MATHEMATICS OF COMPUTATION
Volume 75, Number 256, October 2006, Pages 2049–2085
S 0025-5718(06)01878-3
Article electronically published on July 20, 2006

FAST COMPUTATION OF A RATIONAL POINT OF A VARIETY OVER A FINITE FIELD

ANTONIO CAFURE AND GUILLERMO MATERA

Dedicated to Joos Heintz on the occasion of his 60th birthday

Abstract. We exhibit a probabilistic algorithm which computes a rational point of an absolutely irreducible variety over a finite field defined by a reduced regular sequence. Its time-space complexity is roughly quadratic in the logarithm of the cardinality of the field and a geometric invariant of the input system. This invariant, called the degree, is bounded by the Bézout number of the system. Our algorithm works for fields of any characteristic, but requires the cardinality of the field to be greater than a quantity which is roughly the fourth power of the degree of the input variety.

1. Introduction

Let q be a prime power, let $\mathbb{F}_q$ be the finite field of q elements, and let $\overline{\mathbb{F}}_q$ denote its algebraic closure. For a given $n \in \mathbb{N}$, we denote by $\mathbb{A}^n$ the n-dimensional affine space $\overline{\mathbb{F}}_q^n$ endowed with its Zariski topology. Let a finite set of polynomials $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ be given and let V denote the affine subvariety of $\mathbb{A}^n$ defined by $F_1, \ldots, F_m$. In this paper we consider the problem of computing a q-rational point of the variety V, i.e., a point $x \in \mathbb{F}_q^n$ such that $F_i(x) = 0$ holds for $1 \leq i \leq m$.

This is an important problem of mathematics and computer science, with many applications. It is NP-complete, even if the equations are quadratic and the field considered is $\mathbb{F}_2$. Furthermore, [58] shows that determining the number of rational points of a sparse plane curve over a finite field is #P-complete. In fact, several multivariate cryptographic schemes based on the hardness of solving polynomial equations over a finite field have been proposed and cryptoanalyzed (see, e.g., [12]). The problem is also a critical point in areas such as coding theory (see, e.g., [15], [39]), combinatorics [40], etc.

In the case of systems over the complex or real numbers, the series of papers [22], [45], [21], [20], [23], [2], [3], [4], [5] (see also [29], [25], [38]) introduces a new symbolic elimination algorithm. Its complexity is roughly the product of the complexity of the input polynomials and a *polynomial* function of a certain geometric invariant

Received by the editor December 10, 2003 and, in revised form, October 10, 2005.
2000 *Mathematics Subject Classification.* Primary 11G25, 14G05, 68W30; Secondary 11G20, 13P05, 68Q10, 68Q25.
Key words and phrases. Varieties over finite fields, rational points, geometric solutions, straight-line programs, probabilistic algorithms, first Bertini theorem.
This research was partially supported by the following grants: UBACyT X112, PIP CONICET 2461, and UNGS 30/3005.

of the input system, called its *degree*. The degree is always bounded by the Bézout number of the input system and often happens to be considerably smaller.

1.1. **Main contribution.** In this article we extend this family of elimination algorithms to systems over finite fields. More precisely, we exhibit a new probabilistic algorithm which computes a rational point of an $\mathbb{F}_q$-definable absolutely irreducible variety. Our main result is summarized in the following theorem (see Corollary 6.5 for a precise complexity statement).

Theorem. *Let $n \geq 3$ and $d \geq 2$. Let $F_1, \ldots, F_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ be polynomials of degree at most d which form a regular sequence. Suppose that $F_1, \ldots, F_s$ generate a radical ideal of $\mathbb{F}_q[X_1, \ldots, X_n]$ for $1 \leq s \leq r$ and let $V_s := V(F_1, \ldots, F_s) \subset \mathbb{A}^n$. Let $\delta := \max_{1 \leq s \leq r} \deg V_s$. Suppose further that $V := V_r$ is absolutely irreducible and $q > 8n^2 d\delta_r^4$ holds. Then, a q-rational point of V can be computed by a probabilistic algorithm using space $O^{\sim}\big(\mathcal{S}\delta^2 \log^2 q\big)$ and time $O^{\sim}(\mathcal{T}\delta^2 \log^2 q)$, where $\mathcal{T}$ denotes the number of arithmetic operations in $\mathbb{F}_q$ required to evaluate the polynomials $F_1, \ldots, F_r$ and $\mathcal{S}$ denotes the maximum number of elements of $\mathbb{F}_q$ stored during the evaluation.*

(Here $O^{\sim}$ refers to the standard Soft-Oh notation which does not take into account logarithmic terms. Further, we have ignored terms depending on n and d, in the sense that the Soft-Oh symbol includes polynomial terms in n and d.)

Our algorithm does not impose any restriction on the characteristic $p > 0$, but requires the cardinality q of the field $\mathbb{F}_q$ to satisfy the condition $q > 8n^2 d\delta_r^4$, where δ_r is the degree of the variety V. We observe that [9, Corollary 7.4] asserts that an absolutely irreducible variety over $\mathbb{F}_q$ of dimension $n-r$ and degree δ_r has a rational point if $q > \max\{2(n-r+1)\delta_r^2, 2\delta_r^4\}$ holds. As far as the authors know, this is the best *general* existence result for an absolutely irreducible variety of fixed dimension and degree. Since our algorithm cannot work unless there exists a q-rational point of the variety V, we see that our condition on q comes quite close to this "minimal" requirement.

In the above statement we assume that the input polynomials $F_1, \ldots, F_r$ form a *reduced* regular sequence, i.e., $F_1, \ldots, F_s$ generate a radical ideal for $1 \leq s \leq r$. We remark that this does not represent a significant restriction to the generality of our algorithm. In fact, a generic linear combination of polynomials forming a regular sequence and generating a radical ideal gives a reduced regular sequence (see, e.g., [34, Proposition 37]). Furthermore, using techniques inspired by [37], [38] it is possible to extend our algorithm to *arbitrary* polynomial systems over $\mathbb{F}_q$ defining an absolutely irreducible variety (this extension shall be considered in a forthcoming work). Finally, we observe that our algorithm can be efficiently extended to the case of an $\mathbb{F}_q$-definable variety V with an absolutely irreducible $\mathbb{F}_q$-definable component of dimension equal to $\dim V$. On the other hand, extensions to the general case of an arbitrary variety over $\mathbb{F}_q$ are likely to produce a significant increase of the time-space complexity of our algorithm (see [30]).

1.2. **Related work.** There is not much literature on the subject. In [59], an algorithm for computing the set of q-rational points of a plane curve over a finite field is proposed. On the other hand, [33] and [12] exhibit algorithms which solve an overdetermined system of quadratic equations over a finite field, based on a technique of linearization.

Algorithms for finding rational points on a general variety over a finite field are usually based on rewriting techniques (see, e.g., [13], [14]). Unfortunately, such algorithms have superexponential complexity, which makes them infeasible for realistically sized problems. Indeed, their most efficient variants (see, e.g., [17]) have a worst-case complexity higher than the result of an exhaustive search in polynomial systems over $\mathbb{F}_2$ [12].

A different approach is taken in [30]. In this article, the authors exhibit an algorithm for solving polynomial systems over a finite field by means of deformations, based on a perturbation of the original system and a subsequent path-following method. Nevertheless, the perturbation typically introduces spurious solutions which may be computationally expensive to identify and eliminate in order to obtain the actual solutions. Furthermore, the algorithm is algebraically robust or universal in the sense of [28] and [10], which implies exponential lower bounds on its time complexity.

The complexity of our algorithm is polynomial in the degree of the system δ and the logarithm of q. Therefore, taking into account the *worst-case* estimate $\delta \leq D := \prod_{i=1}^{r} \deg(F_i)$, we conclude that the complexity is *polynomial* in the Bézout number D and $\log q$. This is the first algorithm for solving polynomial systems over finite fields having such complexity. In particular, we significantly improve the $d^{O(n^2)} \log^{O(1)} q$ worst-case estimates of [30] and the algorithms using rewriting techniques (Gröbner bases).

1.3. **Outline of the article.** Our algorithm may be divided into three main parts. The first part is a procedure which has as input a reduced regular sequence $F_1, \ldots, F_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ and as output a complete description of a generic zero-dimensional linear section of the input variety $V := V(F_1, \ldots, F_r)$. Such a description is provided by a K-definable generic linear projection $\pi_r : V \to \mathbb{A}^{n-r}$ and a parametrization of an unramified generic fiber $\pi_r^{-1}(P^{(r)})$, where K is a suitable finite field extension of $\mathbb{F}_q$ (cf. Sections 2.1, 2.2).

In Section 4 we describe this recursive procedure. It proceeds in $r-1$ steps. Its sth step computes a complete description of a generic zero-dimensional linear section of $V_{s+1} := V(F_1, \ldots, F_{s+1})$, which is represented by an unramified fiber $\pi_{s+1}^{-1}(P^{(s+1)})$ of a finite K-definable linear projection $\pi_{s+1} : V_{s+1} \to \mathbb{A}^{n-s-1}$. For this purpose, in Section 4.1 the unramified fiber $\pi_s^{-1}(P^{(s)})$ of the previous step is "lifted" to a suitable curve $W_{P^{(s+1)}}$, contained in $V_s := V(F_1, \ldots, F_s)$, whose intersection with the hypersurface defined by F_{s+1} yields a complete description of the fiber $\pi_{s+1}^{-1}(P^{(s+1)})$. This intersection is considered in Sections 4.2 and 4.3.

In the second part of our algorithm (Section 5), we obtain an $\mathbb{F}_q$-definable description of an $\mathbb{F}_q$-definable generic zero-dimensional linear section of V. For this purpose, we develop a symbolic homotopy algorithm, based on a global Newton–Hensel lifting. It "moves" the K-definable finite morphism $\pi_r : V_r \to \mathbb{A}^{n-r}$ and the K-definable generic unramified fiber $\pi_r^{-1}(P^{(r)})$ previously obtained, into an $\mathbb{F}_q$-definable finite morphism $\pi : V \to \mathbb{A}^{n-r}$ and an $\mathbb{F}_q$-definable generic unramified fiber $\pi^{-1}(Q)$.

Combining this procedure with an effective version of the first Bertini theorem, in the third part of our algorithm we obtain an absolutely irreducible plane $\mathbb{F}_q$-curve $\mathcal{C}$ with the property that any q-rational smooth point of $\mathcal{C}$ immediately yields a q-rational point of the input variety V (see Section 6). Then, in Section 6.1 we compute a q-rational point of the curve $\mathcal{C}$ with a probabilistic algorithm which combines Weil's classical estimate and a procedure based on factorization and gcd computations.

A critical point of our algorithm is the determination of the linear projections π_s and the points $P^{(s)}$ for $1 \le s \le r$. In Section 3 we show that this data can be generically chosen, and we obtain explicit estimates on the degrees of the polynomials underlying this genericity condition. This significantly improves previous estimates. Using the Zippel–Schwartz test (see [62], [52] and Section 2.3) we may randomly find such linear projections and points with a high probability of success.

2. Notions and notations

We use standard notions and notations of commutative algebra and algebraic geometry as can be found in, e.g., [36], [53], [42].

Let $\mathbb{F}_q$ and $\overline{\mathbb{F}}_q$ denote the finite field of q elements and its algebraic closure respectively, and let K be a subfield of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$. Let $\mathsf{K}[X_1, \dots, X_n]$ denote the ring of n-variate polynomials in indeterminates $X_1, \dots, X_n$ and coefficients in K. Let V be a K-definable affine subvariety of $\mathbb{A}^n$ (a K-variety for short). We shall denote by $I(V) \subset \mathsf{K}[X_1, \dots, X_n]$ its defining ideal and by $\mathsf{K}[V]$ its coordinate ring, namely, the quotient ring $\mathsf{K}[V] := \mathsf{K}[X_1, \dots, X_n]/I(V)$. We shall use the notations $\{F_1 = 0, \dots, F_s = 0\}$ and $\{F_1 = 0, \dots, F_s = 0, G \neq 0\}$ to denote the K-variety V defined by $F_1, \dots, F_s$ and the open subset of V defined by the intersection of V with the complement of the hypersurface $\{G = 0\}$.

If V is irreducible as a K-variety (K-irreducible for short), we define its *degree* as the maximum number of points lying in the intersection of V with an affine linear subspace L of $\mathbb{A}^n$ of codimension $\dim(V)$ for which $\#(V \cap L) < \infty$ holds. More generally, if $V = C_1 \cup \cdots \cup C_N$ is the decomposition of V into irreducible K-components, we define the degree of V as $\deg(V) := \sum_{i=1}^{N} \deg(C_i)$ (cf. [26]). In the sequel we shall make use of the following *Bézout inequality* ([26]; see also [18]): if V and W are K-subvarieties of $\mathbb{A}^n$, then

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

A K-variety $V \subset \mathbb{A}^n$ is *absolutely irreducible* if it is irreducible as an $\overline{\mathbb{F}}_q$-variety.

2.1. Geometric solutions.

In order to describe the geometric aspect of our procedure we need some more terminology, essentially borrowed from [20]. Let us consider an equidimensional K-variety $W \subset \mathbb{A}^n$ of dimension $m \ge 0$ and degree $\deg W$, defined by polynomials $F_1, \dots, F_{n-m} \in \mathsf{K}[X_1, \dots, X_n]$ which form a regular sequence. A *geometric solution* of W consists of the following items:

- a linear change of variables, transforming the variables $X_1, \dots, X_n$ into new ones, say $Y_1, \dots, Y_n$, with the following properties:
  - the linear map $\pi : W \to \mathbb{A}^m$ defined by $Y_1, \dots, Y_m$ is a finite surjective morphism. In this case, the change of variables is called a *Noether normalization* of W, and we say that the variables $Y_1, \dots, Y_n$ are in *Noether position* with respect to W, the variables $Y_1, \dots, Y_m$ being *free*. The given Noether normalization induces an integral ring extension $R_m := \overline{\mathbb{F}}_q[Y_1, \dots, Y_m] \hookrightarrow \overline{\mathbb{F}}_q[W]$. Observe that $\overline{\mathbb{F}}_q[W]$ is a free R_m-module whose rank we denote by $\mathrm{rank}_{R_m} \overline{\mathbb{F}}_q[W]$. Note that $\mathrm{rank}_{R_m} \overline{\mathbb{F}}_q[W] \le \deg W$ (see, e.g., [24]) and $\overline{\mathbb{F}}_q[W] \cong \overline{\mathbb{F}}_q[X_1, \dots, X_n]/(F_1, \dots, F_{m-n})$ hold.
  - the linear form Y_{m+1} induces a primitive element of the ring extension $R_m \hookrightarrow \overline{\mathbb{F}}_q[W]$, i.e., an element $y_{m+1} \in \overline{\mathbb{F}}_q[W]$ whose (monic) minimal

polynomial $q^{(m)} \in R_m[T]$ over R_m satisfies the condition $\deg_T q^{(m)} = \mathrm{rank}_{R_m} \overline{\mathbb{F}}_q[W]$. Observe that $\deg q^{(m)} = \deg_T q^{(m)} \leq \deg W$ holds.

- the minimal polynomial $q^{(m)}$ of y_{m+1} over R_m.
- a generic "*parametrization*" of the variety W by the zeroes of $q^{(m)}$, of the form $(\partial q^{(m)}/\partial T)(T)Y_j - v_j^{(m)}(T)$ with $v_j^{(m)} \in R_m[T]$ $(m+2 \leq j \leq n)$. We require that $\deg_T\ v_j^{(m)} < \deg_T q^{(m)}$ and $(\partial q^{(m)}/\partial T)(Y_{m+1})Y_j - v_j^{(m)}(Y_{m+1}) \in (F_1, \ldots, F_{n-m})$ hold for $m+2 \leq j \leq n$. This parametrization is unique up to scaling by nonzero elements of $\overline{\mathbb{F}}_q$.

We remark that if W is a zero-dimensional variety, a linear form Y_1 is a primitive element of the ring extension $\overline{\mathbb{F}}_q \hookrightarrow \overline{\mathbb{F}}_q[W]$ if and only if it separates the points of W, in other words, $Y_1(P) \neq Y_1(Q)$ whenever P and Q are distinct points of W.

This notion of "geometric solution" has a long history, going back at least to L. Kronecker [35] (see also [41], [61]). One might consider [11] and [19] as early references where this notion was implicitly used for the first time in modern symbolic computation.

2.2. **Lifting points and lifting fibers.** Consider as in the previous section an m-dimensional K-variety W and a Noether normalization $\pi : W \to \mathbb{A}^m$. We call a point $P := (p_1, \ldots, p_m) \in \mathbb{A}^m$ a *lifting point* of π if π is unramified at P, i.e., if the equations $F_1 = 0, \ldots, F_{n-m} = 0, Y_1 = p_1, \ldots, Y_m = p_m$ define the fiber $\pi^{-1}(P)$ by transversal cuts. We call the zero-dimensional variety $W_P := \pi^{-1}(P)$ the *lifting fiber* of the point P.

Suppose that a geometric solution of W and a lifting point P of π are given. Suppose further that P is not a zero of the discriminant of the polynomial $q^{(m)}$ with respect to the variable T. Then the geometric solution of the variety W induces a geometric solution of the lifting fiber W_P. This geometric solution of W_P is given by the linear forms $Y_{m+1}, \ldots, Y_n$, the polynomial $q^{(m)}(P, T)$, and the parametrizations $(\partial q^{(m)}/\partial T)(P, T)Y_j - v_j^{(m)}(P, T)$ $(m+2 \leq j \leq n)$. We call such a geometric solution of W *compatible* with the lifting point P.

We observe that π is unramified at a given point $P \in \mathbb{A}^m$ if and only if $J(x) \neq 0$ holds for any $x \in \pi^{-1}(P)$. Here $J \in \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ denotes the Jacobian determinant of $Y_1, \ldots, Y_m, F_1, \ldots, F_{n-m}$ with respect to the variables $X_1, \ldots, X_n$. Furthermore, [43, Proposición 28] shows that π is unramified at $P \in \mathbb{A}^m$ if and only if the condition $\#\pi^{-1}(P) = \deg W$ holds.

For $1 \leq j \leq n - m$, let $F_j(Y_1, \ldots, Y_n)$ denote the element of $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_n]$ obtained by rewriting $F_j(X_1, \ldots, X_n)$ in the variables $Y_1, \ldots, Y_n$. The following result, probably well known, is included here for lack of a suitable reference.

Lemma 2.1. *Let notations and assumptions be as above. Suppose that π is unramified at a point $P \in \mathbb{A}^m$. Then the Jacobian matrix $(\partial F_j/\partial Y_{m+k})_{1 \leq j,k \leq n-m}(x)$ is nonsingular for any point $x \in \pi^{-1}(P)$.*

Proof. Let $W_P := \pi^{-1}(P)$, let $\widetilde{\pi} : W_P \to \mathbb{A}^{n-m}$ be the projection morphism defined by the linear forms $Y_{m+1}, \ldots, Y_n$, and let $\widetilde{\pi}^* : \overline{\mathbb{F}}_q[Y_{m+1}, \ldots, Y_n] \to \overline{\mathbb{F}}_q[W_P]$ denote the corresponding morphism of coordinate rings. Let I_P denote the ideal of $\overline{\mathbb{F}}_q[Y_{m+1}, \ldots, Y_n]$ generated by the polynomials $F_j(P, Y_{m+1}, \ldots, Y_n)$ for $1 \leq j \leq n - m$. We claim that I_P equals the kernel of the morphism $\widetilde{\pi}^*$. Indeed, it is clear that the ideal I_P is included in the kernel of the morphism $\widetilde{\pi}^*$. On the other hand, let $F \in \overline{\mathbb{F}}_q[Y_{m+1}, \ldots, Y_n]$ satisfy the condition $\widetilde{\pi}^*(F) = 0$. This implies that F, considered to be an element of $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$, vanishes on any point of the fiber W_P. This implies that the following relation holds:

$$F \in \big(Y_1 - p_1, \ldots, Y_m - p_m, F_1(Y_1, \ldots, Y_n), \ldots, F_{n-m}(Y_1, \ldots, Y_n)\big). \tag{2.2}$$

Specializing the variables $Y_1, \ldots, Y_m$ into the values $p_1, \ldots, p_m$ in (2.2), we conclude that $F \in I_P$ holds.

From the claim and the fact that $\widetilde{\pi}^*$ is surjective we deduce the existence of an isomorphism of $\overline{\mathbb{F}}_q$-algebras:

$$\overline{\mathbb{F}}_q[Y_1, \ldots, Y_n]/\big(F_1(P, Y_{m+1}, \ldots, Y_n), \ldots, F_{n-m}(P, Y_{m+1}, \ldots, Y_n)\big) \cong \overline{\mathbb{F}}_q[W_P].$$

This shows that the ideal I_P is radical. Since W_P is a zero-dimensional variety, it follows from, e.g., [14, Chapter 4, Corollary 2.6] that W_P is a smooth variety. Therefore, applying the Jacobian criterion finishes the proof of the lemma. $\square$

2.3. **On the algorithmic model.** Algorithms in elimination theory are usually described using the standard dense (or sparse) complexity model, i.e., encoding multivariate polynomials by means of the vector of all (or of all nonzero) coefficients. Taking into account that a generic n-variate polynomial of degree d has $\binom{d+n}{n} = O(d^n)$ nonzero coefficients, we see that the dense or sparse representation of multivariate polynomials requires an exponential size, and their manipulation usually requires an exponential number of arithmetic operations with respect to the parameters d and n. In order to avoid this exponential behavior, we are going to use an alternative encoding of input, output and intermediate results of our computations by means of straight-line programs (cf. [27], [55], [45], [8]). A *straight-line program* β in $\mathsf{K}(X_1, \ldots, X_n)$ is a finite sequence of rational functions $(F_1, \ldots, F_k) \in \mathsf{K}(X_1, \ldots, X_n)^k$ such that for $1 \le i \le k$, the function F_i is either an element of the set $\{X_1, \ldots, X_n\}$, or an element of K (a *parameter*), or there exist $1 \le i_1, i_2 < i$ such that $F_i = F_{i_1} \circ_i F_{i_2}$ holds, where $\circ_i$ is one of the arithmetic operations $+, -, \times, \div$. The straight-line program β is called *division-free* if $\circ_i$ is different from $\div$ for $1 \le i \le k$. Two basic natural measures of the complexity of β are its *space* and *time* (cf. [7], [48]). Space is defined as the maximum number of arithmetic registers used in the evaluation process defined by β, and time is defined as the total number of arithmetic operations performed during the evaluation. We say that the straight-line program β *computes* or *represents* a subset S of $\mathsf{K}(X_1, \ldots, X_n)$ if $S \subset \{F_1, \ldots, F_k\}$ holds.

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*. Time and space of the evaluation of a given computation tree are defined analogously as in the case of straight-line programs (see, e.g., [56], [8] for more details on the notion of computation trees).

