Deterministic Depth-4 PIT and Normalization

Zeyu Guo* Siki Wang†

Abstract

In this paper, we initiate the study of deterministic PIT for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits over fields of any characteristic, where k and δ are bounded. Our main result is a deterministic polynomial-time black-box PIT algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ circuits, under the additional condition that one of the summands at the top Σ gate is squarefree.

Our techniques are purely algebro-geometric: they do not rely on Sylvester–Gallai-type theorems, and our PIT result holds over arbitrary fields.

The core of our proof is based on the normalization of algebraic varieties. Specifically, we carry out the analysis in the integral closure of a coordinate ring, which enjoys better algebraic properties than the original ring.

1 Introduction

Polynomial Identity Testing (PIT) is the fundamental problem of deciding whether a given multivariate algebraic circuit computes the identically zero polynomial. Equivalently, it asks whether two arithmetic circuits compute the same polynomial, by checking whether their difference is identically zero. Despite its simple formulation, PIT captures a striking *randomized vs. deterministic* dichotomy in complexity theory. On the one hand, it admits an efficient randomized algorithm: by the Schwartz–Zippel Lemma [Sch80, Zip79], evaluating a degree-d polynomial at a random point (or tuple of points) over a sufficiently large field yields a correct identity test with high probability. This leads to a fast Monte Carlo algorithm that treats the circuit as a black box. On the other hand, no efficient deterministic algorithm is known, even when the circuit's structure is fully accessible. In complexity-theoretic terms, PIT lies in the class coRP, but whether it can be solved in P remains a major open question. Closing this gap is widely regarded as a central challenge in theoretical computer science. Indeed, PIT is often viewed as the algebraic analogue of the classic P vs. BPP (or P vs. RP) question.

The importance of PIT lies both in its algorithmic applications and its deep connections to complexity theory. It has been used in a wide range of settings, such as primality testing [AKS04], polynomial factoring [KSS14, BSV20, KRS24, DST24], and perfect matching [Lov79, MVV87, CRS95, FGT21, ST17]. More fundamentally, PIT plays a central role in the *hardness vs. randomness* paradigm, and its derandomization is known to imply long-sought arithmetic circuit lower bounds [HS80, KI04].

Over the past few decades, there have been numerous results on deterministic PIT for various restricted models, including sparse polynomials, depth-3 circuits, low-depth circuits, and arithmetic

*The Ohio State University. Email: zguotcs@gmail.com. Supported by the NSF CAREER award (grant no. CCF-2440926).

†Caltech. Email: siki.wang@caltech.edu

branching programs, among others. See, for example, [LST24, AF22] for recent breakthroughs, including subexponential-time deterministic PIT algorithms for low-depth circuits over fields of characteristic zero or large characteristic. For surveys of earlier developments, see [Sax09, Sax14, SY10]. Nonetheless, despite decades of significant progress, a general polynomial-time deterministic PIT algorithm remains elusive. As such, PIT continues to serve as a central testing ground for our understanding of algebraic structure, pseudorandomness, and computational hardness.

Depth-4 PIT. A major breakthrough by Agrawal and Vinay [AV08] revealed that PIT for depth-4 circuits essentially captures the full complexity of general PIT. Roughly speaking, they showed that any arithmetic circuit of subexponential size can be transformed into a depth-4 circuit of subexponential size. Thus, proving lower bounds for the latter would imply lower bounds for the former. Combined with hardness-vs-randomness connections [NW94, KI04], they further showed that a complete derandomization of depth-4 PIT—even for circuits with slightly unbounded top fan-in and $O(\log n)$ bottom fan-in—would yield a quasi-polynomial-time deterministic PIT algorithm for general circuits. Notably, no analogous reduction is known in the Boolean setting.

This equivalence was unexpected: it elevated depth-4 circuits from a technical intermediate to a canonical class encapsulating the full difficulty of PIT. As a result, depth-4 PIT has become a central focus in the broader derandomization program.

Despite this equivalence, the expressive power of general depth-4 circuits makes deterministic PIT for them highly challenging. This has motivated a refined line of work focused on syntactic subclasses, notably $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits—depth-4 circuits in which the top fan-in is at most k, and the bottom multiplication gates have fan-in at most δ, where k and δ are bounded. The study of deterministic PIT for these circuits has led to the development of new techniques grounded in Sylvester–Gallai-type arguments and tools from algebraic geometry.

1.1 Previous Work

Sylvester–Gallai-based approach. A $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuit consists of a top Σ gate of fan-in at most k, followed by alternating layers of unbounded Π, Σ, and Π gates, where the bottom Π gates have fan-in at most δ. This model naturally generalizes bounded top fan-in depth-3 circuits ($\Sigma^{[k]}\Pi\Sigma$), for which efficient deterministic PIT algorithms are known. Over fields of characteristic zero, Sylvester–Gallai (SG)-type theorems [EK66, BM90] from combinatorial geometry have been used to establish constant-rank bounds on the linear forms in $\Sigma^{[k]}\Pi\Sigma$ circuits, leading to deterministic polynomial-time black-box PIT algorithms [DS07, KS09, SS13].

Gupta [Gup14] conjectured a nonlinear Sylvester–Gallai-type statement which, if true, would yield deterministic polynomial-time black-box PIT algorithms for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits with bounded k and δ over fields of characteristic zero. Motivated by this conjecture, Shpilka proved an SG-type theorem for quadratic polynomials, initiating a substantial line of work [Shp20, PS22, PS21, GOS22, OS22, GOPS23, OS24, GOS25b] aimed at fully resolving the conjecture.

Notably, Peleg and Shpilka [PS21], building on earlier work [Shp20, PS22], proved a quadratic SG-type theorem that yields a deterministic polynomial-time black-box PIT algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits. Subsequent works [OS22, GOPS23, OS24, GOS25b] extended these results and introduced new techniques, including connections to the Stillman uniformity phenomenon and applications of the Cohen–Macaulay property from commutative algebra.

However, SG-based methods remain largely confined to characteristic zero. Kayal and Saxena [KS07] showed that the constant-rank bounds implied by SG-type arguments do not hold in

positive characteristic, even for the simpler $\Sigma^{[k]}\Pi\Sigma$ model.

Other work. Dutta, Dwivedi, and Saxena [DDS21] gave a deterministic quasipolynomial-time black-box PIT algorithm for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits. Due to their use of logarithmic derivatives, the result holds only when the characteristic of the base field is zero or sufficiently large. Their approach reduces the problem to black-box PIT for read-once oblivious arithmetic branching programs (ROABPs). However, obtaining a deterministic polynomial-time black-box PIT algorithm for this class remains open despite extensive effort.

We also mention the recent breakthrough of superpolynomial lower bounds for low-depth circuits by Limaye, Srinivasan, and Tavenas [LST24]. This result, together with the earlier work of Chou, Kumar, and Solomon [CKS18] or the work of Andrews and Forbes [AF22], yields subexponential-time black-box PIT algorithms for low-depth circuits, including $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits. These algorithms also rely on properties that only hold when the characteristic is zero or large. Recently, Forbes [For24] extended the superpolynomial lower bound for low-depth circuits to positive characteristics. However, whether the PIT algorithms themselves can be extended to this setting remains an open question [For24].

In summary, all of the results and approaches mentioned above assume that the characteristic of the base field is zero or sufficiently large. This naturally raises the following question: Is it possible to design a nontrivial, or even polynomial-time, deterministic PIT algorithm for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits over arbitrary fields? We believe the answer is yes. In this work, we make progress toward answering this question affirmatively.

As a reality check, any such result must first address the simpler case of $\Sigma^{[k]}\Pi\Sigma$ circuits. Deterministic polynomial-time algorithms for this class are indeed known in positive characteristics: they were first obtained by Kayal and Saxena in the white-box setting [KS07], and later by Saxena and Seshadhri in the black-box setting [SS12]. Notably, these results do not rely on SG-type theorems or other arguments that require assumptions on the characteristic of the base field. Our work is inspired by these approaches and seeks to extend them to the depth-4 setting.

1.2 Our Results

In this paper, we initiate the study of deterministic PIT for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits over fields of any characteristic. Our main result is a deterministic polynomial-time black-box PIT algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ circuits under the condition that one of the summands at the top Σ gate is squarefree.

Our techniques are purely algebro-geometric. Notably, the proof does not rely on Sylvester–Gallai-type theorems, and the result remains valid even over fields of small positive characteristic.

We begin by stating the homogeneous version of our result.

Theorem 1.1 (Main theorem, homogeneous version)**.** *Let $C_{n,d,k,\delta,\mathbb{F}}$ be the set of polynomials $F \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \ldots, X_n]$ over a field $\mathbb{F}$ satisfying the following conditions:*

(1) F can be expressed as a sum $F = \sum_{i=0}^{k_0-1} F_i$, where $k_0 \le k$, $F_i = \prod_{j=1}^{m_i} f_{i,j}$ for $i \in \{0, 1, \ldots, k_0 - 1\}$, and each $f_{i,j} \in \mathbb{F}[\mathbf{X}]$ is a nonzero homogeneous polynomial of degree at most δ.

(2) $\deg(F_i) = d_0$ for some $d_0 \le d$ and all $i \in \{0, 1, \ldots, k_0 - 1\}$.

(3) There exists $i \in \{0, 1, \ldots, k_0 - 1\}$ such that F_i is squarefree, meaning that the irreducible factors of F_i over $\overline{\mathbb{F}}$ are distinct.

Then there exists an explicit $(nd)^{O_\delta(1)}$-sized hitting set $\mathcal{H} \subseteq \overline{\mathbb{F}}^n$ for $C_{n,d,3,\delta,\mathbb{F}}$. Equivalently, there exists a deterministic black-box PIT algorithm for $C_{n,d,3,\delta,\mathbb{F}}$ that makes at most $(nd)^{O_\delta(1)}$ evaluation queries.

The above homogeneous result easily extends to an analogous statement for inhomogeneous polynomials. We now explain how this extension works.

Let $F = \sum_{i=0}^{k_0-1} F_i \in \mathbb{F}[X_1, \ldots, X_n]$, where $F_0, \ldots, F_{k_0-1}$ are nonzero and possibly inhomogeneous polynomials. Define the homogenization of F with respect to $F_0, \ldots, F_{k_0}$ as

$$\mathrm{H}(F, F_0, \ldots, F_{k_0-1}) := \sum_{i=0}^{k_0-1} F_i(X_1/X_0, \ldots, X_n/X_0) X_0^{d_0}, \quad \text{where } d_0 = \max_{0 \le i \le k_0-1}(\deg(F_i)),$$

which is a homogeneous polynomial living in $\mathbb{F}[X_0, X_1, \ldots, X_n]$.

We now state the inhomogeneous version of our result.

Corollary 1.2 (Main theorem, inhomogeneous version)**.** *Let $C^*_{n,d,k,\delta,\mathbb{F}}$ be the set of polynomials $F \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \ldots, X_n]$ over a field $\mathbb{F}$ that can be written as a sum $F = \sum_{i=0}^{k_0-1} F_i$ for some $k_0 \le k$ such that $\mathrm{H}(F, F_0, \ldots, F_{k_0-1}) \in C_{n,d,k,\delta,\mathbb{F}}$. This includes all those $F = \sum_{i=0}^{k_0-1} F_i$ with $k_0 \le k$ for which the following conditions hold:*

(1) $F_i = \prod_{j=1}^{m_i} f_{i,j}$ for $i \in \{0, 1, \ldots, k_0 - 1\}$, where each $f_{i,j} \in \mathbb{F}[\mathbf{X}]$ is a nonzero polynomial of degree at most δ.

(2) $d_0 := \max_{0 \le i \le k_0-1}(\deg(F_i))$ is at most d.

(3) F_i is squarefree for some $i \in \{0, 1, \ldots, k_0 - 1\}$ satisfying $\deg(F_i) = d_0$, or more generally, satisfying $\deg(F_i) \ge d_0 - 1$.

And there exists an explicit $(nd)^{O_\delta(1)}$-sized hitting set $\mathcal{H} \subseteq \overline{\mathbb{F}}^n$ for $C^*_{n,d,3,\delta,\mathbb{F}}$. Equivalently, there exists a deterministic black-box PIT algorithm for $C^*_{n,d,3,\delta,\mathbb{F}}$ that makes at most $(nd)^{O_\delta(1)}$ evaluation queries.

Proof. Consider $i \in \{0, 1, \ldots, k_0 - 1\}$. Note that

$$F_i(X_1/X_0, \ldots, X_n/X_0) X_0^{d_0} = \left(\prod_{j=1}^{m_i} \left(f_{i,j}(X_1/X_0, \ldots, X_n/X_0) X_0^{\deg(f_{i,j})} \right) \right) X_0^{d_0 - \deg(F_i)}.$$

Here, each factor $f_{i,j}(X_1/X_0, \ldots, X_n/X_0) X_0^{\deg(f_{i,j})}$ is not divisible by X_0. Therefore, if F_i is squarefree and $\deg(F_i) \ge d_0 - 1$, then $F_i(X_1/X_0, \ldots, X_n/X_0) X_0^{d_0}$ is also squarefree. So if $F = \sum_{i=0}^{k_0-1} F_i$ satisfies Item 3 in Corollary 1.2, then $\mathrm{H}(F, F_0, \ldots, F_{k_0-1})$ satisfies Item 3 in Theorem 1.1. It is straightforward to verify that Item 1 and Item 2 in Corollary 1.2 imply the corresponding items in Theorem 1.1 as well.

It remains to construct an explicit $(nd)^{O_\delta(1)}$-sized hitting set $\mathcal{H}^* \subseteq \overline{\mathbb{F}}^n$ for $C^*_{n,d,3,\delta,\mathbb{F}}$. First, by Theorem 1.1, there exists an explicit $(nd)^{O_\delta(1)}$-sized hitting set $\mathcal{H} \subseteq \overline{\mathbb{F}}^{n+1}$ for $C_{n+1,d,3,\delta,\mathbb{F}}$.

Let us first assume that $a_0 \neq 0$ for all $(a_0, \ldots, a_n) \in \mathcal{H}$. Construct the set

$$\mathcal{H}^* = \{(a_1/a_0, \ldots, a_n/a_0) : (a_0, \ldots, a_n) \in \mathcal{H}\}.$$

Consider a nonzero polynomial $F = \sum_{i=0}^{k_0-1} F_i \in C^*_{n,d,3,\delta,\mathbb{F}}$. Then $\mathrm{H}(F, F_0, \ldots, F_{k_0-1})$ is a nonzero polynomial in $C_{n,d,3,\delta,\mathbb{F}}$. Choose $\mathbf{a} = (a_0, \ldots, a_n) \in \mathcal{H}$ such that $\mathrm{H}(F, F_0, \ldots, F_{k_0-1})(\mathbf{a}) \neq 0$. By definition,

$$\mathrm{H}(F, F_0, \ldots, F_{k_0-1})(\mathbf{a}) = \sum_{i=0}^{k_0-1} F_i(a_1/a_0, \ldots, a_n/a_0)a_0^{d_0} = F(a_1/a_0, \ldots, a_n/a_0)a_0^{d_0}.$$

Therefore, $F(a_1/a_0, \ldots, a_n/a_0) = \mathrm{H}(F, F_0, \ldots, F_{k_0-1})(\mathbf{a})a_0^{-d_0} \neq 0$, where $(a_1/a_0, \ldots, a_n/a_0) \in \mathcal{H}^*$ by construction. So $\mathcal{H}^*$ is a hitting set for $C^*_{n,d,3,\delta,\mathbb{F}}$, whose size is at most $|\mathcal{H}| = (nd)^{O_\delta(1)}$.

Finally, we remove the assumption that $a_0 \neq 0$ for all $(a_0, \ldots, a_n) \in \mathcal{H}$. Observe that the class $C_{n+1,d,3,\delta,\mathbb{F}}$ is closed under invertible linear transformations of the coordinates. Therefore, the hitting set property for $C_{n+1,d,3,\delta,\mathbb{F}}$ is preserved under such transformations as well.

We may assume that $\mathbf{0} = (0, \ldots, 0) \notin \mathcal{H}$, since any non-constant homogeneous polynomial always vanishes at $\mathbf{0}$. Hence, every point in $\mathcal{H}$ has at least one nonzero coordinate.

We can deterministically and efficiently find an invertible linear transformation $\phi : \overline{\mathbb{F}}^{n+1} \to \overline{\mathbb{F}}^{n+1}$ such that every point $(a_0, \ldots, a_n) \in \phi(\mathcal{H})$ satisfies $a_0 \neq 0$. We then replace $\mathcal{H}$ by $\phi(\mathcal{H})$ and construct $\mathcal{H}^*$ as before. □

We remark that removing Item 3 from Corollary 1.2 (the squarefreeness condition) recovers the class $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$.

Previously, no polynomial-time deterministic PIT algorithm was known for the classes of polynomials described in Theorem 1.1 and Corollary 1.2, and no subexponential-time algorithm was known over fields of small positive characteristic.

1.3 Proof Overview

To explain our ideas, we begin with a solved case: consider a nonzero polynomial $F \in \Sigma^{[2]}\Pi\Sigma\Pi^{[\delta]}$, i.e., a depth-4 circuit with top fan-in two. In this case, we can write $F = F_1 + F_2 \neq 0$, where F_1 and F_2 are products of nonzero polynomials, each of degree at most δ.

Suppose

$$F_1 = g_1 \cdots g_r \quad \text{and} \quad F_2 = h_1 \cdots h_s \tag{1}$$

are factorizations of F_1 and F_2 into irreducible polynomials, respectively. If $F_2 = cF_1$ for some $c \in \mathbb{F}^\times$, then $F = (c+1)F_1$, which is again a product of degree-$(\leq \delta)$ nonzero polynomials. PIT for such polynomials is straightforward. So assume this is not the case. Then the factorizations in (1) do not "match." That is, there does not exist a bijection $\sigma : [r] \to [s]$ such that g_i and $h_{\sigma(i)}$ are scalar multiples of each other for all $i \in [r]$.

It is natural to choose an affine line ℓ such that restricting to ℓ reduces the ambient dimension while preserving the non-matching structure of the factorizations. In other words, we want $F_1|_\ell$ and $F_2|_\ell$ to still have non-matching factorizations. This ensures that $(F_1 + F_2)|_\ell \neq 0$, reducing the problem to PIT for univariate polynomials, which is easy.

To ensure the factorizations remain non-matching after restriction, it suffices to guarantee that any two coprime polynomials $g, h \in \{g_1, \ldots, g_r, h_1, \ldots, h_s\}$ remain coprime after restricting to ℓ, i.e., they do not share a common root on the line. Geometrically, this amounts to ensuring that ℓ avoids the codimension-two variety $V(g, h)$. In [Guo24], it is shown how to construct a polynomial-sized set of lines such that most lines avoid all such varieties. This effectively (re)solves the problem.

We now move to the class $C_{n,d,3,\delta,\mathbb{F}}$. Let F be a nonzero polynomial in this class. Then we may write

$$F = F_0 + F_1 + F_2,$$

where F_0, F_1, F_2 are homogeneous of the same degree and are products of nonzero homogeneous polynomials, each of degree at most δ. Furthermore, one of the summands, say F_0, is squarefree.

In the study of Boolean circuits, one common technique is applying a restriction (i.e. partial assignment) to simplify the circuit. An analogous idea works here: we restrict F to the zero locus of an irreducible factor θ of F_0 to eliminate F_0. Algebraically, this corresponds to working in the quotient ring $\mathbb{F}[X_1, \ldots, X_n]/(\theta)$, where each F_i is replaced by $\overline{F}_i := F_i \bmod \theta$. Since θ divides F_0, we have $\overline{F}_0 = 0$. Thus, we have effectively reduced to the $k = 2$ case, though now over the quotient ring.

Why can't we directly reuse the $k = 2$ argument? The issue is that $\mathbb{F}[X_1, \ldots, X_n]/(\theta)$ is not, in general, a unique factorization domain (UFD), so the factorizations of $\overline{F}_1$ and $\overline{F}_2$ are not well-defined.

But is unique factorization truly necessary? We argue that it is not: even in the absence of unique factorization, working in rings with the weaker property of *normality* still enables us to obtain meaningful results.

Normality. Let A be an integral domain, whose field of fractions is denoted by $\mathrm{Frac}(A)$. We say A is *integrally closed* if for any monic polynomial $P(X) \in A[X]$, all roots of $P(X)$ in $\mathrm{Frac}(A)$ are in A. An irreducible affine variety is said to be *normal* if its coordinate ring is integrally closed.

It is not easy to give a purely geometric definition of normality. However, its usefulness lies in the fact that, if V is a normal variety with coordinate ring A, then for each codimension-one irreducible subvariety $\mathcal{Z} \subseteq V$, there is a well-behaved "order function" $\mathrm{ord}_{\mathcal{Z}} : \mathrm{Frac}(A) \to \mathbb{Z} \cup \{\infty\}$ indicating the order of zeros or poles of every $g \in \mathrm{Frac}(A)$ along $\mathcal{Z}$. For example, for $A = \mathbb{F}[X, Y]$ and $g = (X + Y)^2/X^3 \in \mathrm{Frac}(A)$, we have $\mathrm{ord}_{V(X+Y)}(g) = 2$ and $\mathrm{ord}_{V(X)}(g) = -3$.

If A is normal, then for $g \in A$, one can define a "generalized factorization" of g, where the "irreducible factors" are not polynomials, but codimension-one irreducible subvarieties $\mathcal{Z}$ of V, each with multiplicity $\mathrm{ord}_{\mathcal{Z}}(g)$. (This is called the Weil divisor associated with g, written additively as $\mathrm{div}(g) := \sum_{\mathcal{Z}} \mathrm{ord}_{\mathcal{Z}}(g) \cdot \mathcal{Z}$.)

With this generalized notion of factorization, one can carry out an argument analogous to (and in fact generalizing) the one for the $k = 2$ case, assuming the variety defined by the factor θ of F_0 is normal.

Thus, normality may be viewed as a useful weakening of unique factorization. In general, however, the variety in question may even fail to be normal. To address this, we apply a standard technique from algebraic geometry known as *normalization*.

Normalization. Conceptually, the normalization of a variety V produces a normal variety $\widetilde{V}$ that best approximates V among all normal varieties. Algebraically, if V is affine, normalization corresponds to taking the integral closure $\widetilde{\mathbb{F}[V]}$ of the coordinate ring $\mathbb{F}[V]$ in its field of fractions. Our key idea is to work within the "nicer" ring $\widetilde{\mathbb{F}[V]}$ in place of $\mathbb{F}[V]$.

The strategy of enlarging a ring to recover a weak form of unique factorization has deep roots in number theory. It began with Kummer's introduction of *ideal numbers* to address the failure of unique factorization in cyclotomic rings, and was later formalized by Dedekind through the theory of *ideals*, recovering unique factorization at the level of ideal decomposition in number rings.

In modern terms, this philosophy is embodied in the process of normalization—passing to the integral closure of a ring in its field of fractions—which yields an integrally closed ring that better approximates a unique factorization domain.

As a concrete example, consider the plane curve C defined by $Y^2 - X^2(X+1) = 0$ (see Fig. 1). The rational function $Z = Y/X$ satisfies the monic polynomial $Z^2 - (X+1)$ on C, but is not a regular function in $\mathbb{F}[C]$, meaning that it is not well-defined on the curve. Geometrically, this reflects the fact that C has two branches at the point $(0,0)$, where the limits of Y/X approach 1 and -1, respectively. Introducing Z as a new coordinate function separates these branches. One can show that X, Y, and Z generate an integrally closed ring in $\mathrm{Frac}(\mathbb{F}[C])$, and that their defining relations are generated by $Y^2 - X^2(X+1)$, $XZ = Y$, and $Z^2 - (X+1)$. These equations define the normalization $\widetilde{C} \subseteq \mathbb{A}^3$.

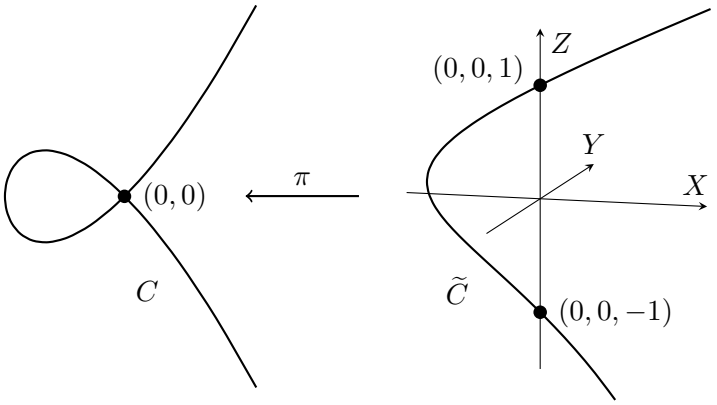

Figure 1: Normalization $\widetilde{C}$ of the curve C defined by $Y^2 - X^2(X+1) = 0$. The map $\pi : \widetilde{C} \to C$ sends $(x, y, z) \mapsto (x, y)$.

This example illustrates why normalization is useful for defining a generalized notion of factorization. On the non-normal curve C, the singular point $(0,0)$ behaves like two overlapping points, with functions like Y/X exhibiting distinct limiting behavior along each branch. After normalization, these branches are separated into two points, $p_1 = (0,0,1)$ and $p_2 = (0,0,-1)$, each admitting a well-behaved order function $\mathrm{ord}_{p_i}(\cdot)$.

A knowledgeable reader may recognize the above example as the resolution of singularities of C. Indeed, the singular locus of a normal variety is known to have codimension at least two. For curves, which have dimension one, normalization therefore coincides with resolution of singularities.

In higher dimensions, by contrast, resolution of singularities is highly complex in characteristic zero [Hir64a, Hir64b], and remains an open problem in positive characteristic. Normalization, on the other hand, is significantly more tractable. A classical theorem of Emmy Noether shows that the integral closure of a coordinate ring $\mathbb{F}[V]$ is finitely generated as a module over $\mathbb{F}[V]$ (see, e.g., [Eis95]).

Constructive normalization has also been extensively studied; see [Sto68, Sei70, Sei75, Tra84, dJ98]. In this paper, we only require normalization for curves, and we follow the framework of Trager [Tra84] to perform this task.

That said, normalization is generally regarded as a computationally expensive problem, often requiring tools such as Gröbner bases. In the context of Geometric Complexity Theory, a key challenge is the non-normality of certain orbit closures related to the determinant and permanent,

a fact established by Kumar [Kum13]. In that setting, the potential utility of normalization remains unclear due to its high complexity.

In our setting, however, this complexity is not a barrier. We apply a dimensionality reduction technique that restricts the input to a carefully chosen constant-dimensional subspace (specifically, a plane). Consequently, all relevant parameters become constant. As a result, even though normalization may be expensive in general, its cost is constant for us and poses no obstacle to obtaining deterministic polynomial-time PIT algorithms.

Dimensionality reduction. We reduce the dimension of the ambient space by restricting to a constant-dimensional subspace (specifically, a plane) while preserving all the structural properties required for our analysis. This naturally raises the question: How should one choose such a plane?

It is not hard to show that a randomly chosen plane will work with high probability. However, using randomness would contradict the goal of this work: derandomization. Instead, we restrict to a *generic plane*. That is, we treat the parameters defining the plane as indeterminates $\mathbf{Y} = (Y_1, \ldots, Y_\ell)$, where $\ell = \Theta(n)$, and work over the function field $\mathbb{F}(\mathbf{Y})$ in place of the original base field $\mathbb{F}$. The analysis is carried out symbolically over this function field, and we eventually specialize $\mathbf{Y}$ to a tuple $\mathbf{a} \in \mathbb{F}$.

This specialization step is constructive. We identify a small collection of polynomials $Q_1, \ldots, Q_m$ in the ring $\mathbb{F}[\mathbf{Y}]$, each of *bounded degree*, such that any assignment $\mathbf{Y} \leftarrow \mathbf{a}$ satisfying $Q_i(\mathbf{a}) \neq 0$ for all i ensures that the chosen plane preserves the desired properties. Verifying such an assignment reduces to testing whether each Q_i is nonzero at $\mathbf{a}$, which is a bounded-degree PIT problem and can be solved deterministically in polynomial time [KS01].

