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 outside a given hypersurface. 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., [37] and [38] 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., [32], [17], [9], [14], [18], [21], [33] and [10], 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 [6], [16] 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 [23] 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., [18] and [22], 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

Date: April 24, 2020.

1991 *Mathematics Subject Classification.* 14Q20, 14G40, 13P15, 68W30.

Key words and phrases. Polynomial system solving over $\mathbb{Q}$, bit complexity, reduced regular sequence, Chow form, lifting fibers, Hensel lifting, lucky primes.

The authors were partially supported by the grants PIP CONICET 11220130100598, PIO CONICET-UNGS 14420140100027 and UNGS 30/3084.

Schost and Safey El Din [41] 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, [18] 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 [19] and [18]. We shall consider the improved version of this algorithm due to [21] (see also [10]), which we now discuss. Let $F_1, \ldots, F_r, G \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials such that $F_1, \ldots, F_r$ form a reduced regular sequence in the open set $\{G \neq 0\}$, that is, the ideal $\mathcal{I}_s := (F_1, \ldots, F_s) : G^\infty \subset \mathbb{Q}[X_1, \ldots, X_n]$ is radical and the affine subvariety $\mathcal{V}_s := \mathcal{V}(\mathcal{I}_s) \subset \mathbb{C}^n$ defined by $\mathcal{I}_s$ is equidimensional of dimension $n - s$ for $1 \leq s \leq r$. Denote by $\delta_s := \deg \mathcal{V}_s$ the degree of $\mathcal{V}_s$ for $1 \leq s \leq r$. Let $\mathcal{V} := \mathcal{V}_r$ and $\delta := \max_{1 \leq s \leq r} \delta_s$. The algorithm outputs a suitable "parametrization" of a "lifting fiber" of $\mathcal{V}$, that is, a $\mathbb{Q}$–definable (zero–dimensional) fiber of maximal cardinality of a general linear projection $\pi : \mathcal{V} \to \mathbb{C}^{n-r}$ defined over $\mathbb{Q}$ (see Section 4 for details). 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 $F_1 = 0, \ldots, F_r = 0, G \neq 0$, both from the numeric and the symbolic point of view (see, e.g., [25], [43], [33], [5], [46]).

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 [21], 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 $(F_1, \ldots, F_s) : G^\infty$ are preserved under modular reduction for $1 \leq s \leq r$. 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 [42] (see also [36]), on modular reduction of smooth fibers of parametric families of zero–dimensional varieties, and [8], on modular reduction of zero–dimensional varieties defined over $\mathbb{Z}$. Unfortunately, these results are not enough for our purposes (particularly for the analysis of Section 5.2; see the remarks after Theorem 1.2).

For the analysis of the bit length of lucky primes, we establish conditions on the coefficients of linear forms $Y_1, \ldots, Y_{n-s+1} \in \mathbb{Q}[X_1, \ldots, X_n]$ and the coordinates of a point $\boldsymbol{p} \in \mathbb{Q}^{n-s}$ which imply that the projection $\pi_s : \mathcal{V}_s \to \mathbb{C}^{n-s}$ defined by $Y_1, \ldots, Y_{n-s}$ is "general" in the sense above, $\boldsymbol{p}$ defines a lifting fiber and Y_{n-s+1} separates the points of $\pi_s^{-1}(\boldsymbol{p})$ (we say that Y_{n-s+1} induces a primitive element of $\pi_s^{-1}(\boldsymbol{p})$). Such a point $\boldsymbol{p}$ is called a "lifting point". 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 4.9).

Theorem 1.1. *Let $V \subset \overline{\mathbb{K}}^n$ be an equidimensional variety defined over $\mathbb{K}$ of dimension $n-s$ and degree $\delta_s > 0$. 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 $\deg_{\boldsymbol{\Lambda}_i} A_V = \delta_s$ $(1 \le i \le n-s)$, $\deg_{\boldsymbol{\Lambda}_i} \rho_V \le \delta_s(2\delta_s - 1)$ $(1 \le i \le n-s+1)$, $\deg_{\boldsymbol{Z}} \rho_V \le \delta_s(2\delta_s - 1)$ 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 $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \ne 0$, 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. *$rank_{\mathbb{K}[\boldsymbol{Y}]}\mathbb{K}[V] = \delta_s$;*
3. *$\boldsymbol{p}$ 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 [5] 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 [7], and then obtain a lucky prime p with "low" bit length. The following statement summarizes our results on modular reduction (see Theorems 5.10 and A.20).

Theorem 1.2. *Let $F_1, \ldots, F_r, G \in \mathbb{Z}[X_1, \ldots, X_n]$ 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 in the open set $\{G \ne 0\}$ and denote $\mathcal{I}_s := (F_1, \ldots, F_s) : G^\infty$, $\mathcal{V}_s := \mathcal{V}(\mathcal{I}_s) \subset \mathbb{C}^n$ and $\delta_s := \deg \mathcal{V}_s$ for $1 \le s \le r$. Let $\delta := \max_{1\le s\le r} \delta_s$. 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 at most $c_1 \log(n^2\delta^3)$, for a suitable $c_1 > 0$. Let $(Y_1, \ldots, Y_n) := \boldsymbol{\lambda}\boldsymbol{X}$ and $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ for $1 \le s \le r$.*

Let p be a random prime number of bit length $c_2 \log(nd^r h)$, for a suitable $c_2 > 0$. Denote by $F_{1,p}, \ldots, F_{r,p}$, G_p, $Y_{1,p}, \ldots, Y_{n,p}$ and $\boldsymbol{p}_p$ the corresponding reductions modulo p. Then the following conditions are satisfied for $1 \le s \le r$ with probability at least $2/3$:

1. *the ideal $\mathcal{I}_{s,p} := (F_{1,p}, \ldots, F_{s,p}) : G_p^\infty \subset \overline{\mathbb{F}}_p[\boldsymbol{X}]$ is radical and the variety $\mathcal{V}_{s,p} := \mathcal{V}(\mathcal{I}_{s,p}) \subset \overline{\mathbb{F}}_p^n$ is equidimensional of dimension $n-s$ and degree δ_s;*
2. *the mapping $\pi_{s,p} : \mathcal{V}_{s,p} \to \overline{\mathbb{F}}_p^{n-s}$ 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 [42] (compare with [36]). Nevertheless, condition (3), which is critical to prove the correctness

of our algorithm for solving the system $F_1 = 0, \ldots, F_r = 0, G \neq 0$, requires a significant extension of these techniques.

Finally, we combine the algorithm of [5] with p–adic lifting, as in [21], to obtain an algorithm for solving the system $F_1 = 0, \ldots, F_r = 0, G \neq 0$ with good bit complexity. We prove the following result (see Theorem 6.9 for a precise statement).

Theorem 1.3. *Let $F_1, \ldots, F_r, G$ 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 $F_1, \ldots, F_r, G$ with at most L arithmetic operations in $\mathbb{Z}$ and integer parameters of bit size at most h, and outputs a parametrization of a lifting fiber of $\mathcal{V}(\mathcal{I}_r)$ with $\mathcal{O}^{\sim}\big((nL + n^5)\delta(d\delta + nd^r h)\big)$ 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 $F_1 = 0, \ldots, F_r = 0, G \neq 0$ 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., [30], [11], [44].

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 $\mathbb{K}$. For $F \in \mathbb{K}[X_1, \ldots, X_n]$ and $S \subset \{X_1, \ldots, X_n\}$, $\deg_S F$ denotes the degree of F as an element of the ring $R[S]$ with $R := \mathbb{K}[\{X_1, \ldots, X_n\} \setminus S]$, while $\deg F$ denotes its total degree.

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 $\mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$.

For polynomials $F_1, \ldots, F_r, G \in \mathbb{K}[X_1, \ldots, X_n]$, we write $(F_1, \ldots, F_r) : G^\infty := \{F \in \mathbb{K}[X_1, \ldots, X_n] : \exists m \geq 0 \text{ with } G^m F \in (F_1, \ldots, F_r)\}$ for the saturation of the ideal $(F_1, \ldots, F_r) \subset \mathbb{K}[X_1, \ldots, X_n]$ with respect to G. We remark that, if $\mathcal{I} \subset \mathbb{K}[X_1, \ldots, X_n]$ denotes the saturation $\mathcal{I} := (F_1, \ldots, F_r) : G^\infty$, then $\mathcal{V}(\mathcal{I}) \subset \mathbb{A}^n$ is the Zariski closure of the locally closed set $\mathcal{V}(F_1, \ldots, F_r) \setminus \mathcal{V}(G)$.

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. [24]). This definition of degree satisfies the following *Bézout inequality* ([24]; see also [15]): if V and W are $\mathbb{K}$–varieties of $\mathbb{A}^n$, then

$$\deg(V \cap W) \leq \deg V \deg W. \tag{2.1}$$

2.1. **Notions and results of commutative algebra.** A proper ideal $\mathcal{I}$ of a Noetherian ring R is *unmixed* if the codimensions of its associated primes are all equal. We say that the *unmixedness theorem* holds for R if any proper ideal $\mathcal{I}$ of R of codimension r generated by r elements is unmixed for any $r \geq 0$. A classical result asserts that the unmixedness theorem holds for any localization $S^{-1}\mathbb{K}[X_1, \ldots, X_n]$ (see, e.g., [35, Theorems 17.6 and 17.7]).

Let $\mathcal{I} \subset \mathbb{K}[X_1, \ldots, X_n]$ be an ideal of dimension $n - r$. Then $\mathcal{I}$ is unmixed 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 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., [10, Theorem 1.27]). We shall call χ and μ respectively the *characteristic* and the *minimal* polynomials of F modulo $\mathcal{I}$ (with respect to the Noether normalization defined by $Y_1, \ldots, Y_n$).

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. [20, 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 and $F_1, \ldots, F_s, G \in \mathbb{K}[X_1, \ldots, X_n]$ polynomials such that the ideal $\mathcal{I} := (F_1, \ldots, F_s) \subset \mathbb{K}[X_1, \ldots, X_n]$ satisfies $\operatorname{codim}(\mathcal{I} : G^\infty) = s$. Let $\overline{\mathcal{J}}$ be the ideal of $R := \mathbb{K}[X_1, \ldots, X_n]/(\mathcal{I} : G^\infty)$ generated by the $(s \times s)$–minors of the Jacobian matrix $(\partial F_i/\partial X_j)_{1 \leq i \leq s, 1 \leq j \leq n}$ taken modulo $\mathcal{I} : G^\infty$. Then $\mathcal{I} : G^\infty$ is radical if and only if $\operatorname{codim}_R(\overline{\mathcal{J}}) \geq 1$.*

Proof. Let $\mathcal{I}_G := \mathcal{I}\mathbb{K}[X_1, \ldots, X_n]_G$ and let $\overline{\mathcal{K}}$ be the ideal of $S := \mathbb{K}[X_1, \ldots, X_n]_G/\mathcal{I}_G$ generated by the $(s \times s)$-minors of the Jacobian matrix $(\partial F_i/\partial X_j)_{1 \leq i \leq s, 1 \leq j \leq n}$ taken

modulo $\mathcal{I}_G$. Since $\operatorname{codim}(\mathcal{I}_G) = \operatorname{codim}(\mathcal{I} : G^\infty) = s$, by [11, Proposition 18.3] we deduce that S is a Cohen-Macaulay ring. Then we can apply [11, Theorem 18.15] and deduce that $\mathcal{I}_G$ is radical if and only if $\operatorname{codim}_S \overline{\mathcal{K}} \geq 1$. Since $\mathcal{I} : G^\infty$ is radical if and only if $\mathcal{I}_G$ is radical, and $\operatorname{codim}_R(\overline{\mathcal{J}}) \geq 1$ if and only if $\operatorname{codim}_S \overline{\mathcal{K}} \geq 1$, the lemma follows. □

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

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).*

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:

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

A univariate representation of $\mathcal{I}$ as above has a simpler structure than a Kronecker representation, and it can be easily obtained from the latter by inverting Q' modulo Q. Nevertheless, since such an inversion typically implies a degree growth of the elements of R involved, we shall be rather concerned with Kronecker representations.

2.3. **Model of computation.** In the sequel, log denotes logarithm to the base 2. 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. More precisely, given two function $f = f(n, d, h)$ and $g = g(n, d, h)$ in integer parameters n, d, h, we say that f is in $\mathcal{O}^\sim(g)$ if there exists $s \geq 0$ such that f is in $\mathcal{O}(g \log^s g)$. 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. [4]). 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 model of computation is based on the concept of straight–line programs. However, a model of computation consisting *only* of straight–line programs is not expressive enough for our purposes. Therefore we allow our model to include decisions and selections (subject to previous decisions). For this reason we shall also consider *computation trees*, which are straight–line programs with *branchings*. Length of a given computation tree is defined similarly to the case of straight–line programs (see, e.g., [4] for more details on the notion of computation trees).

Our algorithm is probabilistic, of *Monte Carlo* type (see, e.g., [47]). 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., [47, 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., [47, 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 correct result with probability at least*

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

Proof. According to, e.g., [47, 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. □

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 $\mathbf{\Lambda}^h := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 0 \leq j \leq n}$ be a matrix of indeterminates over $\mathbb{K}[V]$, let $\mathbf{\Lambda}_i^h := (\Lambda_{i0}, \ldots, \Lambda_{in})$ and $\mathbf{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ for $1 \leq i \leq n - s + 1$. A Chow form of V is a square–free polynomial F_V of $\mathbb{K}[\mathbf{\Lambda}^h]$ 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 [26, Chapter X, Section 6]). We observe that F_V is multihomogeneous 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

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

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 $\mathbb{K}[V][\mathbf{\Lambda}]$:

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

  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 [26, 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) $\deg_{(\Lambda_{1,0},\ldots,\Lambda_{n-s+1,0})} F_V = \deg_{\Lambda_{n-s+1,0}} F_V = \delta$;
(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 $\mathbb{K}[\mathbf{\Lambda}][\Lambda_{1,0}, \ldots, \Lambda_{n-s+1,0}]$. Then (2) implies that A_V is independent of $\Lambda_{1,0}, \ldots, \Lambda_{n-s\,0}$, 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 [34, 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 [34, 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 $\mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$. Since $\mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}]$ is a factorial ring, this implies that the resultant ρ_V of these polynomials does not vanish. □

Further, ρ_V satisfies the following degree estimates:

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

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 $\mathbb{K}[V][\mathbf{\Lambda}]$ as a $\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]$–algebra through the ring homomorphism $\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[V][\mathbf{\Lambda}]$ which maps any $F \in \mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]$ to $F(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi})$. 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 $\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]$–algebra $\mathbb{K}[V][\mathbf{\Lambda}]$.*

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

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

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

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

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

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

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

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

in $\overline{\mathbb{K}}[\mathcal{C}][\mathbf{\Lambda}]$, 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, $F(\mathbf{\Lambda}, \boldsymbol{\xi}) = 0$ in $\mathbb{K}[\mathcal{C}][\mathbf{\Lambda}]$ for every irreducible component $\mathcal{C}$ of V. We conclude that $F(\mathbf{\Lambda}, \boldsymbol{\xi}) = 0$ in $\mathbb{K}[V][\mathbf{\Lambda}]$, which finishes the proof. □

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 $\mathbf{\Lambda}^* = (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$. Recall that A_V is homogeneous of degree δ in the $(n-s) \times (n-s)$–minors of $\mathbf{\Lambda}^*$. 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 $\mathbf{\Lambda}$ for $(\boldsymbol{\lambda}^*, \boldsymbol{w}_k)$. From (3.1) we deduce that

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

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 $1 \leq k \leq n$:

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

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

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

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 $\dim_{R'} B' \leq \delta$. □

4. Lifting points and lifting fibers

Assume as in Section 3 that $\mathbb{K}$ is perfect field. Let $F_1, \ldots, F_s$ and G be polynomials in $\mathbb{K}[\boldsymbol{X}]$ such that the ideal $\mathcal{I} := (F_1, \ldots, F_s) : G^\infty \subset \mathbb{K}[\boldsymbol{X}]$ is radical and the $\mathbb{K}$-variety $V := \mathcal{V}(\mathcal{I}) \subset \mathbb{A}^n$ is equidimensional of dimension $n-s$ and degree δ. Assume further that we are given linearly–independent linear forms $Y_1, \ldots, Y_n \in \mathbb{K}[\boldsymbol{X}]$ defining variables in Noether position with respect to V. Let $\pi : V \to \mathbb{A}^{n-s}$ be the finite morphism defined by $Y_1, \ldots, Y_{n-s}$ and $\mathcal{J} \subset \mathbb{K}[\boldsymbol{X}]$ the ideal $\mathcal{J} := \mathcal{I} + (F_1, \ldots, F_s, Y_1, \ldots, Y_{n-s})$. A point $\boldsymbol{p} \in \mathbb{K}^{n-s}$ is called a *lifting point* of π with respect to the system $F_1 = 0, \ldots, F_s = 0, G \neq 0$ if $\mathcal{J}$ is radical. We call the zero–dimensional variety $\pi^{-1}(\boldsymbol{p})$ the *lifting fiber* of $\boldsymbol{p}$.

The notion of lifting fiber in this framework was first introduced in [18]. The concept was isolated in [25], 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 [21], [43], [2], [40] and [28] 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., [46]; see [45] 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 4.9). 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.** In the sequel we denote $R' := \mathbb{K}(Y_1, \ldots, Y_{n-s})$, $B' := \mathbb{K}(Y_1, \ldots, Y_{n-s})[\boldsymbol{X}]/\mathcal{I}^e$ and $D := \dim_{R'} B'$. The following proposition provides a complete characterization of the notion of lifting point.

