ form a regular sequence of $\mathbb{K}[\boldsymbol{X}]$ and $Y_1, \ldots, Y_n$ are linear forms of $\mathbb{K}[\boldsymbol{X}]$ in Noether position with respect to $V_i := \{F_1 = 0, \ldots, F_i = 0\}$ for $1 \leq i \leq s$. Then $F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ form a regular sequence of $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$ for any $\boldsymbol{p} \in \mathbb{K}^{n-s}$.*

Proof. It suffices to show that $F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_i(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ define a subvariety of $\mathbb{A}^s$ of dimension $s - i$ for $1 \leq i \leq s$. Let $L_s := \{Y_1 = p_1, \ldots, Y_{n-s} = p_{n-s}\} \subset \mathbb{A}^n$ and $\pi_i : V_i \to \mathbb{A}^{n-i}$ the mapping defined by $Y_1, \ldots, Y_{n-i}$. Then $V_i \cap L_s = \pi_i^{-1}(\{Y_1 = p_1, \ldots, Y_{n-s} = p_{n-s}\})$. Since π_i is a finite morphism, we have that $\dim V_i \cap L_s = \dim_{\mathbb{A}^{n-i}}\{Y_1 = p_1, \ldots, t_{n-s} = Y_{n-s}\} = s - i$, and the conclusion of the lemma follows by noting that $\{F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) = 0, \ldots, F_i(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) = 0\}$ and $V_i \cap L_s$ are isomorphic varieties. $\qquad\square$

4.2. **A condition for lifting points.** In this section we obtain a condition for the coordinates of a point $\boldsymbol{p} \in \mathbb{K}^{n-s}$ which implies that it is a lifting point of π. A first step in this direction is provided by the following characterization of the notion of lifting point, which also proves that the concept is independent of the polynomials $F_1, \ldots, F_s$ generating the vanishing ideal of the variety V.

Proposition 4.6. *Assume that $\mathbb{K}[V]$ is a free R–module of finite rank $D := \operatorname{rank}_R \mathbb{K}[V]$. Then $\#\pi^{-1}(\boldsymbol{p}) \leq D$ for any $\boldsymbol{p} \in \mathbb{K}^{n-s}$, with equality if and only if $\boldsymbol{p}$ is a lifting point.*

Proof. Let $\boldsymbol{p} := (p_1, \ldots, p_{n-s})$ and let $\mathcal{J} \subset \mathbb{K}[\boldsymbol{X}]$ be the zero–dimensional ideal of (4.1). By Lemma 4.1 we have $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\mathcal{J} = D$. Since $\#\pi^{-1}(\boldsymbol{p}) = \dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}}$, the inequality of the statement follows.

Now we prove the characterization of lifting points. Let $\chi_J \in R[T]$ be the characteristic polynomial of J modulo $\mathcal{I}$. Since by Lemma 4.1 a basis of $\mathbb{K}[V]$ as R–module induces a

basis of $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}$ as $\mathbb{K}$–vector space, it is easy to see that $\chi_{J}(\boldsymbol{p}, T)$ is the characteristic polynomial of J modulo $\mathcal{J}$. Let $\mu := \chi_{J}(0)$ be the constant term of χ_{J}, so that $\mu(\boldsymbol{p})$ is the constant term of $\chi_{J}(\boldsymbol{p}, T)$. By the Nullstellensatz, $\boldsymbol{p}$ is a lifting point of π if and only if the equality of ideals $\mathcal{J} + (J) = (1)$ holds in $\mathbb{K}[\boldsymbol{X}]$. Note that, by the unmixedness theorem, $\mathcal{J}$ is unmixed. Then $\mathcal{J} + (J) = (1)$ if and only if $\mu(\boldsymbol{p}) \neq 0$ (see, e.g., [9, Lemma 2.1(c)]). Further, $\mu(\boldsymbol{p}) \neq 0$ if and only if J is not a zero divisor in $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}$ (see, e.g., [9, Lemma 2.1(b)]), which in turn holds if and only if J is not contained in any associated prime of $\mathcal{J}$ (see, e.g., [33, Theorem 6.1(ii)]). Finally, by Lemma 2.1, the latter is equivalent to the radicality of $\mathcal{J}$. Summarizing, we have that $\boldsymbol{p}$ is a lifting point of π if and only if $\mathcal{J}$ is a radical ideal. On the other hand, $\mathcal{J}$ is radical if and only if $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\mathcal{J} = \#\pi^{-1}(\boldsymbol{p})$. Since $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\mathcal{J} = D$, the proposition follows. $\square$

Let $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$, $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s+1})$ and let $P_V \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ be a Chow form of V. Denote as before by $A_V \in \mathbb{K}[\boldsymbol{\Lambda}_1, \ldots, \boldsymbol{\Lambda}_{n-s}]$ the (nonzero) coefficient of the monomial Z_{n-s+1}^{δ} in P_V, and by $\rho_V \in \mathbb{K}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ the discriminant of P_V with respect to Z_{n-s+1}. Consider the quotient ring $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V)$ as a $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–algebra by means of the canonical ring homomorphism $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V)$. Further, consider as before $\mathbb{K}[V][\boldsymbol{\Lambda}]$ as a $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–algebra by means of the ring homomorphism $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[V][\boldsymbol{\Lambda}]$ which maps any $F \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ to $F(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})$. By Lemma 3.2, the polynomial $\partial P_V/\partial Z_{n-s+1}$ is nonzero and hence

$$S := \left\{ (\partial P_V/\partial Z_{n-s+1})^{\eta} : \eta \geq 0 \right\}$$

is a multiplicatively closed subset of $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. We consider the localizations

$$\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}} := S^{-1}\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}],$$
$$\left(\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V) \right)_{\partial P_V/\partial Z_{n-s+1}} := S^{-1}\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V),$$
$$\mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}} := S^{-1}\mathbb{K}[V][\boldsymbol{\Lambda}].$$

Let $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V) \to \mathbb{K}[V][\boldsymbol{\Lambda}]$ be the $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–algebra homomorphism that maps $[Z_i]_{\mathrm{mod} P_V}$ to $\boldsymbol{\Lambda}_i \cdot \boldsymbol{\xi}$ for $1 \leq i \leq n-s+1$ and consider the $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$–algebra homomorphism

$$(4.2) \qquad \Phi : \left(\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V) \right)_{\partial P_V/\partial Z_{n-s+1}} \to \mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}}.$$

that extends this map. The next result asserts that Φ is an isomorphism.

Lemma 4.7. Φ *is an isomorphism of* $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$*–algebras.*

Proof. By the minimality of P_V the homomorphism $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V) \to \mathbb{K}[V][\boldsymbol{\Lambda}]$ above is injective, and thus so is Φ. To prove surjectivity, by (3.5) we have $\xi_k = -\frac{\partial P_V/\partial \Lambda_{n-s+1,k}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})}{\partial P_V/\partial Z_{n-s+1}}$ in $\mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}}$ for $1 \leq k \leq n$. It follows that

$$(4.3) \qquad \xi_k = \Phi \left(-\frac{[\partial P_V/\partial \Lambda_{n-s+1,k}]_{\mathrm{mod} P_V}}{\partial P_V/\partial Z_{n-s+1}} \right)$$

for $1 \leq k \leq n$. Since $\xi_1, \ldots, \xi_n$ generate $\mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}}$ as a $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$–algebra, the lemma follows. $\square$

We shall also need the following technical result.

Lemma 4.8. *For any $F \in \mathbb{K}[\boldsymbol{X}]$, let $F_\Lambda \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ be any polynomial such that*

$$(4.4) \qquad F\left(-\frac{\partial P_V/\partial \Lambda_{n-s+1,1}}{\partial P_V/\partial Z_{n-s+1}}, \dots, -\frac{\partial P_V/\partial \Lambda_{n-s+1,n}}{\partial P_V/\partial Z_{n-s+1}}\right) = \frac{F_\Lambda}{(\partial P_V/\partial Z_{n-s+1})^\eta}$$

for some $\eta \in \mathbb{N}$. If F vanishes on V, then F_Λ is a multiple of P_V. Further, for $1 \le i \le n-s+1$, the following polynomial $H_i \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ is a multiple of P_V:

$$(4.5) \qquad H_i := \frac{\partial P_V}{\partial Z_{n-s+1}} Z_i + \sum_{j=1}^n \Lambda_{ij} \frac{\partial P_V}{\partial \Lambda_{n-s+1,j}}.$$

Proof. Considering (4.4) modulo P_V and applying Φ to both sides, by (4.3) we see that

$$F(\boldsymbol{\xi}) = \frac{F_\Lambda(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})}{(\partial P_V/\partial Z_{n-s+1})^\eta}.$$

Since $F(\boldsymbol{\xi}) = 0$ and $\partial P_V/\partial Z_{n-s+1}$ is not a zero divisor of $\mathbb{K}[V][\boldsymbol{\Lambda}]$ (Lemma 3.3), we conclude that $F_\Lambda(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) = 0$. By the minimality of P_V the first assertion follows.

To prove the second assertion, we observe that

$$(4.6) \qquad [Z_i]_{\mathrm{mod}P_V} = \Phi^{-1}(\boldsymbol{\Lambda}_i \cdot \boldsymbol{\xi}) = \sum_{j=1}^n \Lambda_{ij}\, \Phi^{-1}(\xi_j)$$

for $1 \le i \le n-s+1$. By this and (4.3) it follows that

$$[Z_i]_{\mathrm{mod}P_V} = -\sum_{j=1}^n \Lambda_{ij} \frac{[\partial P_V/\partial \Lambda_{n-s+1,j}]_{\mathrm{mod}P_V}}{\partial P_V/\partial Z_{n-s+1}}$$

for $1 \le i \le n-s+1$, which readily implies the second assertion of the lemma. $\qquad\square$

The next result, combined with Proposition 4.6, will yield the condition characterizing lifting points we are looking for.

Proposition 4.9. *Let $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} \in \mathbb{K}^{n-s}$ be such that $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \ne 0$, let $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \le i \le n-s$ and $\pi : V \to \mathbb{A}^{n-s}$ the mapping defined by $Y_1, \dots, Y_{n-s}$. Then $\#\pi^{-1}(\boldsymbol{p}) = \delta$.*

Proof. By the choice of $\boldsymbol{\lambda}$, the polynomial $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ has degree δ. Since

$$\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) = \mathrm{Res}_{Z_{n-s+1}}\left(P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1}), \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})\right)$$

and $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \ne 0$, the polynomial $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ is separable. Let $z_1, \dots, z_\delta \in \overline{\mathbb{K}}$ be the δ different roots of $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ and set $\boldsymbol{y}^k := (\boldsymbol{p}, z_k)$ for $1 \le k \le \delta$. We have that $\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k) \ne 0$ for $1 \le k \le \delta$, and thus the point

$$\boldsymbol{x}^k := \left(-\frac{\partial P_V/\partial \Lambda_{n-s+1,1}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}{\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}, \dots, -\frac{\partial P_V/\partial \Lambda_{n-s+1,n}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}{\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}\right) \in \mathbb{A}^n$$

is well defined for $1 \le k \le \delta$.

We claim that $\boldsymbol{x}^1, \dots, \boldsymbol{x}^\delta$ are pairwise distinct and $\pi^{-1}(\boldsymbol{p}) = \{\boldsymbol{x}^1, \dots, \boldsymbol{x}^\delta\}$. Indeed, let $F \in \mathbb{K}[\boldsymbol{X}]$ be any polynomial vanishing on V and $F_\Lambda \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ a corresponding polynomial according to (4.4). By Lemma 4.8 we have $F_\Lambda(\boldsymbol{\lambda}, \boldsymbol{y}^k) = 0$, and thus $F(\boldsymbol{x}^k) =$

0, for $1 \le k \le \delta$. This proves that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta$ belong to V. Further, Lemma 4.8 also shows that

$$H_i(\boldsymbol{\lambda}, \boldsymbol{y}^k) = \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}, \boldsymbol{y}^k)y_i^k + \sum_{j=1}^{n} \lambda_{ij}\frac{\partial P_V}{\partial \Lambda_{n-s+1,j}}(\boldsymbol{\lambda}, \boldsymbol{y}^k) = 0$$

for $1 \le i \le n - s + 1$ and $1 \le k \le \delta$. By the definition of $\boldsymbol{x}^k$ it follows that

$$(4.7) \qquad\qquad y_i^k = \boldsymbol{\lambda}_i \cdot \boldsymbol{x}^k \quad (1 \le i \le n - s + 1).$$

Since $y_i^k = p_i$ for $1 \le i \le n - s$, (4.7) implies that $\pi(\boldsymbol{x}^k) = \boldsymbol{p}$ and $z_k = \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{x}^k$ for $1 \le k \le \delta$. Since the z_k are pairwise distinct, we deduce that so are the $\boldsymbol{x}^k$. This proves that $\#\pi^{-1}(\boldsymbol{p}) \ge \delta$. On the other hand, since π is a finite morphism (Proposition 3.4), the fiber $\pi^{-1}(\boldsymbol{p})$ is finite, and by (2.1) we have

$$\#\pi^{-1}(\boldsymbol{p}) = \deg\left(V \cap \{Y_1 - p_1 = 0, \ldots, Y_{n-s} - p_{n-s} = 0\}\right) \le \deg V = \delta,$$

which concludes the proof of the claim and the proposition. $\qquad\square$

Now we are able to state the main result of this section.

Theorem 4.10. *Let $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} \in \mathbb{K}^{n-s}$ be such that $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \ne 0$. Let $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \le i \le n - s + 1$ and $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$. Then:*
- *the mapping $\pi : V \to \mathbb{A}^{n-s}$ defined by $Y_1, \ldots, Y_{n-s}$ is a finite morphism and Y_{n-s+1} induces a primitive element of the ring extension $R \hookrightarrow \mathbb{K}[V]$;*
- *if $\mathbb{K}[V]$ is a free R–module, then $\mathrm{rank}_R\mathbb{K}[V] = \delta$;*
- *$\boldsymbol{p}$ is a lifting point of π and Y_{n-s+1} induces a primitive element of $\pi^{-1}(\boldsymbol{p})$.*

Proof. Proposition 3.4 proves the first assertion. Combining Propositions 3.4, 4.6 and 4.9 we deduce that $\delta = \#\pi^{-1}(\boldsymbol{p}) \le \mathrm{rank}_R\mathbb{K}[V] \le \delta$. It follows that $\#\pi^{-1}(\boldsymbol{p}) = \delta$ and $\boldsymbol{p}$ is a lifting point of π. Next, let $\boldsymbol{p} := (p_1, \ldots, p_{n-s})$. By substituting $\boldsymbol{\lambda}$ for $\boldsymbol{\Lambda}$ and $p_1, \ldots, p_{n-s}$ for $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ in (3.6), we deduce that

$$\rho_V(\boldsymbol{\lambda}, \boldsymbol{p})\xi_k = R_k(\boldsymbol{\lambda}, \boldsymbol{p}, \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi})$$

in $\pi^{-1}(\boldsymbol{p})$ for $1 \le k \le n$. Since $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \ne 0$, we conclude that $\mathbb{K}\left[\pi^{-1}(\boldsymbol{p})\right] = \mathbb{K}[\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}]$, which proves that Y_{n-s+1} induces a primitive element of $\pi^{-1}(\boldsymbol{p})$. $\qquad\square$

4.3. Kronecker representations from specializations of the Chow form.
Let be given $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \le i \le n-s+1, 1 \le j \le n} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ satisfying the hypotheses of Proposition 4.6 and Theorem 4.10. Define $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \le i \le n - s + 1$, and let $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$ and $B := \mathbb{K}[V]$. Assume that we are also given linear forms $Y_{n-s+2}, \ldots, Y_n \in \mathbb{K}[\boldsymbol{X}]$ such that $Y_1, \ldots, Y_n$ are linearly independent. Then

- $Y_1, \ldots, Y_n$ are in Noether position with respect to $\mathcal{I}$;
- $\boldsymbol{p}$ is a lifting point of the finite morphism $\pi : V \to \mathbb{A}^{n-s}$ defined by $Y_1, \ldots, Y_{n-s}$;
- B is a free R–module of finite rank equal to δ.

We shall show that Kronecker representations of the definining ideals of V, the lifting fiber $V_{\boldsymbol{p}}$ and the lifting curve $W_{\boldsymbol{p}^*}$ can be obtained by specializing any Chow form of V. This will provide a criterion to check that the modular reductions considered during our main algorithm behave properly.