Such generic-to-specific arguments are common in algebraic complexity. Notably, they appear in Kaltofen's work on multivariate polynomial factorization [Kal95] (see also [KSS14]), and in Sylvester–Gallai-based approaches to PIT for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits, e.g., [Gup14]. The general philosophy—prove that a generic geometric object satisfies a given property, and then deduce that the property holds for a dense open set of specific instances—is also a standard principle in algebraic geometry.

Carrying out this analysis introduces several technical challenges, which we address in this paper. First, the function field $\mathbb{F}(\mathbf{Y})$ is not algebraically closed, so arguments must be written more carefully and sometimes more abstractly. Second, we need to compute Gröbner bases over $\mathbb{F}(\mathbf{Y})$. While degree bounds on the polynomials in a Gröbner basis are well-known [MM82, Dub90], we additionally require bounds on the *coefficient complexity*. Specifically, we need to bound the degrees of numerators and denominators of the rational functions in $\mathbb{F}(\mathbf{Y})$ that appear as coefficients. Since such bounds are not readily available in the literature, we establish them ourselves. These bounds may be of independent interest for other problems concerning algebraic pseudorandomness.

Third, although we may assume that $\mathbb{F}$ is a *perfect field* by passing to its algebraic closure, the function field $\mathbb{F}(\mathbf{Y})$ itself may be non-perfect. In particular, in characteristic $p > 0$, field extensions over $\mathbb{F}(\mathbf{Y})$ may be inseparable, complicating tasks such as computing radicals or primary decompositions. To address this, we adjoin p^e-th roots of the variables $\mathbf{Y}$ for sufficiently large e, thereby passing to the extended function field $\mathbb{F}(\mathbf{Y}^{1/p^e}) := \mathbb{F}(Y_1^{1/p^e}, \ldots, Y_\ell^{1/p^e})$, over which the extensions become separable.

Organization of this paper. We begin with preliminaries in Section 2. In Section 3, we develop computational tools, with a focus on Gröbner bases. Section 4 is devoted to the normalization

of curves. Finally, in Section 5, we bring all components together to prove our main theorem (Theorem 1.1).

2 Preliminaries

Denote by $[n]$ the set $\{1, 2, \ldots, n\}$. For a polynomial f and a monomial m, let $\mathrm{coeff}_f(m)$ denote the coefficient of m in f. For polynomials f and $g \neq 0$, we write $g \mid f$ to indicate that g divides f.

It is well-known that designing deterministic black-box PIT algorithms is equivalent to constructing explicit hitting sets. We now define this notion formally.

Definition 2.1 (Hitting set)**.** *A finite collection $\mathcal{H} \subseteq \mathbb{F}^n$ of points is said to be a* hitting set *for a polynomial $f \in \mathbb{F}[X_1, \ldots, X_n]$ if either $f = 0$ or $f(\mathbf{a}) \neq 0$ for some $\mathbf{a} \in \mathcal{H}$. For a family $\mathcal{C} \subseteq \mathbb{F}[X_1, \ldots, X_n]$ of polynomials, we say $\mathcal{H} \subseteq \mathbb{F}^n$ is a hitting set for $\mathcal{C}$ if it is a hitting set for every $f \in \mathcal{C}$.*

Let $\varepsilon \in [0, 1]$. We say $\mathcal{H} \subseteq \mathbb{F}^n$ is an ε-hitting set *for $f \in \mathbb{F}[X_1, \ldots, X_n]$ if either $f = 0$ or $\Pr_{\mathbf{a} \in \mathcal{H}}[f(\mathbf{a}) \neq 0] \geq 1 - \varepsilon$. We say $\mathcal{H}$ is an ε-hitting set for $\mathcal{C}$ if it is an ε-hitting set for every $f \in \mathcal{C}$.*

We focus on constructing explicit hitting sets, although the stronger notion of ε-hitting sets will also be used. Given a hitting set $\mathcal{H}$, one can boost it to an ε-hitting set as follows: Interpolate a degree-$(|\mathcal{H}| - 1)$ curve C that passes through all points in $\mathcal{H}$, and then choose sufficiently many points on C. It can be shown that the resulting set of points is an ε-hitting set.

2.1 Commutative Algebra

All rings are assumed to be commutative with unity. The algebraic closure of a field $\mathbb{F}$ is denoted by $\overline{\mathbb{F}}$.

A matrix over a ring A is denoted by $A^{n \times m}$, or more generally by $A^{S \times T}$, where S and T are the index sets for rows and columns, respectively. We often use $A[i, j]$ to denote the (i, j)-th entry of A.

The ideal of a ring A generated by a set $S \subseteq A$ is denoted $\langle S \rangle$. And the ideal of A generated by $f_1, \ldots, f_k \in A$ is denoted $\langle f_1, \ldots, f_k \rangle$.

Prime, maximal, and radical ideals. An ideal $\mathfrak{p}$ of a ring A is a *prime ideal* if $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Equivalently, $\mathfrak{p}$ is prime if $A/\mathfrak{p}$ is an integral domain.

An ideal $\mathfrak{p}$ of A is a *maximal ideal* if it is maximal among all ideals properly contained in A. Equivalently, $\mathfrak{p}$ is maximal if $A/\mathfrak{p}$ is a field. All maximal ideals are prime.

For an ideal $\mathfrak{p}$ of A, the *radical* of A is the ideal $\sqrt{\mathfrak{p}} := \{a \in A : a^k \in \mathfrak{p} \text{ for some } k \geq 1\}$. An ideal $\mathfrak{p}$ is *radical* if $\mathfrak{p} = \sqrt{\mathfrak{p}}$. Prime ideals and maximal ideals are both radical.

Absolute irreducibility. A polynomial $f \in \mathbb{F}[\mathbf{X}]$ is *absolutely irreducible* over $\mathbb{F}$ if it is irreducible over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. This is equivalent to f being irreducible over every algebraic extension of $\mathbb{F}$. By convention, the zero polynomial is not considered irreducible.

Separability. A polynomial $f(X) \in \mathbb{F}[X]$ is said to be *separable* over $\mathbb{F}$ if its roots are distinct in the algebraic closure of $\mathbb{F}$. This is equivalent to the statement that $f(X)$ and its derivative $f'(X)$ are coprime. An algebraic element over $\mathbb{F}$ is said to be separable over $\mathbb{F}$ if its minimal polynomial over $\mathbb{F}$ is separable. The set of separable elements in an algebraic extension $\mathbb{K}/\mathbb{F}$ form a subfield of $\mathbb{K}$ containing $\mathbb{F}$, called the *separable closure* of $\mathbb{F}$ in $\mathbb{K}$. An algebraic extension $\mathbb{K}/\mathbb{F}$ is separable if the separable closure of $\mathbb{F}$ in $\mathbb{K}$ equals $\mathbb{K}$. Otherwise, it is inseparable.

A field $\mathbb{F}$ is *perfect* if every irreducible polynomial over $\mathbb{F}$ is separable. Examples of perfect fields include fields of characteristic zero, finite fields, and algebraically closed fields.

An irreducible polynomial can be inseparable over non-perfect fields, which must have positive characteristics. We will need the following lemma to address this issue.

Lemma 2.2. *Suppose $\mathbb{F}$ is a field of characteristic $p > 0$, and $\mathbb{K}/\mathbb{F}$ is a finite extension. Let $e \geq 0$ be the largest integer such that p^e divides $[\mathbb{K} : \mathbb{F}]$. For $i \geq 0$, let $\mathbb{F}^{(i)}$ be the field $\{a^{1/p^i} : a \in \mathbb{F}\}$. Then for $e' \geq e$, every $b \in \mathbb{K}$ is separable over $\mathbb{F}^{(e')}$.*

Proof. Let $b \in \mathbb{K}$, and let $f(X)$ be its minimal polynomial over $\mathbb{F}$. Then there exists $e_0 \leq e'$ such that over $\mathbb{F}^{(e_0)}$, we may write

$$f(X) = g(X)^{p^{e_0}},$$

such that $g \in \mathbb{F}^{(e_0)}[X]$ has a monomial whose degree is not divisible by p. In particular, the derivative g' of g is nonzero. It suffices to show that b is separable over $\mathbb{F}^{(e_0)}$. Since b is a root of g, and $g' \neq 0$, it remains only to show that g is irreducible over $\mathbb{F}^{(e_0)}$.

Assume, for contradiction, that $g(X) = u(X)v(X)$ for some nonconstant $u(X), v(X) \in \mathbb{F}^{(e_0)}[X]$. Then f factors over $\mathbb{F}$ as $f(X) = U(X)V(X)$ where $U(X) = u(X)^{p^{e_0}}$ and $V(X) = v(X)^{p^{e_0}}$, contradicting the irreducibility of f over $\mathbb{F}$. □

Localization. Localization is a construction in algebra that allows us to formally invert a chosen set of elements in a ring, effectively turning them into units. For example, $\mathbb{Q}$ is a localization of $\mathbb{Z}$, where every nonzero integer has been made invertible. We now give the formal definition.

Definition 2.3 (Localization)**.** *Let M be a module over a ring A. Let S be a* multiplicative closed subset *of A, i.e, it holds that $1 \in S$ and $ab \in S$ for $a, b \in S$. Define $S^{-1}M$ to be the set of representations of pairs $(a, s) \in M \times S$ subject to the equivalence relation*

$$(a, s) \equiv (b, t) \quad \iff \quad (at - bs)u = 0 \text{ for some } u \in S.$$

Write a/s or $\frac{a}{s}$ for (a, s). Call $S^{-1}M$ the localization *of M with respect to S.*

$S^{-1}A$ is a ring equipped with addition $(a/s) + (b/t) = (at + bs)/(st)$ and multiplication $(a/s) \cdot (b/t) = (ab)/(st)$. And $S^{-1}M$ is an $S^{-1}A$-module equipped with addition $(a/s) + (b/t) = (at + bs)/(st)$ and scalar multiplication $(a/s) \cdot (b/t) = (ab)/(st)$.

Intuitively, $S^{-1}A$ is the ring obtained from A by making the elements in S invertible. Note that if $0 \notin S$ and A is an integral domain, the condition that $(at - bs)u = 0$ for some $u \in S$ in Definition 2.3 is equivalent to $at - bs = 0$ since A does not have a nonzero zero-divisor.

Definition 2.4. *When $S = \{1, f, f^2, \dots\}$ for some $f \in A$, denote $S^{-1}M$ by M_f. When $S = A \setminus \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of A, denote $S^{-1}M$ by $M_\mathfrak{p}$. When A is an integral domain and $\mathfrak{p}$ is the zero ideal of A, denote $A_\mathfrak{p}$ by* Frac(A)*, called the* field of fractions *of A.*

We also have the following fact. See, e.g., [Mag] for a proof.

Fact 2.5. *Let A be a ring and $f \in A$. Then A_f is isomorphic to $A[X]/\langle Xf-1\rangle$ via the map that sends a/f^i to $aX^i + \langle Xf-1\rangle$ for $a \in A$ and $i \in \mathbb{N}$, with the inverse map sending $X + \langle Xf-1\rangle$ to $1/f$.*

Local rings. A ring A is *local* if it has a unique maximal ideal $\mathfrak{m}$. For a ring A and a prime ideal $\mathfrak{p}$ of A, the ring $A_\mathfrak{p}$ (see Definition 2.4) is a local ring with the unique maximal ideal $\mathfrak{p}_\mathfrak{p}$.

The following statement is well-known.

Lemma 2.6 ([Mat89, Theorem 4.7])**.** *Let A be an integral domain. Then*

$$A = \bigcap_{\text{prime ideal } \mathfrak{p}\subseteq A} A_\mathfrak{p} = \bigcap_{\text{maximal ideal } \mathfrak{m}\subseteq A} A_\mathfrak{m},$$

where the intersections are taken within $\mathrm{Frac}(A)$.

Krull dimension. The *(Krull) dimension* of a ring A, denoted by $\dim A$, is the length ℓ of the longest chain of prime ideals $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_\ell$ of A.

If A is a finitely generated integral domain over a field $\mathbb{K}$, then $\dim A$ equals the transcendence degree of $\mathrm{Frac}(A)$ over $\mathbb{K}$. Under the same assumption, $\dim A = \dim A_\mathfrak{m}$ holds for every maximal ideal $\mathfrak{m}$ of A [AM69, Corollary 11.27].

We say an ideal I of a ring A has dimension k if $\dim(A/I) = k$.

Integrality and finiteness. Let $A \subseteq B$ be commutative rings. We say $b \in B$ is *integral* over A if there exists a monic polynomial $f(X) \in A[X]$ such that $f(b) = 0$. We say B is integral over A if every $b \in B$ is integral over A. The set of elements in B integral over A is called the *integral closure* of A in B, and is a ring [AM69]. The integral closure of an integral domain A in its field of fractions $\mathrm{Frac}(A)$ is simply called the integral closure of A, and denoted $\widetilde{A}$.

Lemma 2.7. *Suppose C is integral over B, and B is integral over A. Then C is integral over A.*

Corollary 2.8. *Suppose $A \subseteq B \subseteq C$ are commutative rings and B is integral over A. Then $c \in C$ is integral over A if and only if it is integral over B. In other words, the integral closure of A in C equals the integral closure of B in C.*

Proof. Suppose c is integral over A. Then as $A \subseteq B$, by definition, c is also integral over B.

To see the converse, let C^* be the integral closure of B in C. Suppose c is integral over B, i.e., $c \in C^*$. As C^* is integral over B and B is integral over A, by Lemma 2.7, C^* is integral over A. So c is integral over A. □

A module or algebra M over a ring B is said to be *finite* over B if M is a finitely generated B-module. Finiteness is closely related to integrality, as indicated by the following lemma.

Lemma 2.9 ([AM69, Proposition 5.1 and Corollary 5.2])**.** *A finitely generated algebra over a ring B is a finite module over B iff it is integral over B.*

We also include the following lemma.

Lemma 2.10 ([AM69, Proposition 5.13])**.** *Let A be an integral domain. The following are equivalent:*

(1) A is integrally closed.

(2) $A_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$ of A.

(3) $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A.

Regular local rings. Let A be a local ring with the maximal ideal $\mathfrak{m}$. Use $\dim_k \mathfrak{m}/\mathfrak{m}^2$ to denote the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $k = A/\mathfrak{m}$. We say a local ring A is *regular* if its Krull dimension $\dim A$ equals $\dim_k \mathfrak{m}/\mathfrak{m}^2$.

Discrete valuation rings. A *discrete valuation* on a field K is a mapping $v : K^\times \to \mathbb{Z} \cup \{\infty\}$ satisfying the conditions:

(1) $v(xy) = v(x) + v(y)$,

(2) $v(x + y) \geq \min(v(x), v(y))$, and

(3) $v(x) = \infty \iff x = 0$.

for all $x, y \in K$. We say a discrete valuation v is *normalized* if $v(K^\times) = \mathbb{Z}$.

Given a discrete valuation $v : K^\times \to \mathbb{Z} \cup \{\infty\}$, the *valuation ring* of v is defined to be $\{x \in K : v(x) \geq 0\}$. An integral domain A is a *discrete valuation ring* if there is a discrete valuation v on $\mathrm{Frac}(A)$ such that A is the valuation ring of v.

We include the following useful characterizations of discrete valuation rings.

Lemma 2.11 ([AM69, Proposition 9.2])**.** *Let A be a Noetherian[1] local domain of dimension one with the maximal ideal $\mathfrak{m}$. Then the following are equivalent:*

(1) A is a discrete valuation ring;

(2) A is integrally closed;

(3) A is a regular local ring;

(4) $\mathfrak{m}$ is a principal ideal;

(5) There exists $t \in A$ such that every nonzero ideal of A is of the form $\left\langle t^k \right\rangle$ for some $k \geq 0$.

We call such t a *uniformizer*. Given a uniformizer $t \in A$, every element $r \in A$ can be written as $r = t^k u$ where u is invertible; the (normalized) valuation v on A is determined by $v(t^k u) = k$.

Valuation at a point. Let A be a (Noetherian) integrally closed domain of dimension one, not necessarily local. Let $\mathfrak{m}$ be a maximal ideal of A. By Lemma 2.10, the localization $A_{\mathfrak{m}}$ is an integrally closed local domain of dimension one. So by Lemma 2.11, it is also a regular local ring and a discrete valuation ring. We often denote the corresponding (normalized) discrete valuation by $\mathrm{ord}_{\mathfrak{m}}(\cdot)$.

From a geometric point of view, the maximal ideal $\mathfrak{m}$ corresponds to a point p, and $\mathrm{ord}_{\mathfrak{m}}(f)$ indicates the order of zero or pole of f at p. If $\mathrm{ord}_{\mathfrak{m}}(f) \geq 0$, then $\mathrm{ord}_{\mathfrak{m}}(f)$ is the order of zero of f at p; otherwise, $-\mathrm{ord}_{\mathfrak{m}}(f)$ is the order of the pole of f at p.

[1] A ring A is Noetherian if every ideal of A is finitely generated. All rings considered in this paper are Noetherian.

Base change. Let A be a ring. For an A-module M and an A-algebra B, their tensor product $M \otimes_A B$ over A is defined to be the A-module generated by the set of elements $\{a \otimes b : a \in M, b \in B\}$ subject to the A-bilinear relations $a \otimes b + a' \otimes b = (a + a') \otimes b$, $a \otimes b + a \otimes b' = a \otimes (b + b')$, and $c(a \otimes b) = (ca) \otimes b = a \otimes (cb)$ for $a, a' \in M$, $b, b' \in B$, and $c \in A$. The A-module $M \otimes_A B$ is also a B-module. Furthermore, if M is an A-algebra, then $M \otimes_A B$ is a B-algebra.

Intuitively, $M \otimes_A B$ is obtained from M by changing the ring of scalars from A to B. For example, if M is an A-algebra $A[X_1, \ldots, X_n]/\langle r_1, \ldots, r_m \rangle$ and $A \to B$ is a ring extension, then $M \otimes_A B$ is simply $B[X_1, \ldots, X_n]/\langle r_1, \ldots, r_m \rangle$.

Noether normalization. The Noether normalization lemma is an important lemma in commutative algebra. Roughly speaking, it states that a finitely generated algebra R over a field is not too far from a polynomial ring, in the sense that R is a finite module over a subring that is isomorphic to a polynomial ring.

Lemma 2.12 (Noether normalization lemma)**.** *Let $\mathbb{K}/\mathbb{F}$ be a field extension. Let I be an ideal of $A = \mathbb{K}[X_1, \ldots, X_n]$ such that the Krull dimension of A/I is k. Then for almost all*[2] *$\mathbf{c} = (c_{1,1}, \ldots, c_{k,n}) \in \mathbb{F}^{kn}$, it holds that that:*

(1) the elements $a_1, \ldots, a_k \in A/I$ defined by $a_i = (\sum_{j=1}^{n} c_{i,j} X_j) + I$ are algebraically independent over $\mathbb{K}$, and

(2) A/I is finite over $\mathbb{K}[a_1, \ldots, a_k]$.

In pariticular, such a vector $\mathbf{c}$ exists if $\mathbb{F}$ is infinite.

See, e.g., [GVJZ23, Lemma 4.8] and its proof.

2.2 Algebraic Geometry

Let $\mathbb{F}$ be a field. We use $\mathbb{A}^n_{\mathbb{F}}$ (or simply $\mathbb{A}^n$) to denote the affine n-space over $\mathbb{F}$, and $\mathbb{P}^n_{\mathbb{F}}$ (or simply $\mathbb{P}^n$) to denote the projective n-space over $\mathbb{F}$. Since $\mathbb{F}$ is not necessarily algebraically closed, affine and projective spaces over $\mathbb{F}$—as well as varieties defined over $\mathbb{F}$ within them—must be carefully formalized, rather than viewed simply as sets of solutions. We refer the reader to [Mum88] and [Vak24] for formal definitions of these objects.

An affine variety V over a field $\mathbb{F}$ is equipped with a ring $\mathbb{F}[V]$, called the *coordinate ring* of V. The elements of $\mathbb{F}[V]$ are called *regular functions* on V. Intuitively, these are algebraic functions that are well-defined on all of V. For example, the coordinate ring of $\mathbb{A}^n_{\mathbb{F}}$ is simply $\mathbb{F}[X_1, \ldots, X_n]$.

The (closed) points of V correspond bijectively to the maximal ideals of $\mathbb{F}[V]$. For a point $p \in V$, the set of regular functions vanishing at p is precisely the maximal ideal corresponding to p.

Any radical ideal I of $\mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \ldots, X_n]$ defines an affine variety in $\mathbb{A}^n_{\mathbb{F}}$, which we denote by $V(I)$. The coordinate ring of $V(I)$ is simply $\mathbb{F}[\mathbf{X}]/I$. A regular function f on $\mathbb{A}^n_{\mathbb{F}}$ can be restricted to the variety $V(I)$, yielding the regular function $f|_{V(I)} := f + I \in \mathbb{F}[\mathbf{X}]/I$ on $V(I)$.

Define $V(S) := V(\sqrt{\langle S \rangle})$ for a set S and $V(f_1, \ldots, f_k) := V(\sqrt{\langle f_1, \ldots, f_k \rangle})$ for $f_1, \ldots, f_k \in \mathbb{F}[\mathbf{X}]$. Affine varieties of the form $V(f)$ with a single polynomial f are called (affine) hypersurfaces.

[2] "Almost all" here means that there exists a nonzero polynomial $Q \in \overline{\mathbb{F}}[X_{1,1}, \ldots, X_{k,n}]$ such that the claim holds for all $\mathbf{c} \in \mathbb{F}^{kn}$ satisfying $Q(\mathbf{c}) \neq 0$.

A projective space $\mathbb{P}^n_{\mathbb{F}}$ has $n+1$ homogeneous coordinates $X_0, \ldots, X_n$. A projective variety in $\mathbb{P}^n_{\mathbb{F}}$ is defined by a set of homogeneous polynomials in $\mathbb{F}[X_0, \ldots, X_n]$. If the variety is defined by a single homogeneous polynomial, it is called a *(projective) hypersurface*.

The space $\mathbb{P}^n_{\mathbb{F}}$ can be covered by $n+1$ standard affine open subsets $U_0, \ldots, U_n$, where U_i is defined as the complement of the projective hyperplane defined by $X_i = 0$, and each U_i is isomorphic to $\mathbb{A}^n_{\mathbb{F}}$. The coordinate ring of U_i is $\mathbb{F}\left[\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right]$. More generally, a projective variety $V \subseteq \mathbb{P}^n_{\mathbb{F}}$ can be covered by the affine varieties $U_0 \cap V, \ldots, U_n \cap V$.

A *rational function* on $\mathbb{P}^n_{\mathbb{F}}$ is an expression of the form $F = \frac{P}{Q}$, where P and Q are homogeneous polynomials of the same degree in $X_0, \ldots, X_n$, with $Q \neq 0$. Such a function can be restricted to the affine chart U_i by substituting $X_j \mapsto \frac{X_j}{X_i}$ for all $j = 0, \ldots, n$, which yields a rational function on $U_i \cong \mathbb{A}^n_{\mathbb{F}}$.

Irreducibility. An (affine or projective) variety is said to be *irreducible* if it cannot be written as the union of two proper closed subvarieties. Otherwise, it is *reducible*. Every variety V can be uniquely expressed as a finite union of maximal irreducible subvarieties, called the *irreducible components* of V.

Suppose V is an irreducible affine variety. Then $\mathbb{F}[V]$ is an integral domain. In this case, the field of fractions $\mathrm{Frac}(\mathbb{F}[V])$ is called the *function field* of V, and is denoted by $\mathbb{F}(V)$.

Given an irreducible projective variety $V \subseteq \mathbb{P}^n_{\mathbb{F}}$, we can restrict a rational function $F = \frac{P}{Q}$ on $\mathbb{P}^n_{\mathbb{F}}$ to V, provided that Q does not vanish identically on V. In fact, such a restriction can be computed locally on any nonempty open subset of V, such as $V \cap U_i$ for some i [Vak24, Exercise 5.2.I].

Let $p \in V$ correspond to a maximal ideal $\mathfrak{m} \subset \mathbb{F}[V]$. A rational function $f \in \mathbb{F}(V)$ is said to be *regular at* p if f lies in the local ring $\mathbb{F}[V]_{\mathfrak{m}}$. Intuitively, this means f is well-defined at (and near) the point p.

Indeed, we can evaluate $f \in \mathbb{F}[V]_{\mathfrak{m}}$ at p via the natural quotient map

$$f \mapsto f + \mathfrak{m}_{\mathfrak{m}} \in \kappa_{\mathfrak{m}} := \mathbb{F}[V]_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} \cong \mathbb{F}[V]/\mathfrak{m}.$$

This value lies in the field $\kappa_{\mathfrak{m}}$, called the *residue field* of the point p (or of the ideal $\mathfrak{m}$). It is a finite field extension of $\mathbb{F}$.

Normality. An irreducible affine variety is said to be *normal* if its coordinate ring is an integrally closed domain.[3] An irreducible projective variety $V \subseteq \mathbb{P}^n_{\mathbb{F}}$ is normal if each of the affine pieces $V \cap U_0, \ldots, V \cap U_n$ is a normal affine variety.

Dimension. Let V be an (affine or projective) variety over an algebraically closed field $\mathbb{F}$. The *dimension* of V, denoted $\dim V$, is the largest integer d such that there exists a chain of irreducible closed subvarieties $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_d \subseteq V$, where each Z_i is a proper irreducible subvariety of Z_{i+1}. In other words, the dimension of V is the length of the longest strictly increasing chain of irreducible closed subsets in V.

If V is a variety over a field $\mathbb{F}$ that is not algebraically closed, its dimension is defined as $\dim V := \dim V_{\overline{\mathbb{F}}}$, where $V_{\overline{\mathbb{F}}}$ denotes the base change of V to the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$.

[3] More generally, a (possibly reducible) affine variety is normal if its coordinate ring is a finite product of integrally closed domains [Sta25, Tag 030C].

In the case of an affine variety $V \subseteq \mathbb{A}^n_{\mathbb{F}}$, the dimension of V coincides with the Krull dimension of its coordinate ring $\mathbb{F}[V]$.

Varieties of dimension one are called curves.

Degree. Suppose $V \subseteq \mathbb{A}^n_{\mathbb{F}}$ is an affine variety over an algebraically closed field $\mathbb{F}$. The *degree* of V, denoted $\deg(V)$, is defined as the number of isolated points in the intersection of V with a general affine linear subspace of codimension d, where $d = \dim V$.

Now suppose $V \subseteq \mathbb{P}^n_{\mathbb{F}}$ is a projective variety over an algebraically closed field $\mathbb{F}$. The degree of V is defined as the number of points in the intersection of V with a general linear subspace $L \subseteq \mathbb{P}^n_{\mathbb{F}}$ of codimension d, where $d = \dim V$.

If $\mathbb{F}$ is not algebraically closed, we define $\deg(V) := \deg(V_{\overline{\mathbb{F}}})$, where $V_{\overline{\mathbb{F}}}$ denotes the base change of V to the algebraic closure $\overline{\mathbb{F}}$.[4]

It can be shown that the degree of a point p (corresponding to a maximal ideal $\mathfrak{m}$) equals the degree of its residue field extension, that is, $[\kappa_{\mathfrak{m}} : \mathbb{F}]$.

Bézout's inequality. We need the following version of Bézout's inequality.

Lemma 2.13 (Bézout's inequality [HS80, Hei83])**.** *Let V and V' be closed affine subvarieties of $\mathbb{A}^n_{\mathbb{F}}$. Then $\deg(V) \cap \deg(V') \leq \deg(V) \cdot \deg(V')$.*

The following statement follows from [BM93, Proposition 3.5].