Proposition 4.1. *For $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$, we have:*

- *$\#\pi^{-1}(\boldsymbol{p}) \leq D$, with equality if and only if $\boldsymbol{p}$ is a lifting point of π.*
- *Assume that $\#\pi^{-1}(\boldsymbol{p}) = D$. For $0 \leq j \leq n-s$, the ideal $\mathcal{J}_j = \mathcal{I} + (Y_1 - p_1, \ldots, Y_j - p_j)$ is radical and equidimensional of dimension $n-s-j$ and the mapping $\mathcal{V}(\mathcal{J}_j) \to \mathbb{A}^{n-s-j}$ defined by $Y_{j+1}, \ldots, Y_{n-s}$ is a finite morphism. Further, if $\mathcal{J}_j^e := \mathcal{J}_j \mathbb{K}(Y_{j+1}, \ldots, Y_{n-s})[\boldsymbol{X}]$, then the quotient ring $\mathbb{K}(Y_{j+1}, \ldots, Y_{n-s})[\boldsymbol{X}]/\mathcal{J}_j^e$ is a $\mathbb{K}(Y_{j+1}, \ldots, Y_{n-s})$-vector space of dimension D.*

Proof. By [10, Corollary 2.5], $\sqrt{\mathcal{J}_j}$ is unmixed of dimension $n-s-j$ and the extension $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}] \subseteq \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}_j}$ is integral. It follows that the radical of $\sqrt{\mathcal{J}_j} + (Y_{j+1} - p_{j+1}) = \mathcal{J}_{j+1}$ is unmixed of dimension $n-s-j-1$ and $\mathbb{K}[Y_{j+2}, \ldots, Y_{n-s}] \subseteq \mathbb{K}[\boldsymbol{X}]/(\sqrt{\mathcal{J}_j} + (Y_{j+1} - p_{j+1}))$ is an integral extension of rings. Further, for $0 \leq j \leq n-s$ let $\mathbb{F}_j := \mathbb{K}(Y_{j+1}, \ldots, Y_{n-s})$ and denote

$$\sqrt{\mathcal{J}_j}^e := \sqrt{\mathcal{J}_j}\,\mathbb{F}_j[\boldsymbol{X}] \text{ and } (\sqrt{\mathcal{J}_j} + (Y_{j+1} - p_{j+1}))^e := (\sqrt{\mathcal{J}_j} + (Y_{j+1} - p_{j+1}))\mathbb{F}_{j+1}[\boldsymbol{X}].$$

We claim that

$$\dim_{\mathbb{F}_{j+1}} \mathbb{F}_{j+1}[\boldsymbol{X}]/(\sqrt{\mathcal{J}_j} + (Y_{j+1} - p_{j+1}))^e = \dim_{\mathbb{F}_j} \mathbb{F}_j[\boldsymbol{X}]/(\sqrt{\mathcal{J}_j})^e \tag{4.1}$$

for $0 \leq j \leq n-s-1$. Indeed, $B := \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}_j}$ is a torsion-free finitely generated $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$-module ([10, Proposition 1.22]). Set $\widetilde{B} := \mathbb{F}_{j+1}[\boldsymbol{X}]/\sqrt{\mathcal{J}_j}\,\mathbb{F}_{j+1}[\boldsymbol{X}]$. Then $\widetilde{B}$ is a torsion-free finitely generated $\mathbb{F}_{j+1}[Y_{j+1}]$-module which, by [31, Theorem 7.3], is a free $\mathbb{F}_{j+1}[Y_{j+1}]$-module of finite rank. Since a basis of $\widetilde{B}$ induces a basis of $\mathbb{F}_j[\boldsymbol{X}]/\sqrt{\mathcal{J}_j}^e$ as $\mathbb{F}_j$-vector space and a basis of $\mathbb{F}_{j+1}[\boldsymbol{X}]/(\sqrt{\mathcal{J}_j} + (Y_{j+1} - p_{j+1}))^e$ as $\mathbb{F}_{j+1}$-vector space, the claim follows.

By (4.1) it follows that

$$\dim_{\mathbb{F}_{j+1}} \mathbb{F}_{j+1}[\boldsymbol{X}]/(\sqrt{\mathcal{J}_{j+1}})^e \leq \dim_{\mathbb{F}_j} \mathbb{F}_j[\boldsymbol{X}]/(\sqrt{\mathcal{J}_j})^e$$

for $0 \leq j \leq n-s-1$. This implies $\#\pi^{-1}(\boldsymbol{p}) = \dim \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}} \leq D$.

Next, suppose that $\#\pi^{-1}(\boldsymbol{p}) = D$. Let $L_{\boldsymbol{U}} := U_1 X_1 + \cdots + U_n X_n$ be a generic linear form, where $\boldsymbol{U} := (U_1, \ldots, U_n)$ is a tuple of new indeterminates over $\mathbb{K}(Y_1, \ldots, Y_{n-s})$. Let $Q_{\boldsymbol{U}} \in \mathbb{K}(\boldsymbol{U}, Y_1, \ldots, Y_{n-s})[T]$ be the minimal polinomial of $L_{\boldsymbol{U}}$ in

$$B'_{\boldsymbol{U}} := \mathbb{K}(\boldsymbol{U}, Y_1, \ldots, Y_{n-s})[\boldsymbol{X}]/\mathcal{I}^e_{\boldsymbol{U}},$$

where $\mathcal{I}^e_{\boldsymbol{U}} := \mathcal{I}\mathbb{K}(\boldsymbol{U}, Y_1, \ldots, Y_{n-s})[\boldsymbol{X}]$. By [10, Proposition 3.3], $Q_{\boldsymbol{U}}$ is a squarefree polynomial of $\mathbb{K}[\boldsymbol{U}, Y_1, \ldots, Y_{n-s}][T]$. Let $\mathbb{C}'_{\boldsymbol{U}} := K(\boldsymbol{U})[\boldsymbol{X}]/\mathcal{J}^e_{\boldsymbol{U}}$, where $\mathcal{J}^e_{\boldsymbol{U}} := \mathcal{J}\mathbb{K}(\boldsymbol{U})[\boldsymbol{X}]$. Let $q_{\boldsymbol{U}} \in \mathbb{K}(\boldsymbol{U})[T]$ be the specialization of $Q_{\boldsymbol{U}}$ at $Y_1 = p_1, \ldots, Y_{n-s} = p_{n-s}$. Note that $q_{\boldsymbol{U}}$ is monic with $\deg_T q_{\boldsymbol{U}} = D$. By hypothesis $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}} = D$. Then $\dim_{\mathbb{K}(\boldsymbol{U})} \mathbb{K}(\boldsymbol{U})[\boldsymbol{X}]/\sqrt{\mathcal{J}_{\boldsymbol{U}}} = D$, where $\sqrt{\mathcal{J}_{\boldsymbol{U}}} := \sqrt{\mathcal{J}}\mathbb{K}(\boldsymbol{U})[\boldsymbol{X}]$. Let $p_{\boldsymbol{U}}$ be the minimal polynomial of $L_{\boldsymbol{U}}$ in $\mathbb{K}(\boldsymbol{U})[\boldsymbol{X}]/\sqrt{\mathcal{J}_{\boldsymbol{U}}}$. By [10, Proposition 3.3], $p_{\boldsymbol{U}} \in \mathbb{K}[\boldsymbol{U}][T]$ and

$\deg_T p_{\boldsymbol{U}} = D$. According to [10, Proposition 3.6 (a)], $p_{\boldsymbol{U}}$ is the squarefree part of $q_{\boldsymbol{U}}$. Since $\deg_T p_{\boldsymbol{U}} = \deg_T q_{\boldsymbol{U}} = D$, we deduce that $q_{\boldsymbol{U}}$ is squarefree and [10, Proposition 3.6 (b)] proves that $\mathcal{J}$ is radical. Further, as $q_{\boldsymbol{U}}$ is squarefree, every partial specialization of $Q_{\boldsymbol{U}}$ at $Y_1 = p_1, \ldots, Y_j = p_j$ is squarefree. By [10, Proposition 3.6 (b)], we deduce that $\mathcal{J}_j$ is radical for $1 \leq j \leq n-s$.

Conversely, suppose that $\mathcal{J}$ is radical. As before, this implies that $\mathcal{J}_j$ is radical for $0 \leq j \leq n-s$. Taking into account that $\mathcal{J}_{j+1} = \mathcal{J}_j + (Y_{j+1} - p_{j+1})$, by (4.1) we see that

$$\dim_{\mathbb{F}_{j+1}} \mathbb{F}_{j+1}[\boldsymbol{X}]/(\mathcal{J}_{j+1})^e = \dim_{\mathbb{F}_j} \mathbb{F}_j[\boldsymbol{X}]/(\mathcal{J}_j)^e$$

for $0 \leq j \leq n-s-1$. We conclude that $\dim_{\mathbb{F}_j} \mathbb{F}_j[\boldsymbol{X}]/(\mathcal{J}_j)^e = D$ for $0 \leq j \leq n-s$ and, in particular, that $\#\pi^{-1}(\boldsymbol{p}) = \dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}} = D$, completing the proof. □

Let $J \in \mathbb{K}[\boldsymbol{X}]$ be the Jacobian determinant of $F_1, \ldots, F_s, Y_1, \ldots, Y_{n-s}$ with respect to $X_1, \ldots, X_n$. 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. For simplicity of notations, given $F \in \mathbb{K}[X_1, \ldots, X_n]$ we shall denote by $F(Y_1, \ldots, Y_n)$ or $F(\boldsymbol{Y})$ the element of $\mathbb{K}[Y_1, \ldots, Y_n]$ obtained by rewriting $F(X_1, \ldots, X_n)$ in the variables $Y_1, \ldots, Y_n$.

We shall need the following technical result.

Lemma 4.2. *Let any $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$. Fix i with $1 \leq i \leq s$ and let $\mathcal{I}_i := (F_1, \ldots, F_i) : G^\infty \subset \mathbb{K}[\boldsymbol{X}]$, $V_i := \mathcal{V}(\mathcal{I}_i) \subset \mathbb{A}^n$ and $\mathcal{H}_i := \mathcal{I}_i + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s})$. Denote by $\overline{\mathcal{H}}_i \subset \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$ the image of $\mathcal{H}_i$ under the homomorphism*

$$\begin{array}{rcl} \mathbb{K}[Y_1, \ldots, Y_n] & \to & \mathbb{K}[Y_{n-s+1}, \ldots, Y_n], \\ F(\boldsymbol{Y}) & \mapsto & F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n). \end{array}$$

Assume that the following conditions hold:

- *V_i is equidimensional of dimension $n-i$ and the mapping $\pi_i : V_i \to \mathbb{A}^{n-i}$ defined by $Y_1, \ldots, Y_{n-i}$ is a finite morphism;*
- *there exist $p_{n-s+1}, \ldots, p_{n-i} \in \mathbb{K}$ such that $\boldsymbol{p}^i := (\boldsymbol{p}, p_{n-s+1}, \ldots, p_{n-i}) \in \mathbb{K}^{n-i}$ is a lifting point of π_i.*

Then

- *$\mathcal{H}_i$ and $\overline{\mathcal{H}}_i$ are equidimensional radical ideals of dimension $s-i$ and the varieties $\mathcal{V}(\mathcal{H}_i) \subset \mathbb{A}^n$ and $\mathcal{V}(\overline{\mathcal{H}}_i) \subset \mathbb{A}^{s-i}$ are isomorphic;*
- *if we further assume that $\pi_i^{-1}(\boldsymbol{p}^i) \subset \{G \neq 0\}$, then the lifting fiber $\pi_i^{-1}(\boldsymbol{p}^i)$ intersects each irreducible $\mathbb{K}$-component of $\mathcal{V}(\mathcal{H}_i)$. In particular, G does not vanish identically on any irreducible $\mathbb{K}$-component of $\mathcal{V}(\mathcal{H}_i)$ and*

$$\overline{\mathcal{H}}_i = \big(F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_i(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)\big) : G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)^\infty.$$

Proof. It is easy to see that the mapping

$$\begin{array}{rcl} \mathbb{K}[Y_1, \ldots, Y_n]/\mathcal{H}_i & \to & \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{H}}_i, \\ F(\boldsymbol{Y}) \mod \mathcal{H}_i & \mapsto & F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) \mod \overline{\mathcal{H}}_i, \end{array}$$

is an isomorphism of $\mathbb{K}$–algebras.

Proposition 4.1 shows that $\mathcal{H}_i$ and $\overline{\mathcal{H}}_i$ are radical, equidimensional ideals of dimension $s-i$. Therefore, we have an isomorphism between the coordinate rings of $\mathcal{V}(\mathcal{H}_i)$ and $\mathcal{V}(\overline{\mathcal{H}}_i)$, which proves that $\mathcal{V}(\mathcal{H}_i)$ and $\mathcal{V}(\overline{\mathcal{H}}_i)$ are isomorphic varieties.

Further, by Proposition 4.1 the mapping $\widetilde{\pi} : \mathcal{V}(\mathcal{H}_i) \to \mathbb{A}^{s-i}$ defined by $Y_{n-s+1}, \ldots, Y_{n-i}$ is a finite morphism. Let $\mathcal{C}_1, \ldots, \mathcal{C}_h$ be the irreducible $\mathbb{K}$-components of $\mathcal{V}(\mathcal{H}_i)$. Let $\widetilde{\pi}_{\mathcal{C}_j}$ be the restriction of $\widetilde{\pi}$ to $\mathcal{C}_j$ for $1 \leq j \leq h$. It follows that $\widetilde{\pi}_{\mathcal{C}_j} : \mathcal{C}_j \to \mathbb{A}^{s-i}$ is a finite morphism, and thus $\mathcal{C}_j \cap \widetilde{\pi}^{-1}(p_{n-s+1}, \ldots, p_{n-i}) \neq \emptyset$ for $1 \leq j \leq h$. Since $\widetilde{\pi}^{-1}(p_{n-s+1}, \ldots, p_{n-i}) = \pi_i^{-1}(\boldsymbol{p}^i)$ and $\pi_i^{-1}(\boldsymbol{p}^i) \subset \{G \neq 0\}$, this shows G does not vanish identically on any irreducible $\mathbb{K}$-component of $\mathcal{V}(\mathcal{H}_i)$.

Finally, we prove the assertion about the equality of ideals. We clearly have

$$\overline{\mathcal{H}}_i \subset \big(F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_i(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)\big) : G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)^\infty.$$

To prove the other inclusion, let $F \in \mathbb{K}[Y_1, \ldots, Y_n]$ be such that $F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ belongs to $\big(F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_i(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)\big) : G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)^\infty$. This implies $F \in (F_1, \ldots, F_i, Y - p_1, \ldots, Y_{n-s} - p_{n-s}) : G^\infty$. The fact that G does not vanish identically on any irreducible $\mathbb{K}$-component of $\mathcal{V}(\mathcal{H}_i)$ implies $\mathcal{H}_i = \mathcal{H}_i : G^\infty$. We deduce that $\mathcal{H}_i = (F_1, \ldots, F_i, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}) : G^\infty$. Thus $F \in \mathcal{H}_i$. It follows that $F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) \in \overline{\mathcal{H}}_i$, which completes the proof of the last assertion. □

Let $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ be a lifting point of π. By Proposition 4.1, the zero–dimensional ideal $\mathcal{J} := \mathcal{I} + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}) \subset \mathbb{K}[\boldsymbol{X}]$ 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 a 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

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

According to Proposition 4.1, $\mathcal{K}$ 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 $\boldsymbol{p}^*$.

Let $\overline{\mathcal{J}} \subset \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$ be the image of $\mathcal{J}$ under the homomorphism $\mathbb{K}[Y_1, \ldots, Y_n] \to \mathbb{K}[Y_{n-s+1}, \ldots, Y_n], F(\boldsymbol{Y}) \mapsto F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$. We shall identify $V_{\boldsymbol{p}}$ with the zero–dimensional variety $\mathcal{V}(\overline{\mathcal{J}}) \subset \mathbb{A}^s$. Further, if $\overline{\mathcal{K}} \subset \mathbb{K}[Y_{n-s}, \ldots, Y_n]$ denotes the image of $\mathcal{K}$ under the homomorphism $\mathbb{K}[Y_1, \ldots, Y_n] \to \mathbb{K}[Y_{n-s}, \ldots, Y_n], F(\boldsymbol{Y}) \mapsto F(\boldsymbol{p}^*, Y_{n-s+1}, \ldots, Y_n)$, we shall identify $W_{\boldsymbol{p}^*}$ with the curve $\mathcal{V}(\overline{\mathcal{K}}) \subset \mathbb{A}^{s+1}$. The next result justifies the correctness of these identifications.

Corollary 4.3. *With the previous hypotheses, the following assertions hold:*

- *$\overline{\mathcal{J}}$ is a radical, zero–dimensional ideal 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 D;*
- *$\overline{\mathcal{K}}$ is a radical, equidimensional ideal 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 $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{K}}^e$, where $\overline{\mathcal{K}}^e := \overline{\mathcal{K}}\,\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]$, is a $\mathbb{K}(Y_{n-s})$–vector space of dimension D;*

- *if we further assume that* $V_{\boldsymbol{p}} \subset \{G \neq 0\}$*, then* $V_{\boldsymbol{p}}$ *intersects each irreducible* $\mathbb{K}$*-component of* $W_{\boldsymbol{p}^*}$ *and the following identities hold:*

$$\overline{\mathcal{J}} = (F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)) : G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)^\infty,$$
$$\overline{\mathcal{K}} = (F_1(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n)) : G(\boldsymbol{p}, Y_{n-s}, \ldots, Y_n)^\infty.$$

Proof. The assertions on $\overline{\mathcal{J}}$, $\mathcal{V}(\overline{\mathcal{J}})$, $\overline{\mathcal{K}}$ and $\mathcal{V}(\overline{\mathcal{K}})$ follow from Proposition 4.1 and Lemma 4.2. Since Y_j is integral over $\mathbb{K}[Y_{n-s}]$ modulo $\overline{\mathcal{K}}$ for $n-s+1 \leq j \leq n$, it follows that $Y_{n-s}, \ldots, Y_n$ are in Noether position with respect to $\overline{\mathcal{K}}$. □

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 the 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 of π outside the hypersurface $\{G = 0\}$.