A difficult point in the manipulation of multivariate polynomials over finite fields is the so-called *identity testing problem*: given two elements F and G of $\mathsf{K}[X_1, \ldots, X_n]$, decide whether F and G represent the same polynomial function on K^n. Indeed, all known deterministic algorithms solving this problem have complexity at least $(\#\mathsf{K})^{\Omega(1)}$. In this article we are going to use *probabilistic* algorithms to solve the identity testing problem, based on the following result.

Theorem 2.2 ([39], [50]). *Let F be a nonzero polynomial of $\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ of degree at most d and let K be a finite field extension of $\mathbb{F}_q$. Then the number of zeros of F in K^n is at most $d(\#\mathsf{K})^{n-1}$.*

For the analysis of our algorithms, we shall interpret the statement of Theorem 2.2 in terms of probabilities. More precisely, given a fixed nonzero polynomial F in $\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ of degree at most d, we conclude from Theorem 2.2 that the probability of randomly choosing a point $a \in \mathsf{K}^n$ such that $F(a)=0$ holds is bounded from above by $d/\#\mathsf{K}$ (assuming a uniform distribution of probability on the elements of K^n).

3. On the preparation of the input data

From now on, let $n \geq 3$ and $d \geq 2$, and let $F_1,\dots,F_r \in \mathbb{F}_q[X_1,\dots,X_n]$ be polynomials of degree at most d that generate a radical ideal and form a regular sequence. Suppose further that $F_1,\dots,F_s$ generate a radical ideal for $1 \leq s \leq r-1$ and that $V_r := V(F_1,\dots,F_r)$ is absolutely irreducible.

In the sequel we shall consider algorithms which "solve" symbolically the input system $F_1=0,\dots,F_r=0$ over $\overline{\mathbb{F}}_q$. As in [21] and [20], we associate to the system $F_1=0,\dots,F_r=0$ a parameter δ, called the *degree of the system*, which is defined as follows: for $1 \leq s \leq r$, let $V_s \subset \mathbb{A}^n$ be the $\mathbb{F}_q$-variety defined by $F_1,\dots,F_s$ and let δ_s denote its degree. The geometric degree of the system $F_1=0,\dots,F_r=0$ is then defined as $\delta := \max_{1\leq s\leq r}\delta_s$.

In this section we are going to determine a genericity condition underlying the choice of a simultaneous Noether normalization of the varieties $V_1,\dots,V_r$ and lifting points $P^{(s)} \in \mathbb{A}^{n-s}$ ($1 \leq s \leq r$) such that, for $1 \leq s \leq r-1$, the lifting fiber $V_{P^{(s+1)}}$ has the following property: for any point $P \in V_{P^{(s+1)}}$, the morphism π_s is unramified at $\pi_s(P)$. By a simultaneous Noether normalization we understand a linear change of variables such that the new variables $Y_1,\dots,Y_n$ are in Noether position with respect to V_s for $1 \leq s \leq r$. Finally, we are going to find an affine linear subspace L of $\mathbb{A}^n$ of dimension $r+1$ such that $V_r \cap L$ is an absolutely irreducible curve of $\mathbb{A}^n$ of degree δ_r.

3.1. Simultaneous Noether normalization.

It is well known that a generic choice of linear forms $Y_1,\dots,Y_n$ yields a simultaneous Noether normalization of the varieties $V_1,\dots,V_r$. In order to prove the existence of a simultaneous Noether normalization defined over a given finite field extension of $\mathbb{F}_q$, we need suitable genericity conditions. The next proposition yields an upper bound on the degree of the genericity condition underlying the choice of such linear forms.

In what follows, for $1 \leq s \leq r$, we shall interpret the elements of $\mathbb{A}^{(n-s+1)(n+1)}$ as $(n-s+1)\times(n+1)$-matrices with entries in $\overline{\mathbb{F}}_q$. We denote such matrices as (λ,γ), where $\lambda \in \mathbb{A}^{(n-s+1)n}$ represents the entries of the submatrix formed by the first n columns of (λ,γ) and $\gamma \in \mathbb{A}^{n-s+1}$ denotes the last column of (λ,γ). The linear forms we are looking for will be given in the form $Y := (Y_1,\dots,Y_{n-s+1}) := \lambda X + \gamma$, with $X := (X_1,\dots,X_n)$.

Proposition 3.1. *Fix s with $1 \leq s \leq r$. Let $\Lambda := (\Lambda_{i,j})_{1\leq i\leq n-s+1, 1\leq j\leq n}$ be a matrix of indeterminates, let $\Lambda^{(i)} := (\Lambda_{i,1},\dots,\Lambda_{i,n})$ for $1 \leq i \leq n-s+1$, and let $\Gamma := (\Gamma_1,\dots,\Gamma_{n-s+1})$ be a vector of indeterminates. Let $\widetilde{Y} := \Lambda X + \Gamma$. Then there exists a nonzero polynomial $A_s \in \overline{\mathbb{F}}_q[\Lambda,\Gamma]$ of degree at most $2(n-s+2)\delta_s^2$*

with the following property: for any $(\lambda,\gamma)\in\mathbb{A}^{(n-s+1)(n+1)}$ *with* $A_s(\lambda,\gamma)\neq 0$*, if* $Y:=\lambda X+\gamma:=(Y_1,\dots,Y_{n-s+1})$*, then*

(i) *the mapping* $\pi_s:V_s\to\mathbb{A}^{n-s}$ *defined by* $Y_1,\dots,Y_{n-s}$ *is a finite morphism,*

(ii) *the linear form* Y_{n-s+1} *induces a primitive element of the integral ring extension* $R_s:=\overline{\mathbb{F}}_q[Y_1,\dots,Y_{n-s}]\hookrightarrow\overline{\mathbb{F}}_q[V_s]$.

Proof. Let us consider the following morphism of algebraic varieties:

$$\begin{array}{rccc}\Phi: & \mathbb{A}^{(n-s+1)(n+1)}\times V_s & \to & \mathbb{A}^{(n-s+1)(n+1)}\times\mathbb{A}^{n-s+1},\\ & (\lambda,\gamma,x) & \mapsto & (\lambda,\gamma,\lambda x+\gamma).\end{array}\tag{3.1}$$

Since Φ is the generic linear projection of V_s into $\mathbb{A}^{n-s+1}$, the Zariski closure $\overline{\mathrm{Im}(\Phi)}$ is a hypersurface of $\mathbb{A}^{(n-s+1)(n+1)}\times\mathbb{A}^{n-s+1}$, known as the Chow form of V_s (see, e.g., [47], [53]). In particular, we have that $\overline{\mathrm{Im}(\Phi)}$ is defined by a squarefree polynomial $P_{V_s}\in\overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s+1}]$ which satisfies the following degree estimates:

- $\deg_{\widetilde{Y}}P_{V_s}=\deg_{\widetilde{Y}_{n-s+1}}P_{V_s}=\delta_s$,
- $\deg_{\Lambda^{(i)},\Gamma_i}P_{V_s}\le\delta_s$ for $1\le i\le n-s+1$.

Let $A_{1,s}\in\overline{\mathbb{F}}_q[\Lambda,\Gamma]$ be the (nonzero) polynomial which arises as a coefficient of the monomial $\widetilde{Y}_{n-s+1}^{\delta_s}$ in the polynomial P_{V_s}, considering P_{V_s} as an element of $\overline{\mathbb{F}}_q[\Lambda,\Gamma][\widetilde{Y}]$. The above estimates imply $\deg A_{1,s}\le(n-s+1)\delta_s$. Let $\widetilde{A}_{1,s}\in\overline{\mathbb{F}}_q[\Lambda^{(i)},\Gamma_i:1\le i\le n-s]$ be a nonzero polynomial arising as the coefficient of a monomial of $A_{1,s}$, considering $A_{1,s}$ as an element of $\overline{\mathbb{F}}_q[\Lambda^{(i)},\Gamma_i:1\le i\le n-s][\Lambda^{(n-s+1)},\Gamma_{n-s+1}]$.

Let $(\lambda^*,\gamma^*)\in\mathbb{A}^{(n-s)(n+1)}$ be any point for which $\widetilde{A}_{1,s}(\lambda^*,\gamma^*)\neq 0$ holds, and let $Y:=(Y_1,\dots,Y_{n-s}):=\lambda^*X+\gamma^*$. We claim that condition (i) of the statement of Proposition 3.1 holds. Indeed, since $A^*_{1,s}:=A_{1,s}(\lambda^*,\gamma^*,\Lambda^{(n-s+1)},\Gamma_{n-s+1})$ is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda^{(n-s+1)},\Gamma_{n-s+1}]$, we deduce the existence of $\overline{\mathbb{F}}_q$-linearly independent vectors $w_1,\dots,w_n\in\mathbb{A}^n$ and values $a_1,\dots,a_n\in\mathbb{A}^1$ such that $A^*_{1,s}(w_j,a_j)\neq 0$ holds for $1\le j\le n$. Let $\ell_j:=w_jX+a_j$ for $1\le j\le n$. By construction, for $1\le j\le n$ the polynomial $P_{V_s}(\lambda^*,\gamma^*,w_j,a_j,Y_1,\dots,Y_{n-s},\ell_j)$ is an integral dependence equation for the coordinate function induced by ℓ_j in the ring extension $R_s\hookrightarrow\overline{\mathbb{F}}_q[V_s]$. Since $\overline{\mathbb{F}}_q[\ell_1,\dots,\ell_n]=\overline{\mathbb{F}}_q[X_1,\dots,X_n]$, we conclude that condition (i) holds.

Furthermore, since $\overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}]/(P_{V_s})$ is a reduced $\overline{\mathbb{F}}_q$-algebra and $\overline{\mathbb{F}}_q$ is a perfect field, from [42, Proposition 27.G] we conclude that the (zero-dimensional) $\overline{\mathbb{F}}_q(\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s})$-algebra $\overline{\mathbb{F}}_q(\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s})[\widetilde{Y}_{n-s+1}]/(P_{V_s})$ is reduced. This implies that P_{V_s} is a separable element of $\overline{\mathbb{F}}_q(\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s})[\widetilde{Y}_{n-s+1}]$, and hence P_{V_s} and $\partial P_{V_s}/\partial\widetilde{Y}_{n-s+1}$ are relatively prime in $\overline{\mathbb{F}}_q(\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s})[\widetilde{Y}_{n-s+1}]$. Then the discriminant

$$\rho_s:=\mathrm{Res}_{\widetilde{Y}_{n-s+1}}(P_{V_s},\partial P_{V_s}/\partial\widetilde{Y}_{n-s+1})\tag{3.2}$$

of P_{V_s} with respect to $\widetilde{Y}_{n-s+1}$ is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s}]$. It satisfies the following degree estimates:

- $\deg_{\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s}}\rho_s\le(2\delta_s-1)\delta_s$.
- $\deg_{\Lambda^{(i)},\Gamma_i}\rho_s\le(2\delta_s-1)\delta_s$ for $1\le i\le n-s+1$.

Let $\rho_{1,s}\in\overline{\mathbb{F}}_q[\Lambda,\Gamma]$ be a nonzero coefficient of a monomial of ρ_s, considering ρ_s as an element of $\overline{\mathbb{F}}_q[\Lambda,\Gamma][\widetilde{Y}_1,\dots,\widetilde{Y}_{n-s}]$, and let $A_s:=\rho_{1,s}\widetilde{A}_{1,s}$. Observe that

$\deg A_s \leq 2(n-s+2)\delta_s^2$ holds. Let $(\lambda,\gamma) \in \mathbb{A}^{(n-s+1)(n+1)}$ satisfy the condition $A_s(\lambda,\gamma) \neq 0$, let $Y := \lambda X + \gamma$ and denote by $(\lambda^*,\gamma^*) \in \mathbb{A}^{(n-s)(n+1)}$ the matrix formed by the first $n-s$ rows of (λ,γ). Let $P_{V_s}^*$ and ρ_s^* be the polynomials obtained from P_{V_s} and ρ_s by evaluating $\Lambda^{(i)},\Gamma_i$ $(1 \leq i \leq n-s)$ at (λ^*,γ^*). Then ρ_s^* is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda^{(n-s+1)},\Gamma_{n-s+1},Y_1,\dots,Y_{n-s}]$ which equals the discriminant of $P_{V_s}^*(\Lambda^{(n-s+1)},\Gamma_{n-s+1},Y_1,\dots,Y_{n-s},\widetilde{Y}_{n-s+1})$ with respect to $\widetilde{Y}_{n-s+1}$. It is clear that condition (i) holds. We claim that condition (ii) holds.

Let $\xi_1,\dots,\xi_n$ be the coordinate functions of V_s induced by $X_1,\dots,X_n$, let $\zeta_i := \sum_{k=1}^n \lambda_{i,k}\xi_k + \gamma_i$ for $1 \leq i \leq n-s$, and let $\widehat{Y}_{n-s+1} := \sum_{k=1}^n \Lambda_{n-s+1,k}\,\xi_k + \Gamma_{n-s+1}$. From the definition of the Chow form of V_s we conclude that the identity

$$\begin{aligned}0 &= P_{V_s}^*(\Lambda^{(n-s+1)},\Gamma_{n-s+1},\zeta_1,\dots,\zeta_{n-s},\widehat{Y}_{n-s+1})\\ &= P_{V_s}^*(\Lambda^{(n-s+1)},\Gamma_{n-s+1},\zeta_1,\dots,\zeta_{n-s},\textstyle\sum_{k=1}^n \Lambda_{n-s+1,k}\,\xi_k + \Gamma_{n-s+1})\end{aligned} \tag{3.3}$$

holds in $\overline{\mathbb{F}}_q[\Lambda^{(n-s+1)},\Gamma_{n-s+1}] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$. Following, e.g., [1] or [46], taking the partial derivative with respect to the variable $\Lambda_{n-s+1,k}$ at both sides of (3.3) we deduce that the following identity holds in $\overline{\mathbb{F}}_q[\Lambda^{(n-s+1)},\Gamma_{n-s+1}] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$ for $1 \leq k \leq n$:

$$\begin{aligned}&(\partial P_{V_s}^*/\partial \widetilde{Y}_{n-s+1})(\Lambda^{(n-s+1)},\Gamma_{n-s+1},\zeta_1,\dots,\zeta_{n-s},\widehat{Y}_{n-s+1})\xi_k\\ &\quad + (\partial P_{V_s}^*/\partial \Lambda_{n-s+1,k})(\Lambda^{(n-s+1)},\Gamma_{n-s+1},\zeta_1,\dots,\zeta_{n-s},\widehat{Y}_{n-s+1}) = 0.\end{aligned} \tag{3.4}$$

Since ρ_s^* is the discriminant of the polynomial $P_{V_s}^*$ with respect to $\widetilde{Y}_{n-s+1}$, it can be written as a linear combination of $P_{V_s}^*$ and $\partial P_{V_s}^*/\partial \widetilde{Y}_{n-s+1}$. Combining this observation with (3.3) and (3.4) we conclude that

$$\begin{aligned}&\rho_s^*(\Lambda^{(n-s+1)},\Gamma_{n-s+1},\zeta_1,\dots,\zeta_{n-s})\xi_k\\ &\quad + P_k(\Lambda^{(n-s+1)},\Gamma_{n-s+1},\zeta_1,\dots,\zeta_{n-s},\widehat{Y}_{n-s+1}) = 0\end{aligned} \tag{3.5}$$

holds, where P_k is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda^{(n-s+1)},\Gamma_{n-s+1},Z_1,\dots,Z_{n-s+1}]$ for $1 \leq k \leq n$. Substituting $\lambda_{n-s+1,k}$ for $\Lambda_{n-s+1,k}$ $(1 \leq k \leq n)$ and γ_{n-s+1} for Γ_{n-s+1} in identity (3.5), we conclude that the coordinate function of $\overline{\mathbb{F}}_q[V_s]$ defined by Y_{n-s+1} is a primitive element of the $\overline{\mathbb{F}}_q$-algebra extension $\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s}) \hookrightarrow \overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s}) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$.

Condition (i) implies that $\overline{\mathbb{F}}_q[V_s]$ is a finite free $R_s := \overline{\mathbb{F}}_q[Y_1,\dots,Y_{n-s}]$-module and hence $\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s}) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$ is a finite-dimensional $\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s})$-vector space. Furthermore, the dimension of

$$\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s}) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$$

as an $\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s})$-vector space equals the rank of $\overline{\mathbb{F}}_q[V_s]$ as an R_s-module. On the other hand, since R_s is integrally closed, the minimal dependence equation of any element $f \in \overline{\mathbb{F}}_q[V_s]$ over $\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s})$ equals the minimal integral dependence equation of f over R_s (see, e.g., [36, Lemma II.2.15]). Combining this remark with the fact that Y_{n-s+1} induces a primitive element of the $\overline{\mathbb{F}}_q$-algebra extension

$$\overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s}) \hookrightarrow \overline{\mathbb{F}}_q(Y_1,\dots,Y_{n-s}) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s],$$

we conclude that Y_{n-s+1} also induces a primitive element of the $\overline{\mathbb{F}}_q$-algebra extension $R_s \hookrightarrow \overline{\mathbb{F}}_q[V_s]$. This shows that condition (ii) holds and finishes the proof of the proposition. $\square$

3.2. **Lifting fibers not meeting a discriminant.** Our second step is to find lifting points $P^{(s+1)} \in \mathbb{A}^{n-s-1}$ for $0 \leq s \leq r-1$ such that the corresponding lifting fiber $V_{P^{(s+1)}}$ has the following property: for any point $P \in V_{P^{(s+1)}}$, the morphism π_s is unramified at $\pi_s(P)$. With this condition we shall be able to find a geometric solution of the variety V_s such that no point $P \in V_{P^{(s+1)}}$ annihilates the discriminant of the corresponding minimal polynomial $q^{(s)}$. This in turn will allow us to avoid dealing with multiplicities during the computations.

For this purpose we need the following technical result. It is a slightly simplified version of [29, Lemma 1 (*iii*)] with an improved degree estimate.

Lemma 3.2. *With notations and assumptions as above, fix s with $1 \leq s \leq r$. Let A_s be the polynomial of the statement of Proposition* 3.1*, and let $H \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, X]$ be a polynomial of degree at most D. Suppose that the Zariski closure $\widehat{V}_s$ of the set $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{H = 0, A_s \neq 0\}$ satisfies the condition* $\dim \widehat{V}_s \leq (n-s+1)(n+2)-2$*. Then the Zariski closure of the image of $\widehat{V}_s$ under the morphism $\Phi^* : \mathbb{A}^{(n-s+1)(n+1)} \times V_s \to \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ defined by $\Phi^*(\lambda, \gamma, x) := (\lambda, \gamma, \lambda^* x + \gamma^*)$ is contained in a hypersurface of $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ of degree at most $2(n-s+2)D\delta_s^2$ (here λ^* and γ^* denote the first $n-s$ rows of λ and γ, respectively).*

Proof. We use the notations of the proof of Proposition 3.1. Since the Chow form P_{V_s} of the variety V_s is a separable element of $\overline{\mathbb{F}}_q(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s})[\widetilde{Y}_{n-s+1}]$, we conclude that $\partial P_{V_s}/\partial \widetilde{Y}_{n-s+1}$ is not a zero divisor of $\overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}]/(P_{V_s})$, and hence of the $\overline{\mathbb{F}}_q$-algebra $\overline{\mathbb{F}}_q[\Lambda, \Gamma] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$. Taking the partial derivative with respect to the variable $\Lambda_{n-s+1,k}$ at both sides of the identity $P_{V_s}(\Lambda, \Gamma, \widehat{Y}) = 0$ of $\overline{\mathbb{F}}_q[\Lambda, \Gamma] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$ for $1 \leq k \leq n$, we see that the following identity holds in $\overline{\mathbb{F}}_q[\Lambda, \Gamma] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$ (cf. [1], [46]):

$$(3.6) \qquad (\partial P_{V_s}/\partial \widetilde{Y}_{n-s+1})(\Lambda, \Gamma, \widehat{Y})\, \xi_k + (\partial P_{V_s}/\partial \Lambda_{n-s+1,k})(\Lambda, \Gamma, \widehat{Y}) = 0,$$

where $\widehat{Y} := \Lambda \xi + \Gamma$ and $\xi := (\xi_1, \ldots, \xi_n)$ is the vector of coordinate functions of V_s induced by X.

Let $\widehat{H} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}]$ be the polynomial obtained by replacing in H the variable X_k by $-(\partial P_{V_s}/\partial \widetilde{Y}_{n-s+1})^{-1}(\partial P_{V_s}/\partial \Lambda_{n-s+1,k})$ for $1 \leq k \leq n$ and clearing denominators. Observe that $\deg_{\widetilde{Y}} \widehat{H} = \deg_{\widetilde{Y}_{n-s+1}} \widehat{H} \leq D\delta_s$ and $\deg_{\Lambda,\Gamma} \widehat{H} \leq (n-s+1)D\delta_s$ holds.

Let $R := \mathrm{Res}_{\widetilde{Y}_{n-s+1}}(P_{V_s}, \widehat{H}) \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}]$ be the resultant of P_{V_s} and $\widehat{H}$ with respect to the variable $\widetilde{Y}_{n-s+1}$. Observe that the Sylvester matrix of P_{V_s} and $\widehat{H}$ is a matrix of size at most $(D+1)\delta_s \times (D+1)\delta_s$ with at most $D\delta_s$ columns consisting of coefficients of P_{V_s} or zero entries, and δ_s columns consisting of coefficients of $\widehat{H}$ or zero entries. This shows that $\deg R \leq 2(n-s+2)D\delta_s^2$ holds. On the other hand, from identity (3.6) and the properties of the resultant we conclude that $R(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s})$ vanishes on the variety $\widehat{V}_s$. Furthermore, the assumption $\dim \widehat{V}_s \leq (n-s+1)(n+2)-2$ implies $R(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}) \neq 0$. This finishes the proof of the lemma. □

Now we are ready to prove the main theorem of this section. This result states an appropriate upper bound for the degree of a certain polynomial. The nonvanishing of this polynomial expresses a suitable genericity condition for the coefficients of the linear forms $Y_1, \dots, Y_n$ and the coordinates of the lifting points $P^{(s+1)}$ $(1 \le s \le r-1)$ we are looking for. We remark that a similar result is proved in [29, Theorem 3] for a $\mathbb{Q}$-definable affine equidimensional variety of $\mathbb{C}^n$. Unfortunately, the proof of [29, Theorem 3] makes essential use of the fact that the underlying variety is defined over $\mathbb{Q}$ and therefore cannot be used in our situation. Furthermore, we obtain a significant improvement of the degree estimates of [29, Theorem 3]. This is a critical point for our subsequent purposes.