Lemma 2.14. *Let $I = \langle f_1, \ldots, f_k \rangle$ be a zero-dimensional ideal of $\mathbb{F}[X_1, \ldots, X_n]$, and let $d = \max(\deg(f_1), \ldots, \deg(f_k))$. Then $\dim_{\mathbb{F}}(\mathbb{F}[\mathbf{X}]/I) \leq d^n$. In particular, $[\kappa_{\mathfrak{m}} : \mathbb{F}] \leq d^n$ for any maximal ideal $\mathfrak{m}$ containing I.*

3 Computational Tools

In this section, we develop various computational tools, with a focus on Gröbner bases, and establish bounds of the form $O_{s_1,\ldots,s_r}(1)$, where $s_1, \ldots, s_r$ are parameters. While such bounds obscure the specific dependence on $s_1, \ldots, s_r$, they suffice for our purposes, as these parameters will be treated as constants in our application. Although it is theoretically possible to make these bounds explicit, doing so would be tedious and distracting, as it involves repeated composition of intermediate results.

That said, one can verify that all bounds in this section are at most constant-height towers of exponentials in the degrees and the number of variables. In most cases, the bounds are at least doubly exponential due to the use of Gröbner bases. As mentioned, this is acceptable since the degrees and number of variables will eventually be fixed constants depending only on the bottom fan-in δ.

Throughout this section, let $\mathbb{K} = \mathbb{F}(\mathbf{Y}) = \mathbb{F}(Y_1, \ldots, Y_\ell)$, where $\mathbb{F}$ is an infinite field.

We define the following complexity measures on rational functions in $\mathbb{F}(\mathbf{Y})$ and polynomials over $\mathbb{F}(\mathbf{Y})$.

[4] The base change $V_{\overline{\mathbb{F}}}$ is not necessarily a variety and must be interpreted as a *scheme* [Mum88, Vak24] to correctly define the degree. For example, consider the affine variety defined by $X^p - T$ in $\mathbb{A}^1_{\mathbb{F}_p(T)}$. After base change to $\overline{\mathbb{F}_p(T)}$, it becomes a "point of multiplicity p," since $X^p - T = (X - T^{1/p})^p$.

Definition 3.1. *For an integer $d \geq 0$, define $C(d)$ to be the set of $a \in \mathbb{K}$ such that $a = \frac{c}{c'}$ for some $c \in \mathbb{F}[\mathbf{Y}]$ and $c' \in \mathbb{F}[\mathbf{Y}] \setminus \{0\}$ satisfying $\deg_{\mathbf{Y}}(c), \deg_{\mathbf{Y}}(c') \leq d$.*

For integers $n, d, d' \geq 0$ and variables $\mathbf{X} = (X_1, \ldots, X_n)$, define $P_{\mathbf{X}}(d, d')$ or simply $P(d, d')$ to be the set of polynomials $f \in \mathbb{K}[\mathbf{X}]$ of degree at most d such that the coefficients of f are all in $C(d')$.

Lemma 3.2. *The following hold:*

(1) $ca \in C(d)$ for $a \in C(d)$ and $c \in \mathbb{F}$.

(2) $a + b, ab \in C(d + d')$ for $a \in C(d)$ and $b \in C(d')$.

(3) $1/a \in C(d)$ for $a \in C(d) \setminus \{0\}$.

Proof. The claims follow straightforwardly by definition. □

Lemma 3.3. *Suppose $f, g \in \mathbb{K}[X_1, ..., X_n]$ are polynomials in $P(d_1, d)$ and $P(d_2, d)$, respectively. Then $fg \in P(d_1 + d_2, d')$ for some $d' = O_{d_1+d_2,d,n}(1)$.*

Proof. Each coefficient of fg is the sum of $O_{d_1+d_2,n}(1)$ terms of the form $\mathrm{coeff}_f(m_1) \cdot \mathrm{coeff}_g(m_2)$, where m_1 is a monomial of f and m_2 is a monomial of g. The claims follows by Lemma 3.2 (2). □

To address the issue of inseparable extensions, we introduce the following definitions.

Definition 3.4. *Let $p = \mathrm{char}(\mathbb{F})$, and let $e \geq 0$. We use the shorthand*

$$\mathbb{F}(\mathbf{Y}^{1/p^e}) := \mathbb{F}(Y_1^{1/p^e}, \ldots, Y_\ell^{1/p^e}) \quad \text{and} \quad \mathbb{F}[\mathbf{Y}^{1/p^e}] := \mathbb{F}[Y_1^{1/p^e}, \ldots, Y_\ell^{1/p^e}].$$

For convenience, if $\mathrm{char}(\mathbb{F}) = 0$, we interpret $p^e = 1$, even though this is not formally correct.

Define $\mathbb{K}^{(e)} := \mathbb{F}(\mathbf{Y}^{1/p^e})$. Let $C^{(e)}(d)$ be the set of elements $a \in \mathbb{K}^{(e)}$ such that $a = \frac{c}{c'}$ for some $c \in \mathbb{F}[\mathbf{Y}^{1/p^e}]$, $c' \in \mathbb{F}[\mathbf{Y}^{1/p^e}] \setminus \{0\}$, and $\deg_{\mathbf{Y}^{1/p^e}}(c), \deg_{\mathbf{Y}^{1/p^e}}(c') \leq d$. That is, the degrees of both the numerator and the denominator of c and those of c' are bounded by d as polynomials in $Y_1^{1/p^e}, \ldots, Y_\ell^{1/p^e}$.

For integers $n, d, d' \geq 0$ and variables $\mathbf{X} = (X_1, \ldots, X_n)$, define $P^{(e)}_{\mathbf{X}}(d, d')$ (or simply $P^{(e)}(d, d')$) to be the set of polynomials $f \in \mathbb{K}^{(e)}[\mathbf{X}]$ of degree at most d, whose coefficients are all in $C^{(e)}(d')$.

Note that the map $Y_i \mapsto Y_i^{p^e}$ induces a bijection

$$P^{(e)}(d, d') \to P(d, d').$$

In this way, statements about polynomials in $P(d, d')$ apply to those in $P^{(e)}(d, d')$ via this transformation. On the other hand, there is also a natural inclusion

$$P(d, d') \hookrightarrow P^{(e)}(d, p^e d')$$

given by the identity map $f \mapsto f$.

Solving a system of linear equations. The following lemma bounds the complexity of a solution of a system of linear equations.

Lemma 3.5. *Let $A = (a_{i,j})_{i\in[N],j\in[M]} \in \mathbb{K}^{N\times M}$ and $\mathbf{b} = (b_1, \ldots, b_N) \in \mathbb{K}^N$ such that all entries of A and those of $\mathbf{b}$ are in $C(d)$. Suppose the system of linear equations $A\mathbf{x} = \mathbf{b}$ has a solution. Then it has a solution $\mathbf{x} \in \mathbb{K}^M$ whose entries are all in $C(d')$, where $d' = O_{N,M,d}(1)$.*

Proof. Suppose A has rank k, and without loss of generality, we may assume the top-leftmost $k \times k$ minor B of A has full rank. Let $\widetilde{A} = (a_{i,j})_{i\in[k],j\in[M]}$ and $\widetilde{\mathbf{b}} = (b_1, \ldots, b_k)$. As $A\mathbf{x} = \mathbf{b}$ has a solution and the first k rows of A span the others, we know $\mathbf{x} = (x_1, \ldots, x_M)$ is a solution of $A\mathbf{x} = \mathbf{b}$ if and only if it is a solution of $\widetilde{A}\mathbf{x} = \widetilde{\mathbf{b}}$. By Cramer's rule, the latter has a solution given by

$$x_i = \begin{cases} \frac{\det(B_i)}{\det(B)} & 1 \le i \le k \\ 0 & k < i \le M, \end{cases} \tag{2}$$

where B_i is the matrix formed by replacing the i-th column of B by $\widetilde{\mathbf{b}}$. As the entries of B and B_i are in $C(d)$, by Lemma 3.2, the entries x_i given by (2) are in $C(d')$ for some $d' = O_{N,M,d}(1)$. □

The following lemma bounds the complexity of the coefficients of a factor of a univariate polynomial f in terms of its degree and the complexity of its coefficients.

Lemma 3.6. *Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ be a nonzero polynomial in $P(d, d')$. Let g be a factor of f. Then there exist $c \in \mathbb{K}^\times$ such that $cg \in P(d, d'')$ for some $d'' = O_{d,d',n}(1)$.*

The proof of Lemma 3.6 is deferred to Appendix A.

Gröbner bases. For $\mathbf{X} = \{X_1, \ldots, X_n\}$, denote by $\mathcal{M}_{\mathbf{X}}$ the set of monomials in $\mathbf{X}$.

Let $\preceq$ be a total order on $\mathcal{M}_{\mathbf{X}}$. We say $\preceq$ is a *monomial order* if (1) $m_1 \preceq m_2 \implies m_1 m \preceq m_2 m$, and (2) $1 \preceq m$ for all $m \in \mathcal{M}_{\mathbf{X}}$. Write $m_1 \prec m_2$ if $m_1 \preceq m_2$ and $m_1 \neq m_2$.

A monomial order is *degree-compatible* if $m_1 \preceq m_2 \implies \deg(m_1) \le \deg(m_2)$. Examples of degree-compatible monomial orders include graded lexicographic and graded reverse lexicographic orders.

Fix a monomial order $\preceq$, for $0 \neq f \in \mathbb{K}[\mathbf{X}]$, the *leading monomial* of f, denoted by $\mathrm{LM}(f)$, is the monomial appearing in f that is greatest under $\preceq$. Its coefficient is called the *leading coefficient* of f and denoted $\mathrm{LC}(f)$. The term $\mathrm{LC}(f) \cdot \mathrm{LM}(f)$ is called the *leading term* of f and denoted $\mathrm{LT}(f)$. Define $\mathrm{LM}(0) = \mathrm{LC}(0) = \mathrm{LT}(0) = 0$.

For a set $S \subseteq \mathbb{K}[\mathbf{X}]$, denote by $\mathrm{LT}(S)$ the ideal of $\mathbb{K}[\mathbf{X}]$ generated by the set $\{\mathrm{LT}(f) : f \in S\}$. It is called *ideal of leading terms* of S, also known as the *initial ideal* of S.

Definition 3.7 (Gröbner basis)**.** *A finite generating set G of an ideal I of $\mathbb{K}[\mathbf{X}]$ is said to be a Gröbner basis for I if $\mathrm{LT}(G) = \mathrm{LT}(I)$.*

Degree bounds for Gröbner bases. We have the following degree bound on Gröbner bases.

Theorem 3.8 ([Dub90, Corollary 8.3])**.** *Let $\mathbb{K} = \mathbb{F}(\mathbf{Y})$. Let I be an ideal of $\mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ generated by polynomials of degree at most d. Then for any monomial order $\preceq$, I has a Gröbner basis with respect to $\preceq$ consisting only of polynomials of degree at most $2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}$.*

We also need the following degree bound for the ideal membership problem. For a proof, see [MM82, Appendix].

Lemma 3.9 ([Her26, MM82])**.** *Let $f_1, \dots, f_k \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \dots, X_n]$ be polynomials of degree at most d. Let $f \in \langle f_1, \dots, f_k \rangle$ be a polynomial of degree at most d'. Then $f = \sum_{i=1}^k h_i f_i$ for some $h_1, \dots, h_k \in \mathbb{K}[\mathbf{X}]$ of degree at most $d' + (kd)^{2^n}$.*

We now strengthen Theorem 3.8 and Lemma 3.9 in the case where $\mathbb{K} = \mathbb{F}(\mathbf{Y})$ by establishing degree bounds on the coefficients.

Lemma 3.10. *Suppose $\mathbb{K} = \mathbb{F}(\mathbf{Y})$. Let I be an ideal of $\mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \dots, X_n]$ generated by polynomials $f_1, \dots, f_k$ in $P(d, d')$. Then for any monomial order $\preceq$, I has a Gröbner basis with respect to $\preceq$ consisting only of polynomials in $P(D, d'')$, where $D = 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}$ and $d'' = O_{d,d',n}(1)$.*

Proof. Note that $k \le \binom{n+d}{d} = O_{d,n}(1)$. By Theorem 3.8, I has a Gröbner basis G consisting of polynomials of degree at most D. Consider nonzero $g \in G$ and let $m_g = \mathrm{LM}(g)$. By replacing g with $\frac{1}{\mathrm{LC}(g)} g$, we may assume $\mathrm{LT}(g) = m_g$. By Lemma 3.9, we have $g = \sum_{i=1}^k h_i f_i$ for some $h_1, \dots, h_k$ of degree at most $D' := D + (kd)^{2^n} = O_{d,n}(1)$.

For every integer $a \in \mathbb{N}$, let S_a be the set of monomials of degree at most a. For each monomial m', as $g = \sum_{i=1}^k h_i f_i$, we have

$$\mathrm{coeff}_g(m') = \sum_{i=1}^{k} \sum_{m \in S_{D'} : m | m'} \mathrm{coeff}_{h_i}(m) \mathrm{coeff}_{f_i}(m'/m). \tag{3}$$

The condition that $\mathrm{LT}(g) = m_g$ is equivalent to that $\mathrm{coeff}_g(m_g) = 1$ and $\mathrm{coeff}_g(m') = 0$ for all $m' \in S_{d+D'}$ strictly greater than m_g with respect to $\preceq$. (Here, we only need to consider monomials $m' \in S_{d+D'}$ since $\deg(f_i) \le d$ and $\deg(h_i) \le D'$ for $i \in [k]$.) We formulate this condition as a system of linear equations as follows. Let S be the set of $m' \in S_{d+D'}$ satisfying $m_g \preceq m'$. Let $T = [k] \times S_{D'}$. Define a matrix $A \in \mathbb{K}^{S \times T}$ by

$$A[m', (i, m)] = \begin{cases} \mathrm{coeff}_{f_i}(m'/m) & m | m' \\ 0 & \text{otherwise.} \end{cases}$$

And define the column vector $\mathbf{b} \in \mathbb{K}^S$ by

$$\mathbf{b}[m'] = \begin{cases} 1 & m' = m_g \\ 0 & \text{otherwise.} \end{cases}$$

Then the condition that $\mathrm{LT}(g) = m_g$ is equivalent to that the column vector $\mathbf{x} = (\mathrm{coeff}_{h_i}(m))_{(i,m) \in T}$ satisfies $A\mathbf{x} = \mathbf{b}$. By assumption, we have $A[m', (i, m)], \mathbf{b}[m'] \in C(d')$ for all $(m', (i, m)) \in S \times T$. By Lemma 3.5, the system of linear equations $A\mathbf{x} = \mathbf{b}$ has a solution $(c_{i,m})_{(i,m) \in T}$ whose entries are all in $C(d'')$ for some

$$d'' = O_{|S|, |T|, d'}(1) = O_{d,d',n}(1),$$

where the last equality holds since $S = |S_{d+D'}| = \binom{n+d+D'}{d+D'} = O_{d,n}(1)$ and $|T| = k|S_{D'}| = k\binom{n+D'}{D'} = O_{d,n}(1)$.

Replacing h_i by $\widetilde{h}_i := \sum_{m \in S_{D'}} c_{i,m} m$ for $i \in [k]$, and replacing g by $\sum_{i=1}^{k} \widetilde{h}_i f_i$, do not change the leading term of g. Performing this replacement for each $g \in G$ preserves the fact that G is a Gröbner basis for I, since $\mathrm{LT}(G)$ remains unchanged. After the replacement, the new Gröbner basis satisfies the requirement of the lemma. □

Lemma 3.11. *Let $f_1, \ldots, f_k \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ be polynomials in $P(d, D)$. Let $f \in \langle f_1, \ldots, f_k \rangle$ be a polynomial in $P(d', D')$. Then $f = \sum_{i=1}^{k} h_i f_i$ for some $h_1, \ldots, h_k \in P(d'', D'')$ where $d'' := d' + (kd)^{2^n}$ and $D'' = O_{n,d,d',D,D'}(1)$.*

Proof. We may assume $k \leq \binom{n+d}{d}$. By Lemma 3.9, there exist polynomials $h_1, \ldots, h_k$ of degree at most d'' such that $f = \sum_{i=1}^{k} h_i f_i$. Viewing the coefficients of $h_1, \ldots, h_k$ as variables, we may build a system of linear equations over $\mathbb{K}$ that expresses the relation $f = \sum_{i=1}^{k} h_i f_i$. It has at most $k \cdot \binom{n+d''}{d''} = O_{n,d,d'}(1)$ variables and at most $\binom{n+d'}{d'} = O_{n,d'}(1)$ linear equations. The coefficients of these linear equations live in $C(\max\{D, D'\})$. So by Lemma 3.5, we may choose $h_1, \ldots, h_k$ such that they live in $P(d'', D'')$ for some $D'' = O_{n,d,d',D,D'}(1)$. □

Elimination of variables. Let $\preceq_{\mathbf{X}}$ and $\preceq_{\mathbf{Z}}$ be monomial orders on $\mathcal{M}_{\mathbf{X}}$ and $\mathcal{M}_{\mathbf{Z}}$, respectively. Denote by $\preceq = (\preceq_{\mathbf{X}}, \preceq_{\mathbf{Z}})$ the following monomial order on the monomials in both $\mathbf{X}$ and $\mathbf{Z}$:

$$m_1 m_2 \prec m_1' m_2' \iff \begin{cases} m_1 \prec m_1' \\ \text{or} \\ m_1 = m_1' \text{ and } m_2 \prec m_2' \end{cases} \qquad \text{for } m_1, m_1' \in \mathcal{M}_{\mathbf{X}} \text{ and } m_2, m_2' \in \mathcal{M}_{\mathbf{Z}}.$$

Call $\preceq$ an *elimination order* for $\mathbf{X}$.

The following is a well-known fact about eliminating variables using an elimination order. See, e.g., [AL94, Theorem 2.3.4].

Lemma 3.12 (Elimination of variables)**.** *Let $\preceq_{\mathbf{X}}$ and $\preceq_{\mathbf{Z}}$ be monomial orders on $\mathcal{M}_{\mathbf{X}}$ and $\mathcal{M}_{\mathbf{Z}}$, respectively. Let $\preceq = (\preceq_{\mathbf{X}}, \preceq_{\mathbf{Z}})$. Let I be an ideal of $\mathbb{K}[\mathbf{X}, \mathbf{Z}]$. Let G be a Gröbner basis for the ideal I with respect to $\preceq$. Then $G \cap \mathbb{K}[\mathbf{Z}]$ is a Gröbner basis for the ideal $I \cap \mathbb{K}[\mathbf{Z}]$ of $\mathbb{K}[\mathbf{Z}]$ with respect to $\preceq_{\mathbf{Z}}$.*

Combining Lemma 3.10 and Lemma 3.12 yields the following statement.

Lemma 3.13. *Let I be an ideal of $\mathbb{K}[\mathbf{X}, \mathbf{Z}] = \mathbb{K}[X_1, \ldots, X_n, Z_1, \ldots, Z_m]$ generated by polynomials $f_1, \ldots, f_k \in P(d, d')$. Then for any monomial order $\preceq_{\mathbf{Z}}$ on $\mathcal{M}_{\mathbf{Z}}$, $I \cap \mathbb{K}[\mathbf{Z}]$ has a Gröbner basis with respect to $\preceq_{\mathbf{Z}}$ consisting only of polynomials in $P(D, D')$, where $D = O_{d,n+m}(1)$ and $D' = O_{d,d',n+m}(1)$.*

Proof. Let $\preceq_{\mathbf{X}}$ be a monomial order on $\mathcal{M}_{\mathbf{X}}$ and let $\preceq = (\preceq_{\mathbf{X}}, \preceq_{\mathbf{Z}})$. Let G be a Gröbner basis for I with respect to $\preceq$. By Lemma 3.10, we may assume that G consists only of polynomials in $P(D, D')$, where $D = 2\left(\frac{d^2}{2} + d\right)^{2^{n+m-1}} = O_{d,n+m}(1)$ and $D' = O_{d,d',n+m}(1)$. By Lemma 3.12, $G \cap \mathbb{K}[\mathbf{Z}]$ is a Gröbner basis for $I \cap \mathbb{K}[\mathbf{Z}]$ with respect to $\preceq_{\mathbf{Z}}$. The lemma follows. □

Reduction algorithm. The reduction algorithm, also known as the division algorithm, generalizes both row reduction in Gaussian elimination and long division of univariate polynomials. Running this algorithm on a polynomial f with respect to a Gröbner basis yields a unique "remainder" of f.

Definition 3.14. *Let G be a subset of $\mathbb{K}[\mathbf{X}]$. $f \in \mathbb{K}[\mathbf{X}]$ is said to be* reducible modulo G *if f has a nonzero term that is in $\mathrm{LT}(G)$. Otherwise, we say f is* reduced modulo G.

Lemma 3.15. *Let $f \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ and let $G = \{g_1, \ldots, g_k\}$ be a Gröbner basis for an ideal I of $\mathbb{K}[\mathbf{X}]$ with respect to a monomial order $\preceq$. Then:*

(1) There exists unique $f_G \in \mathbb{K}[\mathbf{X}]$ such that f_G is reduced mod G and $f - f_G = \sum_{i=1}^{k} h_i g_i \in I$, where $h_1, \ldots, h_k \in \mathbb{K}[\mathbf{X}]$.

(2) Suppose $f, g_1, \ldots, g_k \in P(d, d')$. Further assume that for $i \in [k]$, $\deg(\mathrm{LT}(g_i)) = \deg(g_i)$, which holds if $\preceq$ is degree-compatible. Then in Item 1, $f_G \in P(d, d'')$ and $h_1, \ldots, h_k$ may be chosen in $P(d, d'')$ as well, where $d'' = O_{d,d',n}(1)$.

The reduction algorithm outputting f_G and $h_1, \ldots, h_k$ is given as follows.

Algorithm 1 The reduction algorithm

Input: f, $G = \{g_1, \ldots, g_k\}$
Output: f_G, $h_1, \ldots, h_k$
  $f_G \leftarrow f$; $h_1, \ldots, h_k \leftarrow 0$
  while f_G has a term T divisible by $\mathrm{LT}(g_i)$ for some $i \in [k]$ **do**
    $f_G \leftarrow f_G - \frac{T}{\mathrm{LT}(g_i)} g_i$
    $h_i \leftarrow h_i + \frac{T}{\mathrm{LT}(g_i)}$
  end while
  return f_G, $h_1, \ldots, h_k$

Algorithm 1 terminates in general, even without the assumption that $\deg(\mathrm{LT}(g_i)) = \deg(g_i)$ for $i \in [k]$. This fact follows from Hilbert's basis theorem or Dickson's lemma [BW98]. We make the additional assumption that $\deg(\mathrm{LT}(g_i)) = \deg(g_i)$ for $i \in [k]$, which leads to a simpler proof that bounds the complexity of the coefficients of $f_G, h_1, \ldots, h_k$.

Proof of Lemma 3.15. Item 1 is standard (see, e.g., [AL94]).

We claim $\deg(f_G) \le \deg(f)$ and $\deg(h_i g_i) \le \deg(f)$ for $i \in [k]$. This follows from the following induction: At the beginning of the algorithm, these bounds hold since $f_G = f$ and $h_1, \ldots, h_k = 0$. In each iteration, the degree of $\Delta := \frac{T}{\mathrm{LT}(g_i)} g_i$ is $\deg(T) - \deg(\mathrm{LT}(g_i)) + \deg(g_i) = \deg(T) \le \deg(f_G) \le \deg(f)$. We subtract Δ from f_G, which does not increase the degree of f_G since the degrees of the newly added monomials are bounded by $\deg(\Delta) \le \deg(f_G)$. Similarly, we add Δ/g_i to h_i, which preserves the property that $\deg(h_i g_i) \le \deg(f)$ since $\deg((\Delta/g_i) \cdot g_i) = \deg(\Delta) \le \deg(f)$. So the degree bounds hold during and at the end of the algorithm.

Now we prove Item 2. By Item 1, we already know $\deg(f_G), \deg(h_1), \ldots, \deg(h_k) \le \deg(f) \le d$. We have

$$f_G = f - \sum_{i=1}^{k} h_i g_i = f - \sum_{i=1}^{k} \sum_{m \in S_i} \mathrm{coeff}_{h_i}(m) m g_i,$$

where S_i is the set of monomials m such that $\deg(m \cdot g_i) \le \deg(f)$. Therefore, for each monomial m' of degree at most $\deg(f)$, we have

$$\operatorname{coeff}_{f_G}(m') = \operatorname{coeff}_f(m') - \sum_{i=1}^{k} \sum_{m \in S_i : m | m'} \operatorname{coeff}_{h_i}(m) \operatorname{coeff}_{g_i}(m'/m). \tag{4}$$

Let S be the set of monomials of degree at most $\deg(f) \le d$, and let $T = \{(i, m) : m \in S_i\}$. Note that $k, |S| \le \binom{n+d}{d}$ and $|T| = \sum_{i=1}^{k} |S_i| \le \binom{n+d}{d}^2$. By definition, a polynomial g satisfying $\deg(g) \le \deg(f)$ is reduced mod G if and only if $\operatorname{coeff}_g(m') = 0$ for all $m' \in S$. So the polynomial $f_G = f - \sum_{i=1}^{k} h_i g_i$ with $h_i = \sum_{m \in S_i} \operatorname{coeff}_{h_i}(m) m$ is reduced mod G if and only if the column vectors $\mathbf{x} = (\operatorname{coeff}_{h_i}(m))_{(i,m) \in T}$ and $\mathbf{b} = (\operatorname{coeff}_f(m'))_{m' \in S}$ satisfies $A\mathbf{x} = \mathbf{b}$, where the matrix $A \in \mathbb{K}^{S \times T}$ is given by

$$A[m', (i, m)] = \begin{cases} \operatorname{coeff}_{g_i}(m'/m) & m | m' \\ 0 & \text{otherwise.} \end{cases}$$

By assumption, we have $A[m', (i, m)], \mathbf{b}[m'] \in C(d')$ for all $(m', (i, m)) \in S \times T$. By Lemma 3.5, we may choose the coefficients of $h_1, \dots, h_k$ to be in $C(d_0)$ for some $d_0 = O_{|S|,|T|,d'}(1) = O_{d,d',n}(1)$.

By (4) and Lemma 3.2, for such $h_1, \dots, h_k$, the coefficients of f_G are all in $C(d_1)$, where $d_1 = O_{d,d',n}(1)$. Choose $d'' := \max(d_0, d_1) = O_{d,d',n}(1)$. Then $f_G, h_1, \dots, h_k \in P(d, d'')$ by definition. □

Definition 3.16. *f_G in Lemma 3.15 is called the* remainder *of f modulo G with respect to $\preceq$.*

We also need the following variant of Lemma 3.15 for elimination orders.

Lemma 3.17. *Let $f \in \mathbb{K}[\mathbf{X}, \mathbf{Z}] = \mathbb{K}[X_1, \dots, X_n, Z_1, \dots, Z_m]$. Let $\preceq_{\mathbf{X}}$ and $\preceq_{\mathbf{Z}}$ be degree-compatible monomial orders on $\mathcal{M}_{\mathbf{X}}$ and on $\mathcal{M}_{\mathbf{Z}}$, respectively, and let $\preceq = (\preceq_{\mathbf{X}}, \preceq_{\mathbf{Z}})$. Let $G = \{g_1, \dots, g_k\}$ be a Gröbner basis for an ideal I of $\mathbb{K}[\mathbf{X}, \mathbf{Z}]$ with respect to $\preceq$. Suppose $f, g_1, \dots, g_k \in P(d, d')$. Then the remainder f_G of f is in $P(d_1, d_2)$ for some $d_1 \in O_{d,n}(1)$ and $d_2 = O_{d,d',n}(1)$.*

Proof. We modify the proof of Lemma 3.15 as follows. Let $W = \max\{\deg_{\mathbf{Z}}(g_1), \dots, \deg_{\mathbf{Z}}(g_k)\} + 1 \le d + 1$. Define the weighted degree of a monomial m by $\operatorname{wdeg}(m) = W \cdot \deg_{\mathbf{X}}(m) + \deg_{\mathbf{Z}}(m)$. For a polynomial $P \in \mathbb{K}[\mathbf{X}, \mathbf{Z}]$, define its weighted degree $\operatorname{wdeg}(P)$ to be the maximum weighted degree among the monomials appearing in P, or $-\infty$ if $P = 0$. Note that $\operatorname{wdeg}(\cdot)$ is multiplicative. Also note that the choice of W guarantees that $\operatorname{wdeg}(g_i) = \operatorname{wdeg}(\operatorname{LT}(g_i))$ for $i \in [k]$.