Lemma 4.4. *With the previous hypotheses, 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. □

Finally, assuming that $F_1, \ldots, F_s$ form a regular sequence outside the hypersurface $\{G = 0\}$, 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.

Corollary 4.5. *Assume that* $F_1, \ldots, F_s$ *form a reduced regular sequence of* $\mathbb{K}[\boldsymbol{X}]$ *outside the hypersurface* $\{G = 0\}$ *and the linear forms* $Y_1, \ldots, Y_n$ *are in Noether position with respect to* $V_i := \mathcal{V}\big((F_1, \ldots, F_i) : G^\infty\big)$ *for* $1 \leq i \leq s$*. Further, assume that we are given* $p_{n-s+1}, \ldots, p_{n-1} \in \mathbb{K}$ *such that* $\boldsymbol{p}^i := (\boldsymbol{p}, p_{n-s+1}, \ldots, p_{n-i}) \in \mathbb{K}^{n-i}$ *is a lifting point of the finite morphism* $\pi_i : V_i \to \mathbb{A}^{n-i}$ *defined by* $Y_1, \ldots, Y_{n-i}$ *with* $\pi_i^{-1}(\boldsymbol{p}^i) \subset \{G \neq 0\}$ *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 reduced regular sequence of* $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$ *outside the hypersurface* $\{G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) = 0\}$ *of* $\mathbb{A}^s$*.*

Proof. With the notations of Lemma 4.2, it suffices to show that $\overline{\mathcal{H}_i}$ is a radical ideal of dimension $s-i$ for $1 \leq i \leq s$. Since by assumption $\boldsymbol{p}^i$ is a lifting point of π_i, this follows from the second assertion of the aforesaid lemma. □

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.

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

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

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

$$\begin{aligned}
\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}} &:= S^{-1}\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}],\\
\big(\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]/(P_V)\big)_{\partial P_V/\partial Z_{n-s+1}} &:= S^{-1}\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]/(P_V),\\
\mathbb{K}[V][\mathbf{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}} &:= S^{-1}\mathbb{K}[V][\mathbf{\Lambda}].
\end{aligned}$$

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

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

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

Lemma 4.6. *Φ is an isomorphism of $\mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$–algebras.*

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

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

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

We shall also need the following technical result.

Lemma 4.7. *For any $F \in \mathbb{K}[\boldsymbol{X}]$, let $F_\Lambda \in \mathbb{K}[\mathbf{\Lambda}, \boldsymbol{Z}]$ be any polynomial such that*

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

for some $\eta \in \mathbb{N}$. Then F vanishes on some irreducible component of V if and only if $\mathrm{Res}_{Z_{n-s+1}}(P_V, F_\Lambda) = 0$. Moreover, F vanishes on V if and only if F_Λ is a multiple of P_V. Further, for $1 \le i \le n-s+1$, the following polynomial $H_i \in \mathbb{Z}[\mathbf{\Lambda}, \boldsymbol{Z}]$ is a multiple of P_V:

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

Proof. Suppose that F vanishes on an irreducible component $\mathcal{C}$ of V. Considering (4.4) modulo P_V and applying Φ to both sides, by (4.3) we see that

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

holds in $\mathbb{K}[V][\boldsymbol{\Lambda}]$ and then also in $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. Since $F(\boldsymbol{\xi}) = 0$ in $\mathbb{K}[\mathcal{C}]$ 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 $F_\Lambda(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) = 0$ in $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. It follows that the Chow form $P_\mathcal{C}$ of $\mathcal{C}$ divides F_Λ. Since $P_\mathcal{C}$ is a factor of P_V of positive degree in Z_{n-s+1}, we deduce that $\mathrm{Res}_{Z_{n-s+1}}(P_V, F_\Lambda) = 0$. Conversely, if $\mathrm{Res}_{Z_{n-s+1}}(P_V, F_\Lambda) = 0$, then P_V and F_Λ have a common irreducible factor of positive degree in Z_{n-s+1}. Since this factor is the Chow form $P_\mathcal{C}$ of an irreducible component $\mathcal{C}$ of V, the first assertion of the lemma follows. The proof of the second assertion is similar.

To prove the last assertion, we observe that

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

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. □

The next result, combined with Proposition 4.1, will yield the condition characterizing lifting points we are looking for.

Proposition 4.8. *Let $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} \in \mathbb{K}^{n-s}$ be such that $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. 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 $Y_1, \ldots, Y_{n-s}$. 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 $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, the polynomial $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ is separable. Let $z_1, \ldots, z_\delta \in \overline{\mathbb{K}}$ 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 $\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k) \neq 0$ for $1 \le k \le \delta$, and thus the point

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

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

We claim that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta$ are pairwise distinct and $\pi^{-1}(\boldsymbol{p}) = \{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta\}$. 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 4.7 we have $F_\Lambda(\boldsymbol{\lambda}, \boldsymbol{y}^k) = 0$, and thus $F(\boldsymbol{x}^k) =$

0, for $1 \leq k \leq \delta$. This proves that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta$ belong to V. Further, Lemma 4.7 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 $1 \leq i \leq n-s+1$ and $1 \leq k \leq \delta$. By the definition of $\boldsymbol{x}^k$ it follows that

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

Since $y_i^k = p_i$ for $1 \leq i \leq n-s$, (4.7) implies that $\pi(\boldsymbol{x}^k) = \boldsymbol{p}$ and $z_k = \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{x}^k$ for $1 \leq k \leq \delta$. Since the z_k are pairwise distinct, we deduce that so are the $\boldsymbol{x}^k$. This proves that $\#\pi^{-1}(\boldsymbol{p}) \geq \delta$. 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

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

which concludes the proof of the claim. In particular, $\#\pi^{-1}(\boldsymbol{p}) = \delta$. □

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

Theorem 4.9. *Let $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} \in \mathbb{K}^{n-s}$ be such that $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. Let $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s+1$ 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 $R \hookrightarrow \mathbb{K}[V]$;*
- *$\dim_{R'} B' = \delta$;*
- *$\boldsymbol{p}$ 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, 4.1 and 4.8 we deduce that $\delta = \#\pi^{-1}(\boldsymbol{p}) \leq \dim_{R'} B' \leq \delta$. 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 $1 \leq k \leq n$. Since $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, we conclude that $\mathbb{K}\big[\pi^{-1}(\boldsymbol{p})\big] = \mathbb{K}[\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}]$, which proves that Y_{n-s+1} induces a primitive element of $\pi^{-1}(\boldsymbol{p})$. □

Finally, we give a condition that implies that the lifting fiber $\pi^{-1}(\boldsymbol{p})$ lies outside the hypersurface $\{G = 0\}$. Let $G_\Lambda \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ be the polynomial defined by the identity

$$G\left(-\frac{\partial P_V/\partial \Lambda_{n-s+1,1}}{\partial P_V/\partial Z_{n-s+1}}, \ldots, -\frac{\partial P_V/\partial \Lambda_{n-s+1,n}}{\partial P_V/\partial Z_{n-s+1}}\right) = \frac{G_\Lambda}{(\partial P_V/\partial Z_{n-s+1})^{\deg G}}. \tag{4.8}$$

Since G does not vanish identically on any irreducible component of V, by Lemma 4.7 we see that G_Λ and the resultant $R_V^G := \mathrm{Res}_{Z_{n-s+1}}(P_V, G_\Lambda)$ are both nonzero polynomials.

Lemma 4.10. *With hypotheses and notations as in Proposition 4.8, assume further that $R_V^G(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. Then $\pi^{-1}(\boldsymbol{p}) \subset \{G \neq 0\}$.*

Proof. By hypothesis the resultant

$$R_V^G(\boldsymbol{\lambda}, \boldsymbol{p}) = \mathrm{Res}_{Z_{n-s+1}}\big(P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1}), G_\Lambda(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})\big)$$

is nonzero. Since $P_V(\boldsymbol{\lambda}, \boldsymbol{y}^k) = 0$, it follows that $G_\Lambda(\boldsymbol{\lambda}, \boldsymbol{y}^k) \neq 0$ for $1 \leq k \leq \delta$. By substituting $(\boldsymbol{\lambda}, \boldsymbol{y}^k)$ for $(\boldsymbol{\Lambda}, \boldsymbol{Z})$ in (4.8), we deduce that

$$G(\boldsymbol{x}^k) = \frac{G_{\Lambda,p}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}{(\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k))^{\deg G}}$$

and conclude that $G(\boldsymbol{x}^k) \neq 0$ for $1 \leq k \leq \delta$, which completes the proof. □

4.3. **Kronecker representations from specializations of the Chow form.** Let be given $\boldsymbol{\lambda} := (\lambda_{ij})_{1\leq i\leq n-s+1, 1\leq j\leq n} \in \mathbb{K}^{(n-s+1)n}$ and $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ satisfying the hypotheses of Theorem 4.9. Define $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s+1$, and let $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$, $B := \mathbb{K}[V]$, $R' := \mathbb{K}(Y_1, \ldots, Y_{n-s})$ and $B' := R'[\boldsymbol{X}]/\mathcal{I}^e$, where $\mathcal{I}^e := \mathcal{I}R'[\boldsymbol{X}]$. Further assume that we are 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 an R'-vector space of dimension 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 $P_V \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ be a Chow form of V, and let $A_V \in \mathbb{K}[\boldsymbol{\Lambda}_1, \ldots, \boldsymbol{\Lambda}_{n-s}]$ and $\rho_V \in \mathbb{K}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ be defined as in Section 4.2. By (3.1) and (3.5), we have

$$P_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi}) = 0, \quad \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi})\xi_k + \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi}) = 0 \quad (1 \leq k \leq n), \tag{4.9}$$

in $\mathbb{K}[V][\boldsymbol{\Lambda}]$. 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 $n-s+2 \leq j \leq n$. Substituting $\boldsymbol{\lambda}$ for $\boldsymbol{\Lambda}$ in (4.9) we deduce that

$$Q(Y_{n-s+1}) \in \mathcal{I}, \quad Q'(Y_{n-s+1})Y_j - W_j(Y_{n-s+1}) \in \mathcal{I} \quad (n-s+2 \leq j \leq n), \tag{4.10}$$

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 $n-s+2 \leq j \leq n$. On the other hand, by the choice of $\boldsymbol{\lambda}$, 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 (4.10) 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 $\deg_T W_j \leq \delta - 1$ for $n-s+2 \leq j \leq n$. 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 $\deg_{(Y_1,\ldots,Y_{n-s},T)} W_j \leq \delta$ for $n-s+2 \leq j \leq n$.*

Now, let $\mathcal{J} := \mathcal{I} + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s})$. Denote as in Corollary 4.3 by $\overline{\mathcal{J}}$ the image of $\mathcal{J}$ in $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$ under the homomorphism $F \in \mathbb{K}[\boldsymbol{X}] \mapsto F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$. Substituting $p_1, \ldots, p_{n-s}$ for $Y_1, \ldots, Y_{n-s}$ in (4.10) we obtain

$$Q(\boldsymbol{p}, Y_{n-s+1}) \in \overline{\mathcal{J}}, \;\; Q'(\boldsymbol{p}, Y_{n-s+1}) Y_j - W_j(\boldsymbol{p}, Y_{n-s+1}) \in \overline{\mathcal{J}} \;\; (n-s+2 \leq j \leq n). \tag{4.11}$$

The polynomial $Q(\boldsymbol{p}, T)$ is monic of degree δ and $\deg W_j(\boldsymbol{p}, T) < \delta$ for $n-s+2 \leq j \leq n$. 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 (4.11) shows that the homomorphism of $\mathbb{K}$–algebras

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

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 $\dim_{R'} B'$, and $\dim_{R'} B' = \deg Q(\boldsymbol{p}, T) = \delta$, 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 Corollary 4.3. Then $Y_{n-s}, \ldots, Y_n$ are in Noether position with respect to $\overline{\mathcal{K}}$ and $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{K}}^e$ is a $\mathbb{K}(Y_{n-s})$-vector space of dimension equal to $\dim_{R'} B'$. Substituting $p_1, \ldots, p_{n-s-1}$ for $Y_1, \ldots, Y_{n-s-1}$ in (4.10), we deduce that

$$\begin{gathered} Q(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) \in \overline{\mathcal{K}}, \\ Q'(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) Y_j - W_j(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) \in \overline{\mathcal{K}} \quad (n-s+2 \leq j \leq n). \end{gathered} \tag{4.12}$$

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 $\mathbb{K}(Y_{n-s})[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{K}}^e$. By (4.12) 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 $\dim_{R'} B' = \deg Q(\boldsymbol{p}^*, Y_{n-s}, T) = \delta$, 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 $F_1, \ldots, F_r, G$ in $\mathbb{Z}[\boldsymbol{X}]$ of degree at most d such that $F_1, \ldots, F_r$ define a reduced regular sequence in the open subset $\{G \neq 0\}$ of $\mathbb{A}^n$ and denote $\mathcal{I}_s := (F_1, \ldots, F_s) : G^\infty$, $\mathcal{V}_s := \mathcal{V}(\mathcal{I}_s) = \overline{\mathcal{V}(F_1, \ldots, F_s) \setminus \mathcal{V}(G)}$ 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 $F_1 = 0, \ldots, F_r = 0, G \neq 0$ 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" primes. 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.20). 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 high 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 M any polynomial with integer coefficients, we denote by M_p its reduction modulo p. Further, by $\mathcal{I}_{s,p} \subset \overline{\mathbb{F}}_p[\boldsymbol{X}]$ we denote the ideal $\mathcal{I}_{s,p} := (F_{1,p}, \ldots, F_{s,p}) : G_p^\infty$ and by $\mathcal{V}_{s,p} \subseteq \mathbb{A}^m_{\overline{\mathbb{F}}_p} := \mathbb{A}^m(\overline{\mathbb{F}}_p)$ the variety $\mathcal{V}_{s,p} := \mathcal{V}(\mathcal{I}_{s,p})$ for $1 \leq s \leq r$.

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 $\boldsymbol{\Lambda}\boldsymbol{X} := (\boldsymbol{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \boldsymbol{\Lambda}_{n-s+1} \cdot \boldsymbol{X})$, $\boldsymbol{\Lambda}^* := (\Lambda_{ij})_{1\leq i\leq n-s, 1\leq j\leq n}$ 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 $\boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ $(1 \leq i \leq n-s+1)$, $\boldsymbol{\lambda}\boldsymbol{X}$, $\boldsymbol{\lambda}^*$ 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,

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

According to Lemma 3.2, the polynomials $\partial P_s/\partial Z_{n-s+1}$ and ρ_s are both nonzero. Further, let $G_\Lambda^s \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ be the polynomial defined by the identity

$$G\left(-\frac{\partial P_s/\partial \Lambda_{n-s+1,1}}{\partial P_s/\partial Z_{n-s+1}}, \ldots, -\frac{\partial P_s/\partial \Lambda_{n-s+1,n}}{\partial P_s/\partial Z_{n-s+1}}\right) = \frac{G_\Lambda^s}{(\partial P_s/\partial Z_{n-s+1})^{\deg G}}. \tag{5.1}$$

Since G does not vanish on any irreducible component of $\mathcal{V}_s$, by Lemma 4.7 we see that G_Λ^s and the resultant

$$R_s^G := \mathrm{Res}_{Z_{n-s+1}}(P_s, G_\Lambda^s)$$

are both nonzero polynomials. Further we easily see that

$$\deg(G_\Lambda^s) \leq (n-s+1)\delta_s \deg(G), \quad \deg(R_s^G) \leq (n-s+1)(n-s+2)\delta_s^2 \deg(G). \tag{5.2}$$

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

Lemma 5.1. *Let p be a prime number such that*

$$A_{s,p}(\boldsymbol{\lambda}_p^*)\rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s}) R_{s,p}^G(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s}) \neq 0.$$

Let $Y_{i,p} := \boldsymbol{\lambda}_{i,p} \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s$. If $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ is the mapping defined by $Y_{1,p}, \ldots, Y_{n-s,p}$, then any $\boldsymbol{q} \in \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ with $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) R_{s,p}^G(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$ satisfies $\pi_{s,p}^{-1}(\boldsymbol{q}) \subset \mathcal{V}(F_{1,p}, \ldots, F_{s,p}) \setminus \mathcal{V}(G_p)$ and $\#\pi_{s,p}^{-1}(\boldsymbol{q}) \geq \delta_s$.

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

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

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 $1 \leq k \leq \delta_s$. As $\partial P_{s,p}/\partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) \neq 0$ for $1 \leq k \leq \delta_s$, 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 $1 \leq k \leq \delta_s$.

We claim that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ are pairwise distinct points of $\mathcal{V}(F_{1,p}, \ldots, F_{s,p}) \setminus \mathcal{V}(G_p)$ and $\{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}\} \subset \pi_{s,p}^{-1}(\boldsymbol{q})$. Indeed, let $F_{\Lambda,j} \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ be such that

$$F_j\left(-\frac{\partial P_s/\partial \Lambda_{n-s+1,1}}{\partial P_s/\partial Z_{n-s+1}}, \ldots, -\frac{\partial P_s/\partial \Lambda_{n-s+1,n}}{\partial P_s/\partial Z_{n-s+1}}\right) = \frac{F_{\Lambda,j}}{(\partial P_s/\partial Z_{n-s+1})^{\deg F_j}} \tag{5.3}$$

for $1 \leq j \leq s$. 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 $1 \leq i \leq n-s+1$. Lemma 4.7 shows that $F_{\Lambda,j}$ $(1 \leq j \leq s)$ and H_i $(1 \leq i \leq n-s+1)$ 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 $F_{\Lambda,j,p}$ $(1 \leq j \leq s)$ and $H_{i,p}$ $(1 \leq i \leq n-s+1)$ 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 $1 \leq k \leq \delta_s$, and reducing (5.3) modulo p we deduce that $F_{j,p}(\boldsymbol{x}^k) = 0$ for $1 \leq k \leq \delta_s$. Then following the proof of Proposition 4.8 *mutatis mutandis* we conclude that $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ are pairwise distinct points of $\mathcal{V}(F_{1,p}, \ldots, F_{s,p})$ such that $(Y_{1,p}(\boldsymbol{x}^k), \ldots, Y_{n-k,p}(\boldsymbol{x}^k)) = \boldsymbol{q}$.