Theorem 3.3. *Let notations be as in Proposition* 3.1 *and fix s with $1 \le s < r$. Then there exists a nonzero polynomial $B_s \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \dots, \widetilde{Y}_{n-s}]$, of degree at most $4(n-s+3)^2 nd\delta_s^2\delta_{s+1}^2$, such that for any $(\lambda, \gamma, P) \in \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ with $B_s(\lambda, \gamma, P) \neq 0$ the following conditions are satisfied: if $Y := (Y_1, \dots, Y_{n-s+1}) := \lambda X + \gamma$, then*

- (i) *the mapping $\pi_s : V_s \to \mathbb{A}^{n-s}$ defined by $Y_1, \dots, Y_{n-s}$ is a finite morphism, $P \in \mathbb{A}^{n-s}$ is a lifting point of π_s, and Y_{n-s+1} is a primitive element of $\pi_s^{-1}(P)$.*
- (ii) *Let $P^* \in \mathbb{A}^{n-s-1}$ be the vector that consists of the first $n-s-1$ coordinates of P. Then the mapping $\pi_{s+1} : V_{s+1} \to \mathbb{A}^{n-s-1}$ defined by $Y_1, \dots, Y_{n-s-1}$ is a finite morphism, P^* is a lifting point of π_{s+1}, and Y_{n-s} is a primitive element of $\pi_{s+1}^{-1}(P^*)$.*
- (iii) *Any point $Q \in \pi_s\big(\pi_{s+1}^{-1}(P^*)\big)$ is a lifting point of π_s, and Y_{n-s+1} is a primitive element of $\pi_s^{-1}(Q)$ for any $Q \in \pi_s\big(\pi_{s+1}^{-1}(P^*)\big)$.*

Proof. Let A_s and A_{s+1} be the polynomials obtained by applying Proposition 3.1 to the varieties V_s and V_{s+1}, respectively. Let $D_s, D_{s+1} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, X]$ be the following polynomials:

$$D_s := \det \begin{pmatrix} \Lambda_{1,1} & \cdots & \Lambda_{1,n} \\ \vdots & & \vdots \\ \Lambda_{n-s,1} & \cdots & \Lambda_{n-s,n} \\ \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_s}{\partial X_1} & \cdots & \frac{\partial F_s}{\partial X_n} \end{pmatrix}, \quad D_{s+1} := \det \begin{pmatrix} \Lambda_{1,1} & \cdots & \Lambda_{1,n} \\ \vdots & & \vdots \\ \Lambda_{n-s-1,1} & \cdots & \Lambda_{n-s-1,n} \\ \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_{s+1}}{\partial X_1} & \cdots & \frac{\partial F_{s+1}}{\partial X_n} \end{pmatrix}.$$

We claim that the Zariski closure of the set $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0, A_s \neq 0\}$ is empty or an equidimensional affine subvariety of $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^n$ of dimension $(n-s+1)(n+2)-2$.

In order to prove this claim, let $V_s = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_N$ be the decomposition of V_s into irreducible components. Then we have that $\mathbb{A}^{(n-s+1)(n+1)} \times V_s = \bigcup_{i=1}^N \mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}_i$ is the decomposition of $\mathbb{A}^{(n-s+1)(n+1)} \times V_s$ into irreducible components. Let $\mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}$ be any of these irreducible components and let $x \in \mathcal{C}$ be a nonsingular point of V_s. Then $D_s(\Lambda, x) \neq 0$ holds and therefore there exists $\lambda \in \mathbb{A}^{(n-s+1)n}$ such that $D_s(\lambda, x) \neq 0$ holds. This shows that there exists a point $(\lambda, \gamma, x) \in \mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}$ not belonging to the hypersurface $\{D_s = 0\}$. On the other hand, $D_s(0, x) = 0$ holds for any $x \in V_s$, where 0 represents the zero matrix of $\mathbb{A}^{(n-s+1)n}$. This proves that $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0\}$ is an equidimensional variety of dimension $(n-s+1)(n+2)-2$, and hence the Zariski closure of the set $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0, A_s \neq 0\}$ is either empty or an equidimensional variety of dimension $(n-s+1)(n+2)-2$. This proves the claim.

A similar argument shows that the Zariski closure of the set

$$(\mathbb{A}^{(n-s)(n+1)} \times V_{s+1}) \cap \{D_{s+1} = 0, A_{s+1} \neq 0\}$$

is empty or an equidimensional affine subvariety of $\mathbb{A}^{(n-s)(n+1)} \times \mathbb{A}^n$ of dimension $(n-s)(n+2)-2$. We leave the details to the reader.

Consider the following morphisms:

$$\begin{aligned} \Phi_s : (\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0, A_s \neq 0\} &\to \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s} \\ (\lambda, \gamma, x) &\mapsto \big(\lambda, \gamma, Y_1(x), \ldots, Y_{n-s}(x)\big), \\ \Phi_{s+1} : (\mathbb{A}^{(n-s)(n+1)} \times V_{s+1}) \cap \{D_{s+1} = 0, A_{s+1} \neq 0\} &\to \mathbb{A}^{(n-s)(n+1)} \times \mathbb{A}^{n-s-1} \\ (\lambda^*, \gamma^*, x) &\mapsto \big(\lambda^*, \gamma^*, Y_1(x), \ldots, Y_{n-s-1}(x)\big). \end{aligned}$$

From the claims above and Lemma 3.2 we deduce that the Zariski closure of $\mathrm{Im}(\Phi_s)$ is contained in a hypersurface of $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ of degree at most $2(n-s+2)n(d-1)\delta_s^2$, and the Zariski closure of $\mathrm{Im}(\Phi_{s+1})$ is contained in a hypersurface of $\mathbb{A}^{(n-s)(n+1)} \times \mathbb{A}^{n-s-1}$ of degree at most $2(n-s+1)n(d-1)\delta_{s+1}^2$. We denote by $\widehat{B}_s \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}]$ and $\widehat{B}_{s+1} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s-1}]$ the polynomials defining these hypersurfaces, respectively.

Let $\rho_s, \rho_{s+1} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}]$ be the (nonzero) discriminants of the varieties V_s and V_{s+1}, as defined in (3.2) of the proof of Proposition 3.1. Recall that $\deg \rho_s \leq (n-s+2)(2\delta_s^2 - \delta_s)$ and $\deg \rho_{s+1} \leq (n-s+1)(2\delta_{s+1}^2 - \delta_{s+1})$ holds.

Claim. The Zariski closure of the set $(\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}) \cap \{\rho_s \widehat{B}_s = 0, A_{s+1} \neq 0\}$ has dimension at most $(n-s+1)(n+2)-3$.

Proof of Claim. We observe that the mapping Φ_s above can be regularly extended to $\mathbb{A}^{(n-s+1)(n+1)} \times V_s$. From the definition of the polynomial A_s, we deduce that this extension induces the following finite morphism, denoted also by Φ_s with a slight abuse of notation:

$$\begin{aligned} \Phi_s : (\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{A_s \neq 0\} &\to \big(\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}\big) \cap \{A_s \neq 0\} \\ (\lambda, \gamma, x) &\mapsto \big(\lambda, \gamma, Y_1(x), \ldots, Y_{n-s}(x)\big). \end{aligned}$$

Since $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0, A_s \neq 0\}$ is an equidimensional subvariety of $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{A_s \neq 0\}$ of dimension $(n-s+2)(n+1)-2$, we see that $\Phi_s(\{D_s = 0\})$ is a hypersurface of $(\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}) \cap \{A_s \neq 0\}$, which is therefore definable by the polynomial $\widehat{B}_s$. This means that the identity

$$\Phi_s(\{D_s = 0, A_s \neq 0\}) = \{\widehat{B}_s = 0, A_s \neq 0\}$$

holds.

From the cylindrical structure of the variety $\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}$ we conclude that no irreducible component of this variety is contained in $\{A_s = 0\}$. This implies that $\mathcal{D} \cap \{A_s \neq 0\}$ is a dense open subset of $\mathcal{D}$ for any irreducible component $\mathcal{D}$ of $\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}$. Suppose that there exists an irreducible component $\mathcal{D}$ of $\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}$ contained in $\Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\})$. Then

$$\mathcal{D} \cap \{A_s \neq 0\} \subset \Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\}) \cap \{A_s \neq 0\} = \Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\} \cap \{A_s \neq 0\}),$$

which implies

$$\Phi_s(\mathcal{D} \cap \{A_s \neq 0\}) \subset \Phi_s \circ \Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\} \cap \{A_s \neq 0\}) \subset \{\rho_s \widehat{B}_s = 0\} \cap \{A_s \neq 0\}.$$

We conclude that $\Phi_s(\mathcal{D}) \subset \{\rho_s \widehat{B}_s = 0\}$ holds. Now we are going to show that the condition $\Phi_s(\mathcal{D}) \subset \{\rho_s \widehat{B}_s = 0\}$ leads to a contradiction. Indeed, we observe that there exists an irreducible component $\mathcal{D}_0$ of V_{s+1} for which $\mathcal{D} = \mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{D}_0$ holds. Let $x \in \mathcal{D}_0$ be a nonsingular point of V_{s+1}, which is also a nonsingular point of V_s. Hence, for a generic choice of a point $(\lambda, \gamma) \in \mathbb{A}^{(n-s+1)(n+1)}$, the fiber $W_s := V_s \cap \{\lambda^* X + \gamma^* = \lambda^* x + \gamma^*\}$ is unramified (see, e.g., [44, §5A]) and the linear form $\lambda^{(n-s+1)} X + \gamma_{n-s+1}$ separates the points of W_s. This shows that any point $y \in V_s \cap \{\lambda^* X + \gamma^* = \lambda^* x + \gamma^*\}$ satisfies the conditions $D_s(\lambda, \gamma, y) \neq 0$ and $\rho_s(\lambda, \gamma, y) \neq 0$. We conclude that the point $(\lambda, \gamma, \lambda^* x + \gamma^*)$ belongs to the set $\Phi_s(\mathcal{D}) \setminus \{\rho_s \widehat{B}_s = 0\}$, thus contradicting the condition $\Phi_s(\mathcal{D}) \subset \{\rho_s \widehat{B}_s = 0\}$. This finishes the proof of our claim. □

From the claim and Lemma 3.2 we deduce that the image of the morphism

$$\begin{aligned} \Psi_s : (\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}) \cap \{\rho_s \widehat{B}_s = 0, A_{s+1} \neq 0\} &\to \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s-1} \\ (\lambda, \gamma, x) &\mapsto \big(\lambda, \gamma, Y_1(x), \dots, Y_{n-s-1}(x)\big) \end{aligned}$$

is contained in a hypersurface of $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s-1}$ of degree at most $4(n-s+2)^2 nd\delta_s^2 \delta_{s+1}^2$. Let $\widetilde{B}_s$ denote the defining equation of this hypersurface.

Let $B_s := A_s A_{s+1} \rho_s \rho_{s+1} \widehat{B}_s \widehat{B}_{s+1} \widetilde{B}_s$. Observe that $\deg B_s \leq 4(n-s+3)^2 nd\delta_s^2 \delta_{s+1}^2$ holds. Let $(\lambda, \gamma, P) \in \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ be a point satisfying $B_s(\lambda, \gamma, P) \neq 0$. We claim that (λ, γ, P) satisfies conditions (i), (ii), and (iii) of the statement of Theorem 3.3. Let (λ^*, γ^*) denote the first $n-s$ rows of (λ, γ) and let P^* denote the vector consisting of the first $n-s-1$ coordinates of P. Since $A_s(\lambda, \gamma) A_{s+1}(\lambda^*, \gamma^*) \neq 0$ holds, from Proposition 3.1 we conclude that the mappings $\pi_s : V_s \to \mathbb{A}^{n-s}$ and $\pi_{s+1} : V_{s+1} \to \mathbb{A}^{n-s-1}$ defined by the linear forms $Y_1, \dots, Y_{n-s}$ and $Y_1, \dots, Y_{n-s-1}$ are finite morphisms. Since $A_s(\lambda, \gamma) \neq 0$ holds, the condition $\widehat{B}_s(\lambda, \gamma, P) \neq 0$ implies that $D_s(\lambda, \gamma, x) \neq 0$ holds for any $x \in \pi_s^{-1}(P)$. Therefore, we see that P is a lifting point of the morphism π_s. A similar argument as above shows that P^* is a lifting point of the morphism π_{s+1}. Finally, the conditions $\rho_s(\lambda, \gamma, P) \neq 0$ and $\rho_{s+1}(\lambda^*, \gamma^*, P^*) \neq 0$ show that Y_{n-s+1} and Y_{n-s} are primitive elements of $\pi_s^{-1}(P)$ and $\pi_{s+1}^{-1}(P^*)$, respectively. On the other hand, the conditions $\widetilde{B}_s(\lambda, \gamma, P^*) \neq 0$ and $A_{s+1}(\lambda^*, \gamma^*) \neq 0$ imply that $(\rho_s \widehat{B}_s)\big(\lambda, \gamma, P^*, Y_{n-s}(x)\big) \neq 0$ holds for any $x \in \pi_{s+1}^{-1}(P^*)$. Therefore, since $A_s(\lambda, \gamma) \neq 0$ holds, we deduce that $D_s(\lambda, \gamma, Q) \neq 0$ and $\rho_s(\lambda, \gamma, \pi_s(Q)) \neq 0$ hold for any point $Q \in \pi_s^{-1}(P^*, Y_{n-s}(x))$ with $x \in \pi_{s+1}^{-1}(P^*)$. This shows that condition (iii) of the statement of Theorem 3.3 holds. □

In order to find a rational point of our input variety V we are going to determine a suitable absolutely irreducible plane $\mathbb{F}_q$-curve of the form $V \cap L$, where L is an $\mathbb{F}_q$-definable affine linear subspace of $\mathbb{A}^n$ of dimension $r+1$. For this purpose, we are going to find an $\mathbb{F}_q$-definable Noether normalization of V, represented by a ($\mathbb{F}_q$-definable) finite linear projection $\pi : V \to \mathbb{A}^{n-r}$, and a lifting point $P \in \mathbb{F}_q^{n-r}$ of π. Unfortunately, the existence of the morphism π and the point P cannot be guaranteed unless the number of elements of $\mathbb{F}_q$ is high enough. Our next result exhibits a genericity condition underlying the choice of π and P whose degree depends on $\delta_r := \deg V_r$, rather than on $\delta := \max_{1 \leq s \leq r} \delta_s$.

Corollary 3.4. *With notations as in Proposition* 3.1 *and Theorem* 3.3*, there exists a nonzero polynomial* $\widehat{B} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \dots, \widetilde{Y}_{n-r}]$ *of degree at most*

$$(n-r+2)(2nd\delta_r^2 - \delta_r)$$

such that for any $(\lambda,\gamma,P)\in\mathbb{A}^{(n-r+1)(n+1)}\times\mathbb{A}^{n-r}$ *with* $\widehat{B}(\lambda,\gamma,P)\neq 0$ *the following conditions are satisfied.*

Let $Z:=(Z_1,\dots,Z_{n-r+1}):=\lambda X+\gamma$. *Then the mapping* $\pi:V_r\to\mathbb{A}^{n-r}$ *defined by* $\pi(x):=\big(Z_1(x),\dots,Z_{n-r}(x)\big)$ *is a finite morphism,* $P\in\mathbb{A}^{n-r}$ *is a lifting point of* π, *and* Z_{n-r+1} *is a primitive element of* $\pi^{-1}(P)$.

Proof. Let $\widehat{B}:=A_r\rho_r\widehat{B}_r$, where A_r is the polynomial of the statement of Proposition 3.1, the polynomial $\widehat{B}_r$ is that of the proof of Theorem 3.3 with $s=r-1$, and ρ_r is the discriminant introduced in (3.2) of the proof of Proposition 3.1. Observe that $\deg\widehat{B}\le(n-r+2)(2nd\delta_r^2-\delta_r)$ holds. Now, if $(\lambda,\gamma,P)\in\mathbb{A}^{(n-r+1)(n+1)}\times\mathbb{A}^{n-r}$ is any point for which $\widehat{B}(\lambda,\gamma,P)\neq 0$ holds, a similar argument as in the last paragraph of the proof of Theorem 3.3 shows that the linear forms $Z:=\lambda X+\gamma$ and the point P satisfy the conditions in the statement of the corollary. $\square$

Combining Theorem 2.2 and Corollary 3.4 we conclude that, if

$$q>(n-r+2)(2nd\delta_r^2-\delta_r)$$

holds, then there exists an $\mathbb{F}_q$-definable Noether normalization of the variety V and a lifting point $P\in\mathbb{F}_q^{n-r}$ of π.

3.3. **A reduction to the bidimensional case.** In this section we finish our considerations about the preparation of the input data by reducing our problem of computing a rational point of the absolutely irreducible $\mathbb{F}_q$-variety $V:=V_r$ to that of computing a rational point of an absolutely irreducible plane $\mathbb{F}_q$-curve. For this purpose, we have the first Bertini theorem (see, e.g., [54, §II.6.1, Theorem 1]), which asserts that the intersection $V\cap L$ of V with a generic affine linear subspace L of $\mathbb{A}^n$ of dimension $r+1$ is an absolutely irreducible plane curve. If $V\cap L$ is an absolutely irreducible $\mathbb{F}_q$-curve, then Weil's estimate (see, e.g., [39], [50]) assures that we have a "good probability" of finding a rational point in $V\cap L$. The main result of this section exhibits an estimate on the degree of the genericity condition underlying the choice of L.

Let $(\lambda,\gamma,P)\in\mathbb{A}^{(n-r+1)(n+1)}\times\mathbb{A}^{n-r}$ be a point for which $\widehat{B}(\lambda,\gamma,P)\neq 0$ holds, where $\widehat{B}$ is the polynomial of Corollary 3.4. Let $(Z_1,\dots,Z_{n-r+1})=\lambda X+\gamma$, let $Y_{n-r+2},\dots,Y_n$ be linear forms such that $Z_1,\dots,Z_{n-r+1},Y_{n-r+2},\dots,Y_n$ are $\overline{\mathbb{F}}_q$-linearly independent, and let $P:=(p_1,\dots,p_{n-r})$. Then the mapping $\pi:V\to\mathbb{A}^{n-r}$ defined by $\pi(x):=\big(Z_1(x),\dots,Z_{n-r}(x)\big)$ is a finite morphism, and therefore the image $W:=\widetilde{\pi}(V)$ of V under the mapping $\widetilde{\pi}:V\to\mathbb{A}^{n-r+1}$ defined by $\widetilde{\pi}(x):=\big(Z_1(x),\dots,Z_{n-r+1}(x)\big)$ is a hypersurface of $\mathbb{A}^{n-r+1}$. The choice of $Z_1,\dots,Z_{n-r+1}$ implies that this hypersurface has degree δ_r and is defined by a polynomial $q^{(r)}\in\overline{\mathbb{F}}_q[Z_1,\dots,Z_{n-r+1}]$ that is monic in Z_{n-r+1}.

Let $\widetilde{V}:=\{x\in\mathbb{A}^n:(\partial q^{(r)}/\partial Z_{n-r+1})(Z_1(x),\dots,Z_{n-r+1}(x))=0\}$ and $\widetilde{W}:=\{z\in\mathbb{A}^{n-r+1}:(\partial q^{(r)}/\partial Z_{n-r+1})(z)=0\}$. Our following result shows that the variety V is birationally equivalent to the hypersurface $W\subset\mathbb{A}^{n-r+1}$.

Lemma 3.5. *The map* $\widetilde{\pi}|_{V\setminus\widetilde{V}}:V\setminus\widetilde{V}\to W\setminus\widetilde{W}$ *is an isomorphism of Zariski open sets.*

Proof. We observe that $\widetilde{\pi}(V\setminus\widetilde{V})\subset W\setminus\widetilde{W}$ holds. Then $\widetilde{\pi}|_{V\setminus\widetilde{V}}:V\setminus\widetilde{V}\to W\setminus\widetilde{W}$ is a well-defined morphism.

We claim that $\widetilde{\pi}$ is an injective mapping. Indeed, making the substitutions $\Lambda_{n-r+1,j} := \lambda_{n-r+1,j}$ $(1 \leq j \leq n)$ and $\Gamma_{n-r+1} = \gamma_{n-r+1}$ in identity (3.4) of the proof of Proposition 3.1, we deduce that there exist polynomials $v_1, \ldots, v_n \in \overline{\mathbb{F}}_q[Z_1, \ldots, Z_{n-r+1}]$ such that for $1 \leq k \leq n$ the following identity holds:

$$(3.7)\quad v_k(Z_1, \ldots, Z_{n-r+1}) - X_k \cdot (\partial q^{(r)}/\partial Z_{n-r+1})(Z_1, \ldots, Z_{n-r+1}) \equiv 0 \bmod I(V)\ .$$

Let $x := (x_1, \ldots, x_n), x' := (x'_1, \ldots, x'_n) \in V \setminus \widetilde{V}$ satisfy $\widetilde{\pi}(x) = \widetilde{\pi}(x')$. We have $Z_k(x) = Z_k(x')$ for $1 \leq k \leq n-r+1$. Then from (3.7) we conclude that $x_k = x'_k$ for $1 \leq k \leq n$, which shows our claim.

Now we show that $\widetilde{\pi}|_{V\setminus\widetilde{V}} : V \setminus \widetilde{V} \to W \setminus \widetilde{W}$ is a surjective mapping. Let $q_0 := \partial q^{(r)}/\partial Z_{n-r+1}$. Let $z := (z_1, \ldots, z_{n-r+1})$ be an arbitrary point of $W \setminus \widetilde{W}$, and let

$$x := \big((v_1/q_0)(z), \ldots, (v_n/q_0)(z)\big).$$

We claim that x belongs to $V \setminus \widetilde{V}$. Indeed, let F be an arbitrary element of the ideal $I(V)$ and let $\widetilde{F} := (q_0(Z_1, \ldots, Z_{n-r+1}))^N F$, where $N := \deg F$. Then there exists $G \in \overline{\mathbb{F}}_q[T_1, \ldots, T_{n+1}]$ such that $\widetilde{F} = G(q_0X_1, \ldots, q_0X_n, q_0)$ holds. Since $\widetilde{F} \in I(V)$, for any $z' \in V$ we have $\widetilde{F}(z') = 0$, and hence from (3.7) we conclude that $G(v_1, \ldots, v_n, q_0)(Z_1(z'), \ldots, Z_{n-r+1}(z')) = 0$ holds. This shows that $q^{(r)}$ divides $\widehat{F} := G(v_1, \ldots, v_n, q_0)$ in $\overline{\mathbb{F}}_q[Z_1, \ldots, Z_{n-r+1}]$, and therefore $\widehat{F}(z) = q_0(z)^N F(x) = 0$ holds. Taking into account that $q_0(z) \neq 0$ we conclude that $F(x) = 0$ holds, i.e., $x \in V \setminus \widetilde{V}$.

In order to finish the proof of the surjectivity of $\widetilde{\pi}$ there remains to prove that $\widetilde{\pi}(x) = z$ holds. We observe that (3.7) shows that any $z' \in V$ satisfies

$$Z_i(z')q_0\big(Z_1(z'), \ldots, Z_{n-r+1}(z')\big) - \sum_{k=1}^{n} \lambda_{i,\,k}\, v_k\big(Z_1(z'), \ldots, Z_{n-r+1}(z')\big) = 0$$

for $1 \leq i \leq n-r+1$. Then $q^{(r)}$ divides the polynomial $Z_iq_0 - \sum_{k=1}^n \lambda_{i,k}v_k$ in $\overline{\mathbb{F}}_q[Z_1, \ldots, Z_{n-r+1}]$, which implies $z_i = \sum_{k=1}^n \lambda_{i,\,k}(v_k/q_0)(z) = \sum_{k=1}^n \lambda_{i,\,k}\, x_k$ for $1 \leq i \leq n-r+1$. This proves that $\widetilde{\pi}(x) = z$ holds.