Let $P_V \in \mathbb{K}[\mathbf{\Lambda}, \mathbf{Z}]$ be a Chow form of V, and let $A_V \in \mathbb{K}[\mathbf{\Lambda}_1, \ldots, \mathbf{\Lambda}_{n-s}]$ and $\rho_V \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}]$ be defined as in Section 4.2. By (3.1) and (3.5), we have

$$(4.8) \quad P_V(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi}) = 0, \quad \frac{\partial P_V}{\partial Z_{n-s+1}}(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi})\xi_k + \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi}) = 0 \quad (1 \le k \le n),$$

in $\mathbb{K}[V][\mathbf{\Lambda}]$. Let T be a new indeterminate and define $Q, W_{n-s+2}, \ldots, W_n \in R[T]$ by

$$Q := \frac{P_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}, T)}{A_V(\boldsymbol{\lambda}^*)}, \quad W_j := -\sum_{k=1}^{n} \frac{\lambda_{jk}}{A_V(\boldsymbol{\lambda}^*)} \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}, T)$$

for $n - s + 2 \le j \le n$. Substituting $\boldsymbol{\lambda}$ for $\mathbf{\Lambda}$ in (4.8) we deduce that

$$(4.9) \quad Q(Y_{n-s+1}) \in \mathcal{I}, \quad Q'(Y_{n-s+1})Y_j - W_j(Y_{n-s+1}) \in \mathcal{I} \quad (n - s + 2 \le j \le n),$$

where Q' denotes the first derivative of Q with respect to T.

Note that Q is a monic polynomial of degree δ and $\deg W_j < \delta$ for $n - s + 2 \le j \le n$. On the other hand, by the choice of $\boldsymbol{\lambda}$ we have that the discriminant of Q, which is equal to $\rho_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})/A_V(\boldsymbol{\lambda}^*)^{2\delta-1}$, is a nonzero element of R. Thus Q is square–free and Q' is invertible modulo Q. In particular, $Q'(Y_{n-s+1})$ is invertible in $B' := R'[Y_{n-s+1}, \ldots, Y_n]/\mathcal{I}^e$, and (4.9) shows that the homomorphism of R'–algebras $R'[T]/(Q) \to B'$, which maps $T \mod Q$ to $Y_{n-s+1} \mod \mathcal{I}^e$, is surjective. This means that Y_{n-s+1} is a primitive element for $\mathcal{I}$. On the other hand, since $\dim_{R'} B' = \delta$, the above homomorphism is an isomorphism. We conclude that Q is the minimal polynomial of Y_{n-s+1} over R' modulo $\mathcal{I}^e$, and we have the following identity of ideals in $R'[Y_{n-s+1}, \ldots, Y_n]$:

$$\mathcal{I}^e = \big(Q(Y_{n-s+1}), Q'(Y_{n-s+1})Y_{n-s+2} - W_{n-s+2}(Y_{n-s+1}), \ldots, Q'(Y_{n-s+1})Y_n - W_n(Y_{n-s+1})\big).$$

Further, by construction $\deg_T W_j \le \delta - 1$ for $n - s + 2 \le j \le n$. As a consequence, we obtain the following result.

Proposition 4.11. *The polynomials $Q, W_{n-s+2}, \ldots, W_n$ form the Kronecker representation of $\mathcal{I}$ with primitive element Y_{n-s+1}.*

Remark 4.12. *Since $\deg_{(Z_1, \ldots, Z_{n-s+1})} P_V = \deg_{Z_{n-s+1}} P_V = \delta$ (see Section 3.1), we have $\deg_{(Y_1, \ldots, Y_{n-s}, T)} Q = \delta$ and $\deg_{(Y_1, \ldots, Y_{n-s}, T)} W_j \le \delta$ for $n - s + 2 \le j \le n$.*

Now, let $\mathcal{J} := \mathcal{I} + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s})$. Denote as in Lemma 4.3 by $\overline{\mathcal{J}}$ the image of $\mathcal{J}$ in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$. Substituting $p_1, \ldots, p_{n-s}$ for $Y_1, \ldots, Y_{n-s}$ in (4.9) we obtain

$$(4.10) \quad Q(\boldsymbol{p}, Y_{n-s+1}) \in \overline{\mathcal{J}}, \quad Q'(\boldsymbol{p}, Y_{n-s+1})Y_j - W_j(\boldsymbol{p}, Y_{n-s+1}) \in \overline{\mathcal{J}} \quad (n - s + 2 \le j \le n).$$

The polynomial $Q(\boldsymbol{p}, T)$ is monic of degree δ and $\deg W_j(\boldsymbol{p}, T) < \delta$ for $n - s + 2 \le j \le n$. The discriminant of $Q(\boldsymbol{p}, T)$ is $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p})/A_V(\boldsymbol{\lambda}^*)^{2\delta-1}$, and thus nonzero due to the choice of $\boldsymbol{\lambda}$ and $\boldsymbol{p}$. It follows that $Q(\boldsymbol{p}, T)$ is square–free and $Q'(\boldsymbol{p}, T)$ is invertible modulo $Q(\boldsymbol{p}, T)$. This implies that $Q'(\boldsymbol{p}, Y_{n-s+1})$ is invertible in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$, and (4.10) shows that the homomorphism of $\mathbb{K}$–algebras

$$\mathbb{K}[T]/\big(Q(\boldsymbol{p}, T)\big) \to K[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}, \quad T \mod Q(\boldsymbol{p}, T) \mapsto Y_{n-s+1} \mod \overline{\mathcal{J}},$$

is surjective. This means that Y_{n-s+1} induces a primitive element for $\overline{\mathcal{J}}$. Further, since $\mathbb{K}[V_{\boldsymbol{p}}] \cong \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$ is a $\mathbb{K}$–vector space of dimension equal to $\mathrm{rank}_R \mathbb{K}[V]$, and $\mathrm{rank}_R \mathbb{K}[V] = \deg Q(\boldsymbol{p}, T) = \delta$, it follows that the above homomorphism is an

isomorphism. We conclude that $Q(\boldsymbol{p}, T)$ is the minimal polynomial of Y_{n-s+1} over $\mathbb{K}$ modulo $\overline{\mathcal{J}}$, and that the following equality of ideals holds in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$:

$$\overline{\mathcal{J}} = \big(Q(\boldsymbol{p}, Y_{n-s+1}), Q'(\boldsymbol{p}, Y_{n-s+1})Y_j - W_j(\boldsymbol{p}, Y_{n-s+1}) : n - s + 2 \leq j \leq n\big).$$

Identifying $\mathcal{J}$ with its image in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$, we obtain the following result.

Proposition 4.13. *The polynomials $Q(\boldsymbol{p}, T), W_{n-s+2}(\boldsymbol{p}, T), \ldots, W_n(\boldsymbol{p}, T)$ form the Kronecker representation of $\mathcal{J}$ with primitive element Y_{n-s+1}.*

Finally, we discuss a Kronecker representation of $\mathcal{K} := \mathcal{I} + (Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1})$. Let $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$ and let $\overline{\mathcal{K}}$ be the image of $\mathcal{K}$ in $\mathbb{K}[Y_{n-s}, \ldots, Y_n]$ as in Lemma 4.3. Then $Y_{n-s}, \ldots, Y_n$ are in Noether position with respect to $\overline{\mathcal{K}}$ and $\mathbb{K}[W_{\boldsymbol{p}^*}] \cong \mathbb{K}[Y_{n-s}, \ldots, Y_n]/\overline{\mathcal{K}}$ is a free $\mathbb{K}[Y_{n-s}]$–module of rank equal to $\mathrm{rank}_R \mathbb{K}[V]$. Substituting $p_1, \ldots, p_{n-s-1}$ for $Y_1, \ldots, Y_{n-s-1}$ in (4.9), we deduce that

$$(4.11) \qquad\qquad Q(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) \in \overline{\mathcal{K}},$$

$$Q'(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1})Y_j - W_j(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) \in \overline{\mathcal{K}} \quad (n - s + 2 \leq j \leq n).$$

Observe that $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ is monic of degree δ and $\deg W_j(\boldsymbol{p}^*, Y_{n-s}, T) < \delta$ for $n - s + 2 \leq j \leq n$. By the choice of $\boldsymbol{\lambda}$, the discriminant $\rho_V(\lambda, \boldsymbol{p}^*, Y_{n-s})/A_V(\boldsymbol{\lambda}^*)^{2\delta-1}$ of $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ is a nonzero element of $\mathbb{K}[Y_{n-s}]$. Therefore, $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ is square–free, $Q'(\boldsymbol{p}^*, Y_{n-s}, T)$ is invertible modulo $Q(\boldsymbol{p}^*, Y_{n-s}, T)$, and thus $Q'(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1})$ is invertible in $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{K}}^e$, where $\overline{\mathcal{K}}^e$ is the extension of $\overline{\mathcal{K}}$ to the ring $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]$. By (4.11) the homomorphism of $\mathbb{K}(Y_{n-s})$–algebras

$$\mathbb{K}(Y_{n-s})[T]/\big(Q(\boldsymbol{p}^*, Y_{n-s}, T)\big) \to \mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{K}}^e$$

which maps $T \mod Q(\boldsymbol{p}^*, Y_{n-s}, T)$ to $Y_{n-s+1} \mod \overline{\mathcal{K}}^e$ is surjective. In particular, Y_{n-s+1} induces a primitive element for $\overline{\mathcal{K}}$. Since $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{K}}^e$ is a $\mathbb{K}(Y_{n-s})$–vector space of dimension equal to $\mathrm{rank}_R \mathbb{K}[V] = \deg Q(\boldsymbol{p}^*, Y_{n-s}, T) = \delta$, this homomorphism is an isomorphism. We conclude that $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ is the minimal polynomial of Y_{n-s+1} modulo $\overline{\mathcal{K}}^e$, and the following equality of ideals holds in $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]$:

$$\overline{\mathcal{K}}^e = \big(Q(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}), Q'(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1})Y_{n-s+2} - W_{n-s+2}(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}),$$

$$\ldots, Q'(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1})Y_n - W_n(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1})\big).$$

Identifying $\mathcal{K}$ with its image in $\mathbb{K}[Y_{n-s}, \ldots, Y_n]$, we obtain the following result.

Proposition 4.14. $Q(\boldsymbol{p}^*, Y_{n-s}, T), W_{n-s+2}(\boldsymbol{p}^*, Y_{n-s}, T), \ldots, W_n(\boldsymbol{p}^*, Y_{n-s}, T)$ *form the Kronecker representation of $\mathcal{K}$ with primitive element Y_{n-s+1}.*

5. ON THE CONDITIONS FOR A GOOD MODULAR REDUCTION

From now on we consider polynomials $F_1, \ldots, F_r \in \mathbb{Z}[\boldsymbol{X}]$ of degree at most d that form a reduced regular sequence, and denote $\mathcal{V}_s := V(F_1, \ldots, F_s)$ and $\delta_s := \deg \mathcal{V}_s$ for $1 \leq s \leq r$. As explained in the introduction, our aim is to describe an algorithm for solving the system $F_1 = 0, \ldots, F_r = 0$ and analyze its bit complexity. This algorithm outputs a Kronecker representation of a lifting fiber of $\mathcal{V}_r$ and relies on modular methods. For this reason, a crucial point is the choice of a "lucky" prime number, namely one which provides a good modular reduction, of "low" bit length. In this section we exhibit

a nonzero integer multiple $\mathfrak{N}$ of all the unlucky prime numbers. More precisely, we show that, for a suitable choice of $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2}$ and $\boldsymbol{p} \in \mathbb{Z}^{n-1}$, there is a nonzero integer $\mathfrak{N}$ with the following property: if p is a prime number not dividing $\mathfrak{N}$, then all conditions in Theorem 1.2 modulo p are satisfied. Further, our description of $\mathfrak{N}$ is explicit enough as to allow us to estimate its bit length (Theorem A.13). By this estimate and well–known methods for finding small primes not dividing a given integer we shall be able to compute in Section 6 a lucky prime of low bit length with hight probability of success.

The determination of the integer $\mathfrak{N}$ proceeds in several stages. In Section 5.1 we deal with conditions (1)–(2) of Theorem 1.2, and the corresponding results are summarized in Theorem 5.5. Then in Section 5.2 we discuss the fulfillment of the more involved condition (3) of Theorem 1.2.

In the sequel, if p is a prime number and G any polynomial with integer coefficients, we denote by G_p its reduction modulo p. Further, if $G_1, \ldots, G_t \in \mathbb{Z}[\boldsymbol{X}]$ define a variety $\mathcal{W} := V(G_1, \ldots, G_t) \subset \mathbb{A}^m := \mathbb{A}^m(\overline{Q})$, we denote by $\mathcal{W}_p := V(G_{1,p}, \ldots, G_{t,p}) \subseteq \mathbb{A}^m_{\mathbb{F}_p} := \mathbb{A}^m(\overline{\mathbb{F}}_p)$ the corresponding reduction modulo p.

5.1. **First conditions for a good modular reduction.** Fix s with $1 \leq s \leq r$ and $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ such that the hypotheses of Proposition 3.4 are satisfied. In this section we establish a condition on a prime number p which implies that the variety $\mathcal{V}_{s,p}$ is equidimensional and reduced of dimension $n - s$ and degree δ_s, and the linear forms $(Y_{1,p}, \ldots, Y_{n-s,p}) := \boldsymbol{\lambda}_p \boldsymbol{X}$ are the free variables of a Noether normalization of $\mathcal{V}_{s,p}$.

Throughout this section and the next one, $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$ and $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s+1})$ denote a matrix and a vector of indeterminates over $\mathbb{Q}[\mathcal{V}_s]$. We set $\boldsymbol{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ and $\boldsymbol{\Lambda}_i \cdot \boldsymbol{X} := \sum_{j=1}^n \Lambda_{ij} X_j$ for $1 \leq i \leq n-s+1$. Further, we denote $\boldsymbol{\Lambda X} := (\boldsymbol{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \boldsymbol{\Lambda}_{n-s+1} \cdot \boldsymbol{X})$, $\boldsymbol{\Lambda}^* := (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$ and $\boldsymbol{\Lambda}^* \boldsymbol{X} := (\boldsymbol{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{X})$. Finally, given $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n} \in \mathbb{Z}^{(n-s+1)n}$, we adopt the notations $\boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ $(1 \leq i \leq n-s+1)$, $\boldsymbol{\lambda X}$, $\boldsymbol{\lambda}^*$ and $\boldsymbol{\lambda}^* \boldsymbol{X}$ accordingly. Denote by $P_s \in \mathbb{Q}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ a Chow form of $\mathcal{V}_s$. Since P_s is uniquely determined up to nonzero multiples in $\mathbb{Q}$, we may assume that P_s is a primitive polynomial of $\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Let as before $A_s \in \mathbb{Z}[\boldsymbol{\Lambda}_1, \ldots, \boldsymbol{\Lambda}_{n-s}]$ be the coefficient of the monomial $Z_{n-s+1}^{\delta_s}$ in P_s and $\rho_s \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ the discriminant of P_s with respect to Z_{n-s+1}, that is,

$$\rho_s := \operatorname{Res}_{Z_{n-s+1}}\left(P_s, \frac{\partial P_s}{\partial Z_{n-s+1}}\right).$$

According to Lemma 3.2, the polynomials $\partial P_s / \partial Z_{n-s+1}$ and ρ_s are both nonzero.

As a first step, we give a condition for consistency of the system $F_{1,p} = 0, \ldots, F_{s,p} = 0$.

Lemma 5.1. *Let p be a prime number such that $A_{s,p}(\boldsymbol{\lambda}_p^*)\rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s})$ is nonzero. Let $Y_{i,p} := \boldsymbol{\lambda}_{i,p} \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s$. If $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\mathbb{F}_p}$ is the mapping defined by $Y_{1,p}, \ldots, Y_{n-s,p}$, then any $\boldsymbol{q} \in \mathbb{A}^{n-s}_{\mathbb{F}_p}$ with $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$ satisfies $\#\pi_{s,p}^{-1}(\boldsymbol{q}) \geq \delta_s$.*

Proof. Note that $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})$ has degree δ_s, because $A_{s,p}(\boldsymbol{\lambda}_p^*) \neq 0$. It follows that

$$\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \operatorname{Res}_{Z_{n-s+1}}\left(P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1}), \frac{\partial P_{s,p}}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})\right),$$

and thus the polynomial $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})$ is separable. Let $z_1, \ldots, z_{\delta_s} \in \overline{\mathbb{F}}_p$ be the roots of $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})$ and $\boldsymbol{y}^k := (\boldsymbol{q}, z_k)$ for $1 \le k \le \delta_s$. As $\partial P_{s,p}/\partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) \ne 0$ for $1 \le k \le \delta_s$, the point

$$\boldsymbol{x}^k := \left(-\frac{\partial P_{s,p}/\partial \Lambda_{n-s+1,1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}{\partial P_{s,p}/\partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}, \ldots, -\frac{\partial P_{s,p}/\partial \Lambda_{n-s+1,n}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}{\partial P_{s,p}/\partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)} \right) \in \mathbb{A}^n_{\overline{\mathbb{F}}_p}$$

is well defined for $1 \le k \le \delta_s$.