It remains to prove that $G_p(\boldsymbol{x}^k) \neq 0$ for $1 \leq k \leq \delta_s$. To do this, note that the resultant

$$R_{s,p}^G(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \mathrm{Res}_{Z_{n-s+1}}\left(P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1}), G_{\Lambda,p}^s(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})\right)$$

is not zero. Since $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$, it follows that $G_{\Lambda,p}^s(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) \neq 0$ for $1 \leq k \leq \delta_s$. By reducing modulo p and substituting $(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)$ for $(\boldsymbol{\Lambda}, \boldsymbol{Z})$ in (5.1), we deduce that

$$G_p(\boldsymbol{x}^k) = \frac{G_{\Lambda,p}^s(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}{(\partial P_s/\partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k))^{\deg G}} \neq 0$$

for $1 \leq k \leq \delta_s$, which completes the proof. □

We see that $GP_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X}) \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{X}]$ vanishes on the set $\mathbb{A}^{(n-s+1)n} \times \mathcal{V}(F_1, \ldots, F_s)$ of common zeros 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

$$\alpha_s(GP_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X}))^{\mu_s} \in (F_1, \ldots, F_s)\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{X}]. \tag{5.4}$$

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*

$$\alpha_{s,p} A_{s,p}(\boldsymbol{\lambda}_p^*) \rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s}) R_{s,p}^G(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s}) \neq 0.$$

Let $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s$. Then:

1. *$\mathcal{V}_{s,p}$ is equidimensional of dimension $n-s$;*
2. *the mapping $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}_{\mathbb{F}_p}^{n-s}$ 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 $Y_{n-s+1},\dots,Y_n \in \mathbb{Z}[\boldsymbol{X}]$ such that $Y_{1,p},\dots,Y_{n,p}$ 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

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

From (5.4) we see that $\alpha_s(GQ_k(Y_1,\dots,Y_{n-s},Y_{n-s+k}))^{\mu_s} \in (F_1,\dots,F_s)\mathbb{Z}[\boldsymbol{X}]$ and reducing modulo p we obtain

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

for $1 \le k \le s$. This implies that

$$\alpha_{s,p}(Q_{k,p}(Y_{1,p},\dots,Y_{n-s,p},Y_{n-s+k,p}))^{\mu_s} \in \mathcal{I}_{s,p} \tag{5.5}$$

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 (5.5) may be interpreted as an integral dependence relation for $Y_{n-s+k,p}$ over $\overline{\mathbb{F}}_p[Y_{1,p},\dots,Y_{n-s,p}]$ modulo $\mathcal{I}_{s,p}$. Further, since $\overline{\mathbb{F}}_p[Y_{1,p},\dots,Y_{n,p}] = \overline{\mathbb{F}}_p[\boldsymbol{X}]$, we conclude that $\overline{\mathbb{F}}_p[Y_{1,p},\dots,Y_{n-s,p}] \to \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$ is an integral ring extension. In particular, we have $\dim \mathcal{V}_{s,p} \le n-s$. Moreover, by the choice of p and Lemma 5.1 the variety $\mathcal{V}_{s,p} = \mathcal{V}(\mathcal{I}_{s,p})$ is nonempty. Therefore, $\mathcal{I}_{s,p}$ is a proper ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$. This implies that $(F_{1,p}\dots,F_{s,p})$ is a proper ideal. By the Principal Ideal Theorem (see, e.g., [11, Theorem 10.2]) every irreducible component of $\mathcal{V}(F_{1,p}\dots,F_{s,p})$ has dimension at least $n-s$. Then every irreducible component of $\mathcal{V}_{s,p}$ has dimension at least $n-s$. We conclude that $\mathcal{V}_{s,p}$ is equidimensional of dimension $n-s$. This shows the first assertion. On the other hand, since the ring extension $\overline{\mathbb{F}}_p[Y_{1,p},\dots,Y_{n-s,p}] \to \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$ is integral and $\dim \mathcal{V}_{s,p} = n-s$, it follows that $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ is a finite morphism, which finishes the proof. □

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 (5.4) we see that $(G_pP_{s,p}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X}))^{\mu_s} \in (F_{1,p},\dots,F_{s,p})\mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{X}]$. This implies that $P_{s,p}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})$ vanishes on $\mathbb{A}^{(n-s+1)n}_{\overline{\mathbb{F}}_p} \times \mathcal{V}_{s,p}$. 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

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

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 $(Z_i, \Lambda_{i1}, \dots, \Lambda_{in})$ 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 $\mathcal{V}_{s,p}$. □

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 $A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})R_s^G(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. By Theorem 4.9 and Lemma 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 $Y_1, \ldots, Y_{n-s}$ such that $\pi_s^{-1}(\boldsymbol{p}) \subset \{G \neq 0\}$. Let J_s be the Jacobian determinant of $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ with respect to $X_1, \ldots, X_n$. Lemma 4.4 then implies that G vanishes on the common zeros in $\mathbb{A}^n$ of $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ and J_s. By the Nullstellensatz, there exist $\gamma_s \in \mathbb{Z}\backslash\{0\}$, $\nu_s \in \mathbb{N}$ and $G_1, \ldots, G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ such that

$$\gamma_s G^{\nu_s} = G_1F_1 + \cdots + G_sF_s + G_{s+1}(Y_1 - p_1) + \cdots + G_n(Y_{n-s} - p_{n-s}) + G_{n+1}J_s. \tag{5.6}$$

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

Proposition 5.4. *With the previous hypotheses and notations, let p be a prime number such that $p \nmid \alpha_s\gamma_s A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})R_s^G(\boldsymbol{\lambda}, \boldsymbol{p})$. Then $\mathcal{I}_{s,p}$ is a radical ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$.*

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 $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ defined by $Y_{1,p}, \ldots, Y_{n-s,p}$ is a finite morphism. On the other hand, reducing (5.6) modulo p we see that

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

holds in $\mathbb{F}_p[\boldsymbol{X}]$. Further, by Corollary 5.3 we have that $P_{s,p}$ is the Chow form of $\mathcal{V}_{s,p}$. Then Lemma 5.1 shows that $\pi_{s,p}^{-1}(\boldsymbol{p}) \subset \mathcal{V}(F_{1,p}, \ldots, F_{s,p}) \setminus \mathcal{V}(G_p)$. This and the previous identity imply 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, $\mathcal{C}_i \cap \pi_{s,p}^{-1}(\boldsymbol{p}_p) \neq \emptyset$ 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 $\mathcal{J} \subset \overline{\mathbb{F}}_p[\boldsymbol{X}]$ be the ideal generated by $\mathcal{I}_{s,p}$ 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 $\mathcal{P}_i \subset \overline{\mathbb{F}}_p[\boldsymbol{X}]$ 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 $\mathcal{I}_{s,p}$. 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 $\mathcal{I}_{s,p}$ is a radical ideal. □

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 $A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})R_s^G(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$ and let p be a prime number such that $p \nmid \alpha_s\gamma_s A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})R_s^G(\boldsymbol{\lambda}, \boldsymbol{p})$, where α_s and γ_s are the integers of* (5.4) *and* (5.6) *respectively. Let $Y_{i,p} := \boldsymbol{\lambda}_{i,p} \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s+1$, $R_{s,p} := \overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}]$, $R'_{s,p} := \overline{\mathbb{F}}_p(Y_{1,p}, \ldots, Y_{n-s,p})$ and $B'_{s,p} := R'_{s,p}[\boldsymbol{X}]/\mathcal{I}^e_{s,p}$, where $\mathcal{I}^e_{s,p} := \mathcal{I}_{s,p}R'_{s,p}[\boldsymbol{X}]$. Then the following conditions hold:*

- *$\mathcal{I}_{s,p}$ is radical ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ and defines an equidimensional variety $\mathcal{V}_{s,p} \subset \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ of dimension $n - s$ and degree δ_s;*
- *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 $Y_{n-s+1,p}$ induces a primitive element of the ring extension $R_{s,p} \hookrightarrow \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$;*
- *$\dim_{R'_{s,p}} B'_{s,p} = \delta_s$;*

- *any* $\boldsymbol{q} \in \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ *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* $\pi^{-1}_{s,p}(\boldsymbol{q})$. *For* $\boldsymbol{q} := \boldsymbol{p}_p$, *we also have* $\pi^{-1}_{s,p}(\boldsymbol{p}_p) \subset \{G_p \neq 0\}$.

Proof. The first assertion follows by Proposition 5.2, Corollary 5.3 and Proposition 5.4. Since $P_{s,p}$ is a Chow form of $\mathcal{V}_{s,p}$ by Corollary 5.3, the last three assertions are consequence of Theorem 4.9 and Lemma 4.10 applied to $\mathbb{K} = \overline{\mathbb{F}}_p$. □

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 Kronecker representation of the fiber $\pi^{-1}_{s+1}(\boldsymbol{p}^*)$ from one of the lifting curve $W_{\boldsymbol{p}^*}$. As the Kronecker representation 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 $\pi^{-1}_{s+1}(\boldsymbol{p}^*)$ 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* $\mathsf{R}_s \in \overline{\mathbb{Q}}[\boldsymbol{\Lambda}] \setminus \{0\}$ *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

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

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., [39, §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 $\rho_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}^* \boldsymbol{z}_i)$ is a nonzero polynomial in $\overline{\mathbb{Q}}[\boldsymbol{\Lambda}]$ for $1 \leq i \leq h$ and therefore $\mathsf{R}_s \in \overline{\mathbb{Q}}[\boldsymbol{\Lambda}] \setminus \{0\}$. Since $\deg \rho_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}^* \boldsymbol{z}_i) \leq (n-s+2)(2\delta_s - 1)\delta_s$ 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 $1 \leq i \leq h$. □

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

$$\mathcal{W}_{\boldsymbol{\lambda}^s} := \mathcal{V}_{s+1} \cap \{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\}. \tag{5.7}$$

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 $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) \in \mathbb{Z}[\boldsymbol{X}]$. Since G vanishes on $\mathcal{V}(F_1, \ldots, F_{s+1}) \cap \{\rho_{\boldsymbol{\lambda}^s} = 0\}$, by the Nullstellensatz there exists $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ and $\nu_{\boldsymbol{\lambda}^s} \in \mathbb{N}$ satisfying

$$\mu_{\boldsymbol{\lambda}^s} G^{\nu_{\boldsymbol{\lambda}^s}} \in (F_1, \ldots, F_{s+1}, \rho_{\boldsymbol{\lambda}^s})\mathbb{Z}[\boldsymbol{X}]. \tag{5.8}$$

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 [7, 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

$$B_{\boldsymbol{\lambda}^s}\big(Y_1(\boldsymbol{x}), \ldots, Y_{n-s-1}(\boldsymbol{x})\big) = 0 \tag{5.9}$$

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

$$\deg B_{\boldsymbol{\lambda}^s} \leq 2(n-s+2)\delta_s^2 \delta_{s+1}. \tag{5.10}$$

As $GB_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})$ vanishes on $\mathcal{V}(F_1, \ldots, F_{s+1}) \cap \{\rho_{\boldsymbol{\lambda}^s} = 0\}$, by the Nullstellensatz there exist $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ and $\ell_{\boldsymbol{\lambda}^s} \in \mathbb{N}$ such that

$$\beta_{\boldsymbol{\lambda}^s}\big(GB_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})\big)^{\ell_{\boldsymbol{\lambda}^s}} \in (F_1, \ldots, F_{s+1}, \rho_{\boldsymbol{\lambda}^s})\mathbb{Z}[\boldsymbol{X}]. \tag{5.11}$$

Next we deal with a technical condition which allows us to ensure that no points of the lifting fibers at each step of the algorithm lies in the hypersurface $\{G = 0\}$. For this purpose, consider the following morphism:

$$\begin{aligned} \Phi_s : (\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s) \cap \{A_s \neq 0\} &\to \mathbb{A}^{(n-s+1)n} \times \mathbb{A}^{n-s} \cap \{A_s \neq 0\}, \\ (\boldsymbol{\lambda}, \boldsymbol{x}) &\mapsto (\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{x}) \end{aligned} \tag{5.12}$$

According to Proposition 3.4, the fiber $\Phi_s^{-1}(\boldsymbol{y})$ is finite for $\boldsymbol{y} \in \mathbb{A}^{(n-s+1)n} \times \mathbb{A}^{n-s} \cap \{A_s \neq 0\}$. Further, since the hypersurface $\{G = 0\} \subset \mathbb{A}^n$ intersects properly each irreducible component of $\mathcal{V}_s$, the $\mathbb{Q}$-variety $(\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s) \cap \{G = 0\}$ is equidimensional of dimension $(n-s+1)(n+1)-1$. Thus, by the Theorem on the dimension of fibers (see, e.g, [3, Satz 11.14]) it follows that the Zariski closure $\overline{\Phi_s(\{G = 0\})}$ in $\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^{n-s}$ of the image of $(\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s) \cap \{G = 0, A_s \neq 0\}$ is a hypersurface of $\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^{n-s}$. Let $B_s^G \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ be a primitive and squarefree polynomial defining $\overline{\Phi_s(\{G = 0\})}$. By [7, Theorem 3.24] we have the degree estimates

$$\deg_{\Lambda_{ij}}(B_s^G), \deg_{Z_k}(B_s^G) \leq 2^{n-s}\delta_s \deg(G) \tag{5.13}$$

for $1 \leq i \leq n-s+1$, $1 \leq j \leq n$ and $1 \leq k \leq n-s$.

Fix $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ with $A_s(\boldsymbol{\lambda}^*) \neq 0$ and set $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \leq i \leq n-s$. By construction, the polynomial $B_s^G(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}) \in \mathbb{Z}[\boldsymbol{X}]$ vanishes on $\mathcal{V}_s \cap \{G = 0\}$. Since $\mathcal{V}_s$ is equidimensional, by the Nullstellensatz [7, Theorem 0.2] there exist $\beta_{\boldsymbol{\lambda}^s}^G \in \mathbb{Z} \setminus \{0\}$, $\mu_{\boldsymbol{\lambda}^s}^G \in \mathbb{N}$ and $H_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[\boldsymbol{X}]$ such that

$$\beta_{\boldsymbol{\lambda}^s}^G B_s^G(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})^{\mu_{\boldsymbol{\lambda}^s}^G} - H_{\boldsymbol{\lambda}^s} G = 0 \text{ on } \mathcal{V}_s. \tag{5.14}$$

We deduce that $G\big(\beta_{\boldsymbol{\lambda}^s}^G B_s^G(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})^{\mu_{\boldsymbol{\lambda}^s}^G} - H_{\boldsymbol{\lambda}^s} G\big)$ vanishes on $\mathcal{V}(F_1, \ldots, F_s)$. Again, by the Nullstellensatz, there exist $\gamma_{\boldsymbol{\lambda}^s}^G \in \mathbb{Z} \setminus \{0\}$ and $\nu_{\boldsymbol{\lambda}^s}^G \in \mathbb{N}$ such that

$$\gamma_{\boldsymbol{\lambda}^s}^G \Big(G\big(\beta_{\boldsymbol{\lambda}^s}^G B_s^G(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})^{\mu_{\boldsymbol{\lambda}^s}^G} - H_{\boldsymbol{\lambda}^s} G\big)\Big)^{\nu_{\boldsymbol{\lambda}^s}^G} \in (F_1, \ldots, F_s)\mathbb{Z}[\boldsymbol{X}]. \tag{5.15}$$

Let $\widehat{B}_s := \mathrm{Res}_{Z_{n-s}}\big(B_s^G, P_{s+1}\big) \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s-1}]$.

Lemma 5.7. *$\widehat{B}_s$ is nonzero of degree at most $(n-s+1)^2(n+1)2^{n-s}\delta_s\delta_{s+1}\deg(G)$.*

Proof. Let $(\boldsymbol{\lambda}, \boldsymbol{p}) \in \mathbb{Z}^{(n-s+1)(n+1)}$ be such that $(A_s A_{s+1}\rho_s\rho_{s+1})(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. By Theorem 4.9 the following conditions hold:

- the mapping $\pi_s := (Y_1, \ldots, Y_{n-s}) : \mathcal{V}_s \to \mathbb{A}^{n-s}$ is a finite morphism, $\boldsymbol{p} := (p_1, \ldots, p_{n-s})$ is a lifting point of π_s and Y_{n-s+1} is a primitive element of $\pi_s^{-1}(\boldsymbol{p})$;
- the mapping $\pi_{s+1} := (Y_1, \ldots, Y_{n-s-1}) : \mathcal{V}_{s+1} \to \mathbb{A}^{n-s-1}$ is a finite morphism, $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$ is a lifting point of π_{s+1} and Y_{n-s} is a primitive element of $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$.