Finally we show that $\widetilde{\pi}|_{V\setminus\widetilde{V}} : V \setminus \widetilde{V} \to W \setminus \widetilde{W}$ is an isomorphism. Let

$$\begin{array}{rcrcl} \phi & : & W \setminus \widetilde{W} & \to & V \setminus \widetilde{V}, \\ & & z & \mapsto & \big((v_1/q_0)(z), \ldots, (v_n/q_0)(z)\big). \end{array}$$

Our previous discussion shows that ϕ is a well-defined morphism. Furthermore, our arguments above show that $\widetilde{\pi} \circ \phi$ is the identity mapping of $W \setminus \widetilde{W}$. This finishes the proof of the lemma. □

We remark that a similar result for the varieties $V_1, \ldots, V_{r-1}$ can be easily established following the proof of Lemma 3.5.

Now we prove the main result of this section.

Theorem 3.6. *Let notations and assumptions be as above. Suppose further that the variety $V := V_r$ is absolutely irreducible. Let $\Omega := (\Omega_1, \ldots, \Omega_{n-r})$ and T be new indeterminates. Then there exists a nonzero polynomial $C \in \overline{\mathbb{F}}_q[\Omega]$ of degree at most $2\delta_r^4$ with the following property: let $\omega := (\omega_1, \ldots, \omega_{n-r}) \in \mathbb{A}^{n-r}$ satisfy $C(\omega) \neq 0$, and let L_ω be the $(r+1)$-dimensional affine linear subvariety of $\mathbb{A}^n$ parametrized by $Z_k = \omega_k T + p_k$ $(1 \leq k \leq n-r)$. Then $V \cap L_\omega$ is an absolutely irreducible affine variety of dimension* 1.

Proof. Lemma 3.5 shows that V is birational to the hypersurface $W \subset \mathbb{A}^{n-r+1}$ defined by $\{q^{(r)}(Z_1,\dots,Z_{n-r+1}) = 0\}$. Since V is absolutely irreducible, we conclude that W is absolutely irreducible and therefore $q^{(r)}$ is an absolutely irreducible polynomial. Following [32], let $\widetilde{q} \in \overline{\mathbb{F}}_q[\Omega,T][Z_{n-r+1}]$ be the polynomial $\widetilde{q} := q^{(r)}\big(\Omega_1T + p_1,\dots,\Omega_{n-r}T + p_{n-r}, Z_{n-r+1}\big)$.

Since $q^{(r)}$ is a monic element of $\overline{\mathbb{F}}_q[Z_1,\dots,Z_{n-r}][Z_{n-r+1}]$, we easily conclude that $\widetilde{q}$ is a monic element of $\overline{\mathbb{F}}_q[\Omega,T][Z_{n-r+1}]$.

We claim that $\widetilde{q}(\Omega,0,Z_{n-r+1})$ is a separable element of $\overline{\mathbb{F}}_q[\Omega][Z_{n-r+1}]$. Indeed, we have that $\widetilde{q}(\Omega,0,Z_{n-r+1}) = q^{(r)}(P,Z_{n-r+1})$ holds. Then the proof of Proposition 3.1 shows that the choice of P implies that the discriminant of the polynomial $q^{(r)}(P,Z_{n-r+1})$ does not vanish. This means that $\widetilde{q}(\Omega,0,Z_{n-r+1})$ is a separable element of $\overline{\mathbb{F}}_q[\Omega][Z_{n-r+1}]$.

Therefore, applying [32, Theorem 5] we conclude that there exists a polynomial $C \in \overline{\mathbb{F}}_q[\Omega]$ of degree bounded by $\frac{3}{2}\delta_r^4 - 2\delta_r^3 + \frac{1}{2}\delta_r^2 \le 2\delta_r^4$ such that for any $\omega \in \mathbb{A}^{n-r}$ with $C(\omega) \neq 0$, the polynomial $\widetilde{q}(\omega,T,Z_{n-r+1})$ is absolutely irreducible. From this we immediately deduce the statement of the theorem. □

4. The computation of a geometric solution of V

Let notations and assumptions be as in Section 3. In this section we shall exhibit an algorithm which computes a geometric solution of a K-definable lifting fiber $V_{P^{(r)}}$ of the input variety V, where K is a suitable finite field extension of $\mathbb{F}_q$.

In order to describe this algorithm, we need a simultaneous Noether normalization of the varieties $V_1,\dots,V_r$ and lifting points $P^{(s+1)} \in \mathbb{A}^{n-s-1}$ for $0 \le s \le r-1$ such that the corresponding lifting fiber $V_{P^{(s+1)}}$ has the following property: for any point $P \in V_{P^{(s+1)}}$, the morphism π_s is unramified at $\pi_s(P)$. For this purpose, let $\Lambda := (\Lambda_{i,j})_{1\le i,j\le n}$ be a matrix of indeterminates and let $\Gamma := (\Gamma_1,\dots,\Gamma_n)$ be a vector of indeterminates. Let $X := (X_1,\dots,X_n)$ and let $\widetilde{Y} := \Lambda X + \Gamma$. Let $B_s \in \overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}]$ be the polynomial of the statement of Theorem 3.3 for $1 \le s \le r-1$ and let $B := \det(\Lambda)\prod_{s=1}^{r-1} B_s$. Observe that $\deg B \le 4n^4d\delta^4$ holds.

Let K be a finite field extension of $\mathbb{F}_q$ of cardinality greater than $60n^4d\delta^4$ and let (λ,γ,P) be a point randomly chosen in the set $\mathsf{K}^{n(n+1)} \times \mathsf{K}^{n-1}$. Theorem 2.2 shows that $B(\lambda,\gamma,P)$ does not vanish with probability at least $14/15$. From now on, we shall assume that we have chosen $(\lambda,\gamma,P) \in \mathsf{K}^{n(n+1)} \times \mathsf{K}^{n-1}$ satisfying $B(\lambda,\gamma,P) \neq 0$. Let $(Y_1,\dots,Y_n) := \lambda X + \gamma$ and $P := (p_1,\dots,p_{n-1})$.

From Theorem 3.3 we conclude that $Y_1,\dots,Y_n$ induce a simultaneous Noether normalization of the varieties $V_1,\dots,V_r$, and the point $P^{(s+1)} := (p_1,\dots,p_{n-s-1})$ satisfies the condition above for $0 \le s \le r-1$. We observe that the fact that the linear forms $Y_1,\dots,Y_n$ belong to $\mathsf{K}[X_1,\dots,X_n]$ and P belongs to K^{n-1}, immediately implies that the lifting fiber $V_{P^{(s)}}$ is a K-variety for $1 \le s \le r$.

The algorithm for computing a geometric solution of $V_{P^{(r)}}$ is a recursive procedure which proceeds in $r-1$ steps. In the sth step we compute a geometric solution of the lifting fiber $V_{P^{(s+1)}}$ from a geometric solution of the lifting fiber $V_{P^{(s)}}$. Recall that $V_{P^{(s)}} := \pi_s^{-1}(P^{(s)}) = V_s \cap \{Y_1 = p_1,\dots,Y_{n-s} = p_{n-s}\}$. For this purpose, we first "lift" the geometric solution of the fiber $V_{P^{(s)}}$ to a geometric solution of the affine equidimensional unidimensional K-variety

$$W_{P^{(s+1)}} := V_s \cap \{Y_1 = p_1,\dots,Y_{n-s-1} = p_{n-s-1}\}$$

(see Section 4.1 below). The variety $W_{P^{(s+1)}}$ is called a *lifting curve*. Then, from this geometric solution we obtain a geometric solution of the lifting fiber $V_{P^{(s+1)}} = W_{P^{(s+1)}} \cap V(F_{s+1})$. This is done by computing the minimal equation satisfied by Y_{n-s+1} in $V_{P^{(s+1)}}$ (see Section 4.2), from which we obtain a geometric solution of $V_{P^{(s+1)}}$ by an effective version of the Shape Lemma (see Section 4.3).

4.1. **From the lifting fiber $V_{P^{(s)}}$ to the lifting curve $W_{P^{(s+1)}}$.** In this section we describe the procedure which computes a geometric solution of the lifting curve $W_{P^{(s+1)}}$ from a geometric solution of the lifting fiber $V_{P^{(s)}}$.

Let $\pi_s : V_s \to \mathbb{A}^{n-s}$ and $\widetilde{\pi}_s : V_s \to \mathbb{A}^{n-s+1}$ be the linear projection mappings defined by the linear forms $Y_1, \dots, Y_{n-s}$ and $Y_1, \dots, Y_{n-s+1}$, respectively. From Theorem 3.3 we know that π_s is a finite morphism and that Y_{n-s+1} is a primitive element of the integral ring extension $\overline{\mathbb{F}}_q[Y_1, \dots, Y_{n-s}] \hookrightarrow \overline{\mathbb{F}}_q[V_s]$. Furthermore, the minimal polynomial $q^{(s)} \in \overline{\mathbb{F}}_q[Y_1, \dots, Y_{n-s+1}]$ of the coordinate function of $\overline{\mathbb{F}}_q[V_s]$ defined by Y_{n-s+1} has degree δ_s and is a defining polynomial of the hypersurface $\widetilde{\pi}_s(V_s)$. Since $\widetilde{\pi}_s(V_s)$ is a K-hypersurface, we may assume without loss of generality that $q^{(s)}$ belongs to $\mathsf{K}[Y_1, \dots, Y_{n-s+1}]$. This assumption, together with the proof of Lemma 3.5, shows that there exists a geometric solution of V_s consisting of polynomials $q^{(s)}, v_{n-s+2}^{(s)}, \dots, v_n^{(s)}$ of $\mathsf{K}[Y_1, \dots, Y_{n-s+1}]$.

Our choice of $P^{(s)}$ implies that the discriminant of $q^{(s)}$ with respect to Y_{n-s+1} does not vanish in $P^{(s)}$. Therefore, the above geometric solution of V_s is compatible with $P^{(s)}$ in the sense of Section 2.2, and $q^{(s)}(P^{(s)}, Y_{n-s+1}), v_{n-s+k}^{(s)}(P^{(s)}, Y_{n-s+1})$ $(2 \le k \le s)$ form a geometric solution of $V_{P^{(s)}}$ with Y_{n-s+1} as primitive element. We shall assume that we are given such a geometric solution of $V_{P^{(s)}}$.

We observe that $W_{P^{(s+1)}}$ can be described as the set of common zeros of the polynomials $Y_1 - p_1, \dots, Y_{n-s-1} - p_{n-s-1}, F_1, \dots, F_s$ or, equivalently, of the polynomials $Y_1 - p_1, \dots, Y_{n-s-1} - p_{n-s-1}, F_1(P^{(s+1)}, Y_{n-s}, \dots, Y_n), \dots, F_s(P^{(s+1)}, Y_{n-s}, \dots, Y_n)$. In particular we see that $W_{P^{(s+1)}}$ is a K-variety. In order to find a geometric solution of $W_{P^{(s+1)}}$ we are going to apply the global Newton–Hensel procedure of [25]. For this purpose, we need the following result.

Lemma 4.1. *The polynomials $F_1(P^{(s+1)}, Y_{n-s}, \dots, Y_n), \dots, F_s(P^{(s+1)}, Y_{n-s}, \dots, Y_n)$ generate a radical ideal and form a regular sequence of $\mathsf{K}[Y_{n-s}, \dots, Y_n]$. Further, $W_{P^{(s+1)}}$ has degree δ_s.*

Proof. We first show that $F_j(P^{(s+1)}, Y_{n-s}, \dots, Y_n)$ $(1 \le j \le s)$ form a regular sequence. Let $L_{s+1} \subset \mathbb{A}^n$ be the affine linear variety $L_{s+1} := \{Y_1 = p_1, \dots, Y_{n-s-1} = p_{n-s-1}\}$. Observe that $\{F_j(P^{(s+1)}, Y_{n-s}, \dots, Y_n) = 0; 1 \le j \le s\} = V_i \cap L_{s+1} = \pi_i^{-1}(L_{s+1})$ for $1 \le i \le s$. Since π_i is a finite morphism, we conclude that $\dim V_i \cap L_{s+1} = \dim_{\mathbb{A}^{n-i}} L_{s+1} = n - i - (n - s - 1) = s + 1 - i$ for $1 \le i \le s$. This proves our first assertion.

Now we prove that $\deg W_{P^{(s+1)}} = \delta_s$ holds. Our previous argumentation shows that $W_{P^{(s+1)}} = V_s \cap L_{s+1}$ is an equidimensional variety of dimension 1. By the Bézout inequality (2.1), we have $\deg W_{P^{(s+1)}} \le \delta_s$. On the other hand, since π_s is a finite morphism, the restriction mapping $\pi_s|_{W_{P^{(s+1)}}} : W_{P^{(s+1)}} \to L_{s+1} \subset \mathbb{A}^{n-s}$ is also a finite morphism. Furthermore, our choice of $P^{(s)}$ implies that $\#(\pi_s|_{W_{P^{(s+1)}}})^{-1}(P^{(s)}) = \#\,\pi_s^{-1}(P^{(s)}) = \delta_s$ holds. Then

$$\delta_s = \#\pi_s^{-1}(P^{(s)}) = \#(W_{P^{(s+1)}} \cap \{Y_{n-s} = p_{n-s}\}) \le \deg W_{P^{(s+1)}} \le \delta_s,$$

which proves our second assertion.

There remains to prove that $F_j(P^{(s+1)}, Y_{n-s}, \dots, Y_n)$ $(1 \le j \le s)$ generate a radical ideal of $\mathsf{K}[Y_{n-s}, \dots, Y_n]$. Since $P^{(s)}$ is a lifting point of π_s, from Lemma 2.1 we conclude that the Jacobian determinant

$$J_F(P^{(s+1)}, Y_{n-s}, \dots, Y_n) := \det \big(\partial F_i(P^{(s+1)}, Y_{n-s}, \dots, Y_n)/\partial Y_{n-s+j}\big)_{1 \le i,j \le s}$$

does not vanish at any point of $W_{P^{(s+1)}} \cap \{Y_{n-s} = p_{n-s}\}$. Furthermore, the equality $\#(W_{P^{(s+1)}} \cap \{Y_{n-s} = P_{n-s}\}) = \delta_s = \deg W_{P^{(s+1)}}$ shows that the affine linear variety $\{Y_{n-s} = p_{n-s}\}$ meets every irreducible component of $W_{P^{(s+1)}}$. This proves that the coordinate function of $W_{P^{(s+1)}}$ defined by $J_F(P^{(s+1)}, Y_{n-s}, \dots, Y_n)$ is not a zero divisor of $\overline{\mathbb{F}}_q[W_{P^{(s+1)}}]$. Hence, from [16, Theorem 18.15] we conclude that the ideal generated by $F_j(P^{(s+1)}, Y_{n-s}, \dots, Y_n)$ $(1 \le j \le s)$ is radical. $\square$

Now we can describe the algorithm for computing the geometric solution of the lifting curve $W_{P^{(s+1)}}$. In order to state the complexity of our algorithms, we shall use the quantity $\mathcal{U}(m) := m \log^2 m \log\log m$. We remark that the bit-complexity of certain basic operations (such as addition, multiplication, division, and gcd) with integers of bit-size m is $O\big(\mathcal{U}(m)\big)$, and the number of arithmetic operations in a given domain R necessary to compute the multiplication, division, resultant, gcd, and interpolation of univariate polynomials of $R[T]$ of degree at most m is also of order $O\big(\mathcal{U}(m)\big)$ (cf. [57], [6]). In particular, an arithmetic operation in a finite field K of cardinality $\#\mathsf{K}$ can be (deterministically) performed with $O(\mathcal{U}(\log \#\mathsf{K}))$ bit operations, using space $O(\log \#\mathsf{K})$. Our assumptions on K imply $\log \#\mathsf{K} \le O(\log(q\delta))$.

Proposition 4.2. *There exists a deterministic Turing machine M which has as input*

- *a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the polynomials $F_1, \dots, F_s$,*
- *the dense representation of elements of $\mathsf{K}[Y_{n-s+1}]$ which form a geometric solution of $V_{P^{(s)}}$,*

and outputs the dense representation of polynomials of $\mathsf{K}[Y_{n-s}, Y_{n-s+1}]$ which form a geometric solution of $W_{P^{(s+1)}}$. The Turing machine M runs in space $O\big((\mathcal{S}+n)\delta_s^2 \log(q\delta)\big)$ and time $O\big((n\mathcal{T}+n^5)\mathcal{U}(\delta_s)^2\mathcal{U}(\log(q\delta))\big)$.

Proof. Since every point $P \in W_{P^{(s+1)}}$ has fixed its first $n-s-1$ coordinates, the lifting curve $W_{P^{(s+1)}}$ is naturally isomorphic to the affine space curve $W^*_{P^{(s+1)}} \subset \mathbb{A}^{s+1}$ obtained by projecting $W_{P^{(s+1)}}$ on the $(s+1)$-dimensional affine linear space with coordinates $Y_{n-s}, \dots, Y_n$. This projection identifies the lifting fiber $V_{P^{(s+1)}}$ with the zero-dimensional affine variety $V^*_{P^{(s+1)}} := W^*_{P^{(s+1)}} \cap \{Y_{n-s} = p_{n-s}\}$. Furthermore, the projection $\widehat{\pi}_{s+1} : W^*_{P^{(s+1)}} \to \mathbb{A}^1$ induced by Y_{n-s} is a finite generically unramified morphism of degree δ_s, in other words, a generic fiber of $\widehat{\pi}_s$ has cardinality δ_s. In particular, the fiber $\widehat{\pi}_{s+1}^{-1}(p_{n-s}) = V^*_{P^{(s)}}$ is unramified of cardinality δ_s.

The polynomials $q^{(s)}(P^{(s)}, Y_{n-s+1}), v^{(s)}_{n-s+k}(P^{(s)}, Y_{n-s+1})$ $(2 \le k \le s)$, introduced before the statement of Lemma 4.1, form a geometric solution of $V^*_{P^{(s)}}$. Under these conditions, applying the Global Newton algorithm of [25, II.4] we conclude that there exists a computation tree β in K which computes a geometric solution of $W^*_{P^{(s+1)}}$, which is also a geometric solution of $W_{P^{(s+1)}}$. The fact that the input geometric solution of $V^*_{P^{(s)}}$ consists of univariate polynomials with coefficients in K

implies that the output geometric solution of $W_{P^{(s+1)}}$ also consists of polynomials with coefficients in K.

The evaluation of the computation tree β requires $O\big((n\mathcal{T}+n^5)\mathcal{U}(\delta_s)^2\big)$ arithmetic operations in K, using at most $O\big((\mathcal{S}+n)\delta_s^2\big)$ arithmetic registers. Taking into account the cost of the basic arithmetic operations in K we deduce the complexity estimate of the statement of the proposition. $\square$

4.2. **Computing a hypersurface birational to $V_{P^{(s+1)}}$.** The purpose of this section is to exhibit an algorithm which computes the minimal equation satisfied by the coordinate function induced by a linear form $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$ in $\overline{\mathbb{F}}_q[V_{P^{(s+1)}}]$, for a suitable choice of $\lambda \in \mathsf{K}$.

In order to simplify notations, during this section we shall denote the lifting point $P^{(s+1)}$ by P, the lifting fiber $V_{P^{(s+1)}}$ by V_P, and the lifting curve $W_{P^{(s+1)}}$ by W_P.

For any $\lambda \in \mathsf{K}$, let $\mathcal{L}_\lambda \in \mathsf{K}[Y_{n-s}, Y_{n-s+1}]$ denote the linear form $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$, and let $\widehat{\pi}_{s+1,\lambda} : W_P \to \mathbb{A}^1$ be the projection morphism defined by $\widehat{\pi}_{s+1,\lambda}(x) := \mathcal{L}_\lambda(x)$. Our next result yields a sufficient (and consistent) condition on λ, which assures that replacing the variable Y_{n-s} by $\mathcal{L}_\lambda$ does not change the situation obtained after the preprocessing of Section 3.2, namely $\widehat{\pi}_{s+1,\lambda}$ is a finite morphism, and any element of the set $\widehat{\pi}_{s+1,\lambda}(V_P)$ defines an unramified fiber of $\widehat{\pi}_{s+1,\lambda}$.

Lemma 4.3. *Let Λ be an indeterminate. There exists a nonzero polynomial $E_s \in \overline{\mathbb{F}}_q[\Lambda]$ of degree at most $4\delta^3$, with the following property: for any $\lambda \in \mathbb{A}^1$ with $E_s(\lambda) \neq 0$, if $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$, then*

(i) *the projection mapping $\widehat{\pi}_{s+1,\lambda} : W_{P^{(s+1)}} \to \mathbb{A}^1$ defined by $\mathcal{L}_\lambda$ is a finite morphism,*
(ii) *$\mathcal{L}_\lambda$ separates the points of the lifting fiber $V_{P^{(s+1)}}$,*
(iii) *every element of $\widehat{\pi}_{s+1,\lambda}(V_{P^{(s+1)}})$ is a lifting point of $\widehat{\pi}_{s+1,\lambda}$.*

Proof. By the choice of the linear forms $Y_1, \ldots, Y_{n-s+1}$ and the point P, we have that the coordinate function defined by Y_{n-s+1} represents a primitive element of the integral ring extension $\overline{\mathbb{F}}_q[Y_{n-s}] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$, whose minimal polynomial is $q^{(s)}(P, Y_{n-s}, Y_{n-s+1})$. Furthermore, $\overline{\mathbb{F}}_q[W_P]$ is a free $\overline{\mathbb{F}}_q[Y_{n-s}]$-module of rank δ_s.