We claim that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ are pairwise distinct and $\{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}\} \subseteq \pi_{s,p}^{-1}(\boldsymbol{q})$. Indeed, let $F_{\Lambda,j} \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ and $\eta_j \in \mathbb{N}$ be such that

$$(5.1) \qquad F_j \left(-\frac{\partial P_s/\partial \Lambda_{n-s+1,1}}{\partial P_s/\partial Z_{n-s+1}}, \ldots, -\frac{\partial P_s/\partial \Lambda_{n-s+1,n}}{\partial P_s/\partial Z_{n-s+1}} \right) = \frac{F_{\Lambda,j}}{(\partial P_s/\partial Z_{n-s+1})^{\eta_j}}$$

for $1 \le j \le s$. Also let

$$H_i := \frac{\partial P_s}{\partial Z_{n-s+1}} Z_i + \sum_{j=1}^{n} \Lambda_{ij} \frac{\partial P_s}{\partial \Lambda_{n-s+1,j}}.$$

for $1 \le i \le n-s+1$. Lemma 4.8 shows that $F_{\Lambda,j}$ $(1 \le j \le s)$ and H_i $(1 \le i \le n-s+1)$ are multiples of P_s in $\mathbb{Q}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Further, since P_s is a primitive polynomial, we conclude that they are multiples of P_s in $\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$, and thus that $F_{\Lambda,j,p}$ $(1 \le j \le s)$ and $H_{i,p}$ $(1 \le i \le n-s+1)$ are multiples of $P_{s,p}$. As $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$ by construction, we see that $F_{\Lambda,j,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$ and $H_{i,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$ for $1 \le k \le \delta_s$, and reducing (5.1) modulo p we deduce that $F_{j,p}(\boldsymbol{x}^k) = 0$ for $1 \le k \le \delta_s$. Then following the proof of Proposition 4.9 *mutatis mutandis* we conclude that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ are pairwise distinct points of $\pi_{s,p}^{-1}(\boldsymbol{q})$. $\square$

By definition, $P_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X}) \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{X}]$ vanishes on the set of common zeros $\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s$ of $F_1, \ldots, F_s$ in $\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^n$. By the Nullstellensatz, there exist $\alpha_s \in \mathbb{Z} \setminus \{0\}$ and $\mu_s \in \mathbb{N}$ such that

$$(5.2) \qquad\qquad \alpha_s P_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})^{\mu_s} \in (F_1, \ldots, F_s)\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{X}].$$

Our next result provides a condition which implies that the modular reduction preserves dimension and a Noether normalization.

Proposition 5.2. *Let p be a prime number such that $\alpha_{s,p} A_{s,p}(\boldsymbol{\lambda}_p^*)\rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s})$ is nonzero. Let $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \le i \le n-s$. Then:*
  (1) *$F_{1,p}, \ldots, F_{s,p}$ generate an unmixed ideal in $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ of dimension $n-s$;*
  (2) *the mapping $\pi_{s,p}: \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism.*

Proof. Recall that A_s is homogeneous of degree δ_s in the $(n-s) \times (n-s)$–minors of $\boldsymbol{\Lambda}^*$. Since $p \nmid A_s(\boldsymbol{\lambda}^*)$, at least one of the $(n-s) \times (n-s)$–minors of $\boldsymbol{\lambda}^*$ is nonzero modulo p. We deduce that the linear forms $Y_{1,p}, \ldots, Y_{n-s,p}$ are linearly independent, and there exist linear forms $Y_{n-s+1}, \ldots, Y_n \in \mathbb{Z}[\boldsymbol{X}]$ such that $Y_{1,p}, \ldots, Y_{n,p}$ are linearly independent in $\mathbb{F}_p[\boldsymbol{X}]$. Let $\boldsymbol{w}_k \in \mathbb{Z}^n$ be such that $Y_{n-s+k} = \boldsymbol{w}_k \cdot \boldsymbol{X}$ for $1 \le k \le s$ and

$$Q_k := P_s(\boldsymbol{\lambda}^*, \boldsymbol{w}_k, Y_1, \ldots, Y_{n-s}, Y_{n-s+k}) \in \mathbb{Z}[Z_1, \ldots, Z_{n-s+1}].$$

From (5.2) we see that $\alpha_s Q_k(Y_1, \ldots, Y_{n-s}, Y_{n-s+k})^{\mu_s} \in (F_1, \ldots, F_s)\mathbb{Z}[\boldsymbol{X}]$ for $1 \le k \le s$, and reducing modulo p we obtain

$$(5.3) \qquad\qquad \alpha_{s,p}Q_{k,p}(Y_{1,p}, \ldots, Y_{n-s,p}, Y_{n-s+k,p})^{\mu_s} \in (F_{1,p} \ldots, F_{s,p})\mathbb{F}_p[\boldsymbol{X}]$$

for $1 \le k \le s$. Observe that $\deg_{Z_{n-s+1}} Q_k = \delta_s$ and $A_s(\boldsymbol{\lambda}^*)$ is the coefficient of $Z_{n-s+1}^{\delta_s}$ in Q_k. Since $p \nmid \alpha_s A_s(\boldsymbol{\lambda}^*)$, identity (5.3) may be interpreted as an integral dependence relation for $Y_{n-s+k,p}$ over $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}]$ modulo $(F_{1,p} \ldots, F_{s,p})$. Further, since $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n,p}] = \overline{\mathbb{F}}_p[\boldsymbol{X}]$, we conclude that $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}] \to \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$ is an integral ring extension. In particular, we have $\dim \mathcal{V}_{s,p} \le n - s$. Moreover, since $A_{s,p}(\boldsymbol{\lambda}_p^*) \rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s}) \ne 0$, by Lemma 5.1 the variety $\mathcal{V}_{s,p} = V(F_{1,p}, \ldots, F_{s,p})$ is nonempty. Therefore, $(F_{1,p}, \ldots, F_{s,p})$ is a proper ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ of dimension at most $n - s$, while the Principal Ideal theorem (see, e.g., [10, Theorem 10.2]) implies $\dim(F_{1,p}, \ldots, F_{s,p}) \ge n - s$. We conclude that $\dim(F_{1,p}, \ldots, F_{s,p}) = n - s$, and the unmixedness theorem proves that $(F_{1,p}, \ldots, F_{s,p})$ is unmixed. This shows the first assertion. Since the ring extension $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}] \to \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$ is integral and $\dim \mathcal{V}_{s,p} = n - s$, it follows that $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s}$ is a finite morphism, which finishes the proof. $\qquad \square$

Next we show that the hypotheses of Proposition 5.2 also guarantee that the degree is preserved under modular reduction, and the modular Chow form is obtained reducing modulo p that of $\mathcal{V}_s$.

Corollary 5.3. *With notations and hypotheses as in Proposition 5.2, $\deg \mathcal{V}_{s,p} = \delta_s$ and $P_{s,p}$ is a Chow form of $\mathcal{V}_{s,p}$.*

Proof. Since $p \nmid \alpha_s$, from (5.2) we deduce that $P_{s,p}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})^{\mu_s} \in (F_{1,p}, \ldots, F_{s,p}) \mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{X}]$. It follows that $P_{s,p}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})$ vanishes on $\mathbb{A}_{\overline{\mathbb{F}}_p}^{(n-s+1)n} \times \mathcal{V}_{s,p}$. As a consequence, if $Q_s \in \mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ is a Chow form of $\mathcal{V}_{s,p}$, then Q_s divides $P_{s,p}$ in $\mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Since $P_{s,p}$ is nonzero, because P_s is primitive, we conclude that

$$\deg \mathcal{V}_{s,p} = \deg_{Z_{n-s+1}} Q_s \le \deg_{Z_{n-s+1}} P_{s,p} \le \delta_s.$$

On the other hand, Proposition 5.2 shows that $\pi_{s,p}$ is a finite morphism, and the (finite) fiber $\pi_{s,p}^{-1}(\boldsymbol{p}_p)$ satisfies $\#\pi_{s,p}^{-1}(\boldsymbol{p}_p) \ge \delta_s$ by Lemma 5.1. The Bézout inequality (2.1) implies

$$\#\pi_{s,p}^{-1}(\boldsymbol{p}_p) = \deg\big(\mathcal{V}_{s,p} \cap \{Y_{1,p} - p_{1,p} = 0, \ldots, Y_{n-s,p} - p_{n-s} = 0\}\big) \le \deg \mathcal{V}_{s,p}.$$

This proves that $\deg \mathcal{V}_{s,p} = \delta_s$. Since Q_s is homogeneous of degree δ_s and $P_{s,p}$ has degree at most δ_s in each set of variables $(Z_i, \Lambda_{i1}, \ldots, \Lambda_{in})$ for $1 \le i \le n - s + 1$, we deduce that $P_{s,p} = \epsilon Q_s$ for some $\epsilon \in \mathbb{F}_p \setminus \{0\}$, showing thus that $P_{s,p}$ is a Chow form of $\mathcal{V}_{s,p}$. $\qquad \square$

Finally, we obtain a condition which implies that the modular reduction preserves generic smoothness. Let $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{Z}^{n-s}$ be such that $A_s(\boldsymbol{\lambda}^*) \rho_s(\boldsymbol{\lambda}, \boldsymbol{p}) \ne 0$. From Theorem 4.10 it follows that $\boldsymbol{p}$ is a lifting point of the mapping $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ defined by $Y_1, \ldots, Y_{n-s}$. Then $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ and the Jacobian determinant J_s of $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ with respect to $X_1, \ldots, X_n$ do not have common zeros in $\mathbb{A}^n$. By the Nullstellensatz, there exist $\gamma_s \in \mathbb{Z} \setminus \{0\}$ and $G_1, \ldots, G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ such that

$$(5.4) \quad \gamma_s = G_1 F_1 + \cdots + G_s F_s + G_{s+1}(Y_1 - p_1) + \cdots + G_n(Y_{n-s} - p_{n-s}) + G_{n+1} J_s.$$

The nonvanishing of γ_s modulo p provides the additional condition we are looking for.

Lemma 5.4. *With the previous hypotheses and notations, let p be a prime number such that $p \nmid \alpha_s \gamma_s A_s(\boldsymbol{\lambda}^*) \rho_s(\boldsymbol{\lambda}, \boldsymbol{p})$. Then $F_{1,p}, \ldots, F_{s,p}$ generate a radical ideal in $\overline{\mathbb{F}}_p[\boldsymbol{X}]$.*

Proof. Since by hypothesis $\alpha_{s,p}A_{s,p}(\boldsymbol{\lambda}_p^*)\rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s})$ is nonzero, from Proposition 5.2 it follows that $\mathcal{V}_{s,p}$ is equidimensional of dimension $n - s$ and the mapping $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism. On the other hand, reducing (5.4) modulo p we see that

$$\gamma_{s,p} = G_{1,p}F_{1,p} + \cdots + G_{s,p}F_{s,p} + G_{s+1,p}(Y_{1,p} - p_{1,p}) + \cdots + G_{n,p}(Y_{n-s,p} - p_{n-s,p}) + G_{n+1,p}J_{s,p}$$

holds in $\mathbb{F}_p[\boldsymbol{X}]$. We deduce that $J_{s,p}(\boldsymbol{x}) \neq 0$ for any $\boldsymbol{x} \in \pi_{s,p}^{-1}(\boldsymbol{p})$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_h$ be the irreducible components of $\mathcal{V}_{s,p}$ and let $\pi_{\mathcal{C}_i}$ denote the restriction of $\pi_{s,p}$ to $\mathcal{C}_i$ for $1 \leq i \leq h$. Since $\mathcal{V}_{s,p}$ is equidimensional, $\pi_{\mathcal{C}_i}$ is a finite morphism. In particular, $\pi_{\mathcal{C}_i}$ is surjective and $\mathcal{C}_i \cap \pi_{s,p}^{-1}(\boldsymbol{p}_p) \neq \emptyset$ for $1 \leq i \leq h$. It follows that $J_{s,p}$ does not vanish identically on $\mathcal{C}_i$, which implies that there exists an $(s \times s)$–minor $M_i \in \mathbb{F}_p[\boldsymbol{X}]$ of the Jacobian matrix $(\partial F_{i,p}/\partial X_j)_{1 \leq i \leq s, 1 \leq j \leq n}$ not vanishing identically on $\mathcal{C}_i$ for $1 \leq i \leq h$. Let $\mathcal{J} \subseteq \overline{\mathbb{F}}_p[\boldsymbol{X}]$ be the ideal generated by $F_{1,p}, \ldots, F_{s,p}$ and the $(s \times s)$–minors of the Jacobian matrix $(\partial F_{i,p}/\partial X_j)_{1 \leq i \leq s, 1 \leq j \leq n}$. If $\mathcal{P}_i \subseteq \overline{\mathbb{F}}_p[\boldsymbol{X}]$ is the vanishing ideal of $\mathcal{C}_i$ for $1 \leq i \leq h$, then $\mathcal{P}_1, \ldots, \mathcal{P}_h$ are the minimal prime ideals of $(F_{1,p}, \ldots, F_{s,p})$. Since $M_i \notin \mathcal{P}_i$, we have $\mathcal{J} \nsubseteq \mathcal{P}_i$ for $1 \leq i \leq h$, and Lemma 2.1 proves that the ideal $(F_{1,p}, \ldots, F_{s,p})$ is radical. $\square$

We summarize all the previous results in the following theorem.

Theorem 5.5. *Let $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ and $\boldsymbol{p} \in \mathbb{Z}^{n-s}$ be such that $A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$ and p a prime number such that $p \nmid \alpha_s\gamma_sA_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})$, where α_s and γ_s are the integers of (5.2) and (5.4) respectively. Let $Y_{i,p} := \boldsymbol{\lambda}_{i,p} \cdot \boldsymbol{X}$ for $1 \leq i \leq n - s + 1$ and $R_{s,p} := \overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}]$. Then the following conditions hold:*

- *$F_{1,p}, \ldots, F_{s,p}$ generate a radical ideal in $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ and define an equidimensional variety $\mathcal{V}_{s,p} \subset \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s}$ of dimension $n - s$ and degree δ_s;*
- *the mapping $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism and $Y_{n-s+1,p}$ induces a primitive element of the ring extension $R_{s,p} \hookrightarrow \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$;*
- *$\mathrm{rank}_{R_{s,p}}\overline{\mathbb{F}}_p[\mathcal{V}_{s,p}] = \delta_s$;*
- *any $\boldsymbol{q} \in \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s}$ with $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{q})$.*

Proof. The first assertion follows by Proposition 5.2, Corollary 5.3 and Lemma 5.4. Since $P_{s,p}$ is a Chow form of $\mathcal{V}_{s,p}$ by Corollary 5.3, the last three assertions are a consequence of Theorem 4.10 applied to $\mathbb{K} = \overline{\mathbb{F}}_p$. $\square$

5.2. Lifting fibers not meeting a discriminant.

Throughout this section we assume that $s \leq r - 1$. Our main algorithm is recursive, and in its sth step computes a geometric solution of the fiber $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$ from one of the lifting curve $W_{\boldsymbol{p}^*}$. As the geometric solution of $W_{\boldsymbol{p}^*}$ constitutes a "good" representation of $W_{\boldsymbol{p}^*}$ outside the discriminant locus $\{\rho_s(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}) = 0\}$, it is critical that $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$ does not intersect this hypersurface. In this section we show that for a generic choice of the coordinates of $\boldsymbol{\lambda}$ and $\boldsymbol{p}$ this condition is satisfied and discuss when this is preserved under modular reduction.

For this purpose, we use the following terminology: for two subvarieties $\mathcal{V}$ and $\mathcal{W}$ of $\mathbb{A}^n$, we say that $\mathcal{W}$ cuts $\mathcal{V}$ *properly* if $\mathcal{W}$ does not contain any irreducible $\overline{\mathbb{Q}}$–component of $\mathcal{V}$. We have the following result.

Lemma 5.6. *There exists a polynomial* $\mathsf{R}_s \in \overline{\mathbb{Q}}[\mathbf{\Lambda}] \setminus \{0\}$ *of degree at most* $2(n - s + 2)\delta_s^2 \delta_{s+1}$ *with the following property: for every* $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$ *with* $\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$, *the hypersurface* $\{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\} \subset \mathbb{A}^n$ *cuts* $\mathcal{V}_{s+1}$ *properly.*

Proof. Let $\mathcal{C}_1, \ldots, \mathcal{C}_h$ be the irreducible $\overline{\mathbb{Q}}$–components of $\mathcal{V}_{s+1}$, and let $\boldsymbol{z}_i \in \mathcal{C}_i$ be a nonsingular point of $\mathcal{V}_{s+1}$ for $1 \leq i \leq h$. Define

$$\mathsf{R}_s := \prod_{i=1}^{h} \rho_s(\mathbf{\Lambda}, \mathbf{\Lambda}^* \boldsymbol{z}_i).$$

We claim that R_s satisfies the conditions of the lemma. Indeed, fix $1 \leq i \leq h$. Since $\boldsymbol{z}_i$ is a nonsingular point of $\mathcal{V}_{s+1}$ and $\mathcal{I}(\mathcal{V}_{s+1}) = \mathcal{I}(\mathcal{V}_s) + (F_{s+1})$, then $\boldsymbol{z}_i$ is also a nonsingular point of $\mathcal{V}_s$. Hence, for a generic choice of $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$, denoting by $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ the mapping $\pi_s(\boldsymbol{x}) := \boldsymbol{\lambda}^* \boldsymbol{x}$ and $\boldsymbol{p} := \pi_s(\boldsymbol{z}_i)$, the following conditions are satisfied:

- $\#\pi_s^{-1}(\boldsymbol{p}) = \delta_s$;
- the linear form $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{X}$ separates the points of $\pi_s^{-1}(\boldsymbol{p})$;
- the discriminant of the polynomial $P_s(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ is $\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})$.