Since $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ is a finite morphism, $W_{\boldsymbol{p}^*} := \pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1)$ is of pure dimension 1 (and degree at most $\delta_s := \deg \mathcal{V}_s$). Observe that $\pi_s^{-1}(\boldsymbol{p}) = \pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1) \cap \{Y_{n-s} = p_{n-s}\}$ is a zero-dimensional linear section of $\pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1)$. The fact that $\boldsymbol{p} \in \mathbb{Z}^{n-s}$ is a lifting point of π_s with $\pi_s^{-1}(\boldsymbol{p}) \subset \{G \neq 0\}$ implies that $\pi_s^{-1}(\boldsymbol{p})$ intersects each irreducible component of $\pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1)$ (see Corollary 4.3). As $\pi_s^{-1}(\boldsymbol{p}) \subset \{G \neq 0\}$, we see that $\pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1) \cap \{G = 0\}$ is of dimension at most 0. In particular, a generic linear form Y_{n-s} separates the points of $\pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1) \cap \{G = 0\}$ from those of $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$.

We claim that $B_s^G \in k[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ and the Chow form $P_{s+1} \in \mathbb{Z}[\boldsymbol{\Lambda}^*, Z_1, \ldots, Z_{n-s}]$ cannot have a nontrivial common factor in $\mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s-1}][Z_{n-s}]$. Indeed, assume that $Q \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s-1}]Z_{n-s}]$ is such a factor. Clearly, a generic linear form Y_{n-s} separates the points of $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$. Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\delta_{s+1}}$ denote these points. Then the roots of the univariate polynomial $P_{s+1}(\boldsymbol{\lambda}^*, \boldsymbol{p}^*, Z_{n-s})$ are precisely the values $Y_{n-s}(\boldsymbol{x}_1), \ldots, Y_{n-s}(\boldsymbol{x}_{\delta_{s+1}})$. It follows that $Q(\boldsymbol{\lambda}, \boldsymbol{p}^*, Y_{n-s}(\boldsymbol{x}_j)) = 0$ for some $1 \leq j \leq \delta_{s+1}$. Thus $B_s^G(\boldsymbol{\lambda}, \boldsymbol{p}^*, Y_{n-s}(\boldsymbol{x}_j)) = 0$. On the other hand, taking into account the definition of A_s it can be easily shown that Φ_s is a finite morphism and therefore a closed map (see, e.g., [3, Satz 9.27]). In particular, $\Phi_s(\{G = 0\})$ is a closed subset of $(\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^{n-s}) \cap \{A_s \neq 0\}$. Further, it is easy to see that

$$\Phi_s(\{G = 0\}) = \overline{\Phi_s(\{G = 0\})} \cap \{A_s \neq 0\} = \{B_s^G = 0\} \cap \{A_s \neq 0\},$$

where $\overline{\Phi_s(\{G = 0\})}$ denotes the Zariski closure of $\Phi_s(\{G = 0\})$ in $\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^{n-s}$. Since $(\boldsymbol{\lambda}, \boldsymbol{p}^*, Y_{n-s}(\boldsymbol{x}_j)) = \Phi_s(\boldsymbol{\lambda}, \boldsymbol{x}_j) \in \{B_s^G = 0\} \cap \{A_s \neq 0\}$, we see that $(\boldsymbol{\lambda}, \boldsymbol{p}^*, Y_{n-s}(\boldsymbol{x}_j)) = \Phi_s(\boldsymbol{\lambda}, \boldsymbol{y})$ for some $(\boldsymbol{\lambda}, \boldsymbol{y}) \in (\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s) \cap \{A_s \neq 0\} \cap \{G = 0\}$. Thus we have $\boldsymbol{y} \in \pi_s^{-1}(\{\boldsymbol{p}^*\} \times \mathbb{A}^1) \cap \{G = 0\}$ with $Y_{n-s}(\boldsymbol{y}) = Y_{n-s}(\boldsymbol{x}_j)$. This contradicts the hypotheses on Y_{n-s} and proves the claim.

It follows that $\widehat{B}_s$ is nonzero. Since

$$\deg(\widehat{B}_s) \leq \deg_{Z_{n-s}}(P_{s+1}) \deg(B_s^G) + \deg_{Z_{n-s}}(B_s^G) \deg(P_{s+1}),$$

the upper bound for the degree of the lemma readily follows from (5.13) and the upper bound for the degree P_{s+1}. □

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

$$\mathsf{M}_s := \alpha_s \gamma_s A_s(\mathbf{\Lambda}^*) \rho_s(\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}) R_s^G(\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}), \tag{5.16}$$

where α_s and γ_s are the integers of (5.4) and (5.6) respectively. Taking into account (5.2) we observe that

$$\deg \mathsf{M}_s \leq (n-s+2)^2 d \delta_s^2. \tag{5.17}$$

Further, let $\mathsf{C}_s \in \mathbb{Z}[\mathbf{\Lambda}]$ be a nonzero coefficient of $\mathsf{M}_s \mathsf{M}_{s+1} \in \mathbb{Z}[\mathbf{\Lambda}][Z_1, \ldots, Z_{n-s}]$. 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

$$\mathsf{L}_{\boldsymbol{\lambda}^s} := \begin{cases} \mu_{\boldsymbol{\lambda}^s} & \text{if } \mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset, \\ \beta_{\boldsymbol{\lambda}^s} B_{\boldsymbol{\lambda}^s} & \text{if } \mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset, \end{cases} \tag{5.18}$$

where $\mu_{\boldsymbol{\lambda}^s}$, $B_{\boldsymbol{\lambda}^s}$ and $\beta_{\boldsymbol{\lambda}^s}$ are defined as in (5.8), (5.11) and (5.9). Further let $\mathsf{B}_{\boldsymbol{\lambda}^s}^G \in \mathbb{Z}[Z_1, \ldots, Z_{n-s-1}] \setminus \{0\}$ be the polynomial

$$\mathsf{B}_{\boldsymbol{\lambda}^s}^G := \beta_{\boldsymbol{\lambda}^s}^G \gamma_{\boldsymbol{\lambda}^s}^G \widehat{B}_s(\boldsymbol{\lambda}^s, Z_1, \ldots, Z_{n-s-1}), \tag{5.19}$$

where $\beta_{\boldsymbol{\lambda}^s}^G$ and $\gamma_{\boldsymbol{\lambda}^s}^G$ are defined as in (5.15) and $\widehat{B}_s$ is the polynomial of Lemma 5.7. Finally, define

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

Theorem 5.8. *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. *$\mathcal{I}_{s,p}$ is a radical ideal of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ and defines an equidimensional variety $\mathcal{V}_{s,p} \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ of dimension $n-s$ and degree δ_s. The same holds for $\mathcal{I}_{s+1,p}$ and $\mathcal{V}_{s+1,p}$;*
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, $\boldsymbol{p}_p \in \mathbb{F}_p^{n-s}$ is a lifting point of $\pi_{s,p}$ with $\pi_s^{-1}(\boldsymbol{p}) \subset \{G_p \neq 0\}$ and $Y_{n-s+1,p}$ induces a primitive element of $\pi_{s,p}^{-1}(\boldsymbol{p}_p)$;*
3. *the mapping $\pi_{s+1,p} : \mathcal{V}_{s+1,p} \to \mathbb{A}^{n-s-1}_{\overline{\mathbb{F}}_p}$ 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 $\pi_{s+1,p}$ with $\pi_{s+1}^{-1}(\boldsymbol{p}^*) \subset \{G_p \neq 0\}$ 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 $\pi_{s,p}^{-1}(\boldsymbol{q})$;*
5. *no point of $\pi_{s,p}(W_{\boldsymbol{p}^*} \cap \{G_p = 0\})$ belongs to $\pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big)$.*

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 assertion (4), 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 (5.7) is empty. Considering (5.8) 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 ideal (G_p) of $\overline{\mathbb{F}}_p[\boldsymbol{X}]$. As $\boldsymbol{x} \in \pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$ and $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*) \subset \{G_p \neq 0\}$, 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 (5.11) modulo p and taking into account that $p \nmid \beta_{\boldsymbol{\lambda}^s}$ we see that

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

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 $\pi_{s,p}^{-1}(\boldsymbol{q})$.

Finally, to prove condition (5) we note that, since $\widehat{B}_s \in (B_s^G, P_{s+1})\mathbb{Z}[\boldsymbol{\Lambda}, Z_1,\ldots,Z_{n-s}]$, we have $\widehat{B}_{s,p} \in (B_{s,p}^G, P_{s+1,p})\mathbb{F}_p[\boldsymbol{\Lambda}, Z_1,\ldots,Z_{n-s}]$. Since $\widehat{B}_{s,p}(\boldsymbol{\lambda}_p,\boldsymbol{p}_p^*) \neq 0$, we deduce that the polynomials $B_{s,p}^G(\boldsymbol{\lambda}_p,\boldsymbol{p}_p^*,Z_{n-s})$ and $P_{s+1,p}(\boldsymbol{\lambda}_p^*,\boldsymbol{p}_p^*,Z_{n-s})$ have no common roots in $\overline{\mathbb{F}}_p$. Since $P_{s+1,p}$ is a Chow form of $\mathcal{V}_{s+1,p}$ by Corollary 5.3, we have $P_{s+1,p}(\boldsymbol{\lambda}_p^*,\boldsymbol{q}) = 0$ for any $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big)$. Thus, for any such point $\boldsymbol{q}$ we have $B_{s,p}^G(\boldsymbol{\lambda}_p,\boldsymbol{q}) \neq 0$. Considering (5.15) modulo p we have

$$\gamma_{\boldsymbol{\lambda}^s,p}^G\Big(G_p\big(\beta_{\boldsymbol{\lambda}^s,p}^G B_{s,p}^G(\boldsymbol{\lambda}_p,Y_{1,p},\ldots,Y_{n-s,p})^{\mu_{\boldsymbol{\lambda}^s}^G} - H_{\boldsymbol{\lambda}^s,p}G_p\big)\Big)^{\nu_{\boldsymbol{\lambda}^s}^G} \in (F_{1,p},\ldots,F_{s,p})\mathbb{F}_p[\boldsymbol{X}],$$

which implies

$$\gamma_{\boldsymbol{\lambda}^s,p}^G\Big(\beta_{\boldsymbol{\lambda}^s,p}^G\big(B_{s,p}^G(\boldsymbol{\lambda}_p,Y_{1,p},\ldots,Y_{n-s,p})\big)^{\mu_{\boldsymbol{\lambda}^s}^G} - H_{\boldsymbol{\lambda}^s,p}G_p\Big)^{\nu_{\boldsymbol{\lambda}^s}^G} \in \mathcal{I}_{s,p}.$$

This, together with $B_{s,p}^G(\boldsymbol{\lambda}_p,\boldsymbol{q}) \neq 0$, readily implies that $\boldsymbol{q} \notin \pi_{s,p}\big(W_{\boldsymbol{p}_p^*} \cap \{G_p = 0\}\big)$. □

Remark 5.9. *With hypotheses as in Theorem 5.8, 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 5.8 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 $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1\leq i\leq n,1\leq j\leq n}$ denote a set of n^2 indeterminates over $\mathbb{Q}$. For $1 \leq s \leq r$, we write $\boldsymbol{\Lambda}^s := (\Lambda_{ij})_{1\leq i\leq n,1\leq j\leq n-s+1}$. Further, for $\boldsymbol{\lambda} := (\lambda_{ij})_{1\leq i\leq n,1\leq j\leq n} \in \mathbb{Z}^{n^2}$, we denote $\boldsymbol{\lambda}^s := (\lambda_{ij})_{1\leq i\leq n-s+1,1\leq j\leq n}$. Let $\mathsf{R} \in \overline{\mathbb{Q}}[\boldsymbol{\Lambda}] \setminus \{0\}$ be the polynomial defined by

$$\mathsf{R} := \prod_{s=1}^{r-1} \mathsf{C}_s\mathsf{R}_s. \tag{5.20}$$

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

$$\mathsf{N}_{\boldsymbol{\lambda}} := \mathsf{M}_r(\boldsymbol{\lambda}^r, Z_1,\ldots,Z_{n-r}) \prod_{s=1}^{r-1} \mathsf{M}_s(\boldsymbol{\lambda}^s, Z_1,\ldots,Z_{n-s})\mathsf{L}_{\boldsymbol{\lambda}^s}(Z_1,\ldots,Z_{n-s-1})\mathsf{B}_{\boldsymbol{\lambda}^s}^G(Z_1,\ldots,Z_{n-s-1}). \tag{5.21}$$

Since $\deg(\mathsf{B}^G_{\boldsymbol{\lambda}^s}) \leq \deg(\widehat{B}_s)$, taking into account Lemma 5.7 and (5.10) we deduce that

$$\begin{aligned}\deg \mathsf{N}_{\boldsymbol{\lambda}} &\leq \sum_{s=1}^{r} \deg \mathsf{M}_s + \sum_{s=1}^{r-1} \big(\deg(\mathsf{L}_{\boldsymbol{\lambda}^s}) + \deg(\widehat{B}_s)\big)\\ &\leq D := r(n+1)((n+1)d\delta^2 + 2\delta^3 + n^2 2^{n-s} d\delta^2).\end{aligned}$$

Since $\deg \mathsf{C}_s \leq \deg \mathsf{M}_s + \deg \mathsf{M}_{s+1}$, taking into account (5.17) and the estimate for the degree of R_s of Lemma 5.6, we easily deduce that

$$\deg \mathsf{R} \leq D. \tag{5.22}$$

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 $1 \leq s \leq r$. With hypotheses as above we easily obtain the following result.

Theorem 5.10. *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 $1 \leq i \leq n$. 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)–(5) of Theorem 5.8 are satisfied for $1 \leq s \leq r-1$ 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 $\{G_p \neq 0\}$.*

In the sequel, a prime p as in Theorem 5.10 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 5.10, 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 4.9 the following conditions are satisfied:

- $Y_1, \ldots, Y_{n-s}$ are in Noether position with respect 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 $\mathcal{I}_s := (F_1, \ldots, F_s) : G^\infty$ 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 Proposition 4.1, $\mathcal{J}_s$ 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 Corollary 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 $\operatorname{rank}_{R_s}\mathbb{Q}[\mathcal{V}_s]$.

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

$$Q^s := \frac{P_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T)}{A_s(\boldsymbol{\lambda}^{s+1})}, \quad W^s_j := -\sum_{k=1}^{n} \frac{\lambda_{jk}}{A_s(\boldsymbol{\lambda}^{s+1})} \frac{\partial P_s}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T) \tag{5.23}$$

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 5.11. *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 5.10. 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 $\mathcal{I}_{s,p} := (F_{1,p}, \ldots, F_{s,p}) : G_p^\infty$ 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 5.10 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 $\mathcal{V}_{\boldsymbol{p}^s_p}$ and the lifting curve $\mathcal{W}_{\boldsymbol{p}^{s+1}_p}$ respectively. Since $p \nmid A_s(\boldsymbol{\lambda}^{s+1})$, the polynomials $Q^s_p, W^s_{1,p}, \ldots, W^s_{n,p} \in \mathbb{F}_p[T]$ are well–defined, and we have the following result.

Proposition 5.12. *The following assertions hold:*

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

Proof. From (5.23) we deduce that

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

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

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. □

6. Computation of a Kronecker representation

Let $F_1, \ldots, F_r, G \in \mathbb{Z}[\boldsymbol{X}]$ 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 $\mathbb{Q}$-definable fiber $\pi_r^{-1}(\boldsymbol{p}^r)$ of $\mathcal{V}_r := \mathcal{V}(\mathcal{I}_r)$, where $\mathcal{I}_r := (F_1, \ldots, F_r) : G^\infty$. For this purpose, following the approach of [21], we perform this computation modulo a prime number p and apply p–adic lifting to recover the integers coefficients of the polynomials defining a Kronecker representation of $\pi_r^{-1}(\boldsymbol{p}^r)$. Assuming that a "lucky" prime p is given, the complexity of computing

a Kronecker representation of a zero–dimensional fiber of $\mathcal{V}((F_{1,p},\ldots,F_{r,p}) : G_p^\infty)$ was analyzed in [5]. On the other hand, the complexity of the p–adic lifting step was analyzed in [21]. 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 6.9).

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 $\mathsf{b} := \lfloor 9\mathsf{D} \rfloor$. Assume that we have randomly chosen $(\boldsymbol{\lambda},\boldsymbol{p}) \in \mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$ such that $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ and $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$. 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 $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ and $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$ is greater than $\frac{7}{9}$.*

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

For such a choice of $\boldsymbol{\lambda}$ and $\boldsymbol{p}$, let $\mathfrak{N}$ be the integer of Theorem 5.10. According to Theorem A.20, there exists an integer $\mathfrak{H}$ such that

$$h(\mathfrak{N}) \leq \mathfrak{H} \quad \text{and} \quad \log \mathfrak{H} \in \mathcal{O}^\sim\big(\log(d^r 2^n h)\big). \tag{6.1}$$

We shall further assume that $\mathfrak{H} \geq 5n^2 d\delta^4$. 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 $\mathcal{O}^\sim\big(\log^2(d^r 2^n h)\big)$ bit operations and returns a correct 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). □

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 $F_{1,p},\ldots,F_{r,p},G_p$. Since $\mathfrak{H} \geq 5n^2 d\delta^4$, we can assume that $p > 60n^2 d\delta^4$. Thus we can use the algorithm of [5] 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 defined by the Zariski closure of $\{F_{1,p} = 0\} \setminus \{G_p = 0\}$, with $Y_{n,p}$ as primitive element. Observe that such a hypersurface is defined by the polynomial $F_{1,p}^* := F_{1,p}/\gcd(F_{1,p},G_p)$. According to Corollary 4.3, we have

$$V_{\boldsymbol{p}_p^1} = \mathcal{V}(\overline{\mathcal{J}}_{1,p}), \quad \overline{\mathcal{J}}_{1,p} = \big(F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p})\big) : G_p(\boldsymbol{p}_p^1, Y_{n,p})^\infty = \Big(\tfrac{F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p})}{\gcd(F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p}), G_p(\boldsymbol{p}_p^1, Y_{n,p}))}\Big).$$

It follows that $F_{1,p}^*(\boldsymbol{p}_p^1, T) = F_{1,p}(\boldsymbol{p}_p^1, T)/\gcd(F_{1,p}(\boldsymbol{p}_p^1, T), G_p(\boldsymbol{p}_p^1, T))$.