We claim $\operatorname{wdeg}(f_G) \le \operatorname{wdeg}(f)$ and $\operatorname{wdeg}(h_i g_i) \le \operatorname{wdeg}(f)$ for $i \in [k]$. This follows from the following induction: At the beginning of the algorithm, these bounds hold since $f_G = f$ and $h_1, \dots, h_k = 0$. In each iteration, the weighted degree of $\Delta := \frac{T}{\operatorname{LT}(g_i)} g_i$ is $\operatorname{wdeg}(T) - \operatorname{wdeg}(\operatorname{LT}(g_i)) + \operatorname{wdeg}(g_i) = \operatorname{wdeg}(T) \le \operatorname{wdeg}(f_G) \le \operatorname{wdeg}(f)$. We subtract Δ from f_G, which does not increase the weighted degree of f_G since the weighted degrees of the newly added monomials are bounded by $\operatorname{wdeg}(\Delta) \le \operatorname{wdeg}(f_G)$. Similarly, we add Δ / g_i to h_i, which preserves the property that $\operatorname{wdeg}(h_i g_i) \le \operatorname{wdeg}(f)$ since $\operatorname{wdeg}((\Delta / g_i) \cdot g_i) = \operatorname{wdeg}(\Delta) \le \operatorname{wdeg}(f)$. The claim follows by induction.

The rest of the proof follows that of Lemma 3.15, except that we use the weighted degree in place of the standard degree. Note that for any polynomial $P \in \mathbb{K}[\mathbf{X}, \mathbf{Z}]$, we have $\deg(P) \le \operatorname{wdeg}(P) \le W \cdot \operatorname{wdeg}(P)$, where $W \le d + 1$. Using this fact, we can still show that $f_G \in P(d_1, d_2)$ where $d_1 = O_{d,n}(1)$ and $d_2 = O_{d,d',n}(1)$. □

Ring homomorphisms. The following lemma gives degree bounds about the data describing a ring homomorphism between quotients of polynomial rings.

Lemma 3.18. *Let $f_1, \dots, f_k, g_1, \dots, g_m \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \dots, X_n]$ be polynomials in $P_{\mathbf{X}}(d, d')$. Let $I = \langle f_1, \dots, f_k \rangle \subseteq \mathbb{K}[\mathbf{X}]$. Let ϕ be the $\mathbb{K}$-linear ring homomorphism*

$$\begin{aligned} \phi : \mathbb{K}[\mathbf{Z}] = \mathbb{K}[Z_1, \dots, Z_m] &\to \mathbb{K}[\mathbf{X}]/I \\ Z_i &\mapsto g_i + I, \quad i = 1, 2, \dots, m. \end{aligned}$$

Let A be the image of ϕ, i.e., A is the subring of $\mathbb{K}[\mathbf{X}]/I$ generated by $g_1 + I, \dots, g_m + I$. Then:

(1) ϕ induces an isomorphism $\mathbb{K}[Z_1, \dots, Z_m]/\ker(\phi) \cong A$.

(2) For any monomial order $\preceq_{\mathbf{Z}}$ on $\mathcal{M}_{\mathbf{Z}}$, $\ker(\phi)$ has a Gröbner basis with respect to $\preceq_{\mathbf{Z}}$ consisting only of polynomials in $P_{\mathbf{Z}}(D, D')$, where $D = O_{d,n+m}(1)$ and $D' = O_{d,d',n+m}(1)$.

(3) Let $f \in \mathbb{K}[\mathbf{X}]$ such that $f + I \in A$ and $f \in P_{\mathbf{X}}(d_1, d_2)$. Then there exists $h \in \mathbb{K}[\mathbf{Z}]$ such that $\phi(h) = f + I$ and $h \in P_{\mathbf{Z}}(d_3, d_4)$, where $d_3 = O_{d,d_1,n+m}(1)$ and $d_4 = O_{d,d',d_1,d_2,n+m}(1)$.

Proof. Item 1 holds by the first isomorphism theorem. Let $J = \langle f_1, \dots, f_k, Z_1 - g_1, \dots, Z_m - g_m \rangle \subseteq \mathbb{K}[\mathbf{X}, \mathbf{Z}]$. Then $\ker(\phi) = J \cap \mathbb{K}[\mathbf{Z}]$ [AL94, Theorem 2.4.10]. Item 2 then follows from Lemma 3.13.

It remains to prove Item 3. Let $\preceq_{\mathbf{X}}$ and $\preceq_{\mathbf{Z}}$ be degree-compatible monomial orders on $\mathcal{M}_{\mathbf{X}}$ and on $\mathcal{M}_{\mathbf{Z}}$, respectively. Let $\preceq = (\preceq_{\mathbf{X}}, \preceq_{\mathbf{Z}})$. Let G be a Gröbner basis of J with respect to $\preceq$. By Lemma 3.10, we may assume that G consists only of polynomials in $P(d_5, d_6)$, where $d_5 = O_{d,n+m}(1)$ and $d_6 = O_{d,d',n+m}(1)$.

By assumption, $f + I$ is in A and hence in the image of ϕ. Let h be the remainder of f modulo G with respect to $\preceq$. Then $\phi(h) = f + I$ by [AL94, Theorem 2.4.11]. Moreover, $h \in P_{\mathbf{Z}}(d_3, d_4)$ for some $d_3 = O_{\max(d_1,d_5),n+m}(1) = O_{d,d_1,n+m}(1)$ and $d_4 = O_{\max(d_1,d_5),\max(d_2,d_6),n+m}(1) = O_{d,d',d_1,d_2,n+m}(1)$ by Lemma 3.17. □

Primitive element theorem. We now prove a quantitative form of primitive element theorem, following a proof in [ZS75].

Theorem 3.19 (Primitive element theorem, quantitative form)**.** *Let $f_1, f_2, \dots, f_k \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \dots, X_n]$ be polynomials in $P(d, d')$. Suppose $\mathfrak{m} = \langle f_1, \dots, f_k \rangle$ is a maximal ideal of $\mathbb{K}[\mathbf{X}]$ and $\mathbb{L} := \mathbb{K}[\mathbf{X}]/\mathfrak{m}$ is a finite separable extension of $\mathbb{K}$. Let $\alpha_i := X_i + \mathfrak{m} \in \mathbb{L}$ for $i \in [n]$, so that $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Then there exists a nonzero polynomial $Q \in \mathbb{L}[\mathbf{Z}] = \mathbb{L}[Z_1, \dots, Z_n]$ such that for every nonzero $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}^n$ satisfying $Q(\mathbf{c}) \neq 0$, there exist $P_0^{\mathbf{c}}, P_1^{\mathbf{c}}, \dots, P_n^{\mathbf{c}} \in \mathbb{K}[T]$ such that the following hold:*

(1) Let $\beta_{\mathbf{c}} = \sum_{i=1}^n c_i \alpha_i \in \mathbb{L}$. Then $P_0^{\mathbf{c}}(\beta_{\mathbf{c}}) \neq 0$ and $\alpha_i = \frac{P_i^{\mathbf{c}}(\beta_{\mathbf{c}})}{P_0^{\mathbf{c}}(\beta_{\mathbf{c}})}$ for $i \in [n]$. In particular, $\mathbb{L} = \mathbb{K}(\beta_{\mathbf{c}})$.

(2) $P_0^{\mathbf{c}}, \dots, P_n^{\mathbf{c}} \in P(d^n, d_0)$ for some $d_0 = O_{d,d',n}(1)$.

In particular, the above hold for almost all $\mathbf{c} \in \mathbb{F}^n$.

Proof. Let $\mathbb{K}^* = \mathbb{K}(\mathbf{Z}) = \mathbb{K}(Z_1, \ldots, Z_n)$ and $\mathbb{L}^* = \mathbb{L}(\mathbf{Z}) = \mathbb{L}(Z_1, \ldots, Z_n) = \mathbb{K}^*(\alpha_1, \ldots, \alpha_n)$. By assumption, $\alpha_1, \ldots, \alpha_n$ are separable over $\mathbb{K}$. So they are also separable over $\mathbb{K}^*$. It follows that $\mathbb{L}^*$ is a finite separable extension of $\mathbb{K}^*$.

Consider

$$\beta(\mathbf{Z}) := Z_1\alpha_1 + Z_2\alpha_2 + \cdots + Z_n\alpha_n \in \mathbb{L}[\mathbf{Z}] \subseteq \mathbb{L}^*.$$

Let $F(T) \in \mathbb{K}^*[T]$ be the minimal polynomial of $\beta(\mathbf{Z})$ over $\mathbb{K}^*$. We have

$$\deg(F) = [\mathbb{K}^*(\beta(\mathbf{Z})) : \mathbb{K}^*] \leq [\mathbb{L}^* : \mathbb{K}^*] \leq [\mathbb{L} : \mathbb{K}] \leq d^n, \tag{5}$$

where the last inequality follows from Lemma 2.14.

We may construct F as follows. Let $\preceq_{T,\mathbf{Z}}$ be an elimination order for T on $\mathcal{M}_{T,\mathbf{Z}}$, and let $\preceq = (\preceq_{\mathbf{X}}, \preceq_{T,\mathbf{Z}})$ be an elimination order for $\mathbf{X}$ on $\mathcal{M}_{\mathbf{X},T,\mathbf{Z}}$. Let I be the ideal

$$I = \langle f_1, \ldots, f_k, T - (Z_1X_1 + \cdots + Z_nX_n)\rangle$$

of $\mathbb{K}[\mathbf{X}, T, \mathbf{Z}]$. The ideal I is the preimage of the ideal $\langle T - \beta(\mathbf{Z})\rangle$ of $(\mathbb{K}[\mathbf{X}]/\mathfrak{m})[T, \mathbf{Z}] = \mathbb{L}[T, \mathbf{Z}]$ under the natural quotient map $\mathbb{K}[\mathbf{X}, T, \mathbf{Z}] \to (\mathbb{K}[\mathbf{X}]/\mathfrak{m})[T, \mathbf{Z}]$. As $\beta(\mathbf{Z})$ is algebraic over $\mathbb{K}^*$, we have $I \cap \mathbb{K}[T, \mathbf{Z}] \neq \{0\}$.

Let G be a Gröbner basis for I with respect to $\preceq$. Then $G \cap \mathbb{K}[T, \mathbf{Z}]$ is a Gröbner basis for $I \cap \mathbb{K}[T, \mathbf{Z}]$ with respect to $\preceq_{T,\mathbf{Z}}$ by Lemma 3.12. Choose $g \in G \cap \mathbb{K}[T, \mathbf{Z}]$ such that $\mathrm{LM}(g)$ has the form mT^e, where $m \in \mathcal{M}_{\mathbf{Z}}$ and e is minimized. By the choice of $\preceq$, we have $g \in \mathbb{K}[T, \mathbf{Z}]$. Note that such g exists since $\beta(\mathbf{Z})$ is algebraic over $\mathbb{K}^*$. By Lemma 3.10, we may assume $\deg(g) \in P(D, d'')$ with $D = O_{d,n}(1)$ and $d'' = O_{d,d',n}(1)$.

Write $g = \sum_{i=0}^{e} h_iT^i$ with $h_i \in \mathbb{K}[\mathbf{Z}]$ for $i = 0, 1, \ldots, e$. Then $h_e \neq 0$. As e is minimized and I is the preimage of $\langle T - \beta(\mathbf{Z})\rangle$ in $\mathbb{K}[\mathbf{X}, T, \mathbf{Z}]$, $g/h_e = \sum_{i=0}^{e}(h_i/h_e)T^i$ is precisely the minimal polynomial $F(T)$ of $\beta(\mathbf{Z})$ over $\mathbb{K}^*$. And by (5),

$$e = \deg(F) \leq d^n.$$

We also have

$$g(Z_1\alpha_1 + Z_2\alpha_2 + \cdots + Z_n, Z_1, \ldots, Z_n) = g(\beta(\mathbf{Z}), \mathbf{Z}) = 0. \tag{6}$$

Taking the partial derivatives of (6) with respect to $Z_1, \ldots, Z_n$ and applying the chain rule for multivariate polynomials, we obtain

$$\alpha_i g_0(\beta(\mathbf{Z}), \mathbf{Z}) + g_i(\beta(\mathbf{Z}), \mathbf{Z}) = 0, \quad i = 1, 2, \ldots, n, \tag{7}$$

where $g_0(T, \mathbf{Z}) := \frac{\partial g(T,\mathbf{Z})}{\partial T}$ and $g_i(T, \mathbf{Z}) := \frac{\partial g(T,\mathbf{Z})}{\partial Z_i}$ for $i \in [n]$.

As $F(X)$ is the minimal polynomial of $\beta(\mathbf{Z}) \in \mathbb{L}^*$ over $\mathbb{K}^*$ and $\mathbb{L}^*$ is a finite separable extension of $\mathbb{K}^*$, we have $F'(\beta(\mathbf{Z})) \neq 0$. And as $g_0(T, \mathbf{Z}) = \frac{\partial g(T,\mathbf{Z})}{\partial T}$ and $g = h_eF$, we have

$$g_0(\beta(\mathbf{Z}), \mathbf{Z}) = h_e(\mathbf{Z}) \cdot F'(\beta(\mathbf{Z})) \neq 0.$$

Define $Q(\mathbf{Z}) = g_0(\beta(\mathbf{Z}), \mathbf{Z}) \in \mathbb{L}[\mathbf{Z}]$. For every $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}^n$, define $P_0^{\mathbf{c}}(T) = g_0(T, \mathbf{c}) \in \mathbb{K}[T]$ and $P_i^{\mathbf{c}}(T) = -g_i(T, \mathbf{c}) \in \mathbb{K}[T]$ for $i \in [n]$.

Consider $\mathbf{c} \in \mathbb{F}^n$ such that $Q(\mathbf{c}) \neq 0$. Note that $\beta(\mathbf{c}) = \sum_{i=1}^{n} c_i\alpha_i = \beta_{\mathbf{c}}$ and $P_0^{\mathbf{c}}(\beta_{\mathbf{c}}) = g_0(\beta(\mathbf{c}), \mathbf{c}) = Q(\mathbf{c}) \neq 0$. We have by (7) that

$$\alpha_i = -\frac{g_i(\beta(\mathbf{c}), \mathbf{c})}{g_0(\beta(\mathbf{c}), \mathbf{c})} = \frac{P_i^{\mathbf{c}}(\beta_{\mathbf{c}})}{P_0^{\mathbf{c}}(\beta_{\mathbf{c}})}, \quad i = 1, 2, \ldots, n,$$

By definition, $P_0^{\mathbf{c}}(T) = g_0(T, \mathbf{c})$ and $P_i^{\mathbf{c}}(T) = -g_i(T, \mathbf{c})$ for $i \in [n]$. So we have $\deg(P_i^{\mathbf{c}}) \leq \deg_T(g_i) \leq \deg_T(g) = e \leq d^n$ for $i \in 0, 1, \ldots, n$. As already noted above, $\deg(g) \in P(D, d'')$, so the coefficients of g are all in $C(d'')$. For $i = 0, 1 \ldots, n$ and $j = 0, 1, \ldots, \deg(P_i^{\mathbf{c}})$, the coefficient of T^j in $P_i^{\mathbf{c}}$ is a linear combination of the coefficients of the monomials of degree j in T of g_i over $\mathbb{F}$, and g_i has at most $\binom{n+D}{D}$ such monomials since $\deg(g_i) \leq \deg(g) \leq D$. Therefore, by Lemma 3.2, the coefficients of $P_0^{\mathbf{c}}, \ldots, P_n^{\mathbf{c}}$ are in $C(d_0)$, where $d_0 = \binom{n+D}{D} d'' = O_{d,d',n}(1)$. It follows that $P_0^{\mathbf{c}}, \ldots, P_n^{\mathbf{c}} \in P(d^n, d_0)$. □

Extracting a maximal ideal. Let I be a zero-dimensional ideal of $\mathbb{K}[\mathbf{X}]$, whose generators are given. We need to solve the problem of finding the generators of a maximal ideal $\mathfrak{m}$ containing I or, more precisely, to bound the complexity of these generators. This problem is a special case of finding the radical and the primary decomposition of a zero-dimensional ideal, with coefficient bounds. The following lemma provides a direct solution.

Lemma 3.20. *Let $f_1, \ldots, f_k \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ be polynomials in $P(d, d')$. Suppose $I = \langle f_1, \ldots, f_k \rangle$ is a zero-dimensional ideal of $\mathbb{K}[\mathbf{X}]$. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{K}[\mathbf{X}]$ containing I such that $\mathbb{K}[\mathbf{X}]/\mathfrak{m}$ is a finite separable extension of $\mathbb{K}$. Then $\mathfrak{m}$ is generated by polynomials in $P(d^n + 1, d'')$, where $d'' = O_{d,d',n}(1)$.*

Proof. We follow the approach of [GTZ88]. Let $\alpha_i = X_i + \mathfrak{m} \in \mathbb{K}[\mathbf{X}]/\mathfrak{m}$ for $i \in [n]$. By Theorem 3.19, there exist $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}^n$ and $P_0^{\mathbf{c}}, P_1^{\mathbf{c}}, \ldots, P_n^{\mathbf{c}} \in \mathbb{K}[T]$ such that $\beta_{\mathbf{c}} = \sum_{i=1}^n c_i \alpha_i$ satisfies $P_0^{\mathbf{c}}(\beta_{\mathbf{c}}) \neq 0$ and $\alpha_i = \frac{P_i^{\mathbf{c}}(\beta_{\mathbf{c}})}{P_0^{\mathbf{c}}(\beta_{\mathbf{c}})}$ for $i \in [n]$. Moreover, $P_0^{\mathbf{c}}, \ldots, P_n^{\mathbf{c}} \in P(d^n, d_0)$ for some $d_0 = O_{d,d',n}(1)$.

Let $T = \sum_{i=1}^n c_i X_i \in \mathbb{K}[\mathbf{X}]$. Let $\mathfrak{m}_0 = \mathfrak{m} \cap \mathbb{K}[T]$, which is a prime ideal of $\mathbb{K}[T]$. Let $I_0 = I \cap \mathbb{K}[T]$. As $\mathbb{K}[T]$ is a PID, $\mathfrak{m}_0$ and I_0 are generated by polynomials $g, h \in \mathbb{K}[T]$ over $\mathbb{K}$, respectively, and $g | h$. The inclusion $\mathbb{K}[T] \hookrightarrow \mathbb{K}[\mathbf{X}]$ induces an inclusion $\mathbb{K}[T]/I_0 \hookrightarrow \mathbb{K}[\mathbf{X}]/I$. So we have

$$\deg(g) \leq \deg(h) = \dim_{\mathbb{K}}(\mathbb{K}[T]/I_0) \leq \dim_{\mathbb{K}}(\mathbb{K}[\mathbf{X}]/I) \leq d^n,$$

where the last inequality holds by Lemma 2.14. By Lemma 3.13 and the fact that $I_0 = \langle h \rangle$, we may assume that $h \in P(d^n, d_1)$ for some $d_1 = O_{d,d',n}(1)$.[5] As $g | h$, by Lemma 3.6, we may assume that $g \in P(d^n, d_2)$ for some $d_2 = O_{d,d',n}(1)$.

For $i \in [n]$, let $g_i = P_0^{\mathbf{c}}(T) X_i - P_i^{\mathbf{c}}(T) \in \mathbb{K}[\mathbf{X}]$, whose degree is at most $d^n + 1$. And the coefficients of each g_i are in $C(d_0)$ since the same holds for $P_0^{\mathbf{c}}$ and $P_i^{\mathbf{c}}$. So $g_1, \ldots, g_n \in P(d^n + 1, d_0)$. Let $d'' = \max(d_0, d_2)$. The $g, g_1, \ldots, g_n \in P(d^n + 1, d'')$.

For $i \in [n]$, the image of g_i in $\mathbb{K}[\mathbf{X}]/\mathfrak{m}$ is $P_0^{\mathbf{c}}(\beta_{\mathbf{c}})\alpha_i - P_i^{\mathbf{c}}(\beta_{\mathbf{c}})$, which is zero since $\alpha_i = \frac{P_i^{\mathbf{c}}(\beta_{\mathbf{c}})}{P_0^{\mathbf{c}}(\beta_{\mathbf{c}})}$. So $g_1, \ldots, g_n \in \mathfrak{m}$.

Note that $\mathbb{K}[\mathbf{X}]/\langle g, g_1, \ldots, g_n \rangle \cong \mathbb{K}[T]/\langle g \rangle = \mathbb{K}[T]/\mathfrak{m}_0$. This follows by noting that $P_0^{\mathbf{c}}(T) \in \mathbb{K}[T]$ is invertible modulo $\langle g \rangle = \mathfrak{m}_0$ (since $P_0^{\mathbf{c}}(\beta_{\mathbf{c}}) \neq 0$ and $\mathfrak{m}_0 = \mathfrak{m} \cap \mathbb{K}[T]$), and therefore, we can use the relations $g_i = P_0^{\mathbf{c}}(T) X_i - P_i^{\mathbf{c}}(T) = 0$, $i = 1, \ldots, n$, to eliminate $X_1, \ldots, X_n$. As $\mathbb{K}[T]/\mathfrak{m}_0$ is a field, $\langle g, g_1, \ldots, g_n \rangle$ is a maximal ideal of $\mathbb{K}[\mathbf{X}]$. As $g, g_1, \ldots, g_n \in \mathfrak{m}$ and $\mathfrak{m}$ is also a maximal ideal of $\mathbb{K}[\mathbf{X}]$, we have $\mathfrak{m} = \langle g, g_1, \ldots, g_n \rangle$. The lemma follows. □

[5] We may view h as a polynomial in T and another $n - 1$ variables by performing an $\mathbb{F}$-linear transformation on the system of coordinates, which does not affect the degrees of the numerators and denominators of the coefficients.

Idealizer. Let A be an integral domain and J be an ideal of A. The *idealizer* of J is defined as

$$\mathrm{Id}_A(J) := \{a \in \mathrm{Frac}(A) : aJ \subseteq J\}.$$

It is the largest subring of $\mathrm{Frac}(A)$ in which J is still an ideal.

A closely related notion is the *ideal quotient* of two ideals. For ideals I and J of a ring R, define the ideal quotient $(I : J) := \{a \in R : aJ \subseteq I\}$, which is an ideal of R.

Lemma 3.21. *Let $f_1, \ldots, f_k, g_1, \ldots, g_m \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ be polynomials in $P(d, d')$. Suppose $I := \langle f_1, \ldots, f_k\rangle$ is a prime ideal of $\mathbb{K}[\mathbf{X}]$, or equivalently, $A := \mathbb{K}[\mathbf{X}]/I$ is an integral domain. Let J be the ideal $\langle g_1 + I, \ldots, g_m + I\rangle$ of A.*

Assume that $c \cdot \mathrm{Id}_A(J) \subseteq A$, where $c = f + I \in A \setminus \{0\}$ and $f \in P(d, d')$. Then with respect to any monomial order, the preimage of $c \cdot \mathrm{Id}_A(J)$ in $\mathbb{K}[\mathbf{X}]$ under the natural quotient map $\mathbb{K}[\mathbf{X}] \to A$ has a Gröbner basis consisting only of polynomials in $P(D, D')$, where $D = O_{d,n}(1)$ and $D' = O_{d,d',n}(1)$.

Proof. For any ideal I_0 of A, denote by $\widehat{I_0}$ the preimage of I_0 in $\mathbb{K}[\mathbf{X}]$ under the natural quotient map, i.e., $\widehat{I_0} = \{a \in \mathbb{K}[\mathbf{X}] : a + I \in I_0\}$.

As $c \neq 0$ and A is an integral domain, we know c is a non-zero-divisor of A. As $c \cdot \mathrm{Id}_A(J) \subseteq A$, we know

$$c \cdot \mathrm{Id}_A(J) = \{b \in A : b = ca, aJ \subseteq J\} = \{b \in A : bJ \subseteq cJ\} = (cJ : J),$$

where the second equality uses the fact that c is a non-zero-divisor. It follows that

$$c \cdot \widehat{\mathrm{Id}_A(J)} = \widehat{(cJ : J)} = (\widehat{cJ} : \widehat{J}). \tag{8}$$

By definition, $\widehat{J} = \langle f_1, \ldots, f_k, g_1, \ldots, g_m\rangle$ and $\widehat{cJ} = \langle f_1, \ldots, f_k, fg_1, \ldots, fg_m\rangle$. It follows from [AL94, Lemmas 2.3.10 and 2.3.11] that

$$\begin{aligned}(\widehat{cJ} : \widehat{J}) &= \bigcap_{h \in \{f_1, \ldots, f_k, g_1, \ldots, g_m\}} \frac{1}{h}(\langle f_1, \ldots, f_k, fg_1, \ldots, fg_m\rangle \cap \langle h\rangle) \\ &= \bigcap_{i=1}^{m} \frac{1}{g_i}(\langle f_1, \ldots, f_k, fg_1, \ldots, fg_m\rangle \cap \langle g_i\rangle) \\ &= \bigcap_{i=1}^{m} \frac{1}{g_i} I_i,\end{aligned} \tag{9}$$

where $I_i := \langle f_1, \ldots, f_k, fg_1, \ldots, fg_m\rangle \cap \langle g_i\rangle$ for $i \in [m]$. By [AL94, Proposition 2.3.5], we can compute this intersection by introducing a new variable T and then eliminating it:

$$\begin{aligned}I_i &= (T \cdot \langle f_1, \ldots, f_k, fg_1, \ldots, fg_m\rangle + (1 - T) \cdot \langle g_i\rangle) \cap \mathbb{K}[\mathbf{X}] \\ &= \langle Tf_1, \ldots, Tf_k, Tfg_1, \ldots, Tfg_m, (1 - T)g_i\rangle \cap \mathbb{K}[\mathbf{X}].\end{aligned} \tag{10}$$

As $f, f_1, \ldots, f_k, g_1, \ldots, g_m \in P(d, d')$, we have by Lemma 3.3 that $Tf_1, \ldots, Tf_k, Tfg_1, \ldots, Tfg_m, (1 - T)g_1, \ldots, (1 - T)g_m$ are in $P(2d + 1, d_0)$ for some $d_0 = O_{d,d',n}(1)$. By (10) and Lemma 3.13, for $i \in [m]$, I_i has a Gröbner basis $G_i \subseteq P(d_1, d_2)$ with $d_1 = O_{d,n}(1)$ and $d_2 = O_{d,d',n}(1)$.

Consider $i \in [m]$. The polynomials in G_i are all divisible by g_i since $I_i \subseteq \langle g_i\rangle$. Let $\frac{1}{g_i}G_i = \{\frac{g}{g_i} : g \in G_i\}$. Note that $\mathrm{LT}(\frac{1}{g_i}G_i) = \mathrm{LT}(\frac{1}{g_i}I_i)$ since $\mathrm{LT}(G_i) = \mathrm{LT}(I_i)$. So $\frac{1}{g_i}G_i$ is a Gröbner basis of the ideal $\frac{1}{g_i}I_i$. By Lemma 3.6, $\frac{1}{g_i}G_i \subseteq P(d_1, d_3)$ for some $d_3 = O_{d,d',n}(1)$.