Indeed, since $\boldsymbol{z}_i$ is a nonsingular point of $\mathcal{V}_s$, then $\mathcal{V}_s$ has multiplicity 1 at $\boldsymbol{z}_i$ (see, e.g., [37, §5A, Corollary 5.15]). This means that a generic linear space of dimension s passing through $\boldsymbol{z}_i$ meets $\mathcal{V}_s$ in exactly $\delta_s - 1$ points different from $\boldsymbol{z}_i$, which shows the first condition. The remaining conditions are clearly satisfied.

Let $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ be the δ_s points of $\pi_s^{-1}(\boldsymbol{p})$. Since $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{X}$ separates these points, the polynomial $P_s(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ has δ_s different roots, namely $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{x}^i$ for $1 \leq i \leq \delta_s$. We conclude that $\rho_s(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. It follows that $\rho_s(\mathbf{\Lambda}, \mathbf{\Lambda}^* \boldsymbol{z}_i)$ is a nonzero polynomial in $\overline{\mathbb{Q}}[\mathbf{\Lambda}]$ for $1 \leq i \leq h$ and therefore $\mathsf{R}_s \in \overline{\mathbb{Q}}[\mathbf{\Lambda}] \setminus \{0\}$. Since $\deg \rho_s(\mathbf{\Lambda}, \mathbf{\Lambda}^* \boldsymbol{z}_i) \leq (n-s+2)(2\delta_s-1)\delta_s$ and $h \leq \delta_{s+1}$, the estimate for the degree R_s follows. Finally, let $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$ be such that $\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$. Then $\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{z}_i) \neq 0$ for $1 \leq i \leq h$, which shows that $\mathcal{C}_i$ is not contained in the hypersurface $\{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\}$ of $\mathbb{A}^n$ for $1 \leq i \leq h$. $\qquad\square$

Let $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n} \setminus \{0\}$ be such that $\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$ and let $\mathcal{W}_{\boldsymbol{\lambda}^s} \subset \mathbb{A}^n$ be the variety

$$(5.5) \qquad\qquad \mathcal{W}_{\boldsymbol{\lambda}^s} := \mathcal{V}_{s+1} \cap \{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\}.$$

By Lemma 5.6, $\mathcal{W}_{\boldsymbol{\lambda}^s}$ is either empty or equidimensional of dimension $n - s - 2$.

Assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$ and let $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) \in \mathbb{Z}[\boldsymbol{X}]$. By the Nullstellensatz there exists $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ satisfying

$$(5.6) \qquad\qquad \mu_{\boldsymbol{\lambda}^s} \in (F_1, \ldots, F_{s+1}, \rho_{\boldsymbol{\lambda}^s})\mathbb{Z}[\boldsymbol{X}].$$

On the other hand, assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$ and let $Y_j := \boldsymbol{\lambda}_j \cdot \boldsymbol{X}$ for $1 \leq j \leq n - s - 1$. By [26, Theorem 3.3] (see also [6, Theorem 3.1]) there exists a nonzero polynomial $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s-1}]$ with $\deg B_{\boldsymbol{\lambda}^s} \leq \deg \mathcal{W}_{\boldsymbol{\lambda}^s}$ such that

$$(5.7) \qquad\qquad B_{\boldsymbol{\lambda}^s}\big(Y_1(\boldsymbol{x}), \ldots, Y_{n-s-1}(\boldsymbol{x})\big) = 0$$

for every $\boldsymbol{x} \in \mathcal{W}_{\boldsymbol{\lambda}^s}$. Since $\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \leq \deg \mathcal{V}_{s+1} \deg \rho_{\boldsymbol{\lambda}^s}$, we have

$$(5.8) \qquad\qquad \deg B_{\boldsymbol{\lambda}^s} \leq 2(n-s+2)\delta_s^2 \delta_{s+1}.$$

As $B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})$ vanishes on the variety $\mathcal{W}_{\boldsymbol{\lambda}^s} \subset \mathbb{A}^n$ defined by $F_1, \ldots, F_{s+1}$ and $\rho_{\boldsymbol{\lambda}^s}$, by the Nullstellensatz there exist $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ and $\ell_{\boldsymbol{\lambda}^s} \in \mathbb{N}$ such that

$$(5.9) \qquad \beta_{\boldsymbol{\lambda}^s} B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})^{\ell_{\boldsymbol{\lambda}^s}} \in (F_1, \ldots, F_{s+1}, \rho_{\boldsymbol{\lambda}^s})\mathbb{Z}[\boldsymbol{X}].$$

Now we are able to establish our condition for a good modular reduction at the sth step. Let $\mathsf{M}_s \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}] \setminus \{0\}$ be the polynomial defined by

$$(5.10) \qquad \mathsf{M}_s := \alpha_s \gamma_s A_s(\boldsymbol{\Lambda}^*)\rho_s(\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}),$$

where α_s and γ_s are the integers of (5.2) and (5.4) respectively. Observe that

$$(5.11) \qquad \deg \mathsf{M}_s \leq 2(n - s + 2)\delta_s^2.$$

Further, let $\mathsf{C}_s \in \mathbb{Z}[\boldsymbol{\Lambda}]$ be a nonzero coefficient of $\mathsf{M}_s\mathsf{M}_{s+1} \in \mathbb{Z}[\boldsymbol{\Lambda}][Z_1, \ldots, Z_{n-s}]$. For $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n} \setminus \{0\}$ with $\mathsf{C}_s(\boldsymbol{\lambda})\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$, define $\mathsf{L}_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s}] \setminus \{0\}$ as

$$(5.12) \qquad \mathsf{L}_{\boldsymbol{\lambda}^s} := \begin{cases} \mu_{\boldsymbol{\lambda}^s} & \text{if } \mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset, \\ \beta_{\boldsymbol{\lambda}^s} B_{\boldsymbol{\lambda}^s} & \text{if } \mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset, \end{cases}$$

where $\mu_{\boldsymbol{\lambda}^s}$, $B_{\boldsymbol{\lambda}^s}$ and $\beta_{\boldsymbol{\lambda}^s}$ are defined as in (5.6), (5.9) and (5.7). Finally, define

$$\mathsf{N}_{\boldsymbol{\lambda}^s} := \mathsf{M}_s(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s})\mathsf{M}_{s+1}(\boldsymbol{\lambda}^*, Z_1, \ldots, Z_{n-s-1})\mathsf{L}_{\boldsymbol{\lambda}^s}(Z_1, \ldots, Z_{n-s-1}).$$

Theorem 5.7. *Let $1 \leq s \leq r - 1$. Let $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ and $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{Z}^{n-s}$ be such that $\mathsf{C}_s(\boldsymbol{\lambda})\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$ and $\mathsf{N}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}) \neq 0$, and let p be a prime number with $p \nmid \mathsf{N}_{\boldsymbol{\lambda}^s}(\boldsymbol{p})$. If $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n - s + 1$, then the following conditions are satisfied:*

(1) *$F_{1,p}, \ldots, F_{s,p}$ generate a radical ideal in $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ and define an equidimensional variety $\mathcal{V}_{s,p} \subset \mathbb{A}_{\overline{\mathbb{F}}_p}^n$ of dimension $n - s$ and degree δ_s. The same holds for $F_{1,p}, \ldots, F_{s+1,p}$ and $\mathcal{V}_{s+1,p}$;*

(2) *the mapping $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism, $\boldsymbol{p}_p \in \mathbb{F}_p^{n-s}$ is a lifting point of $\pi_{s,p}$, and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{p}_p)$;*

(3) *the mapping $\pi_{s+1,p} : \mathcal{V}_{s+1,p} \to \mathbb{A}_{\overline{\mathbb{F}}_p}^{n-s-1}$ defined by $Y_{1,p}, \ldots, Y_{n-s-1,p}$ is a finite morphism. Furthermore, if $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$, then $\boldsymbol{p}_p^*$ is a lifting point of $\pi_{s+1,p}$ and $Y_{n-s,p}$ induces a primitive element of $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$;*

(4) *any $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big)$ satisfies $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$. In particular, any such $\boldsymbol{q}$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{q})$.*

Proof. Since $p \nmid \mathsf{M}_s(\boldsymbol{\lambda}, \boldsymbol{p})\mathsf{M}_{s+1}(\boldsymbol{\lambda}^*, \boldsymbol{p}^*)$, the first three assertions follow by Theorem 5.5.

To prove the last assertion, let $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big)$. Then there exists $\boldsymbol{x} \in \pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$ such that $\boldsymbol{q} = \big(\boldsymbol{p}_p^*, Y_{n-s,p}(\boldsymbol{x})\big)$. Suppose that the variety $\mathcal{W}_{\boldsymbol{\lambda}^s}$ of (5.5) is empty. Considering (5.6) modulo p, and taking into account that $p \nmid \mu_{\boldsymbol{\lambda}^s}$, we deduce that $F_{1,p}, \ldots, F_{s+1,p}$ and $\rho_{\boldsymbol{\lambda}^s,p}$ generate the unit ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$. As $\boldsymbol{x} \in \mathcal{V}_{s+1,p}$, it follows that $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \rho_{\boldsymbol{\lambda}^s,p}(\boldsymbol{x}) \neq 0$. Since $p \nmid \mathsf{M}_s(\boldsymbol{\lambda}, \boldsymbol{p})$, by Theorem 5.5 we conclude that $\boldsymbol{q}$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{q})$. On the other hand, if $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$, then considering (5.9) modulo p and taking into account that $p \nmid \beta_{\boldsymbol{\lambda}^s}$ we see that

$$B_{\boldsymbol{\lambda}^s,p}(Y_{1,p}, \ldots, Y_{n-s-1,p})^{\ell_{\boldsymbol{\lambda}^s}} \in (F_{1,p}, \ldots, F_{s+1,p}, \rho_{\boldsymbol{\lambda}^s,p})\overline{\mathbb{F}}_p[\boldsymbol{X}].$$

This implies that $B_{\boldsymbol{\lambda}^s,p}$ vanishes on $\mathcal{V}_{s+1,p} \cap \{\rho_{\boldsymbol{\lambda}^s,p} = 0\}$. Further, the fact that $p \nmid B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^*)$ implies $B_{\boldsymbol{\lambda}^s,p}(\boldsymbol{x}) = B_{\boldsymbol{\lambda}^s,p}(\boldsymbol{p}_p^*) \neq 0$, and then $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \rho_{\boldsymbol{\lambda}^s,p}(\boldsymbol{x}) \neq 0$. Arguing as before we deduce that $\boldsymbol{q}$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{q})$. $\qquad\square$

Remark 5.8. *With hypotheses as in Theorem 5.7, let $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*) = \{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_{s+1}}\}$. Since $Y_{n-s,p}$ induces a primitive element of $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$, it separates $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_{s+1}}$. Therefore, if $q \in \overline{\mathbb{F}}_p[T]$ is the minimal polynomial of $Y_{n-s,p}$ over $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$, then its roots in $\overline{\mathbb{F}}_p$ are $Y_{n-s,p}(\boldsymbol{x}^1), \ldots, Y_{n-s,p}(\boldsymbol{x}^{\delta_{s+1}})$. Since*

$$\pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big) = \Big\{ \big(\boldsymbol{p}_p^*, Y_{n-s,p}(\boldsymbol{x}^1)\big), \ldots, \big(\boldsymbol{p}_p^*, Y_{n-s,p}(\boldsymbol{x}^{\delta_{s+1}})\big) \Big\},$$

we can rephrase item (4) of Theorem 5.7 in the following way: $\rho_{s,p}\big(\boldsymbol{\lambda}_p, (\boldsymbol{p}_p^*, a)\big) \neq 0$ for every root $a \in \overline{\mathbb{F}}_p$ of q. Thus, $(\boldsymbol{p}_p^*, a)$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{p}_p^*, a)$.

5.3. Simultaneous Noether normalization and lifting fibers.
From now on, let $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \le i \le n, 1 \le j \le n}$ denote a set of n^2 indeterminates over $\mathbb{Q}$. For $1 \le s \le r$, we write $\boldsymbol{\Lambda}^s := (\Lambda_{ij})_{1 \le i \le n, 1 \le j \le n-s+1}$. Further, for $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \le i \le n, 1 \le j \le n} \in \mathbb{Z}^{n^2}$, we denote $\boldsymbol{\lambda}^s := (\lambda_{ij})_{1 \le i \le n-s+1, 1 \le j \le n}$. Let $\mathsf{R} \in \overline{\mathbb{Q}}[\boldsymbol{\Lambda}] \setminus \{0\}$ be the polynomial defined by

$$(5.13) \qquad\qquad \mathsf{R} := \prod_{s=1}^{r-1} \mathsf{C}_s \mathsf{R}_s.$$

Since $\deg \mathsf{C}_s \le \deg \mathsf{M}_s + \deg \mathsf{M}_{s+1}$, taking into account (5.11) and the estimate for the degree of R_s of Lemma 5.6, we easily deduce that

$$(5.14) \qquad\qquad \deg \mathsf{R} \le D := (2n - r + 4)r(\delta^3 + 2\delta^2).$$

Let $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ be such that $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ and define $\mathsf{N}_{\boldsymbol{\lambda}} \in \mathbb{Z}[Z_1, \ldots, Z_{n-1}] \setminus \{0\}$ as

$$(5.15) \qquad \mathsf{N}_{\boldsymbol{\lambda}} := \mathsf{M}_r(\boldsymbol{\lambda}^r, Z_1, \ldots, Z_{n-r}) \prod_{s=1}^{r-1} \mathsf{M}_s(\boldsymbol{\lambda}^s, Z_1, \ldots, Z_{n-s}) \mathsf{L}_{\boldsymbol{\lambda}^s}(Z_1, \ldots, Z_{n-s-1}).$$

Observe that

$$\deg \mathsf{N}_{\boldsymbol{\lambda}} \le \sum_{s=1}^{r} \deg \mathsf{M}_s + \sum_{s=1}^{r} \deg \mathsf{L}_{\boldsymbol{\lambda}^s} \le 2(\delta^3 + \delta^2) \sum_{s=1}^{r-1}(n - s + 2) + 2(n - r + 2)\delta^2 \le D.$$

Let $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathbb{Z}^{n-1}$ be such that $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$ and denote $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ for $1 \le s \le r$. With hypotheses as above we easily obtain the following result.

Theorem 5.9. *Let $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ and $\boldsymbol{p} \in \mathbb{Z}^{n-1}$ be such that $\det(\boldsymbol{\lambda})\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ and $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$. Let $\mathfrak{N} := \det(\boldsymbol{\lambda})\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p})$ and $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \le i \le n$. If p is a prime number such that $p \nmid \mathfrak{N}$, then $Y_{1,p}, \ldots, Y_{n,p}$ define a new set of variables for $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ and conditions (1)–(4) of Theorem 5.7 are satisfied for $1 \le s \le r - 1$ with $\boldsymbol{p} := \boldsymbol{p}^s$ and $\boldsymbol{p}^* := \boldsymbol{p}^{s+1}$. In particular, $F_{1,p}, \ldots, F_{r,p}$ define a reduced regular sequence in $\overline{\mathbb{F}}_p[\boldsymbol{X}]$.*

In the sequel, a prime p as in Theorem 5.9 will be called "lucky" and a reduction modulo such a prime p is called "good".

We end this section by discussing Kronecker representations for a good modular reduction. Given $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i,j \leq n} \in \mathbb{Z}^{n^2}$ and $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathbb{Z}^{n-1}$ satisfying the hypotheses of Theorem 5.9, define $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n$, and let $R_s := \mathbb{Q}[Y_1, \ldots, Y_{n-s}]$ and $B_s := \mathbb{Q}[\mathcal{V}_s]$ for $1 \leq s \leq r$. Since $A_s(\boldsymbol{\lambda}^{s+1})\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s) \neq 0$ for $1 \leq s \leq r$, by Theorem 4.10 the following conditions are satisfied:

- $Y_1, \ldots, Y_{n-s}$ are in Noether position with respecto to $\mathcal{I}_s$;
- $\boldsymbol{p}^s$ is a lifting point of the finite morphism $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ defined by $Y_1, \ldots, Y_{n-s}$;
- B_s is a free R_s–module of rank equal to δ_s.