First we determine a genericity condition for (i). Let $\mathcal{L}_\Lambda := Y_{n-s} + \Lambda Y_{n-s+1}$, and let $q_\Lambda^{(s)}$ be the following element of $\mathsf{K}[\Lambda, Y_1, \ldots, Y_{n-s-1}, \mathcal{L}_\Lambda, Y_{n-s+1}]$:

$$q_\Lambda^{(s)} := q^{(s)}(Y_1, \ldots, Y_{n-s-1}, \mathcal{L}_\Lambda - \Lambda Y_{n-s+1}, Y_{n-s+1}).$$

Since $q^{(s)}$ has (total) degree δ_s and $\mathcal{L}_\Lambda - \Lambda Y_{n-s+1}$ is linear in $\mathcal{L}_\Lambda, Y_{n-s+1}$, and also in $\mathcal{L}_\lambda, \Lambda$, we conclude that $\deg_{\mathcal{L}_\Lambda, Y_{n-s+1}} q_\Lambda^{(s)} \leq \delta_s$ and $\deg_{\mathcal{L}_\Lambda, \Lambda} q_\Lambda^{(s)} \leq \delta_s$ hold. Therefore, we may express $q_\Lambda^{(s)}(P, \Lambda, \mathcal{L}_\Lambda, Y_{n-s+1})$ in the following way:

$$q_\Lambda^{(s)}(P, \Lambda, \mathcal{L}_\Lambda, Y_{n-s+1}) = a_{\delta_s}(\Lambda) Y_{n-s+1}^{\delta_s} + a_{\delta_s-1}(\Lambda, \mathcal{L}_\Lambda) Y_{n-s+1}^{\delta_s-1} + \cdots + a_0(\Lambda, \mathcal{L}_\Lambda),$$

where $a_{\delta_s}, \ldots, a_0 \in \mathsf{K}[\Lambda, \mathcal{L}_\Lambda]$ have degree at most δ_s. Since $q_\Lambda^{(s)}(P, 0, Y_{n-s}, Y_{n-s+1}) = q^{(s)}(P, Y_{n-s}, Y_{n-s+1})$ holds and the polynomial $q^{(s)}(P, Y_{n-s}, Y_{n-s+1})$ is a monic element of $\mathsf{K}[Y_{n-s}][Y_{n-s+1}]$ of degree δ_s in Y_{n-s+1}, we conclude that the leading coefficient a_{δ_s} is a nonzero element of $\mathsf{K}[\Lambda]$ (of degree at most δ_s). We shall prove below that for any λ with $a_{\delta_s}(\lambda) \neq 0$ condition (i) holds.

Now we consider condition (ii). Let $V_P := \{Q_1, \dots, Q_{\delta_{s+1}}\}$, and consider the following polynomial:

$$E_{s,1}(\Lambda) = \prod_{1 \le j < k \le \delta_{s+1}} \big(\mathcal{L}_\Lambda(Q_j) - \mathcal{L}_\Lambda(Q_k)\big).$$

Observe that $\mathcal{L}_\Lambda(Q_j) - \mathcal{L}_\Lambda(Q_k) = Y_{n-s}(Q_j) - Y_{n-s}(Q_k) + \Lambda\big(Y_{n-s+1}(Q_j) - Y_{n-s+1}(Q_k)\big)$ holds for $1 \le j < k \le \delta_{s+1}$. Therefore, since Y_{n-s} separates the points of the lifting fiber V_P, we conclude that $E_{s,1}$ is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda]$ of degree at most δ_{s+1}^2. We shall show below that for any λ with $E_{s,1}(\lambda) \neq 0$ condition (ii) holds.

Finally, we consider condition (iii). Let $\widehat{\pi}_{s+1,\Lambda} : \mathbb{A}^1 \times V_P \to \mathbb{A}^2$ be the mapping defined by $\widehat{\pi}_{s+1,\Lambda}(\lambda, x) := \big(\lambda, \mathcal{L}_\lambda(x)\big)$. Observe that the image of $\widehat{\pi}_{s+1,\Lambda}$ is a K-hypersurface of $\mathbb{A}^2$ of degree δ_{s+1}, defined by the polynomial $q_{\mathcal{L}_\Lambda}^{(s+1)}(\Lambda, \mathcal{L}_\Lambda) := \prod_{1 \le j \le \delta_{s+1}} (\mathcal{L}_\Lambda - \mathcal{L}_\Lambda(Q_j)) \in \mathsf{K}[\Lambda, \mathcal{L}_\Lambda]$. We claim that $q_{\mathcal{L}_\Lambda}^{(s+1)}$ and the discriminant $\rho_\Lambda^{(s)}(P, \Lambda, \mathcal{L}_\Lambda) \in \mathsf{K}[\Lambda, \mathcal{L}_\Lambda]$ of the polynomial $q_\Lambda^{(s)}(P, \Lambda, \mathcal{L}_\Lambda, Y_{n-s+1})$ introduced above have no nontrivial common factors in $\mathsf{K}(\Lambda)[\mathcal{L}_\Lambda]$. Arguing by contradiction, suppose that there exists a nontrivial common factor $\widetilde{h} \in \mathsf{K}(\Lambda)[\mathcal{L}_\Lambda]$. Since $q_{\mathcal{L}_\Lambda}^{(s+1)}$ is a monic element of $\mathsf{K}[\Lambda][\mathcal{L}_\Lambda]$, we deduce that there exists a common factor $h \in \mathsf{K}[\Lambda, \mathcal{L}_\Lambda] \setminus \mathsf{K}[\Lambda]$ not divisible by Λ. Taking into account that $q_{\mathcal{L}_\Lambda}^{(s+1)}(0, Y_{n-s}) = q^{(s+1)}(P, Y_{n-s})$ and $\rho_\Lambda^{(s)}(P, 0, Y_{n-s})$ equals the discriminant $\rho^{(s)}(P, Y_{n-s})$ of $q^{(s)}(P, Y_{n-s}, Y_{n-s+1})$ with respect to Y_{n-s+1}, we see that $h(0, Y_{n-s})$ is a nontrivial common factor of $\rho^{(s)}(P, Y_{n-s})$ and $q^{(s+1)}(P, Y_{n-s})$. Let $\alpha \in \overline{\mathbb{F}}_q$ be a root of $h(0, Y_{n-s})$ and let Q be a point of V_P for which $\alpha = Y_{n-s}(Q)$ holds. Then $(p_1, \dots, p_{n-s-1}, \alpha) = \pi_s(Q)$, and $q^{(s)}(\pi_s(Q), Y_{n-s+1})$ has less than δ_s roots. We conclude that either $\pi_s(Q)$ is not a lifting point of π_s or Y_{n-s+1} is not a primitive element of $\pi_s^{-1}(\pi_s(Q))$, thus contradicting condition (iii) of Theorem 3.3. This proves our claim.

From our claim we see that the resultant $E_{s,2} \in \mathsf{K}[\Lambda]$ of $q_{\mathcal{L}_\Lambda}^{(s+1)}(\Lambda, \mathcal{L}_\Lambda)$ and $\rho_\Lambda^{(s)}(P, \Lambda, \mathcal{L}_\Lambda)$ with respect to the variable $\mathcal{L}_\Lambda$ is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda]$ of degree at most $2(2\delta_s - 1)\delta_s\delta_{s+1}$. The nonvanishing of $E_{s,2}$ is the genericity condition we are looking for, as will be shown below.

Let $E_s := a_{\delta_s} E_{s,1} E_{s,2} \in \overline{\mathbb{F}}_q[\Lambda]$. Observe that $\deg E_s \le 4\delta^3$ holds. Let $\lambda \in \mathbb{A}^1$ satisfy $E_s(\lambda) \neq 0$ and let $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$. We claim that conditions (i), (ii) and (iii) of the statement of Lemma 4.3 hold.

Let ℓ_λ, y_{n-s} and y_{n-s+1} denote the coordinate functions of $\overline{\mathbb{F}}_q[W_P]$ induced by $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$, Y_{n-s} and Y_{n-s+1}, respectively. We have $\ell_\lambda = y_{n-s} + \lambda y_{n-s+1}$. From $q^{(s)}(P, y_{n-s}, y_{n-s+1}) = 0$ we deduce that $q_\Lambda^{(s)}(\lambda, P, \ell_\lambda, y_{n-s+1}) = 0$ holds. Let $q_\lambda^{(s)} := q_\Lambda^{(s)}(\lambda, Y_1, \dots, Y_{n-s-1}, \mathcal{L}_\lambda, Y_{n-s+1})$. Since $a_{\delta_s}(\lambda) \neq 0$ holds, we see that $q_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ is a monic (up to a nonzero element of $\overline{\mathbb{F}}_q$) element of $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda][Y_{n-s+1}]$, which represents an integral dependence equation over $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda]$ for the coordinate function y_{n-s+1}. Assuming without loss of generality that $\lambda \neq 0$ holds, we see that $\widehat{\pi}_{s+1,\lambda} : W_P \to \mathbb{A}^1$ is a dominant mapping, because otherwise $\widehat{\pi}_{s+1} : W_P \to \mathbb{A}^1$ would not be dominant. We conclude that $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda] \hookrightarrow \overline{\mathbb{F}}_q[\ell_\lambda, y_{n-s+1}]$ is an integral ring extension. Combining this with the fact that $\overline{\mathbb{F}}_q[\ell_\lambda, y_{n-s+1}] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$ is an integral ring extension, we see that $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$ is an integral extension. This proves that $\widehat{\pi}_{s+1,\lambda}$ is a finite morphism and shows that condition (i) holds.

Next, taking into account that $E_{s,1}(\lambda) = \prod_{1\le i<j\le \delta_{s+1}} \big(\mathcal{L}_\lambda(Q_i) - \mathcal{L}_\lambda(Q_j)\big) \neq 0$ holds, we conclude that $\mathcal{L}_\lambda$ separates the points of the fiber V_P. This shows that condition (ii) holds.

Finally, let Q be an arbitrary point of V_P. Since $E_{s,2}(\lambda) \neq 0$ holds, the discriminant $\rho_\lambda^{(s)}(P, \mathcal{L}_\lambda)$ of the polynomial $q_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ with respect to Y_{n-s+1} does not vanish in $\mathcal{L}_\lambda(Q)$. Then $q_\lambda^{(s)}(P, \mathcal{L}_\lambda(Q), Y_{n-s+1})$ has δ_s distinct roots in $\overline{\mathbb{F}}_q$. Therefore, the fiber $\widehat{\pi}_{s+1,\lambda}^{-1}(\mathcal{L}_\lambda(Q))$ has δ_s distinct points, in other words, it is unramified. This shows that condition (iii) holds and finishes the proof of the lemma. □

Since the cardinality of the field K is greater than $60n^4d\delta^4$, from Theorem 2.2 we see that, for a randomly chosen value $\lambda \in \mathsf{K}$, the condition $E_s(\lambda) \neq 0$ holds with probability at least $1 - 1/60n^4$. Assume that we are given such a value $\lambda \in \mathsf{K}$ and let $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$. We are going to exhibit an algorithm that computes the minimal equation of the coordinate function of V_P induced by $\mathcal{L}_\lambda$.

Let $(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})^{-1}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ be the monic element of $\mathsf{K}(\mathcal{L}_\lambda)[Y_{n-s+1}]$ of degree at most $\delta_s - 1$ that is the inverse of $(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})(P, \mathcal{L}_\lambda, Y_{n-s+1})$ modulo $q_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$, and let $w_{n-s+k}^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1}) \in \mathsf{K}(\mathcal{L}_\lambda)[Y_{n-s+1}]$ be the remainder of the product $v_{n-s+k}^{(s)}(P, \mathcal{L}_\lambda - \lambda Y_{n-s+1}, Y_{n-s+1})(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})^{-1}$ $(P, \mathcal{L}_\lambda, Y_{n-s+1})$ modulo $q_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ for $2 \le k \le s$. Finally, let

$$f_{s+1} := F_{s+1}\big(P, \mathcal{L}_\lambda, Y_{n-s+1}, w_{n-s+2}^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1}), \ldots, w_n^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})\big),$$

$$g_{s+1} := \mathrm{Res}_{Y_{n-s+1}}\big(q_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1}), f_{s+1}\big), \tag{4.1}$$

where $\mathrm{Res}_{Y_{n-s+1}}(f, g)$ denotes the resultant of f and g with respect to Y_{n-s+1}.

We observe that $f_{s+1} \in \mathsf{K}(\mathcal{L}_\lambda)[Y_{n-s+1}]$ has degree at most $d\delta_s$ in Y_{n-s+1}, and that the denominators of its coefficients are divisors of a polynomial of $\mathsf{K}[\mathcal{L}_\lambda]$ of degree bounded by $(2\delta_s - 1)\delta_s$. On the other hand, from [25, Corollary 2] it follows that g_{s+1} is an element of $\mathsf{K}[\mathcal{L}_\lambda]$ of degree bounded by $d\delta_s$. Our next result shows that the minimal equation of $\mathcal{L}_\lambda$ in $\mathsf{K}[V_P]$ can be efficiently computed.

Proposition 4.4. *There exists a probabilistic Turing machine M which has as input*

- *a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the polynomial F_{s+1},*
- *the dense representation of elements of $\mathsf{K}[Y_{n-s}, Y_{n-s+1}]$ which form a geometric solution of $W_{P^{(s+1)}}$, as computed in Proposition 4.2,*
- *a value $\lambda \in \mathsf{K}$ satisfying the conditions of Lemma 4.3,*

and outputs the dense representation of the minimal polynomial $q_{\mathcal{L}_\lambda}^{(s+1)}(P^{(s+1)}, \mathcal{L}_\lambda)$ $\in \mathsf{K}[\mathcal{L}_\lambda]$ of the coordinate function of $V_{P^{(s+1)}}$ induced by $\mathcal{L}_\lambda$. The Turing machine M runs in space $O\big((\mathcal{S} + d)\delta_s^2 \log(q\delta)\big)$ and time $O\big((\mathcal{T} + n)\mathcal{U}(d\delta_s)\mathcal{U}(\delta_s)\mathcal{U}(\log(q\delta))\big)$ and outputs the right result with probability at least $1 - 1/45n^3$.

Proof. Let $\lambda \in \mathsf{K}$ satisfy the conditions of Lemma 4.3. Then [29, Lemma 8] shows that the following identity holds:

$$q_{\mathcal{L}_\lambda}^{(s+1)}(P, \mathcal{L}_\lambda) = \frac{g_{s+1}}{\gcd(g_{s+1}, g'_{s+1})}\,.$$

Therefore, the computation of $q_{\mathcal{L}_\lambda}^{(s+1)}(P,\mathcal{L}_\lambda)$ can be efficiently reduced to that of the polynomial g_{s+1} of (4.1). The latter may be defined as the resultant with respect to the variable Y_{n-s+1} of two elements of $\mathsf{K}(\mathcal{L}_\lambda)[Y_{n-s+1}]$ of degrees bounded by δ_s and δ_s-1, namely $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ and the remainder of f_{s+1} modulo $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$. Following [57, Corollary 11.16], such a resultant can be computed using the Extended Euclidean Algorithm (EEA for short) in $\mathsf{K}(\mathcal{L}_\lambda)[Y_{n-s+1}]$, which requires $O\big(\mathcal{U}(\delta_s)\big)$ arithmetic operations in $\mathsf{K}(\mathcal{L}_\lambda)$ storing at most $O(\delta_s)$ elements of $\mathsf{K}(\mathcal{L}_\lambda)$. Furthermore, the computation of f_{s+1} requires the (modular) inversion of $(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})^{-1}(P,\mathcal{L}_\lambda,Y_{n-s+1})$, which can also be computed by applying the EEA in $\mathsf{K}(\mathcal{L}_\lambda)[Y_{n-s+1}]$ to the polynomials $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ and $(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})(P,\mathcal{L}_\lambda,Y_{n-s+1})$.

In order to compute the dense representation of the polynomial g_{s+1}, we shall perform the EEA over a ring of power series $\mathsf{K}[\![\mathcal{L}_\lambda-\alpha]\!]$ for some "lucky" point $\alpha\in\mathsf{K}$. Therefore, we have to determine a value $\alpha\in\mathsf{K}$ such that all the elements of $\mathsf{K}[\mathcal{L}_\lambda]$ which are inverted during the execution of the EEA are invertible elements of the ring $\mathsf{K}[\![\mathcal{L}_\lambda-\alpha]\!]$. Further, in order to make our algorithm "effective", during its execution we shall compute suitable approximations in $\mathsf{K}[\mathcal{L}_\lambda]$ of the intermediate results of our computations, which are obtained by truncating the power series of $\mathsf{K}[\![\mathcal{L}_\lambda-\alpha]\!]$ that constitute these intermediate results. Therefore, we have to determine the degree of precision of the truncated power series required to output the right results.

In order to determine the value $\alpha\in\mathsf{K}$, we observe that, similar to the proof of [57, Theorem 6.52], one deduces that all the denominators of the elements of $\mathsf{K}(\mathcal{L}_\lambda)$ arising during the application of the EEA to $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ and f_{s+1} are divisors of at most δ_s+1 polynomials of $\mathsf{K}[\mathcal{L}_\lambda]$ of degree bounded by $(d\delta_s+\delta_s)(2\delta_s-1)\delta_s$. On the other hand, the denominators arising during the application of the EEA to $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ and $(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})(P,\mathcal{L}_\lambda,Y_{n-s+1})$ are divisors of at most δ_s+1 polynomials of $\mathsf{K}[Y_{n-s}]$ of degree at most $(2\delta_s-1)\delta_s$. Hence the product of all the denominators arising during the two applications of the EEA has degree at most $(d\delta_s+\delta_s+1)(2\delta_s-1)\delta_s(\delta_s+1)\le 4d\delta_s^4$. Since $\#\mathsf{K}>60n^4d\delta^4$ holds, from Theorem 2.2 we conclude that there exists $\alpha\in K$ that does not annihilate any denominator arising as an intermediate results of the EEA. Furthermore, the probability of finding such an α by a random choice in K is at least $1-1/45n^3$.

On the other hand, since the output of our algorithm is a polynomial of degree at most $d\delta_s$, computing all the power series which arise as intermediate results up to order $d\delta_s+1$ allows us to output the right result.

Our algorithm computing g_{s+1} inverts $(\partial q_\lambda^{(s)}/\partial Y_{n-s+1})(P,\mathcal{L}_\lambda,Y_{n-s+1})$ modulo $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$, computes $w_{n-s+k}^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ for $2\le k\le s$, then computes f_{s+1} modulo $q_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$, and finally computes g_{s+1}. All these steps require $O\big((\mathcal{T}+n)\mathcal{U}(\delta_s)\big)$ arithmetic operations in $\mathsf{K}(\mathcal{L}_\lambda)$, storing at most $O(\mathcal{S}\delta_s)$ elements of $\mathsf{K}(\mathcal{L}_\lambda)$. Each of these arithmetic operations is performed in the power series ring $\mathsf{K}[\![\mathcal{L}_\lambda-\alpha]\!]$ at precision $d\delta_s+1$, and then requires $O\big(\mathcal{U}(d\delta_s)\big)$ arithmetic operations in K, storing at most $O(d\delta_s)$ elements of K. Therefore, we conclude that the whole algorithm computing g_{s+1} requires $O\big((\mathcal{T}+n)\mathcal{U}(d\delta_s)\mathcal{U}(\delta_s)\big)$ arithmetic operations in K, storing at most $O\big((\mathcal{S}+d)\delta_s^2\big)$ elements of K.

Finally, the computation of $g_{s+1}/\gcd(g_{s+1}, g'_{s+1})$ requires $O\big(\mathcal{U}(d\delta_s)\big)$ operations in K, storing at most $O(d\delta_s)$ elements of K. This finishes the proof of the proposition. $\square$

The algorithm underlying Proposition 4.4 is essentially an extension to the finite field context of [25, Algorithm II.7]. We have contributed further to the latter by quantifying the probability of success of our algorithm. We also remark that the complexity estimate of Proposition 4.4 significantly improves that of [29, Proposition 1].

4.3. **Computing a geometric solution of $V_{P^{(s+1)}}$.** In this section we exhibit an algorithm which computes a parametrization of the variables $Y_{n-s+1}, \dots, Y_n$ by the zeros of $q^{(s+1)}(P^{(s+1)}, Y_{n-s})$, thus completing the sth recursive step of our main procedure for computing a geometric solution of the input variety V.

In order to simplify notations, in this section we shall denote, as in the previous section, the lifting point $P^{(s+1)}$ by P, the lifting fiber $V_{P^{(s+1)}}$ by V_P, and the lifting curve $W_{P^{(s+1)}}$ by W_P.

First we discuss how we obtain the parametrization of Y_{n-s+1} by the zeros of $q^{(s+1)}(P, Y_{n-s})$. Recall that such a parametrization is represented by a polynomial $(\partial q^{(s+1)}/\partial Y_{n-s})(P, Y_{n-s})Y_{n-s+1} - v^{(s+1)}_{n-s+1}(P, Y_{n-s}) \in \mathsf{K}[Y_{n-s}, Y_{n-s+1}]$, with $v^{(s+1)}_{n-s+1}(P, Y_{n-s})$ of degree at most $\delta_{s+1} - 1$.

Let $\lambda_1, \lambda_2 \in \mathsf{K} \setminus \{0\}$ satisfy the conditions of Lemma 4.3 and let $\mathcal{L}_i := Y_{n-s} + \lambda_i Y_{n-s+1}$ for $i = 1, 2$. Observe that the value $\lambda = 0$ also satisfies the conditions of Lemma 4.3. By Proposition 4.4 we may assume that we have already computed the minimal equations $q_1^{(s+1)}(P, \mathcal{L}_1)$, $q_2^{(s+1)}(P, \mathcal{L}_2)$, and $q^{(s+1)}(P, Y_{n-s})$ satisfied by $\mathcal{L}_1$, $\mathcal{L}_2$, and Y_{n-s} in $\overline{\mathbb{F}}_q[V_P]$. Interpreting these polynomials as elements of $\mathsf{K}[Y_{n-s}, Y_{n-s+1}]$, assume further that $\mathcal{L}_2$ separates the common zeros of $q^{(s+1)}(P, Y_{n-s})$ and $q_1^{(s+1)}(P, \mathcal{L}_1)$. Arguing as in the proof of Lemma 4.3, we easily conclude that there exists a nonzero polynomial $\widehat{E}_s \in \overline{\mathbb{F}}_q[\Lambda]$ of degree at most δ^4 such that, for any λ_2 with $\widehat{E}_s(\lambda_2) \neq 0$, the linear form $\mathcal{L}_2$ satisfies our last assumption.

In our subsequent argumentations we shall consider the following (zero-dimensional) K-variety:

$$W_{s+1} := \big\{(x_1, x_2) \in \mathbb{A}^2 : q^{(s+1)}(P, x_1) = 0, q_i^{(s+1)}(P, x_1 + \lambda_i x_2) = 0 \text{ for } i = 1, 2\big\}.$$

Let $\widetilde{\pi}_s : V_P \to \mathbb{A}^2$ be the projection mapping induced by Y_{n-s}, Y_{n-s+1}. Observe that $\widetilde{\pi}_s(V_P) \subset W_{s+1}$ holds. Furthermore, since $\mathcal{L}_2$ separates the common zeros of $q^{(s+1)}(P, Y_{n-s})$ and $q_1^{(s+1)}(P, \mathcal{L}_1)$, and $q_2^{(s+1)}(P, \mathcal{L}_2)$ vanishes in the set $\mathcal{L}_2\big(\widetilde{\pi}_s(V_P)\big)$ (of cardinality δ_{s+1}) and has degree δ_{s+1}, we conclude that $W_{s+1} = \widetilde{\pi}_s(V_P)$ holds.