By [AL94, Exercise 2.3.8], we have

$$\bigcap_{i=1}^{m} \frac{1}{g_i} I_i = I^* \cap \mathbb{K}[\mathbf{X}] \tag{11}$$

where

$$I^* := \left\langle 1 - \sum_{i=1}^{m} T_i \right\rangle + T_1 \cdot \frac{1}{g_1} I_1 + \cdots + T_m \cdot \frac{1}{g_m} I_m \subseteq \mathbb{K}[\mathbf{X}, T_1, \ldots, T_m].$$

The ideal I^* has the set of generators $\{1 - \sum_{i=1}^{m} T_i\} \cup \{T_i \cdot g : g \in \frac{1}{g_i} G_i, i \in [m]\}$. These generators are in $P(d_1 + 1, d_3)$ as $\frac{1}{g_i} G_i \subseteq P(d_1, d_3)$. By (11) and Lemma 3.13, $\bigcap_{i=1}^{m} \frac{1}{g_i} I_i$ has a Gröbner basis contained in $P(D, D')$, where $D = O_{d,n}(1)$ and $D' = O_{d,d',n}(1)$. Finally, by (8) and (9), we know that $\bigcap_{i=1}^{m} \frac{1}{g_i}$ is the preimage $\widehat{c \cdot \mathrm{Id}_A(J)}$ of $c \cdot \mathrm{Id}_A(J)$ under the natural quotient map $\mathbb{K}[\mathbf{X}] \to A$, concluding the proof. □

4 Normalization of Curves

In this section, we essentially present a constructive normalization procedure for affine curves, following the framework of Trager [Tra84], which itself is a function field analog of an algorithm by Ford and Zassenhaus [For78]. The core idea is to start with a subring of the coordinate ring of the curve and iteratively adjoin elements until the ring becomes integrally closed. These elements are identified by computing the idealizer of certain ideals.

We revisit these arguments primarily because the bounds on coefficient complexity that we need are not provided in Trager [Tra84] or other literature. Moreover, our treatment differs in several respects from that of Trager. In particular, Trager uses a different method for computing the idealizer, which imposes restrictions on the characteristic of the base field. In contrast, our method uses Gröbner bases and is characteristic-free.

Throughout this section, let $\mathbb{K} = \mathbb{F}(\mathbf{Y}) = \mathbb{F}(Y_1, \ldots, Y_\ell)$, where $\mathbb{F}$ is an infinite field.

4.1 Orders, Integral Bases, and Discriminants

In this subsection, let $\mathbb{L}$ be a finite separable extension of $\mathbb{K}(X)$ of degree s. Denote by $\mathcal{O}_{\mathbb{L}}$ the integral closure of $\mathbb{K}[X]$ in $\mathbb{L}$.

Orders. A subring $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{L}}$ is said to be a $(\mathbb{K}[X], \mathbb{L})$-order if it is a finite $\mathbb{K}[X]$-module and $\mathcal{O} \otimes_{\mathbb{K}[X]} \mathbb{K}(X) = \mathbb{L}$ (i.e., the elements in $\mathcal{O}$ span $\mathbb{L}$ over $\mathbb{K}(X)$).

Integral bases. It is known that every $(\mathbb{K}[X], \mathbb{L})$-order is a free $\mathbb{K}[X]$-module of rank $[\mathbb{L} : \mathbb{K}(X)] = s$. For a $(\mathbb{K}[X], \mathbb{L})$-order $\mathcal{O}$, we say $\mathbf{b} = (b_1, \ldots, b_s) \in \mathcal{O}^s$ is an *integral basis* of $\mathcal{O}$ if $b_1, \ldots, b_s$ form a basis of $\mathcal{O}$ over $\mathbb{K}[X]$.

Discriminants. Let $\mathbf{b} = (b_1, \ldots, b_s) \in \mathbb{L}^s$. As $\mathbb{L}/\mathbb{K}(X)$ is separable, by Galois theory, $\mathbb{L}$ has s distinct embeddings $\sigma_1, \ldots, \sigma_s$ into the Galois closure of $\mathbb{L}$ over $\mathbb{K}(X)$. The *discrminiant* of $\mathbf{b}$ is

defined to be

$$\mathrm{disc}(\mathbf{b}) = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_s) \\ \sigma_2(b_1) & \sigma_2(b_2) & \cdots & \sigma_2(b_s) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_s(b_1) & \sigma_d(b_2) & \cdots & \sigma_s(b_s) \end{pmatrix}^2.$$

It is fixed by the Galois group of $\mathbb{L}$ over $\mathbb{K}(X)$, and hence is an element of $\mathbb{K}(X)$.

We also need the definition of the discriminant of a univariate polynomial. For simplicity, we only give the definition for univariate monic polynomials. Let $f(T) = \sum_{i=0}^{d} a_i T^i \in R[T]$ be a univariate monic (i.e., $a_d = 1$) polynomial of degree d over a ring R. The *discriminant* $\mathrm{disc}(f)$ of f is defined to be $(-1)^{d(d-1)/2}\mathrm{Res}(f, f') \in R$, where $\mathrm{Res}(f, f')$ denotes the resultant of f and $f' = \sum_{i=0}^{d-1}(i+1)a_{i+1}T^i$, given by

$$\mathrm{Res}(f, f') = \det \begin{pmatrix} a_d & a_{d-1} & a_{d-2} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_d & a_{d-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_d & a_{d-1} & a_{d-2} & \cdots & a_0 \\ da_d & (d-1)a_{d-1} & (d-2)a_{d-2} & \cdots & a_1 & 0 & \cdots & 0 \\ 0 & da_d & (d-1)a_{d-1} & \cdots & 2a_2 & a_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & da_d & (d-1)a_{d-1} & (d-2)a_{d-2} & \cdots & a_1 \end{pmatrix}.$$

The following lemma follows straightforwardly from the definition of $\mathrm{disc}(f)$ and Lemma 3.2.

Lemma 4.1. *Let $R = \mathbb{K}[X]$. Suppose $f \in R[T]$ is in $P_{X,T}(d, d')$ when viewed as a polynomial in both X and T over $\mathbb{K}$. Then $\mathrm{disc}(f) \in P_X(D, D')$ for some $D = O_d(1)$ and $D' = O_{d,d'}(1)$.*

We now list some facts about the discriminant of a tuple, the discriminant of a polynomial, and their relations. These facts can be found in, e.g., [Tra84].

Lemma 4.2. *We have the following facts:*

(1) Let $\mathbf{b} = (b_1, \ldots, b_s) \in \mathbb{L}^s$. Then $\mathrm{disc}(\mathbf{b}) \neq 0$ if and only if $b_1, \ldots, b_s$ are linearly independent over $\mathbb{K}(X)$.

(2) Let $\mathbf{b} = (b_1, \ldots, b_s) \in \mathbb{L}^s$ such that $b_1, \ldots, b_s$ are integral over $\mathbb{K}[X]$. Then $\mathrm{disc}(\mathbf{b}) \in \mathbb{K}[X]$.

(3) Let $\mathbf{b}, \mathbf{b}' \in \mathbb{L}^s$. Suppose $\mathbf{b} = A \cdot \mathbf{b}'$ for some $A \in \mathbb{K}[X]^{s \times s}$, then $\mathrm{disc}(\mathbf{b}) = \det(A)^2 \cdot \mathrm{disc}(\mathbf{b}')$. And $\mathbf{b}$ and $\mathbf{b}'$ generate the same $\mathbb{K}[X]$-module if and only if A is invertible as a matrix over $\mathbb{K}[X]$, i.e., $\det(A) \in \mathbb{K}[X]^\times = \mathbb{K}^\times$.

(4) Suppose $\mathbb{L} = \mathbb{K}(X)(\alpha)$ and $\alpha \in \mathbb{L}$ is integral over $\mathbb{K}[X]$. Let f be the minimal polynomial of α over $\mathbb{K}(X)$, which is a monic polynomial with all coefficients in $\mathbb{K}[X]$ [Mat89, Theorem 9.2]. Then $\mathrm{disc}(1, \alpha, \ldots, \alpha^{s-1}) = \pm\mathrm{disc}(f)$.

Recall that $\mathcal{O}_\mathbb{L}$ denotes the integral closure of $\mathbb{K}[X]$ in $\mathbb{L}$. We have the following statement, whose proof can be found in, e.g., [Eis95, Proof of Proposition 13.14].

Lemma 4.3. *Let $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{L}}$ be a $(\mathbb{K}[X], \mathbb{L})$-order with an integral basis $\mathbf{b}$. Then*

$$\mathcal{O}_{\mathbb{L}} \subseteq \frac{1}{\operatorname{disc}(\mathbf{b})}\mathcal{O} \subseteq \frac{1}{\operatorname{disc}(\mathbf{b})}\mathcal{O}_{\mathbb{L}}.$$

Definition 4.4 (Discriminant ideal)**.** *Let $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{L}}$ be a $(\mathbb{K}[X], \mathbb{L})$-order with an integral basis $\mathbf{b}$. Define $\mathfrak{D}_{\mathcal{O}/\mathbb{K}[X]}$ to be the ideal of $\mathbb{K}[X]$ generated by* $\operatorname{disc}(\mathbf{b})$*, called the* discriminant ideal *of $\mathcal{O}$. By Lemma 4.2(3), $\mathfrak{D}_{\mathcal{O}/\mathbb{K}[X]}$ is well-defined and does not depend on the choice of $\mathbf{b}$.*

The following theorem gives a criterion for $\mathcal{O}$ being integrally closed.

Theorem 4.5 ([Tra84])**.** *$\mathcal{O}$ is integrally closed if and only if the idealizer $\operatorname{Id}_{\mathcal{O}}(\mathfrak{m})$ of every maximal ideal $\mathfrak{m}$ of $\mathcal{O}$ containing $\mathfrak{D}_{\mathcal{O}/\mathbb{K}[X]}$ equals $\mathcal{O}$.*

The next lemma states that taking the idealizer does not introduce non-integral elements.

Lemma 4.6 ([Tra84])**.** *The idealizer $\operatorname{Id}_{\mathcal{O}}(I)$ is contained in the integral closure of $\mathcal{O}$ for any nonzero ideal I of $\mathcal{O}$.*

4.2 Finding the Integral Closure

The main result of this section is the following theorem.

Theorem 4.7. *Let $f_1, \ldots, f_k \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ be polynomials in $P(d, d')$. Let α be an element in the $\mathbb{F}$-linear span of $X_1, \ldots, X_n$ such that the natural ring homomorphism $\mathbb{K}[\alpha] \to A := \mathbb{K}[\mathbf{X}]/\langle f_1, \ldots, f_k\rangle$ sending α to $\alpha + \langle f_1, \ldots, f_k\rangle$ is injective and makes A a finite $\mathbb{K}[\alpha]$-module. Moreover, suppose the following hold:*

(1) For any algebraic extension $\mathbb{L}$ of $\mathbb{K}$, $A_{\mathbb{L}} := \mathbb{L}[\mathbf{X}]/\langle f_1, \ldots, f_k\rangle$ is an integral domain of Krull dimension one.

(2) $\operatorname{Frac}(A)$ *is a finite separable extension of $\mathbb{K}(\alpha)$.*

Then there exist $D, D', m, k', e \in \mathbb{N}$ and $g_1, \ldots, g_n, h_1, \ldots, h_{k'} \in \mathbb{K}^{(e)}[\mathbf{Z}] = \mathbb{K}^{(e)}[Z_1, \ldots, Z_m]$ such that $D, D', m, k', p^e = O_{d,d',n}(1)$ and the following hold:

(1) $g_1, \ldots, g_n, h_1, \ldots, h_{k'} \in P^{(e)}(D, D')$.

(2) The map

$$\begin{aligned} \phi : A_{\mathbb{K}^{(e)}} &\to \mathbb{K}^{(e)}[\mathbf{Z}]/\langle h_1, \ldots, h_{k'}\rangle \\ X_i + \langle f_1, \ldots, f_k\rangle &\mapsto g_i + \langle h_1, \ldots, h_{k'}\rangle, \quad i = 1, 2, \ldots, n. \end{aligned}$$

defines an injective $\mathbb{K}^{(e)}$-linear ring homomorphism.

(3) $\mathbb{K}^{(e)}[\mathbf{Z}]/\langle h_1, \ldots, h_{k'}\rangle$ is isomorphic to the integral closure of $A_{\mathbb{K}^{(e)}}$, and this isomorphism composed with ϕ is the natural inclusion of $A_{\mathbb{K}^{(e)}}$ in its integral closure.

Remark 1. The subring $\mathbb{K}[\alpha]$ in Theorem 4.7 can be obtained via Noether normalization, though we defer this step to the next section.

Remark 2. The assumptions that $A_{\mathbb{L}}$ is an integral domain and that $\mathrm{Frac}(A)$ is separable over $\mathbb{K}(\alpha)$ are imposed for simplicity; they hold in our setting. It may be possible to eliminate these assumptions, but doing so could require additional tools, such as primary decomposition.

In the following, we adopt the notations and assumptions of Theorem 4.7.

By assumption, $\mathrm{Frac}(A)$ is a finite separable extension of $\mathbb{K}(\alpha)$. We view α as a variable as it is transcendental over $\mathbb{K}$. By the primitive element theorem [ZS75, §II.9, Theorem 19], we can fix $X = \sum_{i=1}^{n} c_i X_i$ with $c_i \in \mathbb{F}$ such that $\overline{X} := X + \langle f_1, \ldots, f_k \rangle$ generates the field $\mathrm{Frac}(A)$ over $\mathbb{K}(\alpha)$. Let $s := [\mathrm{Frac}(A) : \mathbb{K}(\alpha)]$ and $\mathbf{b}_0 = (1, \overline{X}, \ldots, \overline{X}^{s-1})$.

To prove Theorem 4.7, we first prove several lemmas. First, the following lemma bounds the complexity of the discriminant of $\mathbf{b}_0$.

Lemma 4.8. $\mathrm{disc}(\mathbf{b}_0) \in P_\alpha(d_1, d_2)$ *for some* $d_1 = O_{d,n}(1)$ *and* $d_2 = O_{d,d',n}(1)$.

Proof. By assumption, A is a finite $\mathbb{K}[\alpha]$-module. So by Lemma 2.9, it is integral over $\mathbb{K}[\alpha]$. Therefore, by Lemma 4.2 (4), the minimal polynomial F of $\overline{X}$ over $\mathbb{K}(\alpha)$ is a monic polynomial over $\mathbb{K}[\alpha]$, and $\mathrm{disc}(\mathbf{b}_0) = \pm\mathrm{disc}(F)$.

We first find F as follows: Introduce new variables T and Z. Let $\preceq_{T,Z}$ be the elimination order for T on $\mathcal{M}_{T,Z}$. Let $\preceq = (\preceq_{\mathbf{X}}, \preceq_{T,Z})$ be an elimination order for $\mathbf{X}$ on $\mathcal{M}_{\mathbf{X},T,Z}$. Let G be a Gröbner basis for the ideal $I = \left\langle f_1, \ldots, f_k, T - \overline{X}, Z - \alpha \right\rangle$ of $\mathbb{K}[\mathbf{X}, T, Z]$ with respect to $\preceq$. By Lemma 3.10, we may assume $G \subseteq P(d_3, d_4)$ for some $d_3 = O_{d,n}(1)$ and $d_4 = O_{d,d',n}(1)$. By Lemma 3.12, $G \cap \mathbb{K}[T, Z]$ is a Gröbner basis for $I \cap \mathbb{K}[T, Z]$ with respect to $\preceq_{T,Z}$. Choose some $g \in G \cap \mathbb{K}[T, Z]$ such that $\mathrm{LM}(g)$ has the form mT^e, where $m \in \mathcal{M}_Z$ and e is minimized. We actually have $m = 1$ since F is monic over $\mathbb{K}[\alpha]$. Let $u \in \mathbb{K}^\times$ be the leading coefficient of g. Then $u^{-1}g(T, \alpha) \in (\mathbb{K}[\alpha])[T]$ equals the minimal polynomial F of $\overline{X}$ over $\mathbb{K}[\alpha]$. By Lemma 3.2, $F \in P_{T,\alpha}(d_3, d_5)$ for some $d_5 = O_{d,d',n}(1)$. Finally, by Lemma 4.1, we have $\mathrm{disc}(\mathbf{b}_0) = \pm\mathrm{disc}(F) \in P_\alpha(d_1, d_2)$, where $d_1 = O_{d,n}(1)$ and $d_2 = O_{d,d',n}(1)$. □

For an algebraic extension $\mathbb{L}$ of $\mathbb{K}$, we denote by $I_{\mathbb{L}}$ the ideal $\langle f_1, \ldots, f_k \rangle$ of $\mathbb{L}[\mathbf{X}]$. The following lemma shows how to use a ring homomorphism to describe an order.

Lemma 4.9. *Let* $\mathbb{L}$ *be an algebraic extension of* $\mathbb{K}$. *Let* $a_1, \ldots, a_t \in \mathbb{L}[\mathbf{X}]$. *Assume that the elements* $\frac{a_1 + I_{\mathbb{L}}}{\mathrm{disc}(\mathbf{b}_0)}, \ldots, \frac{a_t + I_{\mathbb{L}}}{\mathrm{disc}(\mathbf{b}_0)} \in (A_{\mathbb{L}})_{\mathrm{disc}(\mathbf{b}_0)}$ *generate an algebra* $\mathcal{O}$ *over* $\mathbb{L}[\alpha]$ *that is a* $(\mathbb{L}[\alpha], \mathrm{Frac}(A_{\mathbb{L}}))$*-order. Also assume* $a_1, \ldots, a_t \in P(d_1, d_2)$. *Then there exist* $r_1, \ldots, r_{t+1} \in \mathbb{L}[\mathbf{X}, U]$ *and* $h_1, \ldots, h_{k'} \in \mathbb{L}[\mathbf{Z}] = \mathbb{L}[Z_1, \ldots, Z_{t+1}]$, *where* $k' = O_{d,d_1,n}(1)$, *such that the following hold:*

(1) $r_1, \ldots, r_{t+1} \in P_{\mathbf{X},U}(d_1 + 1, d_2)$ *and* $h_1, \ldots, h_{k'} \in P_{\mathbf{Z}}(d_3, d_4)$ *for some* $d_3 = O_{d,d_1,n}(1)$ *and* $d_4 = O_{d,d',d_1,d_2,n}(1)$. *Moreover,* $r_{t+1} = \alpha$.

(2) The map

$$\psi : \mathbb{L}[\mathbf{Z}] / \langle h_1, \ldots, h_{k'} \rangle \to \mathbb{L}[\mathbf{X}, U] / \langle f_1, \ldots, f_k, \mathrm{disc}(\mathbf{b}_0) \cdot U - 1 \rangle \cong A_{\mathbb{L}}[U] / \langle \mathrm{disc}(\mathbf{b}_0) \cdot U - 1 \rangle$$
$$Z_i + \langle h_1, \ldots, h_{k'} \rangle \mapsto r_i + \langle f_1, \ldots, f_k, \mathrm{disc}(\mathbf{b}_0) \cdot U - 1 \rangle, \quad i = 1, 2, \ldots, t+1.$$

defines an injective $\mathbb{L}$*-linear ring homomorphism.*

(3) Let

$$\theta : A_{\mathbb{L}}[U] / \langle \mathrm{disc}(\mathbf{b}_0) \cdot U - 1 \rangle \to (A_{\mathbb{L}})_{\mathrm{disc}(\mathbf{b}_0)}$$

be the $A_{\mathbb{L}}$*-linear ring isomorphism sending* $U + \langle \mathrm{disc}(\mathbf{b}_0) \cdot U - 1 \rangle$ *to* $1/\mathrm{disc}(\mathbf{b}_0)$ *given by Fact 2.5. Then the image of* $\theta \circ \psi$ *is* $\mathcal{O}$.

Proof. By assumption, $\frac{a_1+I_{\mathbb{L}}}{\operatorname{disc}(\mathbf{b}_0)}, \ldots, \frac{a_t+I_{\mathbb{L}}}{\operatorname{disc}(\mathbf{b}_0)}$ and α generate the algebra $\mathcal{O}$ over $\mathbb{L}$. Let $r_i = a_i \cdot U$ for $i \in [t]$ and $r_{t+1} = \alpha$. Then $r_1, \ldots, r_{t+1} \in P_{\mathbf{X},U}(d_1+1, d_2)$.

Identifying $\mathbb{L}[\mathbf{X}, U]/\langle f_1, \ldots, f_k, \operatorname{disc}(\mathbf{b}_0) \cdot U - 1\rangle$ with $(A_{\mathbb{L}})_{\operatorname{disc}(\mathbf{b}_0)}$ via θ, we see that the image of the map $\mathbb{L}[\mathbf{Z}] \to \mathbb{L}[\mathbf{X}, U]/\langle f_1, \ldots, f_k, \operatorname{disc}(\mathbf{b}_0) \cdot U - 1\rangle$ sending Z_i to $r_i + \langle f_1, \ldots, f_k, \operatorname{disc}(\mathbf{b}_0) \cdot U - 1\rangle$ for $i \in [t+1]$ is precisely $\mathcal{O}$. The kernel of this map is generated by a collection of polynomials $h_1, \ldots, h_{k'} \in \mathbb{L}[\mathbf{Z}]$. Note that we may assume $t \leq \binom{n+d_1}{d_1}$. By Lemma 3.18 and Lemma 4.8, we may choose $h_1, \ldots, h_{k'}$ to be in $P_{\mathbf{Z}}(d_3, d_4)$ for sufficiently large $d_3 = O_{d,d_1,n}(1)$ and $d_4 = O_{d,d',d_1,d_2,n}(1)$. We may also assume $k' \leq \binom{n+d_3}{d_3} = O_{d,d_1,n}(1)$. □

The next lemma constructively identifies integral elements that can be adjoined to a non-integrally closed order $\mathcal{O}$ to obtain a larger one.

Lemma 4.10. *Let $e \geq 0$ be an integer and let $\mathbb{L} = \mathbb{K}^{(e)}$. Let $a_1, \ldots, a_t \in \mathbb{L}[\mathbf{X}]$. Assume $\frac{a_1+I_{\mathbb{L}}}{\operatorname{disc}(\mathbf{b}_0)}, \ldots, \frac{a_t+I_{\mathbb{L}}}{\operatorname{disc}(\mathbf{b}_0)}$ generate an algebra $\mathcal{O}$ over $\mathbb{L}[\alpha]$ that is a $(\mathbb{L}[\alpha], \operatorname{Frac}(A_{\mathbb{L}}))$-order. Also assume $a_1, \ldots, a_t \in P^{(e)}(d_1, d_2)$. Then there exist d_3, d_4, and $e' \geq e$ such that $p^{e'}, d_3, d_4 = O_{d,d',d_1,d_2,n,p^e}(1)$, and one of the following is true:*

(1) $\mathcal{O}$ is integrally closed.

(2) There exists $a_{t+1} \in P^{(e')}(d_3, d_4)$ such that $\frac{a_1+I_{\mathbb{L}'}}{\operatorname{disc}(\mathbf{b}_0)}, \ldots, \frac{a_{t+1}+I_{\mathbb{L}'}}{\operatorname{disc}(\mathbf{b}_0)}$ generate an algebra $\mathcal{O}'$ over $\mathbb{L}'[\alpha]$ that is a $(\mathbb{L}'[\alpha], \operatorname{Frac}(A_{\mathbb{L}'}))$-order strictly larger than $\mathcal{O} \otimes_{\mathbb{L}} \mathbb{L}'$, where $\mathbb{L}' = \mathbb{K}^{(e')}$.

Proof. Assume that $\mathcal{O}$ is not integrally closed. We will prove that Item 2 holds.

By Lemma 4.9, there exist $r_1, \ldots, r_{t+1} \in P^{(e)}_{\mathbf{X},U}(d_5, d_6)$ and $h_1, \ldots, h_{k'} \in P^{(e)}_{\mathbf{Z}}(d_5, d_6)$ for some $d_5 = O_{d,d_1,n}(1)$ and $d_6 = O_{d,d',d_1,d_2,n}(1)$ such that $r_{t+1} = \alpha$, the ring homomorphism

$$\begin{aligned}\psi : \mathbb{L}[\mathbf{Z}]/\langle h_1, \ldots, h_{k'}\rangle &\to \mathbb{L}[\mathbf{X}, U]/\langle f_1, \ldots, f_k, \operatorname{disc}(\mathbf{b}_0) \cdot U - 1\rangle \\ Z_i + \langle h_1, \ldots, h_{k'}\rangle &\mapsto r_i + \langle f_1, \ldots, f_k, \operatorname{disc}(\mathbf{b}_0) \cdot U - 1\rangle, \quad i = 1, 2, \ldots, t+1.\end{aligned}$$

is injective, and the image of ψ equals $\mathcal{O}$ if we identify $\mathbb{L}[\mathbf{X}, U]/\langle f_1, \ldots, f_k, \operatorname{disc}(\mathbf{b}_0) \cdot U - 1\rangle$ with $(A_{\mathbb{L}})_{\operatorname{disc}(\mathbf{b}_0)}$.

By Lemma 4.2 (3), the discriminant ideal $\mathfrak{D}_{\mathcal{O}/\mathbb{L}[\alpha]}$ is generated by some factor $Q(\alpha) \in \mathbb{L}[\alpha]$ of $\operatorname{disc}(\mathbf{b}_0)$ and is not the unital ideal. So by Lemma 4.8 and Lemma 3.3, $Q \in P^{(e)}(d_7, d_8)$ for some $d_7 = O_{d,n}(1)$ and $d_8 = O_{d,d',n,p^e}(1)$. Identify $\mathbb{L}[\mathbf{Z}]/\langle h_1, \ldots, h_{k'}\rangle$ with $\mathcal{O}$. Then $Q(Z_{t+1}) + \langle h_1, \ldots, h_{k'}\rangle$ is identified with $Q(\alpha)$ since $r_{t+1} = \alpha$. As $\mathcal{O}$ is an integral domain of Krull dimension one and $\mathfrak{D}_{\mathcal{O}/\mathbb{L}[\alpha]}$ is not the unital ideal, we know $\mathfrak{D}_{\mathcal{O}/\mathbb{L}[\alpha]} = \langle Q(\alpha)\rangle$ is a zero-dimensional ideal of $\mathcal{O}$.

For each maximal ideal $\mathfrak{m}$ of $\mathcal{O}$ containing $Q(\alpha)$, let $e_{\mathfrak{m}}$ be the largest nonnegative integer such that $p^{e_{\mathfrak{m}}}$ divides $[\mathcal{O}/\mathfrak{m} : \mathbb{L}]$. Let e_0 be the maximum of $e_{\mathfrak{m}}$ over all maximal ideals $\mathfrak{m}$ of $\mathcal{O}$ containing $Q(\alpha)$. By Lemma 2.14, we have $p^{e_0} \leq \max(\deg(Q), \deg(h_1), \ldots, \deg(h_{k'}))^{t+1}$, where t may be assumed to be at most $\binom{n+d_1}{d_1}$. So $p^{e_0} = O_{d,d_1,n,p^e}(1)$. Let $e' = e + e_0$ and $\mathbb{L}' = \mathbb{K}^{(e')}$. Then $p^{e'} = O_{d,d_1,n,p^e}(1)$.

By Lemma 2.2 and the fact that $\mathbb{F}$ is algebraically closed, any maximal ideal of $\mathcal{O} \otimes_{\mathbb{L}} \mathbb{L}'$ containing $Q(\alpha)$ is separable over $\mathbb{L}'$. As $\mathcal{O}$ is not integrally closed, neither is $\mathcal{O} \otimes_{\mathbb{L}} \mathbb{L}'$. This follows from Lemma 2.7 and the fact that $\mathcal{O} \otimes_{\mathbb{L}} \mathbb{L}'$ is integral over $\mathcal{O}$. Then by Theorem 4.5 and Lemma 4.6, $\mathcal{O} \otimes_{\mathbb{L}} \mathbb{L}'$ has a maximal ideal $\mathfrak{m}$ containing $Q(\alpha)$ whose idealizer $\operatorname{Id}_{\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}'}(\mathfrak{m})$ is integral over $\mathcal{O} \otimes_{\mathbb{L}} \mathbb{L}'$ and strictly larger than it.

We now find an element in $\mathrm{Id}_{\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}'}(\mathfrak{m}) \setminus (\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}')$. Let $c = Q(Z_{t+1}) + \langle h_1,\dots,h_{k'}\rangle \in \mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle$. View $\mathfrak{m}$ as a maximal ideal of $\mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle$ containing c. Let $\widetilde{\mathfrak{m}}$ be the preimage of $\mathfrak{m}$ in $\mathbb{L}'[\mathbf{Z}]$ under the natural quotient map, which is also maximal. As $(\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}')/\mathfrak{m}$ is separable, by Lemma 3.20, $\widetilde{\mathfrak{m}}$ is generated by polynomials in $P^{(e')}(d_9, d_{10})$ where $d_9 = O_{d,d_1,n}(1)$ and $d_{10} = O_{d,d',d_1,d_2,n,p^e}(1)$.