Let $\mathcal{I}_s := (F_1, \ldots, F_s)$ and $\mathcal{J}_s := \mathcal{I}_s + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s})$ for $1 \leq s \leq r$ and $\mathcal{K}_s := \mathcal{I}_s + (Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1})$ for $1 \leq s \leq r - 1$. According to Lemma 4.2, $\mathcal{J}_s$ and $\mathcal{K}_s$ are the vanishing ideals of the lifting fiber $\mathcal{V}_{\boldsymbol{p}^s}$ and the lifting curve $\mathcal{W}_{\boldsymbol{p}^s}$ respectively. Further, identifying $\mathcal{I}_s$ with its image in $\mathbb{Q}[Y_{n-s+1}, \ldots, Y_n]$ and $\mathcal{K}_s$ with its image in $\mathbb{Q}[Y_{n-s}, \ldots, Y_n]$ as in Lemma 4.3, the following conditions hold for $1 \leq s \leq r$:

- $\mathbb{Q}[Y_{n-s+1}, \ldots, Y_n]/\mathcal{J}_s$ is a $\mathbb{Q}$–vector space of dimension δ_s;
- $Y_{n-s}, \ldots, Y_n$ are in Noether position with respect to $\mathcal{K}_s$;
- $\mathbb{Q}[Y_{n-s}, \ldots, Y_n]/\mathcal{K}_s$ is a free $\mathbb{Q}[Y_{n-s}]$–module of rank equal to $\mathrm{rank}_{R_s}\mathbb{Q}[\mathcal{V}_s]$.

We can obtain Kronecker representations of $\mathcal{I}_s$, $\mathcal{J}_s$, and $\mathcal{K}_s$ as in Section 4.3, namely let T be a new indeterminate and define $Q^s, W^s_{n-s+2}, \ldots, W^s_n \in R_s[T]$ by
(5.16)
$$Q^s := \frac{P_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T)}{A_s(\boldsymbol{\lambda}^{s+1})}, \quad W^s_j := -\sum_{k=1}^n \frac{\lambda_{jk}}{A_s(\boldsymbol{\lambda}^{s+1})} \frac{\partial P_s}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T)$$

for $n - s + 2 \leq j \leq n$, where $P_s \in \mathbb{Z}[\boldsymbol{\Lambda}^s, Z_1, \ldots, Z_{n-s+1}]$ is a primitive Chow form of $\mathcal{V}_s$. Propositions 4.11, 4.13 and 4.14 then read as follows.

Proposition 5.10. *The following assertions hold:*

- *the polynomials $Q^s, W^s_{n-s+2}, \ldots, W^s_n$ form the Kronecker representation of $\mathcal{I}_s$ with primitive element Y_{n-s+1};*
- *the polynomials $Q^s(\boldsymbol{p}^s, T), W^s_{n-s+2}(\boldsymbol{p}^s, T), \ldots, W^s_n(\boldsymbol{p}^s, T)$ form the Kronecker representation of $\mathcal{J}_s$ with primitive element Y_{n-s+1};*
- *the polynomials $Q^s(\boldsymbol{p}^{s+1}, Y_{n-s}, T), W^s_{n-s+2}(\boldsymbol{p}^{s+1}, Y_{n-s}, T), \ldots, W^s_n(\boldsymbol{p}^{s+1}, Y_{n-s}, T)$ form the Kronecker representation of $\mathcal{K}_s$ with primitive element Y_{n-s+1}.*

Now let p be a prime number as in Theorem 5.9. Let $\mathcal{I}_{s,p}$, $\mathcal{J}_{s,p}$ and $\mathcal{K}_{s,p}$ be the ideals of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ defined by $\mathcal{I}_{s,p} := (F_{1,p}, \ldots, F_{s,p})$ and $\mathcal{J}_{s,p} := \mathcal{I}_{s,p} + (Y_{1,p} - p_{1,p}, \ldots, Y_{n-s,p} - p_{n-s,p})$ for $1 \leq s \leq r$, and $\mathcal{K}_{s,p} := \mathcal{I}_{s,p} + (Y_{1,p} - p_{1,p}, \ldots, Y_{n-s-1,p} - p_{n-s-1,p})$ for $1 \leq s \leq r - 1$. By Theorem 5.9 the following conditions are satisfied for $1 \leq s \leq r$:

- $\mathcal{I}_{s,p}$ is a radical, equidimensional ideal of dimension $n - s$;
- the variables $Y_{1,p}, \ldots, Y_{n,p}$ are in Noether position with respect to $\mathcal{I}_{s,p}$;
- the mapping $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism and $\boldsymbol{p}_p$ is a lifting point of $\pi_{s,p}$;
- $P_{s,p}$ is a Chow form of $\mathcal{V}_{s,p}$.

It follows that $\mathcal{I}_{s,p}$, $\mathcal{J}_{s,p}$ and $\mathcal{K}_{s,p}$ are the defining ideals of the variety $\mathcal{V}_{s,p}$, the lifting fiber $\mathcal{V}_{\boldsymbol{p}_p^s}$ and the lifting curve $\mathcal{W}_{\boldsymbol{p}_p^{s+1}}$ respectively. Since $p \nmid A_s(\boldsymbol{\lambda}^{s+1})$, the polynomials $Q_p^s, W_{1,p}^s, \ldots, W_{n,p}^s \in \mathbb{F}_p[T]$ are well–defined, and we have the following result.

Proposition 5.11. *The following assertions hold:*
- $Q_p^s, W_{n-s+2,p}^s, \ldots, W_{n,p}^s$ *form the Kronecker representation of* $\mathcal{I}_{s,p}$ *with primitive element* $Y_{n-s+1,p}$;
- $Q_p^s(\boldsymbol{p}_p^s, T), W_{n-s+2,p}^s(\boldsymbol{p}_p^s, T), \ldots, W_{n,p}^s(\boldsymbol{p}_p^s, T)$ *form the Kronecker representation of* $\mathcal{J}_{s,p}$ *with primitive element* $Y_{n-s+1,p}$;
- $Q_p^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2,p}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_{n,p}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ *form the Kronecker representation of* $\mathcal{K}_{s,p}$ *with primitive element* $Y_{n-s+1,p}$.

Proof. From (5.16) we deduce that

$$Q_p^s = \frac{P_{s,p}\big(\boldsymbol{\lambda}_p^s, Y_{1,p}, \ldots, Y_{n-s,p}, T\big)}{A_{s,p}(\boldsymbol{\lambda}_p^{s+1})},$$

$$W_{j,p}^s = -\sum_{k=1}^{n} \frac{\lambda_{jk,p}}{A_{s,p}(\boldsymbol{\lambda}_p^{s+1})} \frac{\partial P_{s,p}}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}_p^s, Y_{1,p}, \ldots, Y_{n-s,p}, T) \quad (n-s+2 \le j \le n).$$

As $P_{s,p}$ is a Chow form of $\mathcal{V}_{s,p}$, the proposition follows taking into account the condition $p \nmid A_s(\boldsymbol{\lambda}^{s+1})\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$ and arguing as in Propositions 4.11, 4.13 and 4.14. $\qquad\square$

6. Computation of a Kronecker representation

Let $F_1, \ldots, F_r \in \mathbb{Z}[\boldsymbol{X}]$ be, as in Section 5, polynomials defining a reduced regular sequence. In this section we establish an upper bound on the bit complexity of computing a Kronecker representation of a zero–dimensional fiber $\pi_r^{-1}(\boldsymbol{p}^r)$ of $\mathcal{V}(F_1, \ldots, F_r)$. For this purpose, following the approach of [20], we perform this computation modulo a prime number p and apply p–adic lifting to recover the integers of a Kronecker representation of $\pi_r^{-1}(\boldsymbol{p}^r)$ over $\mathbb{Q}$. Assuming that a "lucky" prime p is given, the complexity of computing a Kronecker representation of a zero–dimensional fiber of $\mathcal{V}(F_{1,p}, \ldots, F_{r,p})$ was analyzed in [4]. On the other hand, the complexity of the p–adic lifting step was analyzed in [20]. Accordingly, in this section we analyze the cost of computing a "lucky" prime (Proposition 6.2), and then obtain an upper bound on the bit complexity of computing a Kronecker representation of $\pi_r^{-1}(\boldsymbol{p}^r)$ over $\mathbb{Q}$ (Theorem 6.8).

6.1. **Computation of a Kronecker representation modulo** p. Let $\mathsf{S} := \{0, \ldots, \mathsf{a}\}$ and $\mathsf{T} := \{0, \ldots, \mathsf{b}\}$, where $\mathsf{a} := \lfloor 8D \rfloor$ and $\mathsf{b} := \lfloor 9D \rfloor$. Assume that we have randomly chosen $(\boldsymbol{\lambda}, \boldsymbol{p}) \in \mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$ such that $\mathsf{R}(\boldsymbol{\lambda}) \ne 0$ and $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \ne 0$. The following result asserts that this can be done with a high probability of success.

Lemma 6.1. *Let* $(\boldsymbol{\lambda}, \boldsymbol{p})$ *be a point chosen uniformly at random in* $\mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$. *Then the probability that* $\mathsf{R}(\boldsymbol{\lambda}) \ne 0$ *and* $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \ne 0$ *is greater than* $\frac{7}{9}$.

Proof. Since $\deg \mathsf{R} \le D$, by Lemma 2.3 we see that for a random choice of $\boldsymbol{\lambda}$ in S^{n^2}, the probability that $\mathsf{R}(\boldsymbol{\lambda}) \ne 0$ is greater than $\frac{7}{8}$. Similarly, as $\deg(\mathsf{N}_{\boldsymbol{\lambda}}) \le D$, for a point $\boldsymbol{p}$ chosen uniformly at random in T^{n-1}, the conditional probability that $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \ne 0$, given that $\mathsf{R}(\boldsymbol{\lambda}) \ne 0$, is greater than $\frac{8}{9}$. This finishes the proof of the lemma. $\qquad\square$

For such a choice of $\boldsymbol{\lambda}$ and $\boldsymbol{p}$, let $\mathfrak{N}$ be the integer of Theorem 5.9. According to Theorem A.13, we have

$$(6.1) \qquad h(\mathfrak{N}) \leq \mathfrak{H} \quad \text{and} \quad \log \mathfrak{H} \in \mathcal{O}^{\sim}\big(\log(d^r n h)\big).$$

Now we can estimate the complexity of computing a "lucky" prime p of "low" bit length.

Proposition 6.2. *There is a probabilistic algorithm which takes $\mathfrak{H}$ as input and computes a prime p with $12\mathfrak{H} + 1 \leq p \leq 24\mathfrak{H}$ such that $p \nmid \mathfrak{N}$. The algorithm uses $\mathcal{O}^{\sim}\big(\log^2(d^r n h)\big)$ bit operations and returns a right result with probability at least $\frac{3}{4}$.*

Proof. The proposition follows applying Lemma 2.4 with $B = m\mathfrak{H}$, $M = \mathfrak{N}$, $m = 12$, and $k = 5 + \log\log(12\mathfrak{H})$, and taking into account (6.1). $\qquad\square$

Assume that we have computed a "lucky" prime p as in Proposition 6.2. Further, assume that we are given a straight–line program of length at most L which represents the polynomials $F_{1,p}, \dots, F_{r,p}$. Since the integer $\mathfrak{H}$ of (6.1) can certainly be chosen with $\mathfrak{H} \geq 5n^2 d\delta^4$, we can assume that $p > 60n^2 d\delta^4$. Thus we can apply the algorithm described in [4] to compute a Kronecker representation of the lifting fiber $V_{\boldsymbol{p}_p^r}$.

The algorithm starts computing the Kronecker representation of the fiber $V_{\boldsymbol{p}_p^1}$ of the hypersurface $\{F_{1,p} = 0\}$, with $Y_{n,p}$ as primitive element. With the notations of Proposition 5.11, such a Kronecker representation only consists of the minimal polynomial $Q^1\big(\boldsymbol{p}^1, T\big)$ of $Y_{n,p}$ modulo $\mathcal{J}_{1,p}$. Since, with notations as in Section 4, we have $\mathcal{J}_{1,p} = \big(F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p})\big)$, we see that $\overline{\mathbb{F}}_p[V_{\boldsymbol{p}_p^1}] = \overline{\mathbb{F}}_p[Y_{n,p}]/\big(F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p})\big)$. It follows that $Q^1\big(\boldsymbol{p}_p^1, T\big)$ equals the polynomial $F_{1,p}(\boldsymbol{p}_p^1, T)$ divided by its leading coefficient.

Then the algorithm proceeds in $r-1$ stages. For $s \in \{1, \dots, r-1\}$, the sth stage takes as input a Kronecker representation $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \dots, W_n^s(\boldsymbol{p}_p^s, T)$ of $\mathcal{J}_{s,p}$ and outputs a Kronecker representation $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T), W_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, T), \dots, W_n^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ of $\mathcal{J}_{s+1,p}$. This stage, whose cost is analyzed below, consists in two main tasks, which are called the lifting step and the intersection step.

6.1.1. *Lifting step.* In the lifting step we compute the Kronecker representation $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \dots, W^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ of $\mathcal{K}_{s,p}$ with primitive element $Y_{n-s+1,p}$, from the univariate representation of $\mathcal{J}_{s,p}$ with $Y_{n-s+1,p}$ as primitive element. By Proposition 5.11, such a Kronecker representation is defined by the specializations of $Q_p^s, W_{n-s+2,p}^s, \dots, W_{n,p}^s$ at $Y_{1,p} = p_{1,p}, \dots, Y_{n-s-1,p} = p_{n-s-1,p}$. Let $\widehat{R}_{s,p} := \mathbb{F}_p[\![Y_{1,p} - p_{1,p}, \dots, Y_{n-s,p} - p_{n-s,p}]\!]$. By Remark 4.12 we conclude that it suffices to compute the approximation of $Q_p^s, W_{n-s+2,p}^s, \dots, W_{n,p}^s$ to precision $(Y_{1,p} - p_{1,p}, \dots, Y_{n-s,p} - p_{n-s,p})^{\delta_s+1}$ in $\widehat{R}_{s,p}[T]$. As $F_{1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \dots, Y_{n,p}), \dots, F_{s,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \dots, Y_{n,p})$ generate the radical ideal $\mathcal{K}_{s,p}$ and form a regular sequence of $\overline{\mathbb{F}}_p[Y_{n-s,p}, \dots, Y_{n,p}]$ by Lemma 4.5, applying the Global Newton algorithm of [20, II.4] we have the following result.

Proposition 6.3. *There exists a deterministic algorithm that takes as input:*

- *a straight–line program of length L which represents the polynomials $F_{1,p}, \dots, F_{s,p}$;*
- *the dense representation of the polynomials in $\mathbb{F}_p[T]$ which form the univariate representation of $\mathcal{J}_{s,p}$ with primitive element $Y_{n-s+1,p}$;*

and outputs the dense representation of the polynomials in $\mathbb{F}_p[Y_{n-s,p}, T]$ which form the Kronecker representation of $\mathcal{K}_{s,p}$ with primitive element $Y_{n-s+1,p}$. The algorithm uses $\mathcal{O}^{\sim}\big((nL + n^5)\delta_s^2 \log p\big)$ bit operations.

6.1.2. *Intersection step.* The input of the intersection step is the output of the algorithm underlying Proposition 6.3, namely the Kronecker representation of $\mathcal{K}_{s,p}$ with primitive element $Y_{n-s+1,p}$. Let $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), V_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ be the corresponding univariate representation. The output is the univariate representation $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T), V_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ of $\mathcal{J}_{s+1,p}$ with primitive element $Y_{n-s,p}$. Consider $F_{s+1,p}$ as an element of $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n,p}]$ and define $h \in \mathbb{F}_p(Y_{n-s,p})[T]$ by

$$h(T) := F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T, V_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, T)\big)$$
$$\mod \big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big).$$

The following result provides an expression for $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ from which we shall be able to compute it efficiently.

Proposition 6.4. *We have*

$$Q^{s+1}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}) = \epsilon \operatorname{Res}_T\big(h(T), Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big),$$

for some $\epsilon \in \mathbb{F}_p \setminus \{0\}$.