Our intention is to reduce the computation of $v^{(s+1)}_{n-s+1}(P, Y_{n-s})$ to gcd computations over suitable field extensions of K. From our previous argumentation and the fact that Y_{n-s} separates the points of V_P, it follows that Y_{n-s} also separates the points of W_{s+1}. Then, applying the classical Shape Lemma to this (zero-dimensional) K-variety (see, e.g., [14]), we see that there exists a polynomial $w_{n-s+1} \in \mathsf{K}[Y_{n-s}]$ of degree at most $\delta_{s+1} - 1$ such that $Y_{n-s+1} - w_{n-s+1}(Y_{n-s})$ vanishes on the variety W_{s+1}.

Let $\alpha \in \overline{\mathbb{F}}_q$ be an arbitrary root of $q^{(s+1)}(P, Y_{n-s})$ and let $\beta := w_{n-s+1}(\alpha)$. Then the fact that Y_{n-s} separates the points of W_{s+1} shows that (α, β) is the only point of W_{s+1} with Y_{n-s}-coordinate α. Hence, $Y_{n-s+1} = \beta$ is the only common root of $q_1^{(s+1)}(P, \alpha+\lambda_1 Y_{n-s+1})$ and $q_2^{(s+1)}(P, \alpha+ \lambda_2 Y_{n-s+1})$. Furthermore, the assumption on λ_2 implies that $q_2^{(s+1)}(P, \alpha + \lambda_2 Y_{n-s+1})$ is squarefree. Therefore, we conclude that the following identity holds in $\mathsf{K}(\alpha)[Y_{n-s+1}]$:

$$\gcd\left(q_1^{(s+1)}(P, \alpha + \lambda_1 Y_{n-s+1}), q_2^{(s+1)}(P, \alpha + \lambda_2 Y_{n-s+1})\right) = Y_{n-s+1} - \beta. \tag{4.2}$$

Let $q^{(s+1)}(P, Y_{n-s}) = h_1 \cdots h_N$ be the irreducible factorization of the polynomial $q^{(s+1)}(P, Y_{n-s})$ in $\mathsf{K}[Y_{n-s}]$. Every irreducible factor h_j represents a K-irreducible component $\mathcal{C}_j$ of W_{s+1}. Let $\alpha_j \in \overline{\mathbb{F}}_q$ be an arbitrary root of h_j. Taking into account the field isomorphism $\mathsf{K}(\alpha_j) \simeq \mathsf{K}[Y_{n-s}]/\big(h_j(Y_{n-s})\big)$, from identity (4.2) we conclude that there exists $v_j \in \mathsf{K}[Y_{n-s}]$ of degree at most $\deg h_j - 1$ such that the following identity holds in $\big(\mathsf{K}[Y_{n-s}]/\big(h_j(Y_{n-s})\big)\big)\,[Y_{n-s+1}]$:

$$\gcd\Big(q_1^{(s+1)}(P, Y_{n-s} + \lambda_1 Y_{n-s+1}), q_2^{(s+1)}(P, Y_{n-s} + \lambda_2 Y_{n-s+1})\Big) = Y_{n-s+1} - v_j(Y_{n-s}). \tag{4.3}$$

Fix $j \in \{1, \ldots, N\}$. From the Bézout identity we deduce that the congruence relation $Y_{n-s+1} - v_j(Y_{n-s}) \equiv 0 \bmod I(\mathcal{C}_j)$ holds. This implies that $h'_j \cdot (Y_{n-s+1} - v_j)$ belongs to the ideal $I(\mathcal{C}_j)$ for $1 \le j \le N$. Hence, $h'_j\big(\prod_{i\neq j} h_i\big)(Y_{n-s+1} - v_j)$ belongs to the ideal $I(W_{s+1}) \subset I(V_P)$ for $1 \le j \le N$.

Let

$$v_{n-s+1}^{(s+1)}(P, Y_{n-s}) := \sum_{1\le j\le N} h'_j v_j \prod_{i\neq j} h_i \mod q^{(s+1)}(P, Y_{n-s}). \tag{4.4}$$

By construction we have that $v_{n-s+1}^{(s+1)}(P, Y_{n-s})$ is an element of $\mathsf{K}[Y_{n-s}]$ of degree at most $\delta_{s+1} - 1$. Furthermore, our previous argumentation shows that $(\partial q^{(s+1)}/\partial Y_{n-s})(P, Y_{n-s})Y_{n-s+1} - v_{n-s+1}^{(s+1)}(P, Y_{n-s}) = \sum_{j=1}^N h'_j\big(\prod_{i\neq j} h_i\big)(Y_{n-s+1} - v_j)$ belongs to the ideal $I(V_P)$, and hence it represents the parametrization of Y_{n-s+1} by the zeros of $q^{(s+1)}(P, Y_{n-s})$ we are looking for.

Now we estimate the complexity and probability of the success of the algorithm described above.

Lemma 4.5. *The algorithm described above takes as input*

- *a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the polynomial F_{s+1},*
- *the polynomials $q^{(s)}(P^{(s+1)}, Y_{n-s}, Y_{n-s+1})$ and $v_{n-s+k}^{(s)}(P^{(s+1)}, Y_{n-s}, Y_{n-s+1})$ $(2 \le k \le s)$. They form the geometric solution of the lifting curve $W_{P^{(s+1)}}$ computed in Proposition 4.2,*

and outputs

- *the minimal polynomial $q^{(s+1)}(P^{(s+1)}, Y_{n-s})$ of the coordinate function of $\mathsf{K}[V_{P^{(s+1)}}]$ defined by Y_{n-s},*
- *the parametrization of Y_{n-s+1} by the zeros of $q^{(s+1)}(P^{(s+1)}, Y_{n-s})$.*

This algorithm can be implemented in a probabilistic Turing machine M running in space $O\big((\mathcal{S}+n+d)\delta^2 \log(q\delta)\big)$ and time $O\big((\mathcal{T}+n)\mathcal{U}(\delta)\big(\mathcal{U}(d\delta)+\log(q\delta)\big)\mathcal{U}(\log(q\delta))\big)$, and outputs the right result with probability at least $1 - 1/60n$.

Proof. Let E_s be the polynomial of the statement of Lemma 4.3 and let $\widehat{E}_s$ be the polynomial introduced at the beginning of this section. Recall that $\deg E_s \le 4\delta^3$ and $\deg \widehat{E}_s \le \delta^4$ hold. Let λ_1, λ_2 be two distinct values of K randomly chosen and let $\mathcal{L}_i := Y_{n-s} + \lambda_i Y_{n-s+1}$ $(i = 1, 2)$. Applying Theorem 2.2 we conclude that $E_s(\lambda_1)E_s(\lambda_2)\widehat{E}_s(\lambda_2) \neq 0$ holds with probability at least $1 - 1/72n^3$. Suppose that this is the case. Then, applying the algorithm underlying Proposition 4.4, we conclude that the minimal equations $q^{(s+1)}(P, Y_{n-s}), q_i(P, \mathcal{L}_i)$ $(i = 1, 2)$ satisfied by $Y_{n-s}, \mathcal{L}_i$ $(i = 1, 2)$ in $\mathsf{K}[V_P]$ can be computed by a probabilistic Turing machine which runs in space $O\big((\mathcal{S} + d)\delta_s^2 \log(q\delta)\big)$ and time $O\big((\mathcal{T} + n)\mathcal{U}(d\delta_s)\mathcal{U}(\delta_s)\mathcal{U}(\log(q\delta))\big)$, with probability of success at least $1 - 1/15n^3$.

Next we compute the irreducible factorization $q^{(s+1)}(P, Y_{n-s}) = h_1 \cdots h_N$ of $q^{(s+1)}(P, Y_{n-s})$ in $\mathsf{K}[Y_{n-s}]$. From [57, Corollary 14.30] we conclude that such a factorization can be computed with space $O(\delta_{s+1}^2 \log(q\delta))$ and time

$$O\big(\log(n)\big(\mathcal{U}(\delta_{s+1}^2) + \mathcal{U}(\delta_{s+1}) \log(q\delta)\big)\mathcal{U}(\log(q\delta))\big),$$

with probability of success at least $1 - 1/16n^3$.

Then we compute the polynomials $v_1, \ldots, v_N$ of (4.3) and the polynomial $v_{n-s+1}^{(s+1)}$ of (4.4) by using the EEA (see, e.g., [6], [57]). According to [57, Corollary 11.16], this step can be done deterministically using space $O(\delta_s \delta_{s+1} \log(q\delta))$ and time $O\big(\delta_{s+1}\mathcal{U}(\delta_s)\mathcal{U}(\log(q\delta))\big)$. Adding the complexity and probability estimates of each step, we easily deduce the statement of the proposition. $\square$

Now we discuss how we can obtain the parametrizations of the remaining variables Y_{n-s+k} for $2 \leq k \leq s$.

Lemma 4.6. *Given the geometric solution of the lifting curve $W_{P^{(s+1)}}$ and the output of the algorithm underlying Lemma 4.5, the polynomials $v_{n-s+k}^{(s+1)}(P^{(s+1)}, Y_{n-s})$ which parametrize Y_{n-s+k} by the zeros of $q^{(s+1)}(P^{(s+1)}, Y_{n-s})$ for $2 \leq k \leq s$ can be deterministically computed in space $O(\delta \log(q\delta))$ and time $O(s\delta\mathcal{U}(\delta) \log(q\delta))$.*

Proof. Let $(\partial q^{(s+1)}/\partial Y_{n-s})^{-1}(P, Y_{n-s}) \in \mathsf{K}[Y_{n-s}]$ denote the inverse of the polynomial $(\partial q^{(s+1)}/\partial Y_{n-s})(P, Y_{n-s})$ modulo $q^{(s+1)}(P, Y_{n-s})$. This polynomial can be computed by means of the EEA using space $O(\delta_s \log(q\delta))$ and time $O(\mathcal{U}(\delta_s) \log(q\delta))$. Let $w_{n-s+1}^{(s+1)}(P, Y_{n-s}) := (\partial q^{(s+1)}/\partial Y_{n-s})^{-1}(P, Y_{n-s})\, v_{n-s+1}^{(s+1)}(P, Y_{n-s})$. Observe that $Y_{n-s+1} - w_{n-s+1}^{(s+1)}(P, Y_{n-s})$ belongs to the ideal $I(V_P)$. With this parametrization we shall "eliminate" the variable Y_{n-s+1} of the polynomials $v_{n-s+k}^{(s)}(P, Y_{n-s}, Y_{n-s+1})$.

For this, we observe that the polynomials $q^{(s)}\big(P, Y_{n-s}, w_{n-s+1}^{(s+1)}(P, Y_{n-s})\big)$ and $(\partial q^{(s)}/\partial Y_{n-s+1})\big(P, Y_{n-s}, w_{n-s+1}^{(s+1)}(P, Y_{n-s})\big)Y_{n-s+k} - v_{n-s+k}^{(s)}\big(P, Y_{n-s}, w_{n-s+1}^{(s+1)}(P, Y_{n-s})\big)$ $(2 \leq k \leq s)$ belong to the ideal $I(V_P)$. Furthermore, we have that the polynomial $(\partial q^{(s)}/\partial Y_{n-s+1})\big(P, Y_{n-s}, w_{n-s+1}^{(s+1)}(P, Y_{n-s})\big)$ is a unit of $\mathsf{K}[Y_{n-s}]/\big(q^{(s+1)}(P, Y_{n-s})\big)$, because otherwise the discriminant $\rho^{(s)}(P, Y_{n-s})$ would have common roots with $q^{(s+1)}(P, Y_{n-s})$, thus contradicting condition (iii) of Theorem 3.3. Therefore, its inverse b_{n-s+1} modulo $q^{(s+1)}(P, Y_{n-s})$ is a well-defined element of $\mathsf{K}[Y_{n-s}]$, and $Y_{n-s+k} - b_{n-s+1} \cdot v_{n-s+k}^{(s)}\big(P, Y_{n-s}, w_{n-s+1}^{(s+1)}(P, Y_{n-s})\big)$ belongs to $I(V_P)$ for $2 \leq k \leq s$. Therefore, if we let

$$w_{n-s+k} := b_{n-s+1} \cdot v_{n-s+k}^{(s)}\big(P, Y_{n-s}, w_{n-s+1}^{(s+1)}(P, Y_{n-s})\big) \quad (2 \leq k \leq s), \tag{4.5}$$

we see that $Y_{n-s+k} - w_{n-s+k}$ belongs to $I(V_P)$ for $2 \leq k \leq s$. Multiplying w_{n-s+k} by $(\partial q^{(s+1)}/\partial Y_{n-s})(P, Y_{n-s})$ for $2 \leq k \leq s$, and reducing modulo $q^{(s+1)}(P, Y_{n-s})$, we obtain the polynomials $v_{n-s+k}^{(s+1)} \in \mathsf{K}[Y_{n-s}]$ $(2 \leq k \leq s)$ we are looking for.

The polynomials b_{n-s+1} and w_{n-s+k} $(2 \le k \le s)$ of (4.5) can be computed with space $O(s\delta_{s+1}\log(q\delta))$ and time $O(s\delta_s\mathcal{U}(\delta_{s+1})\log(q\delta))$, and the polynomials $v_{n-s+k}^{(s+1)}(P^{(s+1)}, Y_{n-s})$ for $2 \le k \le s$ can be computed with the same asymptotic complexity estimate. This finishes the proof of the lemma. □

As a consequence of Proposition 4.4 and Lemmas 4.5 and 4.6, we have an algorithm for computing the polynomials $q^{(s+1)}(P, Y_{n-s})$, $v_{n-s+k}^{(s+1)}(P, Y_{n-s}) \in \mathsf{K}[Y_{n-s}]$ $(1 \le k \le s)$. These polynomials form a geometric solution of V_P. We summarize the complexity and probability estimates of this algorithm in the next proposition.

Proposition 4.7. *The algorithm underlying Proposition* 4.4 *and Lemmas* 4.5 *and* 4.6 *has as input*

- *a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the polynomial F_{s+1},*
- *the polynomials $q^{(s)}(P^{(s+1)}, Y_{n-s}, Y_{n-s+1})$ and $v_{n-s+k}^{(s)}(P^{(s+1)}, Y_{n-s}, Y_{n-s+1})$ $(2 \le k \le s)$. They form the geometric solution of the lifting curve $W_{P^{(s+1)}}$ computed in Proposition* 4.2*,*

and outputs a geometric solution of the lifting fiber $V_{P^{(s+1)}}$. It can be implemented in a probabilistic Turing machine running in space $O\big((\mathcal{S}+n+d)\delta^2\log(q\delta)\big)$ and time $O\big((\mathcal{T}+n)\mathcal{U}(\delta)\big(\mathcal{U}(d\delta)+\log(q\delta)\big)\mathcal{U}(\log(q\delta))\big)$, and outputs the right result with probability at least $1-1/60n$.

The algorithm underlying Proposition 4.7 extends to the positive characteristic case the algorithms of [29] and [25], having a better asymptotic complexity estimate (in terms of the number of arithmetic operations performed) than [29], and a similar complexity estimate as in [25]. We also contribute to the latter by providing estimates on the probability of success of the algorithm, which are not present in [25]. Finally, we remark that by means of our preprocessing we have significantly simplified both the algorithms of [29] and [25].

4.4. **A K-definable geometric solution of V.** Now we have all the ingredients necessary to describe our algorithm computing the K-definable geometric solution of our input variety $V := V_r$. We recall that K is a field extension of $\mathbb{F}_q$ of cardinality greater than $60n^4d\delta^4$. Let (λ, γ, P) be a point randomly chosen in the set $\mathsf{K}^{n(n+1)} \times \mathsf{K}^{n-1}$. Theorem 2.2 shows that $B(\lambda, \gamma, P)$ does not vanish with probability at least $14/15$, where B is the polynomial defined at the beginning of Section 4. Assume that we have chosen such a point and let $(Y_1, \dots, Y_n) := \lambda X + \gamma$ and $P := (p_1, \dots, p_{n-1})$. Then $Y_1, \dots, Y_n$ and $P^{(s)} := (p_1, \dots, p_{n-s})$ satisfy the conditions of Theorem 3.3 for $1 \le s \le r-1$.

Therefore, we may recursively apply, for $1 \le s \le r-1$, the algorithms underlying Propositions 4.2 and 4.7, which compute a geometric solution of the lifting curve $W_{P^{(s+1)}}$ and of the lifting fiber $V_{P^{(s+1)}}$, respectively. In this way, at the end of the $(r-1)$-th recursive step we obtain a geometric solution of the lifting fiber $V_{P^{(r)}}$. Taking into account the complexity and probability estimates of Propositions 4.2 and 4.7, we easily deduce the following result.

Theorem 4.8. *The algorithm described above takes as input a straight-line program which represents the input polynomials $F_1, \dots, F_r$ with space $\mathcal{S}$ and time $\mathcal{T}$, and outputs a geometric solution of the lifting fiber $V_{P^{(r)}}$. It can be implemented to run* *in a probabilistic Turing machine M using space $O\big((\mathcal{S}+n+d)\delta^2\log(q\delta)\big)$ and time*

$$O\big((n\mathcal{T}+n^5)\mathcal{U}(\delta)\big(\mathcal{U}(d\delta)+\log(q\delta)\big)\mathcal{U}(\log(q\delta))\big).$$

This Turing machine outputs the right result with probability at least $1-1/12$.

The complexity estimate of Theorem 4.8 significantly improves the $O(d^{n^2})$ complexity estimate of [30], the $O(d^{2r})$ estimate of [31], and the estimates of the algorithms of the so-called Gröbner solving. Furthermore, let us remark that, combining the algorithm underlying Theorem 4.8 with techniques of p-adic lifting, as those of [25], for a "lucky" choice of prime number p one obtains an efficient probabilistic algorithm for computing the geometric solution of an equidimensional variety over $\mathbb{Q}$ given by a reduced regular sequence.

5. An $\mathbb{F}_q$-definable lifting fiber of V

Let notations and assumptions be as in Section 4.4. In this section we obtain a geometric solution of an $\mathbb{F}_q$-definable lifting fiber of V. For this purpose, we shall homotopically deform the K-definable geometric solution of the lifting fiber $V_{P^{(r)}} := \pi_r^{-1}(P^{(r)})$, computed in the previous section, into a geometric solution of an $\mathbb{F}_q$-definable lifting fiber $\pi^{-1}(Q)$ of the linear projection mapping $\pi : V \to \mathbb{A}^{n-r}$. This geometric solution is determined by suitable linear forms $Z_1, \ldots, Z_{n-r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$. The deformation will be given as a homotopy of the form $(1-T)Y_j + TZ_j$ for $1 \le j \le n-r+1$, where T is a new indeterminate.

Let $(\lambda, \gamma, P) \in \mathsf{K}^{n(n+1)} \times \mathsf{K}^{n-r}$ be the point fixed in Section 4, which yields the linear forms $Y := (Y_1, \ldots, Y_n) := \lambda X + \gamma$ and the point $P \in \mathsf{K}^{n-r}$. Write $\gamma := (\gamma_1, \ldots, \gamma_n)$ and $P := (p_1, \ldots, p_{n-r})$. Let Λ be an $(n-r+1)\times n$ matrix of indeterminates. For $1 \le i \le n-r+1$, let $\Lambda^{(i)} := (\Lambda_{i,1}, \ldots, \Lambda_{i,n})$ denote its ith row and let $\Lambda^{[1:i]}$ denote the $i \times n$ submatrix of Λ consisting of the first i rows of Λ. Let $\Gamma := (\Gamma_1, \ldots, \Gamma_{n-r+1})$ be a vector of indeterminates, and let $\widetilde{Y} := (\widetilde{Y}_1, \ldots, \widetilde{Y}_{n-r+1}) := \Lambda X + \Gamma$.

Let $\widehat{B} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-r}]$ be the polynomial of Corollary 3.4, and let $B' := \det(\Delta_1)\det(\Delta_2)\widehat{B}$, where Δ_1 is the $n \times n$ matrix that has $\Lambda^{[1:n-r]}$ as its upper $(n-r)\times n$ submatrix, and the coefficients of the linear forms $Y_{n-r+1}, \ldots, Y_n$ in its last r rows, and Δ_2 is the $n\times n$ matrix having $\Lambda^{[1:n-r+1]}$ as its upper $(n-r+1)\times n$ submatrix, and the coefficients of $Y_{n-r+2}, \ldots, Y_n$ in its last $r-1$ rows. Observe that $\deg B' \le 2(n-r+2)nd\delta_r^2$ holds.

Suppose that $q > 8n^2d\delta_r^4$ holds, and let $(\nu, \eta, Q) \in \mathbb{F}_q^{(n-r+1)(n+1)} \times \mathbb{F}_q^{n-r}$ be a point such that $B'(\nu, \eta, Q) \neq 0$. Theorem 2.2 shows that such a point (ν, η, Q) can be randomly chosen in the set $\mathbb{F}_q^{(n-r+1)(n+1)} \times \mathbb{F}_q^{n-r}$ with probability of success at least $1-1/16$.

Let $\nu := \nu^{[1:n-r+1]}$, $\eta := (\eta_1, \ldots, \eta_{n-r+1})$, $Q := (q_1, \ldots, q_{n-r})$, and $Z := (Z_1, \ldots, Z_{n-r+1}) := \nu X + \eta$. The condition $\det(\Delta_1 \cdot \Delta_2)(\nu) \neq 0$ implies that the sets of linear forms $Z_1, \ldots, Z_{n-r}, Y_{n-r+1}, \ldots, Y_n$ and $Z_1, \ldots, Z_{n-r+1}, Y_{n-r+2}, \ldots, Y_n$ induce linear changes of coordinates. Furthermore, from the condition $\widehat{B}(\nu, \eta, Q) \neq 0$ and Corollary 3.4, we conclude that the linear projection mapping $\pi : V \to \mathbb{A}^{n-r}$ defined by $Z_1, \ldots, Z_{n-r}$ is a finite morphism, $Q \in \mathbb{F}_q^{n-r}$ is a lifting point of π, and Z_{n-r+1} is a primitive element of the lifting fiber $V_Q := \pi^{-1}(Q)$.

Let T be a new indeterminate, and let $\widehat{\Lambda} \in \mathsf{K}[T]^{n\times n}$ and $\widehat{\Gamma} \in \mathsf{K}[T]^n$ be the matrix and column vector defined in the following way:

$$\begin{array}{rcl}\widehat{\Lambda} & := & (1-T)\lambda \;+ T\Delta_1(\nu^{[1:n-r]}),\\ \widehat{\Gamma} & := & (1-T)\gamma^t + T(\eta_1,\ldots,\eta_{n-r},\gamma_{n-r+1},\ldots,\gamma_n)^t,\end{array}$$

where $\nu^{[1:n-r]}$ denotes the $(n-r)\times n$ matrix consisting of the first $n-r$ rows of ν and the symbol ^{t} denotes transposition. Let $\widehat{\Lambda}^{[1:n-r]}$ denote the $(n-r)\times n$ submatrix of $\widehat{\Lambda}$ consisting of the first $n-r$ rows of $\widehat{\Lambda}$ and let $\widehat{\Gamma}^{[1:n-r]}$ be the vector consisting of the first $n-r$ entries of $\widehat{\Gamma}$, respectively.