As $Q(\alpha)$ generates $\mathfrak{D}_{\mathcal{O}/\mathbb{L}[\alpha]}$, identifying $\mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle$ with $\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}'$ and applying Lemma 4.3 and Lemma 4.6 shows that $c\cdot \mathrm{Id}_{\mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle}(\mathfrak{m}) \subseteq \mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle$. Let $J \subseteq \mathbb{L}'[\mathbf{Z}]$ be the preimage of $c\cdot \mathrm{Id}_{\mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle}(\mathfrak{m})$ under the natural quotient map $\mathbb{L}'[\mathbf{Z}] \to \mathbb{L}'[\mathbf{Z}]/\langle h_1,\dots,h_{k'}\rangle$. By Lemma 3.21, J has a Gröbner basis G_1 contained in $P^{(e')}(d_{11}, d_{12})$, where $d_{11} = O_{d,d_1,n}(1)$ and $d_{12} = O_{d,d',d_1,d_2,n,p^e}(1)$.

As $\mathrm{Id}_{\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}'}(\mathfrak{m})$ is strictly larger than $\mathcal{O}\otimes_{\mathbb{L}}\mathbb{L}'$, G_1 contains an element $\gamma \in \mathbb{L}'[\mathbf{Z}]$ such that the image of $\gamma + \langle h_1,\dots,h_{k'}\rangle$ in $(A_{\mathbb{L}'})_{\mathbf{b}_0} \cong \mathbb{L}'[\mathbf{X},U]/\langle f_1,\dots,f_k,\mathrm{disc}(\mathbf{b}_0)\cdot U-1\rangle$ is the desired $a_{t+1}+I_{\mathbb{L}'}$. However, to find a_{t+1}, we cannot simply map each Z_i to r_i and let $a_{t+1} = \gamma(r_1,\dots,r_{t_1})$, as the variable U may appear in a_{t+1}. Instead, we choose a Gröbner basis G_2 of the ideal $\langle f_1,\dots,f_k,\mathrm{disc}(\mathbf{b}_0)\cdot U-1\rangle$ of $\mathbb{L}'[\mathbf{X},U]$ with respect to $\preceq$, where $\preceq$ is an elimination order for U on $\mathcal{M}_{\mathbf{X},U}$ that is degree-compatible in the $\mathbf{X}$ variables. Then we choose a_{t+1} to be the remainder of $\gamma(r_1,\dots,r_{t_1})$ modulo G_2 with respect to $\preceq$. The resulting a_{t+1} is in $\mathbb{L}'[\mathbf{X}]$ and also in $P^{(e')}(d_3,d_4)$ for some $d_3 = O_{d,d_1,n}(1)$ and $d_4 = O_{d,d',d_1,d_2,n,p^e}(1)$ by Lemma 3.13 and Lemma 3.17. □

Now we are ready to prove Theorem 4.7.

Proof of Theorem 4.7. We start from the order $\mathcal{O}_0$ generated by $\overline{X}$ over $\mathbb{K}[\alpha]$. In the i-th step, we use Lemma 4.10 to add a generator, replacing an $(\mathbb{K}^{(e_{i-1})}[\alpha], \mathrm{Frac}(A_{\mathbb{K}^{e_{i-1}}}))$-order $\mathcal{O}_{i-1}$ by a $(\mathbb{K}^{(e_i)}[\alpha], \mathrm{Frac}(A_{\mathbb{K}^{e_i}}))$-order $\mathcal{O}_i$, until we obtain an order that is integrally closed. Suppose this process terminates after τ steps. So $\mathcal{O}_\tau$ is integrally closed. For $i = 0,1,\dots,\tau$, the generators of $\mathcal{O}_i$ are represented by elements $\alpha_1,\dots,\alpha_{i+1} \in \mathbb{K}^{(e_i)}[\mathbf{X}]$ that are in $P^{(e_i)}(d_i, d_i')$.

By Lemma 4.10, the parameters d_i, d_i', p^{e_i} satisfies

$$d_0, d_0', p^{e_0} = O_{d,d',n}(1)$$

and

$$d_i, d_i', p^{e_i} \le F_{d,d',n}(d_{i-1}, d_{i-1}', p^{e_{i-1}}) \quad \text{for } i > 0.$$

where $F_{d,d',n}$ is some non-decreasing function depending only on d, d', and n. Define $F(0) = \max(d_0, d_0', p^{e_0})$ and $F(i) = F_{d,d',n}(F(i-1), F(i-1), F(i-1))$. Then $d_i, d_i', p^{e_i} \le F(i)$.

By Lemma 4.2 (3), replacing $\mathcal{O}_{i-1}$ by $\mathcal{O}_i$ decreases the degree of the generator of the discriminant ideal by at least two. So by Lemma 4.8, it takes $\tau \le \deg_\alpha(\mathrm{disc}(\mathbf{b}_0))/2 = O_{d,n}(1)$ steps before an integrally closed order is found. Therefore, the final parameters d_τ, d_τ', and p^{e_τ} are bounded by $F(\tau) = O_{d,d',n}(1)$.

Note that $\mathcal{O}_\tau$ equals the integral closure of $A_{\mathbb{K}^{(e_\tau)}}$. This follows from Corollary 2.8 and the fact that $A_{\mathbb{K}^{(e_\tau)}}$ is integral over $\mathbb{K}[\alpha]$.

To find the polynomials g_i, use the map ψ associated with $\mathcal{O}_\tau$ given by Lemma 4.9, and then use Lemma 3.18 (3) to compute the inverse of $X_i + \langle f_1,\dots,f_k,\mathrm{disc}(\mathbf{b}_0)\cdot U-1\rangle$ under ψ for $i \in [n]$.

Finally, the parameter m in Theorem 4.7 equals $t+1 = \tau+2$, where $t = \tau+1$ is the the number of elements $a_1,\dots,a_t$ corresponding to the generators of $\mathcal{O}_\tau$ as an algebra over $\mathbb{K}^{(e_\tau)}[\alpha]$. As $a_1,\dots,a_t \in P^{(e_\tau)}(d_\tau, d_\tau')$ with $d_\tau = O_{d,d',n}(1)$, we may assume $m = O_{d,d',n}(1)$. □

5 PIT via Normalization

In this section, let $\mathbb{F}$ be a field and let $\mathbb{K} = \mathbb{F}(\mathbf{Y}) = \mathbb{F}(Y_{0,1}, \dots Y_{0,n}, Y_{1,1}, \dots, Y_{1,n}, Y_{2,1}, \dots, Y_{2,n})$.

5.1 Restricting to a Generic Affine Plane

We start by discussing the algebra resulting from restricting to a generic affine plane.

Definition 5.1 (Restriction to a generic affine plane)**.** *For $f \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \dots, X_n]$ be a polynomial over a field $\mathbb{F}$, define* $\mathrm{res}(f)$ *to be the polynomial*

$$f\left(Y_{0,1} + Y_{1,1}Z_1 + Y_{2,1}Z_2, \dots, Y_{0,n} + Y_{1,n}Z_1 + Y_{2,n}Z_2\right) \in \mathbb{F}[\mathbf{Y}][Z_1, Z_2] \subseteq \mathbb{K}[Z_1, Z_2]. \tag{12}$$

Lemma 5.2. *Let $n \geq 2$. Suppose $\mathbb{F}$ is algebraically closed and $f \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \dots, X_n]$ is irreducible over $\mathbb{F}$. Then* $\mathrm{res}(f) \in \mathbb{K}[\mathbf{Z}]$ *is absolutely irreducible over $\mathbb{K} = \mathbb{F}(\mathbf{Y})$.*

For a proof of Lemma 5.2, see [Kal95, Lemma 7].[6]

Lemma 5.3. *Let $n \geq 2$. Suppose $\mathbb{F}$ is algebraically closed and $f \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \dots, X_n]$ is an irreducible polynomial over $\mathbb{F}$ of degree $d > 0$. Let $\mathbb{L}$ be an algebraic extension of $\mathbb{K} = \mathbb{F}(\mathbf{Y})$. Then $\mathbb{L}[Z_1, Z_2]/\langle \mathrm{res}(f) \rangle$ is an integral domain. Moreover, for every $(c_1, c_2) \in (\mathbb{F}^\times)^2$, the field of fractions $\mathbb{E}$ of $\mathbb{L}[Z_1, Z_2]/\langle \mathrm{res}(f) \rangle$ is a finite separable extension of $\mathbb{L}(\overline{X}_{c_1,c_2})$, where $\overline{X}_{c_1,c_2} := c_1Z_1 + c_2Z_2 + \langle \mathrm{res}(f) \rangle \in \mathbb{L}[Z_1, Z_2]/\langle \mathrm{res}(f) \rangle \subseteq \mathbb{E}$.*

Proof. By Lemma 5.2, $\mathrm{res}(f)$ is absolutely irreducible over $\mathbb{K}$. So it is irreducible over $\mathbb{L}$. Therefore, $\mathbb{L}[Z_1, Z_2]/\mathrm{res}(f)$ is an integral domain.

Consider $(c_1, c_2) \in (\mathbb{F}^\times)^2$ and let $X_{c_1,c_2} := c_1Z_1 + c_2Z_2$. Then $Z_2 = c_2^{-1}(X_{c_1,c_2} - c_1Z_1)$. So $\mathbb{L}[Z_1, Z_2] = \mathbb{L}[Z_1, X_{c_1,c_2}]$. Performing the substitution $Z_2 = c_2^{-1}(X_{c_1,c_2} - c_1Z_1)$ in (12), we have

$$\mathrm{res}(f) = f(T_1, \dots, T_n),$$

where

$$T_i := Y_{0,i} + Y_{1,i}Z_1 + c_2^{-1}Y_{2,i}(X_{c_1,c_2} - c_1Z_1), \quad i = 1, 2, \dots, n \tag{13}$$

View $\mathrm{res}(f)$ as a univariate polynomial in Z_1 over $\mathbb{L}[X_{c_1,c_2}]$ (which is fine as Z_1 and X_{c_1,c_2} are algebraically independent). Its derivative, which we denote by $D_{\mathrm{res}(f)}$, can be determined by the chain rule:

$$D_{\mathrm{res}(f)} = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(T_1, \dots, T_n)\frac{\partial T_i}{\partial Z_1} = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(T_1, \dots, T_n) \cdot (Y_{1,i} - c_2^{-1}c_1Y_{2,i}). \tag{14}$$

As $\mathbb{F}$ is algebraically closed (and hence a perfect field) and f is irreducible over $\mathbb{F}$, we know $\frac{\partial f}{\partial X_i} \neq 0$ for some $i \in [n]$. Choose $i_0 \in [n]$ and a monomial $m = \prod_{i=1}^{n} X_i^{e_i}$ that appears in $\frac{\partial f}{\partial X_{i_0}}$ such that $\deg_{\mathbf{X}}(m)$ is maximized over all choices of i_0 and m. Then by (13) and (14), $D_{\mathrm{res}(f)}$, viewed as a

[6] The statement [Kal95, Lemma 7] is slightly different, where the expression $Y_{0,1}+Y_{1,1}Z_1+Y_{2,1}Z_2$ in (12) is replaced by $Y_{0,1}+Z_1$, resulting another polynomial φ_2. However, the proof can be adapted to prove Lemma 5.2. Alternatively, we can recover (12) from φ_2 by performing the invertible $\mathbb{K}$-linear variable substitution $Z_1 \mapsto Y_{1,1}Z_1+Y_{2,1}Z_2$, followed by applying the field automorphism of $\mathbb{K}$ that maps $Y_{1,i} \mapsto Y_{1,i}/Y_{1,1}$ and $Y_{2,i} \mapsto Y_{2,i} - Y_{2,1}Y_{1,i}/Y_{1,1}$ for $i \in [n] \setminus \{1\}$. Both transformations preserve absolute irreducibility.

polynomial in $\mathbf{Y}$, Z_1, and X_{c_1,c_2} over $\mathbb{F}$, has a monomial $X_{c_1,c_2}^{\deg_{\mathbf{X}}(m)} \left(\prod_{i=1}^{n} Y_{2,i}^{e_i}\right) Y_{1,i_0}$ that comes from the term $\frac{\partial f}{\partial X_{i_0}}(T_1,\ldots,T_n)\cdot Y_{1,i_0}$ in (14) and is not canceled by other monomials. So $D_{\mathrm{res}(f)} \neq 0$.

As the degree of $D_{\mathrm{res}(f)}$ is smaller than that of $\mathrm{res}(f)$, both viewed as univariate polynomials in Z_1 over $\mathbb{L}[X_{c_1,c_2}]$, we have $D_{\mathrm{res}(f)} \notin \langle \mathrm{res}(f)\rangle$.

Let $f_d = f_d(X_1,\ldots,X_n)$ be the homogeneous degree-d component of f, where $d = \deg(f)$. View $\mathrm{res}(f)$ as a univariate polynomial in Z_1 over $\mathbb{L}[X_{c_1,c_2}]$. Then we can write $\mathrm{res}(f) = \sum_{i=0}^{d} a_i Z_1^i$, where $a_i \in \mathbb{L}[X_{c_1,c_2}]$. By (13), we have

$$a_d = f_d(Y_{1,1} - c_2^{-1}c_1 Y_{2,1},\ldots,Y_{1,n} - c_2^{-1}c_1 Y_{2,n}) \neq 0$$

We also have $a_d \notin \langle \mathrm{res}(f)\rangle$ as $d > 0$ and a_d is independent of Z_1.

Note that $\mathbb{L}[X_{c_1,c_2}] \cap \langle \mathrm{res}(f)\rangle = 0$ since $d > 0$. So we have an inclusion

$$\mathbb{L}[X_{c_1,c_2}] \cong \mathbb{L}[X_{c_1,c_2}]/(\mathbb{L}[X_{c_1,c_2}] \cap \langle \mathrm{res}(f)\rangle) \hookrightarrow \mathbb{L}[Z_1,Z_2]/\langle \mathrm{res}(f)\rangle$$

Taking the fields of fractions, we see that $\mathbb{L}(X_{c_1,c_2})$ may be identified with $\mathbb{L}(\overline{X}_{c_1,c_2}) \subseteq \mathbb{E}$. And the minimal polynomial of Z_1 over $\mathbb{L}(X_{c_1,c_2})$ is $F(T) := \sum_{i=1}^{d}(a_i/a_d)T^d \in \mathbb{L}(X_{c_1,c_2})[T]$. We also have $F'(Z_1 + \langle \mathrm{res}(f)\rangle) = (D_{\mathrm{res}(f)} + \langle \mathrm{res}(f)\rangle)/(a_d + \langle \mathrm{res}(f)\rangle) \neq 0$ since $a_d, D_{\mathrm{res}(f)} \notin \langle \mathrm{res}(f)\rangle$. It follows that $Z_1 + \langle \mathrm{res}(f)\rangle \in \mathbb{E}$ is separable over $\mathbb{L}(\overline{X}_{c_1,c_2})$. A symmetric argument shows that $Z_2 + \langle \mathrm{res}(f)\rangle \in \mathbb{E}$ is separable over $\mathbb{L}(\overline{X}_{c_1,c_2})$. As $\mathbb{E}$ is generated by $Z_1 + \langle \mathrm{res}(f)\rangle$ and $Z_2 + \langle \mathrm{res}(f)\rangle$, we conclude that that $\mathbb{E}$ is a finite separable extension of $\mathbb{L}(\overline{X}_{c_1,c_2})$. □

5.2 Proof of the Main Theorem

For convenience, we state our main theorem again.

Theorem 5.4 (Main theorem, homogeneous version)**.** *Let $C_{n,d,k,\delta,\mathbb{F}}$ be the set of polynomials $F \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1,\ldots,X_n]$ over a field $\mathbb{F}$ satisfying the following conditions:*

(1) F can be expressed as a sum $F = \sum_{i=0}^{k_0-1} F_i$, where $k_0 \leq k$, $F_i = \prod_{j=1}^{m_i} f_{i,j}$ for $i \in \{0,1,\ldots,k_0-1\}$, and each $f_{i,j} \in \mathbb{F}[\mathbf{X}]$ is a nonzero homogeneous polynomial of degree at most δ.

(2) $\deg(F_i) = d_0$ for some $d_0 \leq d$ and all $i \in \{0,1,\ldots,k_0-1\}$.

(3) F_i is squarefree for some $i \in \{0,1,\ldots,k_0-1\}$, meaning that the irreducible factors of F_i over $\overline{\mathbb{F}}$ are distinct.

Then there exists an explicit $(nd)^{O_\delta(1)}$-sized hitting set $\mathcal{H} \subseteq \overline{\mathbb{F}}^n$ for $C_{n,d,3,\delta,\mathbb{F}}$.

Assumptions. We make some further assumptions to simplify the discussion, and briefly justify them:

(1) F is non-constant. Otherwise, any set will be a hitting set for F by definition.

(2) $\mathbb{F}$ is algebraically closed. This can be guaranteed by extending $\mathbb{F}$ to $\overline{\mathbb{F}}$.

(3) $k_0 = 3$. This is because Theorem 5.4 is known to hold when $k_0 = 1$ or $k_0 = 2$ even without the condition of squarefreeness. So $F = F_0 + F_1 + F_2$.

(4) $n \geq 3$. This is because there exists an explicit hitting set of size $d^{O(1)}$ for constant-variate polynomials of degree at most d. This follows from either Kronecker substitutions or explicit hitting set constructions for sparse polynomials [KS01].

(5) F_0 is squarefree. Item 3 of Theorem 5.4 states that some F_i is squarefree. So this assumption can be guaranteed by permuting the summands F_i.

(6) The GCD of F_0, F_1, and F_2 is 1. This is because we can take out the GCD of F_0, F_1, and F_2, if it is nontrivial, from each F_i. See [Gup14] for a more detailed discussion.

(7) $f_{i,j}$ is an irreducible non-constant polynomial for $i = 0, 1, 2$ and $j \in [m_i]$. This can be guaranteed by replacing $f_{i,j}$ with its irreducible factors over $\mathbb{F}$, and absorbing the constant $f_{i,j}$ into other factors.

(8) There exists $j_0 \in [m_0]$ such that f_{0,j_0} does not divide any polynomial in $\{F_1, F_2, F_1 + F_2\}$. By permuting the factors of F_0, we may assume, without loss of generality, that $j_0 = 1$.

Assumption (8) is justified by the following lemma.

Lemma 5.5. *There exists an explicit $(nd)^{O_\delta(1)}$-sized hitting set for all $F \in C_{n,d,3,\delta,\mathbb{F}}$ satisfying Assumptions (1)–(7) and the additional assumption that F_0 has factor $f_{0,j}$ dividing some polynomial in $\{F_1, F_2, F_1 + F_2\}$.*

Proof. If $F_1 + F_2 = cF_0$ for some $c \in \mathbb{F}$, then $F = F_0 + F_1 + F_2 = (c+1)F_0$, which is a product of polynomials of degree at most δ. This is the case where $k_0 = 1$, which is already solved as mentioned. So we assume this is not the case. In particular, $F_1 + F_2 \neq 0$. Then, $\deg(F_1 + F_2) = \deg(F_0) = d_0$. As $F_1 + F_2$ is not of the form cF_0 with $c \in \mathbb{F}$ but has degree $d_0 = \deg(F_0)$, we see that F_0 does not divide $F_1 + F_2$. As $F_0 = \prod_{j=1}^{m_0} f_{0,j}$ is squarefree, we conclude that for some $j \in [m_0]$, the factor $f_{0,j}$ does not divide $F_1 + F_2$. Fix such j.

By assumption, $f_{0,j}$ divides F_1 or F_2, but not both since it does not divide $F_1 + F_2$. By symmetry, we may assume $f_{0,j}$ divides F_1 but not F_2. By Assumption (7), $V(f_{0,j})$ is an irreducible hypersurface of $\mathbb{A}^n$. As f_0 divides F_1, we have $V(f_{0,j}, F_1) = V(f_{0,j})$ and therefore its codimension in $\mathbb{A}^n$ equals one. On the other hand, as f_0 does not divide $F_2 = \prod_{i=1}^{m_2} f_{2,i}$, the codimension of $V(f_{0,j}, f_{2,i})$ in $\mathbb{A}^n$ equals two for all $i \in [m_2]$. We also have $\deg(V(f_{0,j})) = \deg(f_{0,j}) \leq \delta$ and $\deg(V(f_{0,j}, f_{2,i})) \leq \delta^2$ for $i \in [m_2]$ by Bézout's inequality.

Guo [Guo24, Theorem 1.6] showed how to explicitly construct a set $\mathcal{H}$ of affine planes in $\mathbb{A}^n$ of size at most $n^{O(\delta^2)} d^{O(1)}$ such that for at least one $P \in \mathcal{H}$, we have $\dim(V(f_{0,j}) \cap P) = 1$ and $\dim(V(f_{0,j}, f_{2,i}) \cap P)) = 0$ for all $i \in [m_2]$. Fix such P. Then

$$\dim(V(f_{0,j}, F_1) \cap P) = \dim(V(f_{0,j}) \cap P) = 1$$

and

$$\dim(V(f_{0,j}, F_2) \cap P) = \dim\left(\bigcup_{i=1}^{m_2} (V(f_{0,j}, f_{2,i}) \cap P)\right) = \max_{i \in [m_2]} (\dim(V(f_{0,j}, V_{2,i}) \cap P)) = 0.$$

Note that this implies that $F_1 + F_2$ is not identically zero when restricting to $V(f_{0,j}) \cap P$, since otherwise we would have

$$V(f_{0,j}, F_1) \cap P = V(f_{0,j}) \cap P \cap V(F_1) = V(f_{0,j}) \cap P \cap V(-F_2) = V(f_{0,j}, F_2) \cap P,$$

contradicting the fact that $\dim(V(f_{0,j}, F_1) \cap P) \neq \dim(V(f_{0,j}, F_2) \cap P)$.

As $f_{0,j}$ divides F_0, we have $F = F_0 + F_1 + F_2 \equiv F_1 + F_2 \not\equiv 0$ when restricting to $V(f_{0,j}) \cap P$. So F is not identically zero on P. As F restricted to P is a bivariate polynomial of degree $\deg(F) = d_0 \leq d$, we know how to construct an explicit hitting set of size $d^{O(1)}$ on P for F. Finally, while we do not know which affine plane $P \in \mathcal{H}$ works, we could construct an explicit hitting set for each affine plane in $\mathcal{H}$ and then take their union as the final hitting set, whose size is at most $|\mathcal{H}| \cdot d^{O(1)} \leq n^{O(\delta^2)} d^{O(1)}$. □

From now on, we assume Assumptions (1)–(8). Next, we introduce the projective analogue of Definition 5.1.

Definition 5.6 (Restriction to a generic projective plane)**.** *$f \in \mathbb{F}[\mathbf{X}] = \mathbb{F}[X_1, \ldots, X_n]$ be a homogeneous polynomial. Define* proj.res(f) *to be the homogeneous polynomial*

$$f\left(Y_{0,1}\widehat{Z}_0 + Y_{1,1}\widehat{Z}_1 + Y_{2,1}\widehat{Z}_2, \ldots, Y_{0,n}\widehat{Z}_0 + Y_{1,n}\widehat{Z}_1 + Y_{2,n}\widehat{Z}_2\right) \in \mathbb{F}[\mathbf{Y}][\widehat{Z}_0, \widehat{Z}_1, \widehat{Z}_2] \subseteq \mathbb{K}[\widehat{Z}_0, \widehat{Z}_1, \widehat{Z}_2]. \tag{15}$$

Consider the projective space $\mathbb{P}^2_{\mathbb{K}}$ over $\mathbb{K} = \mathbb{F}(Y_{0,1}, Y_{1,1}, Y_{2,1}, \ldots, Y_{0,n}, Y_{1,n}, Y_{2,n})$ with homogeneous coordinates $\widehat{Z}_0$, $\widehat{Z}_1$, and $\widehat{Z}_2$. For $i = 0, 1, 2$, let $U_i \cong \mathbb{A}^2_{\mathbb{K}}$ be the affine open chart of $\mathbb{P}^2_{\mathbb{K}}$ defined by $\widehat{Z}_i \neq 0$.

The homogeneous polynomial proj.res$(f_{0,1})$ defines a projective hypersurface $C \subseteq \mathbb{P}^2_{\mathbb{K}}$, which is also a projective curve. Identify U_0 with $\mathbb{A}^2_{\mathbb{K}}$ and let $Z_1 = \widehat{Z}_1/\widehat{Z}_0$ and $Z_2 = \widehat{Z}_2/\widehat{Z}_0$ be the coordinates of U_0. By Definition 5.1 and Definition 5.6, $C \cap U_0 \subseteq U_0$ is defined precisely by the polynomial res$(f_{0,1})$. By Assumption (7), $f_{0,1}$ is irreducible over $\mathbb{F}$. So by Lemma 5.3, res$(f_{0,1})$ is absolutely irreducible. Thus, the affine curve $C \cap U_0$ and the projective curve C are both absolutely irreducible.

Let $g =$ proj.res(F_1)/proj.res(F_2), which is a homogeneous rational function of degree $\deg(F_1) - \deg(F_2) = 0$ on the projective space $\mathbb{P}^2_{\mathbb{K}}$. By Assumption (8), $f_{0,1}$ divides neither F_1 nor F_2. So proj.res$(f_{0,1})$ divides neither proj.res(F_1) nor proj.res(F_2). This follows from the fact that for any homogeneous polynomial $P \in \mathbb{F}[\mathbf{X}]$, we can recover P from proj.res(P) via

$$P(X_1, \ldots, X_n) = (\text{proj.res}(P))|_{Y_{0,i}=X_i, Y_{1,i}=Y_{2,i}=0, \widehat{Z}_0=\widehat{Z}_1=\widehat{Z}_2=1 \text{ for } i\in[n]}$$

So g restricts to a nonzero rational function $g|_C \in \mathbb{K}(C)^\times$ on the projective curve C.

We start with the easy case:

Lemma 5.7. *There exists an explicit set $S \subseteq \mathbb{F}^n$ of size $n^{O(\delta^2)} d^{O(1)}$ independent of F such that, if the restriction[7] of $g =$ proj.res(F_1)/proj.res(F_2) to the normalization $\widetilde{C \cap U_i}$ of $C \cap U_i$ is regular for $i = 0, 1, 2$, then S is a hitting set for F.*

Proof. Suppose the restriction of $g =$ proj.res(F_1)/proj.res(F_2) to $\widetilde{C \cap U_i}$ is regular for $i = 0, 1, 2$. These normalizations $C \cap U_i$ with $i = 0, 1, 2$ glue together to form the normalization $\widetilde{C}$ of C; see [Eis95, Proposition 4.13] and the discussion thereafter. Then $g|_C$ is a regular function on $\widetilde{C}$.

By Lemma 5.2, even after changing the base field $\mathbb{K}$ to $\overline{\mathbb{K}}$, the coordinate ring $\overline{\mathbb{K}}[C \cap U_i]$ is an integral domain, and so is its integral closure $\overline{\mathbb{K}}[\widetilde{C \cap U_i}]$. This means $\widetilde{C}$ is *geometrically integral*

[7] The restriction of g to $\widetilde{C \cap U_i}$ means first restricting g to $C \cap U_i$, and then viewing it as a (rational) function on $\widetilde{C \cap U_i}$. Note that $C \cap U_i$ and $\widetilde{C \cap U_i}$ share the same function field, $\mathrm{Frac}(\mathbb{K}[C \cap U_i])$.

[Sta25, Tag 05DW, Tag 0366]. Moreover, $\widetilde{C}$ is projective and hence *proper* over $\mathbb{K}$.[8] Any regular function on a geometrically integral and proper variety lives in the base field [Sta25, Tag 0BUG]. So $g|_{\widetilde{C}} \in \mathbb{K}$. It follows that $g|_C \in \mathbb{K} = \mathbb{F}(\mathbf{Y})$.