Proof. Let M_h be the matrix of the homothety of multiplication by h in $\overline{\mathbb{F}}_p(Y_{n-s,p})[T]/\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$ with respect to the basis $\{1, T, \ldots, T^{\delta_s-1}\}$. We have (see, e.g., [11, Proposition 5.4]):

$$\det(M_h) = \operatorname{Res}_T\big(h(T), Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big).$$

Consider the isomorphism of $\overline{\mathbb{F}}_p(Y_{n-s,p})$–algebras

$$\Phi : \overline{\mathbb{F}}_p(Y_{n-s,p})[Y_{n-s+1,p}, \ldots, Y_{n,p}]/\overline{\mathcal{K}}_{s,p}^e \to \overline{\mathbb{F}}_p(Y_{n-s,p})[T]/\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big),$$

which maps $Y_{n-s+1,p} \mod \overline{\mathcal{K}}_{s,p}^e$ to $T \mod \big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$. Let S be a new indeterminate and $\chi \in \overline{\mathbb{F}}_p[Y_{n-s,p}][S]$ the characteristic polynomial of the homothety by $F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ modulo $\overline{\mathcal{K}}_{s,p}^e$. Let $\chi_0 \in \mathbb{F}_p[Y_{n-s,p}]$ be the constant term of χ. Since Φ maps $F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}) \mod \overline{\mathcal{K}}_{s,p}^e$ to $h \mod \big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$, χ coincides with the characteristic polynomial of the homothety of multiplication by h modulo $\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$. Thus $\chi_0 = (-1)^{\delta_s} \det(M_h)$. On the other hand, as the hypersurface $\{F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}) = 0\}$ intersects the lifting curve $\mathcal{W}_{\boldsymbol{p}_p^{s+1}}$ in the finite fiber $V_{\boldsymbol{p}_p^{s+1}}$, the polynomial $F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}\big)$ is not a zero divisor in $\overline{\mathbb{F}}_p[Y_{n-s,p}, \ldots, Y_{n,p}]/\overline{\mathcal{K}}_{s,p}$. Since $\overline{\mathcal{J}}_{s+1,p} = \overline{\mathcal{K}}_{s,p} + \big(F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big)$, by [9, Proposition 2.7] we deduce that $\chi_0(T)$ coincides, up to multiples in $\mathbb{F}_p \setminus \{0\}$, with the characteristic polynomial of $Y_{n-s,p}$ in $\overline{\mathbb{F}}_p[Y_{n-s,p}, \ldots, Y_{n,p}]/\overline{\mathcal{J}}_{s+1,p}$. Since $Y_{n-s,p}$ induces a primitive element for $\overline{\mathcal{J}}_{s+1,p}$, we conclude that $\chi_0(T) = \epsilon Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ for some $\epsilon \in \overline{\mathbb{F}}_p \setminus \{0\}$. This finishes the proof of the Proposition. $\square$

Now we discuss the computation of the polynomials $V_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^{s+1}(\boldsymbol{p}_p^{s+1}, T)$. Let $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T) = q_1 \cdots q_\ell$ be the irreducible factorization of $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ in $\mathbb{F}_p[T]$.

We describe below how to compute $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T) \mod q_k$ for $n - s + 1 \le j \le n$ and $1 \le k \le \ell$. Then the $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ can be recovered by means of the Chinese remainder theorem. For $1 \le k \le \ell$, let a be the residue class of T in $\mathbb{F}_p[T]/(q_k)$. Set $\mathbb{L} = \mathbb{F}_p[T]/(q_k)$. Thus $\mathbb{L} := \mathbb{F}_p[a]$ is a finite extension of $\mathbb{F}_p$ which contains the root a of $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$. Let $\overline{\mathbb{L}}$ be the algebraic closure of $\mathbb{L}$. We have a field isomorphism $\overline{\mathbb{L}} = \overline{\mathbb{F}}_p$. By Remark 5.8 we know that $\rho_s\big(\boldsymbol{\lambda}_p^s, (\boldsymbol{p}_p^{s+1}, a)\big) \neq 0$. Thus $(\boldsymbol{p}_p^{s+1}, a)$ is a lifting point of $\pi_{s,p}$ and $Y_{n-s+1,p}$ induces a primitive element of the lifting fiber $\pi_{s,p}^{-1}(\boldsymbol{p}_p^{s+1}, a)$. Moreover, $\mathcal{K}_{s,p} + (Y_{n-s} - a)$ is a radical ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ by Lemma 4.2, and therefore it is the vanishing ideal of $\pi_{s,p}^{-1}(\boldsymbol{p}_p^{s+1}, a)$. Let $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$ be the Kronecker representation of $\mathcal{K}_{s,p} + (Y_{n-s} - a)$ with primitive element $Y_{n-s+1,p}$. Let $Q_p^s, W_{n-s+2,p}^s, \ldots, W_{n,p}^s$ be the Kronecker representation of $\mathcal{I}_{s,p}$ with primitive element $Y_{n-s+1,p}$. By Proposition 4.13 the specializations of $Q_p^s, W_{n-s+2,p}^s, \ldots, W_{n,p}^s$ at $Y_{1,p} = p_{1,p}, \ldots, Y_{n-s-1,p} = p_{n-s-1,p}, Y_{n-s,p} = a$ coincide with $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$. Since the input polynomials $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ coincide with the specializations of $Q_p^s, W_{n-s+2,p}^s, \ldots, W_{n,p}^s$ at $Y_{1,p} = p_{1,p}, \ldots, Y_{n-s-1,p} = p_{n-s-1,p}$, we see that $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$ can be obtained by substituting a for $Y_{n-s,p}$ in $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$. Then we can compute the corresponding univariate representation $q_a, v_{a,n-s+2}, \ldots, v_{a,n}$ by means of the identities $v_{a,j} = (q_a')^{-1} w_{a,j} \mod q_a$ for $n - s + 2 \le j \le n$. Let $g(Y_{n-s+1,p}) := F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, a, Y_{n-s+1,p}, v_{a,n-s+2}(Y_{n-s+1,p}), \ldots, v_{a,n}(Y_{n-s+1,p})\big)$. Now $V_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, a), \ldots, V_n^{s+1}(\boldsymbol{p}_p^{s+1}, a)$ can be computed using the following identities (see, e.g., [9]):

$$Y_{n-s+1,p} - V_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, a) = \gcd\big(g(Y_{n-s+1,p}), q_a(Y_{n-s+1,p})\big),$$
$$V_j^{s+1}(\boldsymbol{p}_p^{s+1}, a) = v_{a,j}\big(V_{n-s+2}^{s+1}(\boldsymbol{p}_p^{s+1}, a)\big) \quad (n - s + 2 \le j \le n).$$

More precisely, these identities allows us to compute $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T) \mod Q_k$ for $n - s + 1 \le j \le n$. Having done this for $1 \le k \le \ell$, we can recover $V_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ by the Chinese remainder theorem.

As it is shown in [4, Section 4], the previous computations can be rendered into an efficient procedure from which we obtain the following result (see [4, Proposition 4.7]).

Proposition 6.5. *There exists a probabilistic algorithm that takes as input*
- *a straight–line program of size at most L which represents the polynomial $F_{s+1,p}$;*
- *the dense representation of the polynomials in $\mathbb{F}_p[Y_{n-s,p}, T]$ which form the Kronecker representation of $\mathcal{K}_{s,p}$ with primitive element $Y_{n-s+1,p}$;*

and outputs the dense representation of the polynomials in $\mathbb{F}_p[T]$ which form the univariate representation of $\mathcal{J}_{s+1,p}$ with primitive element $Y_{n-s,p}$. It uses an expected number of $\mathcal{O}^\sim\big((L+n)\delta_s(d\delta_s + \log p) \log p\big)$ bit operations and returns the right result with probability at least $1 - 1/60n$.

Taking into account the complexity and probability estimates of Propositions 6.3 and 6.5 for $1 \le s \le r - 1$, we easily deduce the following result.

Theorem 6.6. *There exists a probabilistic algorithm that takes as input*
- *a "lucky" prime p as in Proposition 6.2;*
- *the points $\boldsymbol{\lambda}_p \in \mathbb{F}_p^{n^2}$ and $\boldsymbol{p}_p \in \mathbb{F}_p^{n-1}$, which are the images of $\boldsymbol{\lambda}$ and $\boldsymbol{p}$ modulo p;*

- *a straight–line program of length at most L which represents the polynomials $F_{1,p}, \ldots, F_{r,p}$;*

and outputs the Kronecker representation of $\mathcal{J}_{r,p}$ with primitive element $Y_{n-r+1,p}$. It uses an expected number of $\mathcal{O}^{\sim}\big(r(nL + n^5)\delta(d\delta + \log p)\log p\big)$ bit operations and returns the right result with probability at least $1 - 1/12$.

6.2. Lifting the integers.
Let s with $1 \leq s \leq r$ and let p be a "lucky" prime as in Proposition 6.2. We have seen that the Kronecker representation $Q^s(\boldsymbol{p}_p^s, T)$, $W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, w_n^s(\boldsymbol{p}_p^s, T) \in \mathbb{F}_p[T]$ of Proposition 5.11 is obtained by reducing modulo p the integers of the Kronecker representation $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, w_n^s(\boldsymbol{p}^{(s)}, T)$ of Proposition 5.10. Further, by Lemma 4.4 the Jacobian determinant of the polynomials $F_{1,p}(\boldsymbol{p}_p^s, Y_{n-s+1,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^s, Y_{n-s+1,p}, \ldots, Y_{n,p})$ with respect to the variables $Y_{n-s+1,p}, \ldots, Y_{n,p}$ is invertible in $\mathbb{F}_p[Y_{n-s+1,p}, \ldots, Y_{n,p}]/\overline{\mathcal{J}}_{s,p}$. With these conditions, the following result holds (see [20, Theorem 2]).

Proposition 6.7. *Assume that we are given:*
- *an upper bound η_s for the heights of $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$;*
- *a lucky prime number p as in Proposition 6.2;*
- *the polynomials $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^S(\boldsymbol{p}_p^s, T), \ldots, W_n^s(\boldsymbol{p}_p^{(s)}, T) \in \mathbb{F}_p[T]$.*

Then $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ can be computed using $\mathcal{O}^{\sim}\big((nL + n^4)\delta_s \eta_s\big)$ bit operations.

6.3. Computation of a Kronecker representation over the rationals.
Combining the algorithm underlying Theorem 6.6 with the p–adic lifting procedure of Proposition 6.7 we obtain a probabilistic algorithm for computing a Kronecker representation of a zero–dimensional fiber of the variety defined by $F_1, \ldots, F_r$.

More precisely, assume that $F_1, \ldots, F_r$ are given by a straight–line program β of length at most L with integer parameters. We first choose at random a point $(\boldsymbol{\lambda}, \boldsymbol{p}) \in \mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$ such that $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ and $\mathsf{N}_{\boldsymbol{\lambda}} \neq 0$. Then we compute a "lucky" prime p as in Proposition 6.2. By reducing the parameters of β modulo p we obtain a straight–line program β_p of length at most L which represents the polynomials $F_{1,p}, \ldots, F_{r,p}$. Then, by means of the algorithm underlying Theorem 6.6, we compute the Kronecker representation $Q_p^r, W_{1,p}^r, \ldots, W_{n,p}^r$ of the lifting fiber $V_{\boldsymbol{p}_p^r}$ with primitive element $Y_{n-r+1,p}$. Finally, applying the algorithm underlying Proposition 6.7 we lift these polynomials to the Kronecker representation $Q^r, W_1^r, \ldots, W_n^r$ of the lifting fiber $V_{\boldsymbol{p}^r}$ with primitive element Y_{n-r+1}. We have the following result.

Theorem 6.8. *There exists a probabilistic algorithm that takes as input a straight–line program β of length at most L which represents the polynomials $F_1, \ldots, F_r$, and outputs a Kronecker representation of a zero–dimensional fiber of $\mathcal{V}(F_1, \ldots, F_r)$ with probability at least $\frac{77}{144}$. If h is an upper bound for the bit length of the coefficients of $F_1, \ldots, F_r$ and the parameters in β, then the bit complexity of the algorithm is in*

$$\mathcal{O}^{\sim}\big(r(nL + n^5)\delta(d\delta + nd^r h)\big).$$

Proof. Let $\mathcal{C}_p$ denote the bit complexity of computing a "lucky" prime p and η an upper bound for heights of the integers in the output. Combining the complexity estimates in

Theorem 6.6 and Proposition 6.7, the bit complexity of the algorithm above is in

$$\mathcal{O}^{\sim}\Big(r(nL + n^5)\delta\big((d\delta + \log p)\log p + \eta\big)\Big) + \mathcal{C}_p.$$

By Proposition A.5 we can take $\eta \in \mathcal{O}^{\sim}\big(nd^{r-1}(h + rd)\big)$. Then, taking into account the estimate for $\mathcal{C}_p$ in Proposition 6.2, we obtain the complexity estimate of the theorem.

Finally, taking into account Lemma 6.1 and the estimates for the probability of success of Proposition 6.2 and Theorem 6.6, the theorem follows. $\square$

Appendix A. Height estimates

In this appendix we obtain estimates for the height of the integer $\mathfrak{N}$ of Theorem 5.9 and the integers occurring in the output of the algorithm underlying Theorem 6.8, namely the polynomials in Proposition 5.10 which form the Kronecker representation of $\mathcal{J}_r$. For this purpose, we shall rely on the arithmetic Nullstellensätze of [28]. We start recalling the notions of height of polynomials and varieties and basic facts about these, and then proceed to obtain the estimates.

A.1. **Height of polynomials and varieties.** We define the *height* of a nonzero integer a as $h(a) := \log |r|$, where log stands for the logarithm to the base 2. Further, we define $h(0) := 0$. It follows that the height of a bounds from above the bit length of a. The height $h(F)$ of a polynomial $F \in \mathbb{Z}[\boldsymbol{X}]$ is defined as the maximum of the heights of its coefficients. More generally, if $F \in \mathbb{Q}[\boldsymbol{X}] \setminus \{0\}$ and $a \in \mathbb{N}$ is a minimal common denominator of all the coefficients of F, then we define $h(F) := \max\{h(aF), h(a)\}$.

Let $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ be an equidimensional $\mathbb{Q}$–variety of dimension $n - s$, with $1 \le s \le n$, and let $h(V)$ be the Faltings height of its projective closure $\overline{V} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ (see [12]). We have the following identity:

$$(\text{A.1}) \qquad h(V) = m(F_V; S_{n+1}^{n-s+1}) + \sum_p \log |F_V|_p + (n - s + 1)\left(\sum_{i=1}^{n} \frac{1}{2i}\right)\deg V,$$

where F_V is any Chow form of V, $m(F_V; S_{n+1}^{n-s+1})$ is the S_{n+1}^{n-s+1}–*Mahler measure* of F_V and $|F_V|_p$ is the p–adic absolute value over $\mathbb{Q}$ for all rational primes p (see, e.g., [28, Section 1.2.4]). Since F_V is uniquely determined up to nonzero multiples in $\mathbb{Q}$, we may assume that F_V is a primitive polynomial in $\mathbb{Z}[\boldsymbol{\Lambda}_1^h, \ldots, \boldsymbol{\Lambda}_{n-s+1}^h]$, in which case $\log |F_V|_p = 0$ for every prime p and the sum $\sum_p \log |F_V|_p$ in (A.1) disappears. On the other hand, by [28, Lemma 1.1] we have

$$(\text{A.2}) \qquad |m(F_V) - h(F_V)| \le (n - s + 1)\log(n + 2)\deg V,$$

where $m(F_V)$ denotes the *Mahler measure* of F_V. The Mahler measure and the S_{n+1}^{n-s+1}–Mahler measure of F_V are related by

$$(\text{A.3}) \qquad 0 \le m(F_V) - m(F_V; S_{n+1}^{n-s+1}) \le (n - s + 1)\deg(V)\sum_{i=1}^{n}\frac{1}{2i}$$

(see, e.g., [28, (1.2)]). Combining (A.1), (A.2) and (A.3) gives

$$h(F_V) \le h(V) + (n - s + 1)\log(n + 2)\deg V.$$

Further, the canonical height $\widehat{h}(V)$ of V is defined by $\widehat{h}(V) := \widehat{h}(\overline{V})$, where $\widehat{h}(V)$ is the *canonical height* of $\overline{V} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ defined as in [6]. The Faltings and the canonical height of V are related by the inequality

$$|\widehat{h}(V) - h(V)| \leq \frac{7}{2} \log(n+1) \deg V$$

(see, e.g., [6, Proposition 2.39 (5)]). As a consequence, we have

(A.4) $$h(F_V) \leq \widehat{h}(V) + \frac{9}{2}(n-s+1) \log(n+2) \deg V.$$

A.2. **Estimates for Chow forms, discriminants and Kronecker representations.** From now on, we return to the setting of Sections 5 and 6, namely we consider polynomials $F_1, \ldots, F_r \in \mathbb{Z}[\boldsymbol{X}]$ which form a regular sequence, denote by $\mathcal{V}_s$ the affine equidimensional subvariety of $\mathbb{A}^n$ defined by $F_1, \ldots, F_s$ and by δ_s its degree for $1 \leq s \leq r$. Let $d_j := \deg(F_j)$ and $h_j := h(F_j)$ for $1 \leq j \leq r$, and denote

$$\delta := \max_{1 \leq s \leq r} \delta_s, \quad d := \max_{1 \leq j \leq r} d_j, \quad h := \max_{1 \leq j \leq r} h_j.$$

Let $\widehat{h}_s := \widehat{h}(\mathcal{V}_s)$ for $1 \leq s \leq r$ and $\widehat{h} := \max_{1 \leq s \leq r} \widehat{h}_s$. By [6, Corollary 2.62], taking into account [6, Lemma 2.30 (1)], we have

(A.5) $$\widehat{h}(\mathcal{V}_s) \leq \sum_{\ell=1}^{s} h_\ell \left(\prod_{j=1, j \neq \ell}^{s} d_j \right) + s \left(\prod_{j=1}^{s} d_j \right) \log(n+2) \quad (1 \leq s \leq r).$$

Let μ and ε be fixed real numbers with $0 < \mu, \varepsilon < 1$. Let $\mathsf{a} := \lfloor \mathsf{D}/(1-\mu) \rfloor$ and $\mathsf{b} := \lfloor \mathsf{D}/(1-\varepsilon) \rfloor$, where D is defined in (5.14). Recall that D is an upper bound for the degree of the polynomials R and $\mathsf{N}_{\boldsymbol{\lambda}}$ of (5.13) and (5.15). Since $D \in \mathcal{O}(rnd^{3r})$ and $h(\mathsf{a}), h(\mathsf{b}) \in \mathcal{O}(\log D)$, we have the following remark.