By Proposition 5.12, the Kronecker representation of $V_{\boldsymbol{p}_p^1}$ only consists of the minimal polynomial $Q^1\big(\boldsymbol{p}^1, T\big)$ of $Y_{n,p}$ modulo $\mathcal{J}_{1,p}$. Since $\overline{\mathcal{J}}_{1,p} = \big(F_{1,p}^*(\boldsymbol{p}_p^1, Y_{n,p})\big)$, 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 $s \in \{1, \ldots, r-1\}$, the sth stage takes as input a Kronecker representation $Q^s(\boldsymbol{p}_p^s, T), W^s_{n-s+2}(\boldsymbol{p}_p^s, T), \ldots, W^s_n(\boldsymbol{p}_p^s, T)$ of $\mathcal{J}_{s,p}$ and outputs a Kronecker representation $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T), W^{s+1}_{n-s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, W^{s+1}_n(\boldsymbol{p}_p^{s+1}, T)$ 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 $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ 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 5.12, such a Kronecker representation is defined by the specializations of $Q^s_p, W^s_{n-s+2,p}, \ldots, W^s_{n,p}$ at $Y_{1,p} = p_{1,p}, \ldots, Y_{n-s-1,p} = p_{n-s-1,p}$. Let $\widehat{R}_{s,p} := \mathbb{F}_p[\![Y_{1,p} - p_{1,p}, \ldots, Y_{n-s,p} - p_{n-s,p}]\!]$. By Remark 4.12 we conclude that it suffices to compute the approximation of $Q^s_p, W^s_{n-s+2,p}, \ldots, W^s_{n,p}$ to precision $(Y_{1,p} - p_{1,p}, \ldots, Y_{n-s,p} - p_{n-s,p})^{\delta_s+1}$ in $\widehat{R}_{s,p}[T]$.

As the ideal $\mathcal{K}_{s,p} = \big(F_{1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big) : G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)^\infty$ is radical and the polynomials $F_{1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ form a regular sequence of $\overline{\mathbb{F}}_p[Y_{n-s,p}, \ldots, Y_{n,p}]$ outside the hypersurface $\{G(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) = 0\}$ by Corollary 4.5, applying the Global Newton algorithm of [21, 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 $F_{1,p}, \ldots, F_{s,p}$;*
- *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 $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), V^s_{n-s+2}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, V^s_n(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ be the corresponding univariate representation. The output is the univariate representation $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T), V^s_{n-s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, V^{s+1}_n(\boldsymbol{p}_p^{s+1}, T)$ of $\mathcal{J}_{s+1,p}$ with primitive element $Y_{n-s,p}$.

For this purpose, for any $F \in \mathbb{F}_p[Y_{1,p}, \ldots, Y_{n,p}]$ which is not a zero divisor modulo $\mathcal{K}_{s,p}$, define $f \in \mathbb{F}_p(Y_{n-s,p})[T]$ by

$$f := F\big(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T, V^s_{n-s+2}(\boldsymbol{p}_p^{s+1}, T), \ldots, V^s_n(\boldsymbol{p}_p^{s+1}, T)\big) \mod Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T),$$

$$a_f := \mathrm{Res}_T\big(f(T), Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big).$$

We have the following result.

Lemma 6.4. *a_f belongs to $\mathbb{F}_p[Y_{n-s,p}] \setminus \{0\}$ and equals, up to a sign, the constant term of the characteristic polynomial of the homothety by $F(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ modulo $\overline{\mathcal{K}}^e_{s,p}$.*

Proof. Let M_f be the matrix of the homothety of multiplication by f 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., [12, Proposition 5.4]):

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

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 $\chi_F \in \overline{\mathbb{F}}_p[Y_{n-s,p}][S]$ the characteristic polynomial of the homothety by $F(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ modulo $\overline{\mathcal{K}}_{s,p}^e$. Let $\chi_0 \in \mathbb{F}_p[Y_{n-s,p}]$ be the constant term of χ_F. Since Φ maps $F(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}) \mod \overline{\mathcal{K}}_{s,p}^e$ to $f \mod \big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$, χ_F coincides with the characteristic polynomial of the homothety of multiplication by f modulo $\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$. Thus $\chi_0 = (-1)^{\delta_s} \det(M_f)$.

It remains to prove that $a_f \neq 0$. Denote by $\mu_F \in \overline{\mathbb{F}}_p[Y_{n-s,p}][S]$ the minimal polynomial of the homothety by $F(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ modulo $\overline{\mathcal{K}}_{s,p}^e$. The constant term $b_f \in \overline{\mathbb{F}}_p[Y_{n-s,p}]$ of μ_F is equal to zero if and only if $a_f = 0$. Suppose that $b_f = 0$. Then we have a factorization $\mu_F = S \cdot \widetilde{\mu}$ in $\overline{\mathbb{F}}_p[Y_{n-s,p}][S]$, and thus $0 = \mu_F(F) = F \cdot \widetilde{\mu}(F)$ in $\mathcal{K}_{s,p}$. Due to minimality of μ_F we must have $\widetilde{\mu}(F) \neq 0$ in $\mathcal{K}_{s,p}$, which implies that F is a zero divisor in $\mathcal{K}_{s,p}$, contradicting thus the hypothesis on F. □

Let

$$\begin{aligned}
f_{s+1} &:= F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T, V_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, T)\big) \mod Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T),\\
g &:= G_p\big(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T, V_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, T)\big) \mod Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T),\\
a_{f_{s+1}} &:= \mathrm{Res}_T\big(f_{s+1}(T), Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big),\\
a_g &:= \mathrm{Res}_T\big(g(T), Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big).
\end{aligned}$$

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

Proposition 6.5. *We have*

$$Q^{s+1}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}) = \epsilon\, a_{f_{s+1}} / \gcd(a_{f_{s+1}}, a_g),$$

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

Proof. First we show that the expression in the right-hand side is well-defined, namely both $a_{f_{s+1}}$ and a_g are nonzero. Indeed, 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 $V_{\boldsymbol{p}_p^{s+1}}$, while Lemma 4.2 proves that $\{G_p(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}) = 0\}$ does not vanish identically on any irreducible $\mathbb{F}_p$-component of $\mathcal{W}_{\boldsymbol{p}_p^{s+1}}$. We conclude that neither $F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ nor $G_p(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ are zero divisors in $\overline{\mathbb{F}}_p[Y_{n-s,p}, \ldots, Y_{n,p}]/\overline{\mathcal{K}}_{s,p}$. Therefore, the assertion follows from Lemma 6.4.

Lemma 6.4 shows that $a_{f_{s+1}}$ equals, up to a sign, the constant term of the characteristic polynomial of the homothety by $F(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ modulo $\overline{\mathcal{K}}_{s,p}^e$. According to

[10, Proposition 2.7] such a constant term coincides, up to multiples in $\mathbb{F}_p \setminus \{0\}$, with the characteristic polynomial of $Y_{n-s,p}$ modulo $\overline{\mathcal{K}}_{s,p} + \big(F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big)$. Similarly, a_g equals, up to multiples in $\mathbb{F}_p \setminus \{0\}$, the characteristic polynomial of $Y_{n-s,p}$ modulo $\overline{\mathcal{K}}_{s,p} + \big(G_p(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big)$. Then condition (5) of Theorem 5.8 implies that no root of a_g in $\overline{\mathbb{F}}_p$ annihilates $Q^{s+1}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p})$. As a consequence, taking into account that $\overline{\mathcal{J}}_{s+1,p} = \big(\overline{\mathcal{K}}_{s,p} + \big(F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big)\big) : G_p(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})^\infty$, we see that the expression for $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ of the statement of the proposition holds. □

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 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 5.9 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 $Y_{n-s+1,p}$. According to Proposition 4.13,

$$Q_p^s(p_{1,p}, \ldots, p_{n-s-1,p}, a, T) = q_a, \;\; W_{j,p}^s(p_{1,p}, \ldots, p_{n-s-1,p}, a, T) = w_{a,j} \; (n-s+2 \le j \le n).$$

It follows that $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$ are obtained by substituting a for $Y_{n-s,p}$ in the input polynomials $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$, $W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$. Then the corresponding univariate representation $q_a, v_{a,n-s+2}, \ldots, v_{a,n}$ is computed using the identities $v_{a,j} = (q_a')^{-1} w_{a,j} \mod q_a$ for $n - s + 2 \le j \le n$.

Let $g(Y_{n-s+1,p}) := F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, a, Y_{n-s+1,p}, v_{a,n-s+2}(Y_{n-s+1,p}), \ldots, v_{a,n}(Y_{n-s+1,p})\big)$. We have the following identities (see, e.g., [10]):

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

These identities allows us to compute $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T) \mod q_a$ for $n - s + 1 \le j \le n$. Having done this for $1 \le k \le \ell$, we 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 [5, Section 4], the previous computations can be rendered into an efficient procedure from which we obtain the following result (see [5, Proposition 4.7]).

Proposition 6.6. *There exists a probabilistic algorithm that takes as input*

- *a straight–line program of size at most L which represents $F_{s+1,p}$ and G_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 correct result with probability at least* $1-1/60n$.

Taking into account the complexity and probability estimates of Propositions 6.3 and 6.6 for $1 \leq s \leq r-1$, we easily deduce the following result.

Theorem 6.7. *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* $F_{1,p}, \ldots, F_{r,p}, G_p$*;*

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 correct 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 5.12 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 5.11. 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 [21, Theorem 2]).

Proposition 6.8. *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 6.7 with the p–adic lifting procedure of Proposition 6.8 we obtain a probabilistic algorithm for computing a Kronecker representation of a zero–dimensional fiber $V_{\boldsymbol{p}^r}$ of the Zariski closure $\mathcal{V}_r$ of $\mathcal{V}(F_1, \ldots, F_r) \setminus \mathcal{V}(G)$.

More precisely, assume that $F_1, \ldots, F_r, G$ 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 $F_{1,p}, \ldots, F_{r,p}, G_p$. Then, by means of the algorithm underlying Theorem 6.7, 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 6.8 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 6.9. *There exists a probabilistic algorithm that takes as input a straight–line program β of length at most L which represents the polynomials $F_1, \ldots, F_r, G$, and outputs a Kronecker representation of a zero–dimensional fiber of the Zariski closure of $\mathcal{V}(F_1, \ldots, F_r) \setminus \mathcal{V}(G)$ with probability at least $\frac{77}{144}$. If h is an upper bound for the bit length of the coefficients of $F_1, \ldots, F_r, G$ and the parameters in β, then the expected number of bit operations of the algorithm is in*

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

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 6.7 and Proposition 6.8, 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.7 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 6.7, the theorem follows. □

We remark that the probability of success of the algorithm of Theorem 6.9 can be increased by considering random choices of the required integers and the lucky prime p with higher bit size. On the other hand, we do not know how our algorithm behaves in case of unlucky choices.

Appendix A. Height estimates

In this appendix we obtain estimates for the height of the integer $\mathfrak{N}$ of Theorem 5.10 and the integers occurring in the output of the algorithm underlying Theorem 6.9, namely the polynomials in Proposition 5.11 which form the Kronecker representation of $\mathcal{J}_r$. For this purpose, we shall rely on the arithmetic Nullstellensätze of [29]. 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 $1 \leq s \leq n$, and let $h(V)$ be the Faltings height of its projective closure $\overline{V} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ (see [13]). We have the following identity:

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

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., [29, 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 $\mathbb{Z}[\mathbf{\Lambda}_1^h, \ldots, \mathbf{\Lambda}_{n-s+1}^h]$, 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 [29, Lemma 1.1] we have

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

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

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

(see, e.g., [29, (1.2)]). Combining (A.1), (A.2) and (A.3) gives

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

Further, the canonical height $\widehat{h}(V)$ of V is defined by $\widehat{h}(V) := \widehat{h}(\overline{V})$, where $\widehat{h}(\overline{V})$ is the *canonical height* of $\overline{V} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ defined as in [7]. 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., [7, Proposition 2.39 (5)]). As a consequence, we have

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

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 $F_1, \ldots, F_r, G \in \mathbb{Z}[\boldsymbol{X}]$ such that $F_1, \ldots, F_r$ form a regular sequence outside the hypersurface $\{G = 0\}$, denote by $\mathcal{V}_s$ the affine equidimensional subvariety of $\mathbb{A}^n$ defined by $\mathcal{I}_s := (F_1, \ldots, F_s) : G^\infty$ 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

$$\delta := \max_{1\leq s\leq r}\delta_s, \quad d := \max\{d_1, \ldots, d_r, \deg(G)\}, \quad h := \max\{h_1, \ldots, h_r, h(G)\}.$$

Let $\widehat{h}_s := \widehat{h}(\mathcal{V}_s)$ for $1 \leq s \leq r$ and $\widehat{h} := \max_{1\leq s\leq r}\widehat{h}_s$.

Lemma A.1. *We have* $\widehat{h}_{s+1} \leq d_{s+1}\widehat{h}_s + \delta_s h_{s+1} + \delta_s d_{s+1}\log(n+2)$ *for* $1 \leq s \leq r-1$.

Proof. Let $\overline{\mathcal{V}}_s$ be the projective closure of $\mathcal{V}_s$ via the canonical inclusion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ and let F_{s+1}^h be the homogeneization of F_{s+1}. Since by hypothesis F_{s+1} is not a zero divisor modulo $\mathcal{I}_s$, we have that $\mathcal{V}(F_{s+1})$ cuts $\mathcal{V}_s$ properly and therefore $\mathcal{V}(F_{s+1}^h)$ cuts $\overline{\mathcal{V}}_s$ properly. By [7, Corollary 2.62 and Lemma 2.30(1)] we deduce that

$$\widehat{h}\big(\overline{\mathcal{V}}_s \cap \mathcal{V}(F_{s+1}^h)\big) \leq \deg(F_{s+1}^h)\widehat{h}(\overline{\mathcal{V}}_s) + \deg(\overline{\mathcal{V}}_s)h(F_{s+1}^h) + \deg(\overline{\mathcal{V}}_s)\deg(F_{s+1}^h)\log(n+2).$$

As $\overline{\mathcal{V}}_s \cap \mathcal{V}(F_{s+1}^h)$ is equidimensional and contains every irreducible $\mathbb{Q}$-component of $\overline{\mathcal{V}_s \cap \mathcal{V}(F_{s+1})}$, we see that $\widehat{h}\big(\mathcal{V}_s \cap \mathcal{V}(F_{s+1})\big) := \widehat{h}\big(\overline{\mathcal{V}_s \cap \mathcal{V}(F_{s+1})}\big) \leq \widehat{h}\big(\overline{\mathcal{V}}_s \cap \mathcal{V}(F_{s+1}^h)\big)$. Further, since $\mathcal{V}_{s+1} = \overline{\mathcal{V}_s \cap \mathcal{V}(F_{s+1}) \setminus \mathcal{V}(G)}$, we have that $\mathcal{V}_{s+1}$ is the union of the irreducible $\mathbb{Q}$-components of $\mathcal{V}_s \cap \mathcal{V}(F_{s+1})$ which $\mathcal{V}(G)$ cuts properly. This implies $\widehat{h}(\mathcal{V}_{s+1}) \leq \widehat{h}\big(\mathcal{V}_s \cap \mathcal{V}(F_{s+1})\big)$. The lemma follows from the previous estimates by noting that $\widehat{h}_s = \widehat{h}(\overline{\mathcal{V}}_s)$, $\delta_s = \deg(\overline{\mathcal{V}}_s)$, $h_{s+1} = h(F_{s+1}^h)$ and $d_{s+1} = \deg(F_{s+1}^h)$. □

Lemma A.2. *We have $\delta_s \le d^s$ and $\widehat{h}_s \le sd^{s-1}h + sd^s \log(n+2)$ for $1 \le s \le r$. In particular, $\widehat{h}_s \in \mathcal{O}^\sim\big(nd^{s-1}(h+d)\big)$ for $1 \le s \le r$.*

Proof. Since $\mathcal{V}_{s+1}$ is the union of the irreducible $\mathbb{Q}$-components of $\mathcal{V}_s \cap \mathcal{V}(F_{s+1})$ not contained in $\mathcal{V}(G)$, by the Bezóut inequality (2.1) we obtain

$$\deg(\mathcal{V}_{s+1}) \le \deg\big(\mathcal{V}_s \cap \mathcal{V}(F_{s+1})\big) \le \deg(\mathcal{V}_s)\deg(F_{s+1}).$$

Thus $\delta_{s+1} \le d\delta_s$ for $1 \le s \le r-1$. Then the first inequality of the lemma easily follows.

To prove the second inequality, let $\overline{\mathcal{V}}_s$ denote the projective closure of $\mathcal{V}_s$ via the canonical inclusion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ and let F_1^h be the homogeneization of F_1. We have $\widehat{h}_1 = \widehat{h}(\overline{\mathcal{V}}_1) = \widehat{h}\big(\mathcal{V}(F_1^h)\big) = \widehat{h}\big(\mathbb{P}^n \cap \mathcal{V}(F_1^h)\big)$. Thus by [7, Corollary 2.62] we have

$$\widehat{h}_1 \le \deg(F_1^h)\left(\widehat{h}(\mathbb{P}^n) + \deg(\mathbb{P}^n)\frac{h(F_1^h) + \deg(F_1^h)\log(n+2)}{\deg(F_1^h)}\right).$$

As $\widehat{h}(\mathbb{P}^n) = 0$ and $\deg(\mathbb{P}^n) = 1$ we obtain $\widehat{h}_1 \le h(F_1) + \deg(F_1)\log(n+2)$, which shows the claimed inequality for $s = 1$. Assume inductively that $\widehat{h}_s \le sd^{s-1}h + sd^s\log(n+2)$. Combining this inequality and $\delta_s \le d^s$ with the inequality of the previous lemma, we readily deduce that $\widehat{h}_{s+1} \le (s+1)d^s h + (s+1)d^{s+1}\log(n+2)$, which completes the proof of the lemma. □

Let μ and ε be fixed real numbers with $0 < \mu, \varepsilon < 1$. Let $\mathsf{a} := \lfloor D/(1-\mu)\rfloor$ and $\mathsf{b} := \lfloor D/(1-\varepsilon)\rfloor$, where D is defined in (5.22). Recall that D is an upper bound for the degree of the polynomials R and $\mathsf{N}_{\boldsymbol{\lambda}}$ of (5.20) and (5.21). Since $D \in \mathcal{O}(rnd^{3r} + rn^3 2^{n-s}d^{2r+1})$ and $h(\mathsf{a}), h(\mathsf{b}) \in \mathcal{O}(\log D)$, we have the following remark.