View F_0, F_1, F_2 as polynomials on $\mathbb{A}^n_{\mathbb{F}}$. Let H be the irreducible hypersurface in $\mathbb{A}^n_{\mathbb{F}}$ defined by $f_{0,1}$. As $f_{0,1}$ divides neither F_1 nor F_2, we know F_1/F_2 restricts to a nonzero rational function $(F_1/F_2)|_H \in \mathbb{F}(H)$ on H.

Assume $(F_1/F_2)|_H \notin \mathbb{F}$. Then for a general point $\mathbf{x} = (\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathbb{F}^{3n}$, we have

1. $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}^n$ are linearly independent.
2. $g|_C$ is regular at $\mathbf{x}$.
3. The affine line passing through $\mathbf{a}$ and $\mathbf{b}$ intersects H at some point $\mathbf{u}$.
4. The affine line passing through $\mathbf{a}$ and $\mathbf{c}$ intersects H at some point $\mathbf{v}$.
5. F_1/F_2 is regular at $\mathbf{u}$ and $\mathbf{v}$ but $(F_1/F_2)(\mathbf{u}) \neq (F_1/F_2)(\mathbf{v})$.

Fix such $\mathbf{x} = (\mathbf{a}, \mathbf{b}, \mathbf{c})$. We may write $\mathbf{u} = \alpha\mathbf{a} + (1-\alpha)\mathbf{b}$ and $\mathbf{v} = \beta\mathbf{a} + (1-\beta)\mathbf{c}$ for some $\alpha, \beta \in \mathbb{F}$. By definition, as $g|_C(\mathbf{x}) \in \mathbb{K}$ does not depend on $(\widehat{Z_0}, \widehat{Z_1}, \widehat{Z_2})$, we have

$$(F_1/F_2)(\mathbf{u}) = \frac{\text{proj.res}(F_1)}{\text{proj.res}(F_2)}\bigg|_{\mathbf{Y}=\mathbf{x},(\widehat{Z_0},\widehat{Z_1},\widehat{Z_2})=(\alpha,1-\alpha,0)} = g|_C(\mathbf{x}),$$

and similarly,

$$(F_1/F_2)(\mathbf{v}) = \frac{\text{proj.res}(F_1)}{\text{proj.res}(F_2)}\bigg|_{\mathbf{Y}=\mathbf{x},(\widehat{Z_0},\widehat{Z_1},\widehat{Z_2})=(\beta,0,1-\beta)} = g|_C(\mathbf{x}).$$

So $(F_1/F_2)(\mathbf{u}) = (F_1/F_2)(\mathbf{v})$, contradicting the fact that $(F_1/F_2)(\mathbf{u}) \neq (F_1/F_2)(\mathbf{v})$.

Therefore, $(F_1/F_2)|_H \in \mathbb{F}$. Denote $(F_1/F_2)|_H$ by γ. The facts that $(F_1/F_2)|_H = \gamma$, H is defined by $f_{0,1}$, and $f_{0,1}$ divides F_0 imply that

$$F = F_0 + F_1 + F_2 \equiv F_1 + F_2 \equiv (1+\gamma)F_2 = (1+\gamma)\prod_{i=1}^{m_2} f_{2,i} \pmod{f_{0,1}}. \tag{16}$$

If $1+\gamma = 0$, then by (16), $F_1 + F_2$ would be divisible by $f_{0,1}$, contradicting Assumption (8). So $1+\gamma \neq 0$. Therefore, by (16),

$$V(f_{0,1}, F_1 + F_2) = \bigcup_{i=1}^{m_2} V(f_{0,1}, f_{2,i}),$$

where the degree of each $V(f_{0,1}, f_{2,i})$ in $\mathbb{A}^n_{\mathbb{F}}$ is bounded by δ^2 by Bézout's inequality.

As $f_{0,1}$ does not divide F_2, the codimension of each $V(f_{0,1}, f_{2,i})$ is exactly two. By [Guo24, Theorem 1.6], there exists an explicit set $\mathcal{H}$ of affine planes in $\mathbb{A}^n_{\mathbb{F}}$ of size at most $n^{O(\delta^2)}d^{O(1)}$ such that for at least one affine plane $P \in \mathcal{H}$, $\dim(V(f_{0,1}, f_{2,i}) \cap P)) = 0$ for all $i \in [m_2]$. This implies that $\prod_{i=1}^{m_2} f_{2,i}$ is nonzero when restricted to $V(f_{0,1}) \cap P$. Combining this with (16) and the fact that $1+\gamma \neq 0$, we have $F \equiv (1+\gamma)\prod_{i=1}^{m_2} f_{2,i} \not\equiv 0$ when restricted to $V(f_{0,1}) \cap P$. In particular, F is nonzero when restricted to P.

[8] Properness is a version of compactness in algebraic geometry. See [Vak24, §11.4].

The rest of the proof is the same as the last part of the proof of Lemma 5.5: As F restricted to P is a bivariate polynomial of degree $\deg(F) = d_0 \le d$, we know how to construct an explicit hitting set of size $d^{O(1)}$ on P for F. While we do not know which affine plane $P \in \mathcal{H}$ works, we could construct an explicit hitting set for each affine plane in $\mathcal{H}$ and then take their union as the final hitting set, whose size is at most $|\mathcal{H}| \cdot d^{O(1)} \le n^{O(\delta^2)} d^{O(1)}$. □

Next, we address the harder case, where normalization is needed.

Lemma 5.8. *For $i = 0, 1, 2$, there exists an explicit set $\mathcal{H}_i \subseteq \mathbb{F}^n$ of size at most $(nd)^{O_\delta(1)}$ independent of F such that, if the restriction of $g = \text{proj.res}(F_1)/\text{proj.res}(F_2)$ to the normalization $\widetilde{C \cap U_i}$ of $C \cap U_i$ is not regular, then $\mathcal{H}_i$ is a hitting set for F.*

Proof. By symmetry, it suffices to explicitly construct $\mathcal{H}_0$ and prove that this set satisfies the lemma. Let $C_0 = C \cap U_0$. Suppose the restriction of g to $\widetilde{C_0}$ is not regular. Identifying U_0 with the affine plane $\mathbb{A}^2_{\mathbb{K}}$ using the coordinates $Z_1 = \widehat{Z}_1/\widehat{Z}_0$ and $Z_2 = \widehat{Z}_2/\widehat{Z}_0$, one can see that the affine curve C_0 is defined by $\text{res}(f_{0,1})$ in $\mathbb{A}^2_{\mathbb{K}}$, and $g = \text{proj.res}(F_1)/\text{proj.res}(F_2)$ restricted to $\mathbb{A}^2_{\mathbb{K}}$ becomes the rational function $\text{res}(F_1)/\text{res}(F_2)$. So $(\text{res}(F_1)/\text{res}(F_2))|_{\widetilde{C_0}}$ is not regular.

The coordinate ring of C_0 is the integral domain $A := \mathbb{K}[Z_1, Z_2]/\langle \text{res}(f_{0,1})\rangle$. Define

$$g_0 := \frac{\text{res}(F_1) + \langle \text{res}(f_{0,1})\rangle}{\text{res}(F_2) + \langle \text{res}(f_{0,1})\rangle} \in \text{Frac}(A). \tag{17}$$

As mentioned above, $(\text{res}(F_1)/\text{res}(F_2))|_{\widetilde{C_0}}$ is not regular. Algebraically, this means g_0 is not in the integral closure $\widetilde{A}$ of A.

By Lemma 2.12, there exist $c_1, c_2 \in \mathbb{F}^\times$ such that for $\alpha = c_1 Z_1 + c_2 Z_2$, the natural ring homomorphism $\mathbb{K}[\alpha] \to A$ sending α to $\alpha + \langle \text{res}(f_{0,1})\rangle$ is injective and makes A a finite $\mathbb{K}[\alpha]$-module. Moreover, by Lemma 5.2, for any algebraic extension $\mathbb{L}$ of $\mathbb{K}$, $A_{\mathbb{L}} := \mathbb{L}[Z_1, Z_2]/\langle \text{res}(f_{0,1})\rangle$ is an integral domain of Krull dimension one. And by Lemma 5.3, $\text{Frac}(A)$ is a finite separable extension of $\mathbb{K}(\alpha)$. By Definition 5.1 and the fact that $\deg(f_{0,1}) \le \delta$, we have $\text{res}(f_{0,1}) \in P(\delta, \delta)$. (Similarly, $\text{res}(f_{i,j}) \in P(\delta, \delta)$ for all $i = 0, 1, 2$ and $j \in [m_i]$.) So, by Theorem 4.7, there exist integers D, D', m, k', e satisfying $D, D', m, k', p^e = O_\delta(1)$, and $g_1, g_2, h_1, \ldots, h_{k'} \in \mathbb{K}^{(e)}[\mathbf{T}] = \mathbb{K}^{(e)}[T_1, \ldots, T_m]$ such that the following hold:

(1) $g_1, g_2, h_1, \ldots, h_{k'} \in P^{(e)}(D, D')$.

(2) The map

$$\begin{aligned} \phi : A_{\mathbb{K}^{(e)}} &\to \mathbb{K}^{(e)}[\mathbf{T}]/\langle h_1, \ldots, h_{k'}\rangle \\ Z_i + \langle \text{res}(f_{0,1})\rangle &\mapsto g_i + \langle h_1, \ldots, h_{k'}\rangle, \quad i = 1, 2. \end{aligned}$$

defines an injective $\mathbb{K}^{(e)}$-linear ring homomorphism.

(3) $\mathbb{K}^{(e)}[\mathbf{T}]/\langle h_1, \ldots, h_{k'}\rangle$ is isomorphic to the integral closure $\widetilde{A_{\mathbb{K}^{(e)}}}$ of $A_{\mathbb{K}^{(e)}}$, and this isomorphm composed with ϕ is the natural inclusion of $A_{\mathbb{K}^{(e)}}$ in its integral closure.

We claim that g_0 is not in the integral closure $\widetilde{A_{\mathbb{K}^{(e)}}}$ of $A_{\mathbb{K}^{(e)}}$ either. To see this, assume to the contrary that $g_0 \in \widetilde{A_{\mathbb{K}^{(e)}}}$. Then it is integral over $A_{\mathbb{K}^{(e)}}$. And $A_{\mathbb{K}^{(e)}} = A \otimes_{\mathbb{K}} \mathbb{K}^{(e)}$ is integral over A. So by Lemma 2.7. g_0 is integral over A, contradicting the fact that $g_0 \notin \widetilde{A}$. Therefore, $g_0 \notin \widetilde{A_{\mathbb{K}^{(e)}}}$.

By Lemma 2.6, we have

$$\widetilde{A_{\mathbb{K}^{(e)}}} = \bigcap_{\text{maximal ideal } \mathfrak{m} \subseteq \widetilde{A_{\mathbb{K}^{(e)}}}} (\widetilde{A_{\mathbb{K}^{(e)}}})_{\mathfrak{m}}.^{9} \tag{18}$$

By (18), for some maximal ideal $\mathfrak{m}$ of $\widetilde{A_{\mathbb{K}^{(e)}}}$, we have $g_0 \notin (\widetilde{A_{\mathbb{K}^{(e)}}})_{\mathfrak{m}}$. Fix such $\mathfrak{m}$. As $\widetilde{A_{\mathbb{K}^{(e)}}}$ is integrally closed, the one-dimensional local ring $(\widetilde{A_{\mathbb{K}^{(e)}}})_{\mathfrak{m}}$ is a discrete valuation ring and is equipped with a normalized valuation $\mathrm{ord}_{\mathfrak{m}}(\cdot)$. An element $f \in \mathrm{Frac}(A_{\mathbb{K}^{(e)}})$ is in $(\widetilde{A_{\mathbb{K}^{(e)}}})_{\mathfrak{m}}$ if and only if $\mathrm{ord}_{\mathfrak{m}}(f) \geq 0$.

By (17) and the fact that $g_0 \notin (\widetilde{A_{\mathbb{K}^{(e)}}})_{\mathfrak{m}}$, we have

$$0 \leq \mathrm{ord}_{\mathfrak{m}}(\mathrm{res}(F_1) + \langle \mathrm{res}(f_{0,1}) \rangle) < \mathrm{ord}_{\mathfrak{m}}(\mathrm{res}(F_2) + \langle \mathrm{res}(f_{0,1}) \rangle). \tag{19}$$

For $i = 1, 2$ and $j \in [m_i]$, let $k_{i,j} = \mathrm{ord}_{\mathfrak{m}}(\mathrm{res}(f_{i,j}) + \langle \mathrm{res}(f_{0,1}) \rangle)$. Then for $i = 1, 2$, since $F_i = \prod_{j=1}^{m_i} f_{i,j}$, we have

$$\mathrm{ord}_{\mathfrak{m}}(\mathrm{res}(F_i) + \langle \mathrm{res}(f_{0,1}) \rangle) = \sum_{j \in [m_i]} \mathrm{ord}_{\mathfrak{m}}(\mathrm{res}(f_{i,j}) + \langle \mathrm{res}(f_{0,1}) \rangle) = \sum_{j \in [m_i]} k_{i,j}. \tag{20}$$

We know that $\widetilde{A_{\mathbb{K}^{(e)}}}$ may be identified with $\mathbb{K}^{(e)}[\mathbf{T}]/\langle h_1, \ldots, h_{k'} \rangle$ such that ϕ becomes the inclusion $A_{\mathbb{K}^{(e)}} \hookrightarrow \widetilde{A_{\mathbb{K}^{(e)}}}$. We now consider the latter ring $\mathbb{K}^{(e)}[\mathbf{T}]/\langle h_1, \ldots, h_{k'} \rangle$ for computational purposes. Let $\widehat{\mathfrak{m}}$ the the maximal ideal of $\mathbb{K}^{(e)}[\mathbf{T}]$ such that $\widehat{\mathfrak{m}}/\langle h_1, \ldots, h_{k'} \rangle$ corresponds to the maximal ideal $\mathfrak{m}$ of $\widetilde{A_{\mathbb{K}^{(e)}}}$.

Consider $i \in \{0, 1, 2\}$ and $j \in [m_i]$. By definition, we have $\phi(\mathrm{res}(f_{i,j})) = \mathrm{res}(f_{i,j})(g_1, g_2) + \langle h_1, \ldots, h_{k'} \rangle$. As $\mathrm{res}(f_{i,j}) \in P(\delta, \delta)$ and $g_1, g_2 \in P^{(e)}(D, D')$, where $D, D', p^e = O_\delta(1)$, we have $\mathrm{res}(f_{i,j})(g_1, g_2) \in P^{(e)}(d_1, d_2)$ for some $d_1, d_2 = O_\delta(1)$.

By (19) and (20), there exists $j_0 \in [m_2]$ such that $k_{2,j_0} > 0$, implying that $\mathrm{res}(f_{2,j_0}) \in \mathfrak{m}$. So $\phi(\mathrm{res}(f_{2,j_0})) \in \widehat{\mathfrak{m}}/\langle h_1, \ldots, h_{k'} \rangle$, or equivalently, $\mathrm{res}(f_{i,j})(g_1, g_2) \in \widehat{\mathfrak{m}} + \langle h_1, \ldots, h_{k'} \rangle$. Therefore, $\widehat{\mathfrak{m}}$ contains the zero-dimensional ideal $I := \langle h_1, \ldots, h_{k'}, \mathrm{res}(f_{i,j})(g_1, g_2) \rangle$. By increasing e if necessary as in the proof of Lemma 4.10, we may assume that the $\mathbb{K}^{(e)}[\mathbf{T}]/\widehat{\mathfrak{m}}$ is a finite separable extension over $\mathbb{K}^{(e)}$. By Lemma 3.20, $\widehat{\mathfrak{m}}$ admits a Gröbner basis $G \subseteq P^{(e)}(d_3, d_4)$ for some $d_3, d_4 \in O_\delta(1)$.

Let $\overline{\mathfrak{m}} = \widehat{\mathfrak{m}}/\langle h_1, \ldots, h_{k'} \rangle$. The normalized valuation $\mathrm{ord}_{\mathfrak{m}}$ of $(\widetilde{A_{\mathbb{K}^{(e)}}})_{\mathfrak{m}}$ corresponds to a normalized valuation of the discrete valuation ring

$$B := (\mathbb{K}^{(e)}[\mathbf{T}]/\langle h_1, \ldots, h_{k'} \rangle)_{\overline{\mathfrak{m}}},$$

which we again denote by $\mathrm{ord}_{\mathfrak{m}}$ by a slight abuse of notation. As $\mathrm{ord}_{\mathfrak{m}}$ is normalized and G generates the ideal $\widehat{\mathfrak{m}}$, there exists $u \in G$ such that $\overline{u} := u + \langle h_1, \ldots, h_{k'} \rangle$ satisfies $\mathrm{ord}_{\mathfrak{m}}(\overline{u}) = 1$.

Consider $i \in \{1, 2\}$ and $j \in [m_i]$. By the structure of discrete valuation rings, the element

$$\phi(\mathrm{res}(f_{i,j}) + \langle \mathrm{res}(f_{0,1}) \rangle) = \mathrm{res}(f_{i,j})(g_1, g_2) + \langle h_1, \ldots, h_{k'} \rangle$$

equals $\overline{u}^{k_{i,j}}$ multiplied by a unit of B. Combining this with the fact that any element of $\mathbb{K}^{(e)}[\mathbf{T}]$ not in $\widehat{\mathfrak{m}}$ is invertible modulo $\widehat{\mathfrak{m}}$ (since $\widehat{\mathfrak{m}}$ is a maximal ideal) shows that there exists $t_{i,j} \in \mathbb{K}^{(e)}[\mathbf{T}]$ that is invertible modulo $\widehat{\mathfrak{m}}$ such that

$$t_{i,j}(\mathrm{res}(f_{i,j})(g_1, g_2)) - u^{k_{i,j}} \in u^{k_{i,j}}\widehat{\mathfrak{m}} + \langle h_1, \ldots, h_{k'} \rangle. \tag{21}$$

[9] Alternatively, (18) follows from *Algebraic Hartogs's Lemma* [Vak24, 13.5.19], which extends to higher-dimensional normal varieties.

We can find $t_{i,j}$ from (21) by applying Lemma 3.15 with $f = u^{k_{i,j}}$. Note that by Lemma 2.14, we have $k_{i,j} = O_\delta(1)$. Given that the complexity of the data describing the other terms in (21) also only depends on δ, we see that $t_{i,j} \in P^{(e)}(d_5, d_6)$ for some $d_5, d_6 \in O_\delta(1)$.

Recall that $G \subseteq P^{(e)}(d_3, d_4)$ is a Gröbner basis of $\widehat{\mathfrak{m}}$. By Lemma 3.11 and (21), we may write

$$t_{i,j}(\mathrm{res}(f_{i,j})(g_1, g_2)) = u^{k_{i,j}} \left(1 + \sum_{g \in G} a_{i,j,g} g\right) + \sum_{\ell=1}^{k'} b_{i,j,\ell} h_\ell, \tag{22}$$

with $a_{i,j,g}, b_{i,j,\ell} \in P^{(e)}(d_7, d_8)$ for $g \in G$ and $\ell \in [k']$, where $d_7, d_8 \in O_d(1)$.

Recall that $t_{i,j}$ is invertible modulo $\widehat{\mathfrak{m}}$. By applying Lemma 3.15 with $f = 1$, we may find $s_{i,j} \in \mathbb{K}^{(e)}[\mathbf{T}]$ such that

$$s_{i,j} t_{i,j} = 1 + \sum_{g \in G} c_{i,j,g} g. \tag{23}$$

with $s_{i,j}, c_{i,j,g} \in P^{(e)}(d_9, d_{10})$ for all $g \in G$, where $d_9, d_{10} \in O_d(1)$.

Similarly, as $u \in \widehat{\mathfrak{m}}$ and $\langle h_1, \ldots, h_{k'} \rangle \subseteq \widehat{\mathfrak{m}}$, by Lemma 3.11, we can write

$$u = \sum_{g \in G} d_g g \quad \text{and} \quad h_\ell = \sum_{g \in G} e_{\ell,g} g \quad \text{for} \quad \ell \in [k'] \tag{24}$$

with $d_g, e_{\ell,g} \in P^{(e)}(d_{11}, d_{12})$ for all $g \in G$ and $\ell \in [k']$, where $d_{11}, d_{12} \in O_d(1)$.

Suppose Q is a polynomial over $\mathbb{K}^{(e)}$, and $\mathbf{a} \in \mathbb{F}^{3n}$ is a point such that none of the denominators of the coefficients of Q, which are polynomials in $\mathbf{Y}^{1/p^e}$, vanishes after assigning $\mathbf{a}$ to $\mathbf{Y}^{1/p^e}$. Then the resulting polynomial after the assignment $\mathbf{Y}^{1/p^e} \leftarrow \mathbf{a}$ is a well-defined polynomial over $\mathbb{F}$. Denote this polynomial by $Q|_{\mathbf{a}}$.

For convenience, for a set $S \subseteq \mathbb{F}[\mathbf{Y}^{1/p^e}]$ and $\mathbf{a} \in \mathbb{F}^{3n}$, we say $\mathbf{a}$ is a *common non-root* of S if every $Q \in S$ is non-vanishing at $\mathbf{a}$.

We will construct a set $S^* \subseteq \mathbb{F}[\mathbf{Y}^{1/p^e}]$ of size $O_\delta(d)$, where $d = \deg(F)$, such that $\mathrm{res}(F_1 + F_2)|_{\mathbf{a}} \not\equiv 0 \pmod{\mathrm{res}(f_{0,1})|_{\mathbf{a}}}$ for any common non-root $\mathbf{a}$ of S^*.

First, we construct a subset S_0 of S^* of size $O_\delta(d)$ as follows: For all $i = 1, 2$, $j \in [m_i]$, and all polynomials over $\mathbb{K}^{(e)}$ that appear in (22), (23), or (24), add the denominators of all their coefficients to S_0. Define the ideal

$$\widehat{\mathfrak{m}}|_{\mathbf{a}} := \langle \{g|_{\mathbf{a}} : g \in G\} \rangle$$

of $\mathbb{F}[\mathbf{T}]$. Then by (22), (23), and (24), for a common non-root $\mathbf{a}$ of S_0, we have

$$(t_{i,j}(\mathrm{res}(f_{i,j})(g_1, g_2)))|_{\mathbf{a}} = \left(u^{k_{i,j}} \left(1 + \sum_{g \in G} a_g g\right) + \sum_{\ell=1}^{k'} b_\ell h_\ell \right)\Bigg|_{\mathbf{a}}, \tag{25}$$

$$(s_{i,j} t_{i,j})|_{\mathbf{a}} = \left(1 + \sum_{g \in G} c_g g\right)\Bigg|_{\mathbf{a}}, \tag{26}$$

and

$$u|_{\mathbf{a}} \in \widehat{\mathfrak{m}}|_{\mathbf{a}} \quad \text{and} \quad \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle \subseteq \widehat{\mathfrak{m}}|_{\mathbf{a}}. \tag{27}$$

Let $n_i = \mathrm{ord}_{\mathfrak{m}}(\mathrm{res}(F_i) + \langle \mathrm{res}(f_{0,1}) \rangle)$ for $i = 1, 2$. Then $n_1 < n_2$ by (19) and $n_i = \sum_{j=1}^{m_i} k_{i,j}$ for $i = 1, 2$ by (20). Taking the product of (25) over all $j \in [m_i]$, we have that for $i = 1, 2$,

$$\left(\left(\prod_{j \in [m_i]} t_{i,j} \right) \mathrm{res}(F_i)(g_1, g_2) \right) \Bigg|_{\mathbf{a}} - u^{n_i}|_{\mathbf{a}} \in u^{n_i}|_{\mathbf{a}} \cdot \widehat{\mathfrak{m}}|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle . \tag{28}$$

We also need the following two claims, with a proof for one and a proof sketch for the other provided later.

Claim 5.9. *There exists a set $S_1 \subseteq \mathbb{F}[\mathbf{Y}^{1/p^e}] \cap C^{(e)}(D_1)$ of size $O_\delta(1)$, where $D_1 = O_\delta(1)$, such that for any common non-root $\mathbf{a} \in \mathbb{F}^{3n}$ of $S_0 \cup S_1$, it holds that $1 \notin \widehat{\mathfrak{m}}|_{\mathbf{a}}$.*

Claim 5.10. *There exists a set $S_2 \subseteq \mathbb{F}[\mathbf{Y}^{1/p^e}] \cap C^{(e)}(D_2)$ of size $O_\delta(1)$, where $D_2 = O_\delta(1)$, such that for any common non-root $\mathbf{a} \in \mathbb{F}^{3n}$ of $S_0 \cup S_2$, the element $u|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle$ is a non-zero-divisor of $\mathbb{F}[\mathbf{T}] / \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle$.*

Let $S^{**} = S_0 \cup S_1 \cup S_2$. Consider any common non-root $\mathbf{a} \in \mathbb{F}^{3n}$ of S^{**}. Let

$$\overline{\mathfrak{m}}|_{\mathbf{a}} := \widehat{\mathfrak{m}}|_{\mathbf{a}} / \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle ,$$

which is an ideal of $R_{\mathbf{a}} := \mathbb{F}[\mathbf{T}] / \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle$. By Claim 5.9, we have $1 \notin \overline{\mathfrak{m}}|_{\mathbf{a}}$, i.e., $\overline{\mathfrak{m}}|_{\mathbf{a}} \subsetneq R_{\mathbf{a}}$.

Let $\overline{u}|_{\mathbf{a}} := u|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle \in R_{\mathbf{a}}$. By Claim 5.10, $\overline{u}|_{\mathbf{a}}$ is a non-zero-divisor of $R_{\mathbf{a}}$, and so are its powers. Therefore, for any integer $r \geq 0$, we have an isomorphism between the $(R_{\mathbf{a}}/\overline{\mathfrak{m}}|_{\mathbf{a}})$-modules

$$\begin{aligned} \times(\overline{u}|_{\mathbf{a}})^r : R_{\mathbf{a}}/\overline{\mathfrak{m}}|_{\mathbf{a}} &\to \langle (\overline{u}|_{\mathbf{a}})^r \rangle / ((\overline{u}|_{\mathbf{a}})^r \overline{\mathfrak{m}}|_{\mathbf{a}}) \\ x + \overline{\mathfrak{m}}|_{\mathbf{a}} &\mapsto (\overline{u}|_{\mathbf{a}})^r x + (\overline{u}|_{\mathbf{a}})^r \overline{\mathfrak{m}}|_{\mathbf{a}}. \end{aligned}$$

As $1 \notin \overline{\mathfrak{m}}|_{\mathbf{a}}$, using the above isomorphism, we see that $(\overline{u}|_{\mathbf{a}})^r$ is in $\langle (\overline{u}|_{\mathbf{a}})^r \rangle$ but not in $(\overline{u}|_{\mathbf{a}})^r \cdot \overline{\mathfrak{m}}|_{\mathbf{a}}$ for $r \geq 0$.

Let $U \subseteq R_{\mathbf{a}}$ be the set of all finite products of elements in $\{t_{2,j}|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle : j \in [m_2]\}$. By (26), elements in U are already invertible modulo $\overline{\mathfrak{m}}|_{\mathbf{a}}$. So localizing $R_{\mathbf{a}}/\overline{\mathfrak{m}}|_{\mathbf{a}}$ and $\langle (\overline{u}|_{\mathbf{a}})^r \rangle / ((\overline{u}|_{\mathbf{a}})^r \overline{\mathfrak{m}}|_{\mathbf{a}})$ with respect to the multiplicatively closed set U does not change these two modules. The argument in the previous two paragraphs then shows that $(\overline{u}|_{\mathbf{a}})^r$ is not in the localization $U^{-1}((\overline{u}|_{\mathbf{a}})^r \overline{\mathfrak{m}}|_{\mathbf{a}})$ for $r \geq 0$.