Remark A.1. $h(\mathsf{a}), h(\mathsf{b}) \in \mathcal{O}^{\sim}(r \log d + \log n)$.

Set $\mathsf{S} := \{0, \ldots, \mathsf{a}\}$ and $\mathsf{T} := \{0, \ldots, \mathsf{b}\}$. Further, let $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathsf{S}^{n^2}$ and $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathsf{T}^{n-1}$ be such that $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ and $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$. By Lemma 2.3, for a random choice of $\boldsymbol{\lambda}$ and $\boldsymbol{p}$ such a condition holds with probability at least $\mu\varepsilon$.

Write $\boldsymbol{\lambda}^s := (\lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$ and $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ for $1 \leq s \leq r$. Denote $h(\boldsymbol{\lambda}^s) := \max_{1 \leq i \leq n-s+1, 1 \leq j \leq n} h(\lambda_{ij})$ and $h(\boldsymbol{p}^s) := \max_{1 \leq i \leq n-s} h(p_i)$. Finally, let $\boldsymbol{\lambda}_i := (\lambda_{i1}, \ldots, \lambda_{in})$ and $Y_i = \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n$. In the sequel, assuming that $n \geq 2$ and $d \geq 2$, we aim to estimate the height of the integer

(A.6) $$\mathfrak{N} := \det(\boldsymbol{\lambda})\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) = \det(\boldsymbol{\lambda})\mathsf{M}_r\big(\boldsymbol{\lambda}^r, \boldsymbol{p}^r\big) \prod_{s=1}^{r-1} \mathsf{M}_s\big(\boldsymbol{\lambda}^s, \boldsymbol{p}^s\big) L_{\boldsymbol{\lambda}^s}\big(\boldsymbol{p}^{s+1}\big).$$

We start with an estimate for the degree and height of a primitive Chow form of $\mathcal{V}_s$ and related polynomials.

Lemma A.2. *For $1 \leq s \leq r$, we have*

(A.7) $$h(P_s) \in \mathcal{O}^{\sim}\big(nd^{s-1}(h+d)\big),$$

(A.8) $$\deg P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s \boldsymbol{X}) \in \mathcal{O}^{\sim}(nd^s), \quad h\big(P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s \boldsymbol{X})\big) \in \mathcal{O}^{\sim}\big(nd^{s-1}(h+d)\big).$$

Proof. (A.4) and (A.5), combined with the Bézout inequality (2.1), yields (A.7). The degree estimate in (A.8) is clear. Next, observe that P_s is an element of $\mathbb{Z}[\mathbf{\Lambda}^s, Z_1, \ldots, Z_{n-s+1}]$ of total degree $(n-s+1)\delta_s$ and Λ_{ij} $(1 \leq i \leq n-s+1, 1 \leq j \leq n)$, $\mathbf{\Lambda}_i \cdot \mathbf{X}$ $(1 \leq i \leq n-s+1)$ are elements of $\mathbb{Z}[\mathbf{\Lambda}^s, \mathbf{X}]$ having total degrees at most 2 and heights equal to 0. Therefore, from [6, Lemma 2.37(3)] we deduce that

$$h\big(P_s(\mathbf{\Lambda}^s, \mathbf{\Lambda}^s \mathbf{X})\big) \leq h(P_s) + (n-s+1)\delta_s\Big(\log\big((n-s+1)(n+1)+1\big) + 2\log\big((n-s+2)n+1\big)\Big).$$

This, together with (A.7), readily implies the height estimate in (A.8). $\qquad\square$

Next we estimate the degree and height of the discriminant ρ_s and the polynomial $\rho_{\boldsymbol{\lambda}^s}$ of Section 5.2. For this purpose, we use the following result.

Lemma A.3. *Let $U_1, \ldots, U_{k+1}$ be indeterminates over $\mathbb{Z}$ and $F, G \in \mathbb{Z}[U_1, \ldots, U_{k+1}]$ nonzero polynomials with $l := \deg_{U_{k+1}} F$ and $m := \deg_{U_{k+1}} G$. Then*

$$h\big(\operatorname{Res}_{U_{k+1}}(F, G)\big) \leq mh(F) + lh(G) + \log(k+1)\big((m-1)\deg F + l \deg G\big) + \log\big((l+m)!\big).$$

Proof. Write $F = \sum_{i=0}^{l} F_i U_{k+1}^i$ and $G = \sum_{j=0}^{m} G_j U_{k+1}^j$, where $F_i, G_j \in \mathbb{Z}[U_1, \ldots, U_k]$. The determinant $\operatorname{Res}_{U_{k+1}}(F, G)$ is a sum of $(l+m)!$ terms, each of which is a product of the form $\pm F_{i_1} \cdots F_{i_m} G_{j_1} \cdots G_{j_l}$. By [6, Lemma 2.37(2)], each term has height at most $mh(F) + lh(G) + \log(k+1)\big((m-1)\deg F + l \deg G\big)$. Then [6, Lemma 2.37(1)] completes the proof of the lemma. $\qquad\square$

Now we are able to estimate the degree and height of ρ_s and $\rho_{\boldsymbol{\lambda}^s}$.

Lemma A.4. *For $1 \leq s \leq r$, we have*

$$\deg \rho_s \in \mathcal{O}(nd^{2s}), \quad h(\rho_s) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big),$$
$$\deg \rho_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{2s}), \quad h(\rho_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big).$$

Proof. Since $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\mathbf{X})$, we have $\deg \rho_{\boldsymbol{\lambda}^s} \leq \deg \rho_s \leq (n-s+2)\delta_s^2$, which proves the degree estimates. Next, as $\rho_s := \operatorname{Res}_{Z_{n-s+1}}\Big(P_s, \frac{\partial P_s}{\partial Z_{n-s+1}}\Big)$, Lemma A.4 implies

$$h(\rho_s) \leq \delta_s\big(2h(P_s) + \log \delta_s\big) + 2\delta_s^2 \log\big((n-s+1)(n+1)\big) + \log\big((2\delta_s)!\big).$$

This and (A.7) prove the estimate for $h(\rho_s)$. Further, since $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ for all s, from [6, Lemma 2.37 (3)] we deduce that

$$h(\rho_{\boldsymbol{\lambda}^s}) \leq h(\rho_s) + \deg \rho_s\Big(h(\mathsf{a}) + \log\big((n-s+1)(n+1)\big) + \log(n+1)\Big).$$

Combining this, Remark A.1 and the estimate for $h(\rho_s)$ yields the one for $h(\rho_{\boldsymbol{\lambda}^s})$. $\qquad\square$

We end this section with an estimate of the height of the Kronecker representations of the fibers of each recursive step of our main algorithm.

Proposition A.5. *Let η_s be the maximum of the heights of the polynomials $Q^s(\boldsymbol{p}^s, T)$, $W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ of Proposition 5.10. Then $\eta_s \in \mathcal{O}^{\sim}\big(nd^{s-1}(h+rd)\big)$.*

Proof. Note that

$$(A.9) \qquad Q^s(\boldsymbol{p}^s, T) = \frac{P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{A_s(\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_{n-s})},$$

$$(A.10) \qquad W_j^s(\boldsymbol{p}^s, T) = -\sum_{k=1}^{n} \frac{\lambda_{jk}}{A_s(\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_{n-s})} \frac{\partial P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{\partial \Lambda_{n-s+1,k}} \quad (n-s+2 \le j \le n).$$

Since $h(\boldsymbol{\lambda}^s) \le h(\mathsf{a})$ and $h(\boldsymbol{p}^s) \le h(\mathsf{b})$, by [6, Lemma 2.37 (3)] we deduce that

$$h\big(P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)\big) \le h(P_s) + (n-s+1)\delta_s\Big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log\big((n-s+1)(n+1)+1\big)+1\Big)$$

$$\le h(P_s) + (n-s+1)\delta_s\big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log(4n^2)\big).$$

Further, as $h\big(\frac{\partial P_s}{\partial \Lambda_{n-s+1,k}}\big) \le h(P_s) + \log \delta_s$, a similar argument shows that

$$h\left(\frac{\partial P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{\partial \Lambda_{n-s+1,k}}\right) \le h(P_s) + \log \delta_s + (n-s+1)\delta_s\big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log(4n^2)\big).$$

Therefore, by [6, Lemma 2.37(1)] we obtain

$$(A.11) \qquad h\left(\sum_{k=1}^{n} \lambda_{jk} \frac{\partial P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{\partial \Lambda_{n-s+1,k}}\right) \le h(P_s) + \log \delta_s + h(\mathsf{a}) + \log n$$

$$+ (n-s+1)\delta_s\big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log(4n^2)\big)$$

for $n-s+2 \le j \le n$. Similarly we deduce that

$$h\big(A_s(\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_{n-s})\big) \le h(P_s) + (n-s)\delta_s\Big(h(\mathsf{a}) + \log\big((n-s+1)n+1\big)\Big).$$

By (A.9), (A.10) and the previous estimates we see that η_s is bounded above by the right–hand side of (A.11). The proposition then follows by (A.7) and Remark A.1. $\qquad\square$

A.3. **Estimates for unmixedness and generic smoothness.** In this section we estimate the height of integers α_s and γ_s as in (5.2) and (5.4), whose nonvanishing modulo p implies that the corresponding modular reduction is unmixed and generically smooth, and yields new variables in Noether position (Theorem 5.5).

We start with α_s. Taking into account that $\widehat{h}\big(\mathbb{A}^{(n-s+2)n}\big) = 0$ and $\deg\big(\mathbb{A}^{(n-s+2)n}\big) = 1$, from [6, Theorem 2] it follows that there exists $\alpha_s \in \mathbb{Z} \setminus \{0\}$ as in (5.2) with

$$h(\alpha_s) \le 3h\big(P_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{X})\big)\prod_{j=1}^{s} d_j + 2\deg\big(P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s\boldsymbol{X})\big)\prod_{j=1}^{s} d_j\left(h\sum_{\ell=1}^{s}\frac{1}{d_\ell} + c(n)\right),$$

where $c(n) \in \mathcal{O}^\sim(n)$. Combining this with (A.8) we deduce the following result.

Lemma A.6. *We have $h(\alpha_s) \in \mathcal{O}^\sim\big(nd^{2s-1}(h+nd)\big)$.*

Next we consider γ_s. Let J_s be the Jacobian determinant of $Y_1, \dots, Y_{n-s}, F_1, \dots, F_s$ with respect to the variables $X_1, \dots, X_n$.

Lemma A.7. *The following assertions hold:*
- $\deg J_s \le s(d-1)$;
- $h(J_s) \le s(\log d + h) + (n-s)h(\mathsf{a}) + s\,d\log(n+1) + \log(n!)$.

Proof. The assertion on the degree of J_s is clear. To prove the second assertion, we observe that J_s is a sum of $n!$ terms of the form $\pm \partial F_1/\partial X_{j_1} \cdots \partial F_s/\partial X_{j_s} \lambda_{1,l_1} \cdots \lambda_{n-s,l_{n-s}}$. Since $h(\lambda_{ij}) \leq h(\mathsf{a})$ and $h(\partial F_i/\partial X_j) \leq h(F_i) + \log(d_i)$, by [6, Lemma 2.37(2)] we deduce that each term has height at most $s(h + \log d) + (n-s)h(\mathsf{a}) + \log(n+1)\big((s-1)(d-1)\big)$. The estimate for the height of J_s follows by [6, Lemma 2.37(1)]. $\square$

Let $d_j := 1$ and $h_j := h(Y_{j-s} - p_{j-s})$ for $s+1 \leq j \leq n$, $d_{n+1} := \deg J_s$ and $h_{n+1} := h(J_s)$. By [6, Theorem 1], there exist $\gamma_s \in \mathbb{Z} \setminus \{0\}$ and $G_1, \ldots, G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ as in (5.4) with

$$h(\gamma_s) \leq \sum_{\ell=1}^{n+1} \left(\prod_{j \neq \ell} d_j \right) h_\ell + (4n+8)\log(n+3) \prod_{j=1}^{n+1} d_j$$

$$\leq \deg J_s \left(\prod_{j=1}^{s} d_j \right) \left(\sum_{\ell=1}^{s} \frac{h_\ell}{d_\ell} + \sum_{\ell=1}^{n-s} h(Y_\ell - p_\ell) + (4n+8)\log(n+3) \right) + h(J_s) \prod_{j=1}^{s} d_j.$$

Since $h(Y_\ell) \leq h(\mathsf{a})$ and $h(p_\ell) \leq h(\mathsf{b})$ for all ℓ, we obtain

$$h(\gamma_s) \leq \deg J_s \, d^{s-1} sh + \deg J_s \, d^s \big((n-s)\max\{h(\mathsf{a}), h(\mathsf{b})\} + (4n+8)\log(n+3)\big) + h(J_s)d^s.$$

Combining this with Remark A.1 and Lemma A.7, we deduce the following result.

Lemma A.8. *We have* $h(\gamma_s) \in \mathcal{O}^{\sim}\big(d^s(h + rnd)\big)$.

A.4. **Estimates for smooth fibers.** In this section we estimate the height of the integers considered in Section 5.2, namely $\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$ and $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$, where M_s is the polynomial of (5.10) and $\mathsf{L}_{\boldsymbol{\lambda}^s}$ is the polynomial of (5.12). Combining these estimates we shall be able to estimate the height of the integer $\mathfrak{N}$ of (A.6), which comprises all the unlucky primes p.

We start estimating the height of $\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$.

Lemma A.9. *For* $1 \leq s \leq r$, *we have* $h\big(\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\big) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h + nd)\big)$.

Proof. By [6, Lemma 2.37 (3)], we have
(A.12)
$$h\big(\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\big) \leq h(\mathsf{M}_s) + \deg(\mathsf{M}_s)\Big(\max\{h(\boldsymbol{\lambda}^s), h(\boldsymbol{p}^s)\} + \log\big((n-s+1)(n+1)+1\big)\Big).$$

Recall that $\mathsf{M}_s := \alpha_s \gamma_s A_s \rho_s$ and, by definition, $\deg A_s \leq (n-s)\delta_s$ and $h(A_s) \leq h(P_s)$. As a consequence, from [6, Lemma 2.37 (2)] we deduce that

$$h(\mathsf{M}_s) \leq h(\alpha_s) + h(\gamma_s) + h(P_s) + h(\rho_s) + (n-s)\delta_s \log\big((n-s+1)(n+1)+1\big).$$

Combining this with (A.7) and Lemmas A.4, A.6 and A.8 we obtain

$$h(\mathsf{M}_s) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big).$$

On the other hand, since $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ and $h(\boldsymbol{p}^s) \leq h(\mathsf{b})$ for all s, by Remark A.1 we have $\max\{h(\boldsymbol{\lambda}^s), h(\boldsymbol{p}^s)\} \in \mathcal{O}^{\sim}(r \log d + \log n)$. Further, $\deg \mathsf{M}_s \in \mathcal{O}(nd^{2s})$ by (5.11). Combining all these estimates with (A.12), the lemma follows. $\square$

Next we estimate $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$. As this integer is expressed in terms of the integers $\mu_{\boldsymbol{\lambda}^s}$ of (5.6) and $\beta_{\boldsymbol{\lambda}^s}$ of (5.9) and the polynomial $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s-1}] \setminus \{0\}$ of (5.7), we start with an estimate for $\mu_{\boldsymbol{\lambda}^s}$ and $B_{\boldsymbol{\lambda}^s}$.