Let W be the subvariety of $\mathbb{A}^n\big(\overline{\mathbb{F}_q(T)}\big)$ defined by the set of common zeros of $F_1,\ldots,F_r$. Let $\widehat{Z} := (\widehat{Z}_1,\ldots,\widehat{Z}_n) := \widehat{\Lambda}X+\widehat{\Gamma}$ and $\widehat{P} := (\widehat{p}_1,\ldots,\widehat{p}_{n-r}) := (1-T)P+TQ$. Since $\widehat{\Lambda}$ is an invertible element of $\overline{\mathbb{F}}_q(T)^{n\times n}$, we have that $X = \widehat{\Lambda}^{-1}(\widehat{Z}-\widehat{\Gamma})$ holds, and hence $\widehat{F}_j := F_j(\widehat{\Lambda}^{-1}(\widehat{Z}-\widehat{\Gamma}))$ is a well-defined element of $\overline{\mathbb{F}}_q(T)[\widehat{Z}_1,\ldots,\widehat{Z}_n]$ for $1\le j\le r$. Observe that the point $(\widehat{\Lambda},\widehat{\Gamma},\widehat{P}) \in \mathbb{A}^{n(n+1)}\big(\overline{\mathbb{F}_q(T)}\big)\times\mathbb{A}^{n-r}\big(\overline{\mathbb{F}_q(T)}\big)$ does not annihilate the polynomial $\widehat{B}$ of the statement of Corollary 3.4. Therefore, applying Corollary 3.4, replacing the field $\overline{\mathbb{F}}_q$ by $\overline{\mathbb{F}_q(T)}$, we conclude that $\overline{\mathbb{F}_q(T)}[\widehat{Z}_1,\ldots,\widehat{Z}_{n-r}] \hookrightarrow \overline{\mathbb{F}_q(T)}[X]/(F_1,\ldots,F_r)$ is an integral ring extension, $\widehat{P}$ is a lifting point of the linear projection mapping $\pi^e : W \to \overline{\mathbb{F}_q(T)}^{n-r}$ defined by $\widehat{Z}_1,\ldots,\widehat{Z}_{n-r}$, and $\widehat{Z}_{n-r+1} = Y_{n-r+1}$ is a primitive element of the (zero-dimensional) lifting fiber $W_{\widehat{P}} := (\pi^e)^{-1}(\widehat{P})$.

Let $\widehat{q}_{\widehat{Z}_{n-r+1}} := \widehat{q}_{\widehat{Z}_{n-r+1}}(\widehat{P},\widehat{Z}_{n-r+1}) \in \overline{\mathbb{F}_q(T)}[\widehat{Z}_{n-r+1}]$ denote the minimal equation satisfied by $\widehat{Z}_{n-r+1}$ in $\overline{\mathbb{F}_q(T)}[W_{\widehat{P}}]$. By the $\mathsf{K}(T)$-definability of $W_{\widehat{P}}$ and $\widehat{Z}_{n-r+1}$, we see that $\widehat{q}_{\widehat{Z}_{n-r+1}}$ belongs to $\mathsf{K}(T)[\widehat{Z}_{n-r+1}]$. Furthermore, our choice of $\widehat{P}$ and $\widehat{Z}_1,\ldots,\widehat{Z}_{n-r+1}$ implies that $\widehat{q}_{\widehat{Z}_{n-r+1}}$ is a separable element of $\mathsf{K}(T)[\widehat{Z}_{n-r+1}]$ of degree δ_r. Let $\widehat{\rho} \in \mathsf{K}[T]$ be the product of its denominator and the numerator of its discriminant with respect to $\widehat{Z}_{n-r+1}$. In order to perform the homotopic deformation mentioned at the beginning of this section, we need the following preliminary result.

Lemma 5.1. *The polynomials $\widehat{F}_j(\widehat{P},Y_{n-r+1},\ldots,Y_n)$ $(1\le j\le r)$ form a regular sequence and generate a radical ideal $\widehat{I}_{\widehat{P}}$ of $\mathsf{K}[T]_{\widehat{\rho}}[Y_{n-r+1},\ldots,Y_n]$. The ring extension*

$$\mathsf{K}[T]_{\widehat{\rho}} \hookrightarrow \mathsf{K}[T]_{\widehat{\rho}}[Y_{n-r+1},\ldots,Y_n]/\widehat{I}_{\widehat{P}} \tag{5.1}$$

is integral of rank δ_r.

Proof. Arguing by contradiction, suppose that there exists $1\le j\le r$ such that $\widehat{F}_j(\widehat{P},Y_{n-r+1},\ldots,Y_n)$ is a zero divisor modulo the ideal generated by the polynomials $\widehat{F}_1(\widehat{P},Y_{n-r+1},\ldots,Y_n),\ldots,\widehat{F}_{j-1}(\widehat{P},Y_{n-r+1},\ldots,Y_n)$. Substituting $T=0$ in these polynomials, we conclude that $F_j(P,Y_{n-r+1},\ldots,Y_n)$ is a zero divisor modulo $F_1(P,Y_{n-r+1},\ldots,Y_n),\ldots,F_{j-1}(P,Y_{n-r+1},\ldots,Y_n)$, thus contradicting Lemma 4.1. This shows that $\widehat{F}_j(\widehat{P},Y_{n-r+1},\ldots,Y_n)$ $(1\le j\le r)$ form a regular sequence. A similar argument shows that $\det\big(\partial\widehat{F}_i(\widehat{P},Y_{n-r+1},\ldots,Y_n)/\partial Y_{n-r+j}\big)_{1\le i,j\le r}$ is not a zero divisor modulo $\widehat{I}_{\widehat{P}}$. Hence, [16, Theorem 18.15] implies that the ideal $\widehat{I}_{\widehat{P}}$ is radical.

By the remarks before the lemma, we see that $\widehat{q}_{\widehat{Z}_{n-r+1}} \in \mathsf{K}[T]_{\widehat{\rho}}[\widehat{Z}_{n-r+1}]$ yields an integral dependence equation for the coordinate function $\widehat{z}_{n-r+1}$ induced by $\widehat{Z}_{n-r+1}$ in the ring extension (5.1). We conclude that $\mathsf{K}[T]_{\widehat{\rho}} \hookrightarrow \mathsf{K}[T]_{\widehat{\rho}}[\widehat{z}_{n-r+1}]$ is an integral ring extension.

Let $\xi_1, \ldots, \xi_n$ denote the coordinate functions of $\mathsf{K}[T]_{\widehat{\rho}}[Y_{n-r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ induced by $X_1, \ldots, X_n$. Arguing as in (3.5) of the proof of Proposition 3.1, we conclude that there exist polynomials $\widehat{P}_1, \ldots, \widehat{P}_n \in \mathsf{K}[T]_{\widehat{\rho}}[\widehat{Z}_{n-r+1}]$ such that $\xi_k = \widehat{P}_k(\widehat{z}_{n-r+1})$ holds for $1 \le k \le n$. This shows that $\mathsf{K}[T]_{\widehat{\rho}}[\widehat{z}_{n-r+1}] \hookrightarrow \mathsf{K}[T]_{\widehat{\rho}}[\xi_1, \ldots, \xi_n] = \mathsf{K}[T]_{\widehat{\rho}}[Y_{n-r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ is an integral ring extension and, combined with the fact that $\mathsf{K}[T]_{\widehat{\rho}} \hookrightarrow \mathsf{K}[T]_{\widehat{\rho}}[\widehat{z}_{n-r+1}]$ is an integral ring extension, proves that (5.1) is integral.

Our previous assertions imply that $\mathsf{K}[T]_{\widehat{\rho}}[Y_{n-r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ is a free $\mathsf{K}[T]_{\widehat{\rho}}$-module of rank at most δ_r. Since $\widehat{q}_{\widehat{Z}_{n-r+1}}(\widehat{P}, \widehat{Z}_{n-r+1})$ is the minimal dependence equation satisfied by $\widehat{z}_{n-r+1}$ in the extension (5.1), we conclude that the rank of $\mathsf{K}[T]_{\widehat{\rho}}[Y_{n-r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ as a $\mathsf{K}[T]_{\widehat{\rho}}$-module is exactly δ_r. This finishes the proof of the lemma. $\square$

Let $\widehat{V} \subset \mathbb{A}^{r+1}$ be the affine equidimensional variety defined by $\widehat{I}_{\widehat{P}}$ and let $\widehat{\pi} : \widehat{V} \to \mathbb{A}^1$ be the mapping induced by the projection onto the coordinate T. Lemma 5.1 implies that $\widehat{V}$ has dimension 1 and degree δ_r, and $\widehat{\pi}$ is a dominant morphism. Furthermore, taking into account the equalities $\widehat{V} \cap \{T = 0\} = \{0\} \times V_P$ and $\widehat{V} \cap \{T = 1\} = \{1\} \times V_Q$, we conclude that $T = 0$ and $T = 1$ are lifting points of the morphism $\widehat{\pi}$. Therefore, applying the Newton–Hensel procedure mentioned in Section 4.1, we obtain a geometric solution of the lifting fiber V_Q. This is the content of our next result.

Proposition 5.2. *Suppose that $q > 8n^2 d\delta_r^4$ holds. Given as input*

- *a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the input polynomials $F_1, \ldots, F_r$,*
- *the polynomials $q^{(r)}(P^{(r)}, Y_{n-r+1})$, $v_{n-r+k}^{(r)}(P^{(r)}, Y_{n-r+1})$ $(2 \le k \le r)$, which form the geometric solution of the lifting fiber $V_{P^{(r)}}$ computed in Theorem 4.8,*

the polynomials $q(Q, Z_{n-r+1}) \in \mathbb{F}_q[Z_{n-r+1}]$, $v_{n-r+k}(Q, Z_{n-r+1}) \in \mathsf{K}[Z_{n-r+1}]$ $(2 \le k \le r)$ which form a geometric solution of the lifting fiber V_Q can be computed using space $O\big((\mathcal{S}+n)\delta_r^2 \log(q\delta)\big)$ and time $O\big((n\mathcal{T}+n^5)\mathcal{U}(\delta_r)^2\mathcal{U}(\log(q\delta))\big)$. This algorithm outputs the right result with probability at least $1 - 1/16$.

Proof. Let (ν, η, Q) be a point randomly chosen in the set $\mathbb{F}_q^{(n-r+1)(n+1)} \times \mathbb{F}_q^{n-r}$. Let $B' \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-r}]$ be the polynomial introduced at the beginning of this section. Since $\deg B' \le 2(n-r+2)nd\delta_r^2$ holds, from Theorem 2.2 we conclude that $B'(\nu, \eta, Q) \ne 0$ holds with probability at least $1 - 1/16$.

By the remarks before the statement of the proposition, we see that $T = 0$ and $T = 1$ are lifting points of the morphism $\widehat{\pi}$. Then, applying the Newton–Hensel procedure of [51], we see that there exists a computation tree in K, computing polynomials $\widehat{q}(T, Y_{n-r+1})$, $\widehat{v}_{n-r+k}(T, Y_{n-r+1})$ $(2 \le k \le r)$ which form a geometric solution of $\widehat{V}$. This computation tree requires $O\big((n\mathcal{T}+n^5)\mathcal{U}(\delta_r)^2\big)$ operations in K, using at most $O\big((\mathcal{S}+n)\delta_r^2\big)$ arithmetic registers. Making the substitution $T = 1$

in these polynomials we obtain polynomials $\widehat{q}(1, Y_{n-r+1})$, $\widehat{v}_{n-r+k}(1, Y_{n-r+1})$ $(2 \leq k \leq r)$, which form a geometric solution of the lifting fiber $\widehat{V} \cap \{T = 1\} = \{1\} \times V_Q$ (and therefore of V_Q), using Y_{n-r+1} as a primitive element.

Our next goal is to compute a geometric solution of V_Q, using Z_{n-r+1} as a primitive element. In order to do this, let $\widehat{w}_{n-r+k}(1, Y_{n-r+1}) \in \mathsf{K}[Y_{n-r+1}]$ denote the remainder of the product $(\partial\widehat{q}/\partial Y_{n-r+1})(1, Y_{n-r+1})^{-1} \cdot \widehat{v}_{n-r+k}(1, Y_{n-r+1})$ modulo $\widehat{q}(1, Y_{n-r+1})$ for $2 \leq k \leq r$. Observe that $Y_{n-r+k} = \widehat{w}_{n-r+k}(1, Y_{n-r+1})$ holds in $\mathsf{K}[V_Q]$ for $2 \leq k \leq r$. Write $Z_{n-r+1} = \alpha_1 Z_1 + \cdots + \alpha_{n-r} Z_{n-r} + \alpha_{n-r+1} Y_{n-r+1} + \cdots + \alpha_n Y_n$. Then, from the identity

$$\mathrm{Res}\big(\widehat{q}(1, Y_{n-r+1}), g\big) = \prod_{x \in V_Q} g(Y_{n-r+1}(x)),$$

we easily see that the minimal equation satisfied by the linear form $Z_{n-r+1} + TY_{n-r+1}$ in $\overline{\mathbb{F}}_q[T] \otimes \overline{\mathbb{F}}_q[V_Q]$ is given by

$$\begin{aligned} &q_{Z_{n-r+1}+TY_{n-r+1}}(Q, T, S) \\ &\quad = \mathrm{Res}_U\Big(\widehat{q}(1, U), S - \sum_{k=1}^{n-r} \alpha_k q_k - (\alpha_{n-r+1} + T)U - \sum_{k=n-r+2}^{n} \alpha_k \widehat{w}_k(1, U)\Big). \end{aligned} \tag{5.2}$$

Following [1], [46] as in the proof of Proposition 3.1, we have the congruence relation

$$\begin{aligned} &q_{Z_{n-r+1}+TY_{n-r+1}}(Q, T, Z_{n-r+1}) \equiv q(Q, Z_{n-r+1}) \\ &\quad + T\Big(\partial q/\partial Z_{n-r+1}(Q, Z_{n-r+1}) Y_{n-r+1} - v_{n-r+1}(Q, Z_{n-r+1})\Big) \bmod (T^2), \end{aligned}$$

where $q(Q, Z_{n-r+1})$ is the minimal polynomial of the coordinate function defined by Z_{n-r+1} in $\mathsf{K}[V_Q]$ and $(\partial q/\partial Z_{n-r+1})(Q, Z_{n-r+1}) Y_{n-r+1} = v_{n-r+1}(Q, Z_{n-r+1})$ holds in $\mathsf{K}[V_Q]$.

We compute the right-hand side term of (5.2), up to order T^2, by interpolation in the variable S, thus reducing the computation to δ_r resultants of univariate polynomials of $\mathsf{K}[T]$ of degree at most 1. Using fast algorithms for univariate resultants and interpolation over K (see, e.g., [6], [57]), we conclude that the dense representation of $q(Q, S)$ and $v_{n-r+1}(Q, S)$ can be deterministically computed with $O(\delta_r \mathcal{U}(\delta_r))$ arithmetic operations over K, using at most $O(\delta_r^2)$ arithmetic registers.

Finally, it remains to compute the polynomials $v_{n-r+k}(Q, Z_{n-r+1})$ $(2 \leq k \leq r)$ which parametrize Y_{n-r+k} by the zeros of $q(Q, Z_{n-r+1})$. For this purpose, we shall compute polynomials $w_{n-r+k}(Q, Z_{n-r+1})$ $(1 \leq k \leq r)$ of degree at most $\delta_r - 1$ such that $Y_{n-r+k} \equiv w_{n-r+k}(Q, Z_{n-r+1})$ holds in $\mathsf{K}[V_Q]$. From these data the polynomials $v_{n-r+k}(Q, Z_{n-r+1})$ $(2 \leq k \leq r)$ can easily be obtained by multiplication by $(\partial q/\partial Z_{n-r+1})(Q, Z_{n-r+1})$ and modular reduction.

The polynomial $w_{n-r+1}(Q, Z_{n-r+1})$ can be computed as the remainder of the product $(\partial q/\partial Z_{n-r+1})(Q, Z_{n-r+1})^{-1} \cdot v_{n-r+1}(Q, Z_{n-r+1})$ modulo $q(Q, Z_{n-r+1})$. Then, since the identities $Y_{n-r+k} = \widehat{w}_{n-r+k}(1, Y_{n-r+1})$ and $Y_{n-r+1} = v_{n-r+1}(Z_{n-r+1})$ hold in $\mathsf{K}[V_Q]$ for $2 \leq k \leq r$, we conclude that the polynomial $w_{n-r+k}(Q, Z_{n-r+1})$ equals the remainder of $\widehat{w}_{n-r+k}\big(1, v_{n-r+1}(Z_{n-r+1})\big)$ modulo $q(Q, Z_{n-r+1})$ for $2 \leq k \leq r$. Therefore, the polynomials $w_{n-r+k}(Q, Z_{n-r+1})$ $(2 \leq k \leq r)$ can be computed with $O(\delta_r \mathcal{U}(\delta_r))$ arithmetic operations in K, using at most $O(\delta_r^2)$ arithmetic registers.

Putting together the complexity and probability of success of each step of the procedure above finishes the proof of the proposition. $\square$

6. The computation of a rational point of V

In this section we exhibit a probabilistic algorithm which computes a rational point of the variety $V := V_r$. For this purpose, let K be the finite field extension of $\mathbb{F}_q$ introduced in Section 4 and assume that we are given $\overline{\mathbb{F}}_q$-linearly independent linear forms $Z_1, \ldots, Z_{n-r+1}, Y_{n-r+2}, \ldots, Y_n \in \overline{\mathbb{F}}_q[X]$, with $Z_1, \ldots, Z_{n-r+1} \in \mathbb{F}_q[X]$ and $Y_{n-r+2}, \ldots, Y_n \in \mathsf{K}[X]$, and a point $Q := (q_1, \ldots, q_{n-r}) \in \mathbb{F}_q^{n-r}$, such that the linear projection mapping $\pi : V \to \mathbb{A}^{n-r}$ determined by $Z_1, \ldots, Z_{n-r}$ is a finite morphism and Q is a lifting point of π. Furthermore, assume that we are given polynomials $q(Q, Z_{n-r+1}) \in \mathbb{F}_q[Z_{n-r+1}]$, $v_{n-r+k}(Q, Z_{n-r+1}) \in \mathsf{K}[Z_{n-r+1}]$ $(2 \le k \le r)$ which form a geometric solution of the lifting fiber V_Q, as provided by Proposition 5.2.

Let $\omega := (\omega_1, \ldots, \omega_{n-r})$ be an arbitrary point of $\mathbb{A}^{n-r}$, let $L_\omega \subset \mathbb{A}^n$ be the $(r+1)$-dimensional affine linear subvariety of $\mathbb{A}^n$ parametrized by $Z_j = \omega_j T + q_j$ $(1 \le j \le n-r)$ and let $\mathcal{C}_\omega := V \cap L_\omega$. We may consider $\mathcal{C}_\omega$ as the affine subvariety of $\mathbb{A}^{r+1}$ defined by the set of common zeros of the polynomials

$$F_j(\omega T + Q, Z_{n-r+1}, Y_{n-r+2}, \ldots, Y_n) \quad (1 \le j \le r).$$

With this interpretation, let $\pi_\omega : \mathcal{C}_\omega \to \mathbb{A}^1$ be the projection mapping induced by T. We have the following result.

Lemma 6.1. *The variety $\mathcal{C}_\omega \subset \mathbb{A}^{r+1}$ is equidimensional of dimension 1 and degree δ_r, the mapping π_ω is a finite morphism, and 0 is an unramified value of π_ω.*

Proof. Observe that $\mathcal{C}_\omega = V \cap L_\omega = \pi^{-1}(L_\omega)$. Since π is a finite morphism, we conclude that $\dim \mathcal{C}_\omega = \dim_{\mathbb{A}^{n-r}} L_\omega = 1$. Further, $\mathcal{C}_\omega$ is defined by r polynomials in $\mathbb{A}^{r+1}$, and thus it cannot have irreducible components of dimension 0. This shows that $\mathcal{C}_\omega$ is equidimensional of dimension 1.

The fact that the injective mapping $\overline{\mathbb{F}}_q[Z_1, \ldots, Z_{n-r}] \hookrightarrow \overline{\mathbb{F}}_q[V]$ induces an integral ring extension implies that $\overline{\mathbb{F}}_q[T] \hookrightarrow \overline{\mathbb{F}}_q[\mathcal{C}_\omega]$ is an injective mapping which induces an integral ring extension, thus showing that π_ω is a finite morphism. From the Bézout inequality (2.1), we see that $\deg \mathcal{C}_\omega \le \delta_r$ holds. On the other hand, since $\pi_\omega^{-1}(0) = V_Q$ holds, we have $\delta_r = \deg V_Q \le \deg \mathcal{C}_\omega$. We conclude that $\deg \mathcal{C}_\omega = \delta_r$ holds and 0 is an unramified value of π_ω. $\square$

Our intention is to find a rational point of the curve $\mathcal{C}_\omega$ for a suitably chosen $\omega \in \mathbb{F}_q^{n-r}$. For this purpose, we are going to find a rational point (t, z_{n-r+1}) of the plane curve W_ω defined by the polynomial $h := q(\omega T + Q, Z_{n-r+1})$ such that (t, z_{n-r+1}) does not belong to the plane curve $\widetilde{W}_\omega$ defined by the polynomial $\partial h / \partial Z_{n-r+1}$. Here $q(\omega T + Q, Z_{n-r+1})$ denotes the minimal polynomial of the coordinate function defined by Z_{n-r+1} in the integral ring extension $\overline{\mathbb{F}}_q[T] \hookrightarrow \overline{\mathbb{F}}_q[\mathcal{C}_\omega]$. Observe that the $\mathbb{F}_q$-definability of $\mathcal{C}_\omega$ and W_ω imply that $h \in \mathbb{F}_q[T, Z_{n-r+1}]$. Let $\widetilde{\pi}_\omega : \mathcal{C}_\omega \to \mathbb{A}^2$ be the mapping defined by T, Z_{n-r+1}. From Lemma 3.5 we deduce that $\widetilde{\pi}_\omega$ induces a birational mapping $\widetilde{\pi}_\omega : \mathcal{C}_\omega \to W_\omega$, whose inverse is an $\mathbb{F}_q$-definable rational mapping defined on $W_\omega \setminus \widetilde{W}_\omega$. This inverse can easily be expressed in terms of the polynomials $v_{n-r+k}(\omega T + Q, Z_{n-r+1})$ $(2 \le k \le r)$ which parametrize Y_{n-r+k} by the zeros of h. Therefore, using this inverse we shall be able to obtain a rational point of our input variety V.