Remark A.3. $h(\mathsf{a}), h(\mathsf{b}) \in \mathcal{O}^\sim(r\log d + n)$.

Set $\mathsf{S} := \{0, \dots, \mathsf{a}\}$ and $\mathsf{T} := \{0, \dots, \mathsf{b}\}$. Further, let $\boldsymbol{\lambda} := (\lambda_{ij})_{1\le i\le n, 1\le j\le n} \in \mathsf{S}^{n^2}$ and $\boldsymbol{p} := (p_1, \dots, p_{n-1}) \in \mathsf{T}^{n-1}$ be such that $\mathsf{R}(\boldsymbol{\lambda}) \ne 0$ and $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \ne 0$. 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 $\boldsymbol{\lambda}^s := (\lambda_{ij})_{1\le i\le n-s+1, 1\le j\le n}$ and $\boldsymbol{p}^s := (p_1, \dots, p_{n-s})$ for $1 \le s \le r$. Denote $h(\boldsymbol{\lambda}^s) := \max_{1\le i\le n-s+1, 1\le j\le n} h(\lambda_{ij})$ and $h(\boldsymbol{p}^s) := \max_{1\le i\le n-s} h(p_i)$. Finally, let $\boldsymbol{\lambda}_i := (\lambda_{i1}, \dots, \lambda_{in})$ and $Y_i = \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ for $1 \le i \le n$. In the sequel, assuming that $n \ge 2$ and $d \ge 2$, we aim to estimate the height of the integer

$$\mathfrak{N} := \det(\boldsymbol{\lambda})\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) = \det(\boldsymbol{\lambda})\mathsf{M}_r(\boldsymbol{\lambda}^r, \boldsymbol{p}^r)\prod_{s=1}^{r-1}\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\mathsf{B}^G_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1}). \tag{A.5}$$

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

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

$$h(P_s) \in \mathcal{O}^\sim\big(nd^{s-1}(h+d)\big), \tag{A.6}$$

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

Proof. (A.4) and Lemma A.2, combined with the Bézout inequality (2.1), yield (A.6). The degree estimate in (A.7) is clear. Next, observe that P_s is an element of $\mathbb{Z}[\boldsymbol{\Lambda}^s, Z_1, \dots, Z_{n-s+1}]$ of degree $(n-s+1)\delta_s$ and Λ_{ij} $(1 \le i \le n-s+1, 1 \le j \le n)$, $\boldsymbol{\Lambda}_i \cdot \boldsymbol{X}$ $(1 \le i \le n-s+1)$

are elements of $\mathbb{Z}[\mathbf{\Lambda}^s, \boldsymbol{X}]$ of degree at most 2 and height equal to 0. Therefore, from [7, Lemma 2.37(3)] we deduce that

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

This, together with (A.6), readily implies the height estimate in (A.7). □

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.5. *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*

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

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 $\mathrm{Res}_{U_{k+1}}(F, G)$ 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 [7, 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 [7, Lemma 2.37(1)] completes the proof of the lemma. □

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

Lemma A.6. *For $1 \leq s \leq r$, we have*

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

Proof. Since $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\boldsymbol{X})$, 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 $\rho_s := \mathrm{Res}_{Z_{n-s+1}}\left(P_s, \frac{\partial P_s}{\partial Z_{n-s+1}}\right)$, Lemma A.5 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.6) prove the estimate for $h(\rho_s)$. Further, since $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ for all s, from [7, 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.3 and the estimate for $h(\rho_s)$ yields the one for $h(\rho_{\boldsymbol{\lambda}^s})$. □

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.7. *Let η_s be the maximum of the heights of the polynomials $Q^s(\boldsymbol{p}^s, T)$, $W^s_{n-s+2}(\boldsymbol{p}^s, T), \ldots, W^s_n(\boldsymbol{p}^s, T)$ of Proposition 5.11. Then $\eta_s \in \mathcal{O}^{\sim}\big(\widehat{h}(\mathcal{V}_s) + n^2 \deg(\mathcal{V}_s) \log d\big)$, or $\eta_s \in \mathcal{O}^{\sim}\big(nd^{s-1}(h+nd)\big)$.*

Proof. Note that

$$Q^s(\boldsymbol{p}^s, T) = \frac{P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{A_s(\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{n-s})}, \tag{A.8}$$

$$W^s_j(\boldsymbol{p}^s, T) = -\sum_{k=1}^{n} \frac{\lambda_{jk}}{A_s(\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{n-s})} \frac{\partial P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{\partial \Lambda_{n-s+1,k}} \quad (n-s+2 \leq j \leq n). \tag{A.9}$$

Since $h(\boldsymbol{\lambda}^s) \le h(\mathsf{a})$ and $h(\boldsymbol{p}^s) \le h(\mathsf{b})$, by [7, 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 [7, Lemma 2.37(1)] we obtain

$$h\left(\sum_{k=1}^{n} \lambda_{jk}\frac{\partial P_s\,(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{\partial \Lambda_{n-s+1,k}}\right) \le h(P_s) + \log\delta_s + h(\mathsf{a}) + \log n \tag{A.10}$$
$$+ (n-s+1)\delta_s\big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log(4n^2)\big)$$

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

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

By (A.8), (A.9) and the previous estimates we see that η_s is bounded above by the right–hand side of (A.10). The proposition then follows by (A.4), (A.6) and Remark A.3. □

A.3. **Estimates for unmixedness and generic smoothness.** In this section we estimate the height of integers α_s and γ_s as in (5.4) and (5.6), 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 [7, Theorem 2] it follows that there exists $\alpha_s \in \mathbb{Z}\setminus\{0\}$ as in (5.4) with

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

where $c(n) \in \mathcal{O}^{\sim}(n)$. Combining this with (A.7) and recalling that $\deg(G) \le d$ and $h(G) \le h$, we deduce the following result.

Lemma A.8. *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 $Y_1, \ldots, Y_{n-s}, F_1, \ldots, F_s$ with respect to the variables $X_1, \ldots, X_n$.

Lemma A.9. *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 $h(\lambda_{ij}) \le h(\mathsf{a})$ and $h(\partial F_i/\partial X_j) \le h(F_i) + \log(d_i)$, by [7, 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 [7, Lemma 2.37(1)]. □

Let $d_j := 1$ and $h_j := h(Y_{j-s} - p_{j-s})$ for $s+1 \le j \le n$, $d_{n+1} := \deg J_s$ and $h_{n+1} := h(J_s)$. Let $\widetilde{h} := \max_{1\le j\le n+1} h_j$. By [7, Theorem 2], there exist $\gamma_s \in \mathbb{Z}\setminus\{0\}$, $\nu_s \in \mathbb{N}$, and $G_1, \dots, G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ as in (5.6) with

$$\begin{aligned} h(\gamma_s) &\le 2\deg(G)\left(\prod_{j=1}^{n+1} d_j\right)\left(\widehat{h}(\mathbb{A}^n) + \deg(\mathbb{A}^n)\Big(\frac{3h(G)}{2\deg(G)} + \sum_{\ell=1}^{n+1}\frac{\widetilde{h}}{d_\ell} + e(n)\Big)\right)\\ &\le \left(\prod_{j=1}^{s} d_j\right)\deg(J_s)\Big(3h(G) + 2\deg(G)\big((n+1)\widetilde{h} + e(n)\big)\Big), \end{aligned}$$

with $e(n) \in \mathcal{O}^{\sim}(n)$. Since $h(Y_\ell) \le h(\mathsf{a})$ and $h(p_\ell) \le h(\mathsf{b})$ for all ℓ, we obtain

$$h(\gamma_s) \le 3\deg(J_s)d^s h + \deg(J_s)d^{s+1}\big((n+1)\max\{h, h(\mathsf{a}), h(\mathsf{b}), h(J_s)\} + e(n)\big).$$

Combining this with Remark A.3 and Lemma A.9, we deduce the following result.

Lemma A.10. *We have* $h(\gamma_s) \in \mathcal{O}^{\sim}\big(d^{s+2}(h + rn^2 d)\big)$.

A.4. **Estimates for smooth fibers.** In this section we estimate the height of the integers $\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$, $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$ and $\mathsf{B}^G_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$ considered in Section 5.2, where M_s is the polynomial of (5.16), $\mathsf{L}_{\boldsymbol{\lambda}^s}$ is the polynomial of (5.18) and $\mathsf{B}^G_{\boldsymbol{\lambda}^s}$ is the polynomial of (5.19). Combining these estimates we shall be able to estimate the height of the integer $\mathfrak{N}$ of (A.5), which comprises all the unlucky primes p.

We start with an estimate for the height of R^G_s.

Lemma A.11. *Let* $\boldsymbol{U} := (U_1, \dots, U_m)$ *be a tuple of new indeterminates and let* $F \in \mathbb{Z}[X_1, \dots, X_n]$ *and* $G_1, \dots, G_n, H \in \mathbb{Z}[\boldsymbol{U}]$. *Consider the polynomial* $F_{\boldsymbol{U}} \in \mathbb{Z}[\boldsymbol{U}]$ *defined by*

$$F_{\boldsymbol{U}} := H^{\deg(F)} F\left(\frac{G_1}{H}, \dots, \frac{G_n}{H}\right).$$

Let $\widetilde{d} := \max\{\deg(G_1), \dots, \deg(G_n), \deg(H)\}$ *and* $\widetilde{h} := \max\{h(G_1), \dots, h(G_n), h(H)\}$. *Then*

$$\deg(F_{\boldsymbol{U}}) \le \deg(F)\widetilde{d}, \quad h(F_{\boldsymbol{U}}) \le h(F) + \deg(F)\big(\widetilde{h} + \log(n+2) + \widetilde{d}\log(m+1)\big).$$

Proof. Let $F^h \in \mathbb{Z}[X_0, \dots, X_n]$ be the homogeneization of F with respect to a new variable X_0. We have that

$$F^h = X_0^{\deg(F)} F\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right).$$

Substituting $H, G_1, \dots, G_n$ for $X_0, X_1, \dots, X_n$ in this identity we deduce that $F_{\boldsymbol{U}} = F^h(H, G_1, \dots, G_n)$. From this we readily obtain the degree estimate of the lemma. Further, since $\deg(F^h) = \deg(F)$ and $h(F^h) = h(F)$, the height estimate follows from [7, Lemma 2.37 (3)]. □

Lemma A.12. *We have* $\deg(R^G_s) \in \mathcal{O}^{\sim}(nd^{2s+1})$ *and* $h(R^G_s) \in \mathcal{O}^{\sim}\big(nd^{2s}(h+d)\big)$.

Proof. Observe that, for $1 \leq i \leq n$, we have

$$\deg\Big(\frac{\partial P_s}{\partial \Lambda_{n-s+1,i}}\Big) \leq (n-s+1)\delta_s, \quad \deg\Big(\frac{\partial P_s}{\partial Z_{n-s+1}}\Big) \leq (n-s+1)\delta_s,$$
$$h\Big(\frac{\partial P_s}{\partial \Lambda_{n-s+1,i}}\Big) \leq h(P_s) + \log(\delta_s), \quad h\Big(\frac{\partial P_s}{\partial Z_{n-s+1}}\Big) \leq h(P_s) + \log(\delta_s).$$

As a consequence, from Lemma A.11 we deduce that

$$\begin{aligned}\deg(G^s_\Lambda) \leq& \deg(G)(n-s+1)\delta_s,\\ h(G^s_\Lambda) \leq& h(G) + \deg(G)\Big(h(P_s)+\\ &\log(\delta_s) + \log(n+2) + (n-s+1)\delta_s \log\big((n-s+1)(n+1)+1\big)\Big).\end{aligned}$$

Combining these estimates with (A.6) and the fact that $\delta_s \leq d^s$ yields

$$\deg(G^s_\Lambda) \in \mathcal{O}(nd^{s+1}), \quad h(G^s_\Lambda) \in \mathcal{O}^\sim\big(nd^s(h+d)\big). \tag{A.11}$$

Now, since $R^G_s := \mathrm{Res}_{Z_{n-s+1}}(P_s, G^s_\Lambda)$, we see that

$$\deg(R^G_s) \leq \deg_{Z_{n-s+1}}(G^s_\Lambda)\deg(P_s) + \deg_{Z_{n-s+1}}(P_s)\deg(G^s_\Lambda) \leq 2n\deg(G)\delta_s^2,$$

which gives the upper bound for the degree of the lemma. Combining this estimate with Lemma A.5 we obtain

$$\begin{aligned}h(R^G_s) \leq& h(P_s)\deg_{Z_{n-s+1}} G^s_\Lambda + h(G^s_\Lambda)\deg_{Z_{n-s+1}} P_s\\ &+ \log\big((n-s+1)(n+1)+1\big)\big(2n\delta_s^2\deg(G) + \log\big((\deg_{Z_{n-s+1}} G^s_\Lambda + \deg_{Z_{n-s+1}} P_s)!\big)\big).\end{aligned}$$

From this upper bound and (A.11) we deduce the height estimate of the lemma. □

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

Lemma A.13. *For $1 \leq s \leq r$, we have $h\big(\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\big) \in \mathcal{O}^\sim\big(nd^{2s}(h+n^2d)\big)$.*

Proof. By [7, Lemma 2.37 (3)], we have

$$h\big(\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\big) \leq h(\mathsf{M}_s) + \deg(\mathsf{M}_s)\Big(\max\{h(\boldsymbol{\lambda}^s), h(\boldsymbol{p}^s)\} + \log\big((n-s+1)(n+1)+1\big)\Big). \tag{A.12}$$

Recall that $\mathsf{M}_s := \alpha_s\gamma_s A_s\rho_s R^G_s$. Thus, from [7, Lemma 2.37 (2)] we deduce that

$$\begin{aligned}h(\mathsf{M}_s) \leq& h(\alpha_s) + h(\gamma_s) + h(A_s) + h(\rho_s) + h(R^G_s)\\ &+ \log\big((n-s+1)(n+1)+1\big)\big(\deg(A_s) + \deg(\rho_s) + \deg(R^G_s)\big).\end{aligned}$$

By definition, $\deg A_s \leq (n-s)\delta_s$ and $h(A_s) \leq h(P_s)$. Combining this with (A.6) and Lemmas A.6, A.8, A.10 and A.12 we obtain

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

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.3 we have $\max\{h(\boldsymbol{\lambda}^s), h(\boldsymbol{p}^s)\} \in \mathcal{O}^\sim(r\log d + \log n)$. Further, $\deg(\mathsf{M}_s) \in \mathcal{O}(n^2d^{2s+1})$ by (5.17). Combining all these estimates with (A.12), the lemma follows. □

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 (5.8) and $\beta_{\boldsymbol{\lambda}^s}$ of (5.11) and the polynomial $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1,\dots,Z_{n-s-1}] \setminus \{0\}$ of (5.9), we start with an estimate for $\mu_{\boldsymbol{\lambda}^s}$ and $B_{\boldsymbol{\lambda}^s}$.

Proposition A.14. *Let $1 \le s \le r-1$ and assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$. Then there exists $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.8) with*

$$h(\mu_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(n^2 d^{5s+1}(h+nd)\big). \tag{A.13}$$

On the other hand, if $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$, then there exists $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1,\dots,Z_{n-s-1}] \setminus \{0\}$ as in (5.9) with

$$\deg B_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{3s+1}), \quad h(B_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(n^2 d^{3s}(h+d)\big). \tag{A.14}$$

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 $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\boldsymbol{X})$. Let $d_j := \deg(F_j)$ and $h_j := h(F_j)$ for $1 \le j \le s+1$, and $d_{s+2} := \deg \rho_{\boldsymbol{\lambda}^s}$ and $h_{s+2} := h(\rho_{\boldsymbol{\lambda}^s})$. Further, denote $D := \prod_{j=1}^{s+2} d_j$ and $H := \max_{1\le j\le s+2} h_j$. By [7, Theorem 2] there exists $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.8) with

$$h(\mu_{\boldsymbol{\lambda}^s}) \le 2\deg(G) D \left(\frac{3h(G)}{2\deg(G)} + \sum_{\ell=1}^{s+2} \frac{H}{d_\ell} + f(n) \right),$$

where $f(n) \in \mathcal{O}^{\sim}(n)$. By Lemma A.6 we have $d_{s+2} \in \mathcal{O}^{\sim}(nd^{2s})$ and $h_{s+2} \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big)$. Since $D \le d^{s+1} d_{s+2}$ and $H = \max\{h, h_{s+2}\}$, we deduce that $D \in \mathcal{O}^{\sim}(nd^{3s+1})$ and $H \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big)$. The estimate for $h(\mu_{\boldsymbol{\lambda}^s})$ follows from the previous estimates.