Proposition A.10. *Let $1 \leq s \leq r - 1$ and assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$. Then there exists $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.6) with*

$$(A.13) \qquad\qquad\qquad h(\mu_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^\sim\big(n^2 d^{3s}(h+d)\big).$$

On the other hand, if $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$, then there exists $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s-1}] \setminus \{0\}$ as in (5.7) with

$$(A.14) \qquad\quad \deg B_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{3s+1}), \quad h(B_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^\sim\big(nd^{3s}(h+rnd)\big)$$

Proof. Assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} := \mathcal{V}_{s+1} \cap \{\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\boldsymbol{X}) = 0\} = \emptyset$ and let $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\boldsymbol{X})$. By [6, Theorem 1] there exists $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.6) with

$$h(\mu_{\boldsymbol{\lambda}^s}) \leq h(\rho_{\boldsymbol{\lambda}^s}) \prod_{j=1}^{s+1} d_j + \deg(\rho_{\boldsymbol{\lambda}^s}) \prod_{j=1}^{s+1} d_j \left(\sum_{\ell=1}^{s+1} \frac{h_\ell}{d_\ell} + (4n+8)\log(n+3) \right)$$

$$\leq d^{s+1}\big(h(\rho_{\boldsymbol{\lambda}^s}) + \deg(\rho_{\boldsymbol{\lambda}^s})(4n+8)\log(n+3)\big) + (s+1)\deg(\rho_{\boldsymbol{\lambda}^s})d^s h$$

Combining this with Lemma A.4 proves the first assertion of the lemma.

On the other hand, assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$. By hypothesis $\mathsf{R}_s(\boldsymbol{\lambda}^s) \neq 0$, and hence Lemma 5.6 proves that $\mathcal{W}_{\boldsymbol{\lambda}^s}$ is equidimensional of dimension $n-s-2$. By [6, Corollary 3.23] there exists a polynomial $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s-1}] \setminus \{0\}$ as in (5.7) with

$$(A.15) \qquad \deg(B_{\boldsymbol{\lambda}^s}) \leq \deg \mathcal{W}_{\boldsymbol{\lambda}^s},$$

$$(A.16) \qquad h(B_{\boldsymbol{\lambda}^s}) \leq \widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s}) + \deg \mathcal{W}_{\boldsymbol{\lambda}^s} \left(\sum_{\ell=1}^{n-s-1} h(Y_\ell) + (n-s)\log(2n+8) \right).$$

Next we obtain estimates for $\deg \mathcal{W}_{\boldsymbol{\lambda}^s}$ and $h(\mathcal{W}_{\boldsymbol{\lambda}^s})$ in terms of the degrees and heights of $\mathcal{V}_s$ and $\mathcal{V}_{s+1}$. For this purpose, let $\overline{\mathcal{V}}_{s+1}$ and $\overline{\mathcal{W}}_{\boldsymbol{\lambda}^s}$ denote the projective closures of $\mathcal{V}_{s+1}$ and $\mathcal{W}_{\boldsymbol{\lambda}^s}$ respectively, via the canonical inclusion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$. Let $\rho_{\boldsymbol{\lambda}^s}^h$ be the homogenization of $\rho_{\boldsymbol{\lambda}^s}$. Lemma 5.6 implies that $\{\rho_{\boldsymbol{\lambda}^s}^h = 0\}$ of $\mathbb{P}^n$ cuts $\overline{\mathcal{V}}_{s+1}$ properly. By [6, Corollary 2.62] we conclude that

$$\widehat{h}\big(\overline{\mathcal{V}}_{s+1} \cap \{\rho_{\boldsymbol{\lambda}^s}^h = 0\}\big) \leq \deg \rho_{\boldsymbol{\lambda}^s} \, \widehat{h}\big(\overline{\mathcal{V}}_{s+1}\big) + \deg \overline{\mathcal{V}}_{s+1} \, h(\rho_{\boldsymbol{\lambda}^s}^h) + \deg \overline{\mathcal{V}}_{s+1} \deg \rho_{\boldsymbol{\lambda}^s}^h \log(n+2).$$

Since $\overline{\mathcal{V}}_{s+1} \cap \{\rho_{\boldsymbol{\lambda}^s}^h = 0\}$ is equidimensional of dimension $n-s-2$ and contains every component of $\overline{\mathcal{W}}_{\boldsymbol{\lambda}^s}$, we see that $\widehat{h}\big(\overline{\mathcal{W}}_{\boldsymbol{\lambda}^s}\big) \leq \widehat{h}\big(\overline{\mathcal{V}}_{s+1} \cap \{\rho_{\boldsymbol{\lambda}^s}^h = 0\}\big)$. Recalling that $\widehat{h}(\mathcal{V}_{s+1}) = \widehat{h}(\overline{\mathcal{V}}_{s+1})$ and $\deg \mathcal{V}_{s+1} = \deg \overline{\mathcal{V}}_{s+1}$, and taking into account that $\deg \rho_{\boldsymbol{\lambda}^s}^h = \deg \rho_{\boldsymbol{\lambda}^s}$ and $h(\rho_{\boldsymbol{\lambda}^s}^h) = h(\rho_{\boldsymbol{\lambda}^s})$, we obtain

$$\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \leq \deg \mathcal{V}_{s+1} \deg \rho_{\boldsymbol{\lambda}^s},$$

$$\widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s}) \leq \deg \rho_{\boldsymbol{\lambda}^s} \, \widehat{h}(\mathcal{V}_{s+1}) + \deg \mathcal{V}_{s+1} \, h(\rho_{\boldsymbol{\lambda}^s}) + \deg \mathcal{V}_{s+1} \deg \rho_{\boldsymbol{\lambda}^s} \log(n+2).$$

By (A.5) we have $\widehat{h}(\mathcal{V}_{s+1}) \in \mathcal{O}^\sim\big(d^s(h+d)\big)$. Therefore, by Lemma A.4 we conclude that

$$\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{3s+1}), \quad \widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^\sim\big(nd^{3s}(h+d)\big).$$

Combining these estimates with (A.15) and (A.16), and taking into account that $h(Y_\ell) \in \mathcal{O}^\sim(r \log d + \log n)$ for all ℓ, the second assertion of the lemma easily follows. $\qquad\square$

Now we estimate the height of $\beta_{\boldsymbol{\lambda}^s}$.

Lemma A.11. *Let $1 \leq s \leq r - 1$ and assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$. Then there exists $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.9) with $h(\beta_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^\sim\big(n^3 d^{8s+1}(h + rd)\big)$.*

Proof. Let $d_j = \deg f_j$ and $h_j := h(f_j)$ for $1 \leq j \leq s+1$, and $d_{s+2} := \deg \rho_{\boldsymbol{\lambda}^s}$ and $h_{s+2} := h(\rho_{\boldsymbol{\lambda}^s})$. Further, define $d_0 := \deg B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})$ and $h_0 := h(B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1}))$. Finally, denote $D := \prod_{j=1}^{s+2} d_j$ and $H := \max_{1 \leq j \leq s+2} h_j$. By [6, Theorem 2], taking into account that $\deg \mathbb{A}^n = 1$ and $\widehat{h}(\mathbb{A}^n) = 0$, it follows that there exists $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.9) with

$$h(\beta_{\boldsymbol{\lambda}^s}) \leq 2 d_0 D \left(\frac{3 h_0}{2 d_0} + \sum_{\ell=1}^{s+2} \frac{H}{d_\ell} + e(n) \right),$$

where $e(n) \in \mathcal{O}^\sim(n)$. Now, by Lemma A.4 we have $h_{s+2} \in \mathcal{O}^\sim\big(nd^{2s-1}(h+d)\big)$. Since $H = \max\{h, h_{s+2}\}$, we deduce that $H \in \mathcal{O}^\sim\big(nd^{2s-1}(h+d)\big)$. On the other hand, $d_0 \leq \deg B_{\boldsymbol{\lambda}^s} \in \mathcal{O}^\sim(nd^{3s+1})$ by (A.14) and $D \leq d^{s+1} d_{s+2} \in \mathcal{O}^\sim(nd^{3s+1})$. This implies

$$\text{(A.17)} \qquad d_0 D \left(\sum_{\ell=1}^{s+2} \frac{H}{d_\ell} + e(n) \right) \in \mathcal{O}^\sim\big(n^3 d^{8s+1}(h+d)\big).$$

Next, since $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ for all s, by [6, Lemma 2.37 (3)] we have

$$h_0 \leq h(B_{\boldsymbol{\lambda}^s}) + \deg B_{\boldsymbol{\lambda}^s}\big(h(\mathsf{a}) + \log(n-s) + \log(n+1)\big).$$

Combining this with (A.14) and Remark A.1 we deduce that $h_0 \in \mathcal{O}^\sim\big(nd^{3s}(h+rnd)\big)$. Hence $D h_0 \in \mathcal{O}^\sim\big(n^2 d^{6s+1}(h+rnd)\big)$ which, together with (A.17), proves the lemma. $\square$

Now we are finally able to estimate the height of $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$.

Corollary A.12. *For $1 \leq s \leq r-1$, it holds that $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^\sim\big(n^3 d^{8s+1}(h+rd)\big)$.*

Proof. Observe that $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) = h(\mu_{\boldsymbol{\lambda}^s})$ for $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$, and $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) = h(\beta_{\boldsymbol{\lambda}^s}) + h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big)$ for $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$. Since $h(\boldsymbol{p}^{s+1}) \leq h(\mathsf{b})$, by [6, Lemma 2.37 (3)] we have

$$h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \leq h(B_{\boldsymbol{\lambda}^s}) + \deg B_{\boldsymbol{\lambda}^s}\big(h(\mathsf{b}) + \log(n-s)\big).$$

This inequality, Remark A.1 and (A.14) imply $h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^\sim\big(nd^{3s}(h+rnd)\big)$. Comparing this with (A.13) and Lemma A.11 yields the estimate of the lemma. $\square$

As a consequence of Lemma A.9 and Corollary A.12 we are able to estimate the height of the multiple $\mathfrak{N}$ of all the unlucky primes.

Theorem A.13. *The integer $\mathfrak{N}$ of (A.6) satisfies $h(\mathfrak{N}) \in \mathcal{O}^\sim\big(n^3 d^{8r-7}(h+rd)\big)$.*

Proof. Note that $h(\det \boldsymbol{\lambda}) \leq \log(n!) + nh(\mathsf{a}) \in \mathcal{O}^\sim(rn)$. This, together Lemma with A.9 and Corollary A.12, readily implies the theorem. $\square$

References

[1] B. Bank, J. Heintz, G. Matera, J.L. Montaña, L.M. Pardo, and A. Rojas Paredes, *Quiz games as a model for information hiding*, J. Complexity **34** (2016), 1–29.

[2] A. Bompadre, G. Matera, R. Wachenchauzer, and A. Waissbein, *Polynomial equation solving by lifting procedures for ramified fibers*, Theoret. Comput. Sci. **315** (2004), no. 2–3, 335–369.

[3] P. Bürgisser, M. Clausen, and M.A. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer, Berlin, 1997.

[4] A. Cafure and G. Matera, *Fast computation of a rational point of a variety over a finite field*, Math. Comp. **75** (2006), no. 256, 2049–2085.

[5] D. Castro, M. Giusti, J. Heintz, G. Matera, and L.M. Pardo, *The hardness of polynomial equation solving*, Found. Comput. Math. **3** (2003), no. 4, 347–420.

[6] C. D'Andrea, T. Krick, and M. Sombra, *Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze*, Ann. Sci. Éc. Norm. Supér. (4) **46** (2013), no. 4, 571–649.

[7] C. D'Andrea, A. Ostafe, I. Shparlinski, and M. Sombra, *Modular reduction of systems of polynomial equations and algebraic dynamical systems*, Preprint `arXiv:1505.05814 [math.NT]`, 2015.

[8] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time*, Discrete Appl. Math. **33** (1991), 73–94.

[9] C. Durvye and G. Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Expo. Math. **26** (2008), no. 2, 101–139.

[10] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Grad. Texts in Math., vol. 150, Springer, New York, 1995.

[11] M. Elkadi and B. Mourrain, *Introduction à la résolution des systèmes polynomiaux*, Math. Appl. (Berlin), vol. 59, Springer, Berlin, 2007.

[12] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. Math. (2) **133** (1999), no. 3, 549–576.

[13] N. Fitchas, M. Giusti, and F. Smietanski, *Sur la complexité du théorème des zéros*, Approximation and Optimization in the Caribbean II, Proceedings 2nd International Conference on Non–Linear Optimization and Approximation (J. Guddat et al, ed.), Approximation and Optimization, vol. 8, Peter Lange Verlag, Frankfurt am Main, 1995, pp. 247–329.

[14] W. Fulton, *Intersection theory*, Springer, Berlin Heidelberg New York, 1998.

[15] N. Giménez, J. Heintz, G. Matera, and P. Solernó, *Lower complexity bounds for interpolation algorithms*, J. Complexity **27** (2011), no. 2, 151–187.

[16] M. Giusti, *Complexity of standard bases in projective dimension zero*, Proceedings of the European Conference on Computer Algebra (Berlin) (J.H. Davenport, ed.), Lecture Notes in Comput. Sci., vol. 378, Springer, 1989, pp. 333–335.

[17] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, and L.M. Pardo, *Lower bounds for Diophantine approximation*, J. Pure Appl. Algebra **117,118** (1997), 277–317.

[18] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo, *Straight–line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), 101–146.

[19] M. Giusti, J. Heintz, and J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), 56–95.

[20] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211.

[21] K. Hägele, J.E. Morais, L.M. Pardo, and M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz*, J. Pure Appl. Algebra **146** (2000), no. 2, 103–183.

[22] A. Hashemi and D. Lazard, *Sharper complexity bounds for zero–dimensional Gröbner bases and polynomial system solving*, Internat. J. Algebra Comput. **21** (2011), no. 5, 703–713.

[23] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277.

[24] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein, *Deformation techniques for efficient polynomial equation solving*, J. Complexity **16** (2000), no. 1, 70–109.

[25] W. Hodge and D. Pedoe, *Methods of algebraic geometry. Vol. II*, Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1968.

[26] Z. Jelonek, *On the effective Nullstellensatz*, Invent. Math. **162** (2005), no. 1, 1–17.

[27] G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein, *Deformation techniques for sparse systems*, Found. Comput. Math **9** (2009), 1–50.

[28] T. Krick, L.M. Pardo, and M. Sombra, *Sharp estimates for the Arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), no. 3, 521–598.

[29] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston, 1985.

[30] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theoret. Comput. Sci. **15** (1981), 77–110.

[31] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596.

[32] H. Matsumura, *Commutative algebra*, Benjamin, 1980.

[33] _____, *Commutative ring theory*, Cambridge Univ. Press, Cambridge, 1986.

[34] S. Melczer and B. Salvy, *Symbolic–numeric tools for analytic combinatorics in several variables*, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo, ON, Canada, July 19–22, 2016 (New York), ACM Press, 2016, pp. 333–340.

[35] T. Mora, *Solving polynomial equation systems. Vol. II. Macaulay's paradigm and Gröbner technology*, Encyclopedia Math. Appl., vol. 99, Cambridge Univ. Press, Cambridge, 2005.

[36] _____, *Solving polynomial equation systems. Vol. III: Algebraic solving*, Encyclopedia Math. Appl., vol. 157, Cambridge Univ. Press, Cambridge, 2015.

[37] D. Mumford, *Algebraic geometry I. Complex projective varieties*, 2nd ed., Classics Math., Springer, Berlin, 1995.

[38] L.M. Pardo and J. San Martín, *Deformation techniques to solve generalized Pham systems*, Theoret. Comput. Sci. **315** (2004), no. 2–3, 593–625.

[39] M. Safey El Din and E. Schost, *Bit complexity for multi-homogeneous polynomial system solving. Application to polynomial minimization*, Preprint `arXiv:1605.07433 [cs.SC]`, 2016.

[40] E. Schost, *Sur la résolution de systèmes à paramètres*, Ph.D. thesis, École Polytechnique, France, 2000.

[41] _____, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), 349–393.

[42] I.R. Shafarevich, *Basic algebraic geometry: Varieties in projective space*, Springer, Berlin Heidelberg New York, 1994.

[43] A. Sommese, J. Verschelde, and C. Wampler, *Solving polynomial systems equation by equation*, Algorithms in algebraic geometry (A. Dickenstein, F. Schreyer, and A. Somesse, eds.), IMA Vol. Math. Appl., vol. 146, Springer, 2008, pp. 133–152.

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

[45] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999.

[1]INSTITUTO DEL DESARROLLO HUMANO, UNIVERSIDAD NACIONAL DE GENERAL SARMIENTO, J.M. GUTIÉRREZ 1150 (B1613GSX) LOS POLVORINES, BUENOS AIRES, ARGENTINA

E-mail address: {agimenez,gmatera}@ungs.edu.ar

[2] NATIONAL COUNCIL OF SCIENCE AND TECHNOLOGY (CONICET), ARGENTINA