Unfortunately, the existence of a rational point of the plane curve W_ω cannot be asserted if W_ω does not have at least one absolutely irreducible component defined over $\mathbb{F}_q$. In order to assure that this condition holds, let $C \in \overline{\mathbb{F}}_q[\Omega_1, \ldots, \Omega_{n-r}]$ be the (nonzero) polynomial of the statement of Theorem 3.6. Recall that C has degree bounded by $2\delta_r^4$. Theorem 3.6 asserts that, for any $\omega \in \mathbb{F}_q^{n-r}$ with $C(\omega) \neq 0$, the curve W_ω is absolutely irreducible. Assume as in Section 5 that $q > 8n^2 d\delta_r^4$ holds. Theorem 2.2 shows that a random choice of ω in $\mathbb{F}_q^{n-r}$ satisfies the condition $C(\omega) \neq 0$ with probability at least $1 - 1/72$. From now on we shall assume that we have chosen such ω.

Proposition 6.2. *Let $q > 8n^2 d\delta_r^4$. Suppose that we are given:*

- *a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the polynomials $F_1, \ldots, F_r$,*
- *the dense representation of elements of $\mathsf{K}[Z_{n-r+1}]$ which form a geometric solution of the lifting fiber V_Q, as provided by Proposition* 5.2.

Then, we can deterministically compute the dense representation of elements

$$q(\omega T + Q, Z_{n-r+1}) \in \mathbb{F}_q[T, Z_{n-r+1}],$$
$$v_{n-r+k}(\omega T + Q, Z_{n-r+1}) \in \mathsf{K}[T, Z_{n-r+1}] \quad (2 \leq k \leq r)$$

which form a geometric solution of the absolutely irreducible curve $\mathcal{C}_\omega$. The algorithm runs in space $O\big((\mathcal{S}+n)\delta^2 \log(q\delta)\big)$ and time $O\big((n\mathcal{T} + n^5)\mathcal{U}(\delta)^2\mathcal{U}(\log(q\delta))\big)$.

Proof. Arguing as in the proof of Lemma 4.1, we easily conclude that

$$F_j(\omega T + Q, Z_{n-r+1}, Y_{n-r+2}, \ldots, Y_n) \quad (1 \leq j \leq r)$$

form a regular sequence and generate a radical ideal of

$$\mathbb{F}_q[T, Z_{n-r+1}, Y_{n-r+2}, \ldots, Y_n].$$

Then the deterministic algorithm underlying Proposition 4.2 yields a geometric solution of the curve $\mathcal{C}_\omega$. From the complexity estimate of Proposition 4.2 we deduce the statement of the proposition. □

6.1. **Computing a rational point of a plane curve.** In this subsection we exhibit a probabilistic algorithm which computes a rational point of the curve $\mathcal{C}_\omega \subset V$ previously defined.

Let $h := q(\omega T + Q, Z_{n-r+1})$. Recall that h is an absolutely irreducible polynomial of $\mathbb{F}_q[T, Z_{n-r+1}]$ of degree $\delta_r > 0$. Let as in the previous section $W_\omega, \widetilde{W}_\omega \subset \mathbb{A}^2$ denote the plane curves defined by h and $\partial h/\partial Z_{n-r+1}$, respectively. As remarked in the previous section, our aim is to compute a point in the set $(W_\omega \setminus \widetilde{W}_\omega) \cap \mathbb{F}_q^2$, from which we shall immediately obtain a rational of point V.

Lemma 6.3. *If $q > 8n^2 d\delta_r^4$, then*

$$\#\big((W_\omega \setminus \widetilde{W}_\omega) \cap \mathbb{F}_q^2\big) \geq q - q^{1/2}\delta_r^2 - \delta_r^2. \tag{6.1}$$

In particular, there exists at least a rational point of $W_\omega \setminus \widetilde{W}_\omega$, and thus of V.

Proof. Weil's classical estimate on the number of rational points of an absolutely irreducible nonsingular projective plane curve [60] implies that the set of rational points of W_ω satisfies the estimate (see, e.g., [49])

$$|\#(W_\omega \cap \mathbb{F}_q^2) - q| \leq (\delta_r - 1)(\delta_r - 2)q^{1/2} + \delta_r + 1 \leq \delta_r^2 q^{1/2}.$$

We deduce the lower bound $\#(W_\omega \cap \mathbb{F}_q^2) \geq q - \delta_r^2 q^{1/2}$.

On the other hand, by the absolute irreducibility of h we conclude that h has no nontrivial common factor with $\partial h/\partial Z_{n-r+1}$. This implies that $W_\omega \cap \widetilde{W}_\omega$ is a zero-dimensional variety. By the Bézout inequality we have $\deg(W_\omega \cap \widetilde{W}_\omega) \leq \delta_r(\delta_r - 1)$, which implies $\#(W_\omega \cap \widetilde{W}_\omega \cap \mathbb{F}_q^2) \leq \delta_r(\delta_r - 1)$. Combining this upper bound with the previous lower bound, we obtain (6.1).

Finally, since $q > 8n^2 d\delta_r^4$ holds, it is easy to see that the right-hand side of (6.1) is a strictly positive real number, which implies that there exists at least one rational point of $W_\omega \setminus \widetilde{W}_\omega$. $\square$

We remark that [9, Corollary 7.4] asserts that for $q > \max\{2(n-r+1)\delta_r^2, 2\delta_r^4\}$ there exists a rational point of V. This is, as far as the authors know, the best existence result known for a *general* absolutely irreducible variety V of fixed dimension and degree. In this sense, Lemma 6.3 gives us an existence result "close" to [9, Corollary 7.4].

Our goal is to find a value $a \in \mathbb{F}_q$ for which there exists a rational point $(W_\omega \setminus \widetilde{W}_\omega) \cap \mathbb{F}_q^2$ of the form (a, z_{n-r+1}). In order to find such value a, we observe that for any $a \in \mathbb{F}_q$ there exist at most δ_r points $(t, z_{n-r+1}) \in W_\omega \setminus \widetilde{W}_\omega$ with $t = a$. Combining this observation with (6.1), we obtain the following estimate:

$$\#\big\{a \in \mathbb{F}_q : (W_\omega \setminus \widetilde{W}_\omega) \cap \mathbb{F}_q^2 \cap \{T = a\} \neq \emptyset\big\} \geq \frac{q - q^{1/2}\delta_r^2 - \delta_r^2}{\delta_r}.$$

From this we immediately deduce the following lower bound on the probability of finding at random a value a for which there exists a rational point with $t = a$:

$$\text{Prob}\big(a \in \mathbb{F}_q : (W_\omega \setminus \widetilde{W}_\omega) \cap \mathbb{F}_q^2 \cap \{T = a\} \neq \emptyset\big) \geq \frac{q - q^{1/2}\delta_r^2 - \delta_r^2}{q\delta_r}. \tag{6.2}$$

Let $q > 8n^2 d\delta_r^4$. Then the probability estimate (6.2) implies that, after at most δ_r random choices, we shall find a value $a \in \mathbb{F}_q$ for which there exists a rational point of $W_\omega \setminus \widetilde{W}_\omega$ of the form (a, z_{n-r+1}) with probability at least $1 - 2q^{-1/2}\delta_r^2 \geq 1 - 1/6$. Having such $a \in \mathbb{F}_q$ and applying, e.g., [57, Corollary 14.16], we see that the computation of $z_{n-r+1} \in \mathbb{F}_q$ can be reduced to gcd computations and factorization in $\mathbb{F}_q[Z_{n-r+1}]$. Our next result describes the algorithm we have just outlined.

Proposition 6.4. *Let $q > 8n^2 d\delta_r^4$. Suppose that we have a geometric solution of the plane curve $\mathcal{C}_\omega$, as provided by Proposition* 6.2*. Then a rational point of $\mathcal{C}_\omega$ can be computed using space $O(\delta_r \log q \log(q\delta))$ and time $O\big(n\delta_r\mathcal{U}(\delta_r)\log q\,\mathcal{U}(\log(q\delta))\big)$. The algorithm outputs the right results with probability at least $1 - 25/144$.*

Proof. For $a \in \mathbb{F}_q$, let $h_a := \gcd\big(h(a, Z_{n-r+1}), Z_{n-r+1}^q - Z_{n-r+1}\big) \in \mathbb{F}_q[Z_{n-r+1}]$. From [57, Corollary 11.16] we have that the computation of h_a can be performed with $O\big(\mathcal{U}(\delta_r)\log q\big)$ operations in $\mathbb{F}_q$, storing $O(\delta_r \log q)$ elements of $\mathbb{F}_q$. Furthermore, deciding whether $h(a, Z_{n-r+1})$ is a squarefree polynomial requires $O\big(\mathcal{U}(\delta_r)\big)$ operations in $\mathbb{F}_q$, storing $O(\delta_r)$ elements of $\mathbb{F}_q$. From the probability estimate (6.2) we see that, after at most δ_r random choices, with probability at least $1 - 1/6$ we shall find a value $a \in \mathbb{F}_q$ such that $h(a, Z_{n-r+1})$ is squarefree and h_a is a nonconstant polynomial of $\mathbb{F}_q[Z_{n-r+1}]$. Therefore, computing such $a \in \mathbb{F}_q$ and the polynomial h_a requires at most $O\big(\delta_r\mathcal{U}(\delta_r)\log q\big)$ operations in $\mathbb{F}_q$, storing $O(\delta_r \log q)$ elements of $\mathbb{F}_q$.

Observe that h_a factors into linear factors in $\mathbb{F}_q[Z_{n-r+1}]$. Therefore, applying [57, Theorem 14.9] we see that the factorization of h_a in $\mathbb{F}_q[Z_{n-r+1}]$ requires

$O(\mathcal{U}(\delta_r)\log q)$ operations in $\mathbb{F}_q$, storing at most $O(\delta_r \log q)$, and outputs the right result with probability at most $1-1/144$. Any root $b \in \mathbb{F}_q$ of h_a yields a rational point (a,b) of $W_\omega \setminus \widetilde{W}_\omega$.

Evaluating the parametrizations of Y_{n-r+k} $(2 \leq k \leq r)$ by the zeros of $q(\omega T + Q, Z_{n-r+1})$ at $T = a$ and $Z_{n-r+1} = b$, we obtain a rational point of $\mathcal{C}_\omega$ (observe that our choice of a assures that such evaluations are well defined). This completes the proof of the proposition. □

Now we can describe the whole algorithm computing a rational point of the input variety $V := V_r$. First, we execute the algorithm underlying Theorem 4.8 in order to obtain a geometric solution of the lifting fiber $V_{P^{(r)}}$. Then we obtain a geometric solution of the lifting fiber V_Q and of the absolutely irreducible $\mathbb{F}_q$-curve $\mathcal{C}_\omega$, applying the algorithms underlying Propositions 5.2 and 6.2. Finally, the algorithm of Proposition 6.4 outputs a rational point of $\mathcal{C}_\omega \subset V$. We summarize the result obtained in the following corollary.

Corollary 6.5. *Let $q > 8n^2 d\delta_r^4$. Suppose that we have a straight-line program using space $\mathcal{S}$ and time $\mathcal{T}$ which represents the input polynomials $F_1, \ldots, F_r$. Then the coordinates of a rational point of the variety $V := V_r$ can be computed using space $O\big((\mathcal{S}+n+d)\delta \log q(\delta + \log(q\delta))\big)$ and time $O\big((n\mathcal{T}+n^5)\mathcal{U}(\delta)\mathcal{U}(d\delta)\log q\,\mathcal{U}(\log(q\delta))\big)$. The algorithm outputs the right result with probability at least $2/3 > 1/2$.*

We remark that our algorithm can be easily extended to the case of an equidimensional $\mathbb{F}_q$-variety V (given by a reduced regular sequence), which has an absolutely irreducible component defined over $\mathbb{F}_q$. Indeed, the algorithm of Theorem 4.8 may be applied in this case, because it only requires the variety V to be equidimensional and to be given by a reduced regular sequence. With a similar argument as in Theorem 3.6 and Proposition 6.2, we obtain a geometric solution of an $\mathbb{F}_q$-curve $\mathcal{C}$, contained in V, with at least one absolutely irreducible component defined over $\mathbb{F}_q$. Then, using fast algorithms for bivariate factorization and absolute irreducibility testing (see, e.g., [32]), we compute such an absolutely irreducible component, to which we apply the algorithm underlying Proposition 6.4. Under the assumption that $q > 8n^2 d\delta_r^4$ holds, the asymptotic complexity and probability estimates of our algorithm in this case are the same as in Corollary 6.5.

Acknowledgments

The authors are grateful to Luis Miguel Pardo for many helpful comments and discussions on the paper. They also thank to an anonymous referee for several useful remarks, which helped considerably to improve the presentation of the results of this paper.

References

[1] M.E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann, *Zeroes, multiplicities and idempotents for zerodimensional systems*, Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94 (Boston), Progr. Math., vol. 143, Birkhäuser, Boston, 1996, pp. 1–15. MR1414442 (97i:13027)

[2] B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop, *Polar varieties and efficient real equation solving: The hypersurface case*, J. Complexity **13** (1997), no. 1, 5–27. MR1449757 (98h:68123)

[3] ———, *Polar varieties and efficient real elimination*, Math. Z. **238** (2001), no. 1, 115–144. MR1860738 (2002g:14084)

[4] B. Bank, M. Giusti, J. Heintz, and L.M. Pardo, *A first approach to generalized polar varieties*, Kybernetika (Prague) **40** (2004), no. 5, 519–550. MR2120995 (2006e:14078)

[5] ———, *Generalized polar varieties: Geometry and algorithms*, J. Complexity **21** (2005), no. 4, 377–412. MR2152713

[6] D. Bini and V. Pan, *Polynomial and matrix computations*, Progress in Theoretical Computer Science, Birkhäuser, Boston, 1994. MR1289412 (95k:65003)

[7] A. Borodin, *Time space tradeoffs (getting closer to the barriers?)*, 4th International Symposium on Algorithms and Computation, ISAAC '93, Hong Kong, December 15-17, 1993 (Berlin), Lecture Notes in Comput. Sci., vol. 762, Springer, 1993, pp. 209–220.

[8] P. Bürgisser, M. Clausen, and M.A. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer, Berlin, 1997. MR1440179 (99c:68002)

[9] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl., **12** (2006), no. 2, 155–185.

[10] 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. MR2009683 (2004k:68056)

[11] A.L. Chistov and D.Y. Grigoriev, *Subexponential time solving systems of algebraic equations. I, II*, LOMI preprints E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[12] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, EUROCRYPT 2000 (Berlin) (B. Preneel, ed.), Lecture Notes in Comput. Sci., vol. 1807, Springer, 2000, pp. 71–79. MR1772028

[13] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, Undergrad. Texts Math., Springer, New York, 1992. MR1189133 (93j:13031)

[14] ———, *Using algebraic geometry*, Grad. Texts in Math., vol. 185, Springer, New York, 1998. MR1639811 (99h:13033)

[15] M. de Boer and R. Pellikaan, *Gröbner bases for codes*, Some tapas in computer algebra (A. Cohen et al., ed.), Algorithms Comput. Math., vol. 4, Springer, Berlin, 1999, pp. 237–259. MR1679927 (2000d:94029a)

[16] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Grad. Texts in Math., vol. 150, Springer, New York, 1995. MR1322960 (97a:13001)

[17] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, ISSAC'02: Proceedings of the International Symposium on Symbolic and Algebraic Computation, Lille, France, July 7–10, 2002 (New York) (T. Mora, ed.), ACM Press, 2002, pp. 75–83. MR2035234 (2005c:13033)

[18] W. Fulton, *Intersection Theory*, Springer, Berlin, Heidelberg, New York, 1984. MR0732620 (85k:14004)

[19] P. Gianni and T. Mora, *Algebraic solution of systems of polynomial equations using Gröbner bases*, Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC–5, Menorca, Spain, June 15–19, 1987 (Berlin) (L. Huguet and A. Poli, eds.), Lecture Notes in Comput. Sci., vol. 356, Springer, 1989, pp. 247–257. MR1008541 (91e:13024)

[20] 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. MR1457843 (99d:68106)

[21] 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. MR1600277 (99d:68128)

[22] M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo, *When polynomial equation systems can be solved fast?*, Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11 (Berlin) (G. Cohen, M. Giusti, and T. Mora, eds.), Lecture Notes in Comput. Sci., vol. 948, Springer, 1995, pp. 205–231. MR1448166 (98a:68106)

[23] ———, *Le rôle des structures de données dans les problèmes d'élimination*, C. R. Math. Acad. Sci. Paris **325** (1997), 1223–1228. MR1490129 (98j:68068)

[24] M. Giusti, J. Heintz, and J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), 56–95. MR1220078 (94i:13016)

[25] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211. MR1817612 (2002b:68123)

[26] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277. MR0716823 (85a:68062)

[27] ———, *On the computational complexity of polynomials and bilinear mappings. A survey*, Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC–5, Menorca, Spain, June 15–19, 1987 (Berlin) (L. Huguet and A. Poli, eds.), Lecture Notes in Comput. Sci., vol. 356, Springer, 1989, pp. 269–300. MR1008524 (90d:94001)

[28] J. Heintz, G. Matera, L.M. Pardo, and R. Wachenchauzer, *The intrinsic complexity of parametric elimination methods*, Electron. J. SADIO **1** (1998), no. 1, 37–51. MR1675449 (2000b:65249)

[29] J. Heintz, G. Matera, and A. Waissbein, *On the time–space complexity of geometric elimination procedures*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 4, 239–296. MR1818975 (2002c:68108)

[30] M.-D. Huang and Y.-C. Wong, *Solvability of systems of polynomial congruences modulo a large prime*, Comput. Complexity **8** (1999), no. 3, 227–257. MR1737238 (2000j:11044)

[31] ———, *Extended Hilbert irreducibility and its applications*, J. Algorithms **37** (2000), no. 1, 121–145. MR1783251 (2001h:12002)

[32] E. Kaltofen, *Effective Noether irreducibility forms and applications*, J. Comput. System Sci. **50** (1995), no. 2, 274–295. MR1330258 (96g:68053)

[33] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE PublicKeyCryptosystem by relinearization*, Proceedings of Advances in Cryptology – CRYPTO'99, Santa Barbara, California, USA, August 15–19, 1999 (Berlin) (M.J. Wiener, ed.), Lecture Notes in Comput. Sci., vol. 1666, Springer, 1999, pp. 19–30. MR1729291 (2000i:94052)

[34] T. Krick and L.M. Pardo, *A computational method for Diophantine approximation*, Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94 (Boston) (L. González-Vega and T. Recio, eds.), Progr. Math., vol. 143, Birkhäuser Boston, 1996, pp. 193–254. MR1414452 (98h:13039)

[35] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math. **92** (1882), 1–122.

[36] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston, 1985. MR0789602 (86e:14001)

[37] G. Lecerf, *Quadratic Newton iteration for systems with multiplicity*, Found. Comput. Math. **2** (2002), no. 3, 247–293. MR1907381 (2003f:65090)

[38] ———, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596. MR1991984 (2004j:68200)

[39] R. Lidl and H. Niederreiter, *Finite fields*, Addison–Wesley, Reading, Massachusetts, 1983. MR0746963 (86c:11106)

[40] R. Lidl and G. Pilz, *Applied abstract algebra*, Undergrad. Texts Math., Springer, New York, 1984. MR0765220 (86d:00002)

[41] F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge Univ. Press, Cambridge, 1916. MR1281612 (95i:13001)

[42] H. Matsumura, *Commutative algebra*, Benjamin, 1980. MR0575344 (82i:13003)

[43] J.E. Morais, *Resolución eficaz de sistemas de ecuaciones polinomiales*, Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1997.

[44] D. Mumford, *Algebraic geometry I. Complex projective varieties*, 2nd ed., Classics Math., Springer, Berlin, 1995. MR1344216 (96d:14001)

[45] L.M. Pardo, *How lower and upper complexity bounds meet in elimination theory*, Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC–11 (Berlin) (G. Cohen, M. Giusti, and T. Mora, eds.), Lecture Notes in Comput. Sci., vol. 948, Springer, 1995, pp. 33–69. MR1448154 (99a:68097)

[46] F. Rouillier, *Solving zero-dimensional systems through rational univariate representation*, Appl. Algebra Engrg. Comm. Comput. **9** (1997), no. 5, 433–461. MR1697179 (2000e:13038)

[47] P. Samuel, *Méthodes d'algèbre abstraite en géométrie algébrique*, Springer, Berlin, Heidelberg, New York, 1967. MR0213347 (35:4211)

[48] J.E. Savage, *Models of computation. Exploring the power of computing*, Addison-Wesley, Reading, Massachussets, 1998.

[49] W. Schmidt, *A lower bound for the number of solutions of equations over finite fields*, J. Number Theory **6** (1974), no. 6, 448–480. MR0360598 (50:13045)

[50] ______, *Equations over finite fields. An elementary approach*, Lectures Notes in Math., no. 536, Springer, New York, 1976. MR0429733 (55:2744)

[51] E. Schost, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), 349–393. MR1959170 (2003k:13035)

[52] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27** (1980), no. 4, 701–717. MR0594695 (82m:68078)

[53] I.R. Shafarevich, *Basic algebraic geometry*, Grad. Texts in Math., Springer, New York, 1984. MR0447223 (56:5538)

[54] ______, *Basic algebraic geometry: Varieties in projective space*, Springer, Berlin, Heidelberg, New York, 1994. MR1328833 (95m:14001)

[55] V. Strassen, *Algebraic complexity theory*, Handbook of Theoretical Computer Science (J. van Leeuwen, ed.), Elsevier, Amsterdam, 1990, pp. 634–671. MR1127177

[56] J. von zur Gathen, *Parallel arithmetic computations: a survey*, Proceedings of the 12th International Symposium on Mathematical Foundations of Computer Science, Bratislava, Czechoslovakia, August 25–29, 1996 (Berlin) (J. Gruska, B. Rovan, and J. Wiedermann, eds.), Lecture Notes in Comput. Sci., vol. 233, Springer, August 1986, pp. 93–112. MR0874591

[57] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999. MR1689167 (2000j:68205)

[58] J. von zur Gathen, M. Karpinski, and I. Shparlinski, *Counting curves and their projections*, Comput. Complexity **6** (1997), no. 3, 64–99. MR1436303 (98d:68111)

[59] J. von zur Gathen, I. Shparlinski, and A. Sinclair, *Finding points on curves over finite fields*, SIAM J. Comput. **32** (2003), no. 6, 1436–1448. MR2034245 (2005b:68293)

[60] A. Weil, *Sur les courbes algébriques et les varietés qui s'en déduisent*, Hermann, Paris, 1948. MR0027151 (10:262c)

[61] O. Zariski, *Algebraic surfaces*, Classics Math., Springer, Berlin, 1995. MR1336146 (96c:14024)

[62] R. Zippel, *Probabilistic algorithms for sparse polynomials*, EUROSAM '79: Proceedings of International Symposium on Symbolic and Algebraic Computation, Marseille 1979 (Berlin), Lecture Notes in Comput. Sci., vol. 72, Springer, 1979, pp. 216–226. MR0575692 (81g:68061)

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I (1428) Buenos Aires, Argentina
E-mail address: acafure@dm.uba.ar

Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (1613) Los Polvorines, Buenos Aires, Argentina; and National Council of Science and Technology (CONICET), Argentina
E-mail address: gmatera@ungs.edu.ar