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 [7, Corollary 3.23] there exists a polynomial $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1,\dots,Z_{n-s-1}] \setminus \{0\}$ as in (5.9) with

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

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

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 $\rho^h_{\boldsymbol{\lambda}^s}$ be the homogenization of $\rho_{\boldsymbol{\lambda}^s}$. Lemma 5.6 implies that $\{\rho^h_{\boldsymbol{\lambda}^s} = 0\}$ of $\mathbb{P}^n$ cuts $\overline{\mathcal{V}}_{s+1}$ properly. By [7, Corollary 2.62] we conclude that

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

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

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

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

Lemma A.2 asserts that $\widehat{h}_{s+1} \in \mathcal{O}^{\sim}\big(nd^s(h+d)\big)$. Therefore, by Lemma A.6 we conclude that

$$\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{3s+1}), \quad \widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(n^2d^{3s}(h+d)\big).$$

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

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

Lemma A.15. *Let $1 \le s \le r-1$ and assume that $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$. Then there exists $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ as in (5.11) with $h(\beta_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(n^3d^{8s+1}(h+nd)\big)$.*

Proof. Let $d_j = \deg F_j$ and $h_j := h(F_j)$ for $1 \le j \le s+1$, and $d_{s+2} := \deg \rho_{\boldsymbol{\lambda}^s}$ and $h_{s+2} := h(\rho_{\boldsymbol{\lambda}^s})$. Further, define $d_0 := \deg(GB_{\boldsymbol{\lambda}^s}(Y_1,\ldots,Y_{n-s-1}))$ and $h_0 := h(GB_{\boldsymbol{\lambda}^s}(Y_1,\ldots,Y_{n-s-1}))$. Finally, denote $D := \prod_{j=1}^{s+2} d_j$ and $H := \max_{1\le j\le s+2} h_j$. By [7, 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 (5.11) with

$$h(\beta_{\boldsymbol{\lambda}^s}) \le 2d_0D\left(\frac{3h_0}{2d_0} + \sum_{\ell=1}^{s+2}\frac{H}{d_\ell} + g(n)\right),$$

where $g(n) \in \mathcal{O}^{\sim}(n)$. By Lemma A.6 we have $h_{s+2} \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big)$. Since $H = \max\{h, h_{s+2}\}$, we deduce that $H \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big)$. On the other hand, $d_0 \le \deg(G) + \deg B_{\boldsymbol{\lambda}^s} \in \mathcal{O}^{\sim}(nd^{3s+1})$ by (A.14) and $D \le d^{s+1}d_{s+2} \in \mathcal{O}^{\sim}(nd^{3s+1})$. This implies

$$d_0D\left(\sum_{\ell=1}^{s+2}\frac{H}{d_\ell} + g(n)\right) \in \mathcal{O}^{\sim}\big(n^3d^{8s+1}(h+nd)\big). \tag{A.17}$$

Next, since $h(\boldsymbol{\lambda}^s) \le h(\mathsf{a})$ for all s, by [7, Lemma 2.37 (2) and (3)] we have

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

Combining this with (A.14) and Remark A.3 we deduce that $h_0 \in \mathcal{O}^{\sim}\big(n^2d^{3s}(h+d)\big)$. Hence $Dh_0 \in \mathcal{O}^{\sim}\big(n^3d^{6s+1}(h+d)\big)$ which, together with (A.17), proves the lemma. □

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

Corollary A.16. *For $1 \le s \le r-1$, it holds that $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^{\sim}\big(n^3d^{8s+1}(h+nd)\big)$.*

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 $h(\boldsymbol{p}^{s+1}) \le h(\mathsf{b})$, by [7, Lemma 2.37 (3)] we have

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

This inequality, Remark A.3 and (A.14) imply $h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^{\sim}\big(n^2d^{3s}(h+d)\big)$. Comparing this with (A.13) and Lemma A.15 yields the estimate of the lemma. □

Let $B^G_{\boldsymbol{\lambda}^s} := B^G_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\cdot\boldsymbol{X})$, where B^G_s is a primitive and squarefree polynomial defining the Zariski closure of the image of $(\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s) \cap \{G = 0\}$ under the morphism Φ_s of (5.12).

Lemma A.17. *For $1 \leq s \leq r$, we have*

$$\deg B_s^G, \deg(B_{\boldsymbol{\lambda}^s}^G) \in \mathcal{O}(n^2 2^{n-s} d^{s+1}), \quad h(B_s^G), h(B_{\boldsymbol{\lambda}^s}^G) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^s (h+d)\big).$$

Proof. Observe that Λ_{ij} $(1 \leq i \leq n-s+1, 1 \leq j \leq n)$ are elements of $\mathbb{Z}[\boldsymbol{\Lambda}^s, \boldsymbol{X}]$ of degree 1, $\boldsymbol{\Lambda}_i \cdot \boldsymbol{X}$ $(1 \leq i \leq n-s) \in \mathbb{Z}[\boldsymbol{\Lambda}^s, \boldsymbol{X}]$ have degree equal to 2, and all of them have coefficients equal to 1. By [7, Theorem 3.24], setting $\mathcal{W}_s^G := (\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s) \cap \{G = 0\}$, we have

$$\deg\big(B_s^G\big) \leq (n-s+1)(n+1) 2^{n-s} \deg\big(\mathcal{W}_s^G\big), \tag{A.18}$$

$$m\big(B_s^G\big) \leq 2^{n-s} \Big(\widehat{h}\big(\mathcal{W}_s^G\big) + (n-s+1)(n+1) \deg\big(\mathcal{W}_s^G\big)\Big). \tag{A.19}$$

Since the hypersurface of $\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^n$ defined by G cuts properly $\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s$, and taking into account that $\widehat{h}\big(\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s\big) = \widehat{h}(\mathcal{V}_s) =: \widehat{h}_s$ and $\deg\big(\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s\big) = \deg(\mathcal{V}_s) =: \delta_s$ ([7, Lemma 3.16]), from [7, Corollary 2.62] we deduce

$$\deg\big(\mathcal{W}_s^G\big) \leq \delta_s \deg(G),$$
$$\widehat{h}\big(\mathcal{W}_s^G\big) \leq \deg(G)\widehat{h}_s + \delta_s h(G) + \delta_s \deg(G) \log\big((n-s+1)(n+1)\big).$$

Thus Lemma A.2 implies $\deg\big(\mathcal{W}_s^G\big) \in \mathcal{O}(d^{s+1})$ and $\widehat{h}\big(\mathcal{W}_s^G\big) \in \mathcal{O}^\sim\big(nd^s(h+d)\big)$. Since $\deg(B_{\boldsymbol{\lambda}^s}^G) \leq \deg(B_s^G)$ the degree estimate of the lemma follows. We now consider the height estimate. Taking into account (A.19) we obtain $m\big(B_s^G\big) \in \mathcal{O}^\sim\big(n^2 2^{n-s} d^s (h+d)\big)$. As $h\big(B_s^G\big) \leq m\big(B_s^G\big) + \log\big((n-s+1)(n+1)\big) \deg\big(B_s^G\big)$ ([7, Lemma 2.32 (2)]), we obtain $h(B_s^G) \in \mathcal{O}^\sim\big(n^2 2^{n-s} d^s (h+d)\big)$. Further, since $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ for all s, from [7, Lemma 2.37 (3)], we deduce that

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

From Remark A.3 the height estimate of the lemma follows. □

Proposition A.18. *There exist $\beta_{\boldsymbol{\lambda}^s}^G$ as in* (5.14) *and $\gamma_{\boldsymbol{\lambda}^s}^G$ as in* (5.15) *with*

$$h(\beta_{\boldsymbol{\lambda}^s}^G) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{2s+1}(h+d)\big), \quad h(\gamma_{\boldsymbol{\lambda}^s}^G) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{3s+1}(h+d)\big).$$

Proof. Let $B_{\boldsymbol{\lambda}^s}^G := B_s^G(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1} \cdot \boldsymbol{X}) \in \mathbb{Z}[\boldsymbol{X}]$. By [7, Theorem 2] there exist $\beta_{\boldsymbol{\lambda}^s}^G \in \mathbb{Z} \setminus \{0\}$, $\mu_{\boldsymbol{\lambda}^s}^G \in \mathbb{N}$ and $H_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[\boldsymbol{X}]$ as in (5.14) with

- $\mu_{\boldsymbol{\lambda}^s}^G \leq 2 \deg(G) \delta_s$;
- $\deg(H_{\boldsymbol{\lambda}^s} G) \leq 4 \deg(B_{\boldsymbol{\lambda}^s}^G) \deg(G)\, \delta_s$;
- $h(\beta_{\boldsymbol{\lambda}^s}^G), h(H_{\boldsymbol{\lambda}^s}) + h(G) \leq 2 \deg(B_{\boldsymbol{\lambda}^s}^G) \deg(G) \Big(\widehat{h}_s + \delta_s \Big(\frac{3h(B_{\boldsymbol{\lambda}^s}^G)}{2\deg(B_{\boldsymbol{\lambda}^s}^G)} + \frac{h(G)}{\deg(G)} + f(n)\Big)\Big)$, where $f(n) \in \mathcal{O}^\sim(n)$.

These estimates, together with Lemmas A.2 and A.17, yield

$$\mu_{\boldsymbol{\lambda}^s}^G \in \mathcal{O}(d^{s+1}), \quad \deg(H_{\boldsymbol{\lambda}^s} G) \in \mathcal{O}(n^2 2^{n-s} d^{2s+2}),$$
$$h(\beta_{\boldsymbol{\lambda}^s}^G), h(H_{\boldsymbol{\lambda}^s}) + h(G) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{2s+1}(h+d)\big), \tag{A.20}$$

which proves the claimed estimate for the height of $\beta_{\boldsymbol{\lambda}^s}^G$.

Now, let $P := G\big(\beta^G_{\boldsymbol{\lambda}^s}(B^G_{\boldsymbol{\lambda}^s})^{\mu^G_{\boldsymbol{\lambda}^s}} - H_{\boldsymbol{\lambda}^s}G\big)$. By [7, Theorem 2] there exist $\gamma^G_{\boldsymbol{\lambda}^s} \in \mathbb{Z}\setminus\{0\}$ and $\nu^G_{\boldsymbol{\lambda}^s} \in \mathbb{N}$ as in (5.15) with

$$h(\gamma^G_{\boldsymbol{\lambda}^s}) \le 2\deg(P)d^s\left(\widehat{h}(\mathbb{A}^n) + \deg(\mathbb{A}^n)\Big(\frac{3h(P)}{2\deg(P)} + \sum_{\ell=1}^{s}\frac{h}{d_\ell} + g(n)\Big)\right),$$

where $g(n) \in \mathcal{O}^\sim(n)$. Since $\widehat{h}(\mathbb{A}^n) = 0$ and $\deg(\mathbb{A}^n) = 1$, we have

$$h(\gamma^G_{\boldsymbol{\lambda}^s}) \le 3h(P)d^s + 2\deg(P)d^{s-1}hs + 2\deg(P)d^s g(n). \tag{A.21}$$

We estimate $\deg(P)$ and $h(P)$. We have $\deg(P) \le 4\deg(B^G_{\boldsymbol{\lambda}^s})\deg(G)\delta_s + \deg(G)$, which together with Lemma A.17 gives

$$\deg(P) \in \mathcal{O}(n^2 2^{n-s} d^{2s+2}). \tag{A.22}$$

By [7, Lemma 2.37 (1) and (2)] we have

$$h(P) \le \max\Big\{h\big(\beta^G_{\boldsymbol{\lambda}^s}(B^G_{\boldsymbol{\lambda}^s})^{\mu^G_{\boldsymbol{\lambda}^s}}\big), h(H_{\boldsymbol{\lambda}^s}G)\Big\} + h(G) + \log(n+1)\deg(G) + 1.$$

Further, from [7, Lemma 2.37 (2)] we deduce that

$$\begin{aligned} h\big(\beta^G_{\boldsymbol{\lambda}^s}(B^G_{\boldsymbol{\lambda}^s})^{\mu^G_{\boldsymbol{\lambda}^s}}\big) &\le h(\beta^G_{\boldsymbol{\lambda}^s}) + \mu^G_{\boldsymbol{\lambda}^s}h(B^G_{\boldsymbol{\lambda}^s}) + \log(n+1)\mu^G_{\boldsymbol{\lambda}^s}\deg(B^G_{\boldsymbol{\lambda}^s}),\\ h(H_{\boldsymbol{\lambda}^s}G) &\le h(H_{\boldsymbol{\lambda}^s}) + h(G) + \log(n+1)\deg(G), \end{aligned}$$

which, together with Lemma A.17, yields

$$h(P) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{2s+1}(h+d)\big). \tag{A.23}$$

Finally, combining (A.21), (A.22) and (A.23) the lemma follows. □

Corollary A.19. *We have* $h\big(\mathsf{B}^G_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{3s+1}(h+d)\big)$.

Proof. Recall that $\mathsf{B}^G_{\boldsymbol{\lambda}^s} := \beta^G_{\boldsymbol{\lambda}^s}\gamma^G_{\boldsymbol{\lambda}^s}\widehat{B}_s(\boldsymbol{\lambda}^s, Z_1, \ldots, Z_{n-s-1})$, where $\widehat{B}_s := \mathrm{Res}_{Z_{n-s}}(B^G_s, P_{s+1})$. Let $\ell := \deg_{Z_{n-s}} P_{s+1}$ and $m := \deg_{Z_{n-s}} B^G_s$. Then by Lemma A.5 we have

$$h(\widehat{B}_s) \le \ell h(B^G_s) + m h(P_{s+1}) + \log\big((n-s+1)(n+1)\big)\big(\ell\deg(B^G_s) + m\deg P_{s+1}\big) + \log\big((\ell+m)!\big).$$

By Lemma A.17 we conclude that $h(\widehat{B}_s) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{2s+1}(h+d)\big)$. Similarly we deduce that $\deg(\widehat{B}_s) \in \mathcal{O}^\sim(n^2 2^{n-s} d^{2s+2})$. Then, by [7, Lemma 2.37 (3)], and taking into account that $h(\boldsymbol{\lambda}^\ell) \le h(\mathsf{a})$ and $h(\boldsymbol{p}^\ell) \le h(\mathsf{b})$ for all ℓ, we see that

$$h\big(\widehat{B}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^{s+1})\big) \le h(\widehat{B}_s) + \deg(\widehat{B}_s)\Big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log\big((n-s+1)(n+1)\big)\Big).$$

The previous estimates combined with Remark A.3 yield

$$h\big(\widehat{B}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^{s+1})\big) \in \mathcal{O}^\sim\big(n^3 2^{n-s} d^{2s+1}(h+d)\big).$$

Since $\mathsf{B}^G_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1}) = \beta^G_{\boldsymbol{\lambda}^s}\gamma^G_{\boldsymbol{\lambda}^s}\widehat{B}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^{s+1})$, the lemma follows by combining the latter estimate together with the ones of Proposition A.18. □

As a consequence of Lemma A.13 and Corollaries A.16 and A.19 we are able to estimate the height of the multiple $\mathfrak{N}$ of all the unlucky primes.

Theorem A.20. *The integer* $\mathfrak{N}$ *of* (A.5) *satisfies*

$$h(\mathfrak{N}) \in \mathcal{O}^\sim\big(n^3 d^{8r-7}(h+n^2 d) + n^3 2^{n-r+1} d^{3r-2}(h+d)\big).$$

Proof. Note that $h(\det \boldsymbol{\lambda}) \leq \log(n!)+nh(\mathsf{a}) \in \mathcal{O}^{\sim}(rn)$. This, together with Lemma A.13 and Corollaries A.16 and A.19, readily implies the theorem. □

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] M. Brodmann, *Algebraische Geometrie: Eine Einfhürung*, Basler Lehrbücher: A Series of Advanced Textbooks in Mathematics, vol. 1, Birkhäuser, Basel, Boston, Berlin, 1989.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

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

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

[14] 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.

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

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

[17] 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.

[18] 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.

[19] 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.

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

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

[22] 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.

[23] 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.

[24] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277.
[25] 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.
[26] W. Hodge and D. Pedoe, *Methods of algebraic geometry. Vol. II*, Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1968.
[27] Z. Jelonek, *On the effective Nullstellensatz*, Invent. Math. **162** (2005), no. 1, 1–17.
[28] G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein, *Deformation techniques for sparse systems*, Found. Comput. Math **9** (2009), 1–50.
[29] T. Krick, L.M. Pardo, and M. Sombra, *Sharp estimates for the Arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), no. 3, 521–598.
[30] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston, 1985.
[31] S. Lang, *Algebra*, Addison–Wesley, Reading, Massachusetts, 1993
[32] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theoret. Comput. Sci. **15** (1981), 77–110.
[33] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596.
[34] H. Matsumura, *Commutative algebra*, Benjamin, 1980.
[35] ———, *Commutative ring theory*, Cambridge Univ. Press, Cambridge, 1986.
[36] 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.
[37] T. Mora, *Solving polynomial equation systems. Vol. II. Macaulay's paradigm and Gröbner technology*, Encyclopedia Math. Appl., vol. 99, Cambridge Univ. Press, Cambridge, 2005.
[38] ———, *Solving polynomial equation systems. Vol. III: Algebraic solving*, Encyclopedia Math. Appl., vol. 157, Cambridge Univ. Press, Cambridge, 2015.
[39] D. Mumford, *Algebraic geometry I. Complex projective varieties*, 2nd ed., Classics Math., Springer, Berlin, 1995.
[40] L.M. Pardo and J. San Martín, *Deformation techniques to solve generalized Pham systems*, Theoret. Comput. Sci. **315** (2004), no. 2–3, 593–625.
[41] 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.
[42] E. Schost, *Sur la résolution de systèmes à paramètres*, Ph.D. thesis, École Polytechnique, France, 2000.
[43] ———, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), 349–393.
[44] I.R. Shafarevich, *Basic algebraic geometry: Varieties in projective space*, Springer, Berlin Heidelberg New York, 1994.
[45] 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.
[46] A. Sommese and C. Wampler, *The numerical solution of systems of polynomials arising in engineering and science*, World Scientific, Singapore, 2005.
[47] 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