In particular, by (28), we have

$$\left(\left(\prod_{j \in [m_1]} t_{1,j} \right) \mathrm{res}(F_1)(g_1, g_2) \right) \Bigg|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle \notin U^{-1}((\overline{u}|_{\mathbf{a}})^{n_1} \cdot \overline{\mathfrak{m}}|_{\mathbf{a}}).$$

It follows that

$$\mathrm{res}(F_1)(g_1, g_2)|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle \notin U^{-1}((\overline{u}|_{\mathbf{a}})^{n_1} \cdot \overline{\mathfrak{m}}|_{\mathbf{a}}). \tag{29}$$

As $n_2 > n_1$ and $\overline{u}|_{\mathbf{a}} \in \overline{\mathfrak{m}}|_{\mathbf{a}}$ (which holds by (27)), it also follows from (28) that

$$\left(\left(\prod_{j \in [m_2]} t_{2,j} \right) \mathrm{res}(F_2)(g_1, g_2) \right) \Bigg|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}} \rangle \in \langle (\overline{u}|_{\mathbf{a}})^{n_2} \rangle \subseteq (\overline{u}|_{\mathbf{a}})^{n_1} \cdot \overline{\mathfrak{m}}|_{\mathbf{a}}.$$

Localizing with respect to U makes $\left(\prod_{j\in[m_2]} t_{2,j}\right) + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ invertible. Therefore,

$$\operatorname{res}(F_2)(g_1, g_2)|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle \in U^{-1}((\overline{u}|_{\mathbf{a}})^{n_1} \cdot \overline{\mathfrak{m}}|_{\mathbf{a}}). \tag{30}$$

It follows from (29) and (30) that

$$\operatorname{res}(F_1 + F_2)(g_1, g_2)|_{\mathbf{a}} \notin \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle . \tag{31}$$

Finally, we need the following claim, whose proof is given later.

Claim 5.11. *There exists a set $S_3 \subseteq \mathbb{F}[\mathbf{Y}^{1/p^e}] \cap C^{(e)}(D_3)$ of size $O_\delta(d)$, where $D_3 = O_\delta(1)$, such that for any common non-root $\mathbf{a} \in \mathbb{F}^{3n}$ of $S_0 \cup S_3$, the polynomial $\operatorname{res}(f_{i,j})|_{\mathbf{a}} \in \mathbb{F}[Z_1, Z_2]$ is well-defined for all $i \in \{0, 1, 2\}$ and $j \in [m_i]$, and the kernel of the $\mathbb{F}$-linear ring homomorphism $\mathbb{F}[Z_1, Z_2] \to \mathbb{F}[\mathbf{T}]/\langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ sending Z_i to $g_i|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ contains $\langle \operatorname{res}(f_{0,1})|_{\mathbf{a}}\rangle$.*

We define $S^* := S^{**} \cup S_3$. Then for any common non-root $\mathbf{a}$ of S^*, we have that $\operatorname{res}(F_0)|_{\mathbf{a}}$, $\operatorname{res}(F_1)|_{\mathbf{a}}$, and $\operatorname{res}(F_2)|_{\mathbf{a}}$ are well-defined by Claim 5.11. Morever, by (31) and Claim 5.11, $\operatorname{res}(F_1 + F_2)|_{\mathbf{a}} \not\equiv 0 \pmod{\langle \operatorname{res}(f_{0,1})|_{\mathbf{a}}\rangle}$. So

$$\operatorname{res}(F)|_{\mathbf{a}} = \operatorname{res}(F_0 + F_1 + F_2)|_{\mathbf{a}} \equiv \operatorname{res}(F_1 + F_2)|_{\mathbf{a}} \not\equiv 0 \pmod{\langle \operatorname{res}(f_{0,1})|_{\mathbf{a}}\rangle}$$

It follows that $\operatorname{res}(F)|_{\mathbf{a}} \neq 0$. In other words, F is not identically zero when restricted to $P_{\mathbf{a}}$, which is the affine plane $\mathbb{A}^2_{\mathbb{F}} \subseteq \mathbb{A}^n_{\mathbb{F}}$ determined by the parameters $\mathbf{a} = (a_{0,1}, \ldots, a_{2,n})$ via the map $(z_1, z_2) \mapsto (a_{0,1} + a_{1,1}z_1 + a_{2,1}z_2, \ldots, a_{0,n} + a_{1,n}z_1 + a_{2,n}z_2)$.

As F restricted to $P_{\mathbf{a}}$ is a bivariate polynomial of degree at most d, we can construct a hitting set $\mathcal{H}_{\mathbf{a}} \subseteq P_{\mathbf{a}} \subseteq \mathbb{A}^n_{\mathbb{F}}$ of size $d^{O(1)}$ independent of F, assuming a common non-root $\mathbf{a}$ of S^* is given.

We need $\mathbf{a}$ to be a common non-root of all the elements in S^*, where $|S^*| = O_\delta(d)$. Note that the elements in S^* are $3n$-variate polynomials of degree $O_\delta(1)$ in $\mathbf{Y}^{1/p^e}$. Using the deterministic black-box PIT algorithm for sparse polynomials in [KS01], even without knowing F, we may construct an ε-hitting set $\mathcal{H}$ of size at most $d^{O(1)}n^{O_\delta(1)}$ for the polynomials in S^*, where $\varepsilon < 1/|S^*|$. By the union bound, $\mathcal{H}$ is guaranteed to contain a common non-root of S^*. The final hitting set $\mathcal{H}_0$ is then $\bigcup_{\mathbf{a}\in\mathcal{H}} \mathcal{H}_{\mathbf{a}}$. Its size is $d^{O(1)}n^{O_\delta(1)} \leq (nd)^{O_\delta(1)}$. □

Proof of Theorem 5.4. The theorem follows by combining Lemma 5.7 and Lemma 5.8. □

Finally, we prove Claim 5.9, Claim 5.10, and Claim 5.11.

Proof of Claim 5.9. Consider $\mathbf{a} \in S_0$, so that $g|_{\mathbf{a}}$ is well-defined for $g \in G$. Note that if $1 \in \widehat{\mathfrak{m}}|_{\mathbf{a}}$, by Lemma 3.9, we can write 1 as an $\mathbb{F}$-linear combination of polynomials in

$$U := \{mg|_{\mathbf{a}} : g \in G, m \text{ is a monomial of degree at most } d_0\}$$

for some sufficiently large $d_0 = O_\delta(1)$. View 1 and the polynomials in U as (row) vectors of coefficients. These vectors then form a matrix $M|_{\mathbf{a}}$. The statement that $1 \notin \widehat{\mathfrak{m}}|_{\mathbf{a}}$ is equivalent to the statement that the row of $M|_{\mathbf{a}}$ corresponding to 1 is not in the span of the other rows over $\mathbb{F}$.

The same argument works over $\mathbb{K}^{(e)}$ with $mg|_{\mathbf{a}}$ replaced by mg, allowing us to form a matrix M over $\mathbb{K}^{(e)}$. Then $1 \notin \widehat{\mathfrak{m}}$ is equivalent to the statement that the row of M corresponding to 1 is not in the span of the other rows over $\mathbb{K}^{(e)}$.

As we do know that $1 \notin \widehat{\mathfrak{m}}$, over $\mathbb{K}^{(e)}$, we can find a nonsingular minor M_0 of maximal size, and it involves the row corresponding to 1. Note that $\det(M_0) \in \mathbb{K}^{(e)}$ is a nonzero rational function

in $\mathbf{Y}^{1/p^e}$ whose denominators P and numerators Q have degree $O_\delta(1)$. Suppose $P(\mathbf{a}), Q(\mathbf{a}) \neq 0$. Then the determinant of the corresponding minor $M_0|_{\mathbf{a}}$ of $M|_{\mathbf{a}}$ is nonzero too, which, combined with Lemma 3.9, implies that $1 \notin \widehat{\mathfrak{m}}|_{\mathbf{a}}$.

Therefore, we can let $S_1 = \{P, Q\}$. □

Proof sketch of Claim 5.10. $u|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ is a zero-divisor of $\mathbb{F}[\mathbf{T}]/\langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ if and only if there exists $v \in \mathbb{F}[T]$ such that

$$u|_{\mathbf{a}} \cdot v \in \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle \quad \text{but} \quad v \notin \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle . \tag{32}$$

The ideal of $v \in \mathbb{F}[\mathbf{T}]$ satisfying $u|_{\mathbf{a}} \cdot v \in \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ is the ideal quotient $(\langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle : \langle u|_{\mathbf{a}}\rangle)$, and a Gröbner basis of it can be computed via [AL94, Lemma 2.3.10 and Lemma 2.3.11]. Using arguments based on Gröbner bases, one can see that if v satisfying (32) exists, it exists with $\deg_{\mathbf{T}}(v) \leq d_0$ for some $d_0 \in O_\delta(1)$.

Let W (resp. $W|_{\mathbf{a}}$) be the $O_\delta(1)$-dimensional space of polynomials in $\mathbb{K}^{(e)}[\mathbf{T}]$ (resp. $\mathbb{F}[\mathbf{T}]$) of degree at most d_0. Let $W_1 \subseteq W$ (resp. $W_1|_{\mathbf{a}} \subseteq W|_{\mathbf{a}}$) be the subspace of v satisfying $u \cdot v \in \langle h_1, \ldots, h_{k'}\rangle$ (resp. $u|_{\mathbf{a}} \cdot v \in \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$). Let $W_2 \subseteq W$ (resp. $W_2|_{\mathbf{a}} \subseteq W|_{\mathbf{a}}$) be the subspace of v satisfying $v \in \langle h_1, \ldots, h_{k'}\rangle$ (resp. $v \in \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$).

For $v \in W_1$, we have $u \cdot v = \sum_{i=1}^{k'} w_i h_i$ for some polynomial w_i of degree at most $d_1 = O_\delta(1)$ by Lemma 3.9. Viewing the coefficients of v and $w_1, \ldots, w_{k'}$ as unknowns, we can construct a matrix M_1 representing the system of linear equations $u \cdot v = \sum_{i=1}^{k'} w_i h_i$. Solve it to find a basis of W_1. Its elements, viewed as row vectors, form a matrix B_1 over $\mathbb{K}^{(e)}$. Similarly, we can construct a matrix M_2 representing the system of linear equations $v = \sum_{i=1}^{k'} w_i h_i$. Solve it to find a basis of W_2. Its elements, viewed as row vectors, form a matrix B_2 over $\mathbb{K}^{(e)}$.

As we know $u + \langle h_1, \ldots, h_{k'}\rangle$ is a non-zero-divisor of the integral domain $\mathbb{K}^{(e)}[\mathbf{T}]/\langle h_1, \ldots, h_{k'}\rangle$, we know $W_1 \subseteq W_2$. Add the denominators of the entries of M_1, M_2, B_1, B_2 to S_2. Further add the determinants of certain nonsingular minors of M_1, M_2, B_2 to S_2. This would guarantee that if $\mathbf{a}$ is a common non-root of $S_0 \cap S_2$, then $B_1|_{\mathbf{a}}$ is a basis of $W_1|_{\mathbf{a}}$, $B_2|_{\mathbf{a}}$ is a basis of $W_2|_{\mathbf{a}}$, and $W_1|_{\mathbf{a}} \subseteq W_2|_{\mathbf{a}}$, implying that $u|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ is a non-zero-divisor of $\mathbb{F}[\mathbf{T}]/\langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$. Details are omitted. □

Proof of Claim 5.11. First, for all $i \in \{0, 1, 2\}$ and $j \in [m_i]$, add the denominators of all the coefficients of $\mathrm{res}(f_{i,j})$ to S_3.

As $\mathrm{res}(f_{0,1})(g_1, g_2) \in \langle h_1, \ldots, h_{k'}\rangle$, by Lemma 3.11, we may write

$$\mathrm{res}(f_{0,1})(g_1, g_2) = \sum_{i=1}^{k'} q_i h_i,$$

where $q_i \in P(d_0, d_0')$ for some $d_0, d_0' \in O_\delta(1)$. Add the denominators of all the coefficients of $q_1, \ldots, q_{k'}$ to S_3. Then $\mathrm{res}(f_{0,1})(g_1, g_2)|_{\mathbf{a}} = \sum_{i=1}^{k'} q_i|_{\mathbf{a}} h_i|_{\mathbf{a}}$. So $\mathrm{res}(f_{0,1})(g_1, g_2)|_{\mathbf{a}} \in \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$. It follows that the $\mathbb{F}$-linear ring homomorphism $\mathbb{F}[Z_1, Z_2] \to \mathbb{F}[\mathbf{T}]/\langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ sending Z_i to $g_i|_{\mathbf{a}} + \langle h_1|_{\mathbf{a}}, \ldots, h_{k'}|_{\mathbf{a}}\rangle$ maps $\mathrm{res}(f_{0,1})|_{\mathbf{a}}$ to zero, as desired. □

6 Conclusions and Future Directions

In this paper, we present deterministic polynomial-time black-box PIT algorithms for $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ circuits over arbitrary fields, under a squarefreeness assumption. Along the way, we introduce new techniques and establish a novel connection between PIT and normalization.

We emphasize that our approach should not be viewed as entirely disjoint from the Sylvester–Gallai-based line of work. Rather, we see it as complementary and potentially opening up new directions.

A natural and important question is whether the squarefreeness condition can be removed. We suspect that normalization alone is insufficient for this purpose and may need to be combined with other advanced tools, such as those developed in [OS24, GOS25b]. Nevertheless, we believe our approach is both valuable and promising. In particular, to the best of our knowledge, no prior deterministic PIT algorithms, even partial results, were known for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits in small positive characteristic before our work.

Another interesting direction is to identify special cases in which some of the algebraic computation tasks involved in our method can be performed more efficiently. A recent result in this vein was obtained by Garg, Oliveira, and Saxena [GOS25a], who showed that certain instances of primality testing lie in PSPACE or the polynomial hierarchy (some conditionally, assuming the Generalized Riemann Hypothesis).

References

[AF22] Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: proving and using lower bounds for polynomial ideals. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2022)*, pages 389–402, 2022.

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Annals of Mathematics*, pages 781–793, 2004.

[AL94] William Wells Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.

[AM69] Michael F. Atiyah and Ian G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[AV08] Manindra Agrawal and V Vinay. Arithmetic circuits: A chasm at depth four. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2008)*, pages 67–75. IEEE, 2008.

[BM90] Peter Borwein and William O. J. Moser. A survey of Sylvester's problem and its generalizations. *Aequationes Mathematicae*, 40:111–135, 1990.

[BM93] Dave Bayer and David Mumford. What can be computed in algebraic geometry? *arXiv preprint alg-geom/9304003*, 1993.

[BSV20] Vishwas Bhargava, Shubhangi Saraf, and Ilya Volkovich. Deterministic factorization of sparse polynomials with bounded individual degree. *Journal of the ACM*, 67(2):1–28, 2020.

[BW98] Bruno Buchberger and Franz Winkler. *Gröbner Bases and Applications*, volume 251. Cambridge University Press, 1998.

[CKS18] Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Hardness vs randomness for bounded depth arithmetic circuits. In *33rd Computational Complexity Conference (CCC 2018)*, pages 13–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2018.

[CRS95] Suresh Chari, Pankaj Rohatgi, and Aravind Srinivasan. Randomness-optimal unique element isolation with applications to perfect matching and related problems. *SIAM Journal on Computing*, 24(5):1036, 1995.

[DDS21] Pranjal Dutta, Prateek Dwivedi, and Nitin Saxena. Deterministic identity testing paradigms for bounded top-fanin depth-4 circuits. In *36th Computational Complexity Conference (CCC 2021)*, 2021.

[dJ98] Theo de Jong. An algorithm for computing the integral closure. *Journal of Symbolic Computation*, 26(3):273–277, 1998.

[DS07] Zeev Dvir and Amir Shpilka. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM Journal on Computing*, 36(5):1404, 2007.

[DST24] Pranjal Dutta, Amit Sinhababu, and Thomas Thierauf. Derandomizing multivariate polynomial factoring for low degree factors. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2024)*, pages 75–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024.

[Dub90] Thomas W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM Journal on Computing*, 19(4):750–773, 1990.

[Eis95] David Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry.* Springer Verlag, New York, 1995.

[EK66] Michael Edelstein and Leroy M. Kelly. Bisecants of finite collections of sets in linear spaces. *Canadian Journal of Mathematics*, 18:375–380, 1966.

[FGT21] Stephen Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite perfect matching is in quasi-NC. *SIAM Journal on Computing*, 50(3):218–235, 2021.

[For78] David James Ford. *On the computation of the maximal order in a Dedekind domain.* PhD thesis, The Ohio State University, 1978.

[For24] Michael A. Forbes. Low-depth algebraic circuit lower bounds over any field. In *39th Computational Complexity Conference (CCC 2024)*, pages 31–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024.

[GOPS23] Abhibhav Garg, Rafael Oliveira, Shir Peleg, and Akash Kumar Sengupta. Radical Sylvester-Gallai theorem for tuples of quadratics. In *38th Computational Complexity Conference (CCC 2023)*, pages 20–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2023.

[GOS22] Abhibhav Garg, Rafael Oliveira, and Akash Kumar Sengupta. Robust radical Sylvester-Gallai theorem for quadratics. In *38th International Symposium on Computational Geometry (SoCG 2022)*, pages 42–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2022.

[GOS25a] Abhibhav Garg, Rafael Oliveira, and Nitin Saxena. Primes via zeros: Interactive proofs for testing primality of natural classes of ideals, 2025. To appear in STOC 2025.

[GOS25b] Abhibhav Garg, Rafael Oliveira, and Akash Kumar Sengupta. Uniform bounds on product Sylvester-Gallai configurations. *Electronic Colloquium on Computational Complexity (ECCC)*, TR25-037, 2025. To appear in SoCG 2025.

[GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2-3):149–167, 1988.

[Guo24] Zeyu Guo. Variety evasive subspace families. *computational complexity*, 33(2):10, 2024.

[Gup14] Ankit Gupta. Algebraic geometric techniques for depth-4 PIT & Sylvester-Gallai conjectures for varieties. *Electronic Colloquium on Computational Complexity (ECCC)*, TR14-130, 2014.

[GVJZ23] Zeyu Guo, Ben Lee Volk, Akhil Jalan, and David Zuckerman. Extractors for images of varieties. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC 2023)*, pages 46–59, 2023.

[Hei83] Joos Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.

[Her26] Grete Hermann. Die frage der endlich vielen schritte in der theorie der polynomideale. *Mathematische Annalen*, 95(1):736–788, 1926.

[Hir64a] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: I. *Annals of Mathematics*, 79(1):109–203, 1964.

[Hir64b] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: II. *Annals of Mathematics*, 79(2):205–326, 1964.

[HS80] Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute. In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing (STOC 1980)*, pages 262–272, 1980.

[Kal95] Erich Kaltofen. Effective Noether irreducibility forms and applications. *Journal of Computer and System Sciences*, 50(2):274–295, 1995.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *computational complexity*, 13(1/2):1–46, 2004.

[KRS24] Mrinal Kumar, Varun Ramanathan, and Ramprasad Saptharishi. Deterministic algorithms for low degree factors of constant depth circuits. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2024)*, pages 3901–3918. SIAM, 2024.

[KS01] Adam R. Klivans and Daniel Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC 2001)*, pages 216–223, 2001.

[KS07] Neeraj Kayal and Nitin Saxena. Polynomial identity testing for depth 3 circuits. *computational complexity*, 16(2):115–138, 2007.

[KS09] Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pages 198–207. IEEE, 2009.

[KSS14] Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of polynomial identity testing and deterministic multivariate polynomial factorization. In *2014 IEEE 29th Conference on Computational Complexity (CCC 2014)*, pages 169–180. IEEE, 2014.

[Kum13] Shrawan Kumar. Geometry of orbits of permanents and determinants. *Commentarii Mathematici Helvetici*, 88(3):759–788, 2013.

[Lan93] Serge Lang. *Algebra*. Addison-Wesley, New York, 3rd edition, 1993.

[Lov79] László Lovász. On determinants, matchings, and random algorithms. In *Proceedings of the 2nd International Symposium on Fundamentals of Computation Theory (FCT '79)*, pages 565–574. Akademie-Verlag, Berlin, 1979.

[LST24] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Communications of the ACM*, 67(2):101–108, 2024.

[Mag] Arturo Magidin. Localisation is isomorphic to a quotient of polynomial ring. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/152289 (version: 2018-12-07).

[Mat89] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1989.

[MM82] Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in mathematics*, 46(3):305–329, 1982.

[Mum88] David Mumford. *The Red Book of Varieties and Schemes*. Lecture Notes in Mathematics. Springer-Verlag, 1988.

[MVV87] Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of computer and System Sciences*, 49(2):149–167, 1994.

[OS22] Rafael Oliveira and Akash Kumar Sengupta. Radical Sylvester-Gallai theorem for cubics. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS 2022)*, pages 212–220. IEEE, 2022.

[OS24] Rafael Oliveira and Akash Kumar Sengupta. Strong algebras and radical Sylvester-Gallai configurations. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC 2024)*, pages 95–105, 2024.

[PS21] Shir Peleg and Amir Shpilka. Polynomial time deterministic identity testing algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits via Edelstein–Kelly type theorem for quadratic polynomials. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2021)*, pages 259–271, 2021.

[PS22] Shir Peleg and Amir Shpilka. A generalized Sylvester–Gallai-type theorem for quadratic polynomials. In *Forum of Mathematics, Sigma*, volume 10, page e112, 2022.

[Sax09] Nitin Saxena. Progress on polynomial identity testing. *Bulletin of the EATCS*, 99:49–79, 2009.

[Sax14] Nitin Saxena. Progress on polynomial identity testing - II. *Perspectives in Computational Complexity: The Somenath Biswas Anniversary Volume*, pages 131–146, 2014.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[Sei70] Abraham Seidenberg. Construction of the integral closure of a finite integral domain. *Rendiconti del Seminario Matematico e Fisico di Milano*, 40:101–120, 1970.

[Sei75] Abraham Seidenberg. Construction of the integral closure of a finite integral domain. II. *Proceedings of the American Mathematical Society*, 52(1):368–372, 1975.

[Shp20] Amir Shpilka. Sylvester-Gallai type theorems for quadratic polynomials. *Discrete Analysis*, 2020.

[SS12] Nitin Saxena and Comandur Seshadhri. Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM Journal on Computing*, 41(5):1285–1298, 2012.

[SS13] Nitin Saxena and Comandur Seshadhri. From Sylvester-Gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *Journal of the ACM*, 60(5):1–33, 2013.

[ST17] Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS 2017)*, pages 696–707. IEEE, 2017.

[Sta25] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu, 2025.

[Sto68] Gabriel Stolzenberg. Constructive normalization of an algebraic variety. *Bulletin of the American Mathematical Society*, 74(6):595–599, 1968.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends® in Theoretical Computer Science*, 5(3–4):207–388, 2010.

[Tra84] Barry Marshall Trager. *Integration of algebraic functions*. PhD thesis, Massachusetts Institute of Technology, 1984.

[Vak24] Ravi Vakil. The Rising Sea: Foundations of Algebraic Geometry. https://math.stanford.edu/~vakil/216blog/FOAGjul2724public.pdf, 2024. July 27, 2024 version.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *International symposium on symbolic and algebraic manipulation*, pages 216–226. Springer, 1979.

[ZS75] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Volume I.* Graduate Texts in Mathematics. Springer New York, 1975.

A Proof of Lemma 3.6

We now prove Lemma 3.6. First, we introduce some notation. Let $R = \mathbb{F}[\mathbf{Y}] \subseteq \mathbb{K} = \mathbb{F}(\mathbf{Y})$. For an irreducible polynomial $a \in R$ and $b \in \mathbb{K}^\times$, define $\mathrm{ord}_a(b)$ to be the unique integer r such that b can be written as $b = a^r \frac{s}{t}$, where $s \in R$ and $t \in R \setminus \{0\}$ are not divisible by a. For a univariate polynomial $f \in \mathbb{K}[X] \setminus \{0\}$ and an irreducible polynomial $a \in R$ in $\mathbf{Y}$, define $\mathrm{ord}_a(f) := \min_c(\mathrm{ord}_a(c))$, where c ranges over the nonzero coefficients of f. Finally, denote by $\mathrm{cont}(f)$ the *content* of f, defined as

$$\mathrm{cont}(f) := \prod_a a^{\mathrm{ord}_a(f)}$$

with the product taken over the irreducible polynomials $a \in R$ such that $\mathrm{ord}_a(f) \neq 0$. If two such polynomials differ by a unit factor, only one representative is included in the product. Note that $\mathrm{cont}(f)$ is well-defined up to multiplication by a unit of R. Also note that by definition, $f \in R[X]$ as long as $\mathrm{cont}(f) \in R$.

We need the following version of Gauss's lemma, which holds more generally when R is a UFD [Lan93, Theorem 2.1].

Lemma A.1 (Gauss's lemma)**.** $\mathrm{cont}(gh) = \mathrm{cont}(g)\mathrm{cont}(h)$ *for nonzero univariate polynomials* $g, h \in \mathbb{K}[X]$.

Proof of Lemma 3.6. Consider the Kronecker map $\phi : \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}[X]$, which is the $\mathbb{K}$-linear ring homomorphism sending X_i to $X^{(d+1)^i}$ for i. We have $\phi(f) = \phi(g) \cdot \phi(f/g)$. The terms of f (resp. g) correspond one-to-one to the terms of $\phi(f)$ (resp. $\phi(g)$), preserving coefficients. And the degree of $\phi(f)$ is at most $(d+1)^n = O_{d,n}(1)$. This reduces the problem to the univariate case.

Now we prove the lemma for the univariate case. Let $f \in \mathbb{K}[X]$ be a nonzero polynomial in $P(d, d')$. Let g be a factor of f. Recall that $R = \mathbb{F}[\mathbf{Y}]$. Let s be the least common multiple of all the denominators of the nonzero coefficients of f, so that $sf \in R[X]$. Let $t = \mathrm{cont}(sf) \in R \setminus \{0\}$. Then $\mathrm{cont}(\frac{s}{t}f) = 1$. Note that the coefficients of $\frac{s}{t}f$ are polynomials in $\mathbb{F}[\mathbf{Y}]$ of degree at most $d'' := (d+1)d'$. Let $c = \frac{1}{\mathrm{cont}(g)} \in \mathbb{K}^\times$. Then $\mathrm{cont}(cg) = 1$. Let $h = \frac{s}{ct} \cdot \frac{f}{g}$, so that $\frac{s}{t}f = (cg)h$. As $\mathrm{cont}(\frac{s}{t}f) = 1$ and $\mathrm{cont}(cg) = 1$, we have $\mathrm{cont}(h) = 1$ by Lemma A.1. In particular, $\frac{s}{t}f$, cg, and h are all in $R[X]$.

Write $cg = \sum_{i=0}^{\deg(cg)} a_i X^i$ and $h = \sum_{j=0}^{\deg(h)} b_j X^i$ with $a_i, b_j \in R$. Let $D = \max_{0 \leq i \leq \deg(cg)} \deg_{\mathbf{Y}}(a_i)$ and $D' = \max_{0 \leq j \leq \deg(h)} \deg_{\mathbf{Y}}(b_j)$. Choose the maximal $i_0 \in \{0, 1, \ldots, \deg(cg)\}$ such that a_{i_0} has a nonzero degree-D homogeneous component, and let H be this homogeneous component. Similarly, choose the maximal $j_0 \in \{0, 1, \ldots, \deg(h)\}$ such that b_{j_0} has a nonzero degree-D' homogeneous component, and let H' be this homogeneous component. By the maximality of D, D', i_0, and j_0, the degree-$(D + D')$ homogeneous component of the coefficient of $X^{i_0+j_0}$ in $(cg) \cdot h = \frac{s}{t}f$ is exactly $H \cdot H' \neq 0$. However, we know that the coefficients of $\frac{s}{t}f$ all have degrees at most d''. So

$$D + D' \leq d''.$$

Therefore, the coefficients of cg are all polynomials in $\mathbb{F}[\mathbf{Y}]$ of degree at most $D \leq d''$. In particular, $cg \in P(d, d'')$, where $d'' = (d+1)d' \in O_{d,d'}(1)